CHAPTER 5
Induction and Recursion

SECTION 5.1 Mathematical Induction

Understanding and constructing proofs by mathematical induction are extremely difficult tasks for most students. Do not be discouraged, and do not give up, because, without doubt, this proof technique is the most important one there is in mathematics and computer science. Pay careful attention to the conventions to be observed in writing down a proof by induction. As with all proofs, remember that a proof by mathematical induction is like an essay—it must have a beginning, a middle, and an end; it must consist of complete sentences, logically and aesthetically arranged; and it must convince the reader. Be sure that your basis step (also called the "base case") is correct (that you have verified the proposition in question for the smallest value or values of n), and be sure that your inductive step is correct and complete (that you have derived the proposition for $k+1$, assuming the inductive hypothesis that the proposition is true for k).

Some, but not all, proofs by mathematical induction are like Exercises 3–17. In each of these, you are asked to prove that a certain summation has a "closed form" representation given by a certain expression. Here the proofs are usually straightforward algebra. For the inductive step you start with the summation for $P(k+1)$, find the summation for $P(k)$ as its first k terms, replace that much by the closed form given by the inductive hypothesis, and do the algebra to get the resulting expression into the desired form. When doing proofs like this, however, remember to include all the words *surrounding your algebra—the algebra alone is not the proof. Also keep in mind that $P(n)$ is the proposition that the sum equals the closed-form expression, not just the sum and not just the expression.*

Many inequalities can be proved by mathematical induction; see Exercises 18–24, for example. The method also extends to such things as set operations, divisibility, and a host of other applications; a sampling of them is given in other exercises in this set. Some are quite complicated.

One final point about notation. In performing the inductive step, it really does not matter what letter we use. We see in the text the proof of $P(k) \to P(k+1)$; but it would be just as valid to prove $P(n) \to P(n+1)$, since the k in the first case and the n in the second case are just dummy variables. We will use both notations in this Guide*; in particular, we will use k for the first few exercises but often use n afterwards. A student just beginning to write proofs by mathematical induction should be even more formal than we are in this* Guide *and follow the template given at the end of this section. With experience, you can relax a bit and the style can become more informal, as long as all the steps are there.*

1. We can prove this by mathematical induction. Let $P(n)$ be the statement that the train stops at station n. We want to prove that $P(n)$ is true for all positive integers n. For the basis step, we are told that $P(1)$ is true. For the inductive step, we are told that $P(k)$ implies $P(k+1)$ for each $k \ge 1$. Therefore by the principle of mathematical induction, $P(n)$ is true for all positive integers n.

3. **a)** Plugging in $n=1$ we have that $P(1)$ is the statement $1^2 = 1 \cdot 2 \cdot 3/6$.

b) Both sides of $P(1)$ shown in part **(a)** equal 1.

c) The inductive hypothesis is the statement that

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

d) For the inductive step, we want to show for each $k \geq 1$ that $P(k)$ implies $P(k+1)$. In other words, we want to show that assuming the inductive hypothesis (see part **(c)**) we can show

$$1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}.$$

e) The left-hand side of the equation in part **(d)** equals, by the inductive hypothesis, $k(k+1)(2k+1)/6 + (k+1)^2$. We need only do a bit of algebraic manipulation to get this expression into the desired form: factor out $(k+1)/6$ and then factor the rest. In detail,

$$\begin{aligned}\left(1^2 + 2^2 + \cdots + k^2\right) + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \quad \text{(by the inductive hypothesis)}\\ &= \frac{k+1}{6}\big(k(2k+1) + 6(k+1)\big) = \frac{k+1}{6}(2k^2+7k+6)\\ &= \frac{k+1}{6}(k+2)(2k+3) = \frac{(k+1)(k+2)(2k+3)}{6}.\end{aligned}$$

f) We have completed both the basis step and the inductive step, so by the principle of mathematical induction, the statement is true for every positive integer n.

