8

The Principle of Inclusion and Exclusion

We now return to the topic of enumeration as we investigate the *Principle of Inclusion and Exclusion.* Extending the ideas in the counting problems on Venn diagrams in Chapter 3, this principle will assist us in establishing the formula we conjectured in Section 5.3 for the number of onto functions $f: A \to B$, where A, B are finite (nonempty) sets. Other applications of this principle will demonstrate its versatile nature in combinatorial mathematics.

8.1 The Principle of Inclusion and Exclusion

In this section we develop some notation for stating this new counting principle. Then we establish the principle by a combinatorial argument. Following this, a wide range of examples demonstrate how this principle may be applied.

We shall motivate the Principle of Inclusion and Exclusion with a series of three examples, the first two of which will be reminiscent of the work we did with counting and Venn diagrams in Section 3.3.

EXAMPLE 8.1

Let S represent the set of 100 students enrolled in the freshman engineering program at Central College. Then $|S| = 100$. Now let c_1, c_2 denote the following conditions (or properties) satisfied by some of the elements of S:

c_1: A student at Central College is among the 100 students in the freshman engineering program and is enrolled in Freshman Composition.

c_2: A student at Central College is among the 100 students in the freshman engineering program and is enrolled in Introduction to Economics.

Suppose that 35 of these 100 students are enrolled in Freshman Composition and that 30 of them are enrolled in Introduction to Economics. We shall denote this by

$$N(c_1) = 35 \quad \text{and} \quad N(c_2) = 30.$$

If nine of these 100 students are enrolled in both Freshman Composition and Introduction to Economics then we write $N(c_1c_2) = 9$.

Further, of these 100 students, there are $100 - 35 = 65$ who are *not* taking Freshman Composition. Denoting $|S|$ by N, we can designate this by writing $N(\bar{c}_1) = N - N(c_1)$. In a similar way we designate that there are $N(\bar{c}_2) = N - N(c_2) = 100 - 30 = 70$ of these students who are not taking Introduction to Economics. The number who *are* taking Freshman Composition and who are *not* taking Introduction to Economics is $N(c_1\bar{c}_2) = N(c_1) - N(c_1c_2) = 35 - 9 = 26$. Likewise, of these 100 students, there are $N(\bar{c}_1c_2) = N(c_2) - N(c_1c_2) = 30 - 9 = 21$ who are enrolled in Introduction to Economics but not in Freshman Composition. Of particular interest are those students (from among these 100 freshmen) who are taking neither Freshman Composition nor Introduction to Economics—that is, they are *not* taking Freshman Composition and they are also *not* taking Introduction to Economics. Their number is $N(\bar{c}_1\bar{c}_2)$. And since $N(\bar{c}_1) = N(\bar{c}_1c_2) + N(\bar{c}_1\bar{c}_2)$, we learn that $N(\bar{c}_1\bar{c}_2) = N(\bar{c}_1) - N(\bar{c}_1c_2) = 65 - 21 = 44$.

The preceding observations also demonstrate that

$$\begin{aligned} N(\bar{c}_1\bar{c}_2) &= N(\bar{c}_1) - N(\bar{c}_1c_2) = [N - N(c_1)] - [N(c_2) - N(c_1c_2)] \\ &= N - N(c_1) - N(c_2) + N(c_1c_2) = N - [N(c_1) + N(c_2)] + N(c_1c_2) \\ &= 100 - [35 + 30] + 9 = 44, \text{ as we saw above.} \end{aligned}$$

From the Venn diagram in Fig. 8.1, we see that if $N(c_1)$ denotes the number of elements of S in the left-hand circle and $N(c_2)$ denotes the number in the right-hand circle, then $N(c_1c_2)$ is the number of these elements from S in the overlap, while $N(\bar{c}_1\bar{c}_2)$ counts those elements of S that are outside the union of these two circles. Consequently, we see once again—this time from the figure—that

$$N(\bar{c}_1\bar{c}_2) = N - [N(c_1) + N(c_2)] + N(c_1c_2),$$

where the last term is added on because it was eliminated twice in the term $[N(c_1) + N(c_2)]$. (Also, at this point, the reader may wish to look back at the second formula following Example 3.25 to find the same result presented with a different notation.)

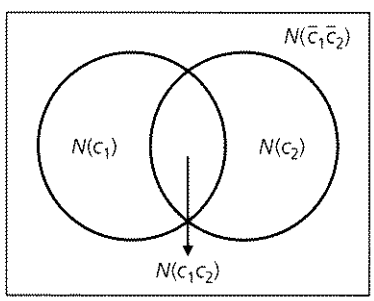


Figure 8.1

[Before we advance to our next example where we will introduce a third condition, let us note that $N(\bar{c}_1\bar{c}_2)$ is *not* the same as $N(\overline{c_1c_2})$. For $N(\overline{c_1c_2}) = N - N(c_1c_2) = 100 - 9 = 91$, in this example, while $N(\bar{c}_1\bar{c}_2) = 44$, as we learned earlier. However, $N(\bar{c}_1 \text{ or } \bar{c}_2) = N(\overline{c_1c_2}) = 91 = 65 + 70 - 44 = N(\bar{c}_1) + N(\bar{c}_2) - N(\bar{c}_1\bar{c}_2)$.]

EXAMPLE 8.2

We start with the same 100 students as in Example 8.1 and the same conditions c_1, c_2, but now we consider a third condition, given as follows:

c_3: A student at Central College is among the 100 students in the freshman engineering program and is enrolled in Fundamentals of Computer Programming.

It is still the case that $N(c_1) = 35$, $N(c_2) = 30$, and $N(c_1c_2) = 9$, but now we are also given that $N(c_3) = 30$, $N(c_1c_3) = 11$, $N(c_2c_3) = 10$, and $N(c_1c_2c_3) = 5$ (that is, there are five of these 100 freshmen who are taking Freshman Composition, Introduction to Economics, and Fundamentals of Computer Programming). Looking to Fig. 8.2, we learn that

$$N(\bar{c}_1\bar{c}_2\bar{c}_3) = N - [N(c_1) + N(c_2) + N(c_3)] + [N(c_1c_2) + N(c_1c_3) + N(c_2c_3)] - N(c_1c_2c_3).$$

So here we have $N(\bar{c}_1\bar{c}_2\bar{c}_3) = 100 - [35 + 30 + 30] + [9 + 11 + 10] - 5 = 30$. That is, out of these 100 students there are 30 who are *not* enrolled in any of the courses: (i) Freshman Composition; (ii) Introduction to Economics; or (iii) Fundamentals of Computer Programming.

[We also learn here that $N(\bar{c}_3) = 70 = 100 - 30 = N - N(c_3)$, $N(\bar{c}_1\bar{c}_3) = 46 = 100 - [35 + 30] + 11 = N - [N(c_1) + N(c_3)] + N(c_1c_3)$, and $N(\bar{c}_2\bar{c}_3) = 50 = 100 - [30 + 30] + 10 = N - [N(c_2) + N(c_3)] + N(c_2c_3)$. Furthermore, we note the similarity here with the result for $|\overline{A} \cap \overline{B} \cap \overline{C}|$ given in the second formula following Example 3.26.]

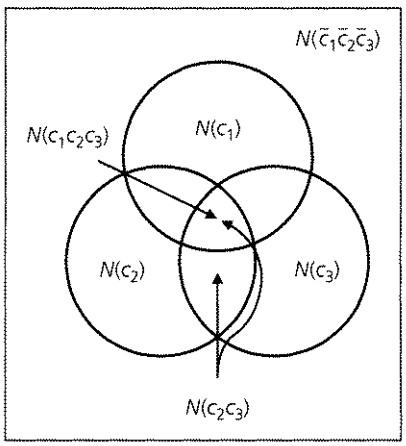


Figure 8.2

EXAMPLE 8.3

Based on the results in the previous two examples we may now feel that for a given finite set S (with $|S| = N$) and four conditions c_1, c_2, c_3, c_4 we should have

$$\begin{aligned} N(\bar{c}_1\bar{c}_2\bar{c}_3\bar{c}_4) = N &- [N(c_1) + N(c_2) + N(c_3) + N(c_4)] \qquad (*) \\ &+ [N(c_1c_2) + N(c_1c_3) + N(c_1c_4) + N(c_2c_3) + N(c_2c_4) + N(c_3c_4)] \\ &- [N(c_1c_2c_3) + N(c_1c_2c_4) + N(c_1c_3c_4) + N(c_2c_3c_4)] \\ &+ N(c_1c_2c_3c_4). \end{aligned}$$

To show that this is the case we consider an arbitrary element x from S and show that it is counted the same number of times on both sides of the above equation.

0) If x satisfies none of the four conditions, then it is counted once on the left side of Eq. (*) [in $N(\bar{c}_1\bar{c}_2\bar{c}_3\bar{c}_4)$], and once on the right side of Eq. (*) [in N].

1) If x satisfies only one of the conditions, say c_1, then it is not counted at all on the left side of Eq. (*). But on the right side of Eq. (*), x is counted once in N and once in $N(c_1)$, for a total of $1 - 1 = 0$ times.

2) Now suppose that x satisfies conditions c_2, c_4 but does *not* satisfy conditions c_1, c_3. Once again x is not counted on the left side of Eq. (*). For the right side of Eq. (*), x is counted once in N, once in each of $N(c_2)$ and $N(c_4)$, and then once in $N(c_2c_4)$, totaling $1 - [1 + 1] + 1 = 1 - \binom{2}{1} + \binom{2}{2} = 0$ times.

3) Continuing with the case for three conditions, we'll suppose here that x satisfies conditions c_1, c_2, and c_4, but *not* c_3. As in the previous two cases, x is not counted on the left side of Eq. (*). On the right side of Eq. (*), x is counted once in N, once in each of $N(c_1)$, $N(c_2)$, and $N(c_4)$, once in each of $N(c_1c_2)$, $N(c_1c_4)$, and $N(c_2c_4)$, and, finally, once in $N(c_1c_2c_4)$. So on the right side of Eq. (*), x is counted $1 - [1 + 1 + 1] + [1 + 1 + 1] - 1 = 1 - \binom{3}{1} + \binom{3}{2} - \binom{3}{3} = 0$ times, in total.

4) Finally, if x satisfies all four of the conditions c_1, c_2, c_3, c_4, then once again it is not counted on the left side of Eq. (*). On the right side of Eq. (*), x is counted once for each of the 16 terms on the right side of this equation — for a total of $1 - [1 + 1 + 1 + 1] + [1 + 1 + 1 + 1 + 1 + 1] - [1 + 1 + 1 + 1] + 1 = 1 - \binom{4}{1} + \binom{4}{2} - \binom{4}{3} + \binom{4}{4} = 0$ times.

   Consequently, from these preceding five cases we have shown that the two sides of Eq. (*) count the same elements from S, and this provides a combinatorial proof for the formula for $N(\overline{c}_1\overline{c}_2\overline{c}_3\overline{c}_4)$.

So now we shall reconsider the situation in Example 8.2 and introduce a fourth condition as follows:

c_4: A student at Central College is among the 100 students in the freshman engineering program and is enrolled in Introduction to Design.

We already know that $N(c_1) = 35$, $N(c_2) = 30$, $N(c_3) = 30$, $N(c_1c_2) = 9$, $N(c_1c_3) = 11$, $N(c_2c_3) = 10$, and $N(c_1c_2c_3) = 5$. If $N(c_4) = 41$, $N(c_1c_4) = 13$, $N(c_2c_4) = 14$, $N(c_3c_4) = 10$, $N(c_1c_2c_4) = 6$, $N(c_1c_3c_4) = 6$, $N(c_2c_3c_4) = 6$, and $N(c_1c_2c_3c_4) = 4$, then, using the equation we derived above, it follows that $N(\overline{c}_1\overline{c}_2\overline{c}_3\overline{c}_4) = 100 - [35 + 30 + 30 + 41] + [9 + 11 + 13 + 10 + 14 + 10] - [5 + 6 + 6 + 6] + 4 = 100 - 136 + 67 - 23 + 4 = 12$. Thus, of the 100 students in the freshman engineering program at Central College, there are 12 who are not taking any of the four courses: Freshman Composition, Introduction to Economics, Fundamentals of Computer Programming, or Introduction to Design.

If we are interested in the number (from these 100 students) who are taking Freshman Composition, but none of the other three courses, then we should want to compute $N(c_1\overline{c}_2\overline{c}_3\overline{c}_4)$. To do so we start by observing that

$$N(\overline{c}_2\overline{c}_3\overline{c}_4) = N(c_1\overline{c}_2\overline{c}_3\overline{c}_4) + N(\overline{c}_1\overline{c}_2\overline{c}_3\overline{c}_4),$$

which can be established by an argument similar to the one above for $N(\overline{c}_1\overline{c}_2\overline{c}_3\overline{c}_4)$. This then leads us to

$$N(c_1\overline{c}_2\overline{c}_3\overline{c}_4) = N(\overline{c}_2\overline{c}_3\overline{c}_4) - N(\overline{c}_1\overline{c}_2\overline{c}_3\overline{c}_4).$$

Using the result in Example 8.2 we find that

$$\begin{aligned} N(\overline{c}_2\overline{c}_3\overline{c}_4) &= N - [N(c_2) + N(c_3) + N(c_4)] + [N(c_2c_3) + N(c_2c_4) + N(c_3c_4)] \\ &\quad - N(c_2c_3c_4) \\ &= 100 - [30 + 30 + 41] + [10 + 14 + 10] - 6 = 27, \text{ and} \\ N(c_1\overline{c}_2\overline{c}_3\overline{c}_4) &= N(\overline{c}_2\overline{c}_3\overline{c}_4) - N(\overline{c}_1\overline{c}_2\overline{c}_3\overline{c}_4) = 27 - 12 = 15. \end{aligned}$$

So there are 15 students in this set of 100 who are taking Freshman Composition, but none of the other courses: Introduction to Economics, Fundamentals of Computer Programming, or Introduction to Design.

Further, we also observe that

$$\begin{aligned}
N(c_1\bar{c}_2\bar{c}_3\bar{c}_4) &= N(\bar{c}_2\bar{c}_3\bar{c}_4) - N(\bar{c}_1\bar{c}_2\bar{c}_3\bar{c}_4) \\
&= \big\{N - [N(c_2) + N(c_3) + N(c_4)] + [N(c_2c_3) + N(c_2c_4) + N(c_3c_4)] \\
&\quad - N(c_2c_3c_4)\big\} - \big\{N - [N(c_1) + N(c_2) + N(c_3) + N(c_4)] \\
&\quad + [N(c_1c_2) + N(c_1c_3) + N(c_1c_4) + N(c_2c_3) + N(c_2c_4) + N(c_3c_4)] \\
&\quad - [N(c_1c_2c_3) + N(c_1c_2c_4) + N(c_1c_3c_4) + N(c_2c_3c_4)] + N(c_1c_2c_3c_4)\big\}, \text{ or} \\
N(c_1\bar{c}_2\bar{c}_3\bar{c}_4) &= N(c_1) - [N(c_1c_2) + N(c_1c_3) + N(c_1c_4)] \\
&\quad + [N(c_1c_2c_3) + N(c_1c_2c_4) + N(c_1c_3c_4)] - N(c_1c_2c_3c_4).
\end{aligned}$$

So here $N(c_1\bar{c}_2\bar{c}_3\bar{c}_4) = 35 - [9 + 11 + 13] + [5 + 6 + 6] - 4 = 35 - 33 + 17 - 4 = 15$, as we found above.

Having seen the results in Examples 8.1, 8.2, and 8.3, now it is time for us to generalize these results and establish the Principle of Inclusion and Exclusion. To do so we once again let S be a set with $|S| = N$, and we let $c_1, c_2, \ldots, c_t$ be a collection of t conditions or properties — each of which may be satisfied by some of the elements of S. Some elements of S may satisfy more than one of the conditions, whereas others may not satisfy any of them. For all $1 \le i \le t$, $N(c_i)$ will denote the number of elements in S that satisfy condition c_i. (Elements of S are counted here when they satisfy only condition c_i, as well as when they satisfy c_i and other conditions c_j, for $j \ne i$.) For all $i, j \in \{1, 2, 3, \ldots, t\}$ where $i \ne j$, $N(c_ic_j)$ will denote the number of elements in S that satisfy both of the conditions c_i, c_j, and perhaps some others. [$N(c_ic_j)$ does *not* count the elements of S that satisfy *only* c_i, c_j.] Continuing, if $1 \le i, j, k \le t$ are three distinct integers, then $N(c_ic_jc_k)$ denotes the number of elements in S satisfying, perhaps among others, each of the conditions c_i, c_j, and c_k.

For each $1 \le i \le t$, $N(\bar{c}_i) = N - N(c_i)$ denotes the number of elements in S that do not satisfy condition c_i. If $1 \le i, j \le t$ with $i \ne j$, $N(\bar{c}_i\bar{c}_j)$ = the number of elements in S that do not satisfy either of the conditions c_i or c_j. [This is *not* the same as $N(\overline{c_ic_j})$, as we observed at the end of Example 8.1.]

With the necessary preliminaries now in hand we state the following theorem.

THEOREM 8.1 *The Principle of Inclusion and Exclusion.* Consider a set S, with $|S| = N$, and conditions c_i, $1 \le i \le t$, each of which may be satisfied by some of the elements of S. The number of elements of S that satisfy *none* of the conditions c_i, $1 \le i \le t$, is denoted by $\overline{N} = N(\bar{c}_1\bar{c}_2\bar{c}_3 \cdots \bar{c}_t)$ where

$$\begin{aligned}
\overline{N} = N &- [N(c_1) + N(c_2) + N(c_3) + \cdots + N(c_t)] \\
&+ [N(c_1c_2) + N(c_1c_3) + \cdots + N(c_1c_t) + N(c_2c_3) + \cdots + N(c_{t-1}c_t)] \\
&- [N(c_1c_2c_3) + N(c_1c_2c_4) + \cdots + N(c_1c_2c_t) + N(c_1c_3c_4) + \cdots \\
&+ N(c_1c_3c_t) + \cdots + N(c_{t-2}c_{t-1}c_t)] + \cdots + (-1)^t N(c_1c_2c_3 \cdots c_t),
\end{aligned} \tag{1}$$

or

$$\overline{N} = N - \sum_{1 \le i \le t} N(c_i) + \sum_{1 \le i < j \le t} N(c_i c_j) - \sum_{1 \le i < j < k \le t} N(c_i c_j c_k) + \cdots \tag{2}$$
$$+ (-1)^t N(c_1 c_2 c_3 \cdots c_t).$$

Proof: Although this result can be established by applying the Principle of Mathematical Induction to the number t of conditions, we shall give a combinatorial proof. The argument will be reminiscent of the ideas we saw in Example 8.3 in establishing the formula for $N(\overline{c}_1 \overline{c}_2 \overline{c}_3 \overline{c}_4)$.

For each $x \in S$ we show that x contributes the same count, either 0 or 1, to each side of Eq. (2).

If x satisfies none of the conditions, then x is counted once in $\overline{N}$ and once in N, but not in any of the other terms in Eq. (2). Consequently, x contributes a count of 1 to each side of the equation.

The other possibility is that x satisfies *exactly* r of the conditions where $1 \le r \le t$. In this case x contributes nothing to $\overline{N}$. But on the right-hand side of Eq. (2), x is counted

(1) One time in N.

(2) r times in $\sum_{1 \le i \le t} N(c_i)$. (Once for each of the r conditions.)

(3) $\binom{r}{2}$ times in $\sum_{1 \le i < j \le t} N(c_i c_j)$. (Once for each pair of conditions selected from the r conditions it satisfies.)

(4) $\binom{r}{3}$ times in $\sum_{1 \le i < j < k \le t} N(c_i c_j c_k)$. (Why?)

. . . . . .

($r+1$) $\binom{r}{r} = 1$ time in $\sum N(c_{i_1} c_{i_2} \cdots c_{i_r})$, where the summation is taken over all selections of size r from the t conditions.

Consequently, on the right-hand side of Eq. (2), x is counted

$$1 - r + \binom{r}{2} - \binom{r}{3} + \cdots + (-1)^r \binom{r}{r} = [1 + (-1)]^r = 0^r = 0 \text{ times},$$

by the binomial theorem. Therefore, the two sides of Eq. (2) count the same elements from S, and the equality is verified.

An immediate corollary of this principle is given as follows:

COROLLARY 8.1 Under the hypotheses of Theorem 8.1, the number of elements in S that satisfy at least one of the conditions c_i, where $1 \le i \le t$, is given by $N(c_1 \text{ or } c_2 \text{ or } \ldots \text{ or } c_t) = N - \overline{N}$.

Before solving some examples, we examine some further notation for simplifying the statement of Theorem 8.1.

We write

$$S_0 = N,$$
$$S_1 = [N(c_1) + N(c_2) + \cdots + N(c_t)],$$
$$S_2 = [N(c_1c_2) + N(c_1c_3) + \cdots + N(c_1c_t) + N(c_2c_3) + \cdots + N(c_{t-1}c_t)],$$

and, in general,

$$S_k = \sum N(c_{i_1}c_{i_2}\cdots c_{i_k}),\ 1 \le k \le t,$$

where the summation is taken over all selections of size k from the collection of t conditions. Hence S_k has $\binom{t}{k}$ summands in it.

Using this notation we can rewrite the result in Eq. (2) as

$$\overline{N} = S_0 - S_1 + S_2 - S_3 + \cdots + (-1)^t S_t.$$

Now let us look at how this principle is used to solve certain enumeration problems.

EXAMPLE 8.4

Determine the number of positive integers n where $1 \le n \le 100$ and n is *not* divisible by 2, 3, or 5.

Here $S = \{1, 2, 3, \ldots, 100\}$ and $N = 100$. For $n \in S$, n satisfies

a) condition c_1 if n is divisible by 2,

b) condition c_2 if n is divisible by 3, and

c) condition c_3 if n is divisible by 5.

Then the answer to this problem is $N(\overline{c}_1\overline{c}_2\overline{c}_3)$.

As in Section 5.2 we use the notation $\lfloor r \rfloor$ to denote the greatest integer less than or equal to r, for any real number r. This function proves to be helpful in this problem as we find that

$N(c_1) = \lfloor 100/2 \rfloor = 50$ [since the 50 ($= \lfloor 100/2 \rfloor$) positive integers 2, 4, 6, 8, ..., 96, 98 ($= 2 \cdot 49$), 100 ($= 2 \cdot 50$) are divisible by 2];

$N(c_2) = \lfloor 100/3 \rfloor = \lfloor 33\ 1/3 \rfloor = 33$ [since the 33 ($= \lfloor 100/3 \rfloor$) positive integers 3, 6, 9, 12, ..., 96 ($= 3 \cdot 32$), 99 ($= 3 \cdot 33$) are divisible by 3];

$N(c_3) = \lfloor 100/5 \rfloor = 20$;

$N(c_1c_2) = \lfloor 100/6 \rfloor = 16$ [since there are 16 ($= \lfloor 100/6 \rfloor$) elements in S that are divisible by both 2 and 3—hence divisible by $\text{lcm}(2, 3) = 2 \cdot 3 = 6$];

$N(c_1c_3) = \lfloor 100/10 \rfloor = 10$;

$N(c_2c_3) = \lfloor 100/15 \rfloor = 6$; and

$N(c_1c_2c_3) = \lfloor 100/30 \rfloor = 3$.

Applying the Principle of Inclusion and Exclusion, we find that

$$\begin{aligned} N(\overline{c}_1\overline{c}_2\overline{c}_3) &= S_0 - S_1 + S_2 - S_3 = N - [N(c_1) + N(c_2) + N(c_3)] \\ &\quad + [N(c_1c_2) + N(c_1c_3) + N(c_2c_3)] - N(c_1c_2c_3) \\ &= 100 - [50 + 33 + 20] + [16 + 10 + 6] - 3 = 26. \end{aligned}$$

(These 26 numbers are 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 77, 79, 83, 89, 91, and 97.)

EXAMPLE 8.5

In Chapter 1 we found the number of nonnegative integer solutions to the equation $x_1 + x_2 + x_3 + x_4 = 18$. We now answer the same question with the extra restriction that $x_i \le 7$, for all $1 \le i \le 4$.

Here S is the set of solutions of $x_1 + x_2 + x_3 + x_4 = 18$, with $0 \le x_i$ for all $1 \le i \le 4$. So $|S| = N = S_0 = \binom{4+18-1}{18} = \binom{21}{18}$.

We say that a solution x_1, x_2, x_3, x_4 satisfies condition c_i, where $1 \le i \le 4$, if $x_i > 7$ (or $x_i \ge 8$). The answer to the problem is then $N(\overline{c}_1\overline{c}_2\overline{c}_3\overline{c}_4)$.

Here by symmetry $N(c_1) = N(c_2) = N(c_3) = N(c_4)$. To compute $N(c_1)$, we consider the integer solutions for $x_1 + x_2 + x_3 + x_4 = 10$, with each $x_i \ge 0$ for all $1 \le i \le 4$. Then we add 8 to the value of x_1 and get the solutions of $x_1 + x_2 + x_3 + x_4 = 18$ that satisfy condition c_1. Hence $N(c_i) = \binom{4+10-1}{10} = \binom{13}{10}$, for each $1 \le i \le 4$, and $S_1 = \binom{4}{1}\binom{13}{10}$.

Likewise, $N(c_1c_2)$ is the number of integer solutions of $x_1 + x_2 + x_3 + x_4 = 2$, where $x_i \ge 0$ for all $1 \le i \le 4$. So $N(c_1c_2) = \binom{4+2-1}{2} = \binom{5}{2}$, and $S_2 = \binom{4}{2}\binom{5}{2}$.

Since $N(c_ic_jc_k) = 0$ for every selection of three conditions, and $N(c_1c_2c_3c_4) = 0$, we have

$$N(\overline{c}_1\overline{c}_2\overline{c}_3\overline{c}_4) = S_0 - S_1 + S_2 - S_3 + S_4 = \binom{21}{18} - \binom{4}{1}\binom{13}{10} + \binom{4}{2}\binom{5}{2} - 0 + 0 = 246.$$

So of the 1330 nonnegative integer solutions of $x_1 + x_2 + x_3 + x_4 = 18$, only 246 of them satisfy $x_i \le 7$ for each $1 \le i \le 4$.

Our next example establishes the formula conjectured in Section 5.3 for counting onto functions.

EXAMPLE 8.6

For finite sets A, B, where $|A| = m \ge n = |B|$, let $A = \{a_1, a_2, \ldots, a_m\}$, $B = \{b_1, b_2, \ldots, b_n\}$, and $S =$ the set of all functions $f: A \to B$. Then $N = S_0 = |S| = n^m$.

For all $1 \le i \le n$, let c_i denote the condition on S where a function $f: A \to B$ satisfies c_i if b_i is *not* in the range of f. (Note the difference between c_i here and c_i in Examples 8.4 and 8.5.) Then $N(\overline{c}_i)$ is the number of functions in S that have b_i in their range, and $N(\overline{c}_1\overline{c}_2 \cdots \overline{c}_n)$ counts the number of onto functions $f: A \to B$.

For all $1 \le i \le n$, $N(c_i) = (n-1)^m$, because each element of B, except b_i, can be used as the second component of an ordered pair for a function $f: A \to B$, whose range does not include b_i. Likewise, for all $1 \le i < j \le n$, there are $(n-2)^m$ functions $f: A \to B$ whose range contains neither b_i nor b_j. From these observations we have $S_1 = [N(c_1) + N(c_2) + \cdots + N(c_n)] = n(n-1)^m = \binom{n}{1}(n-1)^m$, and $S_2 = [N(c_1c_2) + N(c_1c_3) + \cdots + N(c_1c_n) + N(c_2c_3) + \cdots + N(c_2c_n) + \cdots + N(c_{n-1}c_n)] = \binom{n}{2}(n-2)^m$. In general, for each $1 \le k \le n$,

$$S_k = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} N(c_{i_1}c_{i_2} \cdots c_{i_k}) = \binom{n}{k}(n-k)^m.$$

It then follows by the Principle of Inclusion and Exclusion that the number of onto

functions from A to B is

$$\begin{aligned} N(\bar{c}_1\bar{c}_2\bar{c}_3\cdots\bar{c}_n) &= S_0 - S_1 + S_2 - S_3 + \cdots + (-1)^n S_n \\ &= n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \binom{n}{3}(n-3)^m \\ &\quad + \cdots + (-1)^n(n-n)^m = \sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)^m \\ &= \sum_{i=0}^{n}(-1)^i\binom{n}{n-i}(n-i)^m. \end{aligned}$$

Before we finish discussing this example, let us note that

$$\sum_{i=0}^{n}(-1)^i\binom{n}{n-i}(n-i)^m$$

can also be evaluated even if $m < n$. Furthermore, for $m < n$, the expression

$$N(\bar{c}_1\bar{c}_2\bar{c}_3\cdots\bar{c}_n)$$

still counts the number of functions $f\colon A \to B$, where $|A| = m$, $|B| = n$, and each element of B is in the range of f. But now this number is 0.

For example, suppose that $m = 3 < 7 = n$. Then $N(\bar{c}_1\bar{c}_2\bar{c}_3\cdots\bar{c}_7)$ counts the number of onto functions $f\colon A \to B$ for $|A| = 3$ and $|B| = 7$. We know this number is 0, and we also find that

$$\begin{aligned} \sum_{i=0}^{7}(-1)^i\tbinom{7}{7-i}(7-i)^3 &= \tbinom{7}{7}7^3 - \tbinom{7}{6}6^3 + \tbinom{7}{5}5^3 - \tbinom{7}{4}4^3 + \tbinom{7}{3}3^3 - \tbinom{7}{2}2^3 + \tbinom{7}{1}1^3 - \tbinom{7}{0}0^3 \\ &= 343 - 1512 + 2625 - 2240 + 945 - 168 + 7 - 0 = 0. \end{aligned}$$

Hence, for all $m, n \in \mathbf{Z}^+$, if $m < n$, then

$$\sum_{i=0}^{n}(-1)^i\binom{n}{n-i}(n-i)^m = 0.$$

We now solve a problem similar to those in Chapter 3 that dealt with Venn diagrams.

EXAMPLE 8.7

In how many ways can the 26 letters of the alphabet be permuted so that none of the patterns *car*, *dog*, *pun*, or *byte* occurs?

Let S denote the set of all permutations of the 26 letters. Then $|S| = 26!$ For each $1 \le i \le 4$, a permutation in S is said to satisfy condition c_i if the permutation contains the pattern *car*, *dog*, *pun*, or *byte*, respectively.

In order to compute $N(c_1)$, for example, we count the number of ways the 24 symbols *car*, $b, d, e, f, \ldots, p, q, s, t, \ldots, x, y, z$ can be permuted. So $N(c_1) = 24!$, and in a similar way we obtain

$$N(c_2) = N(c_3) = 24!, \quad \text{while } N(c_4) = 23!$$

For $N(c_1c_2)$ we deal with the 22 symbols *car*, *dog*, $b, e, f, h, i, \ldots, m, n, p, q, s, t, \ldots, x, y, z$, which can be permuted in 22! ways. Hence $N(c_1c_2) = 22!$, and comparable calculations give

$$N(c_1c_3) = N(c_2c_3) = 22!, \qquad N(c_ic_4) = 21!, \quad i \ne 4.$$

Furthermore,

$$N(c_1c_2c_3) = 20!, \qquad N(c_ic_jc_4) = 19!, \qquad 1 \le i < j \le 3,$$
$$N(c_1c_2c_3c_4) = 17!$$

So the number of permutations in S that contain none of the given patterns is

$$N(\bar{c}_1\bar{c}_2\bar{c}_3\bar{c}_4) = 26! - [3(24!) + 23!] + [3(22!) + 3(21!)] - [20! + 3(19!)] + 17!$$

Our next example deals with a number theory problem.

EXAMPLE 8.8

For $n \in \mathbf{Z}^+$, $n \ge 2$, let $\phi(n)$ be the number of positive integers m, where $1 \le m < n$ and $\gcd(m, n) = 1$ — that is, m, n are relatively prime. This function is known as *Euler's phi function*, and it arises in several situations in abstract algebra involving enumeration. We find that $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, and $\phi(6) = 2$. For each prime p, $\phi(p) = p - 1$. We would like to derive a formula for $\phi(n)$ that is related to n so that we need not make a case-by-case comparison for each m, $1 \le m < n$, against the integer n.

The derivation of our formula will use the Principle of Inclusion and Exclusion as in Example 8.4. We proceed as follows: For $n \ge 2$, use the Fundamental Theorem of Arithmetic to write $n = p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$, where $p_1, p_2, \ldots, p_t$ are distinct primes and $e_i \ge 1$, for all $1 \le i \le t$. We consider the case where $t = 4$. This will be enough to demonstrate the general idea.

With $S = \{1, 2, 3, \ldots, n\}$, we have $N = S_0 = |S| = n$, and for each $1 \le i \le 4$ we say that $k \in S$ satisfies condition c_i if k is divisible by p_i. For $1 \le k < n$, $\gcd(k, n) = 1$ if k is not divisible by any of the primes p_i, where $1 \le i \le 4$. Hence $\phi(n) = N(\bar{c}_1\bar{c}_2\bar{c}_3\bar{c}_4)$.

For each $1 \le i \le 4$, we have $N(c_i) = n/p_i$; $N(c_ic_j) = n/(p_ip_j)$, for all $1 \le i < j \le 4$. Also, $N(c_ic_jc_\ell) = n/(p_ip_jp_\ell)$, for all $1 \le i < j < \ell \le 4$, and $N(c_1c_2c_3c_4) = n/(p_1p_2p_3p_4)$. So

$$\begin{aligned}
\phi(n) &= S_0 - S_1 + S_2 - S_3 + S_4 \\
&= n - \left[\frac{n}{p_1} + \cdots + \frac{n}{p_4}\right] + \left[\frac{n}{p_1p_2} + \frac{n}{p_1p_3} + \cdots + \frac{n}{p_3p_4}\right] \\
&\quad - \left[\frac{n}{p_1p_2p_3} + \cdots + \frac{n}{p_2p_3p_4}\right] + \frac{n}{p_1p_2p_3p_4} \\
&= n\left[1 - \left(\frac{1}{p_1} + \cdots + \frac{1}{p_4}\right) + \left(\frac{1}{p_1p_2} + \frac{1}{p_1p_3} + \cdots + \frac{1}{p_3p_4}\right)\right. \\
&\quad \left. - \left(\frac{1}{p_1p_2p_3} + \cdots + \frac{1}{p_2p_3p_4}\right) + \frac{1}{p_1p_2p_3p_4}\right] \\
&= \frac{n}{p_1p_2p_3p_4}[p_1p_2p_3p_4 - (p_2p_3p_4 + p_1p_3p_4 + p_1p_2p_4 + p_1p_2p_3) \\
&\quad + (p_3p_4 + p_2p_4 + p_2p_3 + p_1p_4 + p_1p_3 + p_1p_2) \\
&\quad - (p_4 + p_3 + p_2 + p_1) + 1] \\
&= \frac{n}{p_1p_2p_3p_4}[(p_1 - 1)(p_2 - 1)(p_3 - 1)(p_4 - 1)] \\
&= n\left[\frac{p_1 - 1}{p_1} \cdot \frac{p_2 - 1}{p_2} \cdot \frac{p_3 - 1}{p_3} \cdot \frac{p_4 - 1}{p_4}\right] = n\prod_{i=1}^{4}\left(1 - \frac{1}{p_i}\right).
\end{aligned}$$

In general, $\phi(n) = n \prod_{p|n}(1 - (1/p))$, where the product is taken over all primes p dividing n. When $n = p$, a prime, $\phi(n) = \phi(p) = p\,[1 - (1/p)] = p - 1$, as we observed earlier. If $n = 23{,}100$, for example, we find that

$$\begin{aligned}\phi(23{,}100) &= \phi(2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11)\\ &= (23{,}100)(1 - (1/2))(1 - (1/3))(1 - (1/5))(1 - (1/7))(1 - (1/11))\\ &= 4800.\end{aligned}$$

The Euler phi function has many interesting properties. We shall investigate some of them in the exercises for this section and in the Supplementary Exercises.

The next example provides another encounter with the circular arrangements introduced in Chapter 1.

EXAMPLE 8.9

Six married couples are to be seated at a circular table. In how many ways can they arrange themselves so that no wife sits next to her husband? (Here, as in Example 1.16, two seating arrangements are considered the same if one is a rotation of the other.)

For $1 \le i \le 6$, we let c_i denote the condition where a seating arrangement has couple i seated next to each other.

To determine $N(c_1)$, for instance, we consider arranging 11 distinct objects — namely, couple 1 (considered as one object) and the other 10 people. Eleven distinct objects can be arranged around a circular table in $(11 - 1)! = 10!$ ways. However, here $N(c_1) = 2(10!)$, where the 2 takes into account whether the wife in couple 1 is seated to the left or right of her husband. Similarly, $N(c_i) = 2(10!)$, for $2 \le i \le 6$, and $S_1 = \binom{6}{1}2(10!)$.

Continuing, let us now compute $N(c_i c_j)$, for $1 \le i < j \le 6$. Here we are arranging 10 distinct objects — couple i (considered as one object), couple j (likewise considered as one object), and the other eight people. Ten distinct objects can be arranged around a circular table in $(10 - 1)! = 9!$ ways. So here $N(c_i c_j) = 2^2(9!)$ because there are two ways for the wife in couple i to be seated next to her husband, and two ways for the wife in couple j to be seated next to her husband. Consequently, $S_2 = \binom{6}{2}2^2(9!)$.

Similar reasoning shows us that

$$N(c_1c_2c_3) = 2^3(8!),\ S_3 = \binom{6}{3}2^3(8!) \qquad N(c_1c_2c_3c_4) = 2^4(7!),\ S_4 = \binom{6}{4}2^4(7!)$$

$$N(c_1c_2c_3c_4c_5) = 2^5(6!),\ S_5 = \binom{6}{5}2^5(6!) \qquad N(c_1c_2c_3c_4c_5c_6) = 2^6(5!),\ S_6 = \binom{6}{6}2^6(5!).$$

With S_0 (the total number of arrangements of the 12 people) $= (12 - 1)! = 11!$, we find that the number of arrangements where no couple is seated side by side is

$$\begin{aligned}N(\bar{c}_1\bar{c}_2\cdots\bar{c}_6) &= \sum_{i=0}^{6}(-1)^i S_i = \sum_{i=0}^{6}(-1)^i\binom{6}{i}2^i(11-i)!\\ &= 39{,}916{,}800 - 43{,}545{,}600 + 21{,}772{,}800 - 6{,}451{,}200\\ &\quad + 1{,}209{,}600 - 138{,}240 + 7680\\ &= 12{,}771{,}840.\end{aligned}$$

Our final example recalls some of the graph theory we studied in Chapter 7.

EXAMPLE 8.10

In a certain area of the countryside are five villages. An engineer is to devise a system of two-way roads so that after the system is completed, no village will be isolated. In how many ways can he do this?

Calling the villages a, b, c, d, and e, we seek the number of loop-free undirected graphs on these vertices, where no vertex is isolated. Consequently, we want to count situations such as those illustrated in parts (a) and (b) of Fig. 8.3, but not situations such as those shown in parts (c) and (d).

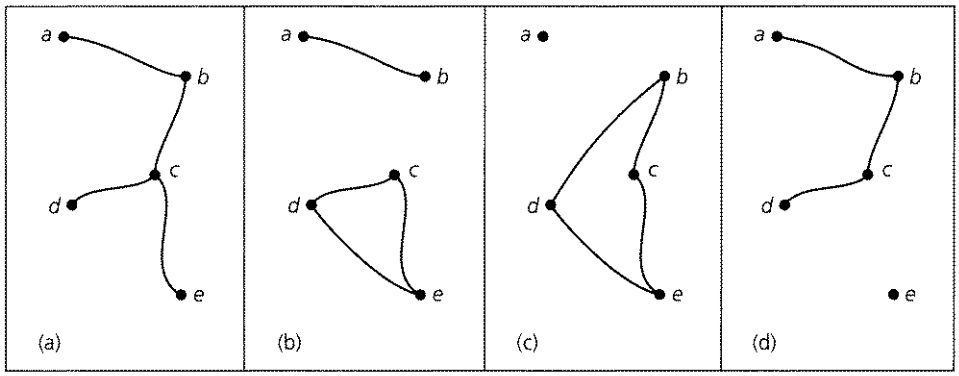


Figure 8.3

Let S be the set of loop-free undirected graphs G on $V = \{a, b, c, d, e\}$. Then $N = S_0 = |S| = 2^{10}$ because there are $\binom{5}{2} = 10$ possible two-way roads for these five villages, and each road can be either included or excluded.

For each $1 \le i \le 5$, let c_i be the condition that a system of these roads isolates village a, b, c, d, and e, respectively. Then the answer to the problem is $N(\bar{c}_1\bar{c}_2\bar{c}_3\bar{c}_4\bar{c}_5)$.

For condition c_1 village a is isolated, so we consider the six edges (roads) $\{b, c\}$, $\{b, d\}$, $\{b, e\}$, $\{c, d\}$, $\{c, e\}$, $\{d, e\}$. With two choices for each edge — namely, put the edge in the graph or leave the edge out — we find that $N(c_1) = 2^6$. Then by symmetry $N(c_i) = 2^6$ for all $2 \le i \le 5$, so $S_1 = \binom{5}{1}2^6$.

When villages a and b are to be isolated, each of the edges $\{c, d\}$, $\{d, e\}$, $\{c, e\}$ may be put in or left out of our graph. This results in 2^3 possibilities, so $N(c_1c_2) = 2^3$, and $S_2 = \binom{5}{2}2^3$.

Similar arguments tell us that $N(c_1c_2c_3) = 2^1$ and $S_3 = \binom{5}{3}2^1$; $N(c_1c_2c_3c_4) = 2^0$ and $S_4 = \binom{5}{4}2^0$; and $N(c_1c_2c_3c_4c_5) = 2^0$ and $S_5 = \binom{5}{5}2^0$.

Consequently,

$$N(\bar{c}_1\bar{c}_2\bar{c}_3\bar{c}_4\bar{c}_5) = 2^{10} - \binom{5}{1}2^6 + \binom{5}{2}2^3 - \binom{5}{3}2^1 + \binom{5}{4}2^0 - \binom{5}{5}2^0 = 768.$$

EXERCISES 8.1

1. Let S be a finite set with $|S| = N$ and let c_1, c_2, c_3, c_4 be four conditions, each of which may be satisfied by one or more of the elements of S. Prove that $N(\bar{c}_2\bar{c}_3\bar{c}_4) = N(c_1\bar{c}_2\bar{c}_3\bar{c}_4) + N(\bar{c}_1\bar{c}_2\bar{c}_3\bar{c}_4)$.

2. Establish the Principle of Inclusion and Exclusion by applying the Principle of Mathematical Induction to the number t of conditions.

3. Of the 100 students in Example 8.3, how many are taking (a) Fundamentals of Computer Programming but none of the other three courses; (b) Fundamentals of Computer Programming and Introduction to Economics but neither of the other two courses?

4. Annually, the 65 members of the maintenance staff sponsor a "Christmas in July" picnic for the 400 summer employees at their company. For these 65 people, 21 bring hot dogs, 35 bring fried chicken, 28 bring salads, 32 bring desserts, 13 bring hot dogs and fried chicken, 10 bring hot dogs and salads, 9 bring hot dogs and desserts, 12 bring fried chicken and salads, 17 bring fried chicken and desserts, 14 bring salads and desserts, 4 bring hot dogs, fried chicken, and salads, 6 bring hot dogs, fried chicken, and desserts, 5 bring hot dogs, salads, and desserts, 7 bring fried chicken, salads, and desserts, and 2 bring all four food items. Those (of the 65) who do not bring any of these four food items are responsible for setting up and cleaning up for the picnic. How many of the 65 maintenance staff will (a) help to set up and clean up for the picnic? (b) bring only hot dogs? (c) bring exactly one food item?

5. Determine the number of positive integers n, $1 \le n \le 2000$, that are

a) not divisible by 2, 3, or 5

b) not divisible by 2, 3, 5, or 7

c) not divisible by 2, 3, or 5, but are divisible by 7

6. Determine how many integer solutions there are to $x_1 + x_2 + x_3 + x_4 = 19$, if

a) $0 \le x_i$ for all $1 \le i \le 4$

b) $0 \le x_i < 8$ for all $1 \le i \le 4$

c) $0 \le x_1 \le 5$, $0 \le x_2 \le 6$, $3 \le x_3 \le 7$, $3 \le x_4 \le 8$

7. In how many ways can one arrange all of the letters in the word INFORMATION so that no pair of consecutive letters occurs more than once? [Here we want to count arrangements such as IINNOOFRMTA and FORTMAIINON but not INFORINMOTA (where "IN" occurs twice) or NORTFNOIAMI (where "NO" occurs twice).]

8. Determine the number of integer solutions to $x_1 + x_2 + x_3 + x_4 = 19$ where $-5 \le x_i \le 10$ for all $1 \le i \le 4$.

9. Determine the number of positive integers x where $x \le 9{,}999{,}999$ and the sum of the digits in x equals 31.

10. Professor Bailey has just completed writing the final examination for his course in advanced engineering mathematics. This examination has 12 questions, whose total value is to be 200 points. In how many ways can Professor Bailey assign the 200 points if each question must count for at least 10, but not more than 25, points and the point value for each question is to be a multiple of 5?

11. At Flo's Flower Shop, Flo wants to arrange 15 different plants on five shelves for a window display. In how many ways can she arrange them so that each shelf has at least one, but no more than four, plants?

12. In how many ways can Troy select nine marbles from a bag of twelve (identical except for color), where three are red, three blue, three white, and three green?

13. Find the number of permutations of $a, b, c, \ldots, x, y, z$, in which none of the patterns *spin*, *game*, *path*, or *net* occurs.

14. Answer the question in Example 8.10 for the case of six villages.

15. If eight distinct dice are rolled, what is the probability that all six numbers appear?

16. How many social security numbers (nine-digit sequences) have each of the digits 1, 3, and 7 appearing at least once?

17. In how many ways can three x's, three y's, and three z's be arranged so that no consecutive triple of the same letter appears?

18. Frostburg township sponsors four Boy Scout troops, each with 20 boys. If the head scoutmaster selects 50 of these boys to represent this township at the state jamboree, what is the probability that his selection will include at least one boy from each of the four troops?

19. If Zachary rolls a fair die five times, what is the probability that the sum of his five rolls is 20?

20. At a 12-week conference in mathematics, Sharon met seven of her friends from college. During the conference she met each friend at lunch 35 times, every pair of them 16 times, every trio eight times, every foursome four times, each set of five twice, and each set of six once, but never all seven at once. If she had lunch every day during the 84 days of the conference, did she ever have lunch alone?

21. Compute $\phi(n)$ for n equal to (a) 51; (b) 420; (c) 12300.

22. Compute $\phi(n)$ for n equal to (a) 5186; (b) 5187; (c) 5188.

23. Let $n \in \mathbf{Z}^+$. (a) Determine $\phi(2^n)$. (b) Determine $\phi(2^n p)$, where p is an odd prime.

24. For which $n \in \mathbf{Z}^+$ is $\phi(n)$ odd?

25. How many positive integers n less than 6000 (a) satisfy $\gcd(n, 6000) = 1$? (b) share a common prime divisor with 6000?

26. If $m, n \in \mathbf{Z}^+$, prove that $\phi(n^m) = n^{m-1}\phi(n)$.

27. Find three values for $n \in \mathbf{Z}^+$ where $\phi(n) = 16$.

28. For which positive integers n is $\phi(n)$ a power of 2?

29. For which positive integers n does 4 divide $\phi(n)$?

30. At an upcoming family reunion, five families — each consisting of a husband, wife, and one child — are to be seated around a circular table. In how many ways can these 15 people be arranged around the table so that no family is seated all together? (Here, as in Example 8.9, two seating arrangements are considered the same if one is a rotation of the other.)

8.2 Generalizations of the Principle

Consider a set S with $|S| = N$, and conditions $c_1, c_2, \ldots, c_t$ satisfied by some of the elements of S. In Section 8.1 we saw how the Principle of Inclusion and Exclusion provides a way to determine $N(\overline{c}_1\overline{c}_2 \cdots \overline{c}_t)$, the number of elements in S that satisfy none of the t conditions. If $m \in \mathbf{Z}^+$ and $1 \le m \le t$, we now want to determine E_m, which denotes the

number of elements in S that satisfy *exactly* m of the t conditions. (At present we can obtain E_0.)

We can write formulas such as

$$E_1 = N(c_1\bar{c}_2\bar{c}_3\cdots\bar{c}_t) + N(\bar{c}_1c_2\bar{c}_3\cdots\bar{c}_t) + \cdots + N(\bar{c}_1\bar{c}_2\bar{c}_3\cdots\bar{c}_{t-1}c_t),$$

and

$$E_2 = N(c_1c_2\bar{c}_3\cdots\bar{c}_t) + N(c_1\bar{c}_2c_3\cdots\bar{c}_t) + \cdots + N(\bar{c}_1\bar{c}_2\bar{c}_3\cdots\bar{c}_{t-2}c_{t-1}c_t),$$

and although these results do not assist us as much as we should like, they will be a useful starting place as we examine the Venn diagrams for the cases where $t = 3$ and 4.

For Fig. 8.4, where $t = 3$, we place a numbered condition beside the circle representing those elements of S satisfying that particular condition and we also number each of the individual regions shown. Then E_1 equals the number of elements in regions 2, 3, and 4. But we can also write

$$E_1 = N(c_1) + N(c_2) + N(c_3) - 2\,[N(c_1c_2) + N(c_1c_3) + N(c_2c_3)] + 3N(c_1c_2c_3).$$

In $N(c_1) + N(c_2) + N(c_3)$ we count the elements in regions 5, 6, and 7 twice and those in region 8 three times. In the next term, the elements in regions 5, 6, and 7 are deleted twice. We remove the elements in region 8 six times in $2\,[N(c_1c_2) + N(c_1c_3) + N(c_2c_3)]$, so we then add on the term $3N(c_1c_2c_3)$ and end up not counting the elements in region 8 at all. Hence we have $E_1 = S_1 - 2S_2 + 3S_3 = S_1 - \binom{2}{1}S_2 + \binom{3}{2}S_3$.

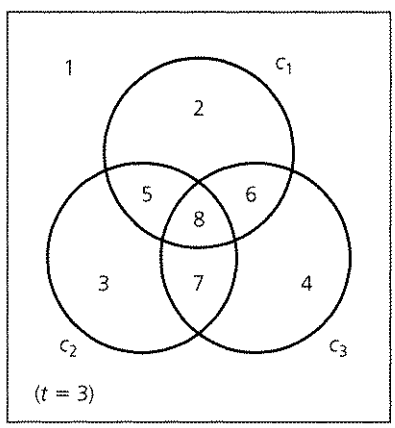


Figure 8.4

When we turn to E_2, our earlier formula indicates that we want to count the elements of S in regions 5, 6, and 7. From the Venn diagram,

$$E_2 = N(c_1c_2) + N(c_1c_3) + N(c_2c_3) - 3N(c_1c_2c_3) = S_2 - 3S_3 = S_2 - \binom{3}{1}S_3,$$

and

$$E_3 = N(c_1c_2c_3) = S_3.$$

In Fig. 8.5, the conditions c_1, c_2, c_3 are associated with circular subsets of S, whereas c_4 is paired with the rather irregularly shaped area made up of regions 4, 8, 9, 11, 12, 13, 14, and 16. For each $1 \le i \le 4$, E_i is determined as follows:

E_1 [regions 2, 3, 4, 5]:

$$\begin{aligned} E_1 &= [N(c_1) + N(c_2) + N(c_3) + N(c_4)] \\ &\quad - 2\,[N(c_1c_2) + N(c_1c_3) + N(c_1c_4) + N(c_2c_3) + N(c_2c_4) + N(c_3c_4)] \\ &\quad + 3\,[N(c_1c_2c_3) + N(c_1c_2c_4) + N(c_1c_3c_4) + N(c_2c_3c_4)] \\ &\quad - 4N(c_1c_2c_3c_4) \\ &= S_1 - 2S_2 + 3S_3 - 4S_4 = S_1 - \binom{2}{1}S_2 + \binom{3}{2}S_3 - \binom{4}{3}S_4. \end{aligned}$$

Note: Taking an element in region 3, we find that it is counted once in E_1 and once in S_1 [in $N(c_3)$]. Taking an element in region 6, we find that it is not counted in E_1; it is counted twice in S_1 [in both $N(c_2)$ and $N(c_3)$] but removed twice in $2S_2$ [for it is counted once in S_2 in $N(c_2c_3)$], so overall it is not counted. The reader should now consider an element from region 12 and one from region 16 and show that each contributes a count of 0 to both sides of the formula for E_1.

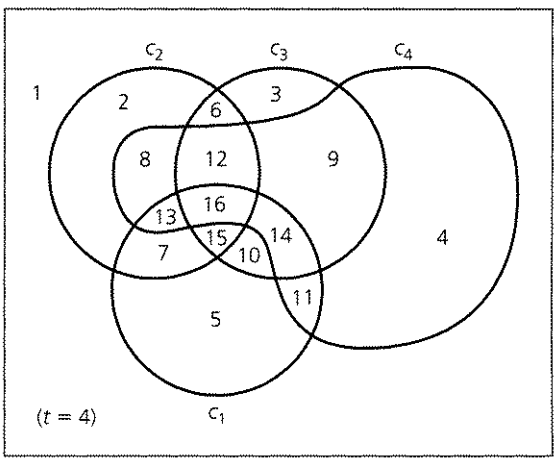


Figure 8.5

E_2 [regions 6–11]:

From Fig. 8.5, $E_2 = S_2 - 3S_3 + 6S_4 = S_2 - \binom{3}{1}S_3 + \binom{4}{2}S_4$. For details on this formula we examine the results in Table 8.1, where next to each summand of S_2, S_3, and S_4 we list the regions whose elements are counted in determining that particular summand. In calculating $S_2 - 3S_3 + 6S_4$ we find the elements in regions 6–11, which are precisely those that are to be counted for E_2.

Table 8.1

S_2	S_3	S_4
$N(c_1c_2)$: 7, 13, 15, 16 $N(c_1c_3)$: 10, 14, 15, 16 $N(c_1c_4)$: 11, 13, 14, 16 $N(c_2c_3)$: 6, 12, 15, 16 $N(c_2c_4)$: 8, 12, 13, 16 $N(c_3c_4)$: 9, 12, 14, 16	$N(c_1c_2c_3)$: 15, 16 $N(c_1c_2c_4)$: 13, 16 $N(c_1c_3c_4)$: 14, 16 $N(c_2c_3c_4)$: 12, 16	$N(c_1c_2c_3c_4)$: 16

Finally, the elements for E_3 are found in regions 12–15, and $E_3 = S_3 - 4S_4 = S_3 - \binom{4}{1}S_4$; the elements for E_4 are those in region 16, and $E_4 = S_4$.

These results suggest the following theorem.

THEOREM 8.2 Under the hypotheses of Theorem 8.1, for each $1 \le m \le t$, the number of elements in S that satisfy *exactly* m of the conditions $c_1, c_2, \ldots, c_t$ is given by

$$E_m = S_m - \binom{m+1}{1}S_{m+1} + \binom{m+2}{2}S_{m+2} - \cdots + (-1)^{t-m}\binom{t}{t-m}S_t. \tag{1}$$

(If $m = 0$, we obtain Theorem 8.1.)

Proof: Arguing as in Theorem 8.1, let $x \in S$ and consider the following three cases.

a) When x satisfies fewer than m conditions, it contributes a count of 0 to each of the terms $E_m, S_m, S_{m+1}, \ldots, S_t$, so it is not counted on either side of the equation.

b) When x satisfies exactly m of the conditions, it is counted once in E_m and once in S_m, but not in $S_{m+1}, \ldots, S_t$. Consequently, it is included once in the count for either side of the equation.

c) Suppose x satisfies r of the conditions, where $m < r \le t$. Then x contributes nothing to E_m. Yet it is counted $\binom{r}{m}$ times in S_m, $\binom{r}{m+1}$ times in $S_{m+1}, \ldots$, and $\binom{r}{r}$ times in S_r, but 0 times for any term beyond S_r. So on the right-hand side of the equation, x is counted $\binom{r}{m} - \binom{m+1}{1}\binom{r}{m+1} + \binom{m+2}{2}\binom{r}{m+2} - \cdots + (-1)^{r-m}\binom{r}{r-m}\binom{r}{r}$ times. For $0 \le k \le r - m$,

$$\begin{aligned}\binom{m+k}{k}\binom{r}{m+k} &= \frac{(m+k)!}{k!\,m!} \cdot \frac{r!}{(m+k)!(r-m-k)!} \\ &= \frac{r!}{m!} \cdot \frac{1}{k!(r-m-k)!} = \frac{r!}{m!(r-m)!} \cdot \frac{(r-m)!}{k!(r-m-k)!} \\ &= \binom{r}{m}\binom{r-m}{k}.\end{aligned}$$

Consequently, on the right-hand side of Eq. (1), x is counted

$$\begin{aligned}&\binom{r}{m}\binom{r-m}{0} - \binom{r}{m}\binom{r-m}{1} + \binom{r}{m}\binom{r-m}{2} - \cdots + (-1)^{r-m}\binom{r}{m}\binom{r-m}{r-m} \\ &\quad = \binom{r}{m}\left[\binom{r-m}{0} - \binom{r-m}{1} + \binom{r-m}{2} - \cdots + (-1)^{r-m}\binom{r-m}{r-m}\right] \\ &\quad = \binom{r}{m}[1-1]^{r-m} = \binom{r}{m} \cdot 0 = 0 \text{ times},\end{aligned}$$

and the formula is verified.

Based on this result, if L_m denotes the number of elements of S (under the hypotheses of Theorem 8.1) that satisfy *at least* m of the t conditions, then we have the following formula.

COROLLARY 8.2 $L_m = S_m - \binom{m}{m-1}S_{m+1} + \binom{m+1}{m-1}S_{m+2} - \cdots + (-1)^{t-m}\binom{t-1}{m-1}S_t.$

Proof: A proof is outlined in the exercises at the end of this section.

When $m = 1$, the result in Corollary 8.2 becomes

$$L_1 = S_1 - \binom{1}{0}S_2 + \binom{2}{0}S_3 - \cdots + (-1)^{t-1}\binom{t-1}{0}S_t$$
$$= S_1 - S_2 + S_3 - \cdots + (-1)^{t-1}S_t.$$

Comparing this with the result in Theorem 8.1, we find that

$$L_1 = N - \overline{N} = |S| - \overline{N}.$$

This result is not much of a surprise, because an element x of S is counted in L_1 if it satisfies at least one of the conditions $c_1, c_2, c_3, \ldots, c_t$ — that is, if $x \in S$ and x is not counted in $\overline{N} = N(\overline{c}_1\overline{c}_2\overline{c}_3 \cdots \overline{c}_t)$.

EXAMPLE 8.11

Looking back to Example 8.10, we shall find the numbers of systems of two-way roads so that exactly (E_2) and at least (L_2) two of the villages remain isolated.

The previously calculated results for this example show

$$E_2 = S_2 - \binom{3}{1}S_3 + \binom{4}{2}S_4 - \binom{5}{3}S_5 = 80 - 3(20) + 6(5) - 10(1) = 40,$$
$$L_2 = S_2 - \binom{2}{1}S_3 + \binom{3}{1}S_4 - \binom{4}{1}S_5 = 80 - 2(20) + 3(5) - 4(1) = 51.$$

EXERCISES 8.2

1. For the situation in Examples 8.10 and 8.11 compute E_i for $0 \le i \le 5$ and show that $\sum_{i=0}^{5} E_i = N = |S|$.

2. **a)** In how many ways can the letters in ARRANGEMENT be arranged so that there are exactly two pairs of consecutive identical letters? at least two pairs of consecutive identical letters?

b) Answer part (a), replacing two with three.

3. In how many ways can one arrange the letters in CORRESPONDENTS so that (a) there is no pair of consecutive identical letters? (b) there are exactly two pairs of consecutive identical letters? (c) there are at least three pairs of consecutive identical letters?

4. Let $A = \{1, 2, 3, \ldots, 10\}$, and $B = \{1, 2, 3, \ldots, 7\}$. How many functions $f: A \to B$ satisfy $|f(A)| = 4$? How many have $|f(A)| \le 4$?

5. In how many ways can one distribute ten distinct prizes among four students with exactly two students getting nothing? How many ways have at least two students getting nothing?

6. Zelma is having a luncheon for herself and nine of the women in her tennis league. On the morning of the luncheon she places name cards at the ten places at her table and then leaves to run a last-minute errand. Her husband, Herbert, comes home from his morning tennis match and unfortunately leaves the back door open. A gust of wind scatters the ten name cards. In how many ways can Herbert replace the ten cards at the places at the table so that exactly four of the ten women will be seated where Zelma had wanted them? In how many ways will at least four of them be seated where they were supposed to be?

7. If 13 cards are dealt from a standard deck of 52, what is the probability that these 13 cards include (a) at least one card from each suit? (b) exactly one void (for example, no clubs)? (c) exactly two voids?

8. The following provides an outline for proving Corollary 8.2. Fill in the needed details.

a) First note that $E_t = L_t = S_t$.

b) What is E_{t-1}, and how are L_t and L_{t-1} related?

c) Show that $L_{t-1} = S_{t-1} - \binom{t-1}{t-2}S_t$.

d) For all $1 \le m \le t-1$, how are L_m, L_{m+1}, and E_m related?

e) Using the results in steps (a) through (d), establish the corollary by a backward type of induction.

8.3 Derangements: Nothing Is in Its Right Place

In elementary calculus the Maclaurin series for the exponential function is given by

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = \sum_{n=0}^{\infty} \frac{x^n}{n!},$$

so

$$e^{-1} = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} = 1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \cdots.$$

To five places, $e^{-1} = 0.36788$ and $1 - 1 + (1/2!) - (1/3!) + \cdots - (1/7!) \doteq 0.36786$. Consequently, for all $k \in \mathbf{Z}^+$, if $k \geq 7$, then $\sum_{n=0}^{k}((-1)^n)/n!$ is a very good approximation to e^{-1}.

We find these ideas helpful in working some of the following examples.

EXAMPLE 8.12

While at the racetrack, Ralph bets on each of the ten horses in a race to come in according to how they are favored. In how many ways can they reach the finish line so that he loses all of his bets?

Removing the words *horses* and *racetrack* from the problem, we really want to know in how many ways we can arrange the numbers $1, 2, 3, \ldots, 10$ so that 1 is not in first place (its natural position), 2 is not in second place (its natural position), $\ldots$, and 10 is not in tenth place (its natural position). These arrangements are called the *derangements* of $1, 2, 3, \ldots, 10$.

The Principle of Inclusion and Exclusion provides the key to calculating the number of derangements. For each $1 \leq i \leq 10$, an arrangement of $1, 2, 3, \ldots, 10$ is said to satisfy condition c_i if integer i is in the ith place. We obtain the number of derangements, denoted by d_{10}, as follows:

$$\begin{aligned} d_{10} &= N(\bar{c}_1\bar{c}_2\bar{c}_3\cdots\bar{c}_{10}) = 10! - \tbinom{10}{1}9! + \tbinom{10}{2}8! - \tbinom{10}{3}7! + \cdots + \tbinom{10}{10}0! \\ &= 10!\left[1 - \tbinom{10}{1}(9!/10!) + \tbinom{10}{2}(8!/10!) - \tbinom{10}{3}(7!/10!) + \cdots + \tbinom{10}{10}(0!/10!)\right] \\ &= 10![1 - 1 + (1/2!) - (1/3!) + \cdots + (1/10!)] \doteq (10!)(e^{-1}). \end{aligned}$$

The sample space here consists of the 10! ways the horses can finish. So the *probability* that Ralph will lose every bet is approximately $(10!)(e^{-1})/(10!) = e^{-1}$. This probability remains (more or less) the same if the number of horses in the race is $11, 12, \ldots$. On the other hand, for n horses, where $n \geq 10$, the probability that our gambler wins at least one of his bets is approximately $1 - e^{-1} \doteq 0.63212$.

EXAMPLE 8.13

The number of derangements of 1, 2, 3, 4 is

$$\begin{aligned} d_4 &= 4![1 - 1 + (1/2!) - (1/3!) + (1/4!)] \\ &= 4![(1/2!) - (1/3!) + (1/4!)] = (4)(3) - 4 + 1 = 9. \end{aligned}$$

These nine derangements are

2143	3142	4123
2341	3412	4312
2413	3421	4321.

Among the $24 - 9 = 15$ permutations of 1, 2, 3, 4 that are *not* derangements one finds 1234, 2314, 3241, 1342, 2431, and 2314.

EXAMPLE 8.14

Peggy has seven books to review for the C–H Company, so she hires seven people to review them. She wants two reviews per book, so the first week she gives each person one book to read and then redistributes the books at the start of the second week. In how many ways can she make these two distributions so that she gets two reviews (by different people) of each book?

She can distribute the books in 7! ways the first week. Numbering both the books and the reviewers (for the first week) as $1, 2, \ldots, 7$, for the second distribution she must arrange these numbers so that none of them is in its natural position. This she can do in d_7 ways. By the rule of product, she can make the two distributions in $(7!)d_7 \doteq (7!)^2(e^{-1})$ ways.

EXERCISES 8.3

1. In how many ways can the integers $1, 2, 3, \ldots, 10$ be arranged in a line so that no even integer is in its natural position?

2. a) List all the derangements of 1, 2, 3, 4, 5 where the first three numbers are 1, 2, and 3, in some order.

b) List all the derangements of 1, 2, 3, 4, 5, 6 where the first three numbers are 1, 2, and 3, in some order.

3. How many derangements are there for 1, 2, 3, 4, 5?

4. How many permutations of 1, 2, 3, 4, 5, 6, 7 are not derangements?

5. a) Let $A = \{1, 2, 3, \ldots, 7\}$. A function $f: A \to A$ is said to have a *fixed point* if for some $x \in A$, $f(x) = x$. How many one-to-one functions $f: A \to A$ have at least one fixed point?

b) In how many ways can we devise a secret code by assigning to each letter of the alphabet a different letter to represent it?

6. How many derangements of 1, 2, 3, 4, 5, 6, 7, 8 start with (a) 1, 2, 3, and 4, in some order? (b) 5, 6, 7, and 8, in some order?

7. For the positive integers $1, 2, 3, \ldots, n-1, n$, there are 11,660 derangements where 1, 2, 3, 4, and 5 appear in the first five positions. What is the value of n?

8. Four applicants for a job are to be interviewed for 30 minutes each: 15 minutes with each of supervisors Nancy and Yolanda. (The interviews are in separate rooms, and interviewing starts at 9:00 A.M.) (a) In how many ways can these interviews be scheduled during a one-hour period? (b) One applicant, named Josephine, arrives at 9:00 A.M. What is the probability that she will have her two interviews one after the other? (c) Regina, another applicant, arrives at 9:00 A.M. and hopes to be finished in time to leave by 9:50 A.M. for another appointment. What is the probability that Regina will be able to leave on time?

9. In how many ways can Mrs. Ford distribute ten distinct books to her ten children (one book to each child) and then collect and redistribute the books so that each child has the opportunity to peruse two different books?

10. a) When n balls, numbered $1, 2, 3, \ldots, n$ are taken in succession from a container, a *rencontre* occurs if the mth ball withdrawn is numbered m, for some $1 \le m \le n$. Find the probability of getting (i) no rencontres; (ii) (exactly) one rencontre, (iii) at least one rencontre; and (iv) r rencontres, where $1 \le r \le n$.

b) Approximate the answers to the questions in part (a).

11. Ten women attend a business luncheon. Each woman checks her coat and attaché case. Upon leaving, each woman is given a coat and case at random. (a) In how many ways can the coats and cases be distributed so that no woman gets either of her possessions? (b) In how many ways can they be distributed so that no woman gets back both of her possessions?

12. Ms. Pezzulo teaches geometry and then biology to a class of 12 advanced students in a classroom that has only 12 desks. In how many ways can she assign the students to these desks so that (a) no student is seated at the same desk for both classes? (b) there are exactly six students each of whom occupies the same desk for both classes?

13. Give a combinatorial argument to verify that for all $n \in \mathbf{Z}^+$,

$$n! = \binom{n}{0}d_0 + \binom{n}{1}d_1 + \binom{n}{2}d_2 + \cdots + \binom{n}{n}d_n = \sum_{k=0}^{n}\binom{n}{k}d_k.$$

(For each $1 \le k \le n$, d_k = the number of derangements of $1, 2, 3, \ldots, k$; $d_0 = 1$.)

14. **a)** In how many ways can the integers $1, 2, 3, \ldots, n$ be arranged in a line so that none of the patterns $12, 23, 34, \ldots, (n-1)n$ occurs?

b) Show that the result in part (a) equals $d_{n-1} + d_n$. (d_n = the number of derangements of $1, 2, 3, \ldots, n$.)

15. Answer part (a) of Exercise 14 if the numbers are arranged in a circle, and, as we count clockwise about the circle, none of the patterns $12, 23, 34, \ldots, (n-1)n, n1$ occurs.

16. What is the probability that the gambler in Example 8.12 wins (a) (exactly) five of his bets? (b) at least five of his bets?

8.4 Rook Polynomials

Consider the six-square "chessboard" shown in Fig. 8.6 (*Note*: The shaded squares are not part of the chessboard.). In chess a piece called a *rook* or *castle* is allowed at one turn to be moved horizontally or vertically over as many unoccupied spaces as one wishes. Here a rook in square 3 of the figure could be moved in one turn to squares 1, 2, or 4. A rook at square 5 could be moved to square 6 or square 2 (even though there is no square between squares 5 and 2).

For $k \in \mathbf{Z}^+$ we want to determine the number of ways in which k rooks can be placed on the unshaded squares of this chessboard so that no two of them can take each other—that is, no two of them are in the same row or column of the chessboard. This number is denoted by r_k, or by $r_k(C)$ if we wish to stress that we are working on a particular chessboard C.

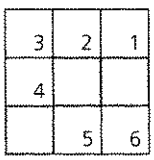


Figure 8.6

For any chessboard, r_1 is the number of squares on the board. Here $r_1 = 6$. Two nontaking rooks can be placed at the following pairs of positions: $\{1, 4\}$, $\{1, 5\}$, $\{2, 4\}$, $\{2, 6\}$, $\{3, 5\}$, $\{3, 6\}$, $\{4, 5\}$, and $\{4, 6\}$, so $r_2 = 8$. Continuing, we find that $r_3 = 2$, using the locations $\{1, 4, 5\}$ and $\{2, 4, 6\}$; $r_k = 0$, for $k \geq 4$.

With $r_0 = 1$, the *rook polynomial*, $r(C, x)$, for the chessboard in Fig. 8.6 is defined as $r(C, x) = 1 + 6x + 8x^2 + 2x^3$. For each $k \geq 0$, the coefficient of x^k is the number of ways we can place k nontaking rooks on chessboard C.

What we have done here (using a case-by-case analysis) soon proves tedious. As the size of the board increases, we have to consider cases wherein numbers such as r_4 and r_5 are nonzero. Consequently, we shall now make some observations that will allow us to make use of small boards and somehow break up a large board into smaller *subboards*.

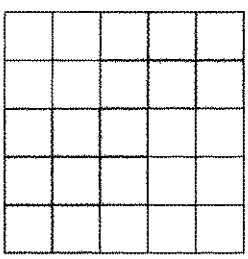


Figure 8.7

The chessboard C in Fig. 8.7 is made up of 11 unshaded squares. We note that C consists of a 2×2 subboard C_1 located in the upper left corner and a seven-square subboard C_2 located in the lower right corner. These subboards are *disjoint* because they have no squares in the same row or column of C.

Calculating as we did for our first chessboard, here we find

$$r(C_1, x) = 1 + 4x + 2x^2, \qquad r(C_2, x) = 1 + 7x + 10x^2 + 2x^3,$$
$$r(C, x) = 1 + 11x + 40x^2 + 56x^3 + 28x^4 + 4x^5 = r(C_1, x) \cdot r(C_2, x).$$

Hence $r(C, x) = r(C_1, x) \cdot r(C_2, x)$. But did this occur by luck or is something happening here that we should examine more closely? For example, to obtain r_3 for C, we need to know in how many ways three nontaking rooks can be placed on board C. These fall into three cases:

a) All three rooks are on subboard C_2 (and none is on C_1): $(2)(1) = 2$ ways.

b) Two rooks are on subboard C_2 and one is on C_1: $(10)(4) = 40$ ways.

c) One rook is on subboard C_2 and two are on C_1: $(7)(2) = 14$ ways.

Consequently, three nontaking rooks can be placed on board C in $(2)(1) + (10)(4) + (7)(2) = 56$ ways. Here we see that 56 arises just as the coefficient of x^3 does in the product $r(C_1, x) \cdot r(C_2, x)$.

In general, if C is a chessboard made up of *pairwise* disjoint subboards $C_1, C_2, \ldots, C_n$, then $r(C, x) = r(C_1, x)r(C_2, x) \cdots r(C_n, x)$.

The last result for this section demonstrates the type of principle we have seen in other results in combinatorial and discrete mathematics: Given a large chessboard, break it into smaller subboards whose rook polynomials can be determined by inspection.

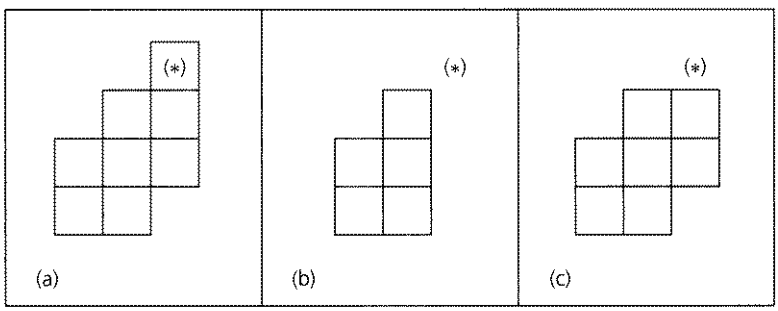


Figure 8.8

Consider chessboard C in Fig. 8.8(a). For $k \geq 1$, suppose we wish to place k nontaking rooks on C. For each square of C, such as the one designated by $(*)$, there are two possibilities to examine.

a) Place one rook on the designated square. Then we remove, as possible locations for the other $k - 1$ rooks, all other squares of C in the same row or column as the designated square. We use C_s to denote the remaining smaller subboard [seen in Fig. 8.8(b)].

b) We do not use the designated square at all. The k rooks are placed on the subboard C_e [C with the one designated square eliminated — as shown in Fig. 8.8(c)].

Since these two cases are all-inclusive and mutually disjoint,

$$r_k(C) = r_{k-1}(C_s) + r_k(C_e).$$

From this we see that

$$r_k(C)x^k = r_{k-1}(C_s)x^k + r_k(C_e)x^k. \tag{1}$$

If n is the number of squares in the chessboard (here n is 8), then Eq. (1) is valid for all $1 \leq k \leq n$, and we write

$$\sum_{k=1}^{n} r_k(C)x^k = \sum_{k=1}^{n} r_{k-1}(C_s)x^k + \sum_{k=1}^{n} r_k(C_e)x^k. \tag{2}$$

For Eq. (2) we realize that the summations may stop before $k = n$. We have seen cases, as in Fig. 8.6, where r_n and some prior r_k's are 0. The summations start at $k = 1$, for otherwise we could find ourselves with the term $r_{-1}(C_s)x^0$ in the first summand on the right-hand side of Eq. (2).

Equation (2) may be rewritten as

$$\sum_{k=1}^{n} r_k(C)x^k = x\sum_{k=1}^{n} r_{k-1}(C_s)x^{k-1} + \sum_{k=1}^{n} r_k(C_e)x^k \tag{3}$$

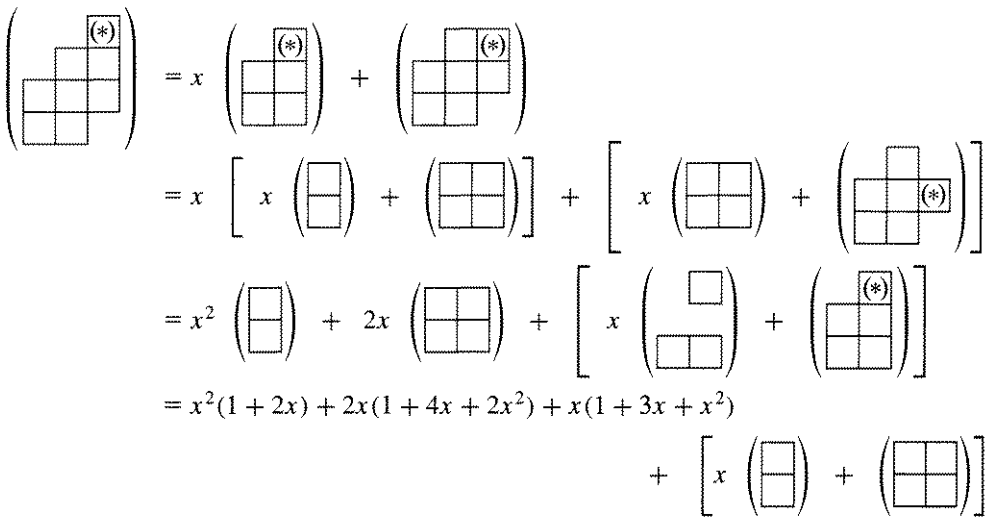
or

$$1 + \sum_{k=1}^{n} r_k(C)x^k = x \cdot r(C_s, x) + \sum_{k=1}^{n} r_k(C_e)x^k + 1,$$

from which it follows that

$$r(C, x) = x \cdot r(C_s, x) + r(C_e, x). \tag{4}$$

We now use this final equation to determine the rook polynomial for the chessboard shown in part (a) of Fig. 8.8. Each time the idea in Eq. (4) is used, we mark the special square we are using with $(*)$. Parentheses are placed about each chessboard to denote the rook polynomial of the board.



$$= x^2(1 + 2x) + 2x(1 + 4x + 2x^2) + x(1 + 3x + x^2)$$

$$= 3x + 12x^2 + 7x^3 + x(1 + 2x) + (1 + 4x + 2x^2) = 1 + 8x + 16x^2 + 7x^3.$$

8.5 Arrangements with Forbidden Positions

The rook polynomials of the previous section seem interesting on their own. Now we shall find them useful in solving the following problems.

EXAMPLE 8.15

In making seating arrangements for their son's wedding reception, Grace and Nick are down to four relatives, denoted R_i, for $1 \le i \le 4$, who do not get along with one another. There is a single open seat at each of the five tables T_j, where $1 \le j \le 5$. Because of family differences,

a) R_1 will not sit at T_1 or T_2.

b) R_2 will not sit at T_2.

c) R_3 will not sit at T_3 or T_4.

d) R_4 will not sit at T_4 or T_5.

This situation is represented in Fig. 8.9. The number of ways we can seat these four people at four different tables, and satisfy conditions (a) through (d), is the number of ways four nontaking rooks can be placed on the chessboard made up of the *unshaded* squares. However, since there are only seven shaded squares, as opposed to thirteen unshaded ones, it would be easier to work with the shaded chessboard.

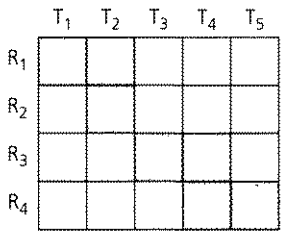


Figure 8.9

We start with the conditions that are required for us to apply the Principle of Inclusion and Exclusion: For each $1 \leq i \leq 4$, let c_i be the condition where a seating assignment of these four people (at different tables) is made with relative R_i in a forbidden (shaded) position. As usual, $|S|$ denotes the total number of ways we can place the four relatives, one to a table. Then $|S| = N = S_0 = 5!$

To determine S_1 we consider each of the following:

- $N(c_1) = 4! + 4!$, for there are 4! ways to seat R_2, R_3, and R_4 if R_1 is in forbidden position T_1 and another 4! ways if R_1 is at table T_2, his or her other forbidden position.
- $N(c_2) = 4!$, for after placing R_2 at forbidden table T_2, we must place R_1, R_3, and R_4 at T_1, T_3, T_4, and T_5, one person to a table.
- $N(c_3) = 4! + 4!$, one summand for R_3 being in forbidden position T_3, and the other summand for R_3 being in the forbidden position T_4.
- $N(c_4) = 4! + 4!$, each of the two summands arising when R_4 is placed at each of the two forbidden positions T_4 and T_5.

Hence $S_1 = 7(4!)$.

Turning to S_2 we have these considerations:

- $N(c_1c_2) = 3!$, because after we place R_1 at T_1 and R_2 at T_2, there are three tables (T_3, T_4, and T_5) where R_3 and R_4 can be seated.
- $N(c_1c_3) = 3! + 3! + 3! + 3!$, because there are four cases where R_1 and R_3 are located at forbidden positions:

  i) R_1 at T_1; R_3 at T_3 **ii)** R_1 at T_2; R_3 at T_3
  iii) R_1 at T_1; R_3 at T_4 **iv)** R_1 at T_2; R_3 at T_4.

In a similar manner we find that $N(c_1c_4) = 4(3!)$, $N(c_2c_3) = 2(3!)$, $N(c_2c_4) = 2(3!)$, and $N(c_3c_4) = 3(3!)$. Consequently, $S_2 = 16(3!)$.

Before continuing, we make a few observations about S_1 and S_2. For S_1 we have $7(4!) = 7(5-1)!$, where 7 is the number of shaded squares in Fig. 8.9. Also, $S_2 = 16(3!) = 16(5-2)!$, where 16 is the number of ways two nontaking rooks can be placed on the shaded chessboard.

In general, for all $0 \leq i \leq 4$, $S_i = r_i(5-i)!$, where r_i is the number of ways in which it is possible to place i nontaking rooks on the shaded chessboard shown in Fig. 8.9.

Consequently, to expedite the solution of this problem, we turn to $r(C, x)$, the rook polynomial of this shaded chessboard. Using the decomposition of C into the disjoint subboards in the upper left and lower right corners, we find that

$$r(C, x) = (1 + 3x + x^2)(1 + 4x + 3x^2) = 1 + 7x + 16x^2 + 13x^3 + 3x^4,$$

so

$$N(\bar{c}_1\bar{c}_2\bar{c}_3\bar{c}_4) = S_0 - S_1 + S_2 - S_3 + S_4 = 5! - 7(4!) + 16(3!) - 13(2!) + 3(1!)$$
$$= \sum_{i=0}^{4}(-1)^i r_i(5-i)! = 25.$$

Grace and Nick can breathe a sigh of relief. There are 25 ways in which they can seat these last four relatives at the reception and avoid any squabbling.

The next example demonstrates how a bit of rearranging of our chessboard can help in our calculations.

EXAMPLE 8.16

We have a pair of dice; one is red, the other green. We roll these dice six times. What is the probability that we obtain all six values on both the red die and the green die if we know that the ordered pairs (1, 2), (2, 1), (2, 5), (3, 4), (4, 1), (4, 5), and (6, 6) did not occur? [Here an ordered pair (a, b) indicates a on the red die and b on the green.]

Recognizing this problem as one dealing with permutations and forbidden positions, we construct the chessboard shown in Fig. 8.10(a), where the row labels represent the outcome on the red die, the column labels the outcome on the green die, and the shaded squares constitute the forbidden positions. In this figure the shaded squares are scattered. Relabeling the rows and columns, we can redraw the chessboard as shown in Fig. 8.10(b), where we have taken shaded squares in the same row (or column) of the board shown in part (a) and made them adjacent. In Fig. 8.10(b), the chessboard C (of seven shaded squares) is the union of four pairwise disjoint subboards, and so

$$r(C, x) = (1 + 4x + 2x^2)(1 + x)^3 = 1 + 7x + 17x^2 + 19x^3 + 10x^4 + 2x^5.$$

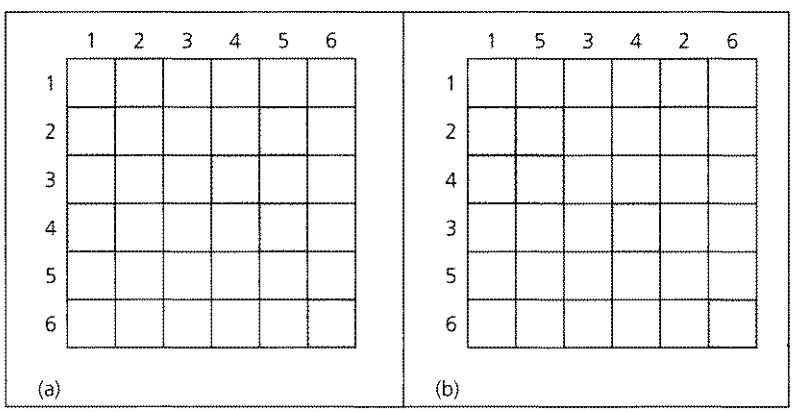


Figure 8.10

For each $1 \le i \le 6$, define c_i as the condition where, having rolled the dice six times, we find that all six values occur on both the red die and the green die, but i on the red die

is paired with one of the forbidden numbers on the green die. [Note that $N(c_5) = 0$.] Then the number of (ordered) sequences of the six rolls of the dice for the event we are interested in is

$$\begin{aligned}(6!)N(\bar{c}_1\bar{c}_2\bar{c}_3\bar{c}_4\bar{c}_5\bar{c}_6) &= (6!)\sum_{i=0}^{6}(-1)^i S_i = (6!)\sum_{i=0}^{6}(-1)^i r_i(6-i)! \\ &= 6![6! - 7(5!) + 17(4!) - 19(3!) + 10(2!) - 2(1!) + 0(0!)] \\ &= 6![192] = 138{,}240.\end{aligned}$$

Since the sample space consists of all sequences of six ordered pairs selected with repetition from the 29 unshaded squares of the chessboard, the probability of this event is $138{,}240/(29)^6 \doteq 0.00023$.

Our last example provides a unifying idea for what we have done in this section.

EXAMPLE 8.17

Let $A = \{1, 2, 3, 4\}$ and $B = \{u, v, w, x, y, z\}$. How many one-to-one functions $f: A \to B$ satisfy none of the following conditions:

c_1: $f(1) = u$ or v $\quad$ c_2: $f(2) = w$ $\quad$ c_3: $f(3) = w$ or x $\quad$ c_4: $f(4) = x, y,$ or z

As in our two prior examples, we construct a chessboard, as shown in Fig. 8.11. Here we are really interested in the chessboard C made up of the eight shaded squares (which comprise two disjoint subboards). Now

$$r(C, x) = (1 + 2x)(1 + 6x + 9x^2 + 2x^3) = 1 + 8x + 21x^2 + 20x^3 + 4x^4.$$

So

$$\begin{aligned}N(\bar{c}_1\bar{c}_2\bar{c}_3\bar{c}_4) &= S_0 - S_1 + S_2 - S_3 + S_4 \\ &= (6!/2!) - 8(5!/2!) + 21(4!/2!) - 20(3!/2!) + 4(2!/2!) \\ &= \sum_{i=0}^{4}(-1)^i r_i(6-i)!/2! = 76\end{aligned}$$

and there are 76 one-to-one functions $f: A \to B$ where none of the conditions c_1, c_2, c_3, c_4 is satisfied.

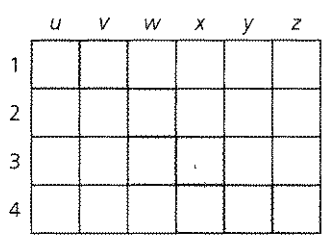


Figure 8.11

Even more so, look back at $N(\bar{c}_1\bar{c}_2\bar{c}_3\bar{c}_4)$ in Example 8.15. Disregarding the vocabulary of the "relatives" and "tables," we realize that we are counting the number of one-to-one functions $g: \{R_1, R_2, R_3, R_4\} \to \{T_1, T_2, T_3, T_4, T_5\}$ where none of the conditions c_1, c_2, c_3, c_4 is satisfied. (The situation is similar for $N(\bar{c}_1\bar{c}_2\bar{c}_3\bar{c}_4\bar{c}_5\bar{c}_6)$ in Example 8.16.)

Finally, for $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$, suppose we want to count the number of one-to-one functions $h: A \to A$ where $h(i) \neq i$ for all $i \in A$. Here the rook polynomial would be

$$r(C, x) = (1 + x)^8 = \sum_{k=0}^{8} \binom{8}{k} x^k$$

and we find that the number of such one-to-one functions h is

$$\begin{aligned} &\binom{8}{0}8! - \binom{8}{1}7! + \binom{8}{2}6! - \binom{8}{3}5! + \cdots + \binom{8}{8}0! \\ &= 8!\left[1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{1}{8!}\right] \\ &= d_8, \text{ the number of derangements of } 1, 2, 3, \ldots, 8. \end{aligned}$$

EXERCISES 8.4 AND 8.5

1. Verify directly the rook polynomials for (a) the unshaded chessboards in Figs. 8.7 and 8.8(a), and (b) the shaded chessboards in Figs. 8.9 and 8.10(b).

2. Construct or describe a smallest (least number of squares) chessboard for which $r_{10} \neq 0$.

3. **a)** Find the rook polynomial for the standard 8×8 chessboard.

b) Answer part (a) with 8 replaced by n, for $n \in \mathbf{Z}^+$.

4. Find the rook polynomials for the shaded chessboards in Fig. 8.12.

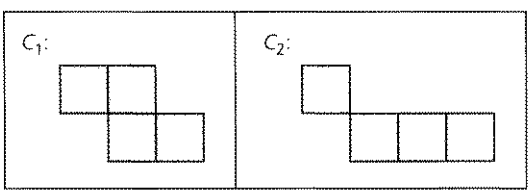


Figure 8.12

5. **a)** Find the rook polynomials for the shaded chessboards in Fig. 8.13.

b) Generalize the chessboard (and rook polynomial) for Fig. 8.13(i).

6. **a)** Let C be a chessboard that has m rows and n columns, with $m \leq n$ (for a total of mn squares). For $0 \leq k \leq m$, in how many ways can we arrange k (identical) nontaking rooks on C?

b) For the chessboard C in part (a), determine the rook polynomial $r(C, x)$.

7. Professor Ruth has five graders to correct programs in her courses in Java, C++, SQL, Perl, and VHDL. Graders Jeanne and Charles both dislike SQL, Sandra wants to avoid C++ and VHDL. Paul detests Java and C++, and Todd refuses to work in SQL and Perl. In how many ways can Professor Ruth assign each grader to correct programs in one language, cover all five languages, and keep everyone content?

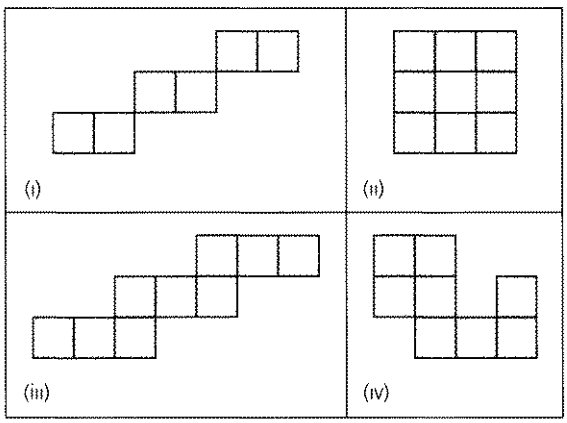


Figure 8.13

8. Why do we have 6! in the term $(6!)N(\bar{c}_1\bar{c}_2 \cdots \bar{c}_6)$ for the solution of Example 8.16?

9. Five professors named Al, Violet, Lynn, Jack, and Mary Lou are to be assigned to teach one class each from among calculus I, calculus II, calculus III, statistics, and combinatorics. Al will not teach calculus II or combinatorics, Lynn cannot stand statistics, Violet and Mary Lou both refuse to teach calculus I or calculus III, and Jack detests calculus II.

a) In how many ways can the head of the mathematics department assign each of these professors one of these five courses and still keep peace in the department?

b) For the assignments in part (a), what is the probability that Violet will get to teach combinatorics?

10. A pair of dice, one red and the other green, is rolled six times. We know that the ordered pairs (1, 1), (1, 5), (2, 4), (3, 6), (4, 2), (4, 4), (5, 1), and (5, 5) did not come up. What is the probability that every value came up on both the red die and the green one?

11. A computer dating service wants to match each of four women with one of six men. According to the information these applicants provided when they joined the service, we can draw the following conclusions.

- Woman 1 would not be compatible with man 1, 3, or 6.
- Woman 2 would not be compatible with man 2 or 4.
- Woman 3 would not be compatible with man 3 or 6.
- Woman 4 would not be compatible with man 4 or 5.

In how many ways can the service successfully match each of the four women with a compatible partner?

12. For $A = \{1, 2, 3, 4, 5\}$ and $B = \{u, v, w, x, y, z\}$, determine the number of one-to-one functions $f: A \to B$ where $f(1) \neq v, w$; $f(2) \neq u, w$; $f(3) \neq x$; and $f(4) \neq v, x, y$.

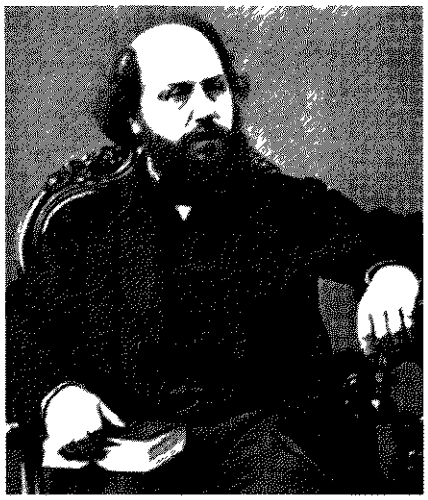
8.6 Summary and Historical Review

In the first and third chapters of this text we were concerned with enumeration problems in which we had to be careful of situations wherein arrangements or selections were overcounted. This situation became even more involved in Chapter 5 when we tried to count the number of onto functions for two finite sets.

With Venn diagrams to lead the way, in this chapter we obtained a pattern called the Principle of Inclusion and Exclusion. Using this principle, we restated each problem in terms of conditions and subsets. Using enumeration formulas on permutations and combinations that were developed earlier, we solved some simpler subproblems and let the principle manage our concern about overcounting. As a result, we were able to solve a variety of problems, some dealing with number theory and one with graph theory. We also proved the formula conjectured earlier in Section 5.3 for the number of onto functions for two finite sets.

This principle has an interesting history, being found in different manuscripts under such names as the "Sieve Method" or the "Principle of Cross Classification." A set-theoretic version of the principle, which concerned itself with set unions and intersections, is found in *Doctrine of Chances* (1718), a text on probability theory by Abraham DeMoivre (1667–1754). Somewhat earlier, in 1708, Pierre Rémond de Montmort (1678–1719) used the idea behind the principle in his solution of the problem generally known as *le problème des rencontres* (matches). (In this old French card game the 52 cards in a first deck are arranged face up in a row — perhaps on a table. Then the 52 cards of a second deck are dealt, with one new card being placed on each of the 52 cards previously arranged on the table top. The score for the game is determined by counting the resulting matches, where both the suit and the face value for each of the two cards must match.)

Credit for the way we developed and dealt with the Principle of Inclusion and Exclusion belongs to James Joseph Sylvester (1814–1897). (This colorful English-born mathematician also made major contributions in the theory of equations; the theory of matrices and determinants; and invariant theory, which he founded with Arthur Cayley (1821–1895). In addition Sylvester founded the *American Journal of Mathematics*, the first American journal established for mathematical research.) The importance of the inclusion-exclusion technique was not generally appreciated, however, until somewhat later, when the publication *Choice and Chance* by W. A. Whitworth [10] made mathematicians more aware of its potential and use.



James Joseph Sylvester (1814–1897)

For more on the application of this principle, examine Chapter 4 of C. L. Liu [4], Chapter 2 of H. J. Ryser [8], or Chapter 8 of A. Tucker [9]. More number-theoretic results related to the principle, including the Möbius inversion formula, can be found in Chapter 2 of M. Hall [1], Chapter X of C. L. Liu [5], and Chapter 16 of G. H. Hardy and E. M. Wright [3]. An extension of this formula is given in the article by G. C. Rota [7].

The article by D. Hanson, K. Seyffarth, and J. H. Weston [2] provides an interesting generalization of the derangement problem discussed in Section 8.3. The ideas behind the rook polynomials and their applications were developed in the late 1930s and during the 1940s and 1950s. Additional material on this topic is found in Chapters 7 and 8 of J. Riordan [6].

REFERENCES

1. Hall, Marshall, Jr. *Combinatorial Theory*. Waltham, Mass.: Blaisdell, 1967.
2. Hanson, Denis, Seyffarth, Karen, and Weston, J. Harley. "Matchings, Derangements, Rencontres." *Mathematics Magazine* 56, no. 4 (September 1983): pp. 224–229.
3. Hardy, Godfrey Harold, and Wright, Edward Maitland. *An Introduction to the Theory of Numbers*, 5th ed. Oxford: Oxford University Press, 1979.
4. Liu, C. L. *Introduction to Combinatorial Mathematics*. New York: McGraw-Hill, 1968.
5. Liu, C. L. *Topics in Combinatorial Mathematics*. Mathematical Association of America, 1972.
6. Riordan, John. *An Introduction to Combinatorial Analysis*. Princeton, N.J.: Princeton University Press, 1980. (Originally published in 1958 by John Wiley & Sons.)
7. Rota, Gian Carlo. "On the Foundations of Combinatorial Theory, I. Theory of Möbius Functions." *Zeitschrift für Wahrscheinlichkeits Theorie 2* (1964): pp. 340–368.
8. Ryser, Herbert J. *Combinatorial Mathematics*. Carus Mathematical Monograph, No. 14. Published by the Mathematical Association of America, distributed by John Wiley & Sons, New York, 1963.
9. Tucker, Alan. *Applied Combinatorics*, 4th ed. New York: Wiley, 2002.
10. Whitworth, William Allen. *Choice and Chance*. Originally published at Cambridge in 1867. Reprint of the 5th ed. (1901), Hafner, New York, 1965.

SUPPLEMENTARY EXERCISES

1. Determine how many $n \in \mathbf{Z}^+$ satisfy $n \leq 500$ and are not divisible by 2, 3, 5, 6, 8, or 10.

2. How many integers n are such that $0 \leq n < 1{,}000{,}000$ and the sum of the digits in n is less than or equal to 37?

3. At next week's church bazaar, Joseph and his cousin Jeffrey must arrange six baseballs, six footballs, six soccer balls, and six volleyballs on the four shelves in the sports booth sponsored by their Boy Scout troop. In how many ways can they do this so that there are at least two, but no more than seven, balls on each shelf? (Here all six balls for any one of the four sports are identical in appearance.)

4. Find the number of positive integers n where $1 \leq n \leq 1000$ and n is *not* a perfect square, cube, or fourth power.

5. In how many ways can we arrange the integers 1, 2, 3, . . . , 8 in a line so that there are no occurrences of the patterns 12, 23, . . . , 78, 81?

6. **a)** If we have k different colors available, in how many ways can we paint the walls of a pentagonal room if adjacent walls are to be painted with different colors?

b) What is the smallest value of k for which such a coloring is possible?

7. Ten students take a physics test in a certain room. When the test is over the students take a break and then return to the room to discuss their answers to the test questions. If there are 14 chairs in this room, in how many ways can the students seat themselves after the break so that no one is in the same chair he, or she, occupied during the test?

8. Using the result of Theorem 8.2, prove that the number of ways we can place s different objects in n distinct containers with m containers each containing exactly r of the objects is

$$\frac{(-1)^m n!\, s!}{m!} \sum_{i=m}^{n} \frac{(-1)^i (n-i)^{s-ir}}{(i-m)!(n-i)!(s-ir)!(r!)^i}.$$

9. If an arrangement of the letters in SURREPTITIOUS is selected at random, what is the probability that it contains (a) (exactly) three pairs of consecutive identical letters? (b) at most three pairs of consecutive identical letters?

10. In how many ways can four w's, four x's, four y's, and four z's be arranged so that there is no consecutive quadruple of the same letter?

11. **a)** Given n distinct objects, in how many ways can we select r of these objects so that each selection includes some particular m of the n objects? (Here $m \leq r \leq n$.)

b) Using the Principle of Inclusion and Exclusion, prove that for $m \leq r \leq n$,

$$\binom{n-m}{n-r} = \sum_{i=0}^{m} (-1)^i \binom{m}{i}\binom{n-i}{r}.$$

12. **a)** Let $\lambda \in \mathbf{Z}^+$. If we have λ different colors available, in how many ways can we color the vertices of the graph shown in Fig. 8.14(a) so that no adjacent vertices share the same color? This result in λ is called the *chromatic polynomial* of the graph, and the smallest value of λ for which the value of this polynomial is positive is called the *chromatic number* of the graph. What is the chromatic number of this graph? (We shall pursue this idea further in Chapter 11.)

b) If there are six colors available, in how many ways can the rooms R_i, $1 \leq i \leq 5$, shown in Fig. 8.14(b) be painted so that rooms with a common doorway, D_j, $1 \leq j \leq 5$, are painted with different colors?

13. Find the number of ways to arrange the letters in LAPTOP so that none of the letters L, A, T, O is in its original position and the letter P is not in the third or sixth position.

14. For $n \in \mathbf{Z}^+$ prove that if $\phi(n) = n - 1$ then n is prime.

15. Let D_{18} denote the set of positive divisors of 18. For $d \in D_{18}$ let $S_d = \{n \mid 0 < n \leq 18 \text{ and } \gcd(n, 18) = d\}$. (a) Show that the collection S_d, $d \in D_{18}$, provides a partition of $\{1, 2, 3, 4, \ldots, 17, 18\}$. (b) Note that $|S_1| = 6 = \phi(18)$ and $|S_2| = 6 = \phi(9)$. For each $d \in D_{18}$, express $|S_d|$ in terms of Euler's phi function.

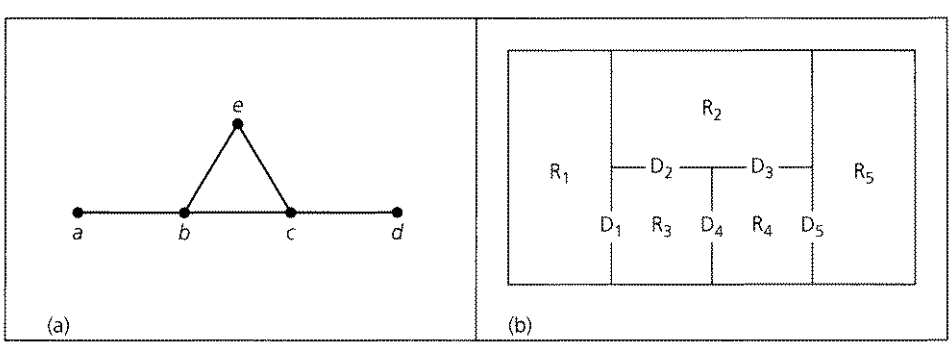


Figure 8.14

16. For $m \in \mathbf{Z}^+$ let $D_m = \{d \in \mathbf{Z}^+ | d \text{ divides } m\}$. For $d \in D_m$ let $S_d = \{n | 0 < n \leq m \text{ and } \gcd(n, m) = d\}$. (a) Show that the collection S_d, $d \in D_m$, provides a partition of $\{1, 2, 3, 4, \ldots, m-1, m\}$. (b) Determine $|S_d|$ for each $d \in D_m$.

17. If $n \in \mathbf{Z}^+$, prove that (a) $\phi(2n) = 2\phi(n)$ when n is even; and (b) $\phi(2n) = \phi(n)$ when n is odd.

18. Let $a, b, c \in \mathbf{Z}^+$ with $c = \gcd(a, b)$. Prove that

$$\phi(ab)\phi(c) = \phi(a)\phi(b)c.$$

19. Caitlyn has 48 different books: 12 each in mathematics, chemistry, physics, and computer science. These books are arranged on four shelves in her office with all books on any one subject on its own shelf. When her office is cleaned, the 48 books are taken down and then replaced on the shelves — once again with all 12 books on any one subject on its own shelf. In how many ways can this be done so that (a) no subject is on its original shelf? (b) one subject is on its original shelf? (c) no subject is on its original shelf and no book is in its original position? [For example, the book originally in the third (from the left) position on the first shelf must not be replaced on the first shelf and must not be in the third (from the left) position on the shelf where it is placed.]

9

Generating Functions

In this chapter and the next, we continue our study of enumeration, introducing at this time the important concept of the *generating function*.

The problem of making selections, with repetitions allowed, was studied in Chapter 1. There we sought, for example, the number of integer solutions to the equation $c_1 + c_2 + c_3 + c_4 = 25$ where $c_i \geq 0$ for all $1 \leq i \leq 4$. With the Principle of Inclusion and Exclusion, in Chapter 8, we were able to solve a more restricted version of the problem, such as $c_1 + c_2 + c_3 + c_4 = 25$ with $0 \leq c_i < 10$ for all $1 \leq i \leq 4$. If, in addition, we wanted c_2 to be even and c_3 to be a multiple of 3, we could apply the results of Chapters 1 and 8 to several subcases.

The power of the generating function rests upon its ability not only to solve the kinds of problems we have considered so far but also to aid us in new situations where additional restrictions may be involved.

9.1 Introductory Examples

Instead of defining a generating function at this point, we shall examine some examples that motivate the idea.

EXAMPLE 9.1

While shopping one Saturday, Mildred buys 12 oranges for her children, Grace, Mary, and Frank. In how many ways can she distribute the oranges so that Grace gets at least four, and Mary and Frank get at least two, but Frank gets no more than five? Table 9.1 lists

Table 9.1

G	M	F	G	M	F
4	3	5	6	2	4
4	4	4	6	3	3
4	5	3	6	4	2
4	6	2	7	2	3
5	2	5	7	3	2
5	3	4	8	2	2
5	4	3			
5	5	2			

all the possible distributions. We see that we have all the integer solutions to the equation $c_1 + c_2 + c_3 = 12$ where $4 \le c_1$, $2 \le c_2$, and $2 \le c_3 \le 5$.

Considering the first two cases in this table, we find the solutions $4 + 3 + 5 = 12$ and $4 + 4 + 4 = 12$. Now where in our prior algebraic experiences did anything like this happen? When multiplying polynomials we add the powers of the variable, and here, when we multiply the three polynomials,

$$(x^4 + x^5 + x^6 + x^7 + x^8)(x^2 + x^3 + x^4 + x^5 + x^6)(x^2 + x^3 + x^4 + x^5),$$

two of the ways to obtain x^{12} are as follows:

1) From the product $x^4x^3x^5$, where x^4 is taken from $(x^4 + x^5 + x^6 + x^7 + x^8)$, x^3 from $(x^2 + x^3 + x^4 + x^5 + x^6)$, and x^5 from $(x^2 + x^3 + x^4 + x^5)$.
2) From the product $x^4x^4x^4$, where the first x^4 is found in the first polynomial, the second x^4 in the second polynomial, and the third x^4 in the third polynomial.

Examining the product

$$(x^4 + x^5 + x^6 + x^7 + x^8)(x^2 + x^3 + x^4 + x^5 + x^6)(x^2 + x^3 + x^4 + x^5)$$

more closely, we realize that we obtain the product $x^ix^jx^k$ for every triple (i, j, k) that appears in Table 9.1. Consequently, the coefficient of x^{12} in

$$f(x) = (x^4 + x^5 + x^6 + x^7 + x^8)(x^2 + x^3 + x^4 + x^5 + x^6)(x^2 + x^3 + x^4 + x^5)$$

counts the number of distributions—namely, 14—that we seek. The function $f(x)$ is called a *generating function* for the distributions.

But where did the factors in this product come from?

The factor $x^4 + x^5 + x^6 + x^7 + x^8$, for example, indicates that we can give Grace 4 *or* 5 *or* 6 *or* 7 *or* 8 of the oranges. Once again we make use of the interplay between the exclusive *or* and ordinary addition. The coefficient of each power of x is 1 because, considering the oranges as identical objects, there is only one way to give Grace four oranges, one way to give her five oranges, and so on. Since Mary and Frank must each receive at least two oranges, the other terms $(x^2 + x^3 + x^4 + x^5 + x^6)$ and $(x^2 + x^3 + x^4 + x^5)$ start with x^2, and for Frank we stop at x^5 so that he doesn't receive more than five oranges. (Why does the term for Mary stop at x^6?)

Most of us are reasonably convinced now that the coefficient of x^{12} in $f(x)$ yields the answer. Some, however, may be a bit skeptical about this new idea. It seems that we could list the cases in Table 9.1 faster than we could multiply out the three factors in $f(x)$ or calculate the coefficient x^{12} in $f(x)$. At present that may seem true. But as we progress to problems with more unknowns and larger quantities to distribute, the generating function will more than demonstrate its worth. (The reader may realize that the rook polynomials of Chapter 8 are examples of generating functions.) For now we consider two more examples.

EXAMPLE 9.2

If there is an unlimited number (or at least 24 of each color) of red, green, white, and black jelly beans, in how many ways can Douglas select 24 of these candies so that he has an even number of white beans and at least six black ones?

The polynomials associated with the jelly bean colors are as follows:

- red (green): $1 + x + x^2 + \cdots + x^{24}$, where the leading 1 is for $1x^0$, because one possibility for the red (and green) jelly beans is that none of that color is selected
- white: $(1 + x^2 + x^4 + x^6 + \cdots + x^{24})$
- black: $(x^6 + x^7 + x^8 + \cdots + x^{24})$

So the answer to the problem is the coefficient of x^{24} in the generating function

$$f(x) = (1 + x + x^2 + \cdots + x^{24})^2(1 + x^2 + x^4 + \cdots + x^{24})(x^6 + x^7 + \cdots + x^{24}).$$

One such selection is five red, three green, eight white, and eight black jelly beans. This arises from x^5 in the first factor, x^3 in the second factor, and x^8 in the last two factors.

One more example before closing this section!

EXAMPLE 9.3

How many integer solutions are there for the equation $c_1 + c_2 + c_3 + c_4 = 25$ if $0 \le c_i$ for all $1 \le i \le 4$?

We can alternatively ask in how many ways 25 (identical) pennies can be distributed among four children.

For each child the possibilities can be described by the polynomial $1 + x + x^2 + x^3 + \cdots + x^{25}$. Then the answer to this problem is the coefficient of x^{25} in the generating function

$$f(x) = (1 + x + x^2 + \cdots + x^{25})^4.$$

The answer can also be obtained as the coefficient of x^{25} in the generating function

$$g(x) = (1 + x + x^2 + x^3 + \cdots + x^{25} + x^{26} + \cdots)^4,$$

if we rephrase the question in terms of distributing, from a large (or unlimited) number of pennies, 25 pennies among four children. [Whereas $f(x)$ is a polynomial, $g(x)$ is a *power series* in x.] Note that the terms x^k, for all $k \ge 26$, are never used. So why bother with them? Because there will be times when it is easier to compute with a power series than with a polynomial.

EXERCISES 9.1

1. For each of the following, determine a generating function and indicate the coefficient in the function that is needed to solve the problem. (Give both the polynomial and power series forms of the generating function, wherever appropriate.)

Find the number of integer solutions for the following equations:

a) $c_1 + c_2 + c_3 + c_4 = 20$, $0 \le c_i \le 7$ for all $1 \le i \le 4$

b) $c_1 + c_2 + c_3 + c_4 = 20$, $0 \le c_i$ for all $1 \le i \le 4$, with c_2 and c_3 even

c) $c_1 + c_2 + c_3 + c_4 + c_5 = 30$, $2 \le c_1 \le 4$ and $3 \le c_i \le 8$ for all $2 \le i \le 5$

d) $c_1 + c_2 + c_3 + c_4 + c_5 = 30$, $0 \le c_i$ for all $1 \le i \le 5$, with c_2 even and c_3 odd

2. Determine the generating function for the number of ways to distribute 35 pennies (from an unlimited supply) among five children if (a) there are no restrictions; (b) each child gets at least 1¢; (c) each child gets at least 2¢; (d) the oldest child gets at least 10¢; and (e) the two youngest children must each get at least 10¢.

3. a) Find the generating function for the number of ways to select 10 candy bars from large supplies of six different kinds.

b) Find the generating function for the number of ways to select, with repetitions allowed, r objects from a collection of n distinct objects.

4. a) Explain why the generating function for the number of ways to have n cents in pennies and nickels is

$$(1 + x + x^2 + x^3 + \cdots)(1 + x^5 + x^{10} + \cdots).$$

b) Find the generating function for the number of ways to have n cents in pennies, nickels, and dimes.

5. Find the generating function for the number of integer solutions to the equation $c_1 + c_2 + c_3 + c_4 = 20$ where $-3 \le c_1$, $-3 \le c_2$, $-5 \le c_3 \le 5$, and $0 \le c_4$.

6. For $S = \{a, b, c\}$, consider the function

$$\begin{aligned} f(x) &= (1 + ax)(1 + bx)(1 + cx) \\ &= 1 + ax + bx + cx + abx^2 + acx^2 \\ &\quad + bcx^2 + abcx^3. \end{aligned}$$

Here, in $f(x)$

- The coefficient of x^0 is 1 — for the subset $\emptyset$ of S.
- The coefficient of x^1 is $a + b + c$ — for the subsets $\{a\}$, $\{b\}$, and $\{c\}$ of S.
- The coefficient of x^2 is $ab + ac + bc$ — for the subsets $\{a, b\}$, $\{a, c\}$, and $\{b, c\}$ of S.

- The coefficient of x^3 is abc—for the subset $\{a, b, c\} = S$.

Consequently, $f(x)$ is the generating function for the subsets of S. For when we calculate $f(1)$, we obtain a sum wherein each of the eight summands corresponds with a subset of S; the summand 1 corresponds with $\emptyset$. [If we go one step further and set $a = b = c = 1$ in $f(x)$, then $f(1) = 8$, the number of subsets of S.]

a) Give the generating function for the subsets of

$$S = \{a, b, c, \ldots, r, s, t\}.$$

b) Answer part (a) for selections wherein each element can be rejected or selected as many as three times.

9.2 Definition and Examples: Calculational Techniques

In this section we shall examine a number of formulas and examples dealing with power series. These will be used to obtain the coefficients of particular terms in a generating function.

We start with the following concept.

Definition 9.1 Let $a_0, a_1, a_2, \ldots$ be a sequence of real numbers. The function

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots = \sum_{i=0}^{\infty} a_ix^i$$

is called the *generating function* for the given sequence.

Where could this idea have come from?

EXAMPLE 9.4 For any $n \in \mathbf{Z}^+$,

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

so $(1+x)^n$ is the generating function for the sequence

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n}, 0, 0, 0, \ldots.$$

EXAMPLE 9.5 **a)** For $n \in \mathbf{Z}^+$,

$$(1 - x^{n+1}) = (1-x)(1 + x + x^2 + x^3 + \cdots + x^n).$$

So

$$\frac{1 - x^{n+1}}{1 - x} = 1 + x + x^2 + \cdots + x^n,$$

and $(1 - x^{n+1})/(1 - x)$ is the generating function for the sequence 1, 1, 1, . . . , 1, 0, 0, 0, . . . , where the first $n + 1$ terms are 1.

b) Extending the idea in part (a), we find that

$$1 = (1 - x)(1 + x + x^2 + x^3 + x^4 + \cdots),$$

so

$$\frac{1}{1 - x}$$

is the generating function for the sequence 1, 1, 1, 1, ... [Note that $1/(1 - x) = 1 + x + x^2 + x^3 + \cdots$ is valid for all real x where $|x| < 1$; it is for this set of values that the *geometric series* $1 + x + x^2 + x^3 + \cdots$ *converges*. In our work with generating functions we shall be primarily concerned with the coefficients of the powers of x. However, later in Example 9.18, we shall use this and two other related series to evaluate infinite sums for values within the set of values for which each such infinite series converges.]

c) With

$$\frac{1}{1 - x} = 1 + x + x^2 + x^3 + \cdots = \sum_{i=0}^{\infty} x^i,$$

taking the derivative yields

$$\begin{aligned}\frac{d}{dx}\frac{1}{1 - x} &= \frac{d}{dx}(1 - x)^{-1} = (-1)(1 - x)^{-2}(-1) = \frac{1}{(1 - x)^2} \\ &= \frac{d}{dx}(1 + x + x^2 + x^3 + \cdots) = 1 + 2x + 3x^2 + 4x^3 + \cdots\end{aligned}$$

Consequently,

$$\frac{1}{(1 - x)^2}$$

is the generating function for the sequence 1, 2, 3, 4, . . . , while

$$\frac{x}{(1 - x)^2} = 0 + 1x + 2x^2 + 3x^3 + 4x^4 + \cdots$$

is the generating function for the sequence 0, 1, 2, 3, ...

d) Continuing from part (c),

$$\frac{d}{dx}\frac{x}{(1 - x)^2} = \frac{d}{dx}(0 + x + 2x^2 + 3x^3 + \cdots),$$

or

$$\frac{x + 1}{(1 - x)^3} = 1 + 2^2x + 3^2x^2 + 4^2x^3 + \cdots.$$

Hence,

$$\frac{x + 1}{(1 - x)^3}$$

generates $1^2, 2^2, 3^2, \ldots$, and

$$\frac{x(x + 1)}{(1 - x)^3}$$

generates $0^2, 1^2, 2^2, 3^2, \ldots$.

e) Now let us take one more look at the results in parts (b), (c), (d) — along with some extensions. But this time we have a change in the notation:

$$
\begin{aligned}
f_0(x) &= \frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots \\
f_1(x) &= x\frac{d}{dx} f_0(x) = \frac{x}{(1-x)^2} \\
&= 0 + x + 2x^2 + 3x^3 + \cdots \\
f_2(x) &= x\frac{d}{dx} f_1(x) = \frac{x^2+x}{(1-x)^3} \\
&= 0^2 + 1^2x + 2^2x^2 + 3^2x^3 + \cdots \\
f_3(x) &= x\frac{d}{dx} f_2(x) = \frac{x^3+4x^2+x}{(1-x)^4} \\
&= 0^3 + 1^3x + 2^3x^2 + 3^3x^3 + \cdots \\
f_4(x) &= x\frac{d}{dx} f_3(x) = \frac{x^4+11x^3+11x^2+x}{(1-x)^5} \\
&= 0^4 + 1^4x + 2^4x^2 + 3^4x^3 + \cdots
\end{aligned}
$$

Now look at the output for the Maple code in Fig. 9.1. Here we find the numerators for $f_0(x)$, $f_1(x)$, ..., $f_4(x)$, along with those for $f_5(x)$ and $f_6(x)$ [where the denominators are $(1-x)^6$ and $(1-x)^7$, respectively]. The coefficients for these numerators are exactly the Eulerian numbers we introduced in Example 4.21. We choose not to pursue this here, but the interested reader, who wants to examine this connection further, should look into reference [4].

```
> f||0(x) := 1/(1-x);
```

$$\mathrm{f0}(x) := \frac{1}{1-x}$$

```
> for i from 1 to 6 do
>    f||i(x) := simplify(x*diff(f||(i-1)(x),x)):
>    print(sort(expand((-1)^(i+1)*numer(f||i(x)))));
> od:
```

$$x$$
$$x^2 + x$$
$$x^3 + 4x^2 + x$$
$$x^4 + 11x^3 + 11x^2 + x$$
$$x^5 + 26x^4 + 66x^3 + 26x^2 + x$$
$$x^6 + 57x^5 + 302x^4 + 302x^3 + 57x^2 + x$$

Figure 9.1

EXAMPLE 9.6

a) Rewriting the result in part (b) of Example 9.5, we have

$$\frac{1}{1-y} = 1 + y + y^2 + y^3 + \cdots.$$

Upon substituting $2x$ for y, we then learn that

$$\frac{1}{1-2x} = 1 + (2x) + (2x)^2 + (2x)^3 + \cdots = 1 + 2x + 2^2x^2 + 2^3x^3 + \cdots,$$

so $1/(1-2x)$ is the generating function for the sequence $1\ (= 2^0)$, $2\ (= 2^1)$, 2^2, $2^3, \ldots$. In fact, for each $a \in \mathbf{R}$, it follows that $1/(1-ax) = 1 + (ax) + (ax)^2 + (ax)^3 + \cdots = 1 + ax + a^2x^2 + a^3x^3 + \cdots$, so $1/(1-ax)$ is the generating function for the sequence $1\ (= a^0), a\ (= a^1), a^2, a^3, \ldots$. [Here we want $0^0 = 1$ for the case where $a = 0$.]

b) Again, from part (b) of Example 9.5, we know that the generating function for the sequence $1, 1, 1, 1, \ldots$ is $f(x) = 1/(1-x)$. Therefore the function

$$g(x) = f(x) - x^2 = \frac{1}{1-x} - x^2$$

is the generating function for the sequence $1, 1, 0, 1, 1, 1, \ldots$, while the function

$$h(x) = f(x) + 2x^3 = \frac{1}{1-x} + 2x^3$$

generates the sequence $1, 1, 1, 3, 1, 1, \ldots$.

c) Finally, can we use the results of Example 9.5 to find a generating function for the sequence $0, 2, 6, 12, 20, 30, 42, \ldots$?

Here we observe that

$$\begin{aligned} a_0 &= 0 = 0^2 + 0, & a_1 &= 2 = 1^2 + 1, \\ a_2 &= 6 = 2^2 + 2, & a_3 &= 12 = 3^2 + 3, \\ a_4 &= 20 = 4^2 + 4, \ldots. \end{aligned}$$

In general, we have $a_n = n^2 + n$, for each $n \geq 0$.

Using the results from parts (c) and (d) of Example 9.5, we now find that

$$\frac{x(x+1)}{(1-x)^3} + \frac{x}{(1-x)^2} = \frac{x(x+1) + x(1-x)}{(1-x)^3} = \frac{2x}{(1-x)^3}$$

is the generating function for the given sequence. (The solution here depends upon our ability to recognize each a_n as the sum of n^2 and n. If we do not see this, we may be unable to answer the given question. Consequently, in Example 10.6 of the next chapter, we shall examine another technique to help us recognize the formula for a_n.)

For each $n \in \mathbf{Z}^+$, the binomial theorem tells us that $(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n$. We want to extend this idea to cases where (a) $n < 0$ and (b) n is not necessarily an integer.

With $n, r \in \mathbf{Z}^+$ and $n \geq r > 0$, we have

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{n(n-1)(n-2)\cdots(n-r+1)}{r!}.$$

If $n \in \mathbf{R}$, we use

$$\frac{n(n-1)(n-2)\cdots(n-r+1)}{r!}$$

as the definition of $\binom{n}{r}$.

Then, for example, if $n \in \mathbf{Z}^+$, we have

$$\begin{aligned}\binom{-n}{r} &= \frac{(-n)(-n-1)(-n-2)\cdots(-n-r+1)}{r!}\\ &= \frac{(-1)^r(n)(n+1)(n+2)\cdots(n+r-1)}{r!}\\ &= \frac{(-1)^r(n+r-1)!}{(n-1)!\,r!} = (-1)^r\binom{n+r-1}{r}.\end{aligned}$$

Finally, for each *real* number n, we define $\binom{n}{0} = 1$.

EXAMPLE 9.7

For $n \in \mathbf{Z}^+$, the Maclaurin series expansion for $(1+x)^{-n}$ is given by

$$\begin{aligned}(1+x)^{-n} &= 1 + (-n)x + (-n)(-n-1)x^2/2!\\ &\quad + (-n)(-n-1)(-n-2)x^3/3! + \cdots\\ &= 1 + \sum_{r=1}^{\infty} \frac{(-n)(-n-1)(-n-2)\cdots(-n-r+1)}{r!}x^r\\ &= \sum_{r=0}^{\infty}(-1)^r\binom{n+r-1}{r}x^r.\end{aligned}$$

Hence $(1+x)^{-n} = \binom{-n}{0} + \binom{-n}{1}x + \binom{-n}{2}x^2 + \cdots = \sum_{r=0}^{\infty}\binom{-n}{r}x^r$. This generalizes the binomial theorem of Chapter 1 and shows us that $(1+x)^{-n}$ is the generating function for the sequence $\binom{-n}{0}, \binom{-n}{1}, \binom{-n}{2}, \binom{-n}{3}, \ldots$.

EXAMPLE 9.8

Find the coefficient of x^5 in $(1-2x)^{-7}$.

With $y = -2x$, use the result in Example 9.7 to write $(1-2x)^{-7} = (1+y)^{-7} = \sum_{r=0}^{\infty}\binom{-7}{r}y^r = \sum_{r=0}^{\infty}\binom{-7}{r}(-2x)^r$. Consequently, the coefficient of x^5 is $\binom{-7}{5}(-2)^5 = (-1)^5\binom{7+5-1}{5}(-32) = (32)\binom{11}{5} = 14{,}784$.

EXAMPLE 9.9

For each real number n, the Maclaurin series expansion for $(1+x)^n$ is

$$\begin{aligned}&1 + nx + n(n-1)x^2/2! + n(n-1)(n-2)x^3/3! + \cdots\\ &\qquad = 1 + \sum_{r=1}^{\infty}\frac{n(n-1)(n-2)\cdots(n-r+1)}{r!}x^r.\end{aligned}$$

Therefore,

$$(1+3x)^{-1/3} = 1 + \sum_{r=1}^{\infty} \frac{(-1/3)(-4/3)(-7/3)\cdots((-3r+2)/3)}{r!}(3x)^r$$
$$= 1 + \sum_{r=1}^{\infty} \frac{(-1)(-4)(-7)\cdots(-3r+2)}{r!}x^r,$$

and $(1+3x)^{-1/3}$ generates the sequence $1, -1, (-1)(-4)/2!, (-1)(-4)(-7)/3!, \ldots, (-1)(-4)(-7)\cdots(-3r+2)/r!, \ldots$.

EXAMPLE 9.10

Determine the coefficient of x^{15} in $f(x) = (x^2+x^3+x^4+\cdots)^4$.

Since $(x^2+x^3+x^4+\cdots) = x^2(1+x+x^2+\cdots) = x^2/(1-x)$, the coefficient of x^{15} in $f(x)$ is the coefficient of x^{15} in $(x^2/(1-x))^4 = x^8/(1-x)^4$. Hence the coefficient sought is that of x^7 in $(1-x)^{-4}$, namely, $\binom{-4}{7}(-1)^7 = (-1)^7\binom{4+7-1}{7}(-1)^7 = \binom{10}{7} = 120$.

In general, for $n \in \mathbf{Z}^+$, the coefficient of x^n in $f(x)$ is 0, when $0 \le n \le 7$. For all $n \ge 8$, the coefficient of x^n in $f(x)$ is the coefficient of x^{n-8} in $(1-x)^{-4}$, which is $\binom{-4}{n-8} \cdot (-1)^{n-8} = \binom{n-5}{n-8}$.

Before continuing, we collect the identities shown in Table 9.2 (on page 424) for future reference.

The next two examples show how generating functions can be applied to derive some of our earlier results.

EXAMPLE 9.11

In how many ways can we select, with repetitions allowed, r objects from n distinct objects?

For each of the n distinct objects, the geometric series $1+x+x^2+x^3+\cdots$ represents the possible choices for that object (namely none, one, two, ...). Considering all of the n distinct objects, the generating function is

$$f(x) = (1+x+x^2+x^3+\cdots)^n,$$

and the required answer is the coefficient of x^r in $f(x)$. Now from identities 5 and 8 in Table 9.2 we have

$$(1+x+x^2+x^3+\cdots)^n = \left(\frac{1}{1-x}\right)^n = \frac{1}{(1-x)^n} = \sum_{i=0}^{\infty}\binom{n+i-1}{i}x^i,$$

so the coefficient of x^r is

$$\binom{n+r-1}{r},$$

the result we found in Chapter 1.

EXAMPLE 9.12

Once again we consider the problem of counting the compositions of a positive integer n — this time using generating functions.

Start with

$$\frac{x}{1-x} = x + x^2 + x^3 + x^4 + \cdots$$

Table 9.2

For all $m, n \in \mathbf{Z}^+$, $a \in \mathbf{R}$,

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

2) $(1+ax)^n = \binom{n}{0} + \binom{n}{1}ax + \binom{n}{2}a^2x^2 + \cdots + \binom{n}{n}a^nx^n$

3) $(1+x^m)^n = \binom{n}{0} + \binom{n}{1}x^m + \binom{n}{2}x^{2m} + \cdots + \binom{n}{n}x^{nm}$

4) $(1-x^{n+1})/(1-x) = 1 + x + x^2 + \cdots + x^n$

5) $1/(1-x) = 1 + x + x^2 + x^3 + \cdots = \sum_{i=0}^{\infty} x^i$

6) $$\begin{aligned} 1/(1-ax) &= 1 + (ax) + (ax)^2 + (ax)^3 + \cdots \\ &= \textstyle\sum_{i=0}^{\infty}(ax)^i = \sum_{i=0}^{\infty} a^ix^i \\ &= 1 + ax + a^2x^2 + a^3x^3 + \cdots \end{aligned}$$

7) $$\begin{aligned} 1/(1+x)^n &= \binom{-n}{0} + \binom{-n}{1}x + \binom{-n}{2}x^2 + \cdots \\ &= \textstyle\sum_{i=0}^{\infty} \binom{-n}{i}x^i \\ &= 1 + (-1)\binom{n+1-1}{1}x + (-1)^2\binom{n+2-1}{2}x^2 + \cdots \\ &= \textstyle\sum_{i=0}^{\infty}(-1)^i\binom{n+i-1}{i}x^i \end{aligned}$$

8) $$\begin{aligned} 1/(1-x)^n &= \binom{-n}{0} + \binom{-n}{1}(-x) + \binom{-n}{2}(-x)^2 + \cdots \\ &= \textstyle\sum_{i=0}^{\infty} \binom{-n}{i}(-x)^i \\ &= 1 + (-1)\binom{n+1-1}{1}(-x) + (-1)^2\binom{n+2-1}{2}(-x)^2 + \cdots \\ &= \textstyle\sum_{i=0}^{\infty} \binom{n+i-1}{i}x^i \end{aligned}$$

If $f(x) = \sum_{i=0}^{\infty} a_ix^i$, $g(x) = \sum_{i=0}^{\infty} b_ix^i$, and $h(x) = f(x)g(x)$, then $h(x) = \sum_{i=0}^{\infty} c_ix^i$, where for all $k \geq 0$,

$$c_k = a_0b_k + a_1b_{k-1} + \cdots + a_{k-1}b_1 + a_kb_0 = \sum_{j=0}^{k} a_jb_{k-j}.$$

where, for example, the coefficient of x^4 is 1, for the one-summand composition of 4—namely, 4. To obtain the number of compositions of n where there are two summands, we need the coefficient of x^n in $(x + x^2 + x^3 + x^4 + \cdots)^2 = [x/(1-x)]^2 = x^2/(1-x)^2$. Here, for instance, we obtain x^4 in $(x + x^2 + x^3 + x^4 + \cdots)^2$ from the products $x^1 \cdot x^3$, $x^2 \cdot x^2$, and $x^3 \cdot x^1$. So the coefficient of x^4 in $x^2/(1-x)^2$ is 3—for the three two-summand compositions $1+3$, $2+2$, and $3+1$ (of 4). Continuing with the three-summand compositions we now examine $(x + x^2 + x^3 + x^4 + \cdots)^3 = [x/(1-x)]^3 = x^3/(1-x)^3$. Once again we look at the ways x^4 comes about—namely, from the products $x^1 \cdot x^1 \cdot x^2$, $x^1 \cdot x^2 \cdot x^1$, $x^2 \cdot x^1 \cdot x^1$. So here the coefficient of x^4 is 3, which accounts for the compositions $1+1+2$, $1+2+1$, and $2+1+1$ (of 4). Finally, the coefficient of x^4 in $(x + x^2 + x^3 + x^4 + \cdots)^4 = [x/(1-x)]^4 = x^4/(1-x)^4$ is 1—for the one four-summand composition $1+1+1+1$ (of 4).

The results in the previous paragraph tell us that the coefficient of x^4 in $\sum_{i=1}^{4}[x/(1-x)]^i$ is $1+3+3+1 = 8\ (= 2^3)$, the number of compositions of 4. In fact, this is also the coefficient of x^4 in $\sum_{i=1}^{\infty}[x/(1-x)]^i$. Generalizing the situation we find that the number of compositions of a positive integer n is the coefficient of x^n in the generating function

$f(x) = \sum_{i=1}^{\infty}[x/(1-x)]^i$. But if we set $y = x/(1-x)$, it then follows that

$$f(x) = \sum_{i=1}^{\infty} y^i = y\sum_{i=0}^{\infty} y^i = y\left(\frac{1}{1-y}\right) = \left(\frac{x}{1-x}\right)\left[\frac{1}{1-\left(\frac{x}{1-x}\right)}\right] = \left(\frac{x}{1-x}\right)\left[\frac{1}{\frac{1-x-x}{1-x}}\right]$$
$$= x/(1-2x) = x[1 + (2x) + (2x)^2 + (2x)^3 + \cdots]$$
$$= 2^0x + 2^1x^2 + 2^2x^3 + 2^3x^4 + \cdots.$$

So the number of compositions of a positive integer n is the coefficient of x^n in $f(x)$ — and this is 2^{n-1} (as we found earlier in Examples 1.37, 3.11, and 4.12.)

EXAMPLE 9.13

Before we look at any specific compositions, let us start by examining identity 4 in Table 9.2. When x is replaced by 2 in this identity, the result tells us that for all $n \in \mathbf{Z}^+$, $1 + 2 + 2^2 + \cdots + 2^n = (1 - 2^{n+1})/(1-2) = 2^{n+1} - 1$. [This result was also established by the Principle of Mathematical Induction — in part (a) of Exercise 2 for Section 4.1.] All well and good — but where would one ever use such a formula? In Table 9.3 we find the special compositions of 6 and 7 that read the same left to right as right to left. These are the *palindromes* of 6 and 7. We find that for 7 there are $1 + (1 + 2 + 4) = 1 + (1 + 2^1 + 2^2) = 1 + (2^3 - 1) = 2^3$ palindromes. There is one palindrome with one summand — namely, 7. There is also one palindrome where the center summand is 5 and where we place the one composition of 1 on either side of this summand.

Table 9.3

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

For the center summand 3 we place one of the two compositions of 2 on the right (of 3) and then match it on the left, with the same composition, in reverse order. This procedure provides the third and fourth palindromes of 7 in the table. Finally, when the center summand is 1, we put a given composition of 3 on the right of this 1 and match it on the left with the same composition, in reverse order. There are $2^{3-1} = 4$ compositions of 3, so this procedure results in the last four palindromes of 7 in the table.

The situation is similar for the palindromes of 6 except for the case where, instead of 0 as the center summand, a plus sign appears in the center. Here we obtain the last $2^{3-1} = 4$ palindromes of 6 in the table — one for each composition of 3. Summarizing for $n = 6$ we have

i)	Center summand 6	1 palindrome
ii)	Center summand 4	1 ($= 2^{1-1}$) palindrome
iii)	Center summand 2	2 ($= 2^{2-1}$) palindromes
iv)	Plus sign at the center	4 ($= 2^{3-1}$) palindromes

So there are $1 + (1 + 2^1 + 2^2) = 1 + (2^3 - 1) = 2^3$ palindromes for 6.

Now we look at the general situation. For $n = 1$ there is one palindrome. If $n = 2k + 1$, for $k \in \mathbf{Z}^+$, then there is one palindrome with center summand n. For $1 \le t \le k$, there are 2^{t-1} palindromes of n with center summand $n - 2t$. (One palindrome for each of the 2^{t-1} compositions of t.) Hence the total number of palindromes of n is $1 + (1 + 2^1 + 2^2 + \cdots + 2^{k-1}) = 1 + (2^k - 1) = 2^k = 2^{(n-1)/2}$. Now consider n even, say $n = 2k$, for $k \in \mathbf{Z}^+$. Here there is also one palindrome with center summand n and, for $1 \le s \le k - 1$, there are 2^{s-1} palindromes of n with center summand $n - 2s$. (One palindrome for each of the 2^{s-1} compositions of s.) In addition, there are 2^{k-1} palindromes where a plus sign is at the center. (One palindrome for each of the 2^{k-1} compositions of k.) In total, n has $1 + (1 + 2^1 + 2^2 + \cdots + 2^{k-2} + 2^{k-1}) = 1 + (2^k - 1) = 2^k = 2^{n/2}$ palindromes.

The preceding results can be simplified. Observe that for $n \in \mathbf{Z}^+$, n has $2^{\lfloor n/2 \rfloor}$ palindromes.

Having dealt with compositions (once again) and palindromes, we continue at this point with some additional examples dealing with generating functions.

EXAMPLE 9.14

In how many ways can a police captain distribute 24 rifle shells to four police officers so that each officer gets at least three shells, but not more than eight?

The choices for the number of shells each officer receives are given by $x^3 + x^4 + \cdots + x^8$. There are four officers, so the resulting generating function is

$$f(x) = (x^3 + x^4 + \cdots + x^8)^4.$$

We seek the coefficient of x^{24} in $f(x)$. With $(x^3 + x^4 + \cdots + x^8)^4 = x^{12}(1 + x + x^2 + \cdots + x^5)^4 = x^{12}((1 - x^6)/(1 - x))^4$, the answer is the coefficient of x^{12} in $(1 - x^6)^4 \cdot (1 - x)^{-4} = \left[1 - \binom{4}{1}x^6 + \binom{4}{2}x^{12} - \binom{4}{3}x^{18} + x^{24}\right]\left[\binom{-4}{0} + \binom{-4}{1}(-x) + \binom{-4}{2}(-x)^2 + \cdots\right]$, which is $\left[\binom{-4}{12}(-1)^{12} - \binom{4}{1}\binom{-4}{6}(-1)^6 + \binom{4}{2}\binom{-4}{0}\right] = \left[\binom{15}{12} - \binom{4}{1}\binom{9}{6} + \binom{4}{2}\right] = 125$.

EXAMPLE 9.15

Verify that for all $n \in \mathbf{Z}^+$, $\binom{2n}{n} = \sum_{i=0}^{n} \binom{n}{i}^2$.

Since $(1 + x)^{2n} = [(1 + x)^n]^2$, by comparison of coefficients (of like powers of x), the coefficient of x^n in $(1 + x)^{2n}$, which is $\binom{2n}{n}$, must equal the coefficient of x^n in $\left[\binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n\right]^2$, and this is $\binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \binom{n}{2}\binom{n}{n-2} + \cdots + \binom{n}{n}\binom{n}{0}$. With $\binom{n}{r} = \binom{n}{n-r}$, for all $0 \le r \le n$, the result follows.

EXAMPLE 9.16

Determine the coefficient of x^8 in $\dfrac{1}{(x - 3)(x - 2)^2}$.

Since $1/(x - a) = (-1/a)(1/(1 - (x/a))) = (-1/a)[1 + (x/a) + (x/a)^2 + \cdots]$ for any $a \ne 0$, we could solve this problem by finding the coefficient of x^8 in $1/[(x - 3)(x - 2)^2]$ expressed as $(-1/3)[1 + (x/3) + (x/3)^2 + \cdots](1/4)\left[\binom{-2}{0} + \binom{-2}{1}(-x/2) + \binom{-2}{2}(-x/2)^2 + \cdots\right]$.

An alternative technique uses the partial fraction decomposition:

$$\frac{1}{(x - 3)(x - 2)^2} = \frac{A}{x - 3} + \frac{B}{x - 2} + \frac{C}{(x - 2)^2}.$$

This decomposition implies that

$$1 = A(x - 2)^2 + B(x - 2)(x - 3) + C(x - 3),$$

or

$$0 \cdot x^2 + 0 \cdot x + 1 = 1 = (A + B)x^2 + (-4A - 5B + C)x + (4A + 6B - 3C).$$

By comparing coefficients (for x^2, x, and 1, respectively), we find that $A + B = 0$, $-4A - 5B + C = 0$, and $4A + 6B - 3C = 1$. Solving these equations yields $A = 1$, $B = -1$, and $C = -1$. Hence

$$\begin{aligned}\frac{1}{(x-3)(x-2)^2} &= \frac{1}{x-3} - \frac{1}{x-2} - \frac{1}{(x-2)^2} \\ &= \left(\frac{-1}{3}\right)\frac{1}{1-(x/3)} + \left(\frac{1}{2}\right)\frac{1}{1-(x/2)} + \left(\frac{-1}{4}\right)\frac{1}{(1-(x/2))^2} \\ &= \left(\frac{-1}{3}\right)\sum_{i=0}^{\infty}\left(\frac{x}{3}\right)^i + \left(\frac{1}{2}\right)\sum_{i=0}^{\infty}\left(\frac{x}{2}\right)^i \\ &\quad + \left(\frac{-1}{4}\right)\left[\binom{-2}{0} + \binom{-2}{1}\left(\frac{-x}{2}\right) + \binom{-2}{2}\left(\frac{-x}{2}\right)^2 + \cdots\right].\end{aligned}$$

The coefficient of x^8 is $(-1/3)(1/3)^8 + (1/2)(1/2)^8 + (-1/4)\binom{-2}{8}(-1/2)^8 = -[(1/3)^9 + 7(1/2)^{10}]$.