5. We proceed by induction. The basis step, $n = 0$, is true, since $1^2 = 1 \cdot 1 \cdot 3/3$. For the inductive step assume the inductive hypothesis that

$$1^2 + 3^2 + 5^2 + \cdots + (2k+1)^2 = \frac{(k+1)(2k+1)(2k+3)}{3}.$$

We want to show that

$$1^2 + 3^2 + 5^2 + \cdots + (2k+1)^2 + (2k+3)^2 = \frac{(k+2)(2k+3)(2k+5)}{3}$$

(the right-hand side is the same formula with $k+1$ plugged in for n). Now the left-hand side equals, by the inductive hypothesis, $(k+1)(2k+1)(2k+3)/3 + (2k+3)^2$. We need only do a bit of algebraic manipulation to get this expression into the desired form: factor out $(2k+3)/3$ and then factor the rest. In detail,

$$\begin{aligned}&\left(1^2 + 3^2 + 5^2 + \cdots + (2k+1)^2\right) + (2k+3)^2\\ &\qquad = \frac{(k+1)(2k+1)(2k+3)}{3} + (2k+3)^2 \quad \text{(by the inductive hypothesis)}\\ &\qquad = \frac{2k+3}{3}\big((k+1)(2k+1) + 3(2k+3)\big) = \frac{2k+3}{3}(2k^2+9k+10)\\ &\qquad = \frac{2k+3}{3}\big((k+2)(2k+5)\big) = \frac{(k+2)(2k+3)(2k+5)}{3}.\end{aligned}$$

7. Let $P(n)$ be the proposition $3 + 3\cdot 5 + 3\cdot 5^2 + \cdots + 3\cdot 5^n = 3(5^{n+1}-1)/4$. To prove that this is true for all nonnegative integers n, we proceed by mathematical induction. First we verify $P(0)$, namely that $3 = 3(5-1)/4$, which is certainly true. Next we assume that $P(k)$ is true and try to derive $P(k+1)$. Now $P(k+1)$ is the formula

$$3 + 3\cdot 5 + 3\cdot 5^2 + \cdots + 3\cdot 5^k + 3\cdot 5^{k+1} = \frac{3(5^{k+2}-1)}{4}.$$

All but the last term of the left-hand side of this equation is exactly the left-hand side of $P(k)$, so by the inductive hypothesis, it equals $3(5^{k+1}-1)/4$. Thus we have

$$\begin{aligned}3 + 3\cdot 5 + 3\cdot 5^2 + \cdots + 3\cdot 5^k + 3\cdot 5^{k+1} &= \frac{3(5^{k+1}-1)}{4} + 3\cdot 5^{k+1}\\ &= 5^{k+1}\left(\frac{3}{4}+3\right) - \frac{3}{4} = 5^{k+1}\cdot\frac{15}{4} - \frac{3}{4}\\ &= 5^{k+2}\cdot\frac{3}{4} - \frac{3}{4} = \frac{3(5^{k+2}-1)}{4}.\end{aligned}$$

9. a) We can obtain a formula for the sum of the first n even positive integers from the formula for the sum of the first n positive integers, since $2+4+6+\cdots+2n = 2(1+2+3+\cdots+n)$. Therefore, using the result of Example 1, the sum of the first n even positive integers is $2\big(n(n+1)/2\big) = n(n+1)$.

b) We want to prove the proposition $P(n): 2+4+6+\cdots+2n = n(n+1)$. The basis step, $n=1$, says that $2 = 1\cdot(1+1)$, which is certainly true. For the inductive step, we assume that $P(k)$ is true, namely that

$$2+4+6+\cdots+2k = k(k+1)\,,$$

and try to prove from this assumption that $P(k+1)$ is true, namely that

$$2+4+6+\cdots+2k+2(k+1) = (k+1)(k+2)\,.$$

(Note that the left-hand side consists of the sum of the first $k+1$ even positive integers.) We have

$$\begin{aligned} 2+4+6+\cdots+2k+2(k+1) &= (2+4+6+\cdots+2k)+2(k+1) \\ &= k(k+1)+2(k+1) \quad \text{(by the inductive hypothesis)} \\ &= (k+1)(k+2)\,, \end{aligned}$$

as desired, and our proof by mathematical induction is complete.

11. a) Let us compute the values of this sum for $n \le 4$ to see whether we can discover a pattern. For $n=1$ the sum is $\frac{1}{2}$. For $n=2$ the sum is $\frac{1}{2}+\frac{1}{4}=\frac{3}{4}$. For $n=3$ the sum is $\frac{1}{2}+\frac{1}{4}+\frac{1}{8}=\frac{7}{8}$. And for $n=4$ the sum is $15/16$. The pattern seems pretty clear, so we conjecture that the sum is always $(2^n-1)/2^n$.

b) We have already verified that this is true in the base case (in fact, in four base cases). So let us assume it for k and try to prove it for $k+1$. More formally, we are letting $P(n)$ be the *statement* that

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^n} = \frac{2^n-1}{2^n}\,,$$

and trying to prove that $P(n)$ is true for all n. We have already verified $P(1)$ (as well as $P(2)$, $P(3)$, and $P(4)$ for good measure). We now assume the inductive hypothesis $P(k)$, which is the equation displayed above with k substituted for n, and must derive $P(k+1)$, which is the equation

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^k}+\frac{1}{2^{k+1}} = \frac{2^{k+1}-1}{2^{k+1}}.$$

The "obvious" thing to try is to add $1/2^{k+1}$ to both sides of the inductive hypothesis and see whether the algebra works out as we hope it will. We obtain

$$\left(\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^k}\right)+\frac{1}{2^{k+1}} = \frac{2^k-1}{2^k}+\frac{1}{2^{k+1}} = \frac{2\cdot 2^k - 2\cdot 1+1}{2^{k+1}} = \frac{2^{k+1}-1}{2^{k+1}}\,,$$

as desired.

13. The base case of the statement $P(n): 1^2-2^2+3^2-\cdots+(-1)^{n-1}n^2 = (-1)^{n-1}n(n+1)/2$, when $n=1$, is $1^2 = (-1)^0\cdot 1\cdot 2/2$, which is certainly true. Assume the inductive hypothesis $P(k)$, and try to derive $P(k+1)$:

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

Starting with the left-hand side of $P(k+1)$, we have

$$\begin{aligned} &\big(1^2-2^2+3^2-\cdots+(-1)^{k-1}k^2\big)+(-1)^k(k+1)^2 \\ &\qquad = (-1)^{k-1}\frac{k(k+1)}{2}+(-1)^k(k+1)^2 \quad \text{(by the inductive hypothesis)} \\ &\qquad = (-1)^k(k+1)\big((-k/2)+k+1\big) \\ &\qquad = (-1)^k(k+1)\left(\frac{k}{2}+1\right) = (-1)^k\frac{(k+1)(k+2)}{2}\,, \end{aligned}$$

the right-hand side of $P(k+1)$.

15. The base case of the statement $P(n): 1\cdot 2 + 2\cdot 3 + \cdots + n(n+1) = n(n+1)(n+2)/3$, when $n=1$, is $1\cdot 2 = 1\cdot 2\cdot 3/3$, which is certainly true. We assume the inductive hypothesis $P(k)$, and try to derive $P(k+1)$:

$$1\cdot 2 + 2\cdot 3 + \cdots + k(k+1) + (k+1)(k+2) = \frac{(k+1)(k+2)(k+3)}{3}$$

Starting with the left-hand side of $P(k+1)$, we have

$$\begin{aligned}
&\big(1\cdot 2 + 2\cdot 3 + \cdots + k(k+1)\big) + (k+1)(k+2)\\
&\quad= \frac{k(k+1)(k+2)}{3} + (k+1)(k+2) \quad \text{(by the inductive hypothesis)}\\
&\quad= (k+1)(k+2)\left(\frac{k}{3}+1\right) = \frac{(k+1)(k+2)(k+3)}{3},
\end{aligned}$$

the right-hand side of $P(k+1)$.

17. This proof follows the basic pattern of the solution to Exercise 3, but the algebra gets more complex. The statement $P(n)$ that we wish to prove is

$$1^4 + 2^4 + 3^4 + \cdots + n^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30},$$

where n is a positive integer. The basis step, $n=1$, is true, since $1\cdot 2\cdot 3\cdot 5/30 = 1$. Assume the displayed statement as the inductive hypothesis, and proceed as follows to prove $P(n+1)$:

$$\begin{aligned}
(1^4 + 2^4 + \cdots + n^4) + (n+1)^4 &= \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30} + (n+1)^4\\
&= \frac{n+1}{30}\big(n(2n+1)(3n^2+3n-1) + 30(n+1)^3\big)\\
&= \frac{n+1}{30}(6n^4 + 39n^3 + 91n^2 + 89n + 30)\\
&= \frac{n+1}{30}(n+2)(2n+3)(3(n+1)^2 + 3(n+1) - 1)
\end{aligned}$$

The last equality is straightforward to check; it was obtained not by attempting to factor the next to last expression from scratch but rather by knowing exactly what we expected the simplified expression to be.