EXAMPLE 9.17

Use generating functions to determine how many four-element subsets of $S = \{1, 2, 3, \ldots, 15\}$ contain no consecutive integers.

a) Consider one such subset (say $\{1, 3, 7, 10\}$), and write $1 \le 1 < 3 < 7 < 10 \le 15$. We see that this set of inequalities determines the differences $1 - 1 = 0$, $3 - 1 = 2$, $7 - 3 = 4$, $10 - 7 = 3$, and $15 - 10 = 5$, and these differences sum to 14. Considering another such subset—say $\{2, 5, 11, 15\}$, we write $1 \le 2 < 5 < 11 < 15 \le 15$; these inequalities yield the differences 1, 3, 6, 4, and 0, which also sum to 14.

Turning things around, we find that the nonnegative integers 0, 2, 3, 2, and 7 sum to 14 and they are the differences that arise from the inequalities $1 \le 1 < 3 < 6 < 8 \le 15$ (for the subset $\{1, 3, 6, 8\}$).

These examples suggest a one-to-one correspondence between the four-element subsets to be counted and the integer solutions to $c_1 + c_2 + c_3 + c_4 + c_5 = 14$ where $0 \le c_1, c_5$, and $2 \le c_2, c_3, c_4$. (*Note*: Here $c_2, c_3, c_4 \ge 2$ guarantee that there are no consecutive integers in the subset.) The answer is the coefficient of x^{14} in

$$\begin{aligned}f(x) &= (1 + x + x^2 + x^3 + \cdots)(x^2 + x^3 + x^4 + \cdots)^3(1 + x + x^2 + x^3 + \cdots) \\ &= x^6(1 - x)^{-5}.\end{aligned}$$

This then is the coefficient of x^8 in $(1 - x)^{-5}$, which is $\binom{-5}{8}(-1)^8 = \binom{5+8-1}{8} = \binom{12}{8} = 495$.

b) Another way to look at the problem is as follows.

For the subset $\{1, 3, 7, 10\}$, we examine the strict inequalities $0 < 1 < 3 < 7 < 10 < 16$ and consider how many integers there are strictly between each successive pair of these numbers. Here we get 0, 1, 3, 2, and 5: 0 because there is no integer between 0 and 1, 1 for the integer 2 between 1 and 3, 3 for the integers 4, 5, 6 between 3 and 7, and so on. These five integers sum to 11. When we do the same thing for the subset $\{2, 5, 11, 15\}$, the strict inequalities $0 < 2 < 5 < 11 < 15 < 16$ yield the results 1, 2, 5, 3, and 0, which also sum to 11.

On the other hand, we find that the nonnegative integers 0, 1, 2, 1, and 7 add up to 11 and they arise as the numbers of distinct integers between the integers in the five successive strict inequalities $0 < 1 < 3 < 6 < 8 < 16$. These correspond to the subset $\{1, 3, 6, 8\}$.

These results suggest a one-to-one correspondence between the desired subsets and the integer solutions to $b_1 + b_2 + b_3 + b_4 + b_5 = 11$, where $0 \leq b_1, b_5$ and $1 \leq b_2, b_3, b_4$. (*Note*: In this case, $b_1, b_2, b_3 \geq 1$ guarantee that there are no consecutive integers in the subset.) The number of these solutions is the coefficient of x^{11} in

$$\begin{aligned} g(x) &= (1 + x + x^2 + \cdots)(x + x^2 + x^3 + \cdots)^3(1 + x + x^2 + \cdots) \\ &= x^3(1 - x)^{-5}. \end{aligned}$$

The answer is $\binom{-5}{8}(-1)^8 = 495$, as above. (The reader may now wish to look back at Supplementary Exercise 15 in Chapter 3.)

Our next example takes us back to the optional material in Chapter 3 where we first encountered the idea of the sample space. But now that we know about generating functions we will be able to deal with a sample space that is discrete but *not* finite — that is, a countably infinite† sample space.

EXAMPLE 9.18‡

a) Suppose that Brianna takes an actuarial examination until she passes it. Further, suppose the probability that Brianna passes the examination on any given attempt is 0.8 and that the result of each attempt, after the first, is independent of any previous attempt. If we let P denote "pass" and F denote "fail", for any given attempt, then here our sample space may be expressed as $\mathcal{S} = \{\text{P, FP, FFP, FFFP}, \ldots\}$, where, for example, $Pr(\text{FFP})$ — the probability Brianna fails the exam twice before she passes it — is given by $(0.2)^2(0.8)$. In addition, the sum of the probabilities for the outcomes in $\mathcal{S}$ is $(0.8) + (0.2)(0.8) + (0.2)^2(0.8) + (0.2)^3(0.8) + \cdots = \sum_{i=0}^{\infty}(0.2)^i(0.8) = (0.8)\sum_{i=0}^{\infty}(0.2)^i = (0.8)\left(\frac{1}{1-0.2}\right) = (0.8)\left(\frac{1}{0.8}\right) = 1$, as it should be — for according to the second axiom of probability (in Section 3.5) we expect $Pr(\mathcal{S}) = 1$. [Note that $\sum_{i=0}^{\infty}(0.2)^i = \frac{1}{1-0.2}$ follows from the result in part (b) of Example 9.5. The given geometric series converges to $\frac{1}{1-0.2}$ because $|0.2| < 1$.]

b) Now suppose we want to know the probability Brianna passes the exam on an even-numbered attempt. That is, we want $Pr(A)$ where A is the event $\{\text{FP, FFFP}, \ldots\}$.

At this point let us introduce the discrete random variable Y where Y counts the number of attempts up to and including the one where Brianna passes the exam. Then the probability distribution for Y is given by $Pr(Y = y) = (0.2)^{y-1}(0.8)$, $y \geq 1$. So $Pr(A)$ can be determined as follows: $Pr(A) = \sum_{i=1}^{\infty} Pr(Y = 2i) = \sum_{i=1}^{\infty}(0.2)^{2i-1}(0.8) = (0.8)\sum_{i=1}^{\infty}(0.2)^{2i-1} = 0.8[(0.2) + (0.2)^3 + (0.2)^5 + \cdots] = (0.8)(0.2)[1 + (0.2)^2 + (0.2)^4 + \cdots] = (0.8)(0.2)\frac{1}{1-(0.2)^2} = \frac{(0.8)(0.2)}{0.96} = \frac{1}{6}$. And once again we have used the result in part (b) of Example 9.5, this time with $x = (0.2)^2$, where $|(0.2)^2| = |0.04| < 1$.

---

†The reader can learn more about countably infinite sets from the material in Appendix 3.

‡This example uses material from the optional sections of Chapter 3. It may be skipped without any loss of continuity.

c) Continuing with Y, now we'd like to find $E(Y)$, the number of times Brianna expects to take the actuarial exam before she passes it. To determine $E(Y)$ we'll start with the formula $1/(1-t) = 1 + t + t^2 + t^3 + \cdots$ and go one step further. Taking the derivative of both sides, we find [as in Example 9.5(c)] that

$$(-1)(1-t)^{-2}(-1) = \frac{1}{(1-t)^2} = \frac{d}{dt}\left[\frac{1}{1-t}\right] = 1 + 2t + 3t^2 + 4t^3 + \cdots,$$

where this series likewise converges† for $|t| < 1$. Therefore,

$$\begin{aligned} E(Y) &= \sum_{y=1}^{\infty} yPr(Y = y) = \sum_{y=1}^{\infty} y(0.2)^{y-1}(0.8) \\ &= (0.8)\sum_{y=1}^{\infty} y(0.2)^{y-1} = (0.8)[1 + 2(0.2) + 3(0.2)^2 + 4(0.2)^3 + \cdots] \\ &= (0.8)\frac{1}{(1-0.2)^2} = (0.8)\frac{1}{(0.8)^2} = \frac{1}{0.8} = \frac{5}{4} = 1.25. \end{aligned}$$

So Brianna expects to take the exam 1.25 times before she passes it.

d) Finally, to determine $\mathrm{Var}(Y)$ we first want to find $E(Y^2)$. To do so we first multiply the result in part (c) by t and find [as in Example 9.5(c)] that

$$\frac{t}{(1-t)^2} = t + 2t^2 + 3t^3 + 4t^4 + \cdots.$$

Differentiating both sides of this equation now gives us

$$\begin{aligned} \frac{(1-t)^2(1) - t(2)(1-t)(-1)}{(1-t)^4} = \frac{1+t}{(1-t)^3} &= \frac{d}{dt}\left[\frac{t}{(1-t)^2}\right] \\ &= 1^2 + 2^2t + 3^2t^2 + 4^2t^3 + \cdots, \end{aligned}$$

and this series is also convergent‡ for $|t| < 1$. So now we have

$$\begin{aligned} E(Y^2) &= \sum_{y=1}^{\infty} y^2 Pr(Y = y) = \sum_{y=1}^{\infty} y^2(0.2)^{y-1}(0.8) \\ &= (0.8)\sum_{y=1}^{\infty} y^2(0.2)^{y-1} = (0.8)[1^2 + 2^2(0.2) + 3^2(0.2)^2 + 4^2(0.2)^3 + \cdots] \\ &= (0.8)\left[\frac{1+0.2}{(1-0.2)^3}\right] = \frac{1.2}{(0.8)^2} = \frac{15}{8}. \end{aligned}$$

---

†Using the Ratio Test from calculus, one finds that

$$\lim_{n\to\infty}\left|\frac{(n+1)t^n}{nt^{n-1}}\right| = |t|\lim_{n\to\infty}\frac{n+1}{n} = |t|\lim_{n\to\infty}\left(1 + \frac{1}{n}\right) = |t|(1) = |t|.$$

When $t = \pm 1$, $\lim_{n\to\infty} nt^{n-1} \neq 0$, so the series does not converge for $t = \pm 1$. Consequently, this infinite series converges for $|t| < 1$.

‡Once again we use the Ratio Test from calculus. Here

$$\lim_{n\to\infty}\left|\frac{(n+1)^2t^n}{n^2t^{n-1}}\right| = |t|\lim_{n\to\infty}\frac{(n+1)^2}{n^2} = |t|\lim_{n\to\infty}\left(1 + \frac{1}{n}\right)^2 = |t|(1)^2 = |t|.$$

When $t = \pm 1$, $\lim_{n\to\infty} n^2t^{n-1} \neq 0$, so the series does not converge for $t = \pm 1$. Consequently, this infinite series converges for $|t| < 1$.

Consequently,

$$\mathrm{Var}(Y) = E(Y^2) - [E(Y)]^2 = \frac{15}{8} - \left(\frac{5}{4}\right)^2 = \frac{30-25}{16} = \frac{5}{16}.$$

The preceding example introduced us to a new discrete random variable — namely, the *geometric random variable*. In this situation we perform a Bernoulli trial until we are successful (for the first time). As with the binomial random variable the outcome of each trial, after the first, is independent of the outcome for any previous trial. Further, the probability of success for each Bernoulli trial is p, and the probability of failure is $q = 1 - p$.

If we let the random variable Y count the number of trials until we are finally successful, then Y is a discrete random variable with probability distribution given by

$$Pr(Y = y) = q^{y-1}p, \quad y = 1, 2, 3, \ldots.$$

In addition, we find that

$$E(Y) = \frac{1}{p} \quad \text{and} \quad \mathrm{Var}(Y) = \frac{q}{p^2}.$$

The following example uses the last identity in Table 9.2. (This identity was used earlier in Examples 9.14 and 9.15 — but rather implicitly.)

EXAMPLE 9.19

Let $f(x) = x/(1-x)^2$. This is the generating function for the sequence $a_0, a_1, a_2, \ldots$, where $a_k = k$ for all $k \in \mathbf{N}$. The function $g(x) = x(x+1)/(1-x)^3$ generates the sequence $b_0, b_1, b_2, \ldots$, for $b_k = k^2$, $k \in \mathbf{N}$.

The function $h(x) = f(x)g(x)$ consequently gives us $a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots$, so $h(x)$ is the generating function for the sequence $c_0, c_1, c_2, \ldots$, where for each $k \in \mathbf{N}$,

$$c_k = a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \cdots + a_{k-2}b_2 + a_{k-1}b_1 + a_kb_0.$$

Here, for example, we find that

$$\begin{aligned} c_0 &= 0 \cdot 0^2 = 0 \\ c_1 &= 0 \cdot 1^2 + 1 \cdot 0^2 = 0 \\ c_2 &= 0 \cdot 2^2 + 1 \cdot 1^2 + 2 \cdot 0^2 = 1 \\ c_3 &= 0 \cdot 3^2 + 1 \cdot 2^2 + 2 \cdot 1^2 + 3 \cdot 0^2 = 6 \end{aligned}$$

and, in general, $c_k = \sum_{i=0}^{k} i(k-i)^2$. (We shall simplify this summation formula in the Section Exercises.)

Whenever a sequence $c_0, c_1, c_2, \ldots$ arises from two generating functions $f(x)$ [for $a_0, a_1, a_2, \ldots$] and $g(x)$ [for $b_0, b_1, b_2, \ldots$], as in this example, the sequence $c_0, c_1, c_2, \ldots$ is called the *convolution* of the sequences $a_0, a_1, a_2, \ldots$ and $b_0, b_1, b_2, \ldots$.

Our last example provides one more instance of the convolution of sequences.

EXAMPLE 9.20

For $f(x) = 1/(1-x) = 1 + x + x^2 + x^3 + \cdots$ and $g(x) = 1/(1+x) = 1 - x + x^2 - x^3 + \cdots$, we find that

$$f(x)g(x) = 1/[(1-x)(1+x)] = 1/(1-x^2) = 1 + x^2 + x^4 + x^6 + \cdots.$$

Consequently, the sequence 1, 0, 1, 0, 1, 0, ... is the convolution of the sequences 1, 1, 1, 1, 1, 1, ... and 1, −1, 1, −1, 1, −1, ...

EXERCISES 9.2

1. Find generating functions for the following sequences. [For example, in the case of the sequence 0, 1, 3, 9, 27, ..., the answer required is $x/(1-3x)$, not $\sum_{i=0}^{\infty} 3^i x^{i+1}$ or simply $0 + x + 3x^2 + 9x^3 + \cdots$.]

a) $\binom{8}{0}, \binom{8}{1}, \binom{8}{2}, \ldots, \binom{8}{8}$

b) $\binom{8}{1}, 2\binom{8}{2}, 3\binom{8}{3}, \ldots, 8\binom{8}{8}$

c) $1, -1, 1, -1, 1, -1, \ldots$

d) $0, 0, 0, 6, -6, 6, -6, 6, \ldots$

e) $1, 0, 1, 0, 1, 0, 1, \ldots$

f) $0, 0, 1, a, a^2, a^3, \ldots, a \neq 0$

2. Determine the sequence generated by each of the following generating functions.

a) $f(x) = (2x-3)^3$ **b)** $f(x) = x^4/(1-x)$

c) $f(x) = x^3/(1-x^2)$ **d)** $f(x) = 1/(1+3x)$

e) $f(x) = 1/(3-x)$

f) $f(x) = 1/(1-x) + 3x^7 - 11$

3. In each of the following, the function $f(x)$ is the generating function for the sequence $a_0, a_1, a_2, \ldots$, whereas the sequence $b_0, b_1, b_2, \ldots$ is generated by the function $g(x)$. Express $g(x)$ in terms of $f(x)$.

a) $b_3 = 3$
$b_n = a_n,\ n \in \mathbf{N},\ n \neq 3$

b) $b_3 = 3$
$b_7 = 7$
$b_n = a_n,\ n \in \mathbf{N},\ n \neq 3, 7$

c) $b_1 = 1$
$b_3 = 3$
$b_n = 2a_n,\ n \in \mathbf{N},\ n \neq 1, 3$

d) $b_1 = 1$
$b_3 = 3$
$b_7 = 7$
$b_n = 2a_n + 5,\ n \in \mathbf{N},\ n \neq 1, 3, 7$

4. Determine the constant (that is, the coefficient of x^0) in $(3x^2 - (2/x))^{15}$.

5. a) Find the coefficient of x^7 in

$$(1 + x + x^2 + x^3 + \cdots)^{15}.$$

b) Find the coefficient of x^7 in

$$(1 + x + x^2 + x^3 + \cdots)^n \text{ for } n \in \mathbf{Z}^+.$$

6. Find the coefficient of x^{50} in $(x^7 + x^8 + x^9 + \cdots)^6$.

7. Find the coefficient of x^{20} in $(x^2 + x^3 + x^4 + x^5 + x^6)^5$.

8. For $n \in \mathbf{Z}^+$, find in $(1 + x + x^2)(1 + x)^n$ the coefficient of (a) x^7; (b) x^8; and (c) x^r for $0 \leq r \leq n + 2$, $r \in \mathbf{Z}$.

9. Find the coefficient of x^{15} in each of the following.

a) $x^3(1-2x)^{10}$

b) $(x^3 - 5x)/(1-x)^3$

c) $(1+x)^4/(1-x)^4$

10. In how many ways can two dozen identical robots be assigned to four assembly lines with (a) at least three robots assigned to each line? (b) at least three, but no more than nine, robots assigned to each line?

11. In how many ways can 3000 identical envelopes be divided, in packages of 25, among four student groups so that each group gets at least 150, but not more than 1000, of the envelopes?

12. Two cases of soft drinks, 24 bottles of one type and 24 of another, are distributed among five surveyors who are conducting taste tests. In how many ways can the 48 bottles be distributed so that each surveyor gets (a) at least two bottles of each type? (b) at least two bottles of one particular type and at least three of the other?

13. If a fair die is rolled 12 times, what is the probability that the sum of the rolls is 30?

14. Carol is collecting money from her cousins to have a party for her aunt. If eight of the cousins promise to give \$2, \$3, \$4, or \$5 each, and two others each give \$5 or \$10, what is the probability that Carol will collect exactly \$40?

15. In how many ways can Traci select n marbles from a large supply of blue, red, and yellow marbles (all of the same size) if the selection must include an even number of blue ones?

16. How can Mary split up 12 hamburgers and 16 hot dogs among her sons Richard, Peter, Christopher, and James in such a way that James gets at least one hamburger and three hot dogs, and each of his brothers gets at least two hamburgers but at most five hot dogs?

17. Verify that $(1 - x - x^2 - x^3 - x^4 - x^5 - x^6)^{-1}$ is the generating function for the number of ways the sum n, where $n \in \mathbf{N}$, can be obtained when a single die is rolled an arbitrary number of times.

18. Show that $(1-4x)^{-1/2}$ generates the sequence $\binom{2n}{n}$, $n \in \mathbf{N}$.

19. a) If a computer generates a random composition of 8, what is the probability the composition is a palindrome?

b) Answer the question in part (a) after replacing 8 by n, a fixed positive integer.

20. a) How many palindromes of 11 start with 1? with 2? with 3? with 4?

b) How many palindromes of 12 start with 1? with 2? with 3? with 4?

21. Let n be a (fixed) positive integer, with $n \geq 2$. If $1 \leq t \leq \lfloor n/2 \rfloor$, how many palindromes of n start with t?

22. Let $n \in \mathbf{Z}^+$, n odd. Can a palindrome of n have an even number of summands?

23. Let $n \in \mathbf{Z}^+$, n even. How many palindromes of n have an even number of summands? How many have an odd number of summands?

24. Determine the number of palindromes of n, where all summands are even, for (a) $n = 10$; (b) $n = 12$; and (c) n even.

25. Shay rolls a fair die until she gets a 6. If the random variable Y counts the number of times Shay rolls the die until she gets her first 6, determine (a) the probability distribution for Y; (b) $E(Y)$; and (c) σ_Y.

26. Referring back to the preceding exercise, what is the probability Shay rolls her first 6 on an even-numbered roll?

27. Leroy has a biased coin where $Pr(\mathrm{H}) = \frac{2}{3}$ and $Pr(\mathrm{T}) = \frac{1}{3}$. Assuming that each toss, after the first, is independent of any previous outcome, if Leroy tosses the coin until he gets a tail, what is the probability he tosses it an odd number of times?

28. If Y is a geometric random variable with $E(Y) = \frac{7}{3}$, determine (a) $Pr(Y = 3)$; (b) $Pr(Y \geq 3)$; (c) $Pr(Y \geq 5)$; (d) $Pr(Y \geq 5 | Y \geq 3)$; (e) $Pr(Y \geq 6 | Y \geq 4)$; and (f) σ_Y.

29. Consider part (a) of Example 9.17.

a) Determine the differences for the inequalities that result from the subset $\{3, 6, 8, 15\}$ of S, and verify that those differences add to the correct sum.

b) Find the subset of S that determines the differences 2, 2, 3, 7, and 0.

c) Find the subset of S that determines the differences a, b, c, d, and e, where $0 \leq a, e$, and $2 \leq b, c, d$.

30. In how many ways can we select seven nonconsecutive integers from $\{1, 2, 3, \ldots, 50\}$?

31. Use the following summation formulas to simplify the expression for c_k in Example 9.19:

$$\sum_{i=0}^{k} i = \sum_{i=1}^{k} i = \frac{k(k+1)}{2},$$

$$\sum_{i=0}^{k} i^2 = \sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}, \qquad \text{and}$$

$$\sum_{i=0}^{k} i^3 = \sum_{i=1}^{k} i^3 = \frac{k^2(k+1)^2}{4}.$$

32. **a)** Find the first four terms c_0, c_1, c_2, and c_3 of the convolutions for each of the following pairs of sequences.

i) $a_n = 1$, $b_n = 1$, for all $n \in \mathbf{N}$

ii) $a_n = 1$, $b_n = 2^n$, for all $n \in \mathbf{N}$

iii) $a_0 = a_1 = a_2 = a_3 = 1$; $a_n = 0$, $n \in \mathbf{N}$, $n \neq 0, 1, 2, 3$; $b_n = 1$, for all $n \in \mathbf{N}$

b) Find a general formula for c_n in each of the results of part (a).

33. Find a formula for the convolution of each of the following pairs of sequences.

a) $a_n = 1$, $0 \leq n \leq 4$, $a_n = 0$, for all $n \geq 5$; $b_n = n$, for all $n \in \mathbf{N}$

b) $a_n = (-1)^n$, $b_n = (-1)^n$, for all $n \in \mathbf{N}$

9.3 Partitions of Integers

In number theory, we are confronted with partitioning a positive integer n into positive summands and seeking the number of such partitions, without regard to order. This number is denoted by $p(n)$. For example,

$$\begin{aligned}
p(1) = 1: &\quad 1 \\
p(2) = 2: &\quad 2 = 1 + 1 \\
p(3) = 3: &\quad 3 = 2 + 1 = 1 + 1 + 1 \\
p(4) = 5: &\quad 4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1 \\
p(5) = 7: &\quad 5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 \\
&\quad\;\; = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1
\end{aligned}$$

We should like to obtain $p(n)$ for a given n without having to list all the partitions. We need a tool to keep track of the numbers of 1's, 2's, $\ldots$, n's that are used as summands for n.

If $n \in \mathbf{Z}^+$, the number of 1's we can use is 0 or 1 or 2 or. . . . The power series $1 + x + x^2 + x^3 + x^4 + \cdots$ keeps account of this for us. In like manner, $1 + x^2 + x^4 + x^6 + \cdots$ keeps track of the number of 2's in the partition of n, while $1 + x^3 + x^6 + x^9 + \cdots$ accounts for the number of 3's. Therefore, in order to determine $p(10)$, for instance, we want the coefficient of x^{10} in $f(x) = (1 + x + x^2 + x^3 + \cdots)(1 + x^2 + x^4 + x^6 + \cdots)(1 + x^3 + x^6 + x^9 + \cdots) \cdots (1 + x^{10} + x^{20} + \cdots)$ or in $g(x) = (1 + x + x^2 + x^3 + \cdots + x^{10})(1 + x^2 + x^4 + \cdots + x^{10})(1 + x^3 + x^6 + x^9) \cdots (1 + x^{10})$.

We prefer to work with $f(x)$, because it can be written in the more compact form

$$f(x) = \frac{1}{(1-x)}\frac{1}{(1-x^2)}\frac{1}{(1-x^3)}\cdots\frac{1}{(1-x^{10})} = \prod_{i=1}^{10}\frac{1}{(1-x^i)}.$$

If this product is extended beyond $i = 10$, we get $P(x) = \prod_{i=1}^{\infty}[1/(1 - x^i)]$, which generates the sequence $p(0), p(1), p(2), p(3), \ldots$, where we define $p(0) = 1$.

Unfortunately, it is impossible to actually calculate the infinite number of terms in the product $P(x)$. If we consider only $\prod_{i=1}^{r}[1/(1 - x^i)]$ for some fixed r, then the coefficient of x^n here is the number of partitions of n into summands that do not exceed r.

Despite the difficulty in calculating $p(n)$ from $P(x)$ for large values of n, the idea of the generating function will be useful in studying certain kinds of partitions.

EXAMPLE 9.21

Find the generating function for the number of ways an advertising agent can purchase n minutes ($n \in \mathbf{Z}^+$) of air time if time slots for commercials come in blocks of 30, 60, or 120 seconds.

Let 30 seconds represent one time unit. Then the answer is the number of integer solutions to the equation $a + 2b + 4c = 2n$ with $0 \le a, b, c$.

The associated generating function is

$$\begin{aligned} f(x) &= (1 + x + x^2 + \cdots)(1 + x^2 + x^4 + \cdots)(1 + x^4 + x^8 + \cdots) \\ &= \frac{1}{1-x}\,\frac{1}{1-x^2}\,\frac{1}{1-x^4}, \end{aligned}$$

and the coefficient of x^{2n} is the number of partitions of $2n$ into 1's, 2's, and 4's, the answer to the problem.

EXAMPLE 9.22

Find the generating function for $p_d(n)$, the number of partitions of a positive integer n into *distinct* summands.

Before we start, let us consider the 11 partitions of 6:

1) $1 + 1 + 1 + 1 + 1 + 1$ **2)** $1 + 1 + 1 + 1 + 2$
3) $1 + 1 + 1 + 3$ **4)** $1 + 1 + 4$
5) $1 + 1 + 2 + 2$ **6)** $1 + 5$
7) $1 + 2 + 3$ **8)** $2 + 2 + 2$
9) $2 + 4$ **10)** $3 + 3$
11) 6

Partitions (6), (7), (9), and (11) have distinct summands, so $p_d(6) = 4$.

In calculating $p_d(n)$, for each $k \in \mathbf{Z}^+$ there are two choices: Either k is not used as one of the summands of n, or it is. This can be accounted for by the polynomial $1 + x^k$, and consequently, the generating function for these partitions is

$$P_d(x) = (1+x)(1+x^2)(1+x^3)\cdots = \prod_{i=1}^{\infty}(1+x^i).$$

For each $n \in \mathbf{Z}^+$, $p_d(n)$ is the coefficient of x^n in $(1+x)(1+x^2)\cdots(1+x^n)$. [We define $p_d(0) = 1$.] When $n = 6$, the coefficient of x^6 in $(1+x)(1+x^2)\cdots(1+x^6)$ is 4.

EXAMPLE 9.23

Considering the partitions in Example 9.22, we see that there are four partitions of 6 into odd summands: namely, (1), (3), (6), and (10). We also have $p_d(6) = 4$. Is this a coincidence?

Let $p_o(n)$ denote the number of partitions of n into odd summands, when $n \geq 1$. We define $p_o(0) = 1$. The generating function for the sequence $p_o(0), p_o(1), p_o(2), \ldots$ is given by

$$P_o(x) = (1+x+x^2+x^3+\cdots)(1+x^3+x^6+\cdots)(1+x^5+x^{10}+\cdots)\cdot$$
$$(1+x^7+\cdots)\cdots = \frac{1}{1-x}\,\frac{1}{1-x^3}\,\frac{1}{1-x^5}\,\frac{1}{1-x^7}\cdots.$$

Now because

$$1+x = \frac{1-x^2}{1-x}, \qquad 1+x^2 = \frac{1-x^4}{1-x^2}, \qquad 1+x^3 = \frac{1-x^6}{1-x^3}, \qquad \ldots,$$

we have

$$P_d(x) = (1+x)(1+x^2)(1+x^3)(1+x^4)\cdots$$
$$= \frac{1-x^2}{1-x}\,\frac{1-x^4}{1-x^2}\,\frac{1-x^6}{1-x^3}\,\frac{1-x^8}{1-x^4}\cdots = \frac{1}{1-x}\,\frac{1}{1-x^3}\cdots = P_o(x).$$

From the equality of the generating functions, $p_d(n) = p_o(n)$, for all $n \geq 0$.

EXAMPLE 9.24

Once again we shall permit only odd summands, but in this example each such (odd) summand must occur an odd number of times — or not at all. Here, for example, there is one such partition of the integer 1 — namely, 1 — but there are *no* such partitions of the integer 2. For the integer 3 we have two of these partitions: 3 and $1+1+1$. When we examine the possibilities for the integer 4, we find the one partition $3+1$.

The generating function for the partitions described here is given by

$$f(x) = (1+x+x^3+x^5+\cdots)(1+x^3+x^9+x^{15}+\cdots)(1+x^5+x^{15}+x^{25}+\cdots)\cdots$$
$$= \prod_{k=0}^{\infty}\left(1+\sum_{i=0}^{\infty}x^{(2k+1)(2i+1)}\right).$$

The generating function is *not* given by

$$(x+x^3+x^5+\cdots)(x^3+x^9+x^{15}+\cdots)(x^5+x^{15}+x^{25}+\cdots)\cdots \qquad (*)$$

If it were, then the product could not contain any terms where x would appear to a finite power. The situation given by equation $(*)$ would occur if we were to believe that *every* odd positive integer must appear as a summand at least once. And in such a "partition" the number of summands and the sum itself would both be infinite. Consequently, whether or not it is stated, we must realize that each odd summand may not appear at all — and this condition is accounted for by the (first) summand, $1 = x^0$, that appears in each factor of

$f(x)$. In fact, for all but a finite number of odd summands, this is the case. Of course, when an odd summand does appear in a partition, it does so an odd number of times.

We close this section with an idea called the *Ferrers graph*. This graph uses rows of dots to represent a partition of an integer where the number of dots per row does not increase as we go from any row to the one below it.

In Fig. 9.2 we find the Ferrers graphs for two partitions of 14: (a) $4 + 3 + 3 + 2 + 1 + 1$ and (b) $6 + 4 + 3 + 1$. The graph in part (b) is said to be the *transposition* of the graph in part (a), and vice versa, because one graph can be obtained from the other by interchanging rows and columns.

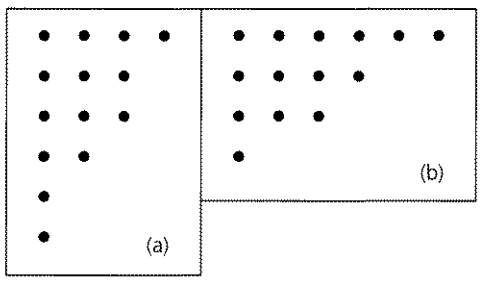


Figure 9.2

These graphs often suggest results about partitions. Here we see a partition of 14 into summands, where 4 is the largest summand, and a second partition of 14 into exactly four summands. There is a one-to-one correspondence between a Ferrers graph and its transposition, so this example demonstrates a particular instance of the general result: The number of partitions of an integer n into m summands is equal to the number of partitions of n into summands where m is the largest summand.

EXERCISES 9.3

1. Find all partitions of 7.

2. Determine the generating function for the sequence $a_0, a_1, a_2, \ldots$, where a_n is the number of partitions of the nonnegative integer n into (a) even summands; (b) distinct even summands; and (c) distinct odd summands.

3. In $f(x) = [1/(1-x)][1/(1-x^2)][1/(1-x^3)]$, the coefficient of x^6 is 7. Interpret this result in terms of partitions of 6.

4. Find the generating function for the number of integer solutions of

a) $2w + 3x + 5y + 7z = n, \quad 0 \le w, x, y, z$

b) $2w + 3x + 5y + 7z = n, \quad 0 \le w, \quad 4 \le x, y, \quad 5 \le z$

5. Find the generating function for the number of partitions of the nonnegative integer n into summands where (a) each summand must appear an even number of times; and (b) each summand must be even.

6. What is the generating function for the number of partitions of $n \in \mathbf{N}$ into summands that (a) cannot occur more than five times; and (b) cannot exceed 12 and cannot occur more than five times?

7. Show that the number of partitions of a positive integer n where no summand appears more than twice equals the number of partitions of n where no summand is divisible by 3.

8. Show that the number of partitions of $n \in \mathbf{Z}^+$ where no summand is divisible by 4 equals the number of partitions of n where no even summand is repeated (although odd summands may or may not be repeated).

9. Using a Ferrers graph, show that the number of partitions of an integer n into summands not exceeding m is equal to the number of partitions of n into at most m summands.

10. Using a Ferrers graph, show that the number of partitions of n is equal to the number of partitions of $2n$ into n summands.

9.4 The Exponential Generating Function

The type of generating function we have been dealing with is often referred to as the *ordinary* generating function for a given sequence. This function arose in selection problems, where order was not relevant. However, turning now to problems of arrangement, where order is crucial, we seek a comparable tool. To find such a tool, we return to the binomial theorem.

For each $n \in \mathbf{Z}^+$, $(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n$, so $(1+x)^n$ is the (ordinary) generating function for the sequence $\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n}, 0, 0, \ldots$. When dealing with this idea in Chapter 1, we also wrote $\binom{n}{r} = C(n, r)$ when we wanted to emphasize that $\binom{n}{r}$ represented the number of combinations of n objects taken r at a time, with $0 \le r \le n$. Consequently, $(1+x)^n$ generates the sequence $C(n, 0), C(n, 1), C(n, 2), \ldots, C(n, n), 0, 0, \ldots$.

Now for all $0 \le r \le n$,

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

where $P(n, r)$ denotes the number of permutations of n objects taken r at a time. So

$$\begin{aligned}(1+x)^n &= C(n, 0) + C(n, 1)x + C(n, 2)x^2 + C(n, 3)x^3 + \cdots + C(n, n)x^n \\ &= P(n, 0) + P(n, 1)x + P(n, 2)\frac{x^2}{2!} + P(n, 3)\frac{x^3}{3!} + \cdots + P(n, n)\frac{x^n}{n!}.\end{aligned}$$

Hence, if in $(1+x)^n$ we consider the coefficient of $x^r/r!$, with $0 \le r \le n$, we obtain $P(n, r)$. On the basis of this observation, we have the following definition.

Definition 9.2 For a sequence $a_0, a_1, a_2, a_3, \ldots$ of real numbers,

$$f(x) = a_0 + a_1 x + a_2\frac{x^2}{2!} + a_3\frac{x^3}{3!} + \cdots = \sum_{i=0}^{\infty} a_i \frac{x^i}{i!},$$

is called the *exponential generating function* for the given sequence.

EXAMPLE 9.25 Examining the Maclaurin series expansion for e^x, we find

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots = \sum_{i=0}^{\infty} \frac{x^i}{i!},$$

so e^x is the exponential generating function for the sequence $1, 1, 1, \ldots$. (The function e^x is the ordinary generating function for the sequence $1, 1, 1/2!, 1/3!, 1/4!, \ldots$.)

Our next example shows how this idea can help us count certain types of arrangements.

EXAMPLE 9.26 In how many ways can four of the letters in ENGINE be arranged?

In Table 9.4 we list the possible selections of size 4 from the letters E, N, G, I, N, E, along with the number of arrangements those four letters determine.

We now obtain the answer by means of an exponential generating function. For the letter E we use $[1 + x + (x^2/2!)]$ because there are 0, 1, or 2 E's to arrange. Note that the coefficient of $x^2/2!$ is 1, the number of distinct ways to arrange (only) two E's. In like

Table 9.4

E	E	N	N	$4!/(2!\,2!)$	E	G	N	N	$4!/2!$
E	E	G	N	$4!/2!$	E	I	N	N	$4!/2!$
E	E	I	N	$4!/2!$	G	I	N	N	$4!/2!$
E	E	G	I	$4!/2!$	E	I	G	N	$4!$

manner, we have $[1 + x + (x^2/2!)]$ for the arrangements of 0, 1, or 2 N's. The arrangements for each of the letters G and I are represented by $(1 + x)$.

Consequently, we find here that the exponential generating function is

$$f(x) = [1 + x + (x^2/2!)]^2(1 + x)^2,$$

and we claim that the required answer is the coefficient of $x^4/4!$ in $f(x)$.

In order to motivate our claim, let us consider two of the eight ways in which the term $x^4/4!$ arises in the expansion of

$$f(x) = [1 + x + (x^2/2!)][1 + x + (x^2/2!)](1 + x)(1 + x).$$

1) From the product $(x^2/2!)(x^2/2!)(1)(1)$, where $(x^2/2!)$ is taken from each of the first two factors (namely, $[1 + x + (x^2/2!)]$) and 1 is taken from each of the last two factors [namely, $(1 + x)$]. Then $(x^2/2!)(x^2/2!)(1)(1) = x^4/(2!\,2!) = (4!/(2!\,2!)) \cdot (x^4/4!)$, and the coefficient of $x^4/4!$ is $4!/(2!\,2!)$—the number of ways one can arrange the four letters E, E, N, N.
2) From the product $(x^2/2!)(1)(x)(x)$, where $(x^2/2!)$ is taken from the first factor (namely, $[1 + x + (x^2/2!)]$), 1 is taken from the second factor (again, $[1 + x + (x^2/2!)]$), and x is taken from each of the last two factors [namely, $(1 + x)$]. Here $(x^2/2!)(1)(x)(x) = x^4/2! = (4!/2!)(x^4/4!)$, so the coefficient of $x^4/4!$ is $4!/2!$—the number of ways the four letters E, E, G, I can be arranged.

In the complete expansion of $f(x)$, the term involving x^4 [and, consequently, $x^4/4!$] is

$$\left(\frac{x^4}{2!\,2!} + \frac{x^4}{2!} + \frac{x^4}{2!} + \frac{x^4}{2!} + \frac{x^4}{2!} + \frac{x^4}{2!} + \frac{x^4}{2!} + x^4\right)$$
$$= \left[\left(\frac{4!}{2!\,2!}\right) + \left(\frac{4!}{2!}\right) + \left(\frac{4!}{2!}\right) + \left(\frac{4!}{2!}\right) + \left(\frac{4!}{2!}\right) + \left(\frac{4!}{2!}\right) + \left(\frac{4!}{2!}\right) + 4!\right]\left(\frac{x^4}{4!}\right),$$

where the coefficient of $x^4/4!$ is the answer (102 arrangements) produced by the eight results in the table.

EXAMPLE 9.27

Consider the Maclaurin series expansions of e^x and e^{-x}.

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots \qquad e^{-x} = 1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} + \frac{x^4}{4!} - \cdots$$

Adding these series together, we find that

$$e^x + e^{-x} = 2\left(1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots\right),$$

or

$$\frac{e^x + e^{-x}}{2} = 1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots.$$

Subtracting e^{-x} from e^x yields

$$\frac{e^x - e^{-x}}{2} = x + \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots.$$

These results now help us in the following.

EXAMPLE 9.28

A ship carries 48 flags, 12 each of the colors red, white, blue, and black. Twelve of these flags are placed on a vertical pole in order to communicate a signal to other ships.

a) How many of these signals use an even number of blue flags and an odd number of black flags?

The exponential generating function

$$f(x) = \left(1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots\right)^2 \left(1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots\right)\left(x + \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots\right)$$

considers all such signals made up of n flags, where $n \geq 1$. The last two factors in $f(x)$ restrict the signals to an even number of blue flags and an odd number of black flags, respectively.

Since

$$f(x) = (e^x)^2\left(\frac{e^x + e^{-x}}{2}\right)\left(\frac{e^x - e^{-x}}{2}\right) = \left(\frac{1}{4}\right)(e^{2x})(e^{2x} - e^{-2x}) = \frac{1}{4}(e^{4x} - 1)$$

$$= \frac{1}{4}\left(\sum_{i=0}^{\infty} \frac{(4x)^i}{i!} - 1\right) = \left(\frac{1}{4}\right)\sum_{i=1}^{\infty} \frac{(4x)^i}{i!},$$

the coefficient of $x^{12}/12!$ in $f(x)$ yields $(1/4)(4^{12}) = 4^{11}$ signals made up of 12 flags with an even number of blue flags and an odd number of black flags.

b) How many of the signals have at least three white flags or no white flags at all? In this situation we use the exponential generating function

$$g(x) = \left(1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots\right)\left(1 + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots\right)\left(1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots\right)^2$$

$$= e^x\left(e^x - x - \frac{x^2}{2!}\right)(e^x)^2 = e^{3x}\left(e^x - x - \frac{x^2}{2!}\right) = e^{4x} - xe^{3x} - \left(\frac{1}{2}\right)x^2e^{3x}$$

$$= \sum_{i=0}^{\infty} \frac{(4x)^i}{i!} - x\sum_{i=0}^{\infty} \frac{(3x)^i}{i!} - \left(\frac{x^2}{2}\right)\left(\sum_{i=0}^{\infty} \frac{(3x)^i}{i!}\right).$$

Here the factor $(1 + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots) = e^x - x - \frac{x^2}{2!}$ in $g(x)$ restricts the signals to those that contain three or more of the 12 white flags, or none at all. The answer for the number of signals sought here is the coefficient of $x^{12}/12!$ in $g(x)$. As we consider each summand (involving an infinite summation), we find:

i) $\displaystyle\sum_{i=0}^{\infty} \frac{(4x)^i}{i!}$ — Here we have the term $\frac{(4x)^{12}}{12!} = 4^{12}\left(\frac{x^{12}}{12!}\right)$, so the coefficient of $x^{12}/12!$ is 4^{12};

ii) $x\left(\sum_{i=0}^{\infty}\frac{(3x)^i}{i!}\right)$ — Now we see that in order to get $x^{12}/12!$ we need to consider the term $x[(3x)^{11}/11!] = 3^{11}(x^{12}/11!) = (12)(3^{11})(x^{12}/12!)$, and here the coefficient of $x^{12}/12!$ is $(12)(3^{11})$; and

iii) $(x^2/2)\left(\sum_{i=0}^{\infty}\frac{(3x)^i}{i!}\right)$ — For this last summand we observe that $(x^2/2)[(3x)^{10}/10!] = (1/2)(3^{10})(x^{12}/10!) = (1/2)(12)(11)(3^{10})(x^{12}/12!)$, where this time the coefficient of $x^{12}/12!$ is $(1/2)(12)(11)(3^{10})$.

Consequently, the number of 12 flag signals with at least three white flags, or none at all, is

$$4^{12} - 12(3^{11}) - (1/2)(12)(11)(3^{10}) = 10{,}754{,}218.$$

Our final example is reminiscent of past results.

EXAMPLE 9.29

A company hires 11 new employees, each of whom is to be assigned to one of four subdivisions. Each subdivision will get at least one new employee. In how many ways can these assignments be made?

Calling the subdivisions A, B, C, and D, we can equivalently count the number of 11-letter sequences in which there is at least one occurrence of each of the letters A, B, C, and D. The exponential generating function for these arrangements is

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

The answer then is the coefficient of $x^{11}/11!$ in $f(x)$:

$$4^{11} - 4(3^{11}) + 6(2^{11}) - 4(1^{11}) = \sum_{i=0}^{4}(-1)^i\binom{4}{i}(4-i)^{11}.$$

This form of the answer should bring to mind some of the enumeration problems in Chapter 5. Once the vocabulary is set aside, we are counting the number of onto functions $g\colon X \to Y$ where $|X| = 11$, $|Y| = 4$.

EXERCISES 9.4

1. Find the exponential generating function for each of the following sequences.

a) $1, -1, 1, -1, 1, -1, \ldots$

b) $1, 2, 2^2, 2^3, 2^4, \ldots$

c) $1, -a, a^2, -a^3, a^4, \ldots, \quad a \in \mathbf{R}$

d) $1, a^2, a^4, a^6, \ldots, \quad a \in \mathbf{R}$

e) $a, a^3, a^5, a^7, \ldots, \quad a \in \mathbf{R}$

f) $0, 1, 2(2), 3(2^2), 4(2^3), \ldots$

2. Determine the sequence generated by each of the following exponential generating functions.

a) $f(x) = 3e^{3x}$

b) $f(x) = 6e^{5x} - 3e^{2x}$

c) $f(x) = e^x + x^2$

d) $f(x) = e^{2x} - 3x^3 + 5x^2 + 7x$

e) $f(x) = 1/(1-x)$

f) $f(x) = 3/(1-2x) + e^x$

3. In each of the following, the function $f(x)$ is the exponential generating function for the sequence $a_0, a_1, a_2, \ldots$, whereas the function $g(x)$ is the exponential generating function for the sequence $b_0, b_1, b_2, \ldots$. Express $g(x)$ in terms of $f(x)$ if

a) $b_3 = 3$
$b_n = a_n,\ n \in \mathbf{N},\ n \neq 3$

b) $a_n = 5^n$, $n \in \mathbf{N}$
$b_3 = -1$
$b_n = a_n$, $n \in \mathbf{N}$, $n \neq 3$

c) $b_1 = 2$
$b_2 = 4$
$b_n = 2a_n$, $n \in \mathbf{N}$, $n \neq 1, 2$

d) $b_1 = 2$
$b_2 = 4$
$b_3 = 8$
$b_n = 2a_n + 3$, $n \in \mathbf{N}$, $n \neq 1, 2, 3$

4. a) For the ship in Example 9.28, how many signals use at least one flag of each color? (Solve this with an exponential generating function.)

b) Restate part (a) in an alternative way that uses the concept of an onto function.

c) How many signals are there in Example 9.28, where the total number of blue and black flags is even?

5. Find the exponential generating function for the sequence $0!, 1!, 2!, 3!, \ldots$.

6. a) Find the exponential generating function for the number of ways to arrange n letters, $n \geq 0$, selected from each of the following words.

i) HAWAII
ii) MISSISSIPPI
iii) ISOMORPHISM

b) For section (ii) of part (a), what is the exponential generating function if the arrangement must contain at least two I's?

7. Say the company in Example 9.29 hires 25 new employees. Give the exponential generating function for the number of ways to assign these people to the four subdivisions so that each subdivision receives at least 3, but no more than 10, new people.

8. Given the sequences $a_0, a_1, a_2, \ldots$ and $b_0, b_1, b_2, \ldots$, with exponential generating functions $f(x)$, $g(x)$, respectively, show that if $h(x) = f(x)g(x)$, then $h(x)$ is the exponential generating function of the sequence $c_0, c_1, c_2, \ldots$, where $c_n = \sum_{i=0}^{n} \binom{n}{i} a_i b_{n-i}$, for each $n \geq 0$.

9. If a 20-digit ternary (0, 1, 2) sequence is randomly generated, what is the probability that: (a) It has an even number of 1's? (b) It has an even number of 1's and an even number of 2's? (c) It has an odd number of 0's? (d) The total number of 0's and 1's is odd? (e) The total number of 0's and 1's is even?

10. How many 20-digit quaternary (0, 1, 2, 3) sequences are there where: (a) There is at least one 2 and an odd number of 0's? (b) No symbol occurs exactly twice? (c) No symbol occurs exactly three times? (d) There are exactly two 3's or none at all?

9.5 The Summation Operator

This final section introduces a technique that helps us go from the (ordinary) generating function for the sequence $a_0, a_1, a_2, \ldots$ to the generating function for the sequence $a_0, a_0 + a_1, a_0 + a_1 + a_2, \ldots$.

For $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots$, consider the function $f(x)/(1-x)$.

$$\frac{f(x)}{1-x} = f(x) \cdot \frac{1}{1-x} = [a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots][1 + x + x^2 + x^3 + \cdots]$$
$$= a_0 + (a_0 + a_1)x + (a_0 + a_1 + a_2)x^2 + (a_0 + a_1 + a_2 + a_3)x^3 + \cdots,$$

so $f(x)/(1-x)$ generates the sequence of sums $a_0, a_0 + a_1, a_0 + a_1 + a_2, a_0 + a_1 + a_2 + a_3, \ldots$. This is why we refer to $1/(1-x)$ as the *summation operator*. Furthermore we see that the sequence $a_0, a_0 + a_1, a_0 + a_1 + a_2, a_0 + a_1 + a_2 + a_3, \ldots$ is the convolution of the sequence $a_0, a_1, a_2, \ldots$ and the sequence $b_0, b_1, b_2, \ldots$, where $b_n = 1$ for all $n \in \mathbf{N}$.

We find this technique handy in the following examples.

EXAMPLE 9.30

a) We know from part (b) of Example 9.5 that $1/(1-x)$ is the generating function for the sequence $1, 1, 1, \ldots$. Consequently, upon applying the summation operator, $1/(1-x)$, we see that $(1/(1-x))(1/(1-x))$ is the generating function for the sequence $1, 1+1, 1+1+1, \ldots$—that is, $1/(1-x)^2$ is the generating function for the sequence $1, 2, 3, \ldots$, as we found in part (c) of Example 9.5.

b) Now let us start with the polynomial $x + x^2$, the generating function for the sequence $0, 1, 1, 0, 0, 0, \ldots$. Applying the summation operator, we have $(x + x^2)(1/(1 - x)) = (x + x^2)/(1 - x)$, the generating function for the sequence $0, 0 + 1, 0 + 1 + 1, 0 + 1 + 1 + 0, \ldots,$—that is, the sequence $0, 1, 2, 2, \ldots$. A second application of the summation operator tells us that $(x + x^2)/(1 - x)^2$ is the generating function for the sequence $0, 0 + 1, 0 + 1 + 2, 0 + 1 + 2 + 2, \ldots,$—that is, the sequence $0, 1, 3, 5, \ldots$. A final application of the summation operator tells us that $(x + x^2)/(1 - x)^3$ is the generating function for the sequence $0, 0 + 1, 0 + 1 + 3, 0 + 1 + 3 + 5, \ldots,$—that is, the sequence $0, 1, 4, 9, \ldots$. This *suggests* that, for $n \geq 1$, $\sum_{k=1}^{n}(2k - 1) = n^2$. To verify this suggestion, we look at the coefficient of x^n in $(x + x^2)/(1 - x)^3 = x(1 - x)^{-3} + x^2(1 - x)^{-3}$. The coefficient of x^{n-1} in $(1 - x)^{-3}$ [which is the coefficient of x^n in $x(1 - x)^{-3}$] is

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

The coefficient of x^{n-2} in $(1 - x)^{-3}$ [which is the coefficient of x^n in $x^2(1 - x)^{-3}$] is $\binom{-3}{n-2}(-1)^{n-2} = (-1)^{n-2}\binom{3 + (n-2) - 1}{n-2}(-1)^{n-2} = \binom{n}{n-2} = \frac{1}{2}(n)(n - 1)$. Consequently, for $n \geq 1$, $\sum_{k=1}^{n}(2k - 1) =$ the coefficient of x^n in $(x + x^2)/(1 - x)^3 = \frac{1}{2}(n + 1)(n) + \frac{1}{2}(n)(n - 1) = \frac{1}{2}(n)[(n + 1) + (n - 1)] = n^2$, as we learned earlier in Example 4.7, using the Principle of Mathematical Induction.

Our last example provides us with a method for deriving some of the summation formulas we encountered in earlier chapters.

EXAMPLE 9.31

Find a formula to express $0^2 + 1^2 + 2^2 + \cdots + n^2$ as a function of n.

As in Section 9.2, we start with $g(x) = 1/(1 - x) = 1 + x + x^2 + \cdots$. Then

$$(-1)(1 - x)^{-2}(-1) = \frac{1}{(1 - x)^2} = \frac{dg(x)}{dx} = 1 + 2x + 3x^2 + 4x^3 + \cdots,$$

so $x/(1 - x)^2$ is the generating function for $0, 1, 2, 3, 4, \ldots$. Repeating this technique, we find that

$$x\frac{d}{dx}\left[x\left(\frac{dg(x)}{dx}\right)\right] = \frac{x(1 + x)}{(1 - x)^3} = x + 2^2x^2 + 3^2x^3 + \cdots,$$

so $x(1 + x)/(1 - x)^3$ generates $0^2, 1^2, 2^2, 3^2, \ldots$. As a consequence of our earlier observations about the summation operator, we find that

$$\frac{x(1 + x)}{(1 - x)^3}\frac{1}{(1 - x)} = \frac{x(1 + x)}{(1 - x)^4}$$

is the generating function for $0^2, 0^2 + 1^2, 0^2 + 1^2 + 2^2, 0^2 + 1^2 + 2^2 + 3^2, \ldots$. Hence the coefficient of x^n in $[x(1 + x)]/(1 - x)^4$ is $\sum_{i=0}^{n} i^2$. But the coefficient of x^n in $[x(1 + x)]/(1 - x)^4$ can also be calculated as follows:

$$\frac{x(1 + x)}{(1 - x)^4} = (x + x^2)(1 - x)^{-4} = (x + x^2)\left[\binom{-4}{0} + \binom{-4}{1}(-x) + \binom{-4}{2}(-x)^2 + \cdots\right],$$

so the coefficient of x^n is

$$\begin{aligned}
&\binom{-4}{n-1}(-1)^{n-1} + \binom{-4}{n-2}(-1)^{n-2} \\
&\quad = (-1)^{n-1}\binom{4+(n-1)-1}{n-1}(-1)^{n-1} + (-1)^{n-2}\binom{4+(n-2)-1}{n-2}(-1)^{n-2} \\
&\quad = \binom{n+2}{n-1} + \binom{n+1}{n-2} = \frac{(n+2)!}{3!(n-1)!} + \frac{(n+1)!}{3!(n-2)!} \\
&\quad = \frac{1}{6}[(n+2)(n+1)(n) + (n+1)(n)(n-1)] \\
&\quad = \frac{1}{6}(n)(n+1)[(n+2)+(n-1)] = \frac{n(n+1)(2n+1)}{6}.
\end{aligned}$$

EXERCISES 9.5

1. Find the generating function for the sequences (a) 1, 2, 3, 3, 3, . . . ; (b) 1, 2, 3, 4, 4, 4, . . . ; (c) 1, 4, 7, 10, 13, ...

2. a) Find the generating function for the sequences (i) 0, 1, 0, 0, 0, . . . ; (ii) 0, 1, 1, 1, 1, . . . ; (iii) 0, 1, 2, 3, 4, . . . ; (iv) 0, 1, 3, 6, 10, ...

b) Use result (iv) from part (a) to find a formula for $\sum_{k=1}^{n} k$.

3. Continue the development of the ideas set forth in Example 9.31 and derive the formula $\sum_{i=0}^{n} i^3 = [n(n+1)/2]^2$.

4. If $f(x) = \sum_{n=0}^{\infty} a_n x^n$, what is the generating function for the sequence $a_0, a_0 + a_1, a_1 + a_2, a_2 + a_3, \ldots$? What is the generating function for the sequence $a_0, a_0 + a_1, a_0 + a_1 + a_2, a_1 + a_2 + a_3, a_2 + a_3 + a_4, \ldots$? What is the generating function for the sequence $\frac{a_0}{4}, \frac{a_0}{2} + \frac{a_1}{4}, \frac{a_0}{4} + \frac{a_1}{2} + \frac{a_2}{4}, \frac{a_1}{4} + \frac{a_2}{2} + \frac{a_3}{4}, \ldots$?

5. Let $f(x)$ be the generating function for the sequence $a_0, a_1, a_2, \ldots$. For what sequence is $(1-x)f(x)$ the generating function?

6. Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$ with $f(1) = \sum_{i=0}^{\infty} a_i$, a finite number. Verify that the quotient $[f(x) - f(1)]/(x-1)$ is the generating function for the sequence $s_0, s_1, s_2, \ldots$, where $s_n = \sum_{i=n+1}^{\infty} a_i$, $n \in \mathbf{N}$.

7. Find the generating function for the sequence $a_0, a_1, a_2, \ldots$, where $a_n = \sum_{i=0}^{n}(1/i!)$, $n \in \mathbf{N}$.

8. a) Find the generating function for the sequence 0, 1, 3, 6, 10, 15, . . . (where 1, 3, 6, 10, 15, . . . are the triangular numbers of Example 4.5).

b) For $n \in \mathbf{Z}^+$, determine a formula for the sum of the first n triangular numbers.

9.6 Summary and Historical Review

In the early thirteenth century the Italian mathematician Leonardo of Pisa (c. 1175–1250), in his *Liber Abaci*, introduced the European world to the Hindu-Arabic notation for numerals and algorithms for arithmetic. In this text he also originated the study of the sequence 0, 1, 1, 2, 3, 5, 8, 13, 21, . . . , which can be given recursively by $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$, $n \geq 0$. Since Leonardo was the son of Bonaccio, the sequence has come to be called the Fibonacci numbers. (Filius Bonaccii is the Latin form for "son of Bonaccio.")

If we consider the formula

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right], \qquad n \geq 0,$$

we find $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, ... Yes, this formula determines each Fibonacci number as a function of n. (Here we have the solution for the recursive Fibonacci relation. We shall learn more about this in the next chapter.) This formula was not derived,

however, until 1718, when Abraham DeMoivre (1667–1754) obtained the result from the generating function

$$f(x) = \frac{x}{1 - x - x^2} = \frac{1}{\sqrt{5}}\left[\frac{1}{1 - \left(\frac{1+\sqrt{5}}{2}\right)x} - \frac{1}{1 - \left(\frac{1-\sqrt{5}}{2}\right)x}\right].$$

Extending the existing techniques of the generating function, Leonhard Euler (1707–1783) advanced the study of the partitions of integers in his 1748 two-volume opus, *Introductio in Analysin Infinitorum*. With

$$P(x) = \frac{1}{1-x}\frac{1}{1-x^2}\frac{1}{1-x^3}\cdots = \prod_{i=1}^{\infty}\frac{1}{1-x^i},$$

we have the generating function for $p(0), p(1), p(2), \ldots$, where $p(n)$ is the number of partitions of n into positive summands and $p(0)$ is defined to be 1.

Leonhard Euler (1707–1783)

In the latter part of the eighteenth century, further developments on generating functions arose in conjunction with ideas in probability theory, especially with what is now called the "moment generating function." These related notions were presented in their first complete treatment by the great scholar Pierre-Simon de Laplace (1749–1827) in his 1812 publication *Théorie Analytique des Probabilités*.

Finally, we mention Norman Macleod Ferrers (1829–1903), after whom the diagram we called the Ferrers graph is named.

For us the study of the ordinary and exponential generating functions provided a powerful technique that unified ideas found in Chapters 1, 5, and 8. Extending our prior experience with polynomials to power series, and extending the binomial theorem to $(1 + x)^n$ for the cases where n need not be positive or even an integer, we found the necessary tools to compute the coefficients in these generating functions. This was more than worth the effort because the algebraic calculations we performed took into account all of the selection

processes we were trying to consider. We also found that we had seen some generating functions in a prior chapter and saw how they arose in the study of partitions.

The concept of a partition of a positive integer now enables us to complete the summaries of our earlier discussions on distributions, as given in Tables 1.11 and 5.13. Here we can now deal with the distributions of m objects into n ($\leq m$) containers for the cases where neither the objects nor the containers are distinct. These are covered by the entries in the second and fourth rows of Table 9.5. The notation $p(m, n)$, which appears in the last column for these entries, is used to denote the number of partitions of the positive integer m into exactly n (positive) summands. (This idea will be examined further in Supplementary Exercise 3 of the next chapter.) The types of distributions in the first and third rows of this table were also listed in Table 5.13. We include them here a second time for the sake of comparison and completeness.

Table 9.5

Objects Are Distinct	Containers Are Distinct	Some Container(s) May Be Empty	Number of Distributions
No	Yes	Yes	$\binom{n+m-1}{m}$
No	No	Yes	(1) $p(m)$, for $n = m$ (2) $p(m, 1) + p(m, 2) + \cdots + p(m, n)$, for $n < m$
No	Yes	No	$\binom{n+(m-n)-1}{(m-n)} = \binom{m-1}{m-n} = \binom{m-1}{n-1}$
No	No	No	$p(m, n)$

For comparable coverage of the material presented in this chapter, the interested reader should consult Chapter 2 of C. L. Liu [3] and Chapter 6 of A. Tucker [8]. The text by J. Riordan [6] has extensive coverage of ordinary and exponential generating functions. An interesting survey article on generating functions, written by Richard P. Stanley, can be found in the text edited by G-C. Rota [7]. The text by H. S. Wilf [9] deals with generating functions and some of the ways they are applied in discrete mathematics. This work also demonstrates how these functions provide a bridge between discrete mathematics and continuous analysis (in particular, the theory of functions of a complex variable).

The reader interested in learning more about the theory of partitions should consult Chapter 10 of I. Niven, H. Zuckerman, and H. Montgomery [5].

Finally, a great deal about the moment generating function and its use in probability theory can be found in Chapter 3 of H. J. Larson [2] and in Chapter XI of the comprehensive work by W. Feller [1].

REFERENCES

1. Feller, William. *An Introduction to Probability Theory and Its Applications*, Vol. I, 3rd ed. New York: Wiley, 1968.
2. Larson, Harold J. *Introduction to Probability Theory and Statistical Inference*, 2nd ed. New York: Wiley, 1969.
3. Liu, C. L. *Introduction to Combinatorial Mathematics*. New York: McGraw-Hill, 1968.
4. Neal, David. "The Series $\sum_{n=1}^{\infty} n^m x^n$ and a Pascal-like Triangle." *The College Mathematics Journal* 25, No. 2 (March 1994): pp. 99–101.

5. Niven, Ivan, Zuckerman, Herbert, and Montgomery, Hugh. *An Introduction to the Theory of Numbers*, 5th ed. New York: Wiley, 1991.
6. Riordan, John. *An Introduction to Combinatorial Analysis*. Princeton, N.J.: Princeton University Press, 1980. (Originally published in 1958 by John Wiley & Sons.)
7. Rota, Gian-Carlo, ed. *Studies in Combinatorics*, Studies in Mathematics, Vol. 17. Washington, D.C.: The Mathematical Association of America, 1978.
8. Tucker, Alan. *Applied Combinatorics*, 4th ed. New York: Wiley, 2002.
9. Wilf, Herbert S. *Generatingfunctionology*, 2nd ed. San Diego, Calif.: Academic Press, 1994.

SUPPLEMENTARY EXERCISES

1. Find the generating function for each of the following sequences.

a) $7, 8, 9, 10, \ldots$

b) $1, a, a^2, a^3, a^4, \ldots, \quad a \in \mathbf{R}$

c) $1, (1+a), (1+a)^2, (1+a)^3, \ldots, \quad a \in \mathbf{R}$

d) $2, 1+a, 1+a^2, 1+a^3, \ldots, \quad a \in \mathbf{R}$

2. Find the coefficient of x^{83} in

$$f(x) = (x^5 + x^8 + x^{11} + x^{14} + x^{17})^{10}.$$

3. Sergeant Bueti must distribute 40 bullets (20 for rifles and 20 for handguns) among four police officers so that each officer gets at least two, but no more than seven, bullets of each type. In how many ways can he do this?

4. Find a generating function for the number of ways to partition a positive integer n into positive-integer summands, where each summand appears an odd number of times or not at all.

5. For $n \in \mathbf{Z}^+$, show that the number of partitions of n in which no even summand is repeated (an odd summand may or may not be repeated) is the same as the number of partitions of n where no summand occurs more than three times.

6. How many 10-digit telephone numbers use only the digits 1, 3, 5 and 7, with each digit appearing at least twice or not at all?

7. **a)** For what sequence of numbers is $g(x) = (1-2x)^{-5/2}$ the exponential generating function?

b) Find a and b so that $(1-ax)^b$ is the exponential generating function for the sequence $1, 7, 7 \cdot 11, 7 \cdot 11 \cdot 15, \ldots$.

8. For integers $n, k \geq 0$ let

- P_1 be the number of partitions of n.
- P_2 be the number of partitions of $2n+k$, where $n+k$ is the greatest summand.
- P_3 be the number of partitions of $2n+k$ into precisely $n+k$ summands.

Using the concept of the Ferrers graph, prove that $P_1 = P_2$ and $P_2 = P_3$, thus concluding that the number of partitions of $2n+k$ into precisely $n+k$ summands is the same for all k.

9. Simplify the following sum where $n \in \mathbf{Z}^+$: $\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n}$. (*Hint*: You may wish to start with the binomial theorem.)

10. Determine the generating function for the number of partitions of $n \in \mathbf{N}$ where 1 occurs at most once, 2 occurs at most twice, 3 at most thrice, and, in general, k occurs at most k times, for every $k \in \mathbf{Z}^+$.

11. In a rural area 12 mailboxes are located at a general store.

a) If a newscarrier has 20 identical fliers, in how many ways can she distribute the fliers so that each mailbox gets at least one flier?

b) If the mailboxes are in two rows of six each, what is the probability that a distribution from part (a) will have 10 fliers distributed to the top six boxes and 10 to the bottom six?

12. Let S be a set containing n distinct objects. Verify that $e^x/(1-x)^k$ is the exponential generating function for the number of ways to choose m of the objects in S, for $0 \leq m \leq n$, and distribute these objects among k distinct containers, with the order of the objects in any container relevant for the distribution.

13. **a)** For $a, d \in \mathbf{R}$, find the generating function for the sequence $a, a+d, a+2d, a+3d, \ldots$.

b) For $n \in \mathbf{Z}^+$, use the result from part (a) to find a formula for the sum of the first n terms of the arithmetic progression $a, a+d, a+2d, a+3d, \ldots$.

14. **a)** For the alphabet $\Sigma = \{0, 1\}$, let a_n count the number of strings of length n in Σ^*—that is, for $n \in \mathbf{N}$, $a_n = |\Sigma^n|$. Determine the generating function for the sequence $a_0, a_1, a_2, \ldots$.

b) Answer the question posed in part (a) when $|\Sigma| = k$, a fixed positive integer.

15. Let $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots$, the generating function for the sequence $a_0, a_1, a_2, a_3, \ldots$. Now let $n \in \mathbf{Z}^+$, n fixed.

a) Find the generating function for the sequence $0, 0, 0, \ldots 0, a_0, a_1, a_2, a_3, \ldots$, where there are n leading zeros.

b) Find the generating function for the sequence $a_n, a_{n+1}, a_{n+2}, \ldots$.

16. Suppose that X is a discrete random variable with probability distribution given by

$$Pr(X = x) = \begin{cases} k\left(\frac{1}{4}\right)^x, & x = 0, 1, 2, 3, \ldots \\ 0, & \text{otherwise,} \end{cases}$$

where k is a constant. Determine (a) the value of k; (b) $Pr(X = 3)$, $Pr(X \leq 3)$, $Pr(X > 3)$, $Pr(X \geq 2)$; and (c) $Pr(X \geq 4 | X \geq 2)$, $Pr(X \geq 104 | X \geq 102)$.

17. Suppose that Y is a geometric random variable where the probability of success for each Bernoulli trial is p. If $m, n \in \mathbf{Z}^+$ with $m > n$, determine $Pr(Y \geq m | Y \geq n)$.

18. A test car is driven a fixed distance of n miles along a straight highway. (Here $n \in \mathbf{Z}^+$.) The car travels at one mile per hour for the first mile, two miles per hour for the second mile, four miles per hour for the third mile, . . . , and 2^{n-1} miles per hour for the nth mile.

a) What is the car's average velocity for the first four miles?

b) For a given value of n, what is the car's average velocity for the first n miles?

c) Find the smallest value of n for which the car's average velocity for the first n miles exceeds 10 miles per hour.

10

Recurrence Relations

In earlier sections of the text we saw some recursive definitions and constructions. In Definitions 5.19, 6.7, 6.12, and 7.9, we obtained concepts at level $n + 1$ (or of size $n + 1$) from comparable concepts at level n (or of size n), after establishing the concept at a first value of n, such as 0 or 1. When we dealt with the Fibonacci and Lucas numbers in Section 4.2, the results at level $n + 1$ turned out to depend on those at levels n and $n - 1$; and for each of these sequences of integers the basis consisted of the first two integers (of the sequence). Now we shall find ourselves in a somewhat similar situation. We shall investigate functions $a(n)$, preferably written as a_n (for $n \geq 0$), where a_n depends on some of the prior terms $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$. This study of what are called either *recurrence relations* or *difference equations* is the discrete counterpart to ideas applied in ordinary differential equations.

Our development will not employ any ideas from differential equations but will start with the notion of a geometric progression. As further ideas are developed, we shall see some of the many applications that make this topic so important.

10.1 The First-Order Linear Recurrence Relation

A *geometric progression* is an infinite sequence of numbers, such as 5, 15, 45, 135, . . . , where the division of each term, other than the first, by its immediate predecessor is a constant, called the *common ratio*. For our sequence this common ratio is 3: $15 = 3(5)$, $45 = 3(15)$, and so on. If $a_0, a_1, a_2, \ldots$ is a geometric progression, then $a_1/a_0 = a_2/a_1 = \cdots = a_{n+1}/a_n = \cdots = r$, the common ratio. In our particular geometric progression we have $a_{n+1} = 3a_n$, $n \geq 0$.

The *recurrence relation* $a_{n+1} = 3a_n$, $n \geq 0$, does not define a unique geometric progression. The sequence 7, 21, 63, 189, . . . also satisfies the relation. To pinpoint a particular sequence described by $a_{n+1} = 3a_n$, we need to know one of the terms of that sequence. Hence

$$a_{n+1} = 3a_n, \qquad n \geq 0, \qquad a_0 = 5,$$

uniquely defines the sequence 5, 15, 45, . . . , whereas

$$a_{n+1} = 3a_n, \qquad n \geq 0, \qquad a_1 = 21,$$

identifies 7, 21, 63, . . . as the geometric progression under study.

The equation $a_{n+1} = 3a_n$, $n \geq 0$ is a recurrence relation because the value of a_{n+1} (the present consideration) is dependent on a_n (a prior consideration). Since a_{n+1} depends only on its immediate predecessor, the relation is said to be of *first order*. In particular, this is a *first-order linear homogeneous* recurrence relation *with constant coefficients*. (We'll say more about these ideas later.) The general form of such an equation can be written $a_{n+1} = da_n$, $n \geq 0$, where d is a constant.

Values such as a_0 or a_1, given in addition to the recurrence relations, are called *boundary conditions*. The expression $a_0 = A$, where A is a constant, is also referred to as an *initial condition*. Our examples show the importance of the boundary condition in determining the unique solution.

Let us return now to the recurrence relation

$$a_{n+1} = 3a_n, \qquad n \geq 0, \qquad a_0 = 5.$$

The first four terms of this sequence are

$$\begin{aligned} a_0 &= 5, \\ a_1 &= 3a_0 = 3(5), \\ a_2 &= 3a_1 = 3(3a_0) = 3^2(5), \quad \text{and} \\ a_3 &= 3a_2 = 3(3^2(5)) = 3^3(5). \end{aligned}$$

These results suggest that for each $n \geq 0$, $a_n = 5(3^n)$. This is the *unique solution* of the given recurrence relation. In this solution, the value of a_n is a function of n and there is no longer any dependence on prior terms of the sequence, once we define a_0. To compute a_{10}, for example, we simply calculate $5(3^{10}) = 295{,}245$; there is no need to start at a_0 and build up to a_9 in order to obtain a_{10}.

From this example we are directed to the following. (This result can be established by the Principle of Mathematical Induction.)

The unique solution of the recurrence relation

$$a_{n+1} = da_n, \qquad \text{where } n \geq 0, \quad d \text{ is a constant, and } \quad a_0 = A,$$

is given by

$$a_n = Ad^n, \qquad n \geq 0.$$

Thus the solution $a_n = Ad^n$, $n \geq 0$, defines a discrete function whose domain is the set $\mathbf{N}$ of all nonnegative integers.

EXAMPLE 10.1

Solve the recurrence relation $a_n = 7a_{n-1}$, where $n \geq 1$ and $a_2 = 98$.

This is just an alternative form of the relation $a_{n+1} = 7a_n$ for $n \geq 0$ and $a_2 = 98$. Hence the solution has the form $a_n = a_0(7^n)$. Since $a_2 = 98 = a_0(7^2)$, it follows that $a_0 = 2$, and $a_n = 2(7^n)$, $n \geq 0$, is the unique solution.

EXAMPLE 10.2

A bank pays 6% (annual) interest on savings, compounding the interest monthly. If Bonnie deposits \$1000 on the first day of May, how much will this deposit be worth a year later?

The annual interest rate is 6%, so the monthly rate is $6\%/12 = 0.5\% = 0.005$. For $0 \leq n \leq 12$, let p_n denote the value of Bonnie's deposit at the end of n months. Then $p_{n+1} = p_n + 0.005p_n$, where $0.005p_n$ is the interest earned on p_n during month $n+1$, for $0 \leq n \leq 11$, and $p_0 = \$1000$.

The relation $p_{n+1} = (1.005)p_n$, $p_0 = \$1000$, has the solution $p_n = p_0(1.005)^n = \$1000(1.005)^n$. Consequently, at the end of one year, Bonnie's deposit is worth $\$1000(1.005)^{12} = \$1061.68$.

In the next example we find a fifth way to count the number of compositions of a positive integer. The reader may recall that this situation was examined earlier in Examples 1.37, 3.11, 4.12, and 9.12.

EXAMPLE 10.3

Figure 10.1 provides the compositions of 3 and 4. Here we see that compositions (1′)–(4′) of 4 arise from the corresponding compositions of 3 by increasing the last summand (in each corresponding composition of 3) by 1. The other four compositions of 4, namely, (1″)–(4″), are obtained from the compositions of 3 by appending "+1" to each of the corresponding compositions of 3. (The reader may recall seeing such results in Fig. 4.7.)

		(1′)	4
		(2′)	1 + 3
(1)	3	(3′)	2 + 2
(2)	1 + 2	(4′)	1 + 1 + 2
(3)	2 + 1		
(4)	1 + 1 + 1	(1″)	3 + 1
		(2″)	1 + 2 + 1
		(3″)	2 + 1 + 1
		(4″)	1 + 1 + 1 + 1

Figure 10.1

What happens in Fig. 10.1 exemplifies the general situation. So if we let a_n count the number of compositions of n, for $n \in \mathbf{Z}^+$, we find that

$$a_{n+1} = 2a_n, \qquad n \geq 1, \qquad a_1 = 1.$$

However, in order to apply the formula for the unique solution (where $n \geq 0$) to this recurrence relation, we let $b_n = a_{n+1}$. Then we have

$$b_{n+1} = 2b_n, \qquad n \geq 0, \qquad b_0 = 1,$$

so $b_n = b_0(2^n) = 2^n$, and $a_n = b_{n-1} = 2^{n-1}$, $n \geq 1$.

The recurrence relation $a_{n+1} - da_n = 0$ is called *linear* because each subscripted term appears to the first power (as do the variables x and y in the equation of a line in the plane). In a linear relation there are no products such as $a_n a_{n-1}$, which appears in the nonlinear recurrence relation $a_{n+1} - 3a_n a_{n-1} = 0$. However, there are times when a nonlinear recurrence relation can be transformed into a linear one by a suitable algebraic substitution.

EXAMPLE 10.4

Find a_{12} if $a_{n+1}^2 = 5a_n^2$, where $a_n > 0$ for $n \geq 0$, and $a_0 = 2$.

Although this recurrence relation is not linear in a_n, if we let $b_n = a_n^2$, then the new relation $b_{n+1} = 5b_n$ for $n \geq 0$, and $b_0 = 4$, is a linear relation whose solution is $b_n = 4 \cdot 5^n$. Therefore, $a_n = 2(\sqrt{5})^n$ for $n \geq 0$, and $a_{12} = 2(\sqrt{5})^{12} = 31{,}250$.

The general first-order linear recurrence relation with constant coefficients has the form $a_{n+1} + ca_n = f(n)$, $n \geq 0$, where c is a constant and $f(n)$ is a function on the set $\mathbf{N}$ of nonnegative integers.

When $f(n) = 0$ for all $n \in \mathbf{N}$, the relation is called *homogeneous*; otherwise it is called *nonhomogeneous*. So far we have only dealt with homogeneous relations. Now we shall solve a nonhomogeneous relation. We shall develop specific techniques that work for all linear homogeneous recurrence relations with constant coefficients. However, many different techniques prove useful when we deal with a nonhomogeneous problem, although none allows us to solve everything that can arise.

EXAMPLE 10.5

Perhaps the most popular, though not the most efficient, method of sorting numeric data is a technique called the *bubble sort*. Here the input is a positive integer n and an array $x_1, x_2, x_3, \ldots, x_n$ of real numbers that are to be sorted into ascending order.

The pseudocode procedure in Fig. 10.2 provides an implementation for an algorithm to carry out this sorting process. Here the integer variable i is the counter for the outer **for** loop, whereas the integer variable j is the counter for the inner **for** loop. Finally, the real variable *temp* is used for storage that is needed when an exchange takes place.

```
procedure BubbleSort(n: positive integer; x1,x2,x3,...,xn: real numbers)
begin
  for i := 1 to n − 1 do
    for j := n downto i + 1 do
      if xj < xj−1 then
        begin        {interchange}
          temp := xj−1
          xj−1 := xj
          xj := temp
        end
end
```

Figure 10.2

We compare the last entry, x_n, in the given array with its immediate predecessor, x_{n-1}. If $x_n < x_{n-1}$, we interchange the values stored in x_{n-1} and x_n. In any event we will now have $x_{n-1} \leq x_n$. Then we compare x_{n-1} with its immediate predecessor, x_{n-2}. If $x_{n-1} < x_{n-2}$, we interchange them. We continue the process. After $n - 1$ such comparisons, the smallest number in the list is stored in x_1. We then repeat this process for the $n - 1$ numbers now stored in the (smaller) array $x_2, x_3, \ldots, x_n$. In this way, each time (counted by i) this process is carried out, the smallest number in the remaining sublist "bubbles up" to the front of that sublist.

A small example wherein $n = 5$ and $x_1 = 7$, $x_2 = 9$, $x_3 = 2$, $x_4 = 5$, and $x_5 = 8$ is given in Fig. 10.3 to show how the bubble sort of Fig. 10.2 places a given sequence in ascending order. In this figure each comparison that leads to an interchange is denoted by the symbol $\circlearrowleft$; the symbol } indicates a comparison that results in no interchange.

To determine the time-complexity function $h(n)$ when this algorithm is used on an input (array) of size $n \geq 1$, we count the total number of *comparisons* made in order to sort the n given numbers into ascending order.

If a_n denotes the number of comparisons needed to sort n numbers in this way, then we get the following recurrence relation:

$$a_n = a_{n-1} + (n - 1), \qquad n \geq 2, \qquad a_1 = 0.$$

i = 1	x_1	7	7	7	7	2
	x_2	9	9	9	2	7
	x_3	2	2	2	9	9
	x_4	5	5	5	5	5
	x_5	8	8	8	8	8
		j = 5	j = 4	j = 3	j = 2	

Four comparisons and two interchanges.

i = 2	x_1	2	2	2	2
	x_2	7	7	7	5
	x_3	9	9	5	7
	x_4	5	5	9	9
	x_5	8	8	8	8
		j = 5	j = 4	j = 3	

Three comparisons and two interchanges.

i = 3	x_1	2	2	2
	x_2	5	5	5
	x_3	7	7	7
	x_4	9	8	8
	x_5	8	9	9
		j = 5	j = 4	

Two comparisons and one interchange.

i = 4	x_1	2
	x_2	5
	x_3	7
	x_4	8
	x_5	9
		j = 5

One comparison but no interchanges.

Figure 10.3

This arises as follows. Given a list of n numbers, we make $n - 1$ comparisons to bubble the smallest number up to the start of the list. The remaining sublist of $n - 1$ numbers then requires a_{n-1} comparisons in order to be completely sorted.

This relation is a linear first-order relation with constant coefficients, but the term $n - 1$ makes it nonhomogeneous. Since we have no technique for attacking such a relation, let us list some terms and see whether there is a recognizable pattern.

$$\begin{aligned}
a_1 &= 0 \\
a_2 &= a_1 + (2 - 1) = 1 \\
a_3 &= a_2 + (3 - 1) = 1 + 2 \\
a_4 &= a_3 + (4 - 1) = 1 + 2 + 3 \\
\cdots \quad & \cdots \quad \cdots \quad \cdots
\end{aligned}$$

In general, $a_n = 1 + 2 + \cdots + (n - 1) = [(n - 1)n]/2 = (n^2 - n)/2$.

As a result, the bubble sort determines the time-complexity function $h: \mathbf{Z}^+ \to \mathbf{R}$ given by $h(n) = a_n = (n^2 - n)/2$. [Here $h(\mathbf{Z}^+) \subset \mathbf{N}$.] Consequently, as a measure of the running time for the algorithm, we write $h \in O(n^2)$. Hence the bubble sort is said to require $O(n^2)$ comparisons.

EXAMPLE 10.6

In part (c) of Example 9.6 we sought the generating function for the sequence 0, 2, 6, 12, 20, 30, 42, . . . , and the solution rested upon our ability to recognize that $a_n = n^2 + n$ for each $n \in \mathbf{N}$. If we fail to see this, perhaps we can examine the given sequence and determine whether there is some other pattern that will help us.

Here $a_0 = 0$, $a_1 = 2$, $a_2 = 6$, $a_3 = 12$, $a_4 = 20$, $a_5 = 30$, $a_6 = 42$, and

$$\begin{array}{lll} a_1 - a_0 = 2 & a_3 - a_2 = 6 & a_5 - a_4 = 10 \\ a_2 - a_1 = 4 & a_4 - a_3 = 8 & a_6 - a_5 = 12. \end{array}$$

These calculations suggest the recurrence relation

$$a_n - a_{n-1} = 2n, \qquad n \geq 1, \qquad a_0 = 0.$$

To solve this relation, we proceed in a slightly different manner from the method we used in Example 10.5. Consider the following n equations:

$$\begin{aligned} a_1 - a_0 &= 2 \\ a_2 - a_1 &= 4 \\ a_3 - a_2 &= 6 \\ \vdots \quad & \quad \vdots \quad \vdots \\ a_n - a_{n-1} &= 2n. \end{aligned}$$

When we add these equations, the sum for the left-hand side will contain a_i and $-a_i$ for all $1 \leq i \leq n - 1$. So we obtain

$$\begin{aligned} a_n - a_0 &= 2 + 4 + 6 + \cdots + 2n = 2(1 + 2 + 3 + \cdots + n) \\ &= 2[n(n + 1)/2] = n^2 + n. \end{aligned}$$

Since $a_0 = 0$, it follows that $a_n = n^2 + n$ for all $n \in \mathbf{N}$, as we found earlier in part (c) of Example 9.6.

At this point we shall examine a recurrence relation with a variable coefficient.

EXAMPLE 10.7

Solve the relation $a_n = n \cdot a_{n-1}$, where $n \geq 1$ and $a_0 = 1$.

Writing the first five terms defined by the relation, we have

$$\begin{array}{lll} a_0 = 1 & a_2 = 2 \cdot a_1 = 2 \cdot 1 & a_4 = 4 \cdot a_3 = 4 \cdot 3 \cdot 2 \cdot 1 \\ a_1 = 1 \cdot a_0 = 1 & a_3 = 3 \cdot a_2 = 3 \cdot 2 \cdot 1 & \end{array}$$

Therefore, $a_n = n!$ and the solution is the discrete function a_n, which counts the number of permutations of n objects, $n \geq 0$.

While on the subject of permutations, we shall examine a recursive algorithm for generating the permutations of $\{1, 2, 3, \ldots, n-1, n\}$ from those for $\{1, 2, 3, \ldots, n-1\}$.[†] There is only one permutation of $\{1\}$. Examining the permutations of $\{1, 2\}$,

	1	2
2	1	

we see that after writing the permutation 1 twice, we intertwine the number 2 about 1 to get the permutations listed. Writing each of these two permutations three times, we intertwine the number 3 and obtain

	1		2	3
	1	3	2	
3	1		2	
3	2		1	
	2	3	1	
	2		1	3

We see here that the first permutation is 123 and that we obtain each of the next two permutations from its immediate predecessor by interchanging two numbers: 3 and the integer to its left. When 3 reaches the left side of the permutation, we examine the remaining numbers and permute them according to the list of permutations we generated for $\{1, 2\}$. (This makes the procedure recursive.) After that we interchange 3 with the integer on its right until 3 is on the right side of the permutation. We note that if we interchange 1 and 2 in the last permutation, we get 123, the first permutation listed.

Continuing for $S = \{1, 2, 3, 4\}$, we first list each of the six permutations of $\{1, 2, 3\}$ four times. Starting with the permutation 1234, we intertwine the 4 throughout the remaining 23 permutations as indicated in Table 10.1 (on page 454). The only new idea here develops as follows. When progressing from permutation (5) to (6) to (7) to (8), we interchange 4 with the integer to its right. At permutation (8), where 4 has reached the right side, we obtain permutation (9) by keeping the location of 4 fixed and replacing the permutation 132 by 312 from the list of permutations of $\{1, 2, 3\}$. After that we continue as for the first eight permutations until we reach permutation (16), where 4 is again on the right. We then permute 321 to obtain 231 and continue intertwining 4 until all 24 permutations have been generated. Once again, if 1 and 2 are interchanged in the last permutation, we obtain the first permutation in our list.

The chapter references provide more information on recursive procedures for generating permutations and combinations.

We shall close this first section by returning to an earlier idea — the greatest common divisor of two positive integers.

EXAMPLE 10.8

Recursive methods are fundamental in the areas of discrete mathematics and the analysis of algorithms. Such methods arise when we want to solve a given problem by breaking it down, or referring it, to smaller similar problems. In many programming languages this can be implemented by the use of recursive functions and procedures, which are permitted to invoke themselves. This example will provide one such procedure.

[†]The material from here to the end of this section is a digression that uses the idea of recursion. It does not deal with methods for solving recurrence relations and may be omitted with no loss of continuity.

Table 10.1

(1)		1		2		3	4
(2)		1		2	4	3	
(3)		1	4	2		3	
(4)	4	1		2		3	
(5)	4	1		3		2	
(6)		1	4	3		2	
(7)		1		3	4	2	
(8)		1		3		2	4
(9)		3		1		2	4
(10)		3		1	4	2	
(11)		3	4	1		2	
...		...		...		...	
(15)		3		2	4	1	
(16)		3		2		1	4
(17)		2		3		1	4
...		...		...		...	
(22)		2	4	1		3	
(23)		2		1	4	3	
(24)		2		1		3	4

In computing gcd(333, 84) we obtain the following calculations when we use the Euclidean algorithm (presented in Section 4.4).

$$333 = 3(84) + 81 \qquad 0 < 81 < 84 \tag{1}$$

$$84 = 1(81) + 3 \qquad 0 < 3 < 81 \tag{2}$$

$$81 = 27(3) + 0. \tag{3}$$

Since 3 is the last nonzero remainder, the Euclidean algorithm tells us that gcd(333, 84) = 3. However, if we use only the calculations in Eqs. (2) and (3), then we find that gcd(84, 81) = 3. And Eq. (3) alone implies that gcd(81, 3) = 3 because 3 divides 81. Consequently,

$$\gcd(333, 84) = \gcd(84, 81) = \gcd(81, 3) = 3,$$

where the integers involved in the successive calculations get smaller as we go from Eq. (1) to Eq. (2) to Eq. (3).

We also observe that

$$81 = 333 \textbf{ mod } 84 \qquad \text{and} \qquad 3 = 84 \textbf{ mod } 81.$$

Therefore it follows that

$$\gcd(333, 84) = \gcd(84, 333 \textbf{ mod } 84) = \gcd(333 \textbf{ mod } 84, 84 \textbf{ mod } (333 \textbf{ mod } 84)).$$

These results suggest the following recursive method for computing $\gcd(a, b)$, where $a, b \in \mathbf{Z}^+$.

Say we have the input $a, b \in \mathbf{Z}^+$.

Step 1: If $b|a$ (or a **mod** $b = 0$), then $\gcd(a, b) = b$.

Step 2: If $b \nmid a$, then perform the following tasks in the order specified.

i) Set $a = b$.

ii) Set $b = a$ **mod** b, where the value of a for this assignment is the *old* value of a.

iii) Return to step (1).

These ideas are used in the pseudocode procedure in Fig. 10.4. (The reader may wish to compare this procedure with the one given in Fig. 4.11.)

```
procedure gcd2(a, b: positive integers)
begin
  if a mod b = 0 then
    gcd = b
  else gcd = gcd2(b, a mod b)
end
```

Figure 10.4

EXERCISES 10.1

1. Find a recurrence relation, with initial condition, that uniquely determines each of the following geometric progressions.

a) 2, 10, 50, 250, . . .

b) 6, −18, 54, −162, . . .

c) 7, 14/5, 28/25, 56/125, . . .

2. Find the unique solution for each of the following recurrence relations.

a) $a_{n+1} - 1.5a_n = 0, \quad n \geq 0$

b) $4a_n - 5a_{n-1} = 0, \quad n \geq 1$

c) $3a_{n+1} - 4a_n = 0, \quad n \geq 0, \quad a_1 = 5$

d) $2a_n - 3a_{n-1} = 0, \quad n \geq 1, \quad a_4 = 81$

3. If a_n, $n \geq 0$, is the unique solution of the recurrence relation $a_{n+1} - da_n = 0$, and $a_3 = 153/49$, $a_5 = 1377/2401$, what is d?

4. The number of bacteria in a culture is 1000 (approximately), and this number increases 250% every two hours. Use a recurrence relation to determine the number of bacteria present after one day.

5. If Laura invests \$100 at 6% interest compounded quarterly, how many months must she wait for her money to double? (She cannot withdraw the money before the quarter is up.)

6. Paul invested the stock profits he received 15 years ago in an account that paid 8% interest compounded quarterly. If his account now has \$7218.27 in it, what was his initial investment?

7. Let $x_1, x_2, \ldots, x_{20}$ be a list of distinct real numbers to be sorted by the bubble-sort technique of Example 10.5. (a) After how many comparisons will the 10 smallest numbers of the original list be arranged in ascending order? (b) How many more comparisons are needed to finish this sorting job?

8. For the implementation of the bubble sort given in Fig. 10.2, the outer **for** loop is executed $n - 1$ times. This occurs regardless of whether any interchanges take place during the execution of the inner **for** loop. Consequently, for $i = k$, where $1 \leq k \leq n - 2$, if the execution of the inner **for** loop results in no interchanges, then the list is in ascending order. So the execution of the outer **for** loop for $k + 1 \leq i \leq n - 1$ is not needed.

a) For the situation described here, how many unnecessary comparisons are made if the execution of the inner **for** loop for $i = k$ $(1 \leq k \leq n - 2)$ results in no interchanges?

b) Write an improved version of the bubble sort shown in Fig. 10.2. (Your result should eliminate the unnecessary comparisons discussed at the start of this exercise.)

c) Using the number of comparisons as a measure of its running time, determine the best-case and the worst-case time complexities for the algorithm implemented in part (b).

9. Say the permutations of {1, 2, 3, 4, 5} are generated by the procedure developed after Example 10.7. (a) What is the last permutation in the list? (b) What two permutations precede 25134? (c) What three permutations follow 25134?

10. For $n > 1$, a permutation $p_1, p_2, p_3, \ldots, p_n$ of the integers $1, 2, 3, \ldots, n$ is called *orderly* if, for each $i = 1, 2, 3, \ldots, n - 1$, there exists a $j > i$ such that $|p_j - p_i| = 1$. [If $n = 2$, the permutations 1, 2 and 2, 1 are both orderly. When $n = 3$ we find that 3, 1, 2 is an orderly permutation, while 2, 3, 1 is not. (Why not?)] (a) List all the orderly permutations for 1, 2, 3. (b) List all the orderly permutations for 1, 2, 3, 4. (c) If p_1, p_2, p_3, p_4, p_5 is an orderly permutation of 1, 2, 3, 4, 5, what value(s) can p_1 be? (d) For $n > 1$, let a_n count the number of orderly permutations for $1, 2, 3, \ldots, n$. Find and solve a recurrence relation for a_n.

10.2 The Second-Order Linear Homogeneous Recurrence Relation with Constant Coefficients

Let $k \in \mathbf{Z}^+$ and C_0 $(\neq 0)$, $C_1, C_2, \ldots, C_k$ $(\neq 0)$ be real numbers. If a_n, for $n \geq 0$, is a discrete function, then

$$C_0 a_n + C_1 a_{n-1} + C_2 a_{n-2} + \cdots + C_k a_{n-k} = f(n), \qquad n \geq k,$$

is a linear recurrence relation (with constant coefficients) of *order* k. When $f(n) = 0$ for all $n \geq 0$, the relation is called *homogeneous*; otherwise, it is called *nonhomogeneous*.

In this section we shall concentrate on the homogeneous relation of order two:

$$C_0 a_n + C_1 a_{n-1} + C_2 a_{n-2} = 0, \qquad n \geq 2.$$

On the basis of our work in Section 10.1, we seek a solution of the form $a_n = cr^n$, where $c \neq 0$ and $r \neq 0$.

Substituting $a_n = cr^n$ into $C_0 a_n + C_1 a_{n-1} + C_2 a_{n-2} = 0$, we obtain

$$C_0 cr^n + C_1 cr^{n-1} + C_2 cr^{n-2} = 0.$$

With $c, r \neq 0$, this becomes $C_0 r^2 + C_1 r + C_2 = 0$, a quadratic equation which is called the *characteristic equation*. The roots r_1, r_2 of this equation determine the following three cases: (a) r_1, r_2 are distinct real numbers; (b) r_1, r_2 form a complex conjugate pair; or (c) r_1, r_2 are real, but $r_1 = r_2$. In all cases, r_1 and r_2 are called the *characteristic roots*.

Case (A): (Distinct Real Roots)

EXAMPLE 10.9

Solve the recurrence relation $a_n + a_{n-1} - 6a_{n-2} = 0$, where $n \geq 2$ and $a_0 = -1$, $a_1 = 8$.

If $a_n = cr^n$ with $c, r \neq 0$, we obtain $cr^n + cr^{n-1} - 6cr^{n-2} = 0$ from which the characteristic equation $r^2 + r - 6 = 0$ follows:

$$0 = r^2 + r - 6 = (r+3)(r-2) \Rightarrow r = 2, -3.$$

Since we have two distinct real roots, $a_n = 2^n$ and $a_n = (-3)^n$ are both solutions [as are $b(2^n)$ and $d(-3)^n$, for arbitrary constants b, d]. They are *linearly independent solutions* because one is not a multiple of the other; that is, there is no real constant k such that $(-3)^n = k(2^n)$ for *all* $n \in \mathbf{N}$.† We write $a_n = c_1(2^n) + c_2(-3)^n$ for the *general* solution, where c_1, c_2 are arbitrary constants.

With $a_0 = -1$ and $a_1 = 8$, c_1 and c_2 are determined as follows:

$$-1 = a_0 = c_1(2^0) + c_2(-3)^0 = c_1 + c_2$$
$$8 = a_1 = c_1(2^1) + c_2(-3)^1 = 2c_1 - 3c_2.$$

Solving this system of equations, one finds $c_1 = 1, c_2 = -2$. Therefore, $a_n = 2^n - 2(-3)^n$, $n \geq 0$, is the *unique* solution of the given recurrence relation.

The reader should realize that to determine the unique solution of a second-order linear homogeneous recurrence relation with constant coefficients one needs two initial conditions

†We can also call the solutions $a_n = 2^n$ and $a_n = (-3)^n$ *linearly independent* when the following condition is satisfied: For $k_1, k_2 \in \mathbf{R}$, if $k_1(2^n) + k_2(-3)^n = 0$ for *all* $n \in \mathbf{N}$, then $k_1 = k_2 = 0$.

(values) — that is, the value of a_n for two values of n, very often $n = 0$ and $n = 1$, or $n = 1$ and $n = 2$.

An interesting second-order homogeneous recurrence relation is the *Fibonacci relation*. (This was mentioned earlier in Sections 4.2 and 9.6.)

EXAMPLE 10.10

Solve the recurrence relation $F_{n+2} = F_{n+1} + F_n$, where $n \geq 0$ and $F_0 = 0$, $F_1 = 1$.

As in the previous example, let $F_n = cr^n$, for $c, r \neq 0$, $n \geq 0$. Upon substitution we get $cr^{n+2} = cr^{n+1} + cr^n$. This gives the characteristic equation $r^2 - r - 1 = 0$. The characteristic roots are $r = (1 \pm \sqrt{5})/2$, so the general solution is

$$F_n = c_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + c_2 \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

To solve for c_1, c_2, we use the given initial values and write $0 = F_0 = c_1 + c_2$, $1 = F_1 = c_1[(1+\sqrt{5})/2] + c_2[(1-\sqrt{5})/2]$. Since $-c_1 = c_2$, we have $2 = c_1(1+\sqrt{5}) - c_1(1-\sqrt{5})$ and $c_1 = 1/\sqrt{5}$. The general solution is given by

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right], \qquad n \geq 0.$$

When dealing with the Fibonacci numbers one often finds the assignments $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$, where α is known as the *golden ratio*. As a result, we find that

$$F_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n) = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad n \geq 0.$$

[This representation is referred to as the *Binet form* for F_n, as it was first published in 1843 by Jacques Philippe Marie Binet (1786–1856).]

EXAMPLE 10.11

For $n \geq 0$, let $S = \{1, 2, 3, \ldots, n\}$ (when $n = 0$, $S = \emptyset$), and let a_n denote the number of subsets of S that contain no consecutive integers. Find and solve a recurrence relation for a_n.

For $0 \leq n \leq 4$, we have $a_0 = 1$, $a_1 = 2$, $a_2 = 3$, $a_3 = 5$, and $a_4 = 8$. [For example, $a_3 = 5$ because $S = \{1, 2, 3\}$ has $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, and $\{1, 3\}$ as subsets with no consecutive integers (and no other such subsets).] These first five terms are reminiscent of the Fibonacci sequence. But do things change as we continue?

Let $n \geq 2$ and $S = \{1, 2, 3, \ldots, n-2, n-1, n\}$. If $A \subseteq S$ and A is to be counted in a_n, there are two possibilities:

a) $n \in A$: When this happens $(n-1) \notin A$, and $A - \{n\}$ would be counted in a_{n-2}.

b) $n \notin A$: For this case A would be counted in a_{n-1}.

These two cases are exhaustive and mutually disjoint, so we conclude that $a_n = a_{n-1} + a_{n-2}$, where $n \geq 2$ and $a_0 = 1$, $a_1 = 2$, is the recurrence relation for the problem. Now we could solve for a_n, but if we notice that $a_n = F_{n+2}$, $n \geq 0$, then the result of Example 10.10 implies that

$$a_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+2}\right], \qquad n \geq 0.$$

EXAMPLE 10.12

Suppose we have a $2 \times n$ chessboard, for $n \in \mathbf{Z}^+$. The case for $n = 4$ is shown in part (a) of Fig. 10.5. We wish to cover such a chessboard using 2×1 (vertical) dominoes, which can also be used as 1×2 (horizontal) dominoes. Such dominoes (or tiles) are shown in part (b) of Fig. 10.5.

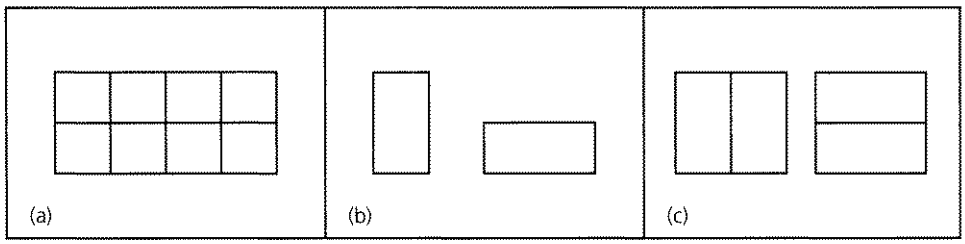


Figure 10.5

For $n \in \mathbf{Z}^+$ we let b_n count the number of ways we can cover (or tile) a $2 \times n$ chessboard using our 2×1 and 1×2 dominoes. Here $b_1 = 1$, for a 2×1 chessboard necessitates one 2×1 (vertical) domino. A 2×2 chessboard can be covered in two ways — using two 2×1 (vertical) dominoes or two 1×2 (horizontal) dominoes, as shown in part (c) of the figure. Hence $b_2 = 2$. For $n \geq 3$, consider the last (nth) column of a $2 \times n$ chessboard. This column can be covered in two ways.

i) By one 2×1 (vertical) domino: Here the remaining $2 \times (n - 1)$ subboard can be covered in b_{n-1} ways.

ii) By the right squares of two 1×2 (horizontal) dominoes placed one above the other: Now the remaining $2 \times (n - 2)$ subboard can be covered in b_{n-2} ways.

Since these two ways have nothing in common and deal with all possibilities, we may write

$$b_n = b_{n-1} + b_{n-2}, \qquad n \geq 3, \qquad b_1 = 1, \qquad b_2 = 2.$$

We find that $b_n = F_{n+1}$, so here is another situation where the Fibonacci numbers arise. The result from Example 10.10 gives us $b_n = (1/\sqrt{5})[((1 + \sqrt{5})/2)^{n+1} - ((1 - \sqrt{5})/2)^{n+1}]$, $n \geq 1$.

EXAMPLE 10.13

At this point we examine an interesting application where the number $\alpha = (1 + \sqrt{5})/2$ plays a major role. This application deals with Gabriel Lamé's work in estimating the number of divisions used in the Euclidean algorithm to find $\gcd(a, b)$, where $a, b \in \mathbf{Z}^+$ with $a \geq b \geq 2$. To find this estimate we need the following property of the Fibonacci numbers, which can be established by the alternative form of the Principle of Mathematical Induction. (A proof is requested in the Section Exercises.)

Property: For $n \geq 3$, $F_n > \alpha^{n-2}$.

Addressing the problem at hand — namely, estimating the number of divisions when the Euclidean algorithm is used to find $\gcd(a, b)$ — we recall the following steps from Theorem 4.7.

Letting $r_0 = a$ and $r_1 = b$, we have

$$\begin{aligned} r_0 &= q_1 r_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= q_2 r_2 + r_3, & 0 < r_3 < r_2 \\ r_2 &= q_3 r_3 + r_4, & 0 < r_4 < r_3 \\ &\cdots\cdots\cdots\cdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= q_n r_n. \end{aligned}$$

So r_n, the last nonzero remainder, is $\gcd(a, b)$.

From the subscripts on r we see that n divisions have been performed in determining $r_n = \gcd(a, b)$. In addition, $q_i \geq 1$, for all $1 \leq i \leq n-1$, and $q_n \geq 2$ because $r_n < r_{n-1}$. Examining the n nonzero remainders $r_n, r_{n-1}, r_{n-2}, \ldots, r_2$, and r_1 $(= b)$, we learn that

$$\begin{aligned} & r_n > 0, \text{ so } r_n \geq 1 = F_2. \\ & [(q_n \geq 2) \wedge (r_n \geq 1)] \Rightarrow r_{n-1} = q_n r_n \geq 2 \cdot 1 = 2 = F_3 \\ & r_{n-2} = q_{n-1} r_{n-1} + r_n \geq 1 \cdot r_{n-1} + r_n \geq F_3 + F_2 = F_4 \\ & \cdots\cdots\cdots\cdots \\ & r_2 = q_3 r_3 + r_4 \geq 1 \cdot r_3 + r_4 \geq F_{n-1} + F_{n-2} = F_n \\ & b = r_1 = q_2 r_2 + r_3 \geq 1 \cdot r_2 + r_3 \geq F_n + F_{n-1} = F_{n+1}. \end{aligned}$$

Therefore, if n divisions are performed by the Euclidean algorithm to determine $\gcd(a, b)$, with $a \geq b \geq 2$, then $b \geq F_{n+1}$. So by virtue of the property introduced earlier, we may write $b > \alpha^{(n+1)-2} = \alpha^{n-1} = [(1 + \sqrt{5})/2]^{n-1}$. Consequently, we find now that

$$b > \alpha^{n-1} \Rightarrow \log_{10} b > \log_{10}(\alpha^{n-1}) = (n-1)\log_{10} \alpha > \frac{n-1}{5},$$

since $\log_{10} \alpha = \log_{10}[(1 + \sqrt{5})/2] \doteq 0.208988 > 0.2 = \frac{1}{5}$.

At this point suppose that $10^{k-1} \leq b < 10^k$, so that the decimal (base 10) representation of b has k digits. Then

$$k = \log_{10} 10^k > \log_{10} b > \frac{n-1}{5}, \quad \text{and} \quad n < 5k + 1.$$

With $n, k \in \mathbf{Z}^+$ we have $n < 5k + 1 \Rightarrow n \leq 5k$, and this last inequality now completes a proof for the following.

Lamé's Theorem: Let $a, b \in \mathbf{Z}^+$ with $a \geq b \geq 2$. Then the number of divisions needed, in the Euclidean algorithm, to determine $\gcd(a, b)$ is at most 5 times the number of decimal digits in b.

Before closing this example, we learn one more fact from Lamé's Theorem. Since $b \geq 2$, it follows that $\log_{10} b \geq \log_{10} 2$, so $5 \log_{10} b \geq 5 \log_{10} 2 = \log_{10} 2^5 = \log_{10} 32 > 1$. From above we know that $n - 1 < 5 \log_{10} b$, so

$$n < 1 + 5 \log_{10} b < 5 \log_{10} b + 5 \log_{10} b = 10 \log_{10} b$$

and $n \in O(\log_{10} b)$. [Hence, the number of divisions needed, in the Euclidean algorithm, to determine $\gcd(a, b)$, for $a, b \in \mathbf{Z}^+$ with $a \geq b \geq 2$, is $O(\log_{10} b)$ — that is, on the order of the number of decimal digits in b.]

Returning to the theme of the section we now examine a recurrence relation in a computer science application.

EXAMPLE 10.14

In many programming languages one may consider those legal arithmetic expressions, *without parentheses*, that are made up of the digits 0, 1, 2, . . . , 9 and the binary operation symbols $+, *, /$. For example, $3 + 4$ and $2 + 3 * 5$ are legal arithmetic expressions; $8 + * 9$ is not. Here $2 + 3 * 5 = 17$, since there is a hierarchy of operations: Multiplication and division are performed before addition. Operations at the same level are performed in their order of appearance as the expression is scanned from left to right.

For $n \in \mathbf{Z}^+$, let a_n be the number of these (legal) arithmetic expressions that are made up of n symbols. Then $a_1 = 10$, since the arithmetic expressions of one symbol are the 10 digits. Next $a_2 = 100$. This accounts for the expressions 00, 01, . . . , 09, 10, 11, . . . , 99. (There are no unnecessary leading plus signs.) When $n \geq 3$, we consider two cases in order to derive a recurrence relation for a_n:

1) If x is an arithmetic expression of $n - 1$ symbols, the last symbol must be a digit. Adding one more digit to the right of x, we get $10a_{n-1}$ arithmetic expressions of n symbols where the last two symbols are digits.
2) Now let y be an arithmetic expression of $n - 2$ symbols. To obtain an arithmetic expression with n symbols (that is not counted in case 1), we adjoin to the right of y one of the 29 two-symbol expressions $+1, \ldots, +9, +0, *1, \ldots, *9, *0, /1, \ldots, /9$.

From these two cases we have $a_n = 10a_{n-1} + 29a_{n-2}$, where $n \geq 3$ and $a_1 = 10$, $a_2 = 100$. Here the characteristic roots are $5 \pm 3\sqrt{6}$ and the solution is $a_n = (5/(3\sqrt{6})) \cdot [(5 + 3\sqrt{6})^n - (5 - 3\sqrt{6})^n]$ for $n \geq 1$. (Verify this result.)

Another way to complete the solution of this problem is to use the recurrence relation $a_n = 10a_{n-1} + 29a_{n-2}$, with $a_2 = 100$ and $a_1 = 10$, to calculate a value for a_0 — namely, $a_0 = (a_2 - 10a_1)/29 = 0$. The solution for the recurrence relation

$$a_n = 10a_{n-1} + 29a_{n-2}, \qquad n \geq 2, \qquad a_0 = 0, \qquad a_1 = 10$$

is

$$a_n = (5/(3\sqrt{6}))[(5 + 3\sqrt{6})^n - (5 - 3\sqrt{6})^n], \qquad n \geq 0.$$

A second method for counting palindromes arises in our next example.

EXAMPLE 10.15

In Fig. 10.6 we find the palindromes of 3, 4, 5, and 6 — that is, the compositions of 3, 4, 5, and 6 that read the same left to right as right to left. (We saw this concept earlier in Example 9.13.) Consider first the palindromes of 3 and 5. To build the palindromes of 5 from those of 3 we do the following:

i) Add 1 to the first and last summands in a palindrome of 3. This is how we get palindromes (1′) and (2′) for 5 from the respective palindromes (1) and (2) for 3. [*Note:* When we have a one summand palindrome n we get the one summand palindrome $n + 2$. That is how we build palindrome (1′) for 5 from palindrome (1) for 3.]
ii) Append "1+" to the start and "+1" to the end of each palindrome of 3. This technique generates the palindromes (1″) and (2″) for 5 from the respective palindromes (1) and (2) for 3.

(1)	3	(1′)	5	(1)	4	(1′)	6
(2)	1 + 1 + 1	(2′)	2 + 1 + 2	(2)	1 + 2 + 1	(2′)	2 + 2 + 2
		(1″)	1 + 3 + 1	(3)	2 + 2	(3′)	3 + 3
		(2″)	1 + 1 + 1 + 1 + 1	(4)	1 + 1 + 1 + 1	(4′)	2 + 1 + 1 + 2
						(1″)	1 + 4 + 1
						(2″)	1 + 1 + 2 + 1 + 1
						(3″)	1 + 2 + 2 + 1
						(4″)	1 + 1 + 1 + 1 + 1 + 1

Figure 10.6

The situation is similar for building the palindromes of 6 from those of 4.

The preceding observations lead us to the following. For $n \in \mathbf{Z}^+$, let p_n count the number of palindromes of n. Then

$$p_n = 2p_{n-2}, \qquad n \geq 3, \qquad p_1 = 1, \qquad p_2 = 2.$$

Substituting $p_n = cr^n$, for $c, r \neq 0$, $n \geq 1$, into this recurrence relation, the resulting characteristic equation is $r^2 - 2 = 0$. The characteristic roots are $r = \pm\sqrt{2}$, so $p_n = c_1(\sqrt{2})^n + c_2(-\sqrt{2})^n$. From

$$\begin{aligned} 1 &= p_1 = c_1(\sqrt{2}) + c_2(-\sqrt{2}) \\ 2 &= p_2 = c_1(\sqrt{2})^2 + c_2(-\sqrt{2})^2 \end{aligned}$$

we find that $c_1 = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)$, $c_2 = \left(\frac{1}{2} - \frac{1}{2\sqrt{2}}\right)$, so

$$p_n = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)(\sqrt{2})^n + \left(\frac{1}{2} - \frac{1}{2\sqrt{2}}\right)(-\sqrt{2})^n, \qquad n \geq 1.$$

Unfortunately, this does not look like the result found in Example 9.13. After all, that answer contained no radical terms. However, suppose we consider n even, say $n = 2k$. Then

$$\begin{aligned} p_n &= \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)(\sqrt{2})^{2k} + \left(\frac{1}{2} - \frac{1}{2\sqrt{2}}\right)(-\sqrt{2})^{2k} \\ &= \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)2^k + \left(\frac{1}{2} - \frac{1}{2\sqrt{2}}\right)2^k = 2^k = 2^{n/2} \end{aligned}$$

For n odd, say $n = 2k - 1$, $k \in \mathbf{Z}^+$, we leave it for the reader to show that $p_n = 2^{k-1} = 2^{(n-1)/2}$.

The preceding results can be expressed by $p_n = 2^{\lfloor n/2 \rfloor}$, $n \geq 1$, as we found in Example 9.13.

The recurrence relation for the next example will be set up in two ways. In the first part we shall see how auxiliary variables may be helpful.

EXAMPLE 10.16

Find a recurrence relation for the number of binary sequences of length n that have no consecutive 0's.

a) For $n \geq 1$, let a_n be the number of such sequences of length n. Let $a_n^{(0)}$ count those that end in 0, and $a_n^{(1)}$ those that end in 1. Then $a_n = a_n^{(0)} + a_n^{(1)}$.

We derive a recurrence relation for a_n, $n \geq 1$, by computing $a_1 = 2$ and then considering each sequence x of length $n - 1$ (> 0) where x contains no consecutive 0's. If x ends in 1, then we can append a 0 or a 1 to it, giving us $2a_{n-1}^{(1)}$ of the sequences counted by a_n. If the sequence x ends in 0, then only 1 can be appended, resulting in $a_{n-1}^{(0)}$ sequences counted by a_n. Since these two cases exhaust all possibilities and have nothing in common, we have

$$a_n = \underbrace{2 \cdot a_{n-1}^{(1)}}_{\text{The } n\text{th position can be 0 or 1.}} + \underbrace{1 \cdot a_{n-1}^{(0)}}_{\text{The } n\text{th position can only be 1.}}$$

If we consider any sequence y counted in a_{n-2} we find that the sequence $y1$ is counted in $a_{n-1}^{(1)}$. Likewise, if the sequence $z1$ is counted in $a_{n-1}^{(1)}$, then z is counted in a_{n-2}. Consequently, $a_{n-2} = a_{n-1}^{(1)}$ and

$$a_n = a_{n-1}^{(1)} + \left[a_{n-1}^{(1)} + a_{n-1}^{(0)}\right] = a_{n-1}^{(1)} + a_{n-1} = a_{n-1} + a_{n-2}.$$

Therefore the recurrence relation for this problem is $a_n = a_{n-1} + a_{n-2}$, where $n \geq 3$ and $a_1 = 2$, $a_2 = 3$. (We leave the details of the solution for the reader.)

b) Alternatively, if $n \geq 1$ and a_n counts the number of binary sequences with no consecutive 0's, then $a_1 = 2$ and $a_2 = 3$, and for $n \geq 3$ we consider the binary sequences counted by a_n. There are two possibilities for these sequences:

(Case 1: The nth symbol is 1) Here we find that the preceding $n - 1$ symbols form a binary sequence with no consecutive 0's. There are a_{n-1} such sequences.

(Case 2: The nth symbol is 0) Here each such sequence actually ends in 10 and the first $n - 2$ symbols provide a binary sequence with no consecutive 0's. In this case there are a_{n-2} such sequences.

Since these two cases cover all the possibilities and have no such sequence in common, we may write

$$a_n = a_{n-1} + a_{n-2}, \qquad n \geq 3, \qquad a_1 = 2, \qquad a_2 = 3,$$

as we found in part (a).

In both part (a) and part (b) we can use the recurrence relation and $a_1 = 2$, $a_2 = 3$ to go back and determine a value for a_0 — namely, $a_0 = a_2 - a_1 = 3 - 2 = 1$. Then we can solve the recurrence relation

$$a_n = a_{n-1} + a_{n-2}, \qquad n \geq 2, \qquad a_0 = 1, \qquad a_1 = 2.$$

Before going any further we want to be sure that the reader understands why a general argument is needed when we develop our recurrence relations. When we are proving a theorem we do *not* draw any general conclusions from a few (or even, perhaps, many) particular instances. The same is true here. The following example should serve to drive this point home.

EXAMPLE 10.17

We start with n identical pennies and let a_n count the number of ways we can arrange these pennies — *contiguous* in each row where each penny above the bottom row touches two pennies in the row below it. (In these arrangements we are *not* concerned with whether any

given penny is heads up or heads down.) In Fig. 10.7 we have the possible arrangements for $1 \leq n \leq 6$. From this it follows that

$$a_1 = 1, \qquad a_2 = 1, \qquad a_3 = 2, \qquad a_4 = 3, \qquad a_5 = 5, \quad \text{and} \quad a_6 = 8.$$

Consequently, these results might *suggest* that, in general, $a_n = F_n$, the nth Fibonacci number. Unfortunately, we have been led astray, as one finds, for example, that

$$a_7 = 12 \neq 13 = F_7, \qquad a_8 = 18 \neq 21 = F_8, \quad \text{and} \quad a_9 = 26 \neq 34 = F_9.$$

(The arrangements in this example were studied by F. C. Auluck in reference [2].)

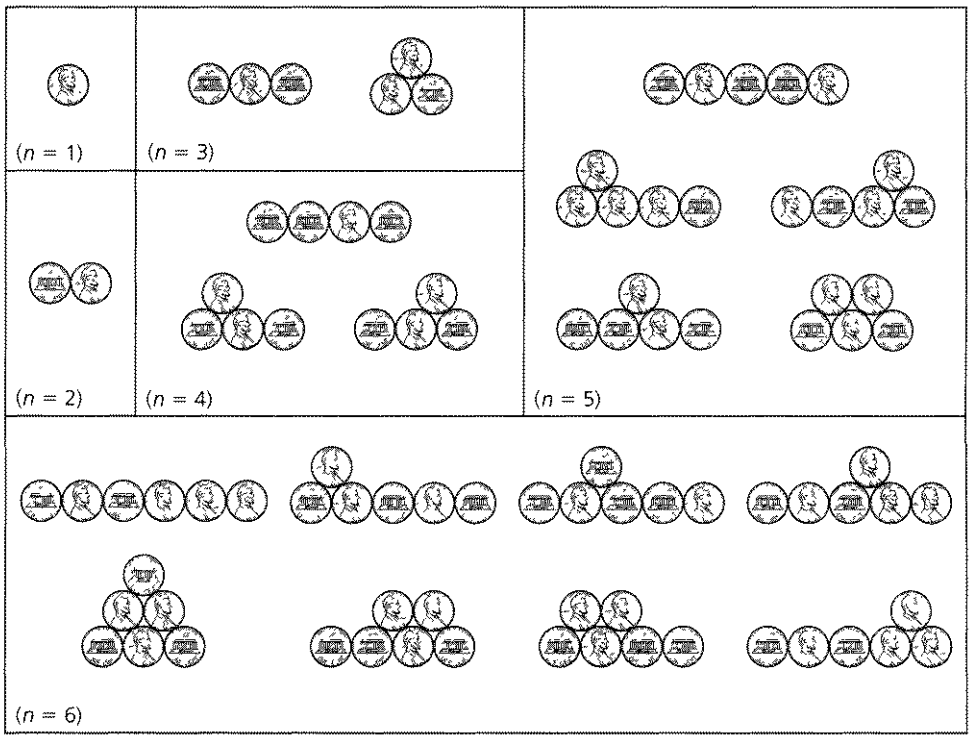


Figure 10.7

The last two examples for case (A) show us how to extend the results for second-order recurrence relations to those of higher order.

EXAMPLE 10.18

Solve the recurrence relation

$$2a_{n+3} = a_{n+2} + 2a_{n+1} - a_n, \qquad n \geq 0, \qquad a_0 = 0, \qquad a_1 = 1, \qquad a_2 = 2.$$

Letting $a_n = cr^n$ for $c, r \neq 0$ and $n \geq 0$, we obtain the characteristic equation $2r^3 - r^2 - 2r + 1 = 0 = (2r - 1)(r - 1)(r + 1)$. The characteristic roots are $1/2$, 1, and -1, so the solution is $a_n = c_1(1)^n + c_2(-1)^n + c_3(1/2)^n = c_1 + c_2(-1)^n + c_3(1/2)^n$. [The solutions 1, $(-1)^n$, and $(1/2)^n$ are called linearly independent because it is impossible to express

any one of them as a linear combination of the other two.†] From $0 = a_0$, $1 = a_1$, and $2 = a_2$, we derive $c_1 = 5/2$, $c_2 = 1/6$, $c_3 = -8/3$. Consequently, $a_n = (5/2) + (1/6)(-1)^n + (-8/3)(1/2)^n$, $n \geq 0$.

EXAMPLE 10.19

For $n \geq 1$ we want to tile a $2 \times n$ chessboard using the two types of tiles shown in part (a) of Fig. 10.8. Letting a_n count the number of such tilings, we find that $a_1 = 1$, since we can tile a 2×1 chessboard (of one column) in only one way — using two 1×1 square tiles. Part (b) of the figure shows us that $a_2 = 5$. Finally, for the 2×3 chessboard there are 11 possible tilings: (i) one that uses six 1×1 square tiles; (ii) eight that use three 1×1 square tiles and one of the larger tiles; and (iii) two that use two of the larger tiles. When $n \geq 4$ we consider the nth column of the $2 \times n$ chessboard. There are three cases to examine:

1) the nth column is covered by two 1×1 square tiles — this case provides a_{n-1} tilings;
2) the $(n-1)$st and nth columns are tiled with one 1×1 square tile and one larger tile — this case accounts for $4a_{n-2}$ tilings; and
3) the $(n-2)$nd, $(n-1)$st, and nth columns are tiled with two of the larger tiles — this results in $2a_{n-3}$ tilings.

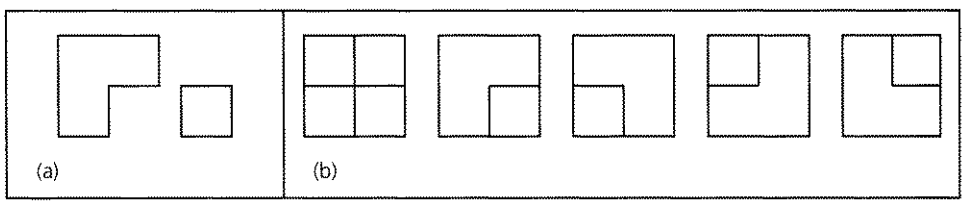


Figure 10.8

These three cases cover all possibilities and no two of the cases have anything in common, so

$$a_n = a_{n-1} + 4a_{n-2} + 2a_{n-3}, \qquad n \geq 4, \qquad a_1 = 1, \qquad a_2 = 5, \qquad a_3 = 11.$$

The characteristic equation $x^3 - x^2 - 4x - 2 = 0$ can be written as $(x+1)(x^2 - 2x - 2) = 0$, so the characteristic roots are -1, $1 + \sqrt{3}$, and $1 - \sqrt{3}$. Consequently, $a_n = c_1(-1)^n + c_2(1+\sqrt{3})^n + c_3(1-\sqrt{3})^n$, $n \geq 1$. From $1 = a_1 = -c_1 + c_2(1+\sqrt{3}) + c_3(1-\sqrt{3})$, $5 = a_2 = c_1 + c_2(1+\sqrt{3})^2 + c_3(1-\sqrt{3})^2$, and $11 = a_3 = -c_1 + c_2(1+\sqrt{3})^3 + c_3(1-\sqrt{3})^3$, we have $c_1 = 1$, $c_2 = 1/\sqrt{3}$, and $c_3 = -1/\sqrt{3}$. So

$$a_n = (-1)^n + (1/\sqrt{3})(1+\sqrt{3})^n + (-1/\sqrt{3})(1-\sqrt{3})^n, \qquad n \geq 1.$$

Case (B): (Complex Roots)

Before getting into the case of complex roots, we recall DeMoivre's Theorem:

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta, \qquad n \geq 0.$$

[This is part (b) of Exercise 12 of Section 4.1.]

†Alternatively, the solutions 1, $(-1)^n$, and $(1/2)^n$ are linearly independent, because if k_1, k_2, k_3 are real numbers, and $k_1(1) + k_2(-1)^n + k_3(1/2)^n = 0$ for *all* $n \in \mathbf{N}$, then $k_1 = k_2 = k_3 = 0$.

If $z = x + iy \in \mathbf{C}$, $z \neq 0$, we can write $z = r(\cos\theta + i\sin\theta)$, where $r = \sqrt{x^2 + y^2}$ and $(y/x) = \tan\theta$, for $x \neq 0$. If $x = 0$, then for $y > 0$,

$$z = yi = yi\sin(\pi/2) = y(\cos(\pi/2) + i\sin(\pi/2)),$$

and for $y < 0$,

$$z = yi = |y|i\sin(3\pi/2) = |y|(\cos(3\pi/2) + i\sin(3\pi/2)).$$

In all cases, $z^n = r^n(\cos n\theta + i\sin n\theta)$, for $n \geq 0$, by DeMoivre's Theorem.

EXAMPLE 10.20

Determine $(1 + \sqrt{3}\,i)^{10}$.

Figure 10.9 shows a geometric way to represent the complex number $1 + \sqrt{3}\,i$ as the point $(1, \sqrt{3})$ in the xy-plane. Here $r = \sqrt{1^2 + (\sqrt{3})^2} = 2$, and $\theta = \pi/3$.

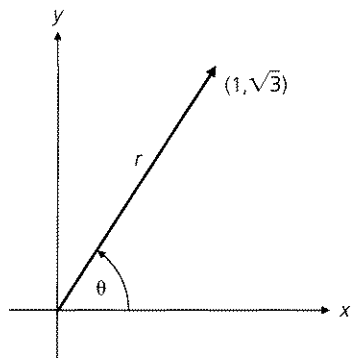


Figure 10.9

So $1 + \sqrt{3}\,i = 2(\cos(\pi/3) + i\sin(\pi/3))$, and

$$\begin{aligned}(1 + \sqrt{3}\,i)^{10} &= 2^{10}(\cos(10\pi/3) + i\sin(10\pi/3)) = 2^{10}(\cos(4\pi/3) + i\sin(4\pi/3)) \\ &= 2^{10}((-1/2) - (\sqrt{3}/2)i) = (-2^9)(1 + \sqrt{3}\,i).\end{aligned}$$

We'll use such results in the following examples.

EXAMPLE 10.21

Solve the recurrence relation $a_n = 2(a_{n-1} - a_{n-2})$, where $n \geq 2$ and $a_0 = 1$, $a_1 = 2$.

Letting $a_n = cr^n$, for $c, r \neq 0$, we obtain the characteristic equation $r^2 - 2r + 2 = 0$, whose roots are $1 \pm i$. Consequently, the general solution has the form $c_1(1 + i)^n + c_2(1 - i)^n$, where c_1 and c_2 presently denote arbitrary *complex* constants. [As in case (A), there are two independent solutions: $(1 + i)^n$ and $(1 - i)^n$.]

$$1 + i = \sqrt{2}(\cos(\pi/4) + i\sin(\pi/4))$$

and

$$1 - i = \sqrt{2}(\cos(-\pi/4) + i\sin(-\pi/4)) = \sqrt{2}(\cos(\pi/4) - i\sin(\pi/4)).$$

This yields

$$\begin{aligned}
a_n &= c_1(1+i)^n + c_2(1-i)^n \\
&= c_1[\sqrt{2}(\cos(\pi/4) + i\sin(\pi/4))]^n + c_2[\sqrt{2}(\cos(-\pi/4) + i\sin(-\pi/4))]^n \\
&= c_1(\sqrt{2})^n(\cos(n\pi/4) + i\sin(n\pi/4)) + c_2(\sqrt{2})^n(\cos(-n\pi/4) + i\sin(-n\pi/4)) \\
&= c_1(\sqrt{2})^n(\cos(n\pi/4) + i\sin(n\pi/4)) + c_2(\sqrt{2})^n(\cos(n\pi/4) - i\sin(n\pi/4)) \\
&= (\sqrt{2})^n[k_1\cos(n\pi/4) + k_2\sin(n\pi/4)],
\end{aligned}$$

where $k_1 = c_1 + c_2$ and $k_2 = (c_1 - c_2)i$.

$$\begin{aligned}
1 &= a_0 = [k_1\cos 0 + k_2\sin 0] = k_1 \\
2 &= a_1 = \sqrt{2}[1\cdot\cos(\pi/4) + k_2\sin(\pi/4)], \text{ or } 2 = 1 + k_2, \text{ and } k_2 = 1.
\end{aligned}$$

The solution for the given initial conditions is then given by

$$a_n = (\sqrt{2})^n[\cos(n\pi/4) + \sin(n\pi/4)], \qquad n \geq 0.$$

[*Note*: This solution contains no complex numbers. A small point may bother the reader here. How did we start with c_1, c_2 complex and end up with $k_1 = c_1 + c_2$ and $k_2 = (c_1 - c_2)i$ real? This happens if c_1, c_2 are complex conjugates.]

Let us now examine an application from linear algebra.

EXAMPLE 10.22

For $b \in \mathbf{R}^+$, consider the $n \times n$ determinant† D_n given by

$$\begin{vmatrix}
b & b & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\
b & b & b & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\
0 & b & b & b & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & b & b & b & \cdots & 0 & 0 & 0 & 0 & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & 0 & 0 & \cdots & b & b & b & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 & b & b & b & 0 \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & b & b & b \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & b & b
\end{vmatrix}$$

Find the value of D_n as a function of n.

Let a_n, $n \geq 1$, denote the value of the $n \times n$ determinant D_n. Then

$$a_1 = |b| = b \quad \text{and} \quad a_2 = \begin{vmatrix} b & b \\ b & b \end{vmatrix} = 0 \quad \left(\text{and} \quad a_3 = \begin{vmatrix} b & b & 0 \\ b & b & b \\ 0 & b & b \end{vmatrix} = -b^3\right).$$

---

†The expansion of determinants is discussed in Appendix 2.

Expanding D_n by its first row, we have $D_n =$

$$b\underbrace{\begin{vmatrix} b & b & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ b & b & b & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & b & b & b & \cdots & 0 & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \cdots & b & b & b & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & b & b & b \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & b & b \end{vmatrix}}_{\text{(This is } D_{n-1}\text{)}} - b\begin{vmatrix} b & b & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & b & b & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & b & b & b & \cdots & 0 & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \cdots & b & b & b & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & b & b & b \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & b & b \end{vmatrix}$$

When we expand the second determinant by its first column, we find that $D_n = bD_{n-1} - (b)(b)D_{n-2} = bD_{n-1} - b^2D_{n-2}$. This translates into the relation $a_n = ba_{n-1} - b^2a_{n-2}$, for $n \geq 3$, $a_1 = b$, $a_2 = 0$.

If we let $a_n = cr^n$ for $c, r \neq 0$ and $n \geq 1$, the characteristic equation produces the roots $b[(1/2) \pm i\sqrt{3}/2]$.

Hence

$$\begin{aligned} a_n &= c_1[b((1/2) + i\sqrt{3}/2)]^n + c_2[b((1/2) - i\sqrt{3}/2)]^n \\ &= b^n[c_1(\cos(\pi/3) + i\sin(\pi/3))^n + c_2(\cos(\pi/3) - i\sin(\pi/3))^n] \\ &= b^n[k_1\cos(n\pi/3) + k_2\sin(n\pi/3)]. \end{aligned}$$

$b = a_1 = b[k_1\cos(\pi/3) + k_2\sin(\pi/3)]$, so $1 = k_1(1/2) + k_2(\sqrt{3}/2)$, or $k_1 + \sqrt{3}\,k_2 = 2$.

$0 = a_2 = b^2[k_1\cos(2\pi/3) + k_2\sin(2\pi/3)]$, so $0 = (k_1)(-1/2) + k_2(\sqrt{3}/2)$, or

$$k_1 = \sqrt{3}\,k_2.$$

Hence $k_1 = 1$, $k_2 = 1/\sqrt{3}$ and the value of D_n is

$$b^n[\cos(n\pi/3) + (1/\sqrt{3})\sin(n\pi/3)].$$

Case (C): (Repeated Real Roots)

EXAMPLE 10.23

Solve the recurrence relation $a_{n+2} = 4a_{n+1} - 4a_n$, where $n \geq 0$ and $a_0 = 1$, $a_1 = 3$.

As in the other two cases, we let $a_n = cr^n$, where $c, r \neq 0$ and $n \geq 0$. Then the characteristic equation is $r^2 - 4r + 4 = 0$ and the characteristic roots are both $r = 2$. (So $r = 2$ is called "a root of multiplicity 2.") Unfortunately, we now lack two independent solutions: 2^n and 2^n are definitely multiples of each other. We need one more independent solution. Let us try $g(n)2^n$ where $g(n)$ is not a constant. Substituting this into the given relation yields

$$g(n+2)2^{n+2} = 4g(n+1)2^{n+1} - 4g(n)2^n$$

or

$$g(n+2) = 2g(n+1) - g(n). \tag{1}$$

One finds that $g(n) = n$ satisfies Eq. (1).† So $n2^n$ is a second independent solution. (It is independent because it is impossible to have $n2^n = k2^n$ for *all* $n \geq 0$ if k is a constant.)

†Actually, the general solution is $g(n) = an + b$, for arbitrary constants a, b, with $a \neq 0$. Here we chose $a = 1$ and $b = 0$ to make $g(n)$ as simple as possible.

The general solution is of the form $a_n = c_1(2^n) + c_2 n(2^n)$. With $a_0 = 1$, $a_1 = 3$ we find $a_n = 2^n + (1/2)n(2^n) = 2^n + n(2^{n-1})$, $n \geq 0$.

In general, if $C_0 a_n + C_1 a_{n-1} + C_2 a_{n-2} + \cdots + C_k a_{n-k} = 0$, with C_0 ($\neq 0$), $C_1, C_2, \ldots, C_k$ ($\neq 0$) real constants, and r a characteristic root of multiplicity m, where $2 \leq m \leq k$, then the part of the general solution that involves the root r has the form

$$A_0 r^n + A_1 n r^n + A_2 n^2 r^n + \cdots + A_{m-1} n^{m-1} r^n$$
$$= (A_0 + A_1 n + A_2 n^2 + \cdots + A_{m-1} n^{m-1}) r^n,$$

where $A_0, A_1, A_2, \ldots, A_{m-1}$ are arbitrary constants.

Our last example involves a little probability.

EXAMPLE 10.24

If a first case of measles is recorded in a certain school system, let p_n denote the probability that at least one case is reported during the nth week after the first recorded case. School records provide evidence that $p_n = p_{n-1} - (0.25)p_{n-2}$, where $n \geq 2$. Since $p_0 = 0$ and $p_1 = 1$, if the first case (of a new outbreak) is recorded on Monday, March 3, 2003, when did the probability for the occurrence of a new case decrease to less than 0.01 for the first time?

With $p_n = cr^n$ for $c, r \neq 0$, the characteristic equation for the recurrence relation is $r^2 - r + (1/4) = 0 = (r - (1/2))^2$. The general solution has the form $p_n = (c_1 + c_2 n)(1/2)^n$, $n \geq 0$. For $p_0 = 0$, $p_1 = 1$, we get $c_1 = 0$, $c_2 = 2$, so $p_n = n2^{-n+1}$, $n \geq 0$.

The first integer n for which $p_n < 0.01$ is 12. Hence, it was not until the week of May 19, 2003, that the probability of another new case occurring was less than 0.01.

EXERCISES 10.2

1. Solve the following recurrence relations. (No final answer should involve complex numbers.)

a) $a_n = 5a_{n-1} + 6a_{n-2}$, $n \geq 2$, $a_0 = 1$, $a_1 = 3$

b) $2a_{n+2} - 11a_{n+1} + 5a_n = 0$, $n \geq 0$, $a_0 = 2$, $a_1 = -8$

c) $a_{n+2} + a_n = 0$, $n \geq 0$, $a_0 = 0$, $a_1 = 3$

d) $a_n - 6a_{n-1} + 9a_{n-2} = 0$, $n \geq 2$, $a_0 = 5$, $a_1 = 12$

e) $a_n + 2a_{n-1} + 2a_{n-2} = 0$, $n \geq 2$, $a_0 = 1$, $a_1 = 3$

2. a) Verify the final solutions in Examples 10.14 and 10.23.

b) Solve the recurrence relation in Example 10.16.

3. If $a_0 = 0$, $a_1 = 1$, $a_2 = 4$, and $a_3 = 37$ satisfy the recurrence relation $a_{n+2} + ba_{n+1} + ca_n = 0$, where $n \geq 0$ and b, c are constants, determine b, c and solve for a_n.

4. Find and solve a recurrence relation for the number of ways to park motorcycles and compact cars in a row of n spaces if each cycle requires one space and each compact needs two. (All cycles are identical in appearance, as are the cars, and we want to use up all the n spaces.)

5. Answer the question posed in Exercise 4 if (a) the motorcycles come in two distinct models; (b) the compact cars come in three different colors; and (c) the motorcycles come in two distinct models and the compact cars come in three different colors.

6. Answer the questions posed in Exercise 5 if empty spaces are allowed.

7. In Exercise 12 of Section 4.2 we learned that $F_0 + F_1 + F_2 + \cdots + F_n = \sum_{i=0}^{n} F_i = F_{n+2} - 1$. This is one of many such properties of the Fibonacci numbers that were discovered by the French mathematician François Lucas (1842–1891). Although we established the result by the Principle of Mathematical Induction, we see that it is easy to develop this formula by adding the system of $n + 1$ equations

$$\begin{aligned} F_0 &= F_2 - F_1 \\ F_1 &= F_3 - F_2 \\ &\cdots \\ F_{n-1} &= F_{n+1} - F_n \\ F_n &= F_{n+2} - F_{n+1}. \end{aligned}$$

Develop formulas for each of the following sums, and then check the general result by the Principle of Mathematical Induction.

a) $F_1 + F_3 + F_5 + \cdots + F_{2n-1}$, where $n \in \mathbf{Z}^+$

b) $F_0 + F_2 + F_4 + \cdots + F_{2n}$, where $n \in \mathbf{Z}^+$

8. a) Prove that

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \frac{1+\sqrt{5}}{2}.$$

(This limit has come to be known as the *golden ratio* and is often designated by α, as we mentioned in Example 10.10.)

b) Consider a regular pentagon $ABCDE$ inscribed in a circle, as shown in Fig. 10.10.

i) Use the law of sines and the double angle formula for the sine to show that $AC/AX = 2\cos 36°$.

ii) As $\cos 18° = \sin 72°$ $= 4\sin 18° \cos 18°(1 - 2\sin^2 18°)$ (Why?), show that $\sin 18°$ is a root of the polynomial equation $8x^3 - 4x + 1 = 0$, and deduce that $\sin 18° = (\sqrt{5} - 1)/4$.

c) Verify that $AC/AX = (1 + \sqrt{5})/2$.

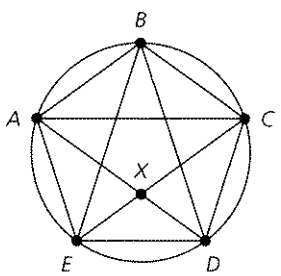


Figure 10.10

9. For $n \geq 0$, let a_n count the number of ways a sequence of 1's and 2's will sum to n. For example, $a_3 = 3$ because (1) 1, 1, 1; (2) 1, 2; and (3) 2, 1 sum to 3. Find and solve a recurrence relation for a_n.

10. For $\Sigma = \{0, 1\}$, let $A \subseteq \Sigma^*$, where $A = \{00, 1\}$. For $n \geq 1$, let a_n count the number of strings in A^* of length n. Find and solve a recurrence relation for a_n. (The reader may wish to refer to Exercise 25 for Section 6.1.)

11. a) For $n \geq 1$, let a_n count the number of binary strings of length n, where there are no consecutive 1's. Find and solve a recurrence relation for a_n.

b) For $n \geq 1$, let b_n count the number of binary strings of length n, where there are no consecutive 1's and the first and last bit of the string are not both 1. Find and solve a recurrence relation for b_n.

12. Suppose that poker chips come in four colors — red, white, green, and blue. Find and solve a recurrence relation for the number of ways to stack n of these poker chips so that there are no consecutive blue chips.

13. An alphabet Σ consists of the four numeric characters 1, 2, 3, 4, and the seven alphabetic characters a, b, c, d, e, f, g. Find and solve a recurrence relation for the number of words of length n (in Σ^*), where there are no consecutive (identical or distinct) alphabetic characters.