19. **a)** $P(2)$ is the statement that $1 + \frac{1}{4} < 2 - \frac{1}{2}$.

b) This is true because $5/4$ is less than $6/4$.

c) The inductive hypothesis is the statement that

$$1 + \frac{1}{4} + \cdots + \frac{1}{k^2} < 2 - \frac{1}{k}.$$

d) For the inductive step, we want to show for each $k \ge 2$ that $P(k)$ implies $P(k+1)$. In other words, we want to show that assuming the inductive hypothesis (see part **(c)**) we can show

$$1 + \frac{1}{4} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2} < 2 - \frac{1}{k+1}.$$

e) Assume the inductive hypothesis. Then we have

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

f) We have completed both the basis step and the inductive step, so by the principle of mathematical induction, the statement is true for every positive integer n greater than 1.

21. Let $P(n)$ be the proposition $2^n > n^2$. We want to show that $P(n)$ is true for all $n > 4$. The base case is therefore $n = 5$, and we check that $2^5 = 32 > 25 = 5^2$. Now we assume the inductive hypothesis that $2^k > k^2$ and want to derive the statement that $2^{k+1} > (k+1)^2$. Working from the right-hand side, we have $(k+1)^2 = k^2 + 2k + 1 < k^2 + 2k + k = k^2 + 3k < k^2 + k^2$ (since $k > 3$). Thus we have $(k+1)^2 < 2k^2 < 2 \cdot 2^k$ (by the inductive hypothesis), which in turn equals 2^{k+1}, as desired.

23. We compute the values of $2n + 3$ and 2^n for the first few values of n and come to the immediate conjecture that $2n + 3 \leq 2^n$ for $n \geq 4$ but for no other nonnegative integer values of n. The negative part of this statement is just the fact that $3 > 1$, $5 > 2$, $7 > 4$, and $9 > 8$. We must prove by mathematical induction that $2n + 3 \leq 2^n$ for all $n \geq 4$. The base case is $n = 4$, in which we see that, indeed, $11 \leq 16$. Next assume the inductive hypothesis that $2n + 3 \leq 2^n$, and consider $2(n+1) + 3$. This equals $2n + 3 + 2$, which by the inductive hypothesis is less than or equal to $2^n + 2$. But since $n \geq 1$, this in turn is at most $2^n + 2^n = 2^{n+1}$, precisely the statement we wished to prove.

25. We can assume that $h > -1$ is fixed, and prove the proposition by induction on n. Let $P(n)$ be the proposition $1 + nh \leq (1+h)^n$. The base case is $n = 0$, in which case $P(0)$ is simply $1 \leq 1$, certainly true. Now we assume the inductive hypothesis, that $1 + kh \leq (1+h)^k$; we want to show that $1 + (k+1)h \leq (1+h)^{k+1}$. Since $h > -1$, it follows that $1 + h > 0$, so we can multiply both sides of the inductive hypothesis by $1 + h$ to obtain $(1+h)(1+kh) \leq (1+h)^{k+1}$. Thus to complete the proof it is enough to show that $1 + (k+1)h \leq (1+h)(1+kh)$. But the right-hand side of this inequality is the same as $1 + h + kh + kh^2 = 1 + (k+1)h + kh^2$, which is greater than or equal to $1 + (k+1)h$ because $kh^2 \geq 0$.

27. This exercise involves some messy algebra, but the logic is the usual logic for proofs using the principle of mathematical induction. The basis step ($n = 1$) is true, since 1 is greater than $2(\sqrt{2} - 1) \approx 0.83$. We assume that

$$1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} > 2(\sqrt{n+1} - 1)$$

and try to derive the corresponding statement for $n + 1$:

$$1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} + \frac{1}{\sqrt{n+1}} > 2(\sqrt{n+2} - 1)$$

Since by the inductive hypothesis we know that

$$1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} + \frac{1}{\sqrt{n+1}} > 2(\sqrt{n+1} - 1) + \frac{1}{\sqrt{n+1}},$$

we will be finished if we can show that the inequality

$$2(\sqrt{n+1} - 1) + \frac{1}{\sqrt{n+1}} > 2(\sqrt{n+2} - 1)$$

holds. By canceling the -2 from both sides and rearranging, we obtain the equivalent inequality

$$2(\sqrt{n+2} - \sqrt{n+1}) < \frac{1}{\sqrt{n+1}},$$

which in turn is equivalent to

$$2(\sqrt{n+2} - \sqrt{n+1})(\sqrt{n+2} + \sqrt{n+1}) < \frac{\sqrt{n+1}}{\sqrt{n+1}} + \frac{\sqrt{n+2}}{\sqrt{n+1}}.$$

This last inequality simplifies to

$$2 < 1 + \frac{\sqrt{n+2}}{\sqrt{n+1}},$$

which is clearly true. Therefore the original inequality is true, and our proof is complete.