14. An alphabet Σ consists of seven numeric characters and k alphabetic characters. For $n \geq 0$, a_n counts the number of strings (in Σ^*) of length n that contain no consecutive (identical or distinct) alphabetic characters. If $a_{n+2} = 7a_{n+1} + 63a_n$, $n \geq 0$, what is the value of k?

15. Solve the recurrence relation $a_{n+2} = a_{n+1}a_n$, $n \geq 0$, $a_0 = 1$, $a_1 = 2$.

16. For $n \geq 1$, let a_n be the number of ways to write n as an ordered sum of positive integers, where each summand is at least 2. (For example, $a_5 = 3$ because here we may represent 5 by 5, by $2 + 3$, and by $3 + 2$.) Find and solve a recurrence relation for a_n.

17. a) For a fixed nonnegative integer n, how many compositions of $n + 3$ have no 1 as a summand?

b) For the compositions in part (a), how many start with (i) 2; (ii) 3; (iii) k, where $2 \leq k \leq n + 1$?

c) How many of the compositions in part (a) start with $n + 2$ or $n + 3$?

d) How are the results in parts (a)–(c) related to the formula derived at the start of Exercise 7?

18. Determine the points of intersection of the parabola $y = x^2 - 1$ and the line $y = x$.

19. Find the points of intersection of the hyperbola $y = 1 + \frac{1}{x}$ and the line $y = x$.

20. a) For $\alpha = (1 + \sqrt{5})/2$, show that $\alpha^2 = \alpha + 1$.

b) If $n \in \mathbf{Z}^+$, prove that $\alpha^n = \alpha F_n + F_{n-1}$.

21. Let F_n denote the nth Fibonacci number, for $n \geq 0$, and let $\alpha = (1 + \sqrt{5})/2$. For $n \geq 3$, prove that (a) $F_n > \alpha^{n-2}$ and (b) $F_n < \alpha^{n-1}$.

22. a) For $n \in \mathbf{Z}^+$, let a_n count the number of palindromes of $2n$. Then $a_{n+1} = 2a_n$, $n \geq 1$, $a_1 = 2$. Solve this first-order recurrence relation for a_n.

b) For $n \in \mathbf{Z}^+$, let b_n count the number of palindromes of $2n - 1$. Set up and solve a first-order recurrence relation for b_n.

(You may want to compare your solutions here with those given in Examples 9.13 and 10.15.)

23. Consider ternary strings — that is, strings where 0, 1, 2 are the only symbols used. For $n \geq 1$, let a_n count the number of ternary strings of length n where there are no consecutive 1's and no consecutive 2's. Find and solve a recurrence relation for a_n.

24. For $n \geq 1$, let a_n count the number of ways to tile a $2 \times n$ chessboard using horizontal (1×2) dominoes [which can also be used as vertical (2×1) dominoes] and square (2×2) tiles. Find and solve a recurrence relation for a_n.

25. In how many ways can one tile a 2×10 chessboard using dominoes and square tiles (as in Exercise 24) if the dominoes come in four colors and the square tiles come in five colors?

26. Let $\Sigma = \{0, 1\}$ and $A = \{0, 01, 11\} \subseteq \Sigma^*$. For $n \geq 1$, let a_n count the number of strings in A^* of length n. Find and solve a recurrence relation for a_n.

27. Let $\Sigma = \{0, 1\}$ and $A = \{0, 01, 011, 111\} \subseteq \Sigma^*$. For $n \geq 1$, let a_n count the number of strings in A^* of length n. Find and solve a recurrence relation for a_n.

28. Let $\Sigma = \{0, 1\}$ and $A = \{0, 01, 011, 0111, 1111\} \subseteq \Sigma^*$. For $n \geq 1$, let a_n count the number of strings in A^* of length n. Find and solve a recurrence relation for a_n.

29. A particle moves horizontally to the right. For $n \in \mathbf{Z}^+$, the distance the particle travels in the $(n+1)$st second is equal to twice the distance it travels during the nth second. If x_n, $n \geq 0$, denotes the position of the particle at the start of the $(n+1)$st second, find and solve a recurrence relation for x_n, where $x_0 = 1$ and $x_1 = 5$.

30. For $n \geq 1$, let D_n be the following $n \times n$ determinant.

$$\begin{vmatrix} 2 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 2 \end{vmatrix}$$

Find and solve a recurrence relation for the value of D_n.

31. Solve the recurrence relation $a_{n+2}^2 - 5a_{n+1}^2 + 4a_n^2 = 0$, where $n \geq 0$ and $a_0 = 4$, $a_1 = 13$.

32. Determine the constants b and c if $a_n = c_1 + c_2(7^n)$, $n \geq 0$, is the general solution of the relation $a_{n+2} + ba_{n+1} + ca_n = 0$, $n \geq 0$.

33. Prove that any two consecutive Fibonacci numbers are relatively prime.

34. Write a computer program (or develop an algorithm) to determine whether a given nonnegative integer is a Fibonacci number.

10.3 The Nonhomogeneous Recurrence Relation

We now turn to the recurrence relations

$$a_n + C_1 a_{n-1} = f(n), \qquad n \geq 1, \tag{1}$$

$$a_n + C_1 a_{n-1} + C_2 a_{n-2} = f(n), \qquad n \geq 2, \tag{2}$$

where C_1 and C_2 are constants, $C_1 \neq 0$ in Eq. (1), $C_2 \neq 0$, and $f(n)$ is not identically 0. Although there is no general method for solving all nonhomogeneous relations, for certain functions $f(n)$ we shall find a successful technique.

We start with the special case for Eq. (1), when $C_1 = -1$. For the nonhomogeneous relation $a_n - a_{n-1} = f(n)$, we have

$$\begin{aligned} a_1 &= a_0 + f(1) \\ a_2 &= a_1 + f(2) = a_0 + f(1) + f(2) \\ a_3 &= a_2 + f(3) = a_0 + f(1) + f(2) + f(3) \\ &\vdots \\ a_n &= a_{n-1} + f(n) = a_0 + f(1) + \cdots + f(n) = a_0 + \sum_{i=1}^{n} f(i). \end{aligned}$$

We can solve this type of relation in terms of n, if we can find a suitable summation formula for $\sum_{i=1}^{n} f(i)$.

EXAMPLE 10.25

Solve the recurrence relation $a_n - a_{n-1} = 3n^2$, where $n \geq 1$ and $a_0 = 7$.

Here $f(n) = 3n^2$, so the unique solution is

$$a_n = a_0 + \sum_{i=1}^{n} f(i) = 7 + 3\sum_{i=1}^{n} i^2 = 7 + \frac{1}{2}(n)(n+1)(2n+1).$$

When a formula for the summation is not known, the following procedure will handle Eq. (1) for certain functions $f(n)$, regardless of the value of C_1 ($\neq 0$). It also works for the second-order nonhomogeneous relation in Eq. (2)—again, for certain functions $f(n)$. Known as the *method of undetermined coefficients*, it relies on the associated homogeneous relation obtained when $f(n)$ is replaced by 0.

For either of Eq. (1) or Eq. (2), we let $a_n^{(h)}$ denote the general solution of the associated homogeneous relation, and we let $a_n^{(p)}$ be a solution of the given nonhomogeneous relation. The term $a_n^{(p)}$ is called a *particular* solution. Then $a_n = a_n^{(h)} + a_n^{(p)}$ is the general solution of the given relation. To determine $a_n^{(p)}$ we use the form of $f(n)$ to suggest a form for $a_n^{(p)}$.

EXAMPLE 10.26

Solve the recurrence relation $a_n - 3a_{n-1} = 5(7^n)$, where $n \geq 1$ and $a_0 = 2$.

The solution of the associated homogeneous relation is $a_n^{(h)} = c(3^n)$. Since $f(n) = 5(7^n)$, we seek a particular solution $a_n^{(p)}$ of the form $A(7^n)$. As $a_n^{(p)}$ is to be a solution of the given nonhomogeneous relation, we place $a_n^{(p)} = A(7^n)$ into the given relation and find that $A(7^n) - 3A(7^{n-1}) = 5(7^n)$, $n \geq 1$. Dividing by 7^{n-1}, we find that $7A - 3A = 5(7)$, so $A = 35/4$, and $a_n^{(p)} = (35/4)7^n = (5/4)7^{n+1}$, $n \geq 0$. The general solution is $a_n = c(3^n) + (5/4)7^{n+1}$. With $2 = a_0 = c + (5/4)(7)$, it follows that $c = -27/4$ and $a_n = (5/4)(7^{n+1}) - (1/4)(3^{n+3})$, $n \geq 0$.

EXAMPLE 10.27

Solve the recurrence relation $a_n - 3a_{n-1} = 5(3^n)$, where $n \geq 1$ and $a_0 = 2$.

As in Example 10.26, $a_n^{(h)} = c(3^n)$, but here $a_n^{(h)}$ and $f(n)$ are not linearly independent. As a result we consider a particular solution $a_n^{(p)}$ of the form $Bn(3^n)$. (What happens if we substitute $a_n^{(p)} = B(3^n)$ into the given relation?)

Substituting $a_n^{(p)} = Bn3^n$ into the given relation yields

$$Bn(3^n) - 3B(n-1)(3^{n-1}) = 5(3^n), \quad \text{or} \quad Bn - B(n-1) = 5, \quad \text{so} \quad B = 5.$$

Hence $a_n = a_n^{(h)} + a_n^{(p)} = (c + 5n)3^n$, $n \geq 0$. With $a_0 = 2$, the unique solution is $a_n = (2 + 5n)(3^n)$, $n \geq 0$.

From the two preceding examples we generalize as follows.

Consider the nonhomogeneous first-order relation

$$a_n + C_1 a_{n-1} = kr^n,$$

where k is a constant and $n \in \mathbf{Z}^+$. If r^n is *not* a solution of the associated homogeneous relation

$$a_n + C_1 a_{n-1} = 0,$$

then $a_n^{(p)} = Ar^n$, where A is a constant. When r^n is a solution of the associated homogeneous relation, then $a_n^{(p)} = Bnr^n$, for B a constant.

Now consider the case of the nonhomogeneous second-order relation

$$a_n + C_1 a_{n-1} + C_2 a_{n-2} = kr^n,$$

where k is a constant. Here we find that

a) $a_n^{(p)} = Ar^n$, for A a constant, if r^n is not a solution of the associated homogeneous relation;

b) $a_n^{(p)} = Bnr^n$, where B is a constant, if $a_n^{(h)} = c_1 r^n + c_2 r_1^n$, where $r_1 \neq r$; and

c) $a_n^{(p)} = Cn^2 r^n$, for C a constant, when $a_n^{(h)} = (c_1 + c_2 n)r^n$.

EXAMPLE 10.28

The Towers of Hanoi. Consider n circular disks (having different diameters) with holes in their centers. These disks can be stacked on any of the pegs shown in Fig. 10.11. In the figure, $n = 5$ and the disks are stacked on peg 1 with no disk resting upon a smaller one. The objective is to transfer the disks one at a time so that we end up with the original stack on peg 3. Each of pegs 1, 2, and 3 may be used as a temporary location for any disk(s), but at no time are we allowed to have a larger disk on top of a smaller one on any peg. What is the minimum number of moves needed to do this for n disks?

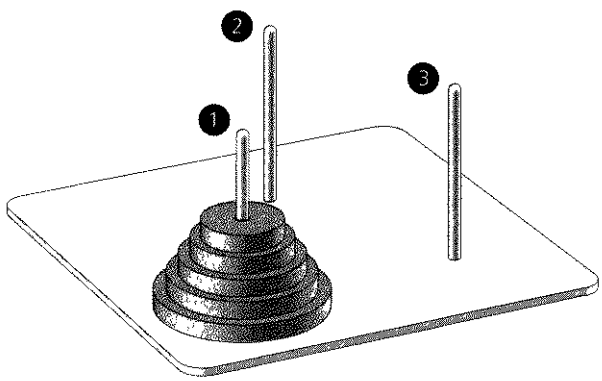


Figure 10.11

For $n \geq 0$, let a_n count the *minimum* number of moves it takes to transfer n disks from peg 1 to peg 3 in the manner described. Then, for $n + 1$ disks we can do the following:

a) Transfer the top n disks from peg 1 to peg 2 according to the directions that are given. This takes at least a_n moves.

b) Transfer the largest disk from peg 1 to peg 3. This takes one move.

c) Finally, transfer the n disks on peg 2 onto the largest disk, now on peg 3 — once again following the specified directions. This also requires at least a_n moves.

Consequently, at this point we know that a_{n+1} is no more than $2a_n + 1$ — that is, $a_{n+1} \leq 2a_n + 1$. But could there be a method where we actually have $a_{n+1} < 2a_n + 1$? Alas, no! For at some point the largest disk (the one at the bottom of the original stack — on peg 1) must be moved to peg 3. This move requires that peg 3 has no disks on it. So this largest disk may only be moved to peg 3 after the n smaller disks have moved to peg 2 [where they are stacked in increasing size from the smallest (on the top) to the largest (on the bottom)]. Getting these n smaller disks moved, accordingly, requires at least a_n moves. The largest

disk must be moved at least once to get it to peg 3. Then, to get the n smaller disks on top of the largest disk (all on peg 3), according to the requirements, requires at least a_n more steps. So $a_{n+1} \geq a_n + 1 + a_n = 2a_n + 1$.

With $2a_n + 1 \leq a_{n+1} \leq 2a_n + 1$, we now obtain the relation $a_{n+1} = 2a_n + 1$, where $n \geq 0$ and $a_0 = 0$.

For $a_{n+1} - 2a_n = 1$, we know that $a_n^{(h)} = c(2^n)$. Since $f(n) = 1 = (1)^n$ is not a solution of $a_{n+1} - 2a_n = 0$, we set $a_n^{(p)} = A(1)^n = A$ and find from the given relation that $A = 2A + 1$, so $A = -1$ and $a_n = c(2^n) - 1$. From $a_0 = 0 = c - 1$ it then follows that $c = 1$, so $a_n = 2^n - 1$, $n \geq 0$.

The next example arises from the mathematics of finance.

EXAMPLE 10.29

Pauline takes out a loan of S dollars that is to be paid back in T periods of time. If r is the interest rate per period for the loan, what (constant) payment P must she make at the end of each period?

We let a_n denote the amount still owed on the loan at the end of the nth period (following the nth payment). Then at the end of the $(n+1)$st period, the amount Pauline still owes on her loan is a_n (the amount she owed at the end of the nth period) $+ ra_n$ (the interest that accrued during the $(n+1)$st period) $- P$ (the payment she made at the end of the $(n+1)$st period). This gives us the recurrence relation

$$a_{n+1} = a_n + ra_n - P, \qquad 0 \leq n \leq T - 1, \qquad a_0 = S, \qquad a_T = 0.$$

For this relation $a_n^{(h)} = c(1+r)^n$, while $a_n^{(p)} = A$ since no constant is a solution of the associated homogeneous relation. With $a_n^{(p)} = A$ we find $A - (1+r)A = -P$, so $A = P/r$. From $a_0 = S$, we obtain $a_n = (S - (P/r))(1+r)^n + (P/r)$, $0 \leq n \leq T$.

Since $0 = a_T = (S - (P/r))(1+r)^T + (P/r)$, it follows that

$$(P/r) = ((P/r) - S)(1+r)^T \quad \text{and} \quad P = (Sr)[1 - (1+r)^{-T}]^{-1}.$$

We now consider a problem in the analysis of algorithms.

EXAMPLE 10.30

For $n \geq 1$, let S be a set containing 2^n real numbers.

The following procedure is used to determine the maximum and minimum elements of S. We wish to determine the number of comparisons made between pairs of elements in S during the execution of this procedure.

If a_n denotes the number of needed comparisons, then $a_1 = 1$. When $n = 2$, $|S| = 2^2 = 4$, so $S = \{x_1, x_2, y_1, y_2\} = S_1 \cup S_2$ where $S_1 = \{x_1, x_2\}$, $S_2 = \{y_1, y_2\}$. Since $a_1 = 1$, it takes one comparison to determine the maximum and minimum elements in each of S_1, S_2. Comparing the minimum elements of S_1 and S_2 and then their maximum elements, we learn the maximum and minimum elements in S and find that $a_2 = 4 = 2a_1 + 2$. In general, if $|S| = 2^{n+1}$, we write $S = S_1 \cup S_2$ where $|S_1| = |S_2| = 2^n$. To determine the maximum and minimum elements in each of S_1 and S_2 requires a_n comparisons. Comparing the maximum (minimum) elements of S_1 and S_2 requires one more comparison; consequently, $a_{n+1} = 2a_n + 2$, $n \geq 1$.

Here $a_n^{(h)} = c(2^n)$ and $a_n^{(p)} = A$, a constant. Substituting $a_n^{(p)}$ into the relation, we find that $A = 2A + 2$, or $A = -2$. So $a_n = c2^n - 2$, and with $a_1 = 1 = 2c - 2$, we obtain $c = 3/2$. Therefore $a_n = (3/2)(2^n) - 2$.

A note of caution! The existence of this procedure, which requires $(3/2)(2^n) - 2$ comparisons, does *not* exclude the possibility that we could achieve the same results via another remarkably clever method that requires fewer comparisons.

An example on counting certain strings of length 10, for the quaternary alphabet $\Sigma = \{0, 1, 2, 3\}$, provides a slight twist to what we've been doing so far.

EXAMPLE 10.31

For the alphabet $\Sigma = \{0, 1, 2, 3\}$, there are $4^{10} = 1{,}048{,}576$ strings of length 10 (in Σ^{10}, or Σ^*). Now we want to know how many of these more than 1 million strings contain an even number of 1's.

Instead of being so specific about the length of the strings, we will start by letting a_n count those strings among the 4^n strings in Σ^n where there are an even number of 1's. To determine how the strings counted by a_n, for $n \geq 2$, are related to those counted by a_{n-1}, consider the nth symbol of one of these strings of length n (where there is an even number of 1's). Two cases arise:

1) The nth symbol is 0, 2, or 3: Here the preceding $n - 1$ symbols provide one of the strings counted by a_{n-1}. So this case provides $3a_{n-1}$ of the strings counted by a_n.
2) The nth symbol is 1: In this case, there must be an odd number of 1's among the first $n - 1$ symbols. There are 4^{n-1} strings of length $n - 1$ and we want to avoid those that have an even number of 1's — there are $4^{n-1} - a_{n-1}$ such strings. Consequently, this second case gives us $4^{n-1} - a_{n-1}$ of the strings counted by a_n.

These two cases are exhaustive and mutually disjoint, so we may write

$$a_n = 3a_{n-1} + (4^{n-1} - a_{n-1}) = 2a_{n-1} + 4^{n-1}, \qquad n \geq 2.$$

Here $a_1 = 3$ (for the strings 0, 2, and 3). We find that $a_n^{(h)} = c(2^n)$ and $a_n^{(p)} = A(4^{n-1})$. Upon substituting $a_n^{(p)}$ into the above relation we have $A(4^{n-1}) = 2A(4^{n-2}) + 4^{n-1}$, so $4A = 2A + 4$ and $A = 2$. Hence, $a_n = c(2^n) + 2(4^{n-1})$, $n \geq 2$. From $3 = a_1 = 2c + 2$ it follows that $c = 1/2$, so $a_n = 2^{n-1} + 2(4^{n-1})$, $n \geq 1$.

When $n = 10$, we learn that of the $4^{10} = 1{,}048{,}576$ strings in Σ^{10}, there are $2^9 + 2(4^9) = 524{,}800$ that contain an even number of 1's.

Before continuing we realize that the answer here for a_n can be checked by using the exponential generating function $f(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}$ (where $a_0 = 1$). From the techniques developed in Section 9.4 we have

$$\begin{aligned} f(x) &= \left(1 + x + \frac{x^2}{2!} + \cdots\right)\left(1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots\right)\left(1 + x + \frac{x^2}{2!} + \cdots\right)\left(1 + x + \frac{x^2}{2!} + \cdots\right) \\ &= e^x \cdot \left(\frac{e^x + e^{-x}}{2}\right) \cdot e^x \cdot e^x \\ &= \left(\frac{1}{2}\right) e^{4x} + \left(\frac{1}{2}\right) e^{2x} \\ &= \left(\frac{1}{2}\right) \sum_{n=0}^{\infty} \frac{(4x)^n}{n!} + \left(\frac{1}{2}\right) \sum_{n=0}^{\infty} \frac{(2x)^n}{n!}. \end{aligned}$$

Here $a_n =$ the coefficient of $\frac{x^n}{n!}$ in $f(x) = \left(\frac{1}{2}\right) 4^n + \left(\frac{1}{2}\right) 2^n = 2^{n-1} + 2(4^{n-1})$, as above.

EXAMPLE 10.32

In 1904, the Swedish mathematician Helge von Koch (1870–1924) created the intriguing curve now known as the Koch "snowflake" curve. The construction of this curve starts with an equilateral triangle, as shown in part (a) of Fig. 10.12, where the triangle has side 1, perimeter 3, and area $\sqrt{3}/4$. (Recall that an equilateral triangle of side s has perimeter $3s$ and area $s^2\sqrt{3}/4$.) The triangle is then transformed into the Star of David in Fig. 10.12(b) by removing the middle one-third of each side (of the original equilateral triangle) and attaching a new equilateral triangle whose side has length $1/3$. So as we go from part (a) to part (b) in the figure, each side of length 1 is transformed into 4 sides of length $1/3$, and we get a 12-sided polygon of area $(\sqrt{3}/4) + (3)(\sqrt{3}/4)(1/3)^2 = \sqrt{3}/3$. Continuing the process, we transform the figure of part (b) into that of part (c) by removing the middle one-third of each of the 12 sides in the Star of David and attaching an equilateral triangle of side $1/9$ $(= (1/3)^2)$. Now we have [in Fig. 10.12(c)] a $4^2(3)$-sided polygon whose area is

$$(\sqrt{3}/3) + (4)(3)(\sqrt{3}/4)[(1/3)^2]^2 = 10\sqrt{3}/27.$$

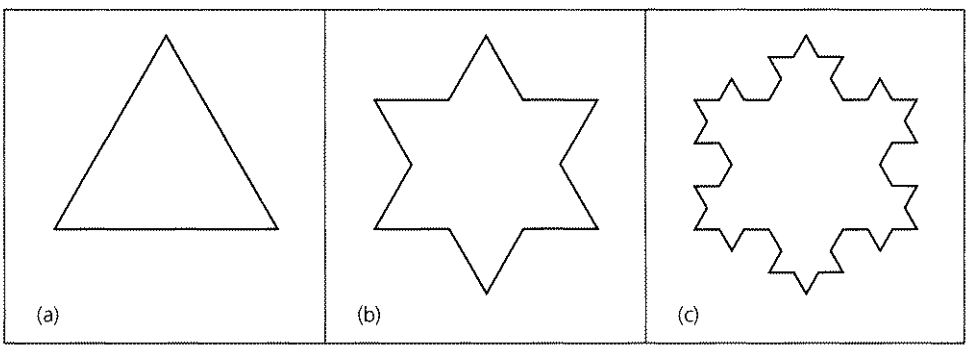


Figure 10.12

For $n \geq 0$, let a_n denote the area of the polygon P_n obtained from the original equilateral triangle after we apply n transformations of the type described above [the first from P_0 in Fig. 10.12(a) to P_1 in Fig. 10.12(b) and the second from P_1 in Fig. 10.12(b) to P_2 in Fig. 10.12(c)]. As we go from P_n (with $4^n(3)$ sides) to P_{n+1} (with $4^{n+1}(3)$ sides), we find that

$$a_{n+1} = a_n + (4^n(3))(\sqrt{3}/4)(1/3^{n+1})^2 = a_n + (1/(4\sqrt{3}))(4/9)^n$$

because in transforming P_n into P_{n+1} we remove the middle one-third of each of the $4^n(3)$ sides of P_n and attach an equilateral triangle of side $(1/3^{n+1})$.

The homogeneous part of the solution for this first-order nonhomogeneous recurrence relation is $a_n^{(h)} = A(1)^n = A$. Since $(4/9)^n$ is not a solution of the associated homogeneous relation, the particular solution is given by $a_n^{(p)} = B(4/9)^n$, where B is a constant. Substituting this into the recurrence relation $a_{n+1} = a_n + (1/(4\sqrt{3}))(4/9)^n$, we find that $B = (-9/5)(1/(4\sqrt{3}))$. Consequently,

$$a_n = A + (-9/5)(1/(4\sqrt{3}))(4/9)^n = A - (1/(5\sqrt{3}))(4/9)^{n-1}, \qquad n \geq 0.$$

Since $\sqrt{3}/4 = a_0 = A - (1/(5\sqrt{3}))(4/9)^{-1}$, it follows that $A = 6/(5\sqrt{3})$ and

$$a_n = (6/(5\sqrt{3})) - (1/(5\sqrt{3}))(4/9)^{n-1} = (1/(5\sqrt{3}))[6 - (4/9)^{n-1}], \qquad n \geq 0.$$

[As n grows larger, we find that $(4/9)^{n-1}$ tends to 0 and a_n approaches $6/(5\sqrt{3})$. We can also obtain this value by continuing the calculations we had before we introduced our recurrence relation, thus noting that this limiting area is also given by

$$(\sqrt{3}/4) + (\sqrt{3}/4)(3)(1/3)^2 + (\sqrt{3}/4)(4)(3)(1/3^2)^2 + (\sqrt{3}/4)(4^2)(3)(1/3^3)^2 + \cdots$$
$$= (\sqrt{3}/4) + (\sqrt{3}/4)(3)\sum_{n=0}^{\infty} 4^n(1/3^{n+1})^2 = (\sqrt{3}/4) + (1/(4\sqrt{3}))\sum_{n=0}^{\infty}(4/9)^n$$
$$= (\sqrt{3}/4) + (1/(4\sqrt{3}))[1/(1-(4/9))] = (\sqrt{3}/4) + (1/(4\sqrt{3}))(9/5) = 6/(5\sqrt{3})$$

by using the result for the sum of a geometric series from part (b) of Example 9.5.]

EXAMPLE 10.33

For $n \geq 1$, let $X_n = \{1, 2, 3, \ldots, n\}$; $\mathcal{P}(X_n)$ denotes the power set of X_n. We want to determine a_n, the number of edges in the Hasse diagram for the partial order $(\mathcal{P}(X_n), \subseteq)$. Here $a_1 = 1$ and $a_2 = 4$, and from Fig. 10.13 it follows that

$$a_3 = 2a_2 + 2^2.$$

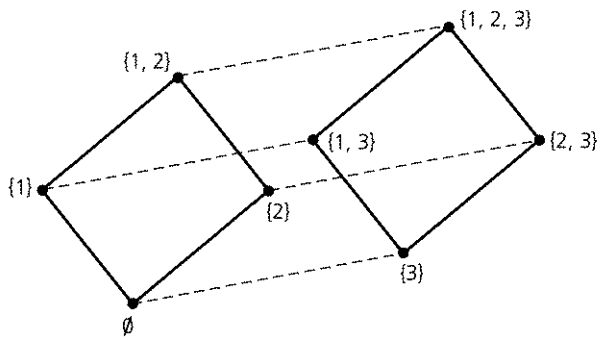


Figure 10.13

This is because the Hasse diagram for $(\mathcal{P}(X_3), \subseteq)$ contains the a_2 edges in the Hasse diagram for $(\mathcal{P}(X_2), \subseteq)$ as well as the a_2 edges in the Hasse diagram for the partial order $(\{\{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}, \subseteq)$. [Note the identical structure shared by the partial orders $(\mathcal{P}(\{1, 2\}), \subseteq)$ and $(\{\{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}, \subseteq)$.] In addition, there are 2^2 other (dashed) edges — one for each subset of $\{1, 2\}$. Now for $n \geq 1$, consider the Hasse diagrams for the partial orders $(\mathcal{P}(X_n), \subseteq)$ and $(\{T \cup \{n+1\} | T \in \mathcal{P}(X_n)\}, \subseteq)$. For each $S \in \mathcal{P}(X_n)$, draw an edge from S in $(\mathcal{P}(X_n), \subseteq)$ to $S \cup \{n+1\}$ in $(\{T \cup \{n+1\} | T \in \mathcal{P}(X_n)\}, \subseteq)$. The result is the Hasse diagram for $(\mathcal{P}(X_{n+1}), \subseteq)$. From the construction we see that

$$a_{n+1} = 2a_n + 2^n, \qquad n \geq 1, \qquad a_1 = 1.$$

The solution to this recurrence relation, with the given condition $a_1 = 1$, is $a_n = n2^{n-1}$, $n \geq 1$.

Each of our next two examples deals with a second-order relation.

EXAMPLE 10.34

Solve the recurrence relation

$$a_{n+2} - 4a_{n+1} + 3a_n = -200, \qquad n \geq 0, \qquad a_0 = 3000, \qquad a_1 = 3300.$$

Here $a_n^{(h)} = c_1(3^n) + c_2(1^n) = c_1(3^n) + c_2$. Since $f(n) = -200 = -200(1^n)$ is a solution of the associated homogeneous relation, here $a_n^{(p)} = An$ for some constant A. This leads us to

$$A(n+2) - 4A(n+1) + 3An = -200, \quad \text{so} \quad -2A = -200, \qquad A = 100.$$

Hence $a_n = c_1(3^n) + c_2 + 100n$. With $a_0 = 3000$ and $a_1 = 3300$, we have $a_n = 100(3^n) + 2900 + 100n$, $n \geq 0$.

Before proceeding any further, a point needs to be made about the role of technology in solving recurrence relations. When a computer algebra system is available, we are spared much of the drudgery of computation. Consequently, all our effort can be directed to analyzing the situation at hand and setting up the recurrence relation with its initial condition(s). Once this is done our job is just about finished. A line or two of code will often do the trick! For example, the Maple code in Fig. 10.14 shows how one can readily solve the recurrence relations of Examples 10.33 and 10.34.

```
> rsolve({a(n+1)=2*a(n)+2^n,a(1)=1},a(n));
```

$$-\frac{2^n}{2} + \left(\frac{n}{2} + \frac{1}{2}\right)2^n$$

```
> simplify(%);
```

$$2^{(n-1)}\, n$$

```
> rsolve({a(n+2)=4*a(n+1)+3*a(n)=-200,a(0)=3000,a(1)=3300},a(n));
```

$$100\, 3^n + 2900 + 100\, n$$

Figure 10.14

EXAMPLE 10.35

In part (a) of Fig. 10.15 we have an *iterative* algorithm (written as a pseudocode procedure) for computing the nth Fibonacci number, for $n \geq 0$. Here the input is a nonnegative integer n and the output is the Fibonacci number F_n. The variables i, *fib*, *last*, *next_to_last*, and *temp* are integer variables. In this algorithm we calculate F_n (in this case for $n \geq 0$) by first assigning or computing all of the previous values $F_0, F_1, F_2, \ldots, F_{n-1}$. Here the number of additions needed to determine F_n is 0 for $n = 0$, 1 and $n - 1$ (within the **for** loop) for $n \geq 2$.

Part (b) of Fig. 10.15 provides a pseudocode procedure to implement a *recursive* algorithm for calculating F_n for $n \in \mathbf{N}$. Here the variable *fib* is likewise an integer variable. For this procedure we wish to determine a_n, the number of additions performed in computing F_n, $n \geq 0$. We find that $a_0 = 0$, $a_1 = 0$, and from the shaded line in the procedure — namely,

```
fib := FibNum2(n - 1) + FibNum2(n - 2)                    (*)
```

we obtain the nonhomogeneous recurrence relation

$$a_n = a_{n-1} + a_{n-2} + 1, \qquad n \geq 2,$$

where the summand of 1 is due to the addition in Eq. (*).

```
procedure FibNum1(n: nonnegative integer)
begin
  if n = 0 then
    fib := 0
  else if n = 1 then
    fib := 1
  else
    begin
      last := 1
      next_to_last := 0
      for i := 2 to n do
        begin
          temp := last
          last := last + next_to_last
          next_to_last := temp
        end
      fib := last
    end
end                                        (a)
```

```
procedure FibNum2(n: nonnegative integer)
begin
  if n = 0 then
    fib := 0
  else if n = 1 then
    fib := 1
  else
    fib := FibNum2(n - 1) + FibNum2(n - 2)
end                                        (b)
```

Figure 10.15

Here we find that $a_n^{(h)} = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n$ and that $a_n^{(p)} = A$, a constant. Upon substituting $a_n^{(p)}$ into the nonhomogeneous recurrence relation we find that

$$A = A + A + 1,$$

so $A = -1$ and $a_n = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n - 1$.

Since $a_0 = 0$ and $a_1 = 0$ it follows that

$$c_1 + c_2 = 1 \quad \text{and} \quad c_1\left(\frac{1+\sqrt{5}}{2}\right) + c_2\left(\frac{1-\sqrt{5}}{2}\right) = 1.$$

From these equations we learn that $c_1 = (1+\sqrt{5})/(2\sqrt{5})$, $c_2 = (\sqrt{5}-1)/(2\sqrt{5})$. Therefore,

$$\begin{aligned} a_n &= \left(\frac{1+\sqrt{5}}{2\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n - 1 \\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1} - 1. \end{aligned}$$

As n gets larger $[(1-\sqrt{5})/2]^{n+1}$ approaches 0 since $|(1-\sqrt{5})/2| < 1$, and $a_n \doteq (1/\sqrt{5})[(1+\sqrt{5})/2]^{n+1} = ((1+\sqrt{5})/(2\sqrt{5}))((1+\sqrt{5})/2)^n$.

Consequently, we can see that, as the value of n increases, the first procedure requires far less computation than the second one does.

We now summarize and extend the solution techniques already discussed in Examples 10.26 through 10.35.

Given a linear nonhomogeneous recurrence relation (with constant coefficients) of the form $C_0a_n + C_1a_{n-1} + C_2a_{n-2} + \cdots + C_ka_{n-k} = f(n)$, where $C_0 \neq 0$ and $C_k \neq 0$, let $a_n^{(h)}$ denote the homogeneous part of the solution a_n.

1) If $f(n)$ is a constant multiple of one of the forms in the first column of Table 10.2 and is not a solution of the associated homogeneous relation, then $a_n^{(p)}$ has the form shown in the second column of Table 10.2. (Here $A, B, A_0, A_1, A_2, \ldots, A_{t-1}, A_t$ are constants determined by substituting $a_n^{(p)}$ into the given relation; t, r, and θ are also constants.)

Table 10.2

	$a_n^{(p)}$
c, a constant	A, a constant
n	$A_1n + A_0$
n^2	$A_2n^2 + A_1n + A_0$
$n^t, t \in \mathbf{Z}^+$	$A_tn^t + A_{t-1}n^{t-1} + \cdots + A_1n + A_0$
$r^n, r \in \mathbf{R}$	Ar^n
$\sin \theta n$	$A \sin \theta n + B \cos \theta n$
$\cos \theta n$	$A \sin \theta n + B \cos \theta n$
n^tr^n	$r^n(A_tn^t + A_{t-1}n^{t-1} + \cdots + A_1n + A_0)$
$r^n \sin \theta n$	$Ar^n \sin \theta n + Br^n \cos \theta n$
$r^n \cos \theta n$	$Ar^n \sin \theta n + Br^n \cos \theta n$

2) When $f(n)$ comprises a sum of constant multiples of terms such as those in the first column of the table for item (1), and none of these terms is a solution of the associated homogeneous relation, then $a_n^{(p)}$ is made up of the sum of the corresponding terms in the column headed by $a_n^{(p)}$. For example, if $f(n) = n^2 + 3 \sin 2n$ and no summand of $f(n)$ is a solution of the associated homogeneous relation, then $a_n^{(p)} = (A_2n^2 + A_1n + A_0) + (A \sin 2n + B \cos 2n)$.

3) Things get trickier if a summand $f_1(n)$ of $f(n)$ is a solution of the associated homogeneous relation. This happens, for example, when $f(n)$ contains summands such as cr^n or $(c_1 + c_2n)r^n$ and r is a characteristic root. If $f_1(n)$ causes this problem, we multiply the trial solution $(a_n^{(p)})_1$ corresponding to $f_1(n)$ by the smallest power of n, say n^s, for which no summand of $n^s f_1(n)$ is a solution of the associated homogeneous relation. Then $n^s\ (a_n^{(p)})_1$ is the corresponding part of $a_n^{(p)}$.

In order to check some of our preceding remarks on particular solutions for nonhomogeneous recurrence relations, the next application provides us with a situation that can be solved in more than one way.

EXAMPLE 10.36

For $n \geq 2$, suppose that there are n people at a party and that each of these people shakes hands (exactly one time) with all of the other people there (and no one shakes hands with himself or herself). If a_n counts the total number of handshakes, then

$$a_{n+1} = a_n + n, \qquad n \geq 2, \qquad a_2 = 1, \tag{3}$$

because when the $(n+1)$st person arrives, he or she will shake hands with the n other people who have already arrived.

According to the results in Table 10.2, we might think that the trial (particular) solution for Eq. (3) is $A_1 n + A_0$, for constants A_0 and A_1. But here the associated homogeneous relation is $a_{n+1} = a_n$, or $a_{n+1} - a_n = 0$, for which $a_n^{(h)} = c(1^n) = c$, where c denotes an arbitrary constant. Therefore, the summand A_0 (in $A_1 n + A_0$) is a solution of the associated homogeneous relation. Consequently, the third remark (given with Table 10.2) tells us that we must multiply $A_1 n + A_0$ by the smallest power of n for which we no longer have any constant summand. This is accomplished by multiplying $A_1 n + A_0$ by n^1, and so we find here that

$$a_n^{(p)} = A_1 n^2 + A_0 n.$$

When we substitute this result into Eq. (3) we have

$$A_1(n+1)^2 + A_0(n+1) = A_1 n^2 + A_0 n + n,$$

or $A_1 n^2 + (2A_1 + A_0)n + (A_1 + A_0) = A_1 n^2 + (A_0 + 1)n$.

By comparing the coefficients on like powers of n we find that

(n^2): $A_1 = A_1$;

(n): $2A_1 + A_0 = A_0 + 1$; and

(n^0): $A_1 + A_0 = 0$.

Consequently, $A_1 = 1/2$ and $A_0 = -1/2$, so $a_n^{(p)} = (1/2)n^2 + (-1/2)n$ and $a_n = a_n^{(h)} + a_n^{(p)} = c + (1/2)(n)(n-1)$. Since $a_2 = 1$, it follows from $1 = a_2 = c + (1/2)(2)(1)$ that $c = 0$, and $a_n = (1/2)(n)(n-1)$, for $n \geq 2$.

We can also obtain this result by considering the n people in the room and realizing that each possible handshake corresponds with a selection of size 2 from this set of size n — and there are $\binom{n}{2} = (n!)/(2!(n-2)!) = (1/2)(n)(n-1)$ such selections. [Or we can consider the n people as vertices of an undirected graph (with no loops) where an edge corresponds with a handshake. Our answer is then the number of edges in the complete graph K_n, and there are $\binom{n}{2} = (1/2)(n)(n-1)$ such edges.]

Our last example further demonstrates how we may use the results in Table 10.2.

EXAMPLE 10.37

a) Consider the nonhomogeneous recurrence relation

$$a_{n+2} - 10a_{n+1} + 21a_n = f(n), \qquad n \geq 0.$$

Here the homogeneous part of the solution is

$$a_n^{(h)} = c_1(3^n) + c_2(7^n),$$

for arbitrary constants c_1, c_2.

In Table 10.3 we list the form for the particular solution for certain choices of $f(n)$. Here the values of the 11 constants A_i, for $0 \leq i \leq 10$, are determined by substituting $a_n^{(p)}$ into the given nonhomogeneous recurrence relation.

Table 10.3

$f(n)$	$a_n^{(p)}$
5	A_0
$3n^2 - 2$	$A_3n^2 + A_2n + A_1$
$7(11^n)$	$A_4(11^n)$
$31(r^n),\ r \neq 3, 7$	$A_5(r^n)$
$6(3^n)$	A_6n3^n
$2(3^n) - 8(9^n)$	$A_7n3^n + A_8(9^n)$
$4(3^n) + 3(7^n)$	$A_9n3^n + A_{10}n7^n$

b) The homogeneous component of the solution for

$$a_n + 4a_{n-1} + 4a_{n-2} = f(n), \qquad n \geq 2,$$

is

$$a_n^{(h)} = c_1(-2)^n + c_2n(-2)^n,$$

where c_1, c_2 denote arbitrary constants. Consequently,

1) if $f(n) = 5(-2)^n$, then $a_n^{(p)} = An^2(-2)^n$;
2) if $f(n) = 7n(-2)^n$, then $a_n^{(p)} = n^2(-2)^n(A_1n + A_0)$; and
3) if $f(n) = -11n^2(-2)^n$, then $a_n^{(p)} = n^2(-2)^n(B_2n^2 + B_1n + B_0)$.
(Here, the constants A, A_0, A_1, B_0, B_1, and B_2 are determined by substituting $a_n^{(p)}$ into the given nonhomogeneous recurrence relation.)

EXERCISES 10.3

1. Solve each of the following recurrence relations.

a) $a_{n+1} - a_n = 2n + 3, \quad n \geq 0, \quad a_0 = 1$

b) $a_{n+1} - a_n = 3n^2 - n, \quad n \geq 0, \quad a_0 = 3$

c) $a_{n+1} - 2a_n = 5, \quad n \geq 0, \quad a_0 = 1$

d) $a_{n+1} - 2a_n = 2^n, \quad n \geq 0, \quad a_0 = 1$

2. Use a recurrence relation to derive the formula for $\sum_{i=0}^{n} i^2$.

3. a) Let n lines be drawn in the plane such that each line intersects every other line but no three lines are ever coincident. For $n \geq 0$, let a_n count the number of regions into which the plane is separated by the n lines. Find and solve a recurrence relation for a_n.

b) For the situation in part (a), let b_n count the number of infinite regions that result. Find and solve a recurrence relation for b_n.

4. On the first day of a new year, Joseph deposits \$1000 in an account that pays 6% interest compounded monthly. At the beginning of each month he adds \$200 to his account. If he continues to do this for the next four years (so that he makes 47 additional deposits of \$200), how much will his account be worth exactly four years after he opened it?

5. Solve the following recurrence relations.

a) $a_{n+2} + 3a_{n+1} + 2a_n = 3^n, \quad n \geq 0, \quad a_0 = 0, \quad a_1 = 1$

b) $a_{n+2} + 4a_{n+1} + 4a_n = 7, \quad n \geq 0, \quad a_0 = 1, \quad a_1 = 2$

6. Solve the recurrence relation $a_{n+2} - 6a_{n+1} + 9a_n = 3(2^n) + 7(3^n)$, where $n \geq 0$ and $a_0 = 1$, $a_1 = 4$.

7. Find the general solution for the recurrence relation $a_{n+3} - 3a_{n+2} + 3a_{n+1} - a_n = 3 + 5n$, $n \geq 0$.

8. Determine the number of n-digit quaternary (0, 1, 2, 3) sequences in which there is never a 3 anywhere to the right of a 0.

9. Meredith borrows \$2500, at 12% compounded monthly, to buy a computer. If the loan is to be paid back over two years, what is his monthly payment?

10. The general solution of the recurrence relation $a_{n+2} + b_1a_{n+1} + b_2a_n = b_3n + b_4$, $n \geq 0$, with b_i constant for $1 \leq i \leq 4$, is $c_12^n + c_23^n + n - 7$. Find b_i for each $1 \leq i \leq 4$.

11. Solve the following recurrence relations.

a) $a_{n+2}^2 - 5a_{n+1}^2 + 6a_n^2 = 7n, \quad n \geq 0, \quad a_0 = a_1 = 1$

b) $a_n^2 - 2a_{n-1} = 0, \quad n \geq 1, \quad a_0 = 2$ (Let $b_n = \log_2 a_n$, $n \geq 0$.)

12. Let $\Sigma = \{0, 1, 2, 3\}$. For $n \geq 1$, let a_n count the number of strings in Σ^n containing an odd number of 1's. Find and solve a recurrence relation for a_n.

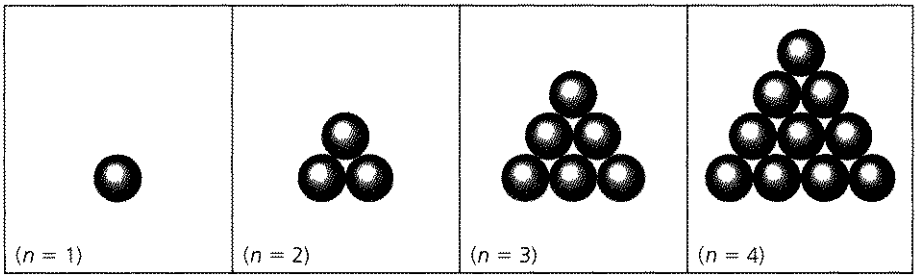


Figure 10.16

13. **a)** For the binary string 001110, there are three runs: 00, 111, and 0. Meanwhile, the string 000111 has only two runs: 000 and 111; while the string 010101 determines the six runs: 0, 1, 0, 1, 0, 1. For $n = 1$, we consider two binary strings, namely, 0 and 1—these two strings (of length 1) determine a total of two runs. There are four binary strings of length $n = 2$ and these strings determine 1 (for 00) + 2 (for 01) + 2 (for 10) + 1 (for 11) = 6 runs. Find and solve a recurrence relation for t_n, the total number of runs determined by the 2^n binary strings of length n, where $n \geq 1$.

b) Answer the question posed in part (a) for quaternary strings of length n. (Here the alphabet comprises 0, 1, 2, 3.)

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

14. **a)** For $n \geq 1$, the nth *triangular number* t_n is defined by $t_n = 1 + 2 + \cdots + n = n(n+1)/2$. Find and solve a recurrence relation for s_n, $n \geq 1$, where $s_n = t_1 + t_2 + \cdots + t_n$, the sum of the first n triangular numbers. [The reader may wish to compare the result obtained here with the formula given in Example 4.5 or with the result requested in part (b) of Exercise 8 of Section 9.5.]

b) In an organic laboratory, Kelsey synthesizes a crystalline structure that is made up of 10,000,000 triangular layers of atoms. The first layer of the structure has one atom, the second layer has three atoms, and, in general, the nth layer has $1 + 2 + \cdots + n = t_n$ atoms. (Consider each layer, other than the last, as if it were placed upon the spaces that result among the neighboring atoms of the succeeding layer. See Fig. 10.16.) (i) How many atoms are there in one of these crystalline structures? (ii) How many atoms are packed (strictly) between the 10,000th and 100,000th layer?

15. Write a computer program (or develop an algorithm) to solve the problem of the Towers of Hanoi. For $n \in \mathbf{Z}^+$, the program should provide the necessary steps for transferring the n disks from peg 1 to peg 3 under the restrictions specified in Example 10.28.

10.4 The Method of Generating Functions

With all the different cases we had to consider for the nonhomogeneous linear recurrence relation, we now get some assistance from the generating function. This technique will find both the homogeneous and the particular solutions for a_n, and it will incorporate the given initial conditions as well. Furthermore, we'll be able to do even more with this method.

We demonstrate the method in the following examples.

EXAMPLE 10.38

Solve the relation $a_n - 3a_{n-1} = n$, $n \geq 1$, $a_0 = 1$.

This relation represents an infinite set of equations:

$$\begin{array}{ll} (n = 1) & a_1 - 3a_0 = 1 \\ (n = 2) & a_2 - 3a_1 = 2 \\ \vdots & \vdots \quad \vdots \end{array}$$

Multiplying the first of these equations by x, the second by x^2, and so on, we obtain

$$\begin{array}{lll} (n=1) & a_1x^1 - 3a_0x^1 = 1x^1 \\ (n=2) & a_2x^2 - 3a_1x^2 = 2x^2 \\ \vdots & \vdots \qquad \vdots \end{array}$$

Adding this second set of equations, we find that

$$\sum_{n=1}^{\infty} a_n x^n - 3\sum_{n=1}^{\infty} a_{n-1}x^n = \sum_{n=1}^{\infty} nx^n. \tag{1}$$

We want to solve for a_n in terms of n. To accomplish this, let $f(x) = \sum_{n=0}^{\infty} a_n x^n$ be the (ordinary) generating function for the sequence $a_0, a_1, a_2 \ldots$. Then Eq. (1) can be rewritten as

$$(f(x) - a_0) - 3x\sum_{n=1}^{\infty} a_{n-1}x^{n-1} = \sum_{n=1}^{\infty} nx^n \left(= \sum_{n=0}^{\infty} nx^n\right). \tag{2}$$

Since $\sum_{n=1}^{\infty} a_{n-1}x^{n-1} = \sum_{n=0}^{\infty} a_n x^n = f(x)$ and $a_0 = 1$, the left-hand side of Eq. (2) becomes $(f(x) - 1) - 3xf(x)$.

Before we can proceed, we need the generating function for the sequence $0, 1, 2, 3, \ldots$. Recall from part (c) of Example 9.5 that

$$\frac{x}{(1-x)^2} = x + 2x^2 + 3x^3 + \cdots, \quad \text{so}$$

$$(f(x) - 1) - 3xf(x) = \frac{x}{(1-x)^2}, \quad \text{and} \quad f(x) = \frac{1}{(1-3x)} + \frac{x}{(1-x)^2(1-3x)}.$$

Using a partial fraction decomposition, we find that

$$\frac{x}{(1-x)^2(1-3x)} = \frac{A}{(1-x)} + \frac{B}{(1-x)^2} + \frac{C}{(1-3x)},$$

or

$$x = A(1-x)(1-3x) + B(1-3x) + C(1-x)^2.$$

From the following assignments for x, we get

$$(x=1): \quad 1 = B(-2), \qquad B = -\frac{1}{2}.$$

$$\left(x = \frac{1}{3}\right): \quad \frac{1}{3} = C\left(\frac{2}{3}\right)^2, \qquad C = \frac{3}{4}.$$

$$(x=0): \quad 0 = A + B + C, \qquad A = -(B+C) = -\frac{1}{4}.$$

Therefore,

$$\begin{aligned} f(x) &= \frac{1}{1-3x} + \frac{(-1/4)}{(1-x)} + \frac{(-1/2)}{(1-x)^2} + \frac{(3/4)}{(1-3x)} \\ &= \frac{(7/4)}{(1-3x)} + \frac{(-1/4)}{(1-x)} + \frac{(-1/2)}{(1-x)^2}. \end{aligned}$$

We find a_n by determining the coefficient of x^n in each of the three summands.

a) $(7/4)/(1-3x) = (7/4)[1/(1-3x)]$
$= (7/4)[1 + (3x) + (3x)^2 + (3x)^3 + \cdots]$, and the coefficient of x^n is $(7/4)3^n$.

b) $(-1/4)/(1-x) = (-1/4)[1 + x + x^2 + \cdots]$, and the coefficient of x^n here is $(-1/4)$.

c) $(-1/2)/(1-x)^2 = (-1/2)(1-x)^{-2}$
$= (-1/2)\left[\binom{-2}{0} + \binom{-2}{1}(-x) + \binom{-2}{2}(-x)^2 + \binom{-2}{3}(-x)^3 + \cdots\right]$
and the coefficient of x^n is given by $(-1/2)\binom{-2}{n}(-1)^n = (-1/2)(-1)^n\binom{2+n-1}{n}\cdot(-1)^n = (-1/2)(n+1)$.

Therefore $a_n = (7/4)3^n - (1/2)n - (3/4)$, $n \geq 0$. (Note that there is no special concern here with $a_n^{(p)}$. Also, the same answer is obtained by using the techniques of Section 10.3.)

In our next example we extend what we learned in Example 10.38 to a second-order relation. This time we present the solution within a list of instructions one can follow in order to apply the generating-function method.

EXAMPLE 10.39

Consider the recurrence relation

$$a_{n+2} - 5a_{n+1} + 6a_n = 2, \qquad n \geq 0, \qquad a_0 = 3, \qquad a_1 = 7.$$

1) We first multiply this given relation by x^{n+2} because $n+2$ is the largest subscript that appears. This gives us

$$a_{n+2}x^{n+2} - 5a_{n+1}x^{n+2} + 6a_nx^{n+2} = 2x^{n+2}.$$

2) Then we sum all of the equations represented by the result in step (1) and obtain

$$\sum_{n=0}^{\infty} a_{n+2}x^{n+2} - 5\sum_{n=0}^{\infty} a_{n+1}x^{n+2} + 6\sum_{n=0}^{\infty} a_nx^{n+2} = 2\sum_{n=0}^{\infty} x^{n+2}.$$

3) In order to have each of the subscripts on a match the corresponding exponent on x, we rewrite the equation in step (2) as

$$\sum_{n=0}^{\infty} a_{n+2}x^{n+2} - 5x\sum_{n=0}^{\infty} a_{n+1}x^{n+1} + 6x^2\sum_{n=0}^{\infty} a_nx^n = 2x^2\sum_{n=0}^{\infty} x^n.$$

Here we also rewrite the power series on the right-hand side of the equation in a form that will permit us to use what we learned in Section 2 of Chapter 9.

4) Let $f(x) = \sum_{n=0}^{\infty} a_nx^n$ be the generating function for the solution. The equation in step (3) now takes the form

$$(f(x) - a_0 - a_1x) - 5x(f(x) - a_0) + 6x^2f(x) = \frac{2x^2}{1-x},$$

or

$$(f(x) - 3 - 7x) - 5x(f(x) - 3) + 6x^2f(x) = \frac{2x^2}{1-x}.$$

5) Solving for $f(x)$ we have

$$(1-5x+6x^2)f(x) = 3-8x+\frac{2x^2}{1-x} = \frac{3-11x+10x^2}{1-x},$$

from which it follows that

$$f(x) = \frac{3-11x+10x^2}{(1-5x+6x^2)(1-x)} = \frac{(3-5x)(1-2x)}{(1-3x)(1-2x)(1-x)} = \frac{3-5x}{(1-3x)(1-x)}.$$

A partial-fraction decomposition (by hand, or via a computer algebra system) gives us

$$f(x) = \frac{2}{1-3x}+\frac{1}{1-x} = 2\sum_{n=0}^{\infty}(3x)^n+\sum_{n=0}^{\infty}x^n.$$

Consequently, $a_n = 2(3^n)+1$, $n \geq 0$.

We consider a third example, which has a familiar result.

EXAMPLE 10.40

Let $n \in \mathbf{N}$. For $r \geq 0$, let $a(n, r)$ = the number of ways we can select, with repetitions allowed, r objects from a set of n distinct objects.

For $n \geq 1$, let $\{b_1, b_2, \ldots, b_n\}$ be the set of these objects, and consider object b_1. Exactly one of two things can happen.

a) The object b_1 is never selected. Hence the r objects are selected from $\{b_2, \ldots, b_n\}$. This we can do in $a(n-1, r)$ ways.

b) The object b_1 is selected at least once. Then we must select $r-1$ objects from $\{b_1, b_2, \ldots, b_n\}$, so we can continue to select b_1 in addition to the one selection of it we've already made. There are $a(n, r-1)$ ways to accomplish this.

Then $a(n, r) = a(n-1, r)+a(n, r-1)$ because these two cases cover all possibilities and are mutually disjoint.

Let $f_n = \sum_{r=0}^{\infty} a(n, r)x^r$ be the generating function for the sequence $a(n, 0)$, $a(n, 1)$, $a(n, 2), \ldots$. [Here f_n is an abbreviation for $f_n(x)$.] From $a(n, r) = a(n-1, r)+a(n, r-1)$, where $n \geq 1$ and $r \geq 1$, it follows that

$$a(n, r)x^r = a(n-1, r)x^r + a(n, r-1)x^r \quad \text{and}$$

$$\sum_{r=1}^{\infty} a(n, r)x^r = \sum_{r=1}^{\infty} a(n-1, r)x^r + \sum_{r=1}^{\infty} a(n, r-1)x^r.$$

Realizing that $a(n, 0) = 1$ for $n \geq 0$ and $a(0, r) = 0$ for $r > 0$, we write

$$f_n - a(n, 0) = f_{n-1} - a(n-1, 0) + x\sum_{r=1}^{\infty} a(n, r-1)x^{r-1},$$

so $f_n - 1 = f_{n-1} - 1 + xf_n$. Therefore, $f_n - xf_n = f_{n-1}$, or $f_n = f_{n-1}/(1-x)$.

If $n = 5$, for example, then

$$f_5 = \frac{f_4}{(1-x)} = \frac{1}{(1-x)}\cdot\frac{f_3}{(1-x)} = \frac{f_3}{(1-x)^2} = \frac{f_2}{(1-x)^3} = \frac{f_1}{(1-x)^4}$$
$$= \frac{f_0}{(1-x)^5} = \frac{1}{(1-x)^5},$$

since $f_0 = a(0, 0)+a(0, 1)x+a(0, 2)x^2+\cdots = 1+0+0+\cdots$.

In general, $f_n = 1/(1-x)^n = (1-x)^{-n}$, so $a(n, r)$ is the coefficient of x^r in $(1-x)^{-n}$, which is $\binom{-n}{r}(-1)^r = \binom{n+r-1}{r}$.

[Here we dealt with a recurrence relation for $a(n, r)$, a discrete function of the two (integer) variables $n, r \geq 0$.]

Our last example shows how generating functions may be used to solve a system of recurrence relations.

EXAMPLE 10.41

This example provides an approximate model for the propagation of high- and low-energy neutrons as they strike the nuclei of fissionable material (such as uranium) and are absorbed. Here we deal with a fast reactor where there is no moderator (such as water). (In reality, all the neutrons have fairly high energy and there are not just two energy levels. There is a continuous spectrum of energy levels, and these neutrons at the upper end of the spectrum are called the high-energy neutrons. The higher-energy neutrons tend to produce more new neutrons than the lower-energy ones.)

Consider the reactor at time 0 and suppose one high-energy neutron is injected into the system. During each time interval thereafter (about 1 microsecond, or 10^{-6} second) the following events occur.

a) When a high-energy neutron interacts with a nucleus (of fissionable material), upon absorption this results (one microsecond later) in two new high-energy neutrons and one low-energy one.

b) For interactions involving a low-energy neutron, only one neutron of each energy level is produced.

Assuming that all free neutrons interact with nuclei one microsecond after their creation, find functions of n such that

$$a_n = \text{the number of high-energy neutrons,}$$
$$b_n = \text{the number of low-energy neutrons,}$$

in the reactor after n microseconds, $n \geq 0$.

Here we have $a_0 = 1$, $b_0 = 0$ and the *system* of recurrence relations

$$a_{n+1} = 2a_n + b_n \tag{3}$$
$$b_{n+1} = a_n + b_n. \tag{4}$$

Let $f(x) = \sum_{n=0}^{\infty} a_n x^n$, $g(x) = \sum_{n=0}^{\infty} b_n x^n$ be the generating functions for the sequences $\{a_n | n \geq 0\}$, $\{b_n | n \geq 0\}$, respectively. From Eqs. (3) and (4), when $n \geq 0$

$$a_{n+1}x^{n+1} = 2a_n x^{n+1} + b_n x^{n+1} \tag{3$'$}$$
$$b_{n+1}x^{n+1} = a_n x^{n+1} + b_n x^{n+1}. \tag{4$'$}$$

Summing Eq. (3)′ over all $n \geq 0$, we have

$$\sum_{n=0}^{\infty} a_{n+1}x^{n+1} = 2x \sum_{n=0}^{\infty} a_n x^n + x \sum_{n=0}^{\infty} b_n x^n. \tag{3$''$}$$

In similar fashion, Eq. (4)′ yields

$$\sum_{n=0}^{\infty} b_{n+1}x^{n+1} = x \sum_{n=0}^{\infty} a_n x^n + x \sum_{n=0}^{\infty} b_n x^n. \tag{4$''$}$$

Introducing the generating functions at this point, we get

$$f(x) - a_0 = 2xf(x) + xg(x) \tag{3}''$$

$$g(x) - b_0 = xf(x) + xg(x), \tag{4}''$$

a system of equations relating the generating functions. Solving this system, we find that

$$f(x) = \frac{1-x}{x^2-3x+1} = \left(\frac{5+\sqrt{5}}{10}\right)\left(\frac{1}{\gamma - x}\right) + \left(\frac{5-\sqrt{5}}{10}\right)\left(\frac{1}{\delta - x}\right) \quad \text{and}$$

$$g(x) = \frac{x}{x^2-3x+1} = \left(\frac{-5-3\sqrt{5}}{10}\right)\left(\frac{1}{\gamma - x}\right) + \left(\frac{-5+3\sqrt{5}}{10}\right)\left(\frac{1}{\delta - x}\right),$$

where

$$\gamma = \frac{3+\sqrt{5}}{2}, \qquad \delta = \frac{3-\sqrt{5}}{2}.$$

Consequently,

$$a_n = \left(\frac{5+\sqrt{5}}{10}\right)\left(\frac{3-\sqrt{5}}{2}\right)^{n+1} + \left(\frac{5-\sqrt{5}}{10}\right)\left(\frac{3+\sqrt{5}}{2}\right)^{n+1} \quad \text{and}$$

$$b_n = \left(\frac{-5-3\sqrt{5}}{10}\right)\left(\frac{3-\sqrt{5}}{2}\right)^{n+1} + \left(\frac{-5+3\sqrt{5}}{10}\right)\left(\frac{3+\sqrt{5}}{2}\right)^{n+1}, \qquad n \geq 0.$$

EXERCISES 10.4

1. Solve the following recurrence relations by the method of generating functions.

a) $a_{n+1} - a_n = 3^n, \quad n \geq 0, \quad a_0 = 1$

b) $a_{n+1} - a_n = n^2, \quad n \geq 0, \quad a_0 = 1$

c) $a_{n+2} - 3a_{n+1} + 2a_n = 0, \quad n \geq 0, \quad a_0 = 1, \quad a_1 = 6$

d) $a_{n+2} - 2a_{n+1} + a_n = 2^n, \quad n \geq 0, \quad a_0 = 1, \quad a_1 = 2$

2. For n distinct objects, let $a(n, r)$ denote the number of ways we can select, without repetition, r of the n objects when $0 \leq r \leq n$. Here $a(n, r) = 0$ when $r > n$. Use the recurrence relation $a(n, r) = a(n-1, r-1) + a(n-1, r)$, where $n \geq 1$ and $r \geq 1$, to show that $f(x) = (1+x)^n$ generates $a(n, r)$, $r \geq 0$.

3. Solve the following systems of recurrence relations.

a) $a_{n+1} = -2a_n - 4b_n$
$b_{n+1} = 4a_n + 6b_n$
$n \geq 0, \quad a_0 = 1, \quad b_0 = 0$

b) $a_{n+1} = 2a_n - b_n + 2$
$b_{n+1} = -a_n + 2b_n - 1$
$n \geq 0, \quad a_0 = 0, \quad b_0 = 1$

10.5 A Special Kind of Nonlinear Recurrence Relation (Optional)

Thus far our study of recurrence relations has dealt with linear relations with constant coefficients. The study of nonlinear recurrence relations and of relations with variable coefficients is not a topic we shall pursue except for one special nonlinear relation that lends itself to the method of generating functions.

We shall develop the method in a counting problem on data structures. Before doing so, however, we first observe that if $f(x) = \sum_{i=0}^{\infty} a_i x^i$ is the generating function for $a_0, a_1, a_2, \ldots$, then $[f(x)]^2$ generates $a_0a_0, a_0a_1 + a_1a_0, a_0a_2 + a_1a_1 + a_2a_0, \ldots,$

$a_0a_n + a_1a_{n-1} + a_2a_{n-2} + \cdots + a_{n-1}a_1 + a_na_0, \ldots,$ the convolution of the sequence $a_0, a_1, a_2, \ldots,$ with itself.

EXAMPLE 10.42

In Sections 3.4 and 5.1, we encountered the idea of a tree diagram. In general, a *tree* is an undirected graph that is connected and has no loops or cycles. Here we examine rooted binary trees.

In Fig. 10.17 we see two such trees, where the circled vertex denotes the *root*. These trees are called *binary* because from each vertex there are at most two edges (called *branches*) descending (since a rooted tree is a directed graph) from that vertex.

In particular, these rooted binary trees are *ordered* in the sense that a left branch descending from a vertex is considered different from a right branch descending from that vertex. For the case of three vertices, the five possible ordered rooted binary trees are shown in Fig. 10.18. (If no attention were paid to order, then the last four rooted trees would be the same structure.)

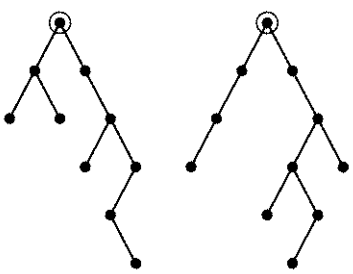


Figure 10.17

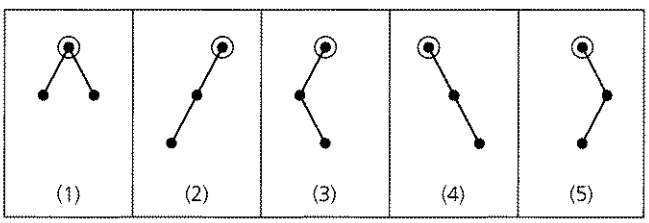


Figure 10.18

Our objective is to count, for $n \geq 0$, the number b_n of rooted ordered binary trees on n vertices. Assuming that we know the values of b_i for $0 \leq i \leq n$, in order to obtain b_{n+1} we select one vertex as the root and note, as in Fig. 10.19, that the substructures descending on the left and right of the root are smaller (rooted ordered binary) trees whose total number of vertices is n. These smaller trees are called *subtrees* of the given tree. Among these possible subtrees is the empty subtree, of which there is only 1 ($= b_0$).

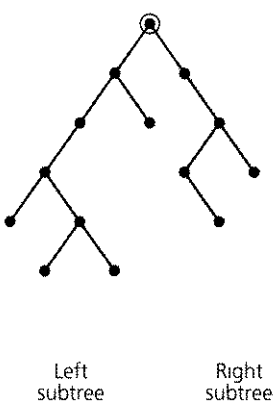


Figure 10.19

Now consider how the n vertices in these two subtrees can be divided up.

(1) 0 vertices on the left, n vertices on the right. This results in $b_0 b_n$ overall substructures to be counted in b_{n+1}.

(2) 1 vertex on the left, $n-1$ vertices on the right, yielding $b_1 b_{n-1}$ rooted ordered binary trees on $n+1$ vertices.

. . . . . .

($i+1$) i vertices on the left, $n-i$ on the right, for a count of $b_i b_{n-i}$ toward b_{n+1}.

. . . . . .

($n+1$) n vertices on the left and none on the right, contributing $b_n b_0$ of the trees.

Hence, for all $n \geq 0$,

$$b_{n+1} = b_0 b_n + b_1 b_{n-1} + b_2 b_{n-2} + \cdots + b_{n-1} b_1 + b_n b_0,$$

and

$$\sum_{n=0}^{\infty} b_{n+1} x^{n+1} = \sum_{n=0}^{\infty} (b_0 b_n + b_1 b_{n-1} + \cdots + b_{n-1} b_1 + b_n b_0) x^{n+1}. \tag{1}$$

Now let $f(x) = \sum_{n=0}^{\infty} b_n x^n$ be the generating function for $b_0, b_1, b_2, \ldots$. We rewrite Eq. (1) as

$$(f(x) - b_0) = x \sum_{n=0}^{\infty} (b_0 b_n + b_1 b_{n-1} + \cdots + b_n b_0) x^n = x[f(x)]^2.$$

This brings us to the quadratic [in $f(x)$]

$$x[f(x)]^2 - f(x) + 1 = 0, \quad \text{so} \quad f(x) = [1 \pm \sqrt{1-4x}]/(2x).$$

But $\sqrt{1-4x} = (1-4x)^{1/2} = \binom{1/2}{0} + \binom{1/2}{1}(-4x) + \binom{1/2}{2}(-4x)^2 + \cdots$, where the coefficient of x^n, $n \geq 1$, is

$$\begin{aligned}
\binom{1/2}{n}(-4)^n &= \frac{(1/2)((1/2)-1)((1/2)-2)\cdots((1/2)-n+1)}{n!}(-4)^n \\
&= (-1)^{n-1}\frac{(1/2)(1/2)(3/2)\cdots((2n-3)/2)}{n!}(-4)^n \\
&= \frac{(-1)2^n(1)(3)\cdots(2n-3)}{n!} \\
&= \frac{(-1)2^n(n!)(1)(3)\cdots(2n-3)(2n-1)}{(n!)(n!)(2n-1)} \\
&= \frac{(-1)(2)(4)\cdots(2n)(1)(3)\cdots(2n-1)}{(2n-1)(n!)(n!)} = \frac{(-1)}{(2n-1)}\binom{2n}{n}.
\end{aligned}$$

In $f(x)$ we select the negative radical; otherwise, we would have negative values for the b_n's. Then

$$f(x) = \frac{1}{2x}\left[1 - \left[1 - \sum_{n=1}^{\infty} \frac{1}{(2n-1)}\binom{2n}{n} x^n\right]\right],$$

and b_n, the coefficient of x^n in $f(x)$, is half the coefficient of x^{n+1} in

$$\sum_{n=1}^{\infty} \frac{1}{(2n-1)}\binom{2n}{n} x^n.$$

So

$$b_n = \frac{1}{2}\left[\frac{1}{2(n+1)-1}\right]\binom{2(n+1)}{n+1} = \frac{(2n)!}{(n+1)!(n!)} = \frac{1}{(n+1)}\binom{2n}{n}.$$

The numbers b_n are called the *Catalan numbers* — the same sequence of numbers we encountered in Section 1.5. As we mentioned earlier (following Example 1.42), these numbers are named after the Belgian mathematician Eugène Charles Catalan (1814–1894), who used them in determining the number of ways to parenthesize the expression $x_1x_2x_3 \cdots x_n$. The first nine Catalan numbers are $b_0 = 1$, $b_1 = 1$, $b_2 = 2$, $b_3 = 5$, $b_4 = 14$, $b_5 = 42$, $b_6 = 132$, $b_7 = 429$, and $b_8 = 1430$.

We continue now with a second application of the Catalan numbers. This is based on an example given by Shimon Even. (See page 86 of reference [6].)

EXAMPLE 10.43

An important data structure that arises in computer science is the *stack*. This structure allows the storage of data items according to the following restrictions.

1) All insertions take place at *one* end of the structure. This is called the *top* of the stack, and the insertion process is referred to as the *push* procedure.
2) All deletions from the (nonempty) stack also take place from the top. We call the deletion process the *pop* procedure.

Since the *last* item inserted *in* this structure is the *first* item that can then be popped *out* of it, the stack is often referred to as a "last-in-first-out" (LIFO) structure.

Intuitive models for this data structure include a pile of poker chips on a table, a stack of trays in a cafeteria, and the discard pile used in playing certain card games. In all three of these cases, we can only (1) insert a new entry at the top of the pile or stack or (2) take (delete) the entry at the top of the (nonempty) pile or stack.

Here we shall use this data structure, with its push and pop procedures, to help us permute the (ordered) list $1, 2, 3, \ldots, n$, for $n \in \mathbf{Z}^+$. The diagram in Fig. 10.20 shows how each integer of the input $1, 2, 3, \ldots, n$ must be pushed onto the top of the stack in the order given. However, we may pop an entry from the top of the (nonempty) stack at any time. But once an entry is popped from the stack, it may not be returned to either the top of the stack or the input left to be pushed onto the stack. The process continues until no entry is left in the stack. Thus the ordered sequence of elements popped from the stack determines a permutation of $1, 2, 3, \ldots, n$.

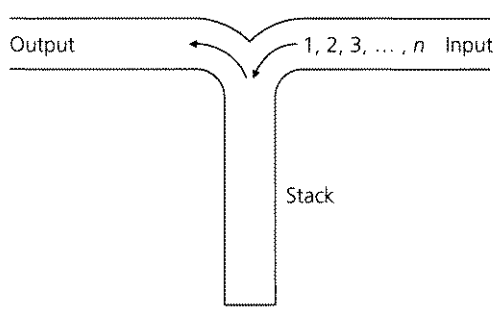


Figure 10.20

If $n = 1$, our input list consists of only the integer 1. We insert 1 at the top of the (empty) stack and then pop it out. This results in the permutation 1.

For $n = 2$, there are two permutations possible for 1, 2, and we can get both of them using the stack.

1) To get 1, 2 we place 1 at the top of the (empty) stack and then pop it. Then 2 is placed at the top of the (empty) stack and it is popped.
2) The permutation 2, 1 is obtained when 1 is placed at the top of the (empty) stack and 2 is then pushed onto the top of this (nonempty) stack. Upon popping first 2 from the top of the stack, and then 1, we obtain 2, 1.

Turning to the case where $n = 3$, we find that we can obtain only five of the $3! = 6$ possible permutations of 1, 2, 3 in this situation. For example, the permutation 2, 3, 1 results when we take the following steps.

- Place 1 at the top of the (empty) stack.
- Push 2 onto the top of the stack (on top of 1).
- Pop 2 from the stack.
- Push 3 onto the top of the stack (on top of 1).
- Pop 3 from the stack.
- Pop 1 from the stack, leaving it empty.

The reason we fail to obtain all six permutations of 1, 2, 3 is that we cannot generate the permutation 3, 1, 2 using the stack. For in order to have 3 in the first position of the permutation, we must build the stack by first pushing 1 onto the (empty) stack, then pushing 2 onto the top of the stack (on top of 1), and finally pushing 3 onto the stack (on top of 2). After 3 is popped from the top of the stack, we get 3 as the first number in our permutation. But with 2 now at the top of the stack, we cannot pop 1 until after 2 has been popped, so the permutation 3, 1, 2 cannot be generated.

When $n = 4$, there are 14 permutations of the (ordered) list 1, 2, 3, 4 that can be generated by the stack method. We list them in the four columns of Table 10.4 according to the location of 1 in the permutation.

Table 10.4

1, 2, 3, 4	2, 1, 3, 4	2, 3, 1, 4	2, 3, 4, 1
1, 2, 4, 3	2, 1, 4, 3	3, 2, 1, 4	2, 4, 3, 1
1, 3, 2, 4			3, 2, 4, 1
1, 3, 4, 2			3, 4, 2, 1
1, 4, 3, 2			4, 3, 2, 1

1) There are five permutations with 1 in the first position, because after 1 is pushed onto and popped from the stack, there are five ways to permute 2, 3, 4 using the stack.
2) When 1 is in the second position, 2 must be in the first position. This is because we pushed 1 onto the (empty) stack, then pushed 2 on top of it and then popped 2 and then 1. There are two permutations in column 2, because 3, 4 can be permuted in two ways on the stack.

3) For column 3 we have 1 in position three. We note that the only numbers that can precede it are 2 and 3, which can be permuted on the stack (with 1 on the bottom) in two ways. Then 1 is popped, and we push 4 onto the (empty) stack and then pop it.

4) In the last column we obtain five permutations: After we push 1 onto the top of the (empty) stack, there are five ways to permute 2, 3, 4 using the stack (with 1 on the bottom). Then 1 is popped from the stack to complete the permutation.

On the basis of these observations, for $1 \leq i \leq 4$, let a_i count the number of ways to permute the integers $1, 2, 3, \ldots, i$ (or any list of i consecutive integers) using the stack. Also, we define $a_0 = 1$ since there is only one way to permute nothing, using the stack. Then

$$a_4 = a_0a_3 + a_1a_2 + a_2a_1 + a_3a_0,$$

where

a) Each summand a_ja_k satisfies $j + k = 3$.

b) The subscript j tells us that there are j integers to the left of 1 in the permutation—in particular, for $j \geq 1$, these are the integers from 2 to $j + 1$, inclusive.

c) The subscript k indicates that there are k integers to the right of 1 in the permutation—for $k \geq 1$, these are the integers from $4 - (k - 1)$ to 4.

This permutation problem can now be generalized to any $n \in \mathbf{N}$, so that

$$a_{n+1} = a_0a_n + a_1a_{n-1} + a_2a_{n-2} + \cdots + a_{n-1}a_1 + a_na_0,$$

with $a_0 = 1$. From the result in Example 10.42 we know that

$$a_n = \frac{1}{(n+1)}\binom{2n}{n}.$$

Now let us make one final observation about the permutations in Table 10.4. Consider, for example, the permutation 3, 2, 4, 1. How did this permutation come about? First 1 is pushed onto the empty stack. This is then followed by pushing 2 on top of 1 and then pushing 3 on top of 2. Now 3 is popped from the top of the stack, leaving 2 and 1; then 2 is popped from the top of the stack, leaving just 1. At this point 4 is pushed on top of 1 and then popped, leaving 1 on the stack. Finally, 1 is popped from the (top of the) stack, leaving the stack empty. So the permutation 3, 2, 4, 1 comes about from the following sequence of four pushes and four pops:

push, push, push, pop, pop, push, pop, pop.

Now replace each "push" with a "1" and each "pop" with a "0". The result is the sequence

$$1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0.$$

Similarly, the permutation 1, 3, 4, 2 is determined by the sequence

push, pop, push, push, pop, push, pop, pop

and this corresponds with the sequence

$$1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0.$$

In fact, each permutation in Table 10.4 gives rise to a sequence of four 1's and four 0's. But there are $8!/(4!\,4!) = 70$ ways to list four 1's and four 0's. Do these 14 sequences have some special property? Yes! As we go from left to right in each of these sequences, the

number of 1's (pushes) is never exceeded by the number of 0's (pops) [just like in part (b) of Example 1.43 — another situation counted by the Catalan numbers].

Our last example for this section is comparable to Example 10.17. Once again we see that we must guard against trying to obtain a general result without a general argument — no matter what a few special cases might suggest.

EXAMPLE 10.44

Here we start with n *distinct objects* and, for $n \geq 1$, we distribute them among at most n *identical containers*, but we do not allow more than three objects in any container, and we are not concerned about how the objects are arranged within any one container. We let a_n count the number of these distributions, and from Fig. 10.21 we see that

$$a_0 = 1, \qquad a_1 = 1, \qquad a_2 = 2, \qquad a_3 = 5, \quad \text{and} \quad a_4 = 14.$$

It appears that we might have the first five terms in the sequence of Catalan numbers. Unfortunately, the pattern breaks down and we find, for example, that

$$a_5 = 46 \neq 42 \text{ (the sixth Catalan number)} \quad \text{and}$$
$$a_6 = 166 \neq 132 \text{ (the seventh Catalan number).}$$

(The distributions in this example were studied by F. L. Miksa, L. Moser, and M. Wyman in reference [22].)

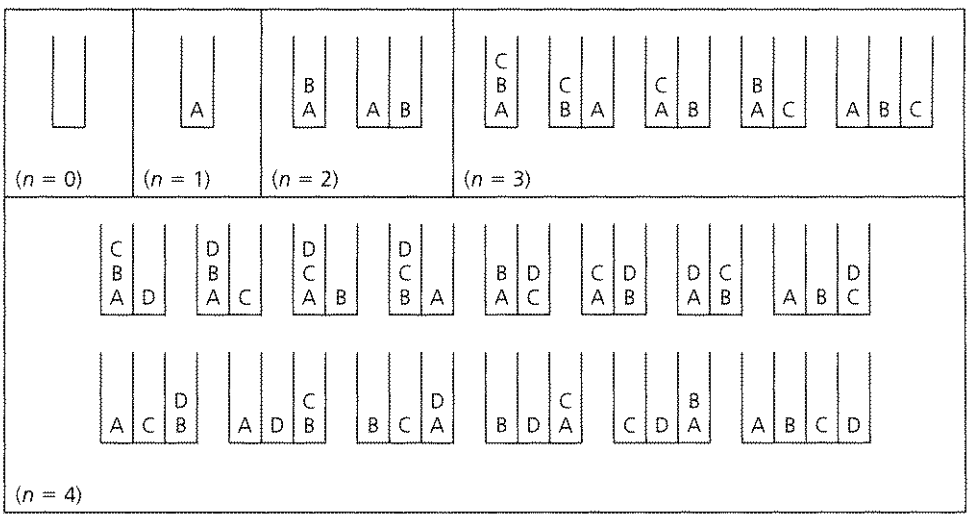


Figure 10.21

Other examples that involve the Catalan numbers can be found in the chapter references.

EXERCISES 10.5

1. For the rooted ordered binary trees of Example 10.42, calculate b_4 and draw all of these four-vertex structures.

2. Verify that for all $n \geq 0$,

$$\frac{1}{2}\left(\frac{1}{2n+1}\right)\binom{2n+2}{n+1} = \left(\frac{1}{n+1}\right)\binom{2n}{n}.$$

3. Show that for all $n \geq 2$,

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

4. Which of the following permutations of 1, 2, 3, 4, 5, 6, 7, 8 can be obtained using the stack (of Example 10.43)?

a) 4, 2, 3, 1, 5, 6, 7, 8 **b)** 5, 4, 3, 6, 2, 1, 8, 7

c) 4, 5, 3, 2, 1, 8, 6, 7 **d)** 3, 4, 2, 1, 7, 6, 8, 5

5. Suppose that the integers 1, 2, 3, 4, 5, 6, 7, 8 are permuted using the stack (of Example 10.43). (a) How many permutations are possible? (b) How many permutations have 1 in position 4 and 5 in position 8? (c) How many permutations have 1 in position 6? (d) How many permutations start with 321?

6. This exercise deals with a problem that was first proposed by Leonard Euler. The problem examines a given convex polygon of n (≥ 3) sides — that is, a polygon of n sides that satisfies the property: For all points P_1, P_2 within the interior of the polygon, the line segment joining P_1 and P_2 also lies within the interior of the polygon. Given a convex polygon of n sides, Euler wanted to count the number of ways the interior of the polygon could be triangulated (subdivided into triangles) by drawing diagonals that do not intersect.

For a convex polygon of $n \geq 3$ sides, let t_n count the number of ways the interior of the polygon can be triangulated by drawing nonintersecting diagonals.

a) Define $t_2 = 1$ and verify that

$$t_{n+1} = t_2 t_n + t_3 t_{n-1} + \cdots + t_{n-1} t_3 + t_n t_2.$$

b) Express t_n as a function of n.

7. In Fig. 10.22 we have two of the five ways in which we can triangulate the interior of a convex pentagon with no intersecting diagonals. Here we have labeled four of the sides — with the letters a, b, c, d — as well as the five vertices. In part (i) we use the labels on sides a and b to give us the label ab on the diagonal connecting vertices 2 and 4. This is because this diagonal (labeled ab), together with the sides a and b, provides us with one of the interior triangles for this triangulation of the convex pentagon. Then the diagonal ab and the side c give rise to the label $(ab)c$ on the diagonal determined by vertices 2 and 5 — and the sides labeled ab, c and $(ab)c$ provide a second interior triangle for this triangulation. Continuing in this way, we label the base edge connecting vertices 1 and 2 with $((ab)c)d$ — one of the five ways we can introduce parentheses in order to obtain the three products (of two numbers at a time) needed to compute $abcd$. The triangulation in part (ii) of the figure corresponds with the parenthesized product $(ab)(cd)$.

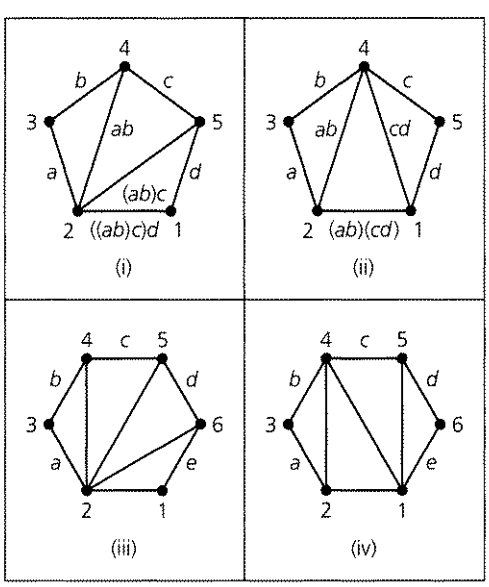


Figure 10.22

a) Determine the parenthesized product involving a, b, c, d for the other three triangulations of the convex pentagon.

b) Find the parenthesized product for each of the triangulated convex hexagons in parts (iii) and (iv) of Fig. 10.22

[From part (a) we learn that there are five ways to parenthesize the expression $abcd$ (and five ways to triangulate a convex pentagon). Part (b) shows us two of the 14 ways one can introduce parentheses for the expression $abcde$ (and triangulate a convex hexagon). In general, there are $\frac{1}{n+1}\binom{2n}{n}$ ways to parenthesize the expression $x_1 x_2 x_3 \cdots x_{n-1} x_n x_{n+1}$. It was in solving this problem that Eugène Charles Catalan discovered the sequence that now bears his name.]

8. For $n \geq 0$,

$$b_n = \left(\frac{1}{n+1}\right)\binom{2n}{n}$$

is the nth Catalan number.

a) Show that for all $n \geq 0$,

$$b_{n+1} = \frac{2(2n+1)}{(n+2)} b_n.$$

b) Use the result of part (a) to write a computer program (or develop an algorithm) that calculates the first 15 Catalan numbers.

9. For $n \geq 0$, evenly distribute $2n$ points on the circumference of a circle, and label these points cyclically with the integers $1, 2, 3, \ldots, 2n$. Let a_n be the number of ways in which these $2n$ points can be paired off as n chords where no two chords intersect. (The case for $n = 3$ is shown in Fig. 10.23.) Find and solve a recurrence relation for a_n, $n \geq 0$.

10. For $n \in \mathbf{N}$, consider all paths from $(0, 0)$ to $(2n, 0)$ using the moves N: $(x, y) \to (x+1, y+1)$ and S: $(x, y) \to (x+1, y-1)$, where any such path can never fall below the x-axis. The five paths (generally called *mountain ranges*) for $n = 3$ are shown in Fig. 10.24. How many mountain ranges are there for each $n \in \mathbf{N}$? (Verify your claim!)

11. For $n \in \mathbf{Z}^+$, let $f: \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, where f is monotone increasing [that is, $1 \leq i < j \leq n \Rightarrow f(i) \leq f(j)$] and $f(i) \geq i$ for all $1 \leq i \leq n$. (a) Determine the five monotone increasing functions $f: \{1, 2, 3\} \to \{1, 2, 3\}$, where $f(i) \geq i$ for all $1 \leq i \leq 3$. (b) Use the graphs of the functions from part (a) to set up a one-to-one correspondence with the paths from $(0, 0)$ to $(3, 3)$ using the moves R: $(x, y) \to (x+1, y)$, U: $(x, y) \to (x, y+1)$, where each such path never falls below the line $y = x$. (The reader may

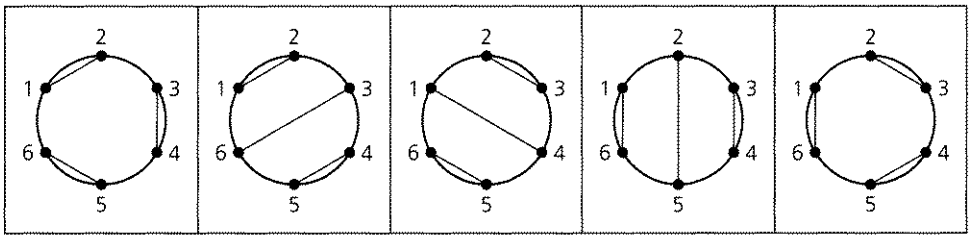


Figure 10.23

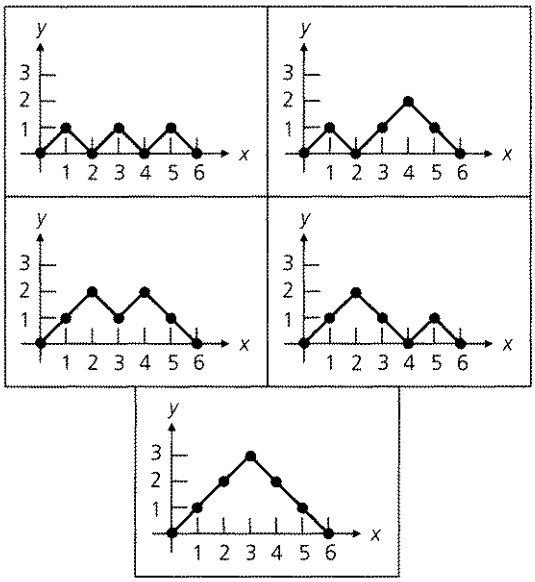


Figure 10.24

wish to check Exercise 3 for Section 1.5.) (c) If the paths in part (b) are rotated clockwise through 45°, what results do we find? (d) How many monotone increasing functions f have domain and codomain equal to $\{1, 2, 3, \ldots, n\}$, for $n \in \mathbf{Z}^+$, and satisfy $f(i) \geq i$ for all $1 \leq i \leq n$?

12. For $n \in \mathbf{Z}^+$, let $g: \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, where $g(i) \leq i$ for all $1 \leq i \leq n$. (a) Determine the five functions $g: \{1, 2, 3\} \to \{1, 2, 3\}$ where $g(i) \leq i$ for all $1 \leq i \leq 3$. (b) Set up a one-to-one correspondence between the functions in part (a) here and those in part (a) of the previous exercise. [You want a one-to-one correspondence that will generalize when you examine the functions $f, g: \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, $n \in \mathbf{Z}^+$, where $f(i) \geq i$ and $g(i) \leq i$ for all $1 \leq i \leq n$.] (c) How many functions g have domain and codomain equal to $\{1, 2, 3, \ldots, n\}$, for $n \in \mathbf{Z}^+$, and satisfy $g(i) \leq i$ for all $1 \leq i \leq n$?

13. For $n \in \mathbf{N}$, consider the arrangements of pennies built on a contiguous row of n pennies. Each penny that is not in the bottom row (of n pennies) rests upon the two pennies below it, and there is no concern about whether heads or tails appears. The situation for $n = 3$ is shown in Fig. 10.25. How many such arrangements are there for a contiguous row of n pennies, $n \in \mathbf{N}$?

14. For $n \in \mathbf{N}$, let s_n count the number of ways one can travel from $(0, 0)$ to (n, n) using the moves R: $(x, y) \to (x + 1, y)$, U: $(x, y) \to (x, y + 1)$, D: $(x, y) \to (x + 1, y + 1)$, where the path can never rise above the line $y = x$. (a) Determine s_2. (b) How is s_2 related to the Catalan numbers b_0, b_1, b_2? (c) How is s_3 related to b_0, b_1, b_2, b_3? What is s_3? (d) For $n \in \mathbf{N}$, how is s_n related to $b_0, b_1, b_2, \ldots, b_n$? (The numbers $s_0, s_1, s_2, \ldots$ are known as the *Schröder numbers*.)

15. A one-to-one function $f: \{1, 2, 3, \ldots, n\} \to \{1, 2, 3, \ldots, n\}$ is often called a *permutation*. Such a permutation is termed a *rise/fall* permutation when $f(1) < f(2)$, $f(2) > f(3)$, $f(3) < f(4)$, ... For example, if $n = 4$ the five permutations 1324 (where $f(1) = 1$, $f(2) = 3$, $f(3) = 2$, $f(4) = 4$), 1423, 2314, 2413, and 3412 are the rise/fall permutations (for 1, 2, 3, 4). This we denote by writing $E_4 = 5$, where, in general, E_n counts the number of rise/fall permutations for $1, 2, 3, \ldots, n$. The numbers $E_0, E_1, E_2, E_3, \ldots$ are called the *Euler numbers* (not to be confused with the Eulerian numbers in Example 4.21). We define $E_0 = 1$ and find that $E_1 = 1$, $E_2 = 1$.

a) Find the rise/fall permutations for 1, 2, 3. What is E_3?

b) Find the rise/fall permutations for 1, 2, 3, 4, 5. What is E_5?

c) Explain why in each rise/fall permutation of $1, 2, 3, \ldots n$, we find n at position $2i$ for some $1 \leq i \leq \lfloor n/2 \rfloor$, if $n > 1$.

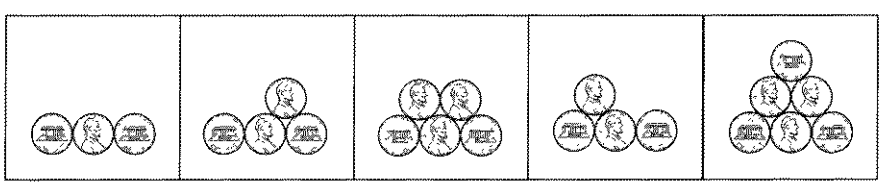


Figure 10.25

d) For $n \geq 2$, show that

$$E_n = \sum_{i=1}^{\lfloor n/2 \rfloor} \binom{n-1}{2i-1} E_{2i-1} E_{n-2i}, \quad E_0 = E_1 = 1.$$

e) Where do we find 1 in a rise/fall permutation of $1, 2, 3, \ldots, n$?

f) For $n \geq 1$, show that

$$E_n = \sum_{i=0}^{\lfloor (n-1)/2 \rfloor} \binom{n-1}{2i} E_{2i} E_{n-2i-1}, \quad E_0 = 1.$$

g) Prove that for $n \geq 2$,

$$E_n = \left(\frac{1}{2}\right) \sum_{i=0}^{n-1} \binom{n-1}{i} E_i E_{n-i-1}, \quad E_0 = E_1 = 1.$$

h) Use the result in part (g) to find E_6 and E_7.

i) Find the Maclaurin series expansion for $f(x) = \sec x + \tan x$. Conjecture (no proof required) the sequence for which this is the exponential generating function.

10.6 Divide-and-Conquer Algorithms (Optional)†

One of the most important and widely applicable types of efficient algorithms is based on a *divide-and-conquer* approach. Here the strategy, in general, is to solve a given problem of size n ($n \in \mathbf{Z}^+$) by

1) Solving the problem for a small value of n directly (this provides an initial condition for the resulting recurrence relation).
2) Breaking the general problem of size n into a smaller problems of the same type and (approximately) the same size—either $\lceil n/b \rceil$ or $\lfloor n/b \rfloor$,‡ where $a, b \in \mathbf{Z}^+$ with $1 \leq a < n$ and $1 < b < n$.

Then we solve the a smaller problems and use their solutions to construct a solution for the original problem of size n. We shall be especially interested in cases where n is a power of b, and $b = 2$.

We shall study those divide-and-conquer algorithms where

1) The time to solve the initial problem of size $n = 1$ is a constant $c \geq 0$, and
2) The time to break the given problem of size n into a smaller (similar) problems, together with the time to combine the solutions of these smaller problems to get a solution for the given problem, is $h(n)$, a function of n.

Our concern here will actually be with the time-complexity function $f(n)$ for these algorithms. Consequently, we shall use the notation $f(n)$ here, instead of the subscripted notation a_n that we used in the earlier sections of this chapter.

The conditions that have now been stated lead to the following recurrence relation.

$$f(1) = c,$$
$$f(n) = af(n/b) + h(n), \qquad \text{for } n = b^k, \qquad k \geq 1.$$

We note that the domain of f is $\{1, b, b^2, b^3, \ldots\} = \{b^i \mid i \in \mathbf{N}\} \subset \mathbf{Z}^+$.

---

†The material in this section may be skipped with no loss of continuity. It will be used in Section 12.3 to determine the time-complexity function for the merge sort algorithm. However, the result there will also be obtained for a special case of the merge sort by another method that does not use the material developed in this section.

‡For each $x \in \mathbf{R}$, recall that $\lceil x \rceil$ denotes the *ceiling* of x and $\lfloor x \rfloor$ the *floor* of x, or *greatest integer* in x, where

a) $\lfloor x \rfloor = \lceil x \rceil = x$, for $x \in \mathbf{Z}$.
b) $\lfloor x \rfloor$ = the integer directly to the left of x, for $x \in \mathbf{R} - \mathbf{Z}$.
c) $\lceil x \rceil$ = the integer directly to the right of x, for $x \in \mathbf{R} - \mathbf{Z}$.

In our first result, the solution of this recurrence relation is derived for the case where $h(n)$ is the constant c.

THEOREM 10.1 Let $a, b, c \in \mathbf{Z}^+$ with $b \geq 2$, and let $f: \mathbf{Z}^+ \to \mathbf{R}$. If

$$f(1) = c, \quad \text{and}$$
$$f(n) = af(n/b) + c, \qquad \text{for } n = b^k, \qquad k \geq 1,$$

then for all $n = 1, b, b^2, b^3, \ldots,$

1) $f(n) = c(\log_b n + 1)$, when $a = 1$, and

2) $f(n) = \dfrac{c(an^{\log_b a} - 1)}{a - 1}$, when $a \geq 2$.

Proof: For $k \geq 1$ and $n = b^k$, we write the following system of k equations. [Starting with the second equation, we obtain each of these equations from its immediate predecessor by (i) replacing each occurrence of n in the prior equation by n/b and (ii) multiplying the resulting equation in (i) by a.]

$$\begin{aligned}
f(n) &= af(n/b) + c \\
af(n/b) &= a^2 f(n/b^2) + ac \\
a^2 f(n/b^2) &= a^3 f(n/b^3) + a^2 c \\
\vdots \qquad & \quad \vdots \qquad\qquad \vdots \\
a^{k-2} f(n/b^{k-2}) &= a^{k-1} f(n/b^{k-1}) + a^{k-2} c \\
a^{k-1} f(n/b^{k-1}) &= a^k f(n/b^k) + a^{k-1} c
\end{aligned}$$

We see that each of the terms $af(n/b), a^2 f(n/b^2), \ldots, a^{k-1} f(n/b^{k-1})$ occurs one time as a summand on both the left-hand and right-hand sides of these equations. Therefore, upon adding both sides of the k equations and canceling these common summands, we obtain

$$f(n) = a^k f(n/b^k) + [c + ac + a^2 c + \cdots + a^{k-1} c].$$

Since $n = b^k$ and $f(1) = c$, we have

$$\begin{aligned}
f(n) &= a^k f(1) + c[1 + a + a^2 + \cdots + a^{k-1}] \\
&= c[1 + a + a^2 + \cdots + a^{k-1} + a^k].
\end{aligned}$$

1) If $a = 1$, then $f(n) = c(k + 1)$. But $n = b^k \iff \log_b n = k$, so $f(n) = c(\log_b n + 1)$, for $n \in \{b^i | i \in \mathbf{N}\}$.

2) When $a \geq 2$, then $f(n) = \dfrac{c(1 - a^{k+1})}{1 - a} = \dfrac{c(a^{k+1} - 1)}{a - 1}$, from identity 4 of Table 9.2. Now $n = b^k \iff \log_b n = k$, so

$$a^k = a^{\log_b n} = (b^{\log_b a})^{\log_b n} = (b^{\log_b n})^{\log_b a} = n^{\log_b a},$$

and

$$f(n) = \frac{c(an^{\log_b a} - 1)}{(a - 1)}, \qquad \text{for } n \in \{b^i | i \in \mathbf{N}\}.$$

EXAMPLE 10.45

a) Let $f: \mathbf{Z}^+ \to \mathbf{R}$, where

$$f(1) = 3, \quad \text{and}$$
$$f(n) = f(n/2) + 3, \qquad \text{for } n = 2^k, \qquad k \in \mathbf{Z}^+.$$

So by part (1) of Theorem 10.1, with $c = 3$, $b = 2$, and $a = 1$, it follows that $f(n) = 3(\log_2 n + 1)$ for $n \in \{1, 2, 4, 8, 16, \ldots\}$.

b) Suppose that $g: \mathbf{Z}^+ \to \mathbf{R}$ with

$$g(1) = 7, \quad \text{and}$$
$$g(n) = 4g(n/3) + 7, \qquad \text{for } n = 3^k, \qquad k \in \mathbf{Z}^+.$$

Then with $c = 7$, $b = 3$, and $a = 4$, part (2) of Theorem 10.1 implies that $g(n) = (7/3)(4n^{\log_3 4} - 1)$, when $n \in \{1, 3, 9, 27, 81, \ldots\}$.

c) Finally, consider $h: \mathbf{Z}^+ \to \mathbf{R}$, where

$$h(1) = 5, \quad \text{and}$$
$$h(n) = 7h(n/7) + 5, \qquad \text{for } n = 7^k, \qquad k \in \mathbf{Z}^+.$$

Once again we use part (2) of Theorem 10.1, this time with $a = b = 7$ and $c = 5$. Here we learn that $h(n) = (5/6)(7n^{\log_7 7} - 1) = (5/6)(7n - 1)$ for $n \in \{1, 7, 49, 343, \ldots\}$.

Considering Theorem 10.1, we must unfortunately realize that although we know about f for $n \in \{1, b, b^2, \ldots\}$, we cannot say anything about the value of f for the integers in $\mathbf{Z}^+ - \{1, b, b^2, \ldots\}$. So at this time we are unable to deal with the concept of f as a time-complexity function. To overcome this, we now generalize Definition 5.23, wherein the idea of function dominance was first introduced.

Definition 10.1

Let $f, g: \mathbf{Z}^+ \to \mathbf{R}$ with S an infinite subset of $\mathbf{Z}^+$. We say that g *dominates* f *on* S (or f *is dominated by* g *on* S) if there exist constants $m \in \mathbf{R}^+$ and $k \in \mathbf{Z}^+$ such that $|f(n)| \le m|g(n)|$ for all $n \in S$, where $n \ge k$.

Under these conditions we also say that $f \in O(g)$ *on* S.

EXAMPLE 10.46

Let $f: \mathbf{Z}^+ \to \mathbf{R}$ be defined so that

$$f(n) = n, \qquad \text{for } n \in \{1, 3, 5, 7, \ldots\} = S_1,$$
$$f(n) = n^2, \qquad \text{for } n \in \{2, 4, 6, 8, \ldots\} = S_2.$$

Then $f \in O(n)$ on S_1 and $f \in O(n^2)$ on S_2. However, we *cannot* conclude that $f \in O(n)$.

EXAMPLE 10.47

From Example 10.45, it now follows from Definition 10.1 that

a) $f \in O(\log_2 n)$ on $\{2^k | k \in \mathbf{N}\}$ **b)** $g \in O(n^{\log_3 4})$ on $\{3^k | k \in \mathbf{N}\}$

c) $h \in O(n)$ on $\{7^k | k \in \mathbf{N}\}$.

Using Definition 10.1, we now consider the following corollaries for Theorem 10.1. The first is a generalization of the first two results given in Example 10.47.

COROLLARY 10.1 Let $a, b, c \in \mathbf{Z}^+$ with $b \geq 2$, and let $f: \mathbf{Z}^+ \to \mathbf{R}$. If

$$f(1) = c, \quad \text{and}$$
$$f(n) = af(n/b) + c, \qquad \text{for } n = b^k, \qquad k \geq 1,$$

then

1) $f \in O(\log_b n)$ on $\{b^k | k \in \mathbf{N}\}$, when $a = 1$, and
2) $f \in O(n^{\log_b a})$ on $\{b^k | k \in \mathbf{N}\}$, when $a \geq 2$.

Proof: This proof is left as an exercise for the reader.

This second corollary changes the equal signs of Theorem 10.1 to inequalities. As a result, the codomain of f must be restricted from $\mathbf{R}$ to $\mathbf{R}^+ \cup \{0\}$.

COROLLARY 10.2 For $a, b, c \in \mathbf{Z}^+$ with $b \geq 2$, let $f: \mathbf{Z}^+ \to \mathbf{R}^+ \cup \{0\}$. If

$$f(1) \leq c, \quad \text{and}$$
$$f(n) \leq af(n/b) + c, \qquad \text{for } n = b^k, \qquad k \geq 1,$$

then for all $n = 1, b, b^2, b^3, \ldots,$

1) $f \in O(\log_b n)$, when $a = 1$, and
2) $f \in O(n^{\log_b a})$, when $a \geq 2$.

Proof: Consider the function $g: \mathbf{Z}^+ \to \mathbf{R}^+ \cup \{0\}$, where

$$g(1) = c, \quad \text{and}$$
$$g(n) = ag(n/b) + c, \qquad \text{for } n \in \{1, b, b^2, \ldots\}.$$

By Corollary 10.1,

$$g \in O(\log_b n) \quad \text{on} \quad \{b^k | k \in \mathbf{N}\}, \quad \text{when } a = 1, \quad \text{and}$$
$$g \in O(n^{\log_b a}) \quad \text{on} \quad \{b^k | k \in \mathbf{N}\}, \quad \text{when } a \geq 2.$$

We claim that $f(n) \leq g(n)$ for all $n \in \{1, b, b^2, \ldots\}$. To prove our claim, we induct on k where $n = b^k$. If $k = 0$, then $n = b^0 = 1$ and $f(1) \leq c = g(1)$ — so the result is true for this first case. Assuming the result is true for some $t \in \mathbf{N}$, we have $f(n) = f(b^t) \leq g(b^t) = g(n)$, for $n = b^t$. Then for $k = t + 1$ and $n = b^k = b^{t+1}$, we find that

$$f(n) = f(b^{t+1}) \leq af(b^{t+1}/b) + c = af(b^t) + c \leq ag(b^t) + c = g(b^{t+1}) = g(n).$$

Therefore, it follows by the Principle of Mathematical Induction that $f(n) \leq g(n)$ for all $n \in \{1, b, b^2, \ldots\}$. Consequently, $f \in O(g)$ on $\{b^k | k \in \mathbf{N}\}$, and the corollary follows because of our earlier statement about g.

Up to this point, our study of divide-and-conquer algorithms has been predominantly theoretical. It is high time we gave an example in which these ideas can be applied. The following result will confirm one of our earlier examples.

EXAMPLE 10.48

For $n = 1, 2, 4, 8, 16, \ldots$, let $f(n)$ count the number of comparisons needed to find the maximum and minimum elements in a set $S \subset \mathbf{R}$, where $|S| = n$ and the procedure in Example 10.30 is used.

If $n = 1$, then the maximum and minimum elements are the same element. Therefore, no comparisons are necessary and $f(1) = 0$.

If $n > 1$, then $n = 2^k$ for some $k \in \mathbf{Z}^+$, and we partition S as $S_1 \cup S_2$ where $|S_1| = |S_2| = n/2 = 2^{k-1}$. It takes $f(n/2)$ comparisons to find the maximum M_i and the minimum m_i for each set S_i, $i = 1, 2$. For $n \geq 4$, knowing m_1, M_1, m_2, and M_2, we then compare m_1 with m_2 and M_1 and M_2 to determine the minimum and maximum elements in S. Therefore,

$$f(n) = 2f(n/2) + 1, \qquad \text{when } n = 2, \quad \text{and}$$
$$f(n) = 2f(n/2) + 2, \qquad \text{when } n = 4, 8, 16, \ldots.$$

Unfortunately, these results do not provide the hypotheses of Theorem 10.1. However, if we change our equations into the inequalities

$$f(1) \leq 2$$
$$f(n) \leq 2f(n/2) + 2, \qquad \text{for } n = 2^k, \qquad k \geq 1,$$

then by Corollary 10.2 the time-complexity function $f(n)$, measured by the number of comparisons made in this recursive procedure, satisfies $f \in O(n^{\log_2 2}) = O(n)$, for all $n = 1, 2, 4, 8, \ldots$.

We can examine the relationship between this example and Example 10.30 even further. From that earlier result, we know that if $|S| = n = 2^k, k \geq 1$, then the number of comparisons $f(n)$ we need (in the given procedure) to find the maximum and minimum elements in S is $(3/2)(2^k) - 2$. (*Note*: Our statement here replaces the variable n of Example 10.30 by the variable k.)

Since $n = 2^k$, we find that we can now write

$$f(1) = 0$$
$$f(n) = f(2^k) = (3/2)(2^k) - 2 = (3/2)n - 2, \qquad \text{for } n = 2, 4, 8, 16, \ldots.$$

Hence $f \in O(n)$ for $n \in \{2^k | k \in \mathbf{N}\}$, just as we obtained above using Corollary 10.2.

All of our results have required that $n = b^k$, for some $k \in \mathbf{N}$, so it is only natural to ask whether we can do anything in the case where n is allowed to be an arbitrary positive integer. To find out, we introduce the following idea.

Definition 10.2

A function $f: \mathbf{Z}^+ \to \mathbf{R}^+ \cup \{0\}$ is called *monotone increasing* if for all $m, n \in \mathbf{Z}^+, m < n \Rightarrow f(m) \leq f(n)$.

This permits us to consider results for all $n \in \mathbf{Z}^+$ — under certain circumstances.

THEOREM 10.2

Let $f: \mathbf{Z}^+ \to \mathbf{R}^+ \cup \{0\}$ be monotone increasing, and let $g: \mathbf{Z}^+ \to \mathbf{R}$. For $b \in \mathbf{Z}^+, b \geq 2$, suppose that $f \in O(g)$ for all $n \in S = \{b^k | k \in \mathbf{N}\}$. Under these conditions,

a) If $g \in O(\log n)$, then $f \in O(\log n)$.

b) If $g \in O(n \log n)$, then $f \in O(n \log n)$.

c) If $g \in O(n^r)$, then $f \in O(n^r)$, for $r \in \mathbf{R}^+ \cup \{0\}$.

Proof: We shall prove part (a) and leave parts (b) and (c) for the Section Exercises. Before starting, we should note that the base for the logarithms in parts (a) and (b) is any positive real number greater than 1.

Since $f \in O(g)$ on S, and $g \in O(\log n)$, we at least have $f \in O(\log n)$ on S. Therefore, by Definition 10.1, there exist constants $m \in \mathbf{R}^+$ and $s \in \mathbf{Z}^+$ such that $f(n) = |f(n)| \leq m|\log n| = m \log n$ for all $n \in S$, $n \geq s$. We need to find a constant $M \in \mathbf{R}^+$ such that $f(n) \leq M \log n$ for *all* $n \geq s$, not just those $n \in S$.

First let us agree to choose s large enough so that $\log s \geq 1$. Now let $n \in \mathbf{Z}^+$, where $n \geq s$ but $n \notin S$. Then there exists $k \in \mathbf{Z}^+$ such that $s \leq b^k < n < b^{k+1}$. Since f is monotone increasing and positive,

$$\begin{aligned} f(n) \leq f(b^{k+1}) &\leq m \log(b^{k+1}) = m[\log(b^k) + \log b] \\ &= m \log(b^k) + m \log b \\ &< m \log(b^k) + m \log b \log(b^k) \\ &= m(1 + \log b) \log(b^k) \\ &< m(1 + \log b) \log n. \end{aligned}$$

So with $M = m(1 + \log b)$ we find that for all $n \in \mathbf{Z}^+ - S$, if $n \geq s$ then $f(n) < M \log n$. Hence $f(n) \leq M \log n$ for *all* $n \in \mathbf{Z}^+$, where $n \geq s$, and $f \in O(\log n)$.

We shall now use the result of Theorem 10.2 in determining the time-complexity function $f(n)$ for a searching algorithm known as *binary search*.

In Example 5.70 we analyzed an algorithm wherein an array $a_1, a_2, a_3, \ldots, a_n$ of integers was searched for the presence of a particular integer called *key*. At that time the array entries were not given in any particular order, so we simply compared the value of *key* with those of the array elements $a_1, a_2, a_3, \ldots, a_n$. This would not be very efficient, however, if we knew that $a_1 < a_2 < a_3 < \cdots < a_n$. (After all, one does not search a telephone book for the telephone number of a particular person by starting at page 1 and examining every name in succession. The alphabetical ordering of the last names is used to speed up the searching process.) Let us look at a particular example.

EXAMPLE 10.49

Consider the array $a_1, a_2, a_3, \ldots, a_7$ of integers, where $a_1 = 2$, $a_2 = 4$, $a_3 = 5$, $a_4 = 7$, $a_5 = 10$, $a_6 = 17$, and $a_7 = 20$, and let $key = 9$. We search this array as follows:

1) Compare *key* with the entry at the center of the array; here it is $a_4 = 7$. Since $key > a_4$, we now concentrate on the remaining elements in the subarray a_5, a_6, a_7.
2) Now compare *key* with the center element a_6. Since $key = 9 < 17 = a_6$, we now turn to the subarray (of a_5, a_6, a_7) that consists of those elements smaller than a_6. Here this is only the element a_5.
3) Comparing *key* with a_5, we find that $key \neq a_5$, so *key* is not present in the given array $a_1, a_2, a_3, \ldots, a_7$.

From the results of Example 10.49, we make the following observations for a general (ordered) array of integers (or real numbers). Let $a_1, a_2, a_3, \ldots, a_n$ denote the given array,

and let *key* denote the integer (or real number) for which we are searching. Unlike our array in Example 5.70, here

$$a_1 < a_2 < a_3 < \cdots < a_n.$$

1) First we compare the value of *key* with the array entry at or near the center. This entry is $a_{(n+1)/2}$ for n odd or $a_{n/2}$ for n even.

   Whether n is even or odd, the array element subscripted by $c = \lfloor (n+1)/2 \rfloor$ is the center, or near center, element. Note that at this point 1 is the value of the smallest subscript for the array subscripts, whereas n is the value of the largest subscript.

2) If *key* is a_c, we are finished. If not, then

   a) If *key* exceeds a_c, we search (with this dividing process) the subarray $a_{c+1}, a_{c+2}, \ldots, a_n$.

   b) If *key* is smaller than a_c, then the dividing process is applied in searching the subarray $a_1, a_2, \ldots, a_{c-1}$.

The preceding observations have been used in developing the pseudocode procedure in Fig. 10.26. Here the input is an ordered array $a_1, a_2, a_3, \ldots, a_n$ of integers, or real numbers, in ascending order, the positive integer n (for the number of entries in the given array), and the value of the integer variable *key*. If the array elements are integers (real numbers), then *key* should be an integer (real number). The variables s and l are integer variables used for storing the smallest and largest subscripts for the subscripts of the array or subarray being searched. The integer variable c stores the index for the array (subarray) element at, or near, the center of the array (subarray). In general, $c = \lfloor (s+l)/2 \rfloor$. The integer variable *location* stores the subscript of the array entry where *key* is located; the value of *location* is 0 when *key* is not present in the given array.

```
procedure BinarySearch(n: positive integer; key, a1, a2, a3, ..., an: integers)
begin
s := 1   {s is the smallest subscript of the subarray being searched}
l := n   {l is the largest subscript of the subarray being searched}
location := 0
while s ≤ l do
  begin
    c := ⌊(s + l)/2⌋
    if key = ac then
      begin
        location := c
        s := l + 1
      end
    else if key < ac then
      l := c - 1
    else s := c + 1
  end
end
```

Figure 10.26

We want to measure the (worst-case) time complexity for the algorithm implemented in Fig. 10.26. Here $f(n)$ will count the maximum number of comparisons (between *key*

and a_c) needed to determine whether the given number *key* appears in the ordered array $a_1, a_2, a_3, \ldots, a_n$.

- For $n = 1$, *key* is compared to a_1 and $f(1) = 1$.
- When $n = 2$, in the worst case *key* is compared to a_1 and then to a_2, so $f(2) = 2$.
- In the case of $n = 3$, $f(3) = 2$ (in the worst case).
- When $n = 4$, the worst case occurs when *key* is first compared to a_2 and then a binary search of a_3, a_4 follows. Searching a_3, a_4 requires (in the worst case) $f(2)$ comparisons. So $f(4) = 1 + f(2) = 3$.

At this point we see that $f(1) \leq f(2) \leq f(3) \leq f(4)$, and we conjecture that f is a monotone increasing function. To verify this, we shall use the Principle of Mathematical Induction in its alternative form. Here we assume that for all $i, j \in \{1, 2, 3, \ldots, n\}$, $i < j \Rightarrow f(i) \leq f(j)$. Now consider the integer $n + 1$. We have two cases to examine.

1) $n + 1$ is odd: Here we write $n = 2k$ and $n + 1 = 2k + 1$, for some $k \in \mathbf{Z}^+$. In the worst case, $f(n + 1) = f(2k + 1) = 1 + f(k)$, where 1 counts the comparison of *key* with a_{k+1}, and $f(k)$ counts the (maximum) number of comparisons needed in a binary search of the subarray $a_1, a_2, \ldots, a_k$ or the subarray $a_{k+2}, a_{k+3}, \ldots, a_{2k+1}$.

Now $f(n) = f(2k) = 1 + \max\{f(k - 1), f(k)\}$. Since $k - 1, k < n$, by the induction hypothesis we have $f(k - 1) \leq f(k)$, so $f(n) = 1 + f(k) = f(n + 1)$.

2) $n + 1$ is even: At this time we have $n + 1 = 2r$, for some $r \in \mathbf{Z}^+$, and in the worst case, $f(n + 1) = 1 + \max\{f(r - 1), f(r)\} = 1 + f(r)$, by the induction hypothesis. Therefore,

$$f(n) = f(2r - 1) = 1 + f(r - 1) \leq 1 + f(r) = f(n + 1).$$

Consequently, the function f is monotone increasing.

Now it is time to determine the worst-case time complexity for the binary search algorithm, using the function $f(n)$. Since

$$\begin{aligned} &f(1) = 1, \quad \text{and} \\ &f(n) = f(n/2) + 1, \qquad \text{for } n = 2^k, \qquad k \geq 1, \end{aligned}$$

it follows from Theorem 10.1 (with $a = 1$, $b = 2$, and $c = 1$) that

$$f(n) = \log_2 n + 1, \quad \text{and} \quad f \in O(\log_2 n) \qquad \text{for } n \in \{1, 2, 4, 8, \ldots\}.$$

But with f monotone increasing, from Theorem 10.2 it now follows that $f \in O(\log_2 n)$ (for all $n \in \mathbf{Z}^+$). Consequently, binary search is an $O(\log_2 n)$ algorithm, whereas the searching algorithm of Example 5.70 is $O(n)$. Therefore, as the value of n increases, binary search is the more efficient algorithm — but then it requires the additional condition that the array be ordered.

This section has introduced some of the basic ideas in the study of divide-and-conquer algorithms. It also extends the material first introduced on computational complexity and the analysis of algorithms in Sections 5.7 and 5.8.

The Section Exercises include some extensions of the results developed in this section. The reader who wants to pursue this topic further should find the chapter references both helpful and interesting.

EXERCISES 10.6

1. In each of the following, $f: \mathbf{Z}^+ \to \mathbf{R}$. Solve for $f(n)$ relative to the given set S, and determine the appropriate "big-Oh" form for f on S.

a) $f(1) = 5$
$f(n) = 4f(n/3) + 5, \quad n = 3, 9, 27, \ldots$
$S = \{3^i | i \in \mathbf{N}\}$

b) $f(1) = 7$
$f(n) = f(n/5) + 7, \quad n = 5, 25, 125, \ldots$
$S = \{5^i | i \in \mathbf{N}\}$

2. Let $a, b, c \in \mathbf{Z}^+$ with $b \geq 2$, and let $d \in \mathbf{N}$. Prove that the solution for the recurrence relation

$$f(1) = d$$
$$f(n) = af(n/b) + c, \qquad n = b^k, \qquad k \geq 1$$

satisfies

a) $f(n) = d + c \log_b n$, for $n = b^k$, $k \in \mathbf{N}$, when $a = 1$.

b) $f(n) = dn^{\log_b a} + (c/(a-1))[n^{\log_b a} - 1]$, for $n = b^k$, $k \in \mathbf{N}$, when $a \geq 2$.

3. Determine the appropriate "big-Oh" forms for f on $\{b^k | k \in \mathbf{N}\}$ in parts (a) and (b) of Exercise 2.

4. In each of the following, $f: \mathbf{Z}^+ \to \mathbf{R}$. Solve for $f(n)$ relative to the given set S, and determine the appropriate "big-Oh" form for f on S.

a) $f(1) = 0$
$f(n) = 2f(n/5) + 3, \quad n = 5, 25, 125, \ldots$
$S = \{5^i | i \in \mathbf{N}\}$

b) $f(1) = 1$
$f(n) = f(n/2) + 2, \quad n = 2, 4, 8, \ldots$
$S = \{2^i | i \in \mathbf{N}\}$

5. Consider a tennis tournament for n players, where $n = 2^k$, $k \in \mathbf{Z}^+$. In the first round $n/2$ matches are played, and the $n/2$ winners advance to round 2, where $n/4$ matches are played. This halving process continues until a winner is determined.

a) For $n = 2^k$, $k \in \mathbf{Z}^+$, let $f(n)$ count the total number of matches played in the tournament. Find and solve a recurrence relation for $f(n)$ of the form

$$f(1) = d$$
$$f(n) = af(n/2) + c, \qquad n = 2, 4, 8, \ldots,$$

where a, c, and d are constants.

b) Show that your answer in part (a) also solves the recurrence relation

$$f(1) = d$$
$$f(n) = f(n/2) + (n/2), \qquad n = 2, 4, 8, \ldots.$$

6. Complete the proofs for Corollary 10.1 and parts (b) and (c) of Theorem 10.2.

7. What is the best-case time-complexity function for binary search?

8. **a)** Modify the procedure in Example 10.48 as follows: For any $S \subset \mathbf{R}$, where $|S| = n$, partition S as $S_1 \cup S_2$, where $|S_1| = |S_2|$, for n even, and $|S_1| = 1 + |S_2|$, for n odd. Show that if $f(n)$ counts the number of comparisons needed (in this procedure) to find the maximum and minimum elements of S, then f is a monotone increasing function.

b) What is the appropriate "big-Oh" form for the function f of part (a)?

9. In Corollary 10.2 we were concerned with finding the appropriate "big-Oh" form for a function $f: \mathbf{Z}^+ \to \mathbf{R}^+ \cup \{0\}$ where

$$f(1) \leq c, \qquad \text{for } c \in \mathbf{Z}^+$$
$$f(n) \leq af(n/b) + c,$$
$$\text{for } a, b \in \mathbf{Z}^+ \text{ with } b \geq 2, \text{ and } n = b^k, k \in \mathbf{Z}^+.$$

Here the constant c in the second inequality is interpreted as the amount of time needed to break down the given problem of size n into a smaller (similar) problems of size n/b and to combine the a solutions of these smaller problems in order to get a solution for the original problem of size n. Now we shall examine a situation wherein this amount of time is no longer constant but depends on n.

a) Let $a, b, c \in \mathbf{Z}^+$, with $b \geq 2$. Let $f: \mathbf{Z}^+ \to \mathbf{R}^+ \cup \{0\}$ be a monotone increasing function, where

$$f(1) \leq c$$
$$f(n) \leq af(n/b) + cn, \qquad \text{for } n = b^k, \qquad k \in \mathbf{Z}^+.$$

Use an argument similar to the one given (for equalities) in Theorem 10.1 to show that for all $n = 1, b, b^2, b^3, \ldots,$

$$f(n) \leq cn \sum_{i=0}^{k} (a/b)^i.$$

b) Use the result of part (a) to show that $f \in O(n \log n)$, where $a = b$. (The base for the log function here is any real number greater than 1.)

c) When $a \neq b$, show that part (a) implies that

$$f(n) \leq \left(\frac{c}{a-b}\right)(a^{k+1} - b^{k+1}).$$

d) From part (c), prove that (i) $f \in O(n)$, when $a < b$; and (ii) $f \in O(n^{\log_b a})$, when $a > b$. [*Note*: The "big-Oh" form for f here and in part (b) is for f on $\mathbf{Z}^+$, not just $\{b^k | k \in \mathbf{N}\}$.]

10. In this exercise we briefly introduce the *Master Theorem*. (For more on this result, including a proof, we refer the reader to pp. 73–84 of reference [5] by T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein.)

Consider the recurrence relation

$$f(1) = 1,$$
$$f(n) = af(n/b) + h(n),$$

where $n \in \mathbf{Z}^+$, $n > 1$, $a \in \mathbf{Z}^+$, $a < n$, and $b \in \mathbf{R}^+$, $1 < b < n$. The function h accounts for the time (or cost) of dividing the given problem of size n into a smaller (similar) problems of size approximately n/b and then combining the results from

the a smaller problems. Further, there exists $k \in \mathbf{Z}^+$ such that $h(n) > 0$ for all $n \geq k$. (Since n/b need not be an integer, the recurrence relation is not properly defined. To get around this we need to replace n/b by either $\lfloor n/b \rfloor$ or $\lceil n/b \rceil$. But as this does not affect the outcome of the result, for large values of n, we shall not concern ourselves with such details.)

Under the above hypothesis we find the following [where Θ (big theta) and Ω (big omega) are as given in Exercises 11–16 for Section 5.7]:

i) If $h \in O(n^{\log_b a - \epsilon})$, for some fixed $\epsilon > 0$, then $f \in \Theta(n^{\log_b a})$;

ii) If $h \in \Theta(n^{\log_b a})$, then $f \in \Theta(n^{\log_b a} \log_2 n)$; and

iii) If $h \in \Omega(n^{\log_b a + \epsilon})$ for some fixed $\epsilon > 0$, and if $a\, h(n/b) \leq c\, h(n)$, for some fixed c, where $0 < c < 1$, and for all sufficiently large n, then $f \in \Theta(h)$.

In all three cases, the function h is compared with $n^{\log_b a}$ and, roughly speaking, the Master Theorem then determines the complexity of the solution $f(n)$ as the larger of the two functions in cases (i) and (iii), while in case (ii) we find the added factor $\log_2 n$. However, it is important to realize that there are some recurrence relations of this type that do not fall under any of these three cases.

For now we consider the following, where $f(1) = 1$ for all three examples.

1) $f(n) = 16f(n/4) + n$
Here $a = 16$, $b = 4$, $n^{\log_b a} = n^{\log_4 16} = n^2$, and $h(n) = n$. So $h \in O(n^{\log_4 16 - \epsilon})$ with $\epsilon = 1$. Consequently, h falls under the hypothesis for case (i) and it follows that $f \in \Theta(n^2)$.

2) $f(n) = f(3n/4) + 5$
Now we have $a = 1$, $b = 4/3$, $n^{\log_b a} = n^{\log_{4/3} 1} = n^0 = 1$, and $h(n) = 5$. Consequently, $h \in \Theta(n^{\log_{4/3} 1})$ and from case (ii) we learn that $f \in \Theta(n^{\log_{4/3} 1} \log_2 n) = \Theta(\log_2 n)$.

3) $f(n) = 7f(n/8) + n \log_2 n$
For this recurrence relation we have $a = 7$, $b = 8$, $n^{\log_b a} = n^{\log_8 7} \doteq n^{0.936}$, and $h(n) = n \log_2 n$. So $h \in \Omega(n^{\log_8 7 + \epsilon})$, where $\epsilon \doteq 0.064 > 0$. Further, for all sufficiently large n, $a\, h(n/b) = 7(n/8) \log_2(n/8) = (7/8)n[\log_2 n - \log_2 8] \leq (7/8)n \log_2 n = c\, h(n)$, for $0 < c = 7/8 < 1$. Thus, h satisfies the hypotheses for case (iii) and we have $f \in \Theta(n \log_2 n)$.

Use the Master Theorem to determine the complexity of f in each of the following, where $f(1) = 1$:

a) $f(n) = 9f(n/3) + n$ **b)** $f(n) = 2f(n/2) + 1$

c) $f(n) = f(2n/3) + 1$ **d)** $f(n) = 2f(n/3) + n$

e) $f(n) = 4f(n/2) + n^2$

10.7 Summary and Historical Review

In this chapter the recurrence relation has emerged as another tool for solving combinatorial problems. In these problems we analyze a given situation and then express the result a_n in terms of the results for certain smaller nonnegative integers. Once the recurrence relation is determined, we can solve for any value of a_n (within reason). When we have access to a computer, such relations are particularly valuable, especially if they cannot be solved explicitly.

The study of recurrence relations can be traced back to the Fibonacci relation $F_{n+2} = F_{n+1} + F_n$, $n \geq 0$, $F_0 = 0$, $F_1 = 1$, which was given by Leonardo of Pisa (c. 1175–1250) in 1202. In his *Liber Abaci*, he deals with a problem concerning the number of pairs of rabbits that result in one year if one starts with a single pair that produces another pair at the end of each month. Each new pair starts to breed similarly one month after its birth, and we assume that no rabbits die during the given year. Hence, at the end of the first month there are two pairs of rabbits; three pairs after two months; five pairs after three months; and so on. [As mentioned in the summary of Chapter 9, Abraham DeMoivre (1667–1754) obtained this result by the method of generating functions in 1718.] This same sequence appears in the work of the German mathematician Johannes Kepler (1571–1630), who used it in his studies on how the leaves of a plant or flower are arranged about its stem. In 1844 the French mathematician Gabriel Lamé (1795–1870) used the sequence in his analysis of the efficiency of the Euclidean algorithm. Later, François Èdouard Anatole Lucas (1842–1891), who popularized the Towers of Hanoi puzzle, derived many properties of this sequence and was the first to call these numbers the Fibonacci sequence.

Leonardo Fibonacci (c. 1175–1250)

Reproduced courtesy of The Granger Collection, New York

For an elementary coverage of examples and properties for the Fibonacci numbers one should examine the book by T. H. Garland [10]. Even more can be learned from the texts by V. E. Hoggatt, Jr. [14] and S. Vajda [29]. The UMAP article by R.V. Jean [16] gives many applications of this sequence. Chapter 8 of the mathematical exposition by R. Honsberger [15] provides an interesting account of the Fibonacci numbers and of the related sequence called the Lucas numbers. The text by R. L. Graham, D. E. Knuth, and O. Patashnik [12] also includes many interesting examples and properties of both the Fibonacci numbers and the Catalan numbers. More counterexamples for the Fibonacci and Catalan numbers, like those found in Examples 10.17 and 10.44, respectively, can be found in the article by R. K. Guy [13]. Additional material on the role of the golden ratio in such areas as geometry, probability, and fractals is given in the book by H. Walser [30]. The book by T. Koshy [19] provides a definitive history and extensive analysis of the Fibonacci and Lucas numbers, together with a wide variety of applications, examples, and exercises.

Comparable coverage of the material presented in this chapter can be found in Chapter 3 of C. L. Liu [21]. For more on the theoretical development of linear recurrence relations with constant coefficients, examine Chapter 9 of N. Finizio and G. Ladas [8].

Applications in probability theory dealing with recurrent events, random walks, and ruin problems can be found in Chapters XIII and XIV of the classic text by W. Feller [7]. The UMAP module by D. R. Sherbert [24] introduces difference equations and includes an application in economics known as the *Cobweb Theorem*. The text by S. Goldberg [11] has more on applications in the social sciences.

Recursive techniques in the generation of permutations and combinations are developed in Chapter 4 of R. A. Brualdi [3]. The algorithm presented in Section 10.1 for the permutations of $\{1, 2, 3, \ldots, n\}$ first appeared in the work of H. D. Steinhaus [27] and is often referred to as the *adjacent mark ordering algorithm*. This result was rediscovered later, independently by H. F. Trotter [28] and S. M. Johnson [17]. Efficient sorting methods for permutations and other combinatorial structures are analyzed in the text by D. E. Knuth [18]. The work of E. M. Reingold, J. Nievergelt, and N. Deo [23] also deals with such algorithms.

For those who enjoyed the rooted ordered binary trees in Section 10.5, Chapter 3 of A. V. Aho, J. E. Hopcroft, and J. D. Ullman [1] should prove interesting. The basis for the

example on stacks is given on page 86 of the text by S. Even [6]. The article by M. Gardner [9] provides other examples where the Catalan numbers arise. Computational considerations in determining Catalan numbers are examined in the article by D. M. Campbell [4]. Much more about the Catalan numbers can be found in the text by R. P. Stanley [26] — in particular, 66 situations, where these numbers arise, are provided on pp. 219–229.

Finally, the coverage on divide-and-conquer algorithms in Section 10.6 is modeled after D. F. Stanat and D. F. McAllister's presentation in Section 5.3 of [25]. Chapter 10 of the text by A. V. Aho, J. E. Hopcroft, and J. D. Ullman [1] provides some further information on this topic. An application of this method in a matrix multiplication algorithm appears in Chapter 10 of the text by C. L. Liu [20]. Additional coverage and a proof for the Master Theorem are given in Chapter 4 of the text by T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein [5].

REFERENCES

1. Aho, Alfred V., Hopcroft, John E., and Ullman, Jeffery D. *Data Structures and Algorithms*. Reading, Mass.: Addison-Wesley, 1983.
2. Auluck, F. C. "On Some New Types of Partitions Associated with Generalized Ferrers Graphs." *Proceedings of the Cambridge Philosophical Society* 47 (1951): pp. 679–685.
3. Brualdi, Richard A. *Introductory Combinatorics*, 3rd ed. Upper Saddle River, N.J.: Prentice-Hall, 1999.
4. Campbell, Douglas M. "The Computation of Catalan Numbers." *Mathematics Magazine* 57, no. 4 (September 1984): pp. 195–208.
5. Cormen, Thomas H., Leiserson, Charles E., Rivest, Ronald L., and Stein, Clifford. *Introduction to Algorithms*, 2nd ed. Boston, Mass.: McGraw-Hill, 2001.
6. Even, Shimon. *Graph Algorithms*. Rockville, Md.: Computer Science Press, 1979.
7. Feller, William. *An Introduction to Probability Theory and Its Applications*, Vol. I, 3rd ed. New York: Wiley, 1968.
8. Finizio, N., and Ladas, G. *An Introduction to Differential Equations*. Belmont, Calif.: Wadsworth Publishing Company, 1982.
9. Gardner, Martin. "Mathematical Games, Catalan Numbers: An Integer Sequence that Materializes in Unexpected Places." *Scientific American* 234, no. 6 (June 1976): pp. 120–125.
10. Garland, Trudi Hammel. *Fascinating Fibonaccis*. Palo Alto, Calif.: Dale Seymour Publications, 1987.
11. Goldberg, Samuel. *Introduction to Difference Equations*. New York: Wiley, 1958.
12. Graham, Ronald Lewis, Knuth, Donald Ervin, and Patashnik, Oren. *Concrete Mathematics*, 2nd ed. Reading, Mass.: Addison-Wesley, 1994.
13. Guy, Richard K. "The Second Strong Law of Small Numbers." *Mathematics Magazine* 63, no. 1 (February 1990): pp. 3–20.
14. Hoggatt, Verner E., Jr. *Fibonacci and Lucas Numbers*. Boston, Mass.; Houghton Mifflin, 1969.
15. Honsberger, Ross. *Mathematical Gems III* (The Dolciani Mathematical Expositions, Number Nine). Washington, D.C.: The Mathematical Association of America, 1985.
16. Jean, Roger V. "The Fibonacci Sequence." *The UMAP Journal* 5, no. 1 (1984): pp. 23–47.
17. Johnson, Selmer M. "Generation of Permutations by Adjacent Transposition." *Mathematics of Computation* 17 (1963): pp. 282–285.
18. Knuth, Donald E. *The Art of Computer Programming/Volume 3 Sorting and Searching*. Reading, Mass: Addison-Wesley, 1973.
19. Koshy, Thomas. *Fibonacci and Lucas Numbers with Applications*. New York: Wiley, 2001.
20. Liu, C. L. *Elements of Discrete Mathematics*, 2nd ed. New York: McGraw-Hill, 1985.
21. Liu, C. L. *Introduction to Combinatorial Mathematics*. New York: McGraw-Hill, 1968.
22. Miksa, F. L., Moser, L., and Wyman, M. "Restricted Partitions of Finite Sets." *Canadian Mathematics Bulletin* 1 (1958): pp. 87–96.

23. Reingold, E. M., Nievergelt, J., and Deo, N. *Combinatorial Algorithms: Theory and Practice.* Englewood Cliffs, N.J.: Prentice-Hall, 1977.
24. Sherbert, Donald R. *Difference Equations with Applications*, UMAP Module 322. Cambridge, Mass.: Birkhauser Boston, 1980.
25. Stanat, Donald F., and McAllister, David F. *Discrete Mathematics in Computer Science.* Englewood Cliffs, N.J.: Prentice-Hall, 1977.
26. Stanley, Richard P. *Enumerative Combinatorics*, Vol. 2. New York: Cambridge University Press, 1999.
27. Steinhaus, Hugo D. *One Hundred Problems in Elementary Mathematics.* New York: Basic Books, 1964.
28. Trotter, H. F. "ACM Algorithm 115—Permutations." *Communications of the ACM* 5 (1962): pp. 434–435.
29. Vajda, S. *Fibonacci & Lucas Numbers, and the Golden Section.* New York: Halsted Press (a division of John Wiley & Sons), 1989.
30. Walser, Hans. *The Golden Section.* Washington, D.C.: The Mathematical Association of America, 2001.

SUPPLEMENTARY EXERCISES

1. For $n \in \mathbf{Z}^+$ and $n \geq k+1 \geq 1$, verify algebraically the recursion formula

$$\binom{n}{k+1} = \left(\frac{n-k}{k+1}\right)\binom{n}{k}.$$

2. **a)** For $n \geq 0$, let B_n denote the number of partitions of $\{1, 2, 3, \ldots, n\}$. Set $B_0 = 1$ for the partitions of $\emptyset$. Verify that for all $n \geq 0$,

$$B_{n+1} = \sum_{i=0}^{n} \binom{n}{n-i} B_i = \sum_{i=0}^{n} \binom{n}{i} B_i.$$

[The numbers B_i, $i \geq 0$, are referred to as the *Bell numbers* after Eric Temple Bell (1883–1960).]

b) How are the Bell numbers related to the Stirling numbers of the second kind?

3. Let $n, k \in \mathbf{Z}^+$, and define $p(n, k)$ to be the number of partitions of n into exactly k (positive-integer) summands. Prove that $p(n, k) = p(n-1, k-1) + p(n-k, k)$.

4. For $n \geq 1$, let a_n count the number of ways to write n as an ordered sum of odd positive integers. (For example, $a_4 = 3$ since $4 = 3 + 1 = 1 + 3 = 1 + 1 + 1 + 1$.) Find and solve a recurrence relation for a_n.

5. Let $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$.

a) Compute A^2, A^3, and A^4.

b) Conjecture a general formula for A^n, $n \in \mathbf{Z}^+$, and establish your conjecture by the Principle of Mathematical Induction.

6. Let $M = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$.

a) Compute M^2, M^3, and M^4.

b) Conjecture a general formula for M^n, $n \in \mathbf{Z}^+$, and establish your conjecture by the Principle of Mathematical Induction.

7. Determine the points of intersection of the parabola $y = x^2 - 1$ and the hyperbola $y = 1 + \frac{1}{x}$.

8. Let $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$.

a) Verify that $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$.

b) Prove that for all $n \geq 0$, $\sum_{k=0}^{n} \binom{n}{k} F_k = F_{2n}$.

c) Show that $\alpha^3 = 1 + 2\alpha$ and $\beta^3 = 1 + 2\beta$.

d) Prove that for all $n \geq 0$, $\sum_{k=0}^{n} \binom{n}{k} 2^k F_k = F_{3n}$.

9. **a)** For $\alpha = (1 + \sqrt{5})/2$, verify that $\alpha^2 + 1 = 2 + \alpha$ and $(2 + \alpha)^2 = 5\alpha^2$.

b) Show that for $\beta = (1 - \sqrt{5})/2$, $\beta^2 + 1 = 2 + \beta$ and $(2 + \beta)^2 = 5\beta^2$.

c) If $n, m \in \mathbf{N}$ prove that

$$\sum_{k=0}^{2n} \binom{2n}{k} F_{2k+m} = 5^n F_{2n+m}.$$

10. Renu wants to sell her laptop for \$4000. Narmada offers to buy it for \$3000. Renu then splits the difference and asks for \$3500. Narmada likewise splits the difference and makes a new offer of \$3250. (a) If the women continue this process (of asking prices and counteroffers), what will Narmada be willing to pay on her 5th offer? 10th offer? kth offer, $k \geq 1$? (b) If the women continue this process (providing many, many new asking prices and counteroffers), what price will they approach? (c) Suppose that Narmada was willing to buy the laptop for \$3200. What should she have offered to pay Renu the first time?

11. Parts (a) and (b) of Fig. 10.27 provide the Hasse diagrams for two partial orders referred to as the *fences* $\mathcal{F}_5$, $\mathcal{F}_6$ [on 5, 6 (distinct) elements, respectively]. If, for instance, $\mathcal{R}$ denotes the

partial order for the fence $\mathcal{F}_5$, then $a_1 \mathcal{R} a_2$, $a_3 \mathcal{R} a_2$, $a_3 \mathcal{R} a_4$, and $a_5 \mathcal{R} a_4$. For each such fence $\mathcal{F}_n$, $n \geq 1$, we follow the convention that an element with an odd subscript is minimal and one with an even subscript is maximal. Let $(\{1, 2\}, \leq)$ denote the partial order where $\leq$ denotes the usual "less than or equal to" relation. As in Exercise 26 of Section 7.3, a function $f: \mathcal{F}_n \to \{1, 2\}$ is called *order-preserving* when for all $x, y \in \mathcal{F}_n$, $x \mathcal{R} y \Rightarrow f(x) \leq f(y)$. Let c_n count the number of such order-preserving functions. Find and solve a recurrence relation for c_n.