29. Recall that $H_k = 1/1 + 1/2 + \cdots + 1/k$. We want to prove that $H_{2^n} \le 1 + n$ for all natural numbers n. We proceed by mathematical induction, noting that the basis step $n = 0$ is the trivial statement $H_1 = 1 \le 1 + 0$. Therefore we assume that $H_{2^n} \le 1 + n$; we want to show that $H_{2^{n+1}} \le 1 + (n+1)$. We have

$$\begin{aligned} H_{2^{n+1}} &= H_{2^n} + \frac{1}{2^n+1} + \frac{1}{2^n+2} + \cdots + \frac{1}{2^{n+1}} \quad \text{(by definition; there are } 2^n \text{ fractions here)} \\ &\le (1+n) + \frac{1}{2^n+1} + \frac{1}{2^n+2} + \cdots + \frac{1}{2^{n+1}} \quad \text{(by the inductive hypothesis)} \\ &\le (1+n) + \frac{1}{2^n+1} + \frac{1}{2^n+1} + \cdots + \frac{1}{2^n+1} \quad \text{(we made the denominators smaller)} \\ &= 1 + n + \frac{2^n}{2^n+1} < 1 + n + 1 = 1 + (n+1). \end{aligned}$$

31. This is easy to prove without mathematical induction, because we can observe that $n^2 + n = n(n+1)$, and either n or $n+1$ is even. If we want to use the principle of mathematical induction, we can proceed as follows. The basis step is the observation that $1^2 + 1 = 2$ is divisible by 2. Assume the inductive hypothesis, that $k^2 + k$ is divisible by 2; we must show that $(k+1)^2 + (k+1)$ is divisible by 2. But $(k+1)^2 + (k+1) = k^2 + 2k + 1 + k + 1 = (k^2 + k) + 2(k+1)$. But now $k^2 + k$ is divisible by 2 by the inductive hypothesis, and $2(k+1)$ is divisible by 2 by definition, so this sum of two multiples of 2 must be divisible by 2.

33. To prove that $P(n): 5 \mid (n^5 - n)$ holds for all nonnegative integers n, we first check that $P(0)$ is true; indeed $5 \mid 0$. Next assume that $5 \mid (n^5 - n)$, so that we can write $n^5 - n = 5t$ for some integer t. Then we want to prove $P(n+1)$, namely that $5 \mid \big((n+1)^5 - (n+1)\big)$. We expand and then factor the right-hand side to obtain

$$\begin{aligned} (n+1)^5 - (n+1) &= n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1 - n - 1 \\ &= (n^5 - n) + 5(n^4 + 2n^3 + 2n^2 + n) \\ &= 5t + 5(n^4 + 2n^3 + 2n^2 + n) \quad \text{(by the inductive hypothesis)} \\ &= 5(t + n^4 + 2n^3 + 2n^2 + n). \end{aligned}$$

Thus we have shown that $(n+1)^5 - (n+1)$ is also a multiple of 5, and our proof by induction is complete. (Note that here we have used n as the dummy variable in the inductive step, rather than k. It really makes no difference.)

We should point out that using mathematical induction is not the only way to prove this proposition; it can also be proved by considering the five cases determined by the value of n **mod** 5. The reader is encouraged to write down such a proof.

35. First let us rewrite this proposition so that it is a statement about all nonnegative integers, rather than just the odd positive integers. An odd positive integer can be written as $2n - 1$, so let us prove the proposition $P(n)$ that $(2n-1)^2 - 1$ is divisible by 8 for all positive integers n. We first check that $P(1)$ is true; indeed $8 \mid 0$. Next assume that $8 \mid ((2n-1)^2 - 1)$. Then we want to prove $P(n+1)$, namely that $8 \mid ((2n+1)^2 - 1)$. Let us look at the difference of these two expressions: $(2n+1)^2 - 1 - ((2n-1)^2 - 1)$. A little algebra reduces this to $8n$, which is certainly a multiple of 8. But if this difference is a multiple of 8, and if, by the inductive hypothesis, $(2n-1)^2 - 1$ is a multiple of 8, then $(2n+1)^2 - 1$ must be a multiple of 8, and our proof by induction is complete.