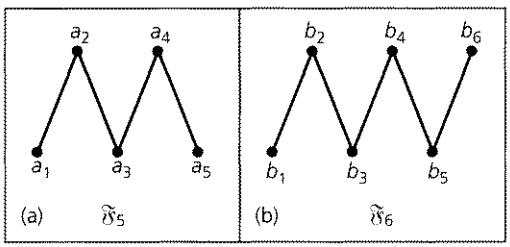


Figure 10.27

12. For $n \geq 0$, let $m = \lfloor (n+1)/2 \rfloor$. Prove that $F_{n+2} = \sum_{k=0}^{m} \binom{n-k+1}{k}$. (You may want to look back at Examples 9.17 and 10.11.)

13. **a)** For $n \in \mathbf{Z}^+$, determine the number of ways one can tile a $1 \times n$ chessboard using 1×1 white (square) tiles and 1×2 blue (rectangular) tiles.

b) How many of the tilings in part (a) use (i) no blue tiles; (ii) exactly one blue tile; (iii) exactly two blue tiles; (iv) exactly three blue tiles; and (v) exactly k blue tiles, where $0 \leq k \leq \lfloor n/2 \rfloor$?

c) How are the results in parts (a) and (b) related?

14. Let $c = \sqrt{1 + \sqrt{1 + \sqrt{1 + \sqrt{1 + \cdots}}}}$. How is c^2 related to c? What is the value of c?

15. For $n \in \mathbf{Z}^+$, d_n denotes the number of derangements of $\{1, 2, 3, \ldots, n\}$, as discussed in Section 8.3.

a) If $n > 2$, show that d_n satisfies the recurrence relation

$$d_n = (n-1)(d_{n-1} + d_{n-2}), \qquad d_2 = 1, \qquad d_1 = 0.$$

b) How can we define d_0 so that the result in part (a) is valid for $n \geq 2$?

c) Rewrite the result in part (a) as

$$d_n - nd_{n-1} = -[d_{n-1} - (n-1)d_{n-2}].$$

How can $d_n - nd_{n-1}$ be expressed in terms of d_{n-2}, d_{n-3}?

d) Show that $d_n - nd_{n-1} = (-1)^n$.

e) Let $f(x) = \sum_{n=0}^{\infty} (d_n x^n)/n!$. After multiplying both sides of the equation in part (d) by $x^n/n!$ and summing for $n \geq 2$, verify that $f(x) = (e^{-x})/(1-x)$. Hence

$$d_n = n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\right].$$

16. For $n \geq 0$, draw n ovals in the plane so that each oval intersects each of the others in exactly two points and no three ovals are coincident. If a_n denotes the number of regions in the plane that results from these n ovals, find and solve a recurrence relation for a_n.

17. For $n \geq 0$, let us toss a coin $2n$ times.

a) If a_n is the number of sequences of $2n$ tosses where n heads and n tails occur, find a_n in terms of n.

b) Find constants r, s, and t so that $(r + sx)^t = f(x) = \sum_{n=0}^{\infty} a_n x^n$.

c) Let b_n denote the number of sequences of $2n$ tosses where the numbers of heads and tails are equal for the first time only after all $2n$ tosses have been made. (For example, if $n = 3$, then HHHTTT and HHTHTT are counted in b_n, but HTHHTT and HHTTHT are not.)

Define $b_0 = 0$ and show that for all $n \geq 1$,

$$a_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0.$$

d) Let $g(x) = \sum_{n=0}^{\infty} b_n x^n$. Show that $g(x) = 1 - 1/f(x)$, and then solve for b_n, $n \geq 1$.

18. For $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$, show that $\sum_{k=0}^{\infty} \beta^k = -\beta = \alpha - 1$ and that $\sum_{k=0}^{\infty} |\beta|^k = \alpha^2$.

19. Let a, b, c be fixed real numbers with $ab = 1$ and let $f: \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ be the binary operation, where $f(x, y) = a + bxy + c(x + y)$. Determine the value(s) of c for which f will be associative.

20. **a)** For $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$, verify that $\alpha^2 - \alpha^{-2} = \alpha - \beta = \beta^{-2} - \beta^2$.

b) Prove that $F_{2n} = F_{n+1}^2 - F_{n-1}^2$, $n \geq 1$.

c) For $n \geq 1$, let T be an isosceles trapezoid with bases of length F_{n-1} and F_{n+1}, and sides of length F_n. Prove that the area of T is $(\sqrt{3}/4)F_{2n}$. [Note that, when $n = 1$, the trapezoid degenerates into a triangle. However, the formula is still correct.]

21. Let $\mathcal{S}$ be the sample space for an experiment $\mathcal{E}$. If A, B are events from $\mathcal{S}$ with $A \cup B = \mathcal{S}$, $A \cap B = \emptyset$, $Pr(A) = p$, and $Pr(B) = p^2$, determine p.

22. De'Jzaun and Sandra toss a loaded coin, where $Pr(H) = p > 0$. The first to obtain a head is the winner. Sandra goes first but, if she tosses a tail, then De'Jzaun gets two chances. If he tosses two tails, then Sandra again tosses the coin and, if her toss is a tail, then De'Jzaun again goes twice (if his first toss is a tail). This continues until someone tosses a head. What value of p makes this a fair game (that is, a game where both Sandra and De'Jzaun have probability $\frac{1}{2}$ of winning)?

23. For $n \geq 1$, let a_n count the number of binary strings of length n, where there is no run of 1's of odd length. Consequently,

when $n = 6$, for instance, we want to include the strings 110000 (which has a run of two 1's and a run of four 0's) and 011110 (which has two runs of one 0 and one run of four 1's), but we do not include either 100011 (which starts with a run of one 1) or 110111 (which ends with a run of three 1's). Find and solve a recurrence relation for a_n.

24. Let a, b be fixed nonzero real numbers. Determine x_n if $x_n = x_{n-1}x_{n-2}$, $n \geq 2$, $x_0 = a$, $x_1 = b$.

25. **a)** Evaluate $F_{n+1}^2 - F_n F_{n+1} - F_n^2$ for $n = 0, 1, 2, 3$.

b) From the results in part (a), conjecture a formula for $F_{n+1}^2 - F_n F_{n+1} - F_n^2$ for $n \in \mathbf{N}$.

c) Establish the conjecture in part (b) using the Principle of Mathematical Induction.

26. Let $n \in \mathbf{Z}^+$. On a $1 \times n$ chessboard two kings are called *nontaking*, if they do not occupy adjacent squares. In how many ways can one place 0 or more nontaking kings on a $1 \times n$ chessboard?

27. **a)** For $1 \leq i \leq 6$, determine the rook polynomial $r(C_i, x)$ for the chessboard C_i shown in Fig. 10.28.

b) For each rook polynomial in part (a), find the sum of the coefficients of the powers of x — that is, determine $r(C_i, 1)$ for $1 \leq i \leq 6$.

28. (Gambler's Ruin) When Cathy and Jill play checkers, each has probability $\frac{1}{2}$ of winning. There is never a tie, and the games are independent in the sense that no matter how many games the girls have played, each girl still has probability $\frac{1}{2}$ of winning the next game. After each game the loser gives the winner a quarter. If Cathy has \$2.00 to play with and Jill has \$2.50 and they play until one of them is broke, what is the probability that Cathy gets wiped out?

29. For $n, m \in \mathbf{Z}^+$, let $f(n, m)$ count the number of partitions of n where the summands form a nonincreasing sequence of positive integers and no summand exceeds m. With $n = 4$ and $m = 2$, for example, we find that $f(4, 2) = 3$ because here we are concerned with the three partitions

$$4 = 2 + 2, \qquad 4 = 2 + 1 + 1, \qquad 4 = 1 + 1 + 1 + 1.$$

a) Verify that for all $n, m \in \mathbf{Z}^+$,

$$f(n, m) = f(n - m, m) + f(n, m - 1).$$

b) Write a computer program (or develop an algorithm) to compute $f(n, m)$ for $n, m \in \mathbf{Z}^+$.

c) Write a computer program (or develop an algorithm) to compute $p(n)$, the number of partitions of a given positive integer n.

30. Let A, B be sets with $|A| = m \geq n = |B|$, and let $a(m, n)$ count the number of *onto* functions from A to B. Show that

$$a(m, 1) = 1$$

$$a(m, n) = n^m - \sum_{i=1}^{n-1} \binom{n}{i} a(m, i), \qquad \text{when } m \geq n > 1.$$

31. When one examines the units digit of each Fibonacci number F_n, $n \geq 0$, one finds that these digits form a sequence that repeats after 60 terms. [This was first proved by Joseph-Louis Lagrange (1736–1813).] Write a computer program (or develop an algorithm) to calculate this sequence of 60 digits.

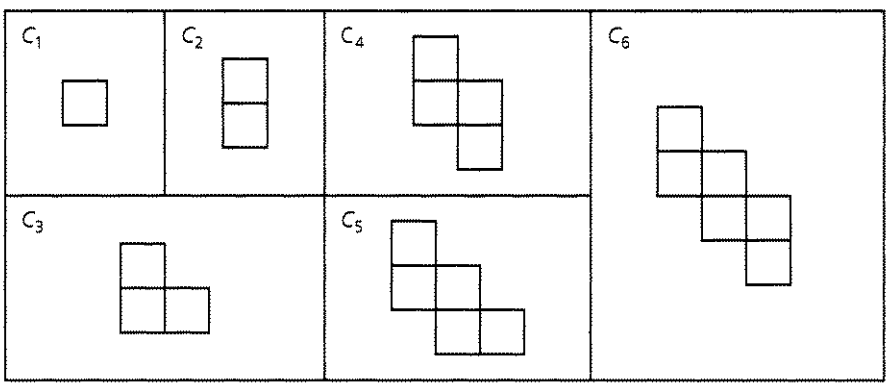


Figure 10.28

PART

4

MODERN APPLIED ALGEBRA

14

Rings and Modular Arithmetic

In this fourth and final part of the text, the emphasis will be on structure again as we begin the investigation of sets of elements that are closed under two binary operations. The concepts of structure and enumeration often reinforce each other. Here we will see this occur as ideas seen in Chapters 1, 4, 5, and 8 come to the forefront again.

When we examined the set $\mathbf{Z}$ in Chapter 4, it was in conjunction with the closed binary operations of addition and multiplication. In this chapter we emphasize these operations by writing $(\mathbf{Z}, +, \cdot)$, instead of just $\mathbf{Z}$. Patterned after some of the properties of $(\mathbf{Z}, +, \cdot)$, the algebraic structure called a *ring* will be defined. Without knowing it, we have been dealing with rings in many mathematical settings. Now we shall be concerned with finite rings that arise in number theory and computer science applications. Of particular interest in the study of computer science is the *hashing function*, which we find provides a means of identifying records stored in a table.

14.1 The Ring Structure: Definition and Examples

We start by defining the ring structure, realizing as we do that most abstract definitions, like theorems, come about from a study of many examples where one recognizes the common idea or ideas present in what may seem to be a collection of unrelated objects.

Definition 14.1 Let R be a nonempty set on which we have two closed binary operations, denoted by $+$ and $\cdot$ (which may be quite different from the ordinary addition and multiplication to which we are accustomed). Then $(R, +, \cdot)$ is a *ring* if for all $a, b, c \in R$, the following conditions are satisfied:

a)	$a + b = b + a$	Commutative Law of $+$
b)	$a + (b + c) = (a + b) + c$	Associative Law of $+$
c)	There exists $z \in R$ such that $a + z = z + a = a$ for every $a \in R$.	Existence of an identity for $+$
d)	For each $a \in R$ there is an element $b \in R$ with $a + b = b + a = z$.	Existence of inverses under $+$
e)	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$	Associative Law of $\cdot$

f) $a \cdot (b + c) = a \cdot b + a \cdot c$ Distributive Laws of $\cdot$ over $+$
$(b + c) \cdot a = b \cdot a + c \cdot a$

Since the closed binary operations of $+$ (ring addition) and $\cdot$ (ring multiplication) are both associative, no ambiguity will arise if we write $a + b + c$ for either $(a + b) + c$ or $a + (b + c)$, or $a \cdot b \cdot c$ for either $(a \cdot b) \cdot c$ or $a \cdot (b \cdot c)$. When dealing with the (closed) binary operation of ring multiplication, we shall often write ab for $a \cdot b$. In addition, we can extend the associative laws (given in the definition of a ring) as we did in Exercises 8 and 9 of Section 4.2. Using mathematical induction, it can be verified that for all $r, n \in \mathbf{Z}^+$, with $n \geq 3$ and $1 \leq r < n$,

$$(a_1 + a_2 + \cdots + a_r) + (a_{r+1} + \cdots + a_n) = a_1 + a_2 + \cdots + a_r + a_{r+1} + \cdots + a_n,$$

and

$$(a_1 a_2 \cdots a_r)(a_{r+1} \cdots a_n) = a_1 a_2 \cdots a_r a_{r+1} \cdots a_n,$$

where $a_1, a_2, \ldots, a_r, a_{r+1}, \ldots, a_n$ are elements of a given ring $(R, +, \cdot)$. In a corresponding way, the distributive laws generalize as follows:

$$a(b_1 + b_2 + \cdots + b_n) = ab_1 + ab_2 + \cdots + ab_n,$$
$$(b_1 + b_2 + \cdots + b_n)a = b_1 a + b_2 a + \cdots + b_n a,$$

for arbitrary ring elements $a, b_1, b_2, \ldots, b_n$ and all $n \in \mathbf{Z}^+$ where $n \geq 3$.

In the next section we shall learn that the additive identity (or zero element) is unique, as is the additive inverse of each ring element. For now, let us consider some examples of rings.

EXAMPLE 14.1

Under the (closed) binary operations of ordinary addition and multiplication, we find that $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ are rings. In all of these rings the additive identity z is the integer 0, and the additive inverse of each number x is the familiar $-x$.

EXAMPLE 14.2

Let $M_2(\mathbf{Z})$ denote the set of all 2×2 matrices with integer entries. [The sets $M_2(\mathbf{Q})$, $M_2(\mathbf{R})$, and $M_2(\mathbf{C})$ are defined similarly.] In $M_2(\mathbf{Z})$ two matrices are equal if their corresponding entries are equal in $\mathbf{Z}$.

Here we define $+$ and $\cdot$ by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}, \qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}.$$

Under these (closed) binary operations, $M_2(\mathbf{Z})$ is a ring. Here $z = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and the additive inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

A few things happen here, however, that do not occur in the rings of Example 14.1. For example,

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 3 & 7 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 7 \\ 4 & 7 \end{bmatrix} \neq \begin{bmatrix} 10 & 13 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$$

shows that multiplication need not be commutative in a ring. That is why there are two distributive laws. Also,

$$\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

even though neither $\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$ nor $\begin{bmatrix} 2 & 1 \\ 2 & 1 \end{bmatrix}$ is the additive identity. Hence a ring may contain what are called *proper divisors of zero* — that is, nonzero elements whose product is the zero element of the ring.

We extend our study of the ring structure in the following.

Definition 14.2 Let $(R, +, \cdot)$ be a ring.

a) If $ab = ba$ for all $a, b \in R$, then R is called a *commutative* ring.

b) The ring R is said to have no *proper divisors of zero* if for all $a, b \in R, ab = z \Rightarrow a = z$ or $b = z$.

c) If an element $u \in R$ is such that $u \neq z$ and $au = ua = a$ for all $a \in R$, we call u a *unity*, or *multiplicative identity*, of R. Here R is called a *ring with unity*.

It follows from part (c) of Definition 14.2 that whenever we have a ring R with unity, then R contains at least two elements. Furthermore, if a ring has a unity we shall learn in the next section that it is unique.

The rings in Example 14.1 are all commutative rings whose unity is the integer 1. None of these rings has any proper divisors of zero. Meanwhile, the ring $M_2(\mathbf{Z})$ is a noncommutative ring whose unity is the matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. This ring does contain proper divisors of zero.

Also, whenever we want to verify that a particular structure $(R, +, \cdot)$ is a ring, we can start by showing that R is closed under both binary operations. Then we can continue and verify conditions (a)–(e) of Definition 14.1. Before we try to establish the distributive laws, however, we might want to first determine if the multiplication operation is commutative. Should we find this operation to be commutative, then we need only establish one of the distributive laws (for the other will follow automatically). Further, if we are able to verify all of the preceding conditions, then we'll know that $(R, +, \cdot)$ is not just a ring, but a commutative ring.

Now ~~let us study~~ another example as we further investigate the ideas set down in Definitions 14.1 and 14.2.

EXAMPLE 14.3 Consider the set $\mathbf{Z}$ together with the binary operations of $\oplus$ and $\odot$, which are defined by

$$x \oplus y = x + y - 1, \qquad x \odot y = x + y - xy.$$

Consequently, here we find, for instance, that $3 \oplus 7 = 3 + 7 - 1 = 9$ and $3 \odot 7 = 3 + 7 - 3 \cdot 7 = -11$.

Since ordinary addition, subtraction, and multiplication are closed binary operations for $\mathbf{Z}$, these new binary operations — namely, $\oplus$ and $\odot$ — are also closed for $\mathbf{Z}$. In fact, we shall find that $(\mathbf{Z}, \oplus, \odot)$ is a ring.

a) In order to verify that $(\mathbf{Z}, \oplus, \odot)$ is a ring we must establish the six conditions given in Definition 14.1. We shall examine three of these conditions and leave the other three for the Section Exercises.

1) First, since ordinary addition is a commutative binary operation for $\mathbf{Z}$, we find that for all $x, y \in \mathbf{Z}$,

$$x \oplus y = x + y - 1 = y + x - 1 = y \oplus x.$$

So the binary operation $\oplus$ is also commutative for $\mathbf{Z}$.

2) When we examine condition (c) we realize that we need to find an integer z such that $a \oplus z = z \oplus a = a$, for every a in $\mathbf{Z}$. Therefore, we must solve the equation $a + z - 1 = a$, which leads us to $z = 1$. Hence the *nonzero* integer 1 is the *zero* element (or additive identity) for $\oplus$.

3) What about additive inverses? At this point if we are given an (arbitrary) integer a, we want to know if there is an integer b such that $a \oplus b = b \oplus a = z$. From part (2) above and the definition of $\oplus$ this says that the integer b must satisfy $a + b - 1 = 1$, and it follows that $b = 2 - a$. So, for instance, the additive inverse of 7 is $2 - 7 = -5$ and the additive inverse for -42 is $2 - (-42) = 44$. After all, in the case of 7 we find that $7 \oplus (-5) = 7 + (-5) - 1 = 7 - 5 - 1 = 1$, where 1 is the additive identity. [*Note*: Since we showed in part (1) that $\oplus$ is commutative, we also know that $(-5) \oplus 7 = 1$.]

b) Furthermore, the ring $(\mathbf{Z}, \oplus, \odot)$ also possesses the additional properties given in Definition 14.2. In particular this ring has a unity (that is, a multiplicative identity). To determine the unity, let a be any integer and consider the element u $(\neq z = 1)$ where

$$a \odot u = u \odot a = a.$$

Since $a \odot u = a + u - au$, we solve $a + u - au = a$ to find that $u(1 - a) = 0$. Since a is arbitrary, this must hold even when $a \neq 1$. Consequently, the integer $u = 0$ is the unity for the ring $(\mathbf{Z}, \oplus, \odot)$.

After these examples of infinite rings, we turn now to rings with finitely many elements.

EXAMPLE 14.4

Let $\mathcal{U} = \{1, 2\}$ and $R = \mathcal{P}(\mathcal{U})$. Define $+$ and $\cdot$ on the elements of R by

$$A + B = A \triangle B = \{x \mid x \in A \text{ or } x \in B, \text{ but not both}\}$$
$$A \cdot B = A \cap B = \text{the intersection of sets } A, B \subseteq \mathcal{U}.$$

We form Tables 14.1(a) and (b) for these operations.

From results in Chapter 3, one finds that R satisfies conditions (a), (b), (e), and (f) of Definition 14.1 for these (closed) binary operations of "addition" and "multiplication." The table for "addition" shows that $\emptyset$ is the additive identity. For each $x \in R$, the additive inverse of x is x itself. The multiplication table is symmetric about the diagonal from the upper left to the lower right, so the operation described by the table is commutative. The table also indicates that R has *unity* $\mathcal{U}$. So R is a finite commutative ring with unity. The elements $\{1\}$, $\{2\}$ provide an example of proper divisors of zero.

Table 14.1

$+ (\Delta)$	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$
$\emptyset$	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$
$\{1\}$	$\{1\}$	$\emptyset$	$\mathcal{U}$	$\{2\}$
$\{2\}$	$\{2\}$	$\mathcal{U}$	$\emptyset$	$\{1\}$
$\mathcal{U}$	$\mathcal{U}$	$\{2\}$	$\{1\}$	$\emptyset$

(a)

$\cdot (\cap)$	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$	$\{1\}$
$\{2\}$	$\emptyset$	$\emptyset$	$\{2\}$	$\{2\}$
$\mathcal{U}$	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$

(b)

EXAMPLE 14.5

For $R = \{a, b, c, d, e\}$ we define $+$ and $\cdot$ by Tables 14.2(a) and (b).

Table 14.2

$+$	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

(a)

$\cdot$	a	b	c	d	e
a	a	a	a	a	a
b	a	b	c	d	e
c	a	c	e	b	d
d	a	d	b	e	c
e	a	e	d	c	b

(b)

Although we do not verify them here, the 125 equalities needed to establish each of the associative laws and the distributive laws all hold, so $(R, +, \cdot)$ turns out to be a finite commutative ring with unity, and it has no proper divisors of zero. The element a is the zero (that is, the additive identity) of R, whereas b is the unity. Here every nonzero element x has a *multiplicative inverse* y, where $xy = yx = b$, the unity. Elements c and d are multiplicative inverses of each other; b is its own inverse, as is e.

We now consider the concept of a multiplicative inverse for a ring element in general.

Definition 14.3

Let R be a ring with unity u. If $a \in R$ and there exists $b \in R$ such that $ab = ba = u$, then b is called a *multiplicative inverse* of a and a is called a *unit* of R. (The element b is also a unit of R.)

In Section 14.2 we shall see that if a ring element does have a multiplicative inverse, then it has only one such inverse. In the meantime, we'll examine two special kinds of ring structures.

Definition 14.4

Let R be a commutative ring with unity. Then

a) R is called an *integral domain* if R has no proper divisors of zero.

b) R is called a *field* if every nonzero element of R is a unit.

The ring $(\mathbf{Z}, +, \cdot)$ is an integral domain but not a field, while $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, under ordinary addition and multiplication, are both integral domains and fields. The ring in Example 14.5 is both an integral domain and a field.

It follows from part (c) of Definition 14.2 that if R is an integral domain or a field, then $|R| \geq 2$.

EXAMPLE 14.6

For our last ring of this section we let $R = \{s, t, v, w, x, y\}$ and $+$ and $\cdot$ are given by Tables 14.3(a) and(b).

Table 14.3

$+$	s	t	v	w	x	y
s	s	t	v	w	x	y
t	t	v	w	x	y	s
v	v	w	x	y	s	t
w	w	x	y	s	t	v
x	x	y	s	t	v	w
y	y	s	t	v	w	x

(a)

$\cdot$	s	t	v	w	x	y
s	s	s	s	s	s	s
t	s	t	v	w	x	y
v	s	v	x	s	v	x
w	s	w	s	w	s	w
x	s	x	v	s	x	v
y	s	y	x	w	v	t

(b)

From these tables we see that $(R, +, \cdot)$ is a commutative ring with unity, but it is neither an integral domain nor a field. The element t is the unity, and t and y are the units of R.

We also note that $vv = vy$, and even though v is not the zero element of R, we cannot cancel and say that $v = y$. So a general ring does *not* satisfy the cancellation law of multiplication that we may sometimes take for granted. We shall look at this idea again in the next section.

EXERCISES 14.1

1. Find the additive inverse for each element in the rings of Examples 14.5 and 14.6.

2. Determine whether or not each of the following sets of numbers is a ring under ordinary addition and multiplication.

a) R = the set of positive integers and zero

b) $R = \{kn | n \in \mathbf{Z}, k \text{ a fixed positive integer}\}$

c) $R = \{a + b\sqrt{2} \mid a, b \in \mathbf{Z}\}$

d) $R = \{a + b\sqrt{2} + c\sqrt{3} \mid a \in \mathbf{Z}, b, c \in \mathbf{Q}\}$

3. Let $(R, +, \cdot)$ be a ring with a, b, c, d elements of R. State the conditions (from the definition of a ring) that are needed to prove each of the following results.

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

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

c) $c(d + b) + ab = (a + c)b + cd$

d) $a(bc) + (ab)d = (ab)(d + c)$

4. For the set R in Example 14.4, keep $A \cdot B = A \cap B$, but define $A + B = A \cup B$. Is $(R, \cup, \cap)$ a ring?

5. Consider the set $\mathbf{Z}$ together with the binary operations $\oplus$ and $\odot$ given in Example 14.3. (a) Verify the associative laws for $\oplus$ and $\odot$ and the distributive laws in order to complete the work started in part (a) of Example 14.3. [This now establishes that $(\mathbf{Z}, \oplus, \odot)$ is a ring.] (b) Is this ring commutative? (c) In part (b) of Example 14.3 we showed that 0 is the unity for $(\mathbf{Z}, \oplus, \odot)$. What are the units for this ring? (d) Is this ring an integral domain? a field?

6. Define the binary operations $\oplus$ and $\odot$ on $\mathbf{Z}$ by $x \oplus y = x + y - 7$, $x \odot y = x + y - 3xy$, for all $x, y \in \mathbf{Z}$. Explain why $(\mathbf{Z}, \oplus, \odot)$ is *not* a ring.

7. Let k, m be fixed integers. Find all values for k, m for which $(\mathbf{Z}, \oplus, \odot)$ is a ring under the binary operations $x \oplus y = x + y - k$, $x \odot y = x + y - mxy$, where $x, y \in \mathbf{Z}$.

8. Tables 14.4(a) and (b) make $(R, +, \cdot)$ into a ring, where $R = \{s, t, x, y\}$. (a) What is the zero for this ring? (b) What is the additive inverse of each element? (c) What is $t(s + xy)$? (d) Is R a commutative ring? (e) Does R have a unity? (f) Find a pair of zero divisors.

9. Define addition and multiplication, denoted by $\oplus$ and $\odot$, respectively, on the set $\mathbf{Q}$ as follows. For $a, b \in \mathbf{Q}$, $a \oplus b =$

Table 14.4

$+$	s	t	x	y
s	y	x	s	t
t	x	y	t	s
x	s	t	x	y
y	t	s	y	x

(a)

$\cdot$	s	t	x	y
s	y	y	x	x
t	y	y	x	x
x	x	x	x	x
y	x	x	x	x

(b)

$a + b + 7$, $a \odot b = a + b + (ab/7)$. (a) Prove that $(\mathbf{Q}, \oplus, \odot)$ is a ring. (b) Is this ring commutative? (c) Does the ring have a unity? What about units? (d) Is this ring an integral domain? a field?

10. Let $(\mathbf{Q}, \oplus, \odot)$ denote the field where $\oplus$ and $\odot$ are defined by

$$a \oplus b = a + b - k, \qquad a \odot b = a + b + (ab/m),$$

for fixed elements k, m ($\neq 0$) of $\mathbf{Q}$. Determine the value for k and the value for m in each of the following.

a) The zero element for the field is 3.

b) The additive inverse of the element 6 is -9.

c) The multiplicative inverse of 2 is $1/8$.

11. Let $R = \{a + bi \mid a, b \in \mathbf{Z},\ i^2 = -1\}$, with addition and multiplication defined by $(a + bi) + (c + di) = (a + c) + (b + d)i$ and $(a + bi)(c + di) = (ac - bd) + (bc + ad)i$, respectively. (a) Verify that R is an integral domain. (b) Determine all units in R.

12. a) Determine the multiplicative inverse of the matrix $\begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix}$ in the ring $M_2(\mathbf{Z})$—that is, find a, b, c, d so that

$$\begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

b) Show that $\begin{bmatrix} 1 & 2 \\ 3 & 8 \end{bmatrix}$ is a unit in the ring $M_2(\mathbf{Q})$ but not a unit in $M_2(\mathbf{Z})$.

13. If $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbf{R})$, prove that $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is a unit of this ring if and only if $ad - bc \neq 0$.

14. Give an example of a ring with eight elements. How about one with 16 elements? Generalize.

15. For $R = \{s, t, x, y\}$, define $+$ and $\cdot$, making R into a ring, by Table 14.5(a) for $+$ and by the partial table for $\cdot$ in Table 14.5(b).

Table 14.5

$+$	s	t	x	y
s	s	t	x	y
t	t	s	y	x
x	x	y	s	t
y	y	x	t	s

(a)

$\cdot$	s	t	x	y
s	s	s	s	s
t	s	t	?	?
x	s	t	?	y
y	s	?	s	?

(b)

a) Using the associative and distributive laws, determine the entries for the missing spaces in the multiplication table.

b) Is this ring commutative?

c) Does it have a unity? How about units?

d) Is the ring an integral domain or a field?

14.2 Ring Properties and Substructures

In each ring of Section 14.1 we were concerned with *the* zero element of the ring and *the* additive inverse of each ring element. It is time now to show, along with other properties, that these elements are truly unique.

THEOREM 14.1 In any ring $(R, +, \cdot)$,

a) the zero element z is unique, and

b) the additive inverse of each ring element is unique.

Proof:

a) If R has more than one additive identity, let z_1, z_2 denote two such elements. Then

$$z_1 \underset{\substack{\uparrow \\ \text{Since } z_2 \text{ is an} \\ \text{additive identity}}}{=} z_1 + z_2 \underset{\substack{\uparrow \\ \text{Since } z_1 \text{ is an} \\ \text{additive identity}}}{=} z_2.$$

b) For $a \in R$, suppose there are two elements $b, c \in R$ where $a + b = b + a = z$ and $a + c = c + a = z$. Then $b = b + z = b + (a + c) = (b + a) + c = z + c = c$. (The reader should supply the condition that establishes each equality.)

As a result of the uniqueness in part (b), from this point on we shall denote *the* additive inverse of $a \in R$ by $-a$. Further, we may now speak of *subtraction* in the ring, where we understand that $a - b = a + (-b)$.

From Theorem 14.1(b) we also obtain the following for any ring R.

THEOREM 14.2 *The Cancellation Laws of Addition.* For all $a, b, c \in R$,

a) $a + b = a + c \Rightarrow b = c$, and

b) $b + a = c + a \Rightarrow b = c$.

Proof:

a) Since $a \in R$, it follows that $-a \in R$ and we have

$$\begin{aligned} a + b = a + c &\Rightarrow (-a) + (a + b) = (-a) + (a + c) \\ &\Rightarrow [(-a) + a] + b = [(-a) + a] + c \\ &\Rightarrow z + b = z + c \Rightarrow b = c. \end{aligned}$$

b) We leave this similar proof for the reader.

Note that when we examine the addition table for a finite ring we find that each element of the ring occurs exactly one time in each row and column of the table. This is a direct consequence of Theorem 14.2 — where part (a) handles the rows and part (b) the columns.

THEOREM 14.3 For any ring $(R, +, \cdot)$ and any $a \in R$, we have $az = za = z$.

Proof: If $a \in R$, then $az = a(z + z)$ because $z + z = z$. Hence $z + az = az = az + az$. (Why?) Using the cancellation law of addition, we have $z = az$.

The proof that $za = z$ is done similarly.

The reader may feel that the result of Theorem 14.3 is obvious. But we are not dealing with just $\mathbf{Z}$ or $\mathbf{Q}$ or $M_2(\mathbf{Z})$. Our objective is to show that *any* ring satisfies such a result, and to get the result we may only use the conditions in the definition of a ring and whatever properties we've derived for arbitrary rings up to this point.

The uniqueness of additive inverses [from part (b) of Theorem 14.1] now implies the following result.

THEOREM 14.4 Given a ring $(R, +, \cdot)$, for all $a, b \in R$,

a) $-(-a) = a$,

b) $a(-b) = (-a)b = -(ab)$, and

c) $(-a)(-b) = ab$.

Proof:

a) By the convention stated after Theorem 14.1, $-(-a)$ denotes *the* additive inverse of $-a$. Since $(-a) + a = z$, a is also an additive inverse for $-a$. Consequently, by the uniqueness of such inverses, $-(-a) = a$.

b) We shall prove that $a(-b) = -(ab)$ and shall leave the other part for the reader. We know that $-(ab)$ denotes *the* additive inverse of ab. However, $ab + a(-b) = a[b + (-b)] = az = z$, by Theorem 14.3, so by the uniqueness of additive inverses, $a(-b) = -(ab)$.

c) Here we establish an idea we have used in algebra since our first encounter with *signed numbers*. "Minus times minus does indeed equal plus," and the proof follows from the properties and definition of a ring. From part (b) we have $(-a)(-b) = -[a(-b)] = -[-(ab)]$, and the result then follows from part (a).

For the operation of multiplication one also finds the following, which is comparable to Theorem 14.1.

THEOREM 14.5 For a ring $(R, +, \cdot)$,

a) if R has a unity, then it is unique, and

b) if R has a unity, and x is a unit of R, then the multiplicative inverse of x is unique.

Proof: The proofs of these results are left to the reader.

As a result of this theorem, when $(R, +, \cdot)$ is a ring with unity, we shall denote *the* unity by u. Furthermore, in such a ring *the* multiplicative inverse of each unit x will be denoted by x^{-1}. Also, one may now restate the definition of a field as a commutative ring F with unity, such that for all $x \in F$, $x \neq z \Rightarrow x^{-1} \in F$.

With this notion to assist us, we examine some further properties and relations between fields and integral domains.

THEOREM 14.6 Let $(R, +, \cdot)$ be a commutative ring with unity. Then R is an integral domain if and only if, for all $a, b, c \in R$ where $a \neq z$, $ab = ac \Rightarrow b = c$. (Hence, a commutative ring with unity that satisfies the *cancellation law of multiplication* is an integral domain.)

Proof: If R is an integral domain and $x, y \in R$, then $xy = z \Rightarrow x = z$ or $y = z$. Now if $ab = ac$, then $ab - ac = a(b - c) = z$, and because $a \neq z$, it follows that $b - c = z$ or $b = c$. Conversely, if R is commutative with unity and R satisfies multiplicative cancellation, then let $a, b \in R$ with $ab = z$. If $a = z$, we are finished. If not, as $az = z$, we can write $ab = az$ and conclude that $b = z$. So there are no proper divisors of zero and R is an integral domain.

Before going on, let us realize that the cancellation law of multiplication does *not* imply the existence of multiplicative inverses. The integral domain $(\mathbf{Z}, +, \cdot)$ satisfies multiplicative cancellation, but it contains only two elements — namely, 1 and -1 — that are units. Hence, an integral domain need not be a field. But what about a field? Is it necessarily an integral domain?

THEOREM 14.7 If $(F, +, \cdot)$ is a field, then it is an integral domain.

Proof: Let $a, b \in F$ with $ab = z$. If $a = z$, we are finished. If not, a has a multiplicative inverse a^{-1} because F is a field. Then

$$ab = z \Rightarrow a^{-1}(ab) = a^{-1}z \Rightarrow (a^{-1}a)b = a^{-1}z \Rightarrow ub = z \Rightarrow b = z.$$

Hence F has no proper divisors of zero and is an integral domain.

In Chapter 5 we found that functions $f: A \to A$ could be one-to-one (or onto) without being onto (or one-to-one). However, if A were *finite*, such a function f was one-to-one if and only if it was onto. (See Theorem 5.11.) The same situation occurs with *finite* integral domains. An integral domain need not be a field, but when it is finite we find that this structure is a field.

THEOREM 14.8 A *finite* integral domain $(D, +, \cdot)$ is a field.

Proof: Since D is finite, we may list the elements of D as $\{d_1, d_2, \ldots, d_n\}$. For $d \in D$, where $d \neq z$, we have $dD = \{dd_1, dd_2, \ldots, dd_n\} \subseteq D$ because D is closed under multiplication. Now $|D| = n$ and $dD \subseteq D$, so if we could show that dD contains n elements, we would have $dD = D$. If $|dD| < n$, then $dd_i = dd_j$, for some $1 \leq i < j \leq n$. But since D is an integral domain and $d \neq z$, we have $d_i = d_j$, when they are supposed to be distinct. So $dD = D$ and for some $1 \leq k \leq n$, $dd_k = u$, the unity of D. Then $dd_k = u \Rightarrow d$ is a unit of D, and since d was chosen arbitrarily, it follows that $(D, +, \cdot)$ is a field.

From the proof of Theorem 14.8 we also realize that when we are dealing with the *nonzero* elements of a finite field, the multiplication table for these elements is such that each element of the field occurs exactly once in each of the rows and columns.

In the next section we shall look at finite fields that are useful in discrete mathematics. Before closing this section, however, let us examine some special subsets of a ring.

When we were dealing with finite state machines in Chapter 6, we saw instances where subsets of the set of internal states gave rise to machines on their own (when the next state and output functions of the original machines were suitably restricted). These were called submachines. Since closed binary operations are special kinds of functions, we encounter a similar idea in the following definition.

Definition 14.5 For a ring $(R, +, \cdot)$, a nonempty subset S of R is called a *subring* of R if $(S, +, \cdot)$—that is, S under the addition and multiplication of R, restricted to S—is a ring.

EXAMPLE 14.7 For every ring R, the subsets $\{z\}$ and R are always subrings of R.

EXAMPLE 14.8

a) The set of all even integers is a subring of $(\mathbf{Z}, +, \cdot)$. In fact, for each $n \in \mathbf{Z}^+$, $n\mathbf{Z} = \{nx \mid x \in \mathbf{Z}\}$ is a subring of $(\mathbf{Z}, +, \cdot)$.

b) $(\mathbf{Z}, +, \cdot)$ is a subring of $(\mathbf{Q}, +, \cdot)$, which is a subring of $(\mathbf{R}, +, \cdot)$, which is a subring of $(\mathbf{C}, +, \cdot)$.

EXAMPLE 14.9

In Example 14.6, the subsets $S = \{s, w\}$ and $T = \{s, v, x\}$ are subrings of R.

The next result characterizes those subsets of a ring that are subrings.

THEOREM 14.9

Given a ring $(R, +, \cdot)$, a nonempty subset S of R is a subring of R if and only if

1) for all $a, b \in S$, we have $a + b, ab \in S$ (that is, S is closed under the binary operations of addition and multiplication defined on R), and
2) for all $a \in S$, we have $-a \in S$.

Proof: If $(S, +, \cdot)$ is a subring of R, then in its own right it satisfies all the conditions of a ring. Hence it satisfies conditions 1 and 2 of the theorem. Conversely, let S be a nonempty subset of R that satisfies conditions 1 and 2. Conditions (a), (b), (e), and (f) of the definition of a ring are inherited by the elements of S, because they are also elements of R. Thus, all we need to verify here is that S has an additive identity. Now $S \neq \emptyset$, so there is an element $a \in S$, and by condition 2, $-a \in S$. Then by condition 1, $z = a + (-a) \in S$.

EXAMPLE 14.10

Consider the ring $(\mathbf{Z}, \oplus, \odot)$ that we examined in Example 14.3 and Exercise 5 of Section 14.1. Here we have $x \oplus y = x + y - 1$ and $x \odot y = x + y - xy$. Now consider the subset $S = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$ of all odd integers. Since, for example, 3 and 5 are in S but the ordinary sum $3 + 5 = 8 \notin S$, this set S is *not* a subring of $(\mathbf{Z}, +, \cdot)$. However, $3 \oplus 5 = 3 + 5 - 1 = 7 \in S$. In fact, for all $a, b \in S$ we have $a \oplus b = a + b - 1$, where $a + b$ is even, and $a + b - 1$ is odd—so $a \oplus b \in S$. Also, $a \odot b = a + b - ab$, where $a + b$ is even and ab is odd—so $a \odot b \in S$. Finally, $-a$ [the additive inverse of a in the ring $(\mathbf{Z}, \oplus, \odot)$] is equal to $2 - a$, which is odd whenever a is odd. Consequently, if $a \in S$ then $-a \in S$, and it follows from Theorem 14.9 that S is a subring of $(\mathbf{Z}, \oplus, \odot)$.

Note that $(\mathbf{Z}^+, +, \cdot)$ satisfies condition 1 in Theorem 14.9, but not condition 2, so it is not a subring of $(\mathbf{Z}, +, \cdot)$.

The result in Theorem 14.9 can also be given as follows.

THEOREM 14.10

For any ring $(R, +, \cdot)$, if $\emptyset \neq S \subseteq R$,

a) then $(S, +, \cdot)$ is a subring of R if and only if for all $a, b \in S$, we have $a - b \in S$ and $ab \in S$;
b) and if S is finite, then $(S, +, \cdot)$ is a subring of R if and only if for all $a, b \in S$, we have $a + b, ab \in S$. (Once again, additional help comes from a finiteness condition.)

Proof: These proofs we leave for the reader.

The next example demonstrates how one might use the first part of the preceding theorem.

EXAMPLE 14.11

Let us consider the ring $R = M_2(\mathbf{Z})$ and the subset

$$S = \left\{ \begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} \middle| \, x, y \in \mathbf{Z} \right\}$$

of R. When $x = y = 0$ it follows that $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S$, and $S \neq \emptyset$. So now we examine any two elements of S — namely, two matrices of the form

$$\begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} v & v+w \\ v+w & v \end{bmatrix},$$

where $x, y, v, w \in \mathbf{Z}$. We find that

$$\begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} - \begin{bmatrix} v & v+w \\ v+w & v \end{bmatrix} = \begin{bmatrix} x-v & (x-v)+(y-w) \\ (x-v)+(y-w) & x-v \end{bmatrix},$$

so S is closed under subtraction. Turning to multiplication we have

$$\begin{aligned}
&\begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix}\begin{bmatrix} v & v+w \\ v+w & v \end{bmatrix} \\
&= \begin{bmatrix} xv+(x+y)(v+w) & x(v+w)+(x+y)v \\ (x+y)v+x(v+w) & (x+y)(v+w)+xv \end{bmatrix} \\
&= \begin{bmatrix} xv+xv+yv+xw+yw & xv+xw+xv+yv \\ xv+yv+xv+xw & xv+yv+xw+yw+xv \end{bmatrix} \\
&= \begin{bmatrix} xv+xv+yv+xw+yw & (xv+xv+yv+xw+yw)+(-yw) \\ (xv+xv+yv+xw+yw)+(-yw) & xv+xv+yv+xw+yw \end{bmatrix},
\end{aligned}$$

so S is also closed under multiplication.

Appealing now to part (a) of Theorem 14.10, one finds that S is a subring of R.

We shall now single out an important type of subring.

Definition 14.6 A nonempty subset I of a ring R is called an *ideal* of R if for all $a, b \in I$ and all $r \in R$, we have (a) $a - b \in I$ and (b) $ar, ra \in I$.

An ideal is a subring, but the converse does not necessarily hold: $(\mathbf{Z}, +, \cdot)$ is a subring of $(\mathbf{Q}, +, \cdot)$ but not an ideal because, for example, $(1/2)9 \notin \mathbf{Z}$ for $(1/2) \in \mathbf{Q}$, $9 \in \mathbf{Z}$. Meanwhile, all the subrings in Example 14.8(a) are ideals of $(\mathbf{Z}, +, \cdot)$.

Looking back to Example 14.10 we see that if $a \in S$, $x \in \mathbf{Z}$, then $a \odot x = a + x - ax$ $(= x \odot a)$, and if x is even (because the case for x odd has already been covered within Example 14.10), then $a + x$ is odd and ax is even, making $a + x - ax$ odd. Consequently, for all $a \in S$ and all $x \in \mathbf{Z}$, $a \odot x$ and $x \odot a$ are in S, so S is an ideal of the ring $(\mathbf{Z}, \oplus, \odot)$.

EXERCISES 14.2

1. Complete the proofs of Theorems 14.2, 14.4, 14.5, and 14.10.

2. If a, b, and c are any elements in a ring $(R, +, \cdot)$, prove that (a) $a(b - c) = ab - (ac) = ab - ac$ and (b) $(b - c)a = ba - (ca) = ba - ca$.

3. **a)** If R is a ring with unity and a, b are units of R, prove that ab is a unit of R and that $(ab)^{-1} = b^{-1}a^{-1}$.

b) For the ring $M_2(\mathbf{Z})$, find A^{-1}, B^{-1}, $(AB)^{-1}$, $(BA)^{-1}$, and $B^{-1}A^{-1}$ if

$$A = \begin{bmatrix} 4 & 7 \\ 1 & 2 \end{bmatrix}, \qquad B = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}.$$

4. Prove that a unit in a ring R cannot be a proper divisor of zero.

5. If a is a unit in ring R, prove that $-a$ is also a unit in R.

6. **a)** Verify that the subsets $S = \{s, w\}$ and $T = \{s, v, x\}$ are subrings of the ring R in Example 14.6. (The binary operations for the elements of S, T are those given in Table 14.3.)

b) Are the subrings in part (a) ideals of R?

7. Let S and T be subrings of a ring R. Prove that $S \cap T$ is a subring of R.

8. Let $R = M_2(\mathbf{Z})$ and let S be the subset of R where

$$S = \left\{ \begin{bmatrix} x & x-y \\ x-y & y \end{bmatrix} \middle| \, x, y \in \mathbf{Z} \right\}.$$

Prove that S is a subring of R.

9. Let $(R, +, \cdot)$ be a ring. If S, T_1, and T_2 are subrings of R, and $S \subseteq T_1 \cup T_2$, prove that $S \subseteq T_1$ or $S \subseteq T_2$.

10. a) Let $(R, +, \cdot)$ be a finite commutative ring with unity u. If $r \in R$ and r is not the zero element of R, prove that r is either a unit or a proper divisor of zero.

b) Does the result in part (a) remain valid when R is infinite?

11. a) For $R = M_2(\mathbf{Z})$, prove that

$$S = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \middle| \, a \in \mathbf{Z} \right\}$$

is a subring of R.

b) What is the unity of R?

c) Does S have a unity?

d) Does S have any properties that R does not have?

e) Is S an ideal of R?

12. Let S and T be the following subsets of the ring $R = M_2(\mathbf{Z})$:

$$S = \left\{ \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} \middle| \, a, b, c \in \mathbf{Z} \right\},$$

$$T = \left\{ \begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix} \middle| \, a, b, c, d \in \mathbf{Z} \right\}.$$

a) Verify that S is a subring of R. Is it an ideal?

b) Verify that T is a subring of R. Is it an ideal?

13. Let $(R, +, \cdot)$ be a commutative ring, and let z denote the zero element of R. For a fixed element $a \in R$, define $N(a) = \{r \in R | ra = z\}$. Prove that $N(a)$ is an ideal of R.

14. Let R be a commutative ring with unity u, and let I be an ideal of R. (a) If $u \in I$, prove that $I = R$. (b) If I contains a unit of R, prove that $I = R$.

15. If R is a field, how many ideals does R have?

16. Let $(R, +, \cdot)$ be the (finite) commutative ring with unity given by Tables 14.6(a) and (b).

Table 14.6

$+$	z	u	a	b
z	z	u	a	b
u	u	z	b	a
a	a	b	z	u
b	b	a	u	z

(a)

$\cdot$	z	u	a	b
z	z	z	z	z
u	z	u	a	b
a	z	a	b	u
b	z	b	u	a

(b)

a) Verify that R is a field.

b) Find a subring of R that is not an ideal.

c) Let x and y be unknowns. Solve the following system of linear equations in R: $bx + y = u$; $x + by = z$.

17. Let R be a commutative ring with unity u.

a) For any (fixed) $a \in R$, prove that $aR = \{ar | r \in R\}$ is an ideal of R.

b) If the only ideals of R are $\{z\}$ and R, prove that R is a field.

18. Let $(S, +, \cdot)$ and $(T, +', \cdot')$ be two rings. For $R = S \times T$, define addition "$\oplus$" and multiplication "$\odot$" by

$$(s_1, t_1) \oplus (s_2, t_2) = (s_1 + s_2, t_1 +' t_2),$$

$$(s_1, t_1) \odot (s_2, t_2) = (s_1 \cdot s_2, t_1 \cdot' t_2).$$

a) Prove that under these closed binary operations, R is a ring.

b) If both S and T are commutative, prove that R is commutative.

c) If S has unity u_S and T has unity u_T, what is the unity of R?

d) If S and T are fields, is R also a field?

19. Let $(R, +, \cdot)$ be a ring with unity u, and $|R| = 8$. On $R^4 = R \times R \times R \times R$, define $+$ and $\cdot$ as suggested by Exercise 18. In the ring R^4, (a) how many elements have exactly two nonzero components? (b) how many elements have all nonzero components? (c) is there a unity? (d) how many units are there if R has four units?

20. Let $(R, +, \cdot)$ be a ring, with $a \in R$. Define $0a = z$, $1a = a$, and $(n+1)a = na + a$, for all $n \in \mathbf{Z}^+$. (Here we are multiplying elements of R by elements of $\mathbf{Z}$, so we have yet another operation that is different from the multiplications in either of $\mathbf{Z}$ or R.) For $n > 0$, we define $(-n)a = n(-a)$, so, for example, $(-3)a = 3(-a) = 2(-a) + (-a) = [(-a) + (-a)] + (-a) = [-(a+a)] + (-a) = -[(a+a)+a] = -[2a+a] = -(3a)$.

For all $a, b \in R$, and all $m, n \in \mathbf{Z}$, prove that

a) $ma + na = (m+n)a$ **b)** $m(na) = (mn)a$

c) $n(a+b) = na + nb$ **d)** $n(ab) = (na)b = a(nb)$

e) $(ma)(nb) = (mn)(ab) = (na)(mb)$

21. a) For ring $(R, +, \cdot)$ and each $a \in R$, we define $a^1 = a$, and $a^{n+1} = a^n a$, for all $n \in \mathbf{Z}^+$. Prove that for all $m, n \in \mathbf{Z}^+$, $(a^m)(a^n) = a^{m+n}$ and $(a^m)^n = a^{mn}$.

b) Can you suggest how we might define a^0 or a^{-n}, $n \in \mathbf{Z}^+$, including any necessary conditions that R must satisfy for these definitions to make sense?

14.3 The Integers Modulo n

Enough abstraction for a while! We shall now concentrate on the construction and use of special finite rings and fields.

Definition 14.7 Let $n \in \mathbf{Z}^+$, $n > 1$. For $a, b \in \mathbf{Z}$, we say that *a is congruent to b modulo n*, and we write $a \equiv b \pmod{n}$, if $n|(a-b)$, or, equivalently, $a = b + kn$ for some $k \in \mathbf{Z}$.

EXAMPLE 14.12

i) We find that $17 \equiv 2 \pmod{5}$, since $17 - 2 = 15 = 3(5)$, or $17 = 2 + 3(5)$.

ii) As $-7 + 49 = -7 - (-49) = 42 = 7(6)$ [or, $-7 = -49 + 7(6)$], we have $-7 \equiv -49 \pmod{6}$.

iii) Since $11 - (-5) = 16 = 2(8)$ [or, $11 = -5 + 2(8)$], it follows that $11 \equiv -5 \pmod{8}$.

Before we examine our first theorem, let us make three observations about this new concept of congruence modulo n. Here, as above, we have $a, b, n \in \mathbf{Z}$, with $n > 1$.

i) Using the division algorithm, we can write $a = q_1 n + r_1$ and $b = q_2 n + r_2$, with $0 \le r_1 < n$, $0 \le r_2 < n$. So $a - b = (q_1 - q_2)n + (r_1 - r_2)$. Then, if $a \equiv b \pmod{n}$, it follows that $n|(a-b)$, and, consequently, $n|(r_1 - r_2)$. But with $0 \le |r_1 - r_2| < n$, we now find that $r_1 = r_2$.

   Hence, if $a \equiv b \pmod{n}$, then a, b have the same remainder upon division by n.

ii) The converse of the result in (i) is also true. That is, if $a = q_1 n + r_1$ and $b = q_2 n + r_2$, with $r_1 = r_2$, then $a - b = (q_1 - q_2)n$ and $a \equiv b \pmod{n}$.

iii) Although $a = b \Rightarrow a \equiv b \pmod{n}$, we can*not* expect $a \equiv b \pmod{n} \Rightarrow a = b$. However, if $a \equiv b \pmod{n}$ and $a, b \in \{0, 1, 2, \ldots, n-1\}$, then $a = b$.

THEOREM 14.11 Congruence modulo n is an equivalence relation on $\mathbf{Z}$.

Proof: The proof is left for the reader.

Since an equivalence relation on a set induces a partition of that set, for $n \ge 2$, congruence modulo n partitions $\mathbf{Z}$ into the n equivalence classes

$$\begin{aligned}
[0] &= \{\ldots, -2n, -n, 0, n, 2n, \ldots\} = \{0 + nx | x \in \mathbf{Z}\} \\
[1] &= \{\ldots, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\} = \{1 + nx | x \in \mathbf{Z}\} \\
[2] &= \{\ldots, -2n+2, -n+2, 2, n+2, 2n+2, \ldots\} = \{2 + nx | x \in \mathbf{Z}\} \\
&\vdots \\
[n-1] &= \{\ldots, -n-1, -1, n-1, 2n-1, 3n-1, \ldots\} \\
&= \{(n-1) + nx | x \in \mathbf{Z}\}.
\end{aligned}$$

For all $t \in \mathbf{Z}$, by the division algorithm (of Section 4.3) we can write $t = qn + r$, where $0 \le r < n$, so $t \in [r]$, or $[t] = [r]$. We use the notation $\mathbf{Z}_n$ to denote $\{[0], [1], [2], \ldots, [n-1]\}$. (When there is no danger of ambiguity, we often replace $[a]$ by a and write $\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$.) Our objective now is to define closed binary operations of addition and multiplication on the set $\mathbf{Z}_n$ of equivalence classes so that we obtain a ring.

For $[a], [b] \in \mathbf{Z}_n$, define $+$ and $\cdot$ by

$$[a] + [b] = [a + b] \quad \text{and} \quad [a] \cdot [b] = [a][b] = [ab].$$

For example, if $n = 7$, then $[2] + [6] = [2 + 6] = [8] = [1]$, and $[2][6] = [12] = [5]$.

Before these definitions are so readily accepted, we must investigate whether or not these (closed binary) operations are *well-defined* in the sense that if $[a] = [c]$, $[b] = [d]$, then $[a] + [b] = [c] + [d]$ and $[a][b] = [c][d]$. Since $[a] = [c]$ can occur with $a \neq c$, do the results of our addition and multiplication depend on which representatives are chosen from the equivalence classes? We shall prove that the results of the two operations are independent of the choice of class representatives and that the operations are very definitely well-defined.

First, we observe that $[a] = [c] \Rightarrow a = c + sn$, for some $s \in \mathbf{Z}$, and $[b] = [d] \Rightarrow b = d + tn$, for some $t \in \mathbf{Z}$. Hence

$$a + b = (c + sn) + (d + tn) = c + d + (s + t)n,$$

so $(a + b) \equiv (c + d) \pmod{n}$ and $[a + b] = [c + d]$. Also,

$$ab = (c + sn)(d + tn) = cd + (sd + ct + stn)n$$

and $ab \equiv cd \pmod{n}$, or $[ab] = [cd]$.

This result now leads us to the following.

THEOREM 14.12 For $n \in \mathbf{Z}^+$, $n > 1$, under the closed binary operations defined above, $\mathbf{Z}_n$ is a commutative ring with unity $[1]$ (and additive identity $[0]$).

Proof: The proof is left to the reader. Verification of the ring properties follows from the definitions of addition and multiplication in $\mathbf{Z}_n$ and from the corresponding properties for the ring $(\mathbf{Z}, +, \cdot)$.

Before stating any further results, let us examine two particular examples, $\mathbf{Z}_5$ and $\mathbf{Z}_6$. In Tables 14.7(a) and (b) and 14.8(a) and (b), we simplify $[a]$ by writing a.

Table 14.7

$\mathbf{Z}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(a)

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(b)

In $\mathbf{Z}_5$ every nonzero element has a multiplicative inverse, so $\mathbf{Z}_5$ is a field. For $\mathbf{Z}_6$, however, 1 and 5 are the only units and 2, 3, 4 are proper divisors of zero. Meanwhile, in $\mathbf{Z}_9$, $3 \cdot 3 = 3 \cdot 6 = 0$, so 3 and 6 are proper divisors of zero. Consequently, for $\mathbf{Z}_n$, $n > 2$, to be a field, we need more than just an odd modulus.

Table 14.8

$\mathbf{Z}_6$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(a)

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(b)

THEOREM 14.13 $\mathbf{Z}_n$ is a field if and only if n is a prime.

Proof: Let n be a prime, and suppose that $0 < a < n$. Then $\gcd(a, n) = 1$, so as we learned in Section 4.4 there are integers s, t with $as + tn = 1$. Thus $as \equiv 1 \pmod{n}$, or $[a][s] = [1]$, and $[a]$ is a unit of $\mathbf{Z}_n$, which is consequently a field.

Conversely, if n is not a prime, then $n = n_1 n_2$, where $1 < n_1, n_2 < n$. So $[n_1] \neq [0]$ and $[n_2] \neq [0]$ but $[n_1][n_2] = [n_1 n_2] = [0]$, and $\mathbf{Z}_n$ is not even an integral domain, so it cannot be a field.

In $\mathbf{Z}_6$, $[5]$ is a unit and $[3]$ is a zero divisor. We seek a way to recognize when $[a]$ is a unit in $\mathbf{Z}_n$, for n composite.

THEOREM 14.14 In $\mathbf{Z}_n$, $[a]$ is a unit if and only if $\gcd(a, n) = 1$.

Proof: If $\gcd(a, n) = 1$, the result follows as in the proof of Theorem 14.13. For the converse, let $[a] \in \mathbf{Z}_n$ and $[a]^{-1} = [s]$. Then $[as] = [a][s] = [1]$, so $as \equiv 1 \pmod{n}$ and $as = 1 + tn$, for some $t \in \mathbf{Z}$. But $1 = as + n(-t) \Rightarrow \gcd(a, n) = 1$.

EXAMPLE 14.13 Find $[25]^{-1}$ in $\mathbf{Z}_{72}$.

Since $\gcd(25, 72) = 1$, the Euclidean algorithm leads us to

$$\begin{aligned} 72 &= 2(25) + 22, & 0 < 22 < 25 \\ 25 &= 1(22) + 3, & 0 < 3 < 22 \\ 22 &= 7(3) + 1, & 0 < 1 < 3. \end{aligned}$$

As 1 is the last nonzero remainder, we have

$$\begin{aligned} 1 &= 22 - 7(3) = 22 - 7[25 - 22] = (-7)(25) + (8)(22) \\ &= (-7)(25) + 8[72 - 2(25)] = 8(72) - 23(25). \end{aligned}$$

But

$$1 = 8(72) - 23(25) \Rightarrow 1 \equiv (-23)(25) \equiv (-23 + 72)(25) \pmod{72},$$

so $[1] = [49][25]$ and $[25]^{-1} = [49]$ in $\mathbf{Z}_{72}$.

In addition, from this result we are now able to solve the following linear congruences for x:

1) If $25x \equiv 1 \pmod{72}$, then $x \equiv 49 \pmod{72}$.

2) If $25x \equiv 3 \pmod{72}$, then $x \equiv 49 \cdot 3 \pmod{72} \equiv 3 \pmod{72}$.

Now [25] is a unit in $\mathbf{Z}_{72}$, but is there any way of knowing how many units this ring has? From Theorem 14.14, if $1 \leq a < 72$, then $[a]^{-1}$ exists if and only if $\gcd(a, 72) = 1$. Consequently, the number of units in $\mathbf{Z}_{72}$ is the number of integers a, such that $1 \leq a < 72$ and $\gcd(a, 72) = 1$. Using Euler's phi function (Example 8.8), we find that this is

$$\phi(72) = \phi(2^3 3^2) = (72)[1 - (1/2)][1 - (1/3)] = (72)(1/2)(2/3) = 24.$$

In general, for any $n \in \mathbf{Z}^+$, $n > 1$, there are $\phi(n)$ units and $n - 1 - \phi(n)$ proper divisors of zero in $\mathbf{Z}_n$.

Before we continue with some examples where congruence plays a role, we want to look back at the binary operation **mod** that was introduced earlier in Examples 4.36 and 10.8. In those examples we considered $x, y \in \mathbf{Z}^+$ and defined x **mod** y as the remainder obtained when we divide x by y. At this point we shall extend this concept to include the case where $x \leq 0$. Hence, for $x \in \mathbf{Z}$ and $y \in \mathbf{Z}^+$, x **mod** y is the remainder that results upon division of x by y.

But, now, how is **mod** related to the mod of Definition 14.7? Here we find that if $a, b, n \in \mathbf{Z}$, with $n > 1$, then $a \equiv b \pmod{n}$ if and only if a **mod** $n = b$ **mod** n. (This follows from the observations we made prior to Theorem 14.11.)

And now the time has arrived for some additional examples.

EXAMPLE 14.14

Randomly generated numbers arise in many applications. In particular, they are often used for the computer simulation of experiments that are too expensive, too dangerous, or just plain impossible to conduct in the real world.

The idea of using a computer to generate random numbers was first developed by John von Neumann (1903–1957) in 1946. However, although these numbers may *appear* to be random, they are not — hence the title *pseudorandom* numbers.

Proposed in 1949 by Derrick H. Lehmer (1905–1991), the most commonly used technique for generating such pseudorandom numbers employs the notion of congruence. For the *linear congruential generator*, one starts with the four integers: the multiplier a, the increment c, the modulus m, and the seed x_0, where

$$2 \leq a < m, \qquad 0 \leq c < m, \qquad \text{and} \qquad 0 \leq x_0 < m.$$

These nonnegative integers are used to generate a sequence of pseudorandom numbers, $x_1, x_2, x_3, \ldots$, recursively, by

$$x_{n+1} = (ax_n + c) \textbf{ mod } m.$$

So $0 \leq x_{n+1} < m$, for $n \geq 0$. For example, if $a = 3$, $c = 2$, $m = 11$, and $x_0 = 1$, then

$$x_1 = (ax_0 + c) \textbf{ mod } m = [3(1) + 2] \textbf{ mod } 11 = 5, \text{ so } x_1 = 5.$$

Similarly, $x_2 = (ax_1 + c)$ **mod** $m = [3(5) + 2]$ **mod** $11 = 17$ **mod** $11 = 6$, so $x_2 = 6$.

Continuing in this manner, one finds that $x_3 = 9$, $x_4 = 7$, and $x_5 = 1$, the seed. Consequently, this linear congruential generator produces five distinct integers before repeating. The sequence of pseudorandom numbers thus obtained is 1, 5, 6, 9, 7, 1, 5, 6, ...

With $a = 3, c = 5, m = 12$, and $x_0 = 6$, we first learn that $x_1 = [3(6) + 5]$ **mod** $12 = 11$, so $x_1 = 11$. Next, $x_2 = [3(11) + 5]$ **mod** $12 = 38$ **mod** $12 = 2$, so $x_2 = 2$. Further computation yields $x_3 = 11$. This time the linear congruential generator yields only three distinct integers before repeating. The sequence of pseudorandom numbers generated here is 6, 11, 2, 11, 2, 11, 2, . . . , where the seed is not repeated.

In practice large values for a and m are used — especially for critical simulations. For $a = 16{,}807$ $(= 7^5)$, $c = 0$, $m = 2{,}147{,}483{,}647$ $(= 2^{31} - 1$, a prime), and $x_0 = 1$, one obtains a sequence of 2,147,483,647 pseudorandom numbers before a repeated integer appears.

EXAMPLE 14.15

a) Whether it's youngsters using decoder rings or military leaders sending battle plans to troops, throughout history, various people have wanted to keep certain information unintelligible, should it fall into the wrong hands.

As early as the first century B.C., the Roman general Gaius Julius Caesar (100 B.C.–44 B.C.) used a *cipher shift* to make the contents of certain messages understandable only for those he intended the messages to reach. To describe this early form of *cryptosystem* — often termed the *Caesar cipher* — we shall make certain conventions to simplify the presentation. First, we shall write the original message, the *plaintext*, using only lowercase letters, with no punctuation or spaces. Then to encrypt the plaintext, each lowercase letter, from a to w, is *shifted* to the letter three places forward in the alphabet, and the last three letters — namely, x, y, and z — are shifted to the first three letters, respectively. We use the uppercase letters for the resulting *ciphertext*. Consequently, a is encrypted as D, b as E, c as F, . . . , j as M, . . . , m as P, . . . , y as B, and z as C.

If Caesar wanted to inform a senator in Rome of a recent victory, he might have sent the message "I came, I saw, I conquered." Encryption of this message takes place as follows:

Plaintext	*i*	*c*	*a*	*m*	*e*	*i*	*s*	*a*	*w*	*i*	*c*	*o*	*n*	*q*	*u*	*e*	*r*	*e*	*d*
Ciphertext	*L*	*F*	*D*	*P*	*H*	*L*	*V*	*D*	*Z*	*L*	*F*	*R*	*Q*	*T*	*X*	*H*	*U*	*H*	*G*

Upon receiving the ciphertext, as long as this senator knows the size and direction of the shift, he can reverse the process. Decryption then results by replacing each uppercase letter, from D to Z, in the ciphertext by the lowercase letter three places back in the alphabet, and A by x, B by y, and C by z. After decrypting, one then inserts the appropriate spaces and punctuation in the plaintext. (Note that by removing spaces in the plaintext, the resulting absence of spaces in the ciphertext helps make the message more unintelligible. If one does not know the size and direction of the shift for decryption, the presence of spaces may suggest certain information about the structure of the original message.)

b) The idea of Caesar's cipher can be generalized and modeled mathematically by using the concept of congruence. Start by assigning each of the 26 letters of the plaintext a nonnegative integer as shown:

a	b	c	d	$\cdots$	k	ℓ	m	n	$\cdots$	w	x	y	z
0	1	2	3	$\cdots$	10	11	12	13	$\cdots$	22	23	24	25

The 26 letters for the ciphertext are assigned the same integers — that is, A is assigned 0, B is assigned 1, . . . , Y is assigned 24, and Z is assigned 25.

Now select a nonnegative integer κ, where $0 \leq \kappa \leq 25$. For instance, Caesar chose $\kappa = 3$. This integer κ is called the *key* and helps us define the encrypting function $E: \mathbf{Z}_{26} \to \mathbf{Z}_{26}$ as follows. Given a letter of the plaintext, let θ be the nonnegative integer to which it corresponds. Then $E(\theta) = (\theta + \kappa)$ **mod** 26 and this result determines the corresponding ciphertext letter for the plaintext letter assigned the nonnegative integer θ. To decrypt we apply the inverse function $D: \mathbf{Z}_{26} \to \mathbf{Z}_{26}$ where we write $D(\theta) = (\theta - \kappa)$ **mod** 26. Replacing each nonnegative integer with its corresponding plaintext letter, one captures the plaintext version of the original message.

If we do not know the key, a trial-and-error approach can be used. There are 26 possibilities — one for each of the 26 possible values of κ. A more efficient method of attack takes into account the most frequently occurring letters in the alphabet and the most frequently occurring letters in the ciphertext. In the English language, the letter e occurs most often, with t, a, o and i the next four most frequently occurring letters.

Now if a parent receives the ciphertext $Z\ L\ U\ K\ T\ V\ Y\ L\ T\ V\ U\ L\ F$ from a college student, and does not know the key, what can the parent do? Since the most frequently occurring letter in the ciphertext is L, the parent can correspond e with L under the encryption. This suggests that $E: \mathbf{Z}_{26} \to \mathbf{Z}_{26}$ be defined by $E(\theta) = (\theta + 7)$ **mod** 26, since L is seven places after e in the alphabet. So here the key, κ, is 7 and the decryption function is $D: \mathbf{Z}_{26} \to \mathbf{Z}_{26}$ with $D(\theta) = (\theta - 7)$ **mod** 26.

Decoding the ciphertext message received by the parent can be analyzed as follows:

(1)	Z	L	U	K	T	V	Y	L	T	V	U	L	F
(2)	25	11	20	10	19	21	24	11	19	21	20	11	5
(3)	18	4	13	3	12	14	17	4	12	14	13	4	24
(4)	s	e	n	d	m	o	r	e	m	o	n	e	y

Here (1) provides the given (encrypted) ciphertext. In (2) each ciphertext letter is replaced by the nonnegative integer assigned to it. Upon applying the decryption function D, the results in (2) provide the assignments in (3). Replacing each nonnegative integer in (3) by its corresponding plaintext letter yields the original message

"Send more money."

c) The security of the shift cipher in part (b) can be slightly enhanced by means of the *affine cipher*. The letters of the plaintext and ciphertext are assigned nonnegative integers, as in part (b). Here, however, the encryption function E is given by $E(\theta) = (\alpha\theta + \kappa)$ **mod** 26, where $0 \leq \alpha, \kappa \leq 25$, and $\gcd(\alpha, 26) = 1$.

If $\theta_1, \theta_2 \in \mathbf{Z}_{26}$, then $E(\theta_1) = E(\theta_2) \Rightarrow (\alpha\theta_1 + \kappa)$ **mod** $26 = (\alpha\theta_2 + \kappa)$ **mod** $26 \Rightarrow \alpha\theta_1$ **mod** $26 = \alpha\theta_2$ **mod** $26 \Rightarrow \theta_1 = \theta_2$, by Theorem 14.14. So E is one-to-one. Further, E is also onto and invertible, by Theorem 5.11, because $\mathbf{Z}_{26}$ is finite.

Let us consider a specific example. Suppose $\alpha = 11$ and $\kappa = 7$. Then the encryption of the plaintext letter g proceeds as follows:

i) g is assigned the nonnegative integer 6;

ii) applying E, we have $E(6) = (11 \cdot 6 + 7)$ **mod** $26 = 73$ **mod** $26 = 21$; and

iii) the nonnegative integer 21 determines the ciphertext letter V.

[So using this affine cipher, where $E(\theta) = (11\theta + 7)$ **mod** 26, the plaintext letter g is encrypted as the ciphertext letter V.]

Now suppose we have the following ciphertext for a message encrypted by an affine cipher:

$$QYYFGCULBLKYZVOSTCOYPURGCULYZYWKYOSTCOYL$$

With no knowledge of α or κ, one might have to examine as many as $[\phi(26)](26) = \left[26\left(1-\frac{1}{2}\right)\left(1-\frac{1}{13}\right)\right](26) = \left[26\left(\frac{1}{2}\right)\left(\frac{12}{13}\right)\right](26) = (12)(26) = 312$ cases for the key α, κ. However, let's say that by some means — perhaps by considering the frequencies of occurrence for the letters in the plaintext and ciphertext — we deduce two correspondences. Specifically, we know that e and Y correspond, as do t and R. In addition, the nonnegative integers 4 and 19 are the replacements for the plaintext letters e and t, respectively, while 24 and 17 are the respective replacements for Y and R, in the ciphertext, so the encryption function E is determined as follows:

1) The correspondence of $e(4)$ and $Y(24)$ tells us that $E(4) = (4\alpha + \kappa)$ **mod** $26 = 24$.

2) The correspondence of $t(19)$ and $R(17)$ tells us that $E(19) = (19\alpha + \kappa)$ **mod** $26 = 17$.

Consequently, $E(19) - E(4) = [(19\alpha + \kappa) - (4\alpha + \kappa)]$ **mod** $26 = 15\alpha$ **mod** $26 = (17 - 24)$ **mod** $26 = -7$ **mod** $26 = 19$. Since $15 \cdot 7 = 105 = 1 + 104 = 1 + 4(26)$, we have $15 \cdot 7 = 1$ **mod** 26, so $15^{-1} = 7$ (in $\mathbf{Z}_{26}$). Then $15\alpha = 19$ **mod** $26 \Rightarrow$ $\alpha = 15^{-1} \cdot 19$ **mod** $26 = 7 \cdot 19$ **mod** $26 = 133$ **mod** $26 = 3$, as $133 = 3 + 5(26)$. With $\alpha = 3$ **mod** 26 it now follows from (1) that $\kappa = (24 - 4\alpha)$ **mod** $26 = (24 - 12)$ **mod** $26 = 12$. [Or, from (2), $\kappa = (17 - 19\alpha)$ **mod** $26 = (17 - 57)$ **mod** $26 = -40$ **mod** $26 = 12$.]

Consequently, $E\colon \mathbf{Z}_{26} \to \mathbf{Z}_{26}$ is defined by $E(\theta) = (3\theta + 12)$ **mod** 26 and the decryption function $D\colon \mathbf{Z}_{26} \to \mathbf{Z}_{26}$ is given by $D(\theta) = (9\theta + 22)$ **mod** 26, since $E^{-1}(\theta) = 3^{-1}(\theta - 12)$ **mod** $26 = 9(\theta - 12)$ **mod** $26 = (9\theta - 108)$ **mod** $26 = (9\theta + 22)$ **mod** 26. This function D is used in the following to obtain the results in row 3 from the nonnegative integers (that replace the ciphertext letters) in row 2.

(1)	Ciphertext	Q	Y	Y	F	G	C	U	L	B	L	K	Y	Z	V	O	S	T	C	O	Y
(2)		16	24	24	5	6	2	20	11	1	11	10	24	25	21	14	18	19	2	14	24
(3)		10	4	4	15	24	14	20	17	5	17	8	4	13	3	18	2	11	14	18	4
(4)	Plaintext	k	e	e	p	y	o	u	r	f	r	i	e	n	d	s	c	ℓ	o	s	e

(1)	Ciphertext	P	U	R	G	C	U	L	Y	Z	Y	W	K	Y	O	S	T	C	O	Y	L
(2)		15	20	17	6	2	20	11	24	25	24	22	10	24	14	18	19	2	14	24	11
(3)		1	20	19	24	14	20	17	4	13	4	12	8	4	18	2	11	14	18	4	17
(4)	Plaintext	b	u	t	y	o	u	r	e	n	e	m	i	e	s	c	ℓ	o	s	e	r

Here, for example, the ciphertext letter Q is replaced by the nonnegative integer 16. Applying the decryption function D to 16 we have $D(16) = (9 \cdot 16 + 22)$ **mod** $26 = 166$ **mod** $26 = 10$, and 10 is the nonnegative integer that corresponds to the plaintext letter k.

The decrypted message now reveals the sage advice given by Don Vito Corleone (of Mario Puzo's *The Godfather*) to his youngest son, Michael — namely, "Keep your friends close but your enemies closer."

The security of each of the cryptosystems in Example 14.15 depends on the key [$\kappa = 3$ in part (a), κ in part (b), and α, κ in part (c)]. For such *private key cryptosystems*, the two people wishing to use the system need to securely exchange the key. Should any unauthorized person discover the key, then that person could readily encrypt or decrypt messages.

Our next example deals with modular exponentiation.

EXAMPLE 14.16

In the study of cryptology† one often needs to perform modular exponentiation to compute a result such as b^e **mod** n, where b, e, and n are large integers. To demonstrate this — on a somewhat smaller scale — let us determine 5^{143} **mod** 222. We realize that it is rather inefficient to actually compute 5^{143} (a very large integer) and then find the remainder upon dividing the result (for 5^{143}) by 222. A more efficient approach starts with the binary representation for the exponent — here, 143. With

$$\begin{aligned} 143 &= 1(128) + 0(64) + 0(32) + 0(16) + 1(8) + 1(4) + 1(2) + 1(1) \\ &= 1(2^7) + 0(2^6) + 0(2^5) + 0(2^4) + 1(2^3) + 1(2^2) + 1(2^1) + 1(2^0) \\ &= (10001111)_2, \end{aligned}$$

we compute 5^{143} **mod** 222 by using the binary representation (of 143) in reverse order — that is, going from the right to the left. The pseudocode procedure in Fig. 14.1 provides the necessary steps for this computation. Here the input is an integer b, the positive integer n (the modulus), and the binary representation $(a_m a_{m-1} \cdots a_2 a_1 a_0)_2$ for the exponent e, another positive integer. The output x equals b^e **mod** n.

```
procedure ModularExponentiation(b: integer;
                    n, e = (a_m a_{m-1} ··· a_2 a_1 a_0)_2: positive integers)
begin
  x := 1
  power := b mod n
  for i = 0 to m do
    begin
      if a_i = 1 then x := (x * power) mod n
      power := (power * power) mod n
    end
end
```

Figure 14.1

For our example, $b = 5$, $e = 143 = (10001111)_2 = (a_7 a_6 a_5 \cdots a_2 a_1 a_0)_2$ [so $m = 7$], and $n = 222$. The results in Table 14.9 show us the steps that are followed in the execution of the **for** loop. This is after the initial assignments are made: x is 1 and *power* is b **mod** n — that is, 5 **mod** 222 = 5.

Following the execution of this procedure, the last entry in the column for x tells us that 5^{143} **mod** 222 is 89.

---

†For more on cryptology (and related topics), the reader should find the references by T. H. Barr [3], P. Garrett [6], and W. Trappe and L. C. Washington [13] of interest.

Table 14.9

i	a_i	x	*power*
0	1	$1 * 5 = 5$	5^2 (= 25) **mod** 222 = 25
1	1	$5 * 25$ **mod** 222 = 125	25^2 (= 625) **mod** 222 = 181
2	1	$125 * 181$ **mod** 222 = 203	181^2 (= 32761) **mod** 222 = 127
3	1	$203 * 127$ **mod** 222 = 29	127^2 (= 16129) **mod** 222 = 145
4	0	29	145^2 (= 21025) **mod** 222 = 157
5	0	29	157^2 (= 24649) **mod** 222 = 7
6	0	29	7^2 (= 49) **mod** 222 = 49
7	1	$29 * 49$ **mod** 222 = 89	49^2 (= 2401) **mod** 222 = 181

The next example provides an application of modular congruence in information retrieval.

EXAMPLE 14.17

When searching a table of records stored in a computer, each record is assigned a memory location or *address* in the computer's memory. The record itself is often made up of fields (this has nothing to do with ring structures). For instance, a college registrar keeps a record on each student, with the record containing information on the student's social security number, name, and major, for a total of three fields.

In searching for a particular student's record, we can use his or her social security number as the *key* to the record because it uniquely identifies that record. As a result, we develop a function from the set of keys to the set of addresses in the table.

If the college is small enough, we may find that the first four digits of the social security number are enough for identification. We develop a *hashing* (or *scattering*) function h from the set of keys (still social security numbers) to the set of addresses, determined now by the first four digits of the key. For example, h(081-37-6495) identifies the record at the address associated with 0813. In this way we can store the table using at most 10,000 addresses. All is well as long as h is one-to-one. Should a second student have social security number 081-39-0207, then h would no longer uniquely identify a student's record. When this happens, a *collision* is said to occur. Since increasing the size of the stored table often results in more unused storage, we must balance the cost of this storage against the cost of handling such collisions. Techniques for resolving collisions have been devised. They depend on the data structures (such as vectors or linear linked lists) that are used to store the records.

Different kinds of hashing functions that have been developed include the following.

a) The *division* method: Here we restrict the number of addresses we want to use to a fixed integer n. For any key k (a positive integer), we define $h(k) = r$, where $r = k$ **mod** n — that is, $r \equiv k \pmod{n}$ and $0 \leq r < n$.

b) Often implemented is the *folding* method, where the key is split into parts and the parts are added together to give h(key). For example, h(081-37-6495) = 081 + 37 + 6495 = 6613 utilizes folding, and if we want only three-digit addresses, suppressing the first digit 6, we can have h(081-37-6495) = 613.

The importance of choosing a pertinent hashing function cannot be emphasized enough as we try to improve efficiency in terms of greater speed and less unused storage.

Using the modular concept, we can develop a hashing function h, using the same keys as above, where

$$h(x_1x_2x_3\text{-}x_4x_5\text{-}x_6x_7x_8x_9) = y_1y_2y_3,$$

with

$$y_1 = (x_1 + x_2 + x_3) \textbf{ mod } 5$$
$$y_2 = (x_4 + x_5) \textbf{ mod } 3$$
$$y_3 = (x_6 + x_7 + x_8 + x_9) \textbf{ mod } 7.$$

Here, for example, $h(081\text{-}37\text{-}6495) = 413$.

Our last example for this section provides one more encounter with the Catalan numbers (of Sections 1.5 and 10.5).

EXAMPLE 14.18

In how many ways can we select three elements a, b, c from $\{0, 1, 2, 3\}$, if *repetitions are allowed* and we want $a + b + c \equiv 0 \pmod 4$? The selections are listed in column 1 of Table 14.10. (Here each selection sums to 0, 4, or 8, and order is *not* relevant. For instance, $a = 0$, $b = 1$, $c = 3$ is considered the same selection as $a = 1$, $b = 0$, $c = 3$.) We see that there are five such selections and we recall that $5 = \left(\frac{1}{3+1}\right)\binom{2\cdot 3}{3}$, the third Catalan number. Furthermore, by adding 1 to each entry of the selection 0, 0, 0 (in row 1 and column 1) we obtain the selection 1, 1, 1 (in row 1 and column 2). Likewise, the selection 2, 3, 1 (in row 2 and column 3) arises by adding 2 to each entry of the selection 0, 1, 3 (in row 2 and column 1) and reducing each sum modulo 4. Similar computations provide the other 13 selections in columns 2, 3, 4.

Table 14.10

Sum Is 0 (mod 4)	Sum Is 3 (mod 4)	Sum Is 2 (mod 4)	Sum Is 1 (mod 4)
0, 0, 0	1, 1, 1	2, 2, 2	3, 3, 3
0, 1, 3	1, 2, 0	2, 3, 1	3, 0, 2
0, 2, 2	1, 3, 3	2, 0, 0	3, 1, 1
1, 1, 2	2, 2, 3	3, 3, 0	0, 0, 1
2, 3, 3	3, 0, 0	0, 1, 1	1, 2, 2

To generalize this result, we count the number of selections $x_1, x_2, \ldots, x_n$, from $\{0, 1, 2, 3, \ldots, n\}$, where repetitions are allowed and $x_1 + x_2 + \cdots + x_n \equiv 0 \pmod{n+1}$. From Section 1.4 we know there are $\binom{(n+1)+n-1}{n} = \binom{2n}{n}$ ways to select n objects from $n + 1$ distinct objects, with repetitions allowed. Let Sel_n denote the set of these $\binom{2n}{n}$ selections. (The 20 selections in Table 14.10 illustrate Sel_3.) Define the relation $\mathcal{R}$ on Sel_n by $s_1 \mathcal{R} s_2$, if the sum of the entries in selection s_1 is the same, *modulo* $n + 1$, as the sum of the entries in selection s_2. Then $\mathcal{R}$ is an equivalence relation, so Sel_n can be partitioned into $n + 1$ equivalence classes (one for each of the selection sums $0, 1, 2, \ldots, n$—taken *modulo* $n + 1$). [*Note*: We get all $n + 1$ possible selection sums, for if $0 \le k_1 \le n$, $0 \le k_2 \le n$, and $nk_1 \equiv nk_2 \pmod{n+1}$, then $k_1 \equiv k_2 \pmod{n+1}$. This is due to Theorem 14.14 since $\gcd(n, n+1) = 1$. With $k_1, k_2 \in \{0, 1, \ldots, n\}$ it then follows that $k_1 = k_2$.]

For $0 \le s \le n$, let Sel_n^s denote the selections that sum to s, *modulo* $n + 1$. When $1 \le s \le n$, write $s = nk$ (for $k = n^{-1}s$). Define $f: Sel_n^0 \to Sel_n^s$ as follows. For

$\{x_1, x_2, \ldots, x_n\} \in Sel_n^0$, $f(\{x_1, x_2, \ldots, x_n\}) = \{x_1 + k, x_2 + k, \ldots, x_n + k\}$, where $x_i + k$ is reduced *modulo* $n + 1$. Now consider $\{y_1, y_2, \ldots, y_n\} \in Sel_n^s$ and define $g: Sel_n^s \to Sel_n^0$ by $g(\{y_1, y_2, \ldots, y_n\}) = \{y_1 + (n + 1 - k), y_2 + (n + 1 - k), \ldots, y_n + (n + 1 - k)\}$. One finds that $g = f^{-1}$ so $|Sel_n^0| = |Sel_n^1| = \cdots = |Sel_n^n|$. Consequently, each equivalence class has the same size, namely, $\left(\frac{1}{n+1}\right)\binom{2n}{n}$, the nth Catalan number.

EXERCISES 14.3

1. **a)** Determine whether each of the following pairs of integers is congruent modulo 8.

i) 62, 118 **ii)** −43, −237 **iii)** −90, 230

b) Determine whether each of the following pairs of integers is congruent modulo 9.

i) 76, 243 **ii)** −137, 700 **iii)** −56, −1199

2. For each of the following determine the value(s) of the integer $n > 1$ for which the given congruence is true.

a) $28 \equiv 6 \pmod{n}$ **b)** $68 \equiv 37 \pmod{n}$

c) $301 \equiv 233 \pmod{n}$ **d)** $49 \equiv 2 \pmod{n}$

3. List four elements in each of the following equivalence classes.

a) $[1]$ in $\mathbf{Z}_7$ **b)** $[2]$ in $\mathbf{Z}_{11}$ **c)** $[10]$ in $\mathbf{Z}_{17}$

4. Prove that if $a, b, c, n \in \mathbf{Z}$ with $a, n > 0$, and $b \equiv c \pmod{n}$, then $ab \equiv ac \pmod{an}$.

5. Let $a, b, m, n \in \mathbf{Z}$ with $m, n > 0$. Prove that if $a \equiv b \pmod{n}$ and $m|n$, then $a \equiv b \pmod{m}$.

6. Let $m, n \in \mathbf{Z}^+$ with $\gcd(m, n) = 1$ and let $a, b \in \mathbf{Z}$. Prove that $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ if and only if $a \equiv b \pmod{mn}$.

7. Provide a counterexample to show that the result in the preceding exercise is false if $\gcd(m, n) > 1$.

8. Prove that for all integers n exactly one of n, $2n - 1$, and $2n + 1$ is divisible by 3.

9. If $n \in \mathbf{Z}^+$ and $n > 2$ prove that

$$\sum_{i=1}^{n-1} i \equiv \begin{cases} 0 \pmod{n}, & n \text{ odd} \\ \frac{n}{2} \pmod{n}, & n \text{ even.} \end{cases}$$

10. Complete the proofs of Theorems 14.11 and 14.12.

11. Define relation $\mathcal{R}$ on $\mathbf{Z}^+$ by $a \mathcal{R} b$, if $\tau(a) = \tau(b)$, where $\tau(a) =$ the number of positive (integer) divisors of a. For example, $2 \mathcal{R} 3$ and $4 \mathcal{R} 25$ but $5 \not\mathcal{R} 9$.

a) Verify that $\mathcal{R}$ is an equivalence relation on $\mathbf{Z}^+$.

b) For the equivalence classes $[a]$ and $[b]$ induced by $\mathcal{R}$, define operations of addition and multiplication by $[a] + [b] = [a + b]$ and $[a][b] = [ab]$. Are these operations well-defined [that is, does $a \mathcal{R} c$, $b \mathcal{R} d \Rightarrow (a + b) \mathcal{R} (c + d)$, $(ab) \mathcal{R} (cd)$]?

12. Find the multiplicative inverse of each element in $\mathbf{Z}_{11}$, $\mathbf{Z}_{13}$, and $\mathbf{Z}_{17}$.

13. Find $[a]^{-1}$ in $\mathbf{Z}_{1009}$ for (a) $a = 17$, (b) $a = 100$, and (c) $a = 777$.

14. **a)** Find all subrings of $\mathbf{Z}_{12}$, $\mathbf{Z}_{18}$, and $\mathbf{Z}_{24}$.

b) Construct the Hasse diagram for each of these collections of subrings, where the partial order arises from set inclusion. Compare these diagrams with those for the set of positive divisors of n ($n = 12$; 18; 24), where the partial order now comes from the divisibility relation.

c) Find the formula for the number of subrings in $\mathbf{Z}_n$, $n > 1$.

15. How many units and how many (proper) zero divisors are there in (a) $\mathbf{Z}_{17}$? (b) $\mathbf{Z}_{117}$? (c) $\mathbf{Z}_{1117}$?

16. Prove that in any list of n consecutive integers, one of the integers is divisible by n.

17. If three distinct integers are randomly selected from the set $\{1, 2, 3, \ldots, 1000\}$, what is the probability that their sum is divisible by 3?

18. **a)** For $c, d, n, m \in \mathbf{Z}$, with $n > 1$ and $m > 0$, prove that if $c \equiv d \pmod{n}$, then $mc \equiv md \pmod{n}$ and $c^m \equiv d^m \pmod{n}$.

b) If $x_n x_{n-1} \cdots x_1 x_0 = x_n \cdot 10^n + \cdots + x_1 \cdot 10 + x_0$ denotes an $(n + 1)$-digit integer, then prove that

$$x_n x_{n-1} \cdots x_1 x_0 \equiv x_n + x_{n-1} + \cdots + x_1 + x_0 \pmod{9}.$$

19. **a)** Prove that for all $n \in \mathbf{N}$, $10^n \equiv (-1)^n \pmod{11}$.

b) Consider the result for mod 9 in part (b) of Exercise 18. State and prove a comparable result for mod 11.

20. For p a prime determine all elements $a \in \mathbf{Z}_p$ where $a^2 = a$.

21. For $a, b, n \in \mathbf{Z}^+$ and $n > 1$, prove that $a \equiv b \pmod{n} \Rightarrow \gcd(a, n) = \gcd(b, n)$.

22. **a)** Show that for all $[a] \in \mathbf{Z}_7$, if $[a] \neq [0]$, then

$$[a]^6 = [1].$$

b) Let $n \in \mathbf{Z}^+$ with $\gcd(n, 7) = 1$. Prove that

$$7 | (n^6 - 1).$$

23. Use the Caesar cipher to encrypt the plaintext: "All Gaul is divided into three parts."

24. The ciphertext $FTQIMKIQIQDQ$ was encrypted using the encryption function $E: \mathbf{Z}_{26} \to \mathbf{Z}_{26}$ where $E(\theta) = (\theta + \kappa)$ **mod** 26. Considering the frequencies of occurrence for the letters in the ciphertext, determine (a) the key κ for this

cipher shift; (b) the decryption function D; and (c) the original (plaintext) message.

25. Determine the total number of affine ciphers for an alphabet of (a) 24 letters; (b) 25 letters; (c) 27 letters; and (d) 30 letters.

26. The ciphertext

$$RWJWQTOOMYHKUXGOEMYP$$

was encrypted with an affine cipher. Given that the plaintext letters e, t are encrypted as the ciphertext letters W, X, respectively, determine (a) the encryption function E; (b) the decryption function D; and (c) the original (plaintext) message.

27. (a) How many distinct terms does the linear congruential generator with $a = 5$, $c = 3$, $m = 19$, and $x_0 = 10$, produce? (b) What is the sequence of pseudorandom members generated?

28. Given the modulus m and the two seeds x_0, x_1, with $0 < x_0, x_1 < m$, a sequence of pseudorandom numbers can be generated recursively from $x_n = (x_{n-1} + x_{n-2})$ **mod** m, $n \geq 2$. This generator is called the *Fibonacci generator.*

Find the first ten pseudorandom numbers generated when $m = 37$ and $x_0 = 1$, $x_1 = 28$.

29. Let $x_{n+1} = (ax_n + c)$ **mod** m, where $2 \leq a < m$, $0 \leq c < m$, $0 \leq x_0 < m$, $0 \leq x_{n+1} < m$, and $n \geq 0$. Prove that

$$x_n = (a^n x_0 + c[(a^n - 1)/(a - 1)]) \textbf{ mod } m,\ 0 \leq x_n < m.$$

30. Consider the linear congruential generator with $a = 7$, $c = 4$, and $m = 9$. If $x_4 = 1$, determine the seed x_0.

31. Prove that the sum of the cubes of three consecutive integers is divisible by 9.

32. Determine the last digit in 3^{55}.

33. For $m, n, r \in \mathbf{Z}^+$, let $p(m, n, r)$ count the number of partitions of m into at most n (positive) summands each no larger than r. Evaluate $\sum_{k=0}^{n-1} p(k(n+1), n, n)$, $n \in \mathbf{Z}^+$.

34. Given a ring $(R, +, \cdot)$, an element $r \in R$ is called *idempotent* when $r^2 = r$. If $n \in \mathbf{Z}^+$ with $n \geq 2$, prove that if $k \in \mathbf{Z}_n$ and k is idempotent, then $n - k + 1$ is idempotent.

35. For the hashing function at the end of Example 14.17, find (a) h(123-04-2275); (b) a social security number n such that $h(n) = 413$, thus causing a collision with the number 081-37-6495 of the example.

36. Write a computer program (or develop an algorithm) that implements the hashing function of Exercise 35.

37. The parking lot for a local restaurant has 41 parking spaces, numbered consecutively from 0 to 40. Upon driving into this lot, a patron is assigned a parking space by the parking attendant who uses the hashing function $h(k) = k$ **mod** 41, where k is the integer obtained from the last three digits on the patron's license plate. Further, to avoid a *collision* (where an occupied space might be assigned), when such a situation arises, the patron is directed to park in the next (consecutive) available space — where 0 is assumed to follow 40.

a) Suppose that eight automobiles arrive as the restaurant opens. If the last three digits in the license plates for these eight patrons (in their order of arrival) are

206, 807, 137, 444, 617, 330, 465, 905,

respectively, which spaces are assigned to the drivers of these eight automobiles by the parking attendant?

b) Following the arrival of the eight patrons in part (a), and before any of the eight could leave, a ninth patron arrives with a license plate where the last three digits are $00x$. If this patron is assigned to space 5, what is (are) the possible value(s) of x?

38. Solve the following linear congruences for x.

a) $3x \equiv 7 \pmod{31}$ **b)** $5x \equiv 8 \pmod{37}$

c) $6x \equiv 97 \pmod{125}$

14.4 Ring Homomorphisms and Isomorphisms

In this final section we shall examine functions (between rings) that obey special properties which depend on the closed binary operations in the rings.

EXAMPLE 14.19

Consider the rings $(\mathbf{Z}, +, \cdot)$ and $(\mathbf{Z}_6, +, \cdot)$, where addition and multiplication in $\mathbf{Z}_6$ are as defined in Section 14.3.

Define $f: \mathbf{Z} \to \mathbf{Z}_6$ by $f(x) = [x]$. For example, $f(1) = [1] = [7] = f(7)$ and $f(2) = f(8) = f(2 + 6k) = [2]$, for all $k \in \mathbf{Z}$. (So f is onto though not one-to-one.)

For $2, 3 \in \mathbf{Z}$, $f(2) = [2]$, $f(3) = [3]$ and we have $f(2 + 3) = f(5) = [5] = [2] + [3] = f(2) + f(3)$, and $f(2 \cdot 3) = f(6) = [0] = [2][3] = f(2) \cdot f(3)$.

In fact, for all $x, y \in \mathbf{Z}$,

$$\underset{\substack{\uparrow \\ \text{Addition in } \mathbf{Z}}}{f(x+y)} = [x+y] = [x]+[y] = \underset{\substack{\uparrow \\ \text{Addition in } \mathbf{Z}_6}}{f(x)+f(y)},$$

and

$$\underset{\substack{\uparrow \\ \text{Multiplication in } \mathbf{Z}}}{f(x \cdot y)} = [xy] = [x][y] = \underset{\substack{\uparrow \\ \text{Multiplication in } \mathbf{Z}_6}}{f(x) \cdot f(y)}.$$

This example suggests the following definition.

Definition 14.8 Let $(R, +, \cdot)$ and $(S, \oplus, \odot)$ be rings. A function $f: R \to S$ is called a *ring homomorphism* if for all $a, b \in R$,

a) $f(a+b) = f(a) \oplus f(b)$, and

b) $f(a \cdot b) = f(a) \odot f(b)$.

When the function f is onto we say that S is a *homomorphic image* of R.

This function is said to *preserve* the ring operations for the following reasons: Consider $f(a+b) = f(a) \oplus f(b)$. *Adding a, b in R* first and then finding the image (under f) in S of this sum, we get the same result as when we first determine the images (under f) in S of a, b, and then *add* these images *in S*. (Hence we have the function operation and the additive operations commuting with each other.) Similar remarks can be made about the multiplicative operations in the rings.

For the rings $\mathbf{Z}_4$ and $\mathbf{Z}_8$, define the function $f: \mathbf{Z}_4 \to \mathbf{Z}_8$ by $f([a]) = [a]^2 \ (= [a^2])$. Then for all $[a], [b] \in \mathbf{Z}_4$, we have

$$\underset{\substack{\uparrow \\ \text{Multiplication in } \mathbf{Z}_4}}{f([a][b])} = f([ab]) = [ab]^2 = ([a][b])^2 = [a]^2[b]^2 = \underset{\substack{\uparrow \\ \text{Multiplication in } \mathbf{Z}_8}}{f([a])f([b])}.$$

Consequently, this function f preserves the multiplicative operations in the rings. However, for $[1], [2] \in \mathbf{Z}_4$, we find that $f([1]+[2]) = f([3]) = [3]^2 = [1]$, while $f([1]) + f([2]) = [1]^2 + [2]^2 = [1] + [4] = [5] \ (\neq [1] \text{ in } \mathbf{Z}_8)$. So f does *not* preserve the additive operations in the rings—hence, f is *not* a ring homomorphism.

The function $g: \mathbf{Z}_4 \to \mathbf{Z}_8$, defined by $g([a]) = 3[a]$, preserves the additive operations, but not the multiplicative operations, in the rings.

Definition 14.9 Let $f: (R, +, \cdot) \to (S, \oplus, \odot)$ be a ring homomorphism. If f is one-to-one and onto, then f is called a *ring isomorphism* and we say that R and S are *isomorphic rings*.

We can think of isomorphic rings arising when the "same" ring is dealt with in two different languages. The function f then provides a dictionary for unambiguously translating from one language into the other.

The terms "homomorphism" and "isomorphism" come from the Greek, where *morphe* refers to shape or structure, *homo* means similar, and *iso* means identical or same. Hence homomorphic rings (that is, rings where one is a homomorphic image of the other) may

be thought of as similar in structure, while isomorphic rings are (abstractly) replicas of the same structure.

In Definition 11.13 we defined the concept of *graph* isomorphism. There we called the undirected graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ isomorphic when we could find a function $f: V_1 \to V_2$ such that

a) f is one-to-one and onto, and

b) $\{a, b\} \in E_1$ if and only if $\{f(a), f(b)\} \in E_2$.

In light of our statements about ring isomorphisms, another way to think about condition (b) here is in terms of the function f preserving the structures of the undirected graphs G_1 and G_2. When $|V_1| = |V_2|$, it is not difficult to find a function $f: V_1 \to V_2$ that is one-to-one and onto. However, for a given set V of vertices, what determines the structure of an undirected graph $G = (V, E)$ is its set of edges (where the vertex adjacencies are defined). Therefore a one-to-one correspondence $f: V_1 \to V_2$ is a graph isomorphism when it preserves the structures of G_1 and G_2 by preserving these vertex adjacencies.

EXAMPLE 14.20

For the ring R in Example 14.5 and the ring $\mathbf{Z}_5$, the function $f: R \to \mathbf{Z}_5$ given by

$$f(a) = [0], \qquad f(b) = [1], \qquad f(c) = [2], \qquad f(d) = [3], \qquad f(e) = [4]$$

provides us with a ring isomorphism.

For example, $f(c + d) = f(a) = [0] = [2] + [3] = f(c) + f(d)$, while $f(be) = f(e) = [4] = [1][4] = f(b)f(e)$. (In the absence of other methods and theorems, there are 25 such equalities that must be verified for the preservation of each of the binary operations.)

Inasmuch as there are $5! = 120$ one-to-one functions from R onto $\mathbf{Z}_5$, is there any assistance we can call upon in attempting to determine when one of these functions is an isomorphism? Suggested by Example 14.20, the following theorem provides ways of at least starting to determine when functions between rings can be homomorphisms and isomorphisms. [Parts (c) and (d) of this theorem rely on the results of Exercises 20 and 21 in Section 14.2.]

THEOREM 14.15

If $f: (R, +, \cdot) \to (S, \oplus, \odot)$ is a ring homomorphism, then

a) $f(z_R) = z_S$, where z_R, z_S are the zero elements of R, S, respectively;

b) $f(-a) = -f(a)$, for all $a \in R$;

c) $f(na) = nf(a)$, for all $a \in R$, $n \in \mathbf{Z}$;

d) $f(a^n) = [f(a)]^n$, for all $a \in R$, $n \in \mathbf{Z}^+$; and

e) if A is a subring of R, it follows that $f(A)$ is a subring of S.

Proof:

a) $z_S \oplus f(z_R) = f(z_R) = f(z_R + z_R) = f(z_R) \oplus f(z_R)$. (Why?) So by the cancellation law of addition in S, we have $f(z_R) = z_S$.

b) $z_S = f(z_R) = f(a + (-a)) = f(a) \oplus f(-a)$. Since additive inverses in S are unique and $f(-a)$ is an additive inverse of $f(a)$, it follows that $f(-a) = -f(a)$.

c) If $n = 0$, then $f(na) = f(z_R) = z_S = nf(a)$. The result is also true for $n = 1$, so we assume the truth for $n = k$ (≥ 1). Proceeding by mathematical induction, we examine the case where $n = k + 1$. By the results of Exercise 20 of Section 14.2, we get $f((k+1)a) = f(ka + a) = f(ka) \oplus f(a) = kf(a) \oplus f(a)$ (Why?) $= (k+1)(f(a))$ (Why?). (*Note*: There are three different kinds of addition here.)

When $n > 0$, $f(-na) = -nf(a)$. This follows from our prior proof by induction, part (b) of this proof, and part (b) of Theorem 14.1, because $f(-na) + f(na) = f(n(-a)) + f(na) = nf(-a) + nf(a) = n[f(-a) + f(a)] = n[-f(a) + f(a)] = nz_S = z_S$. Hence the result follows for all $n \in \mathbf{Z}$.

d) We leave this result for the reader to prove.

e) Since $A \neq \emptyset$, $f(A) \neq \emptyset$. If $x, y \in f(A)$, then $x = f(a)$, $y = f(b)$ for some $a, b \in A$. Then $x \oplus y = f(a) \oplus f(b) = f(a + b)$, and $x \odot y = f(a) \odot f(b) = f(ab)$, with $a + b, ab \in A$ (Why?), so $x \oplus y, x \odot y \in f(A)$. Also, if $x \in f(A)$ then $x = f(a)$ for some $a \in A$. So we have $f(-a) = -f(a) = -x$, and because $-a \in A$ (Why?), we have $-x \in f(A)$. Therefore $f(A)$ is a subring of S.

When the homomorphism is onto, we obtain the following theorem.

THEOREM 14.16 If $f: (R, +, \cdot) \to (S, \oplus, \odot)$ is a ring homomorphism from R *onto* S, where $|S| > 1$, then

a) if R has unity u_R, then $f(u_R)$ is the unity of S;

b) if R has unity u_R and a is a unit in R, then $f(a)$ is a unit in S and $f(a^{-1}) = [f(a)]^{-1}$;

c) if R is commutative, then S is commutative; and

d) if I is an ideal of R, then $f(I)$ is an ideal of S.

Proof: We shall prove part (d) and leave the other parts to the reader. Since I is a subring of R, it follows that $f(I)$ is a subring of S by part (e) of Theorem 14.15. To verify that $f(I)$ is an ideal, let $x \in f(I)$ and $s \in S$. Then $x = f(a)$ and $s = f(r)$, for some $a \in I, r \in R$. So $s \odot x = f(r) \odot f(a) = f(ra)$, with $ra \in I$, and we have $s \odot x \in f(I)$. Similarly, $x \odot s \in f(I)$, so $f(I)$ is an ideal of S.

These theorems reinforce the way in which homomorphisms and isomorphisms preserve structure. But can we find any use for these functions, aside from using them to prove more theorems? To help answer this, we start by considering the following example.

EXAMPLE 14.21 Extending the idea developed in Exercise 18 of Section 14.2, let R be the ring $\mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$. Then $|R| = |\mathbf{Z}_2| \cdot |\mathbf{Z}_3| \cdot |\mathbf{Z}_5| = 30$, and the operations of addition and multiplication are defined in R as follows:

For all $(a_1, a_2, a_3), (b_1, b_2, b_3) \in R$ where $a_1, b_1 \in \mathbf{Z}_2$, $a_2, b_2 \in \mathbf{Z}_3$, and $a_3, b_3 \in \mathbf{Z}_5$,

$$\underset{\substack{\uparrow \\ \text{Addition} \\ \text{in } R}}{(a_1, a_2, a_3) + (b_1, b_2, b_3)} = (\underset{\substack{\uparrow \\ \text{Addition} \\ \text{in } \mathbf{Z}_2}}{a_1 + b_1}, \underset{\substack{\uparrow \\ \text{Addition} \\ \text{in } \mathbf{Z}_3}}{a_2 + b_2}, \underset{\substack{\uparrow \\ \text{Addition} \\ \text{in } \mathbf{Z}_5}}{a_3 + b_3})$$

and

$$(a_1, a_2, a_3) \cdot (b_1, b_2, b_3) = (a_1 \cdot b_1, a_2 \cdot b_2, a_3 \cdot b_3).$$

Multiplication in R — Multiplication in $\mathbf{Z}_2$ — Multiplication in $\mathbf{Z}_3$ — Multiplication in $\mathbf{Z}_5$

Define the function $f: \mathbf{Z}_{30} \to R$ by $f(x) = (x_1, x_2, x_3)$, where

$$x_1 = x \textbf{ mod } 2$$
$$x_2 = x \textbf{ mod } 3$$
$$x_3 = x \textbf{ mod } 5.$$

In other words, x_1, x_2, and x_3 are the remainders that result when x is divided by 2, 3, and 5, respectively.

The results in Table 14.11 show that f is a function that is one-to-one and onto.

Table 14.11

x (in $\mathbf{Z}_{30}$)	$f(x)$ (in R)	x (in $\mathbf{Z}_{30}$)	$f(x)$ (in R)	x (in $\mathbf{Z}_{30}$)	$f(x)$ (in R)
0	(0, 0, 0)	10	(0, 1, 0)	20	(0, 2, 0)
1	(1, 1, 1)	11	(1, 2, 1)	21	(1, 0, 1)
2	(0, 2, 2)	12	(0, 0, 2)	22	(0, 1, 2)
3	(1, 0, 3)	13	(1, 1, 3)	23	(1, 2, 3)
4	(0, 1, 4)	14	(0, 2, 4)	24	(0, 0, 4)
5	(1, 2, 0)	15	(1, 0, 0)	25	(1, 1, 0)
6	(0, 0, 1)	16	(0, 1, 1)	26	(0, 2, 1)
7	(1, 1, 2)	17	(1, 2, 2)	27	(1, 0, 2)
8	(0, 2, 3)	18	(0, 0, 3)	28	(0, 1, 3)
9	(1, 0, 4)	19	(1, 1, 4)	29	(1, 2, 4)

To verify that f is an isomorphism, let $x, y \in \mathbf{Z}_{30}$. Then

$$\begin{aligned} f(x+y) &= ((x+y) \textbf{ mod } 2, (x+y) \textbf{ mod } 3, (x+y) \textbf{ mod } 5) \\ &= (x \textbf{ mod } 2, x \textbf{ mod } 3, x \textbf{ mod } 5) + (y \textbf{ mod } 2, y \textbf{ mod } 3, y \textbf{ mod } 5) \\ &= f(x) + f(y), \end{aligned}$$

and

$$\begin{aligned} f(xy) &= (xy \textbf{ mod } 2, xy \textbf{ mod } 3, xy \textbf{ mod } 5) \\ &= (x \textbf{ mod } 2, x \textbf{ mod } 3, x \textbf{ mod } 5) \cdot (y \textbf{ mod } 2, y \textbf{ mod } 3, y \textbf{ mod } 5) \\ &= f(x)f(y), \end{aligned}$$

so f is an isomorphism.

In examining Table 14.11 we find, for example, that

1) $f(0) = (0, 0, 0)$, where 0 is the zero element of $\mathbf{Z}_{30}$ and (0, 0, 0) is the zero element of $\mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$.
2) $f(2+4) = f(6) = (0, 0, 1) = (0, 2, 2) + (0, 1, 4) = f(2) + f(4)$.
3) The element 21 is the additive inverse of 9 in $\mathbf{Z}_{30}$, whereas $f(21) = (1, 0, 1)$ is the additive inverse of $(1, 0, 4) = f(9)$ in $\mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$.

4) $\{0, 5, 10, 15, 20, 25\}$ is a subring of $\mathbf{Z}_{30}$ with $\{(0, 0, 0)\ (= f(0)), (1, 2, 0)\ (= f(5)), (0, 1, 0)\ (= f(10)), (1, 0, 0)\ (= f(15)), (0, 2, 0)\ (= f(20)), (1, 1, 0)\ (= f(25))\}$ the corresponding subring in $\mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$.

But what else can we do with this isomorphism between $\mathbf{Z}_{30}$ and $\mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$? Suppose, for example, that we need to calculate $28 \cdot 17$ in $\mathbf{Z}_{30}$. We can transfer the problem to $\mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$ and compute $f(28) \cdot f(17) = (0, 1, 3) \cdot (1, 2, 2)$, where the moduli 2, 3, and 5 are smaller than 30 and easier to work with. Since $(0, 1, 3) \cdot (1, 2, 2) = (0 \cdot 1, 1 \cdot 2, 3 \cdot 2) = (0, 2, 1)$ and $f^{-1}(0, 2, 1) = 26$, it follows that $28 \cdot 17$ (in $\mathbf{Z}_{30}$) is 26.

In Example 14.21 we see that if we are given an element (x_1, x_2, x_3) in $\mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$, then we can use Table 14.11 to find the unique element x in $\mathbf{Z}_{30}$ so that $f(x) = (x_1, x_2, x_3)$. But what would we do if we did not have such a table—especially, if we found ourselves working with larger rings, such as $\mathbf{Z}_{32736}$ and $\mathbf{Z}_{31} \times \mathbf{Z}_{32} \times \mathbf{Z}_{33}$, and the isomorphism $g\colon \mathbf{Z}_{32736} \to \mathbf{Z}_{31} \times \mathbf{Z}_{32} \times \mathbf{Z}_{33}$ where $g(x) = (x \textbf{ mod } 31,\ x \textbf{ mod } 32,\ x \textbf{ mod } 33)$ for $x \in \mathbf{Z}_{32736}$? The following result provides a technique for determining the unique preimage for a given element of the codomain for such an isomorphism g.

THEOREM 14.17 *The Chinese Remainder Theorem.* Let $m_1, m_2, \ldots, m_k \in \mathbf{Z}^+ - \{1\}$ with $k \geq 2$, and with $\gcd(m_i, m_j) = 1$ for all $1 \leq i < j \leq k$. Then the system of k congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a simultaneous solution. Further, any two such solutions of the system are congruent modulo $m_1 m_2 \cdots m_k$.

Proof: We start by showing how to construct a simultaneous solution of the system of k congruences.

Let $m = m_1 m_2 \cdots m_k$ and, for $1 \leq j \leq k$, let $M_j = m/m_j$. [So, for example, $M_1 = m_2 m_3 m_4 \cdots m_k$ and $M_2 = m_1 m_3 m_4 \cdots m_k$.] We find that for all $1 \leq j \leq k$, $\gcd(m_j, M_j) = 1$. If not, then for some (fixed) j, with $1 \leq j \leq k$, there exists a prime p such that $p|m_j$ and $p|M_j$. But from Lemma 4.3 it follows that if $p|M_j$ then $p|m_i$ for some $1 \leq i \leq k$, where $i \neq j$. Consequently, we find that $p|m_j$ and $p|m_i$ for $i \neq j$, and this contradicts $\gcd(m_j, m_j) = 1$.

For each $1 \leq j \leq k$, $\gcd(m_j, M_j) = 1$. Consequently, from Theorem 14.14 we know that M_j is a unit in $\mathbf{Z}_{m_j}$. So there exists $x_j \in \mathbf{Z}_{m_j}$ such that $M_j x_j \equiv 1 \pmod{m_j}$. Now consider the sum

$$x = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots + a_k M_k x_k.$$

We claim that x is a simultaneous solution of the system of k congruences. Note that for $1 \leq j \leq k$ and $1 \leq i \leq k$, if $i \neq j$ then $M_i \equiv 0 \pmod{m_j}$ because $m_j | M_i$. Hence $M_i x_i \equiv 0 \pmod{m_j}$. Since $M_j x_j \equiv 1 \pmod{m_j}$ we find that

$$x \equiv a_j M_j x_j \equiv a_j \pmod{m_j},$$

for each $1 \leq j \leq k$.

Now suppose that x, y are both simultaneous solutions of the system of k congruences. Then $x \equiv y \pmod{m_j}$ for all $1 \le j \le k$. Consider the prime factorization of $m = m_1 m_2 \cdots m_k$. Let p be a prime such that $p^t | m$ but $p^{t+1} \nmid m$, for some $t \in \mathbf{Z}^+$. Since $\gcd(m_i, m_j) = 1$ for all $1 \le i < j \le k$, it follows that $p^t | m_j$ for one (and only one) modulus m_j. Consequently, we see that $p^t | (x - y)$, and so it follows from the Fundamental Theorem of Arithmetic that $m | (x - y)$, or $x \equiv y \pmod{m}$.

Now let us see how one can apply the Chinese Remainder Theorem.

EXAMPLE 14.22

In Marjorie's fourth-grade arithmetic class, three students — namely, Megan, Avery, and Elizabeth — enjoy doing long-division problems (without a calculator). So Marjorie selects a positive integer n and asks for the remainder upon division by three different divisors. Upon dividing by 31 Megan learns that the remainder is 14. Avery divides n by 32 and finds the remainder is 16. Meanwhile, Elizabeth obtains the remainder of 18 when she divides n by 33. What is the smallest value of n that Marjorie could have selected?

Here we seek a simultaneous solution for the three congruences

$$x \equiv 14 \pmod{31}, \qquad x \equiv 16 \pmod{32}, \qquad x \equiv 18 \pmod{33}.$$

So $a_1 = 14$, $a_2 = 16$, $a_3 = 18$, $m_1 = 31$, $m_2 = 32$, $m_3 = 33$, and $m = m_1 m_2 m_3 = 32736$. Further, $M_1 = m/m_1 = 1056$, $M_2 = m/m_2 = 1023$, and $M_3 = m/m_3 = 992$. Using the Euclidean algorithm (when necessary), as in Example 14.13, we learn that

$$\begin{aligned}
[x_1] &= [M_1]^{-1} = [1056]^{-1} = [34(31) + 2]^{-1} = [2]^{-1} = [16] \text{ in } \mathbf{Z}_{m_1} = \mathbf{Z}_{31},\\
[x_2] &= [M_2]^{-1} = [1023]^{-1} = [31(32) + 31]^{-1} = [31]^{-1} = [31] \text{ in } \mathbf{Z}_{m_2} = \mathbf{Z}_{32}, \quad \text{and}\\
[x_3] &= [M_3]^{-1} = [992]^{-1} = [30(33) + 2]^{-1} = [2]^{-1} = [17] \text{ in } \mathbf{Z}_{m_3} = \mathbf{Z}_{33}.
\end{aligned}$$

Hence,

$$\begin{aligned}
x &\equiv (14)(1056)(16) + (16)(1023)(31) + (18)(992)(17) \pmod{32736}\\
&\equiv 1047504 \pmod{32736}\\
&\equiv 31(32736) + 32688 \pmod{32736}\\
&\equiv 32688 \pmod{32736}.
\end{aligned}$$

So the (smallest) positive integer n that Marjorie could have selected is 32688.

(As a check we find that $32688 = 1054(31) + 14 = 1021(32) + 16 = 990(33) + 18$, so x satisfies the given system of three congruences and is the smallest positive integer that does so.)

Now if we look back at the isomorphism $g: \mathbf{Z}_{32736} \to \mathbf{Z}_{31} \times \mathbf{Z}_{32} \times \mathbf{Z}_{33}$ (that we mentioned prior to stating the Chinese Remainder Theorem) we see that for the codomain element (14, 16, 18) in $\mathbf{Z}_{31} \times \mathbf{Z}_{32} \times \mathbf{Z}_{33}$, the element 32688 in the domain $\mathbf{Z}_{32736}$ is the (unique) preimage. That is, $g(32688) = (14, 16, 18)$ and for any other integer y, if $g(y) = (14, 16, 18)$, then $y \equiv 32688 \pmod{32736}$ — so 32688 is the only solution in $\{0, 1, 2, 3, \ldots, 32735\}$.

The isomorphisms f (of Example 14.21) and g (of Example 14.22) are special cases of a more general result† that we shall now state. If $n = n_1 n_2 \cdots n_k$, where $n_i > 1$ for all $1 \le i \le k$ and $\gcd(n_i, n_j) = 1$ for all $1 \le i < j \le k$, then the rings $\mathbf{Z}_n$ and $\mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_k}$ are isomorphic. In particular, we know from the Fundamental Theorem of Arithmetic that for each $n \in \mathbf{Z}^+ - \{1\}$, we can factor n as $p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, where $p_1, p_2, \ldots, p_t$ are t distinct primes, $t \ge 1$, and $e_1, e_2, \ldots, e_t \in \mathbf{Z}^+$. It then follows that the rings $\mathbf{Z}_n$ and $\mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times \cdots \times \mathbf{Z}_{m_t}$ are isomorphic for $m_1 = p_1^{e_1}, m_2 = p_2^{e_2}, \ldots, m_t = p_t^{e_t}$.

As a result of this isomorphism, arithmetic involving large integers (that exceed the word size of a given computer) can be performed using the smaller different moduli. Further, the computation for these smaller moduli can be carried out in parallel—thus, reducing computation time. [For more on the Chinese Remainder Theorem in conjunction with applications of residue arithmetic in computers, we direct the interested reader to pages 146–149 of the text by K. H. Rosen [12], pages 344–359 of the text by J. P. Tremblay and R. Manohar [14], as well as the text by D. E. Knuth [8].

EXERCISES 14.4

1. If R is the ring of Example 14.6, construct an isomorphism $f: R \to \mathbf{Z}_6$.

2. Complete the proofs of Theorems 14.15 and 14.16.

3. If R, S, and T are rings and $f: R \to S$, $g: S \to T$ are ring homomorphisms, prove that the composite function $g \circ f: R \to T$ is a ring homomorphism.

4. If $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \middle| \, a \in \mathbf{R} \right\}$, then S is a ring under matrix addition and multiplication. Prove that $\mathbf{R}$ is isomorphic to S.

5. **a)** Let $(R, +, \cdot)$ and $(S, \oplus, \odot)$ be rings with zero elements z_R and z_S, respectively. If $f: R \to S$ is a ring homomorphism, let $K = \{a \in R \mid f(a) = z_S\}$. Prove that K is an ideal of R. (K is called the *kernel* of the homomorphism f.)

b) Find the kernel of the homomorphism in Example 14.19.

c) Let f, $(R, +, \cdot)$, and $(S, \oplus, \odot)$ be as in part (a). Prove that f is one-to-one if and only if the kernel of f is $\{z_R\}$.

6. Use the information in Table 14.11 to compute each of the following in $\mathbf{Z}_{30}$.

a) $(13)(23) + 18$ **b)** $(11)(21) - 20$

c) $(13 + 19)(27)$ **d)** $(13)(29) + (24)(8)$

7. **a)** Construct a table (as in Example 14.21) for the isomorphism $f: \mathbf{Z}_{20} \to \mathbf{Z}_4 \times \mathbf{Z}_5$.

b) Use the table from part (a) to compute the following in $\mathbf{Z}_{20}$.

i) $(17)(19) + (12)(14)$

ii) $(18)(11) - (9)(15)$

8. Let $n, r, s \in \mathbf{Z}^+$ with $n, r, s \ge 2$, $n = rs$, and $\gcd(r, s) = 1$. If $f: \mathbf{Z}_n \to \mathbf{Z}_r \times \mathbf{Z}_s$ is a ring isomorphism with $f(a) = (1, 0)$ and $f(b) = (0, 1)$, prove that if $(m, t) \in \mathbf{Z}_r \times \mathbf{Z}_s$, then $f^{-1}(m, t) \equiv ma + tb \pmod{n}$.

9. **a)** How many units are there in the ring $\mathbf{Z}_8$?

b) How many units are there in the ring $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$?

c) Are $\mathbf{Z}_8$ and $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ isomorphic rings?

10. **a)** How many units are there in $\mathbf{Z}_{15}$? How many in $\mathbf{Z}_3 \times \mathbf{Z}_5$?

b) Are $\mathbf{Z}_{15}$ and $\mathbf{Z}_3 \times \mathbf{Z}_5$ isomorphic?

11. Are $\mathbf{Z}_4$ and the ring in Example 14.4 isomorphic?

12. If $f: R \to S$ is a ring homomorphism and J is an ideal of S, prove that $f^{-1}(J) = \{a \in R \mid f(a) \in J\}$ is an ideal of R.

13. Find a simultaneous solution for the system of two congruences:

$$x \equiv 5 \pmod 8$$
$$x \equiv 73 \pmod{81}.$$

14. A band of 17 pirates captures a treasure chest full of (identical) gold coins. When the coins are divided up into equal numbers, three coins remain. One pirate accuses the distributor of miscounting and kills him in a duel. As a result, the second time the coins are distributed, in equal numbers, among the 16 surviving pirates, there are 10 coins remaining. An argument erupts and leads to gun play, resulting in the demise of another pirate. Now when the coins are divided up, in 15 equal piles, there are no remaining coins. What is the smallest number of coins that could have been in the chest?

15. Find a simultaneous solution for the system of four congruences:

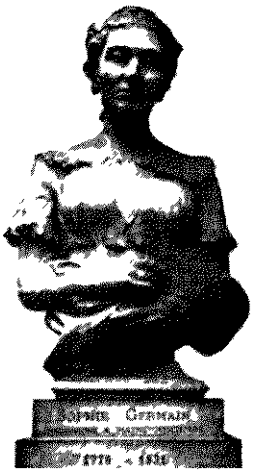
$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 5 \pmod 7.$$

†In some textbooks this result is referred to as the Chinese Remainder Theorem.

14.5 Summary and Historical Review

Emphasizing structure induced by two closed binary operations, this chapter has introduced us to the mathematical system called a ring. Throughout the development of mathematics, the ring of integers has played a key role. In the branch of mathematics called number theory, we examine the basic properties of $(\mathbf{Z}, +, \cdot)$, as well as the finite rings $(\mathbf{Z}_n, +, \cdot)$. The matrix rings provide familiar examples of noncommutative rings.

Pierre de Fermat (1601–1665)

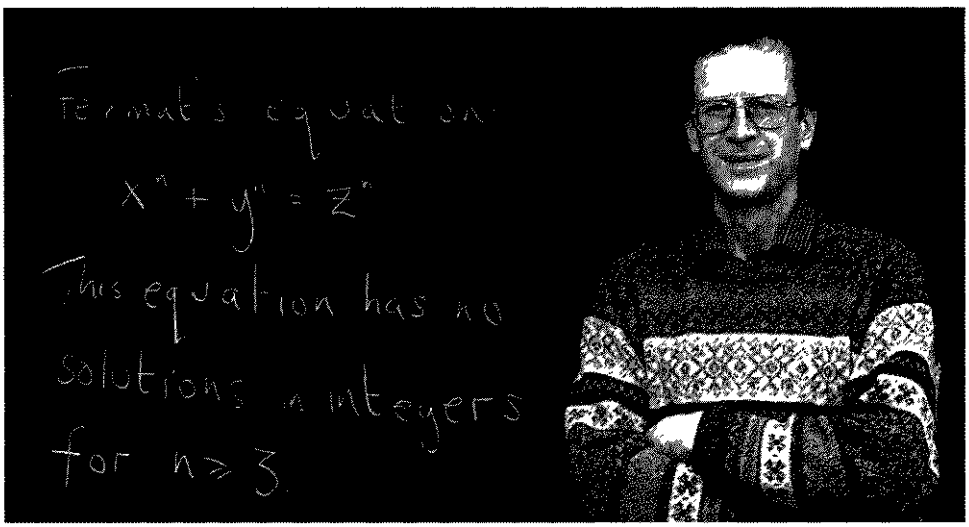


Sophie Germain (1776–1831)

This chapter contains the development of an abstract theory. On the basis of the definition of a ring, we established principles of elementary algebra that we have been using since our early encounters with arithmetic, signed numbers, and the manipulation of unknowns. The reader may have found some of the proofs tedious, as we justified all the steps in the derivations. Faced with the challenge of trying to prove a result in abstract mathematics, one should follow the advice given by the Roman rhetorician Marcus Fabius Quintilianus (first century A.D.), when he said, "One should not aim at being possible to understand (or follow), but at being impossible to be misunderstood."

A famous problem in number theory, known as *Fermat's Last Theorem*, claims that the equation $x^n + y^n = z^n$, $n \in \mathbf{Z}^+$, $n > 1$, has no solutions in $\mathbf{Z}^+$ when $n > 2$. In 1637 the French mathematician Pierre de Fermat (1601–1665) wrote that he had proved this result but that the proof was too long to be included in the margin of his manuscript. Many renowned mathematicians of the eighteenth and nineteenth centuries tried to prove this result — among them Leonhard Euler (1707–1783), Peter Gustav Lejeune Dirichlet (1805–1859), Carl Friedrich Gauss (1777–1855), Sophie Germain (1776–1831), Adrien-Marie Legendre (1752–1833), Niels Henrik Abel (1802–1829), Gabriel Lamé (1795–1870), and Leopold Kronecker (1823–1891). Although unsuccessful, attempts to resolve Fermat's claim did result in new mathematical ideas and theories. The twentieth century also produced scholars who expended tremendous efforts on this problem. One such scholar was born in Cambridge, England, in 1953. There, at the age of 10, he went to the public library in his town and looked into a book on mathematics. As he read about Fermat's Last Theorem, it seemed so simple — and he wanted to prove it. In the 1970s Andrew Wiles went to Cambridge University, and after he finished his degree, he became a research student there,

working in number theory — in an area called Iwasawa theory. For at this time Fermat's Last Theorem was not in fashion. When Wiles completed his doctorate, he moved to the United States, to a position at Princeton University. In the 1980s his enthusiasm for his childhood dream was rekindled and he spent close to seven years working alone — locked up in his attic office. He finally confided in his colleague Nick Katz — in January 1993. Then in June 1993 Professor Wiles returned to Cambridge to deliver a series of three lectures at a number-theory conference. The last lecture ended in grand applause, accompanied by flashing cameras and reporters' questions. It appeared that he had solved Fermat's Last Theorem. Unfortunately, when his 200-page write-up was peer-reviewed, by experts such as Nick Katz, problems started to arise, and a hole in the proof caused everything to collapse like a house of cards. The fall of 1993 found Wiles back at Princeton — now crestfallen, angry, and humiliated. But then, after renewed effort, on September 19, 1994, he took one last look at his proposed proof. The next morning he wrote up a new proof, as everything fell into place. This time no one could find any flaws. The May 1995 issue of the journal *Annals of Mathematics* contains the original Cambridge paper by Andrew Wiles and the correction by Wiles and his friend and former student Richard Taylor. At last Fermat's Last Theorem was laid to rest. (Although Wiles gets much of the praise, other mathematicians deserve accolades as well — among them, Kenneth Ribet, Barry Mazur, Goro Shimura, Yutaka Taniyama, Gerhard Frey, Matthias Flach, and Richard Taylor.) For more on the history and development of the proof of this famous theorem, the reader is directed to the very readable account given by A. D. Aczel [1].



Andrew John Wiles (1953–)

AP/Wide World Photos

In trying to prove Fermat's Last Theorem, the German mathematician Ernst Kummer (1810–1893) developed the foundations for the concept of the *ideal*. This concept was later formulated, named, and utilized by his countryman Richard Dedekind (1831–1916) in his research on what are now called Dedekind domains. Use of the term "ring," however, seems to be attributable to the German mathematician David Hilbert (1862–1943).

Ring homomorphisms and their interplay with ideals were extensively developed by the German mathematician Emmy Noether (1882–1935). This great genius received little remuneration, financial or otherwise, from the governing bodies of her native land because

of the sexual bias that was prevalent in the universities at that time. Emmy Noether's talents were nonetheless recognized by her colleagues, and she was eulogized in the *New York Times* on May 3, 1935, by Albert Einstein (1879–1955), who acknowledged the influence and importance of her work for the development of relativity theory. In addition to enduring sexual bias, as a Jew she was forced to flee her homeland in 1933, when the Nazis came to power. She spent the last two years of her life guiding young mathematicians in the United States. For more on the life of this fascinating person, examine the biography by A. Dick [4] and the article by C. Kimberling [7].

The special rings called *fields* arise in the rational, real, and complex number systems. But we also saw some interesting finite fields. These structures will be examined again in Chapter 17 in connection with combinatorial designs. The field theory developed by the French genius Evariste Galois (1811–1832) answered questions about the solutions of polynomial equations of degree > 4. These questions had baffled mathematicians for centuries, and his ideas, now known as Galois theory, still comprise one of the most elegant mathematical theories ever developed. More on Galois theory appears in the text by O. Zariski and P. Samuel [16].

Emmy Noether (1882–1935)

For supplemental reading on ring theory at the introductory level, the interested reader should examine Chapters 12–18 of J. A. Gallian [5], Chapter 6 of V. H. Larney [9], and Chapters 6, 7, and 12 of N. H. McCoy and T. R. Berger [10]. A somewhat more advanced coverage can be found in Chapter 4 of the text by E. A. Walker [15].

The development of modular congruence, along with many related ideas, we owe primarily to Carl Friedrich Gauss. Problems involving systems of congruences date back to the late first century where they appear in the work of the Greek mathematician Nicomachus of Gerasa. Systems of two congruences can also be found in the writings of the seventh-century mathematician Brahmagupta (born in 1598 in northwestern India). However, it was not until 1247 that we find the publication of a general method for solving systems of linear congruences. In his *Shushu jiuzhang (Mathematical Treatise in Nine Sections)*, the method now called the Chinese Remainder Theorem is presented by the Chinese mathematician Qin Jiushao (c. 1202–1261). Born in the province of Sichuan during the time of Genghis Khan, this remarkable mathematical talent was also an accomplished architect, musician, and poet, as well as being quite the sportsman—in archery, fencing, and horsemanship.

More on the solution of congruences and the Chinese Remainder Theorem can be found in the texts by I. Niven, H. S. Zuckerman, and H. L. Montgomery [11] and K. H. Rosen [12].

As mentioned earlier (in the footnote in Example 14.16), more on the history, development, and applications of cryptology can be found in the texts by T. H. Barr [3], P. Garrett [6], and W. Trappe and L. C. Washington [13].

Finally, the topic of hashing, or scattering, can be further investigated in Chapter 2 of J. P. Tremblay and R. Manohar [14]. Chapter 4 of A. V. Aho, J. E. Hopcroft, and J. D. Ullman [2] includes a discussion on the efficiency of hashing functions and a probabilistic investigation of the collision problem that arises for these functions.

REFERENCES

1. Aczel, Amir D. *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem.* New York: Four Walls Eight Windows, 1996.
2. Aho, Alfred V., Hopcroft, John E., and Ullman, Jeffrey D. *Data Structures and Algorithms.* Reading, Mass.: Addison-Wesley, 1983.
3. Barr, Thomas H. *Invitation to Cryptology.* Upper Saddle River, N.J.: Prentice-Hall, 2002.
4. Dick, Auguste. *Emmy Noether (1882–1935)*, trans. Heidi Blocher. Boston: Birkhäuser-Boston, 1981.
5. Gallian, Joseph A. *Contemporary Abstract Algebra*, 5th ed. Boston: Houghton Mifflin, 2002.
6. Garrett, Paul. *Making, Breaking Codes: An Introduction to Cryptology.* Upper Saddle River, N.J.: Prentice-Hall, 2001.
7. Kimberling, Clark. "Emmy Noether, Greatest Woman Mathematician." *Mathematics Teacher* (March 1982): pp. 246–249.
8. Knuth, Donald Ervin. *The Art of Computer Programming*, 3rd ed., Volume 2, *Semi-Numerical Algorithms.* Reading, Mass.: Addison-Wesley, 1997.
9. Larney, Violet Hachmeister. *Abstract Algebra: A First Course.* Boston: Prindle, Weber & Schmidt, 1975.
10. McCoy, Neal H., and Berger, Thomas R. *Algebra: Groups, Rings and Other Topics.* Boston: Allyn and Bacon, 1977.
11. Niven, Ivan, Zuckerman, Herbert S., and Montgomery, Hugh L. *An Introduction to the Theory of Numbers*, 5th ed. New York: Wiley, 1991.
12. Rosen, Kenneth H. *Elementary Number Theory*, 4th ed. Reading, Mass.: Addison-Wesley, 1999.
13. Trappe, Wade, and Washington, Lawrence C. *Introduction to Cryptography with Coding Theory.* Upper Saddle River, N.J.: Prentice-Hall, 2002.
14. Tremblay, Jean-Paul, and Manohar, R. *Discrete Mathematical Structures with Applications to Computer Science.* New York: McGraw-Hill, 1975.
15. Walker, Elbert A. *Introduction to Abstract Algebra.* New York: Random House/Birkhäuser, 1987.
16. Zariski, Oscar, and Samuel, Pierre. *Commutative Algebra*, Vol. I. Princeton, N.J.: Van Nostrand, 1958.

SUPPLEMENTARY EXERCISES

1. Determine whether each of the following statements is true or false. For each false statement give a counterexample.

a) If $(R, +, \cdot)$ is a ring, and $\emptyset \neq S \subseteq R$ with S closed under $+$ and $\cdot$, then S is a subring of R.

b) If $(R, +, \cdot)$ is a ring with unity, and S is a subring of R, then S has a unity.

c) If $(R, +, \cdot)$ is a ring with unity u_R, and S is a subring of R with unity u_S, then $u_R = u_S$.

d) Every field is an integral domain.

e) Every subring of a field is a field.

f) A field can have only two subrings.

g) Every finite field has a prime number of elements.

h) The field $(\mathbf{Q}, +, \cdot)$ has an infinite number of subrings.

2. Prove that a ring R is commutative if and only if $(a + b)^2 = a^2 + 2ab + b^2$, for all $a, b \in R$.

3. A ring R is called *Boolean* if $a^2 = a$ for all $a \in R$. If R is Boolean, prove that (a) $a + a = 2a = z$, for all $a \in R$; and (b) R is commutative.

4. With $\mathbf{C}$ the field of complex numbers and S the ring of 2×2 real matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, define $f: \mathbf{C} \to S$ by $f(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, for $a + bi \in \mathbf{C}$. Prove that f is a ring isomorphism.

5. If $(R, +, \cdot)$ is a ring, prove that $C = \{r \in R | ar = ra$, for all $a \in R\}$ is a subring of R. (The subring C is called the *center* of R.)

6. Given a finite field F, let $M_2(F)$ denote the set of all 2×2 matrices with entries from F. As in Example 14.2, $(M_2(F), +, \cdot)$ becomes a noncommutative ring with unity.

a) Determine the number of elements in $M_2(F)$ if F is

i) $\mathbf{Z}_2$ **ii)** $\mathbf{Z}_3$ **iii)** $\mathbf{Z}_p$, p a prime

b) As in Exercise 13 of Section 14.1, $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbf{Z}_p)$ is a unit if and only if $ad - bc \neq z$. This occurs if the first row of A does not contain all zeros (that is, z's) and the second row is not a multiple (by an element of $\mathbf{Z}_p$) of the first. Use this observation to determine the number of units in

i) $M_2(\mathbf{Z}_2)$ **ii)** $M_2(\mathbf{Z}_3)$ **iii)** $M_2(\mathbf{Z}_p)$, p a prime

7. Given an integral domain $(D, +, \cdot)$ with zero element z, let $a, b \in D$ with $ab \neq z$. (a) If $a^3 = b^3$ and $a^5 = b^5$, prove that $a = b$. (b) Let $m, n \in \mathbf{Z}^+$ with $\gcd(m, n) = 1$. If $a^m = b^m$ and $a^n = b^n$, prove that $a = b$.

8. Let $A = \mathbf{R}^+$. Define $\oplus$ and $\odot$ on A by $a \oplus b = ab$, the ordinary product of a, b; and $a \odot b = a^{\log_2 b}$.

a) Verify that $(A, \oplus, \odot)$ is a commutative ring with unity.

b) Is this ring an integral domain or field?

9. Let R be a ring with ideals A and B. Define $A + B = \{a + b | a \in A, b \in B\}$. Prove that $A + B$ is an ideal of R. (For any ring R, the ideals of R form a poset under set inclusion. If A and B are ideals of R, with $\text{glb}\{A, B\} = A \cap B$ and $\text{lub}\{A, B\} = A + B$, the poset is a lattice.)

10. a) If p is a prime, prove that p divides $\binom{p}{k}$, for all $0 < k < p$.

b) If $a, b \in \mathbf{Z}$, prove that $(a + b)^p \equiv a^p + b^p \pmod{p}$.

11. Given n positive integers $x_1, x_2, \ldots, x_n$, not necessarily distinct, prove that either $n | (x_1 + x_2 + \cdots + x_i)$, for some $1 \leq i \leq n$, or there exist $1 \leq i < j \leq n$ such that $n | (x_{i+1} + \cdots + x_{j-1} + x_j)$.

12. Consider the ring $(\mathbf{Z}^3, \oplus, \odot)$ where addition and multiplication are defined by $(a, b, c) \oplus (d, e, f) = (a + d, b + e, c + f)$ and $(a, b, c) \odot (d, e, f) = (ad, be, cf)$. (Here, for example, $a + d$ and ad are computed by using the standard binary operations of addition and multiplication in $\mathbf{Z}$.) Let S be the subset of $\mathbf{Z}^3$ where $S = \{(a, b, c) | a = b + c\}$. Prove that S is *not* a subring of $(\mathbf{Z}^3, \oplus, \odot)$.

13. a) In how many ways can one select two positive integers m, n, not necessarily distinct, so that $1 \leq m \leq 100$, $1 \leq n \leq 100$ and the last digit of $7^m + 3^n$ is 8?

b) Answer part (a) for the case where $1 \leq m \leq 125$, $1 \leq n \leq 125$.

c) If one randomly selects m, n [as in part (a)], what is the probability that 2 is now the last digit of $7^m + 3^n$?

14. Let $n \in \mathbf{Z}^+$ with $n > 1$.

a) If $n = 2k$ where k is an odd integer, prove that

$$k^3 \equiv k \pmod{n}.$$

b) If $n = 4k$ for some $k \in \mathbf{Z}^+$, prove that

$$(2k)^2 \equiv 0 \pmod{n}.$$

c) Prove that

$$\sum_{i=1}^{n-1} i^3 \equiv \begin{cases} \frac{n}{2} \pmod{n}, & \text{for } n \text{ even with } \frac{n}{2} \text{ odd}, \\ 0 \pmod{n}, & \text{otherwise.} \end{cases}$$

15. Suppose that $a, b, c \in \mathbf{Z}$ and $5 | (a^2 + b^2 + c^2)$. Prove that $5 | a$ or $5 | b$ or $5 | c$.

16. Write a computer program (or develop an algorithm) that reverses the order of the digits in a given positive integer. For example, the input 1374 should result in the output 4731.

17. Suppose that $a, b, k \in \mathbf{Z}^+$ with $a - b = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, for $p_1, p_2, \ldots, p_k$ prime and $e_1, e_2, \ldots, e_k \in \mathbf{Z}^+$. For how many values of n (> 1) is $a \equiv b \pmod{n}$ true?

18. As the co-chairs of the Homecoming Parade Committee, Jerina and Noor must organize the freshmen for a pregame presentation. When they arrange these students in rows of 8, there are three students remaining. When rows of 11 are tried, four students remain. Finally, rows of 15 leave five students remaining. So the co-chairs use the rows of 15 and place the remaining five students at the center (in positions 6–10) of the first row. What is the smallest number of freshmen Jerina and Noor are trying to organize?