37. It is not easy to stumble upon the trick needed in the inductive step in this exercise, so do not feel bad if you did not find it. The form is straightforward. For the basis step $(n = 1)$, we simply observe that $11^{1+1} + 12^{2\,1-1} = 121 + 12 = 133$, which is divisible by 133. Then we assume the inductive hypothesis, that

$11^{n+1} + 12^{2n-1}$ is divisible by 133, and let us look at the expression when $n+1$ is plugged in for n. We want somehow to manipulate it so that the expression for n appears. We have

$$\begin{aligned} 11^{(n+1)+1} + 12^{2(n+1)-1} &= 11 \cdot 11^{n+1} + 144 \cdot 12^{2n-1} \\ &= 11 \cdot 11^{n+1} + (11 + 133) \cdot 12^{2n-1} \\ &= 11(11^{n+1} + 12^{2n-1}) + 133 \cdot 12^{2n-1}. \end{aligned}$$

Looking at the last line, we see that the expression in parentheses is divisible by 133 by the inductive hypothesis, and obviously the second term is divisible by 133, so the entire quantity is divisible by 133, as desired.

39. The basis step is trivial, as usual: $A_1 \subseteq B_1$ implies that $\bigcap_{j=1}^{1} A_j \subseteq \bigcap_{j=1}^{1} B_j$ because the intersection of one set is itself. Assume the inductive hypothesis that if $A_j \subseteq B_j$ for $j = 1, 2, \ldots, k$, then $\bigcap_{j=1}^{k} A_j \subseteq \bigcap_{j=1}^{k} B_j$. We want to show that if $A_j \subseteq B_j$ for $j = 1, 2, \ldots, k+1$, then $\bigcap_{j=1}^{k+1} A_j \subseteq \bigcap_{j=1}^{k+1} B_j$. To show that one set is a subset of another we show that an arbitrary element of the first set must be an element of the second set. So let $x \in \bigcap_{j=1}^{k+1} A_j = \left(\bigcap_{j=1}^{k} A_j\right) \cap A_{k+1}$. Because $x \in \bigcap_{j=1}^{k} A_j$, we know by the inductive hypothesis that $x \in \bigcap_{j=1}^{k} B_j$; because $x \in A_{k+1}$, we know from the given fact that $A_{k+1} \subseteq B_{k+1}$ that $x \in B_{k+1}$. Therefore $x \in \left(\bigcap_{j=1}^{k} B_j\right) \cap B_{k+1} = \bigcap_{j=1}^{k+1} B_j$.

This is really easier to do directly than by using the principle of mathematical induction. For a noninductive proof, suppose that $x \in \bigcap_{j=1}^{n} A_j$. Then $x \in A_j$ for each j from 1 to n. Since $A_j \subseteq B_j$, we know that $x \in B_j$. Therefore by definition, $x \in \bigcap_{j=1}^{n} B_j$.

41. In order to prove this statement, we need to use one of the distributive laws from set theory: $(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$ (see Section 2.2). Indeed, the proposition at hand is the generalization of this distributive law, from two sets in the union to n sets in the union. We will also be using implicitly the associative law for set union.

The basis step, $n = 1$, is the statement $A_1 \cap B = A_1 \cap B$, which is obviously true. Therefore we assume the inductive hypothesis that

$$(A_1 \cup A_2 \cup \cdots \cup A_n) \cap B = (A_1 \cap B) \cup (A_2 \cap B) \cup \cdots \cup (A_n \cap B).$$

We wish to prove the similar statement for $n+1$, namely

$$(A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1}) \cap B = (A_1 \cap B) \cup (A_2 \cap B) \cup \cdots \cup (A_n \cap B) \cup (A_{n+1} \cap B).$$

Starting with the left-hand side, we apply the distributive law for two sets:

$$\begin{aligned} \big((A_1 \cup A_2 \cup \cdots \cup A_n) \cup A_{n+1}\big) \cap B &= \big((A_1 \cup A_2 \cup \cdots \cup A_n) \cap B\big) \cup (A_{n+1} \cap B) \\ &= \big((A_1 \cap B) \cup (A_2 \cap B) \cup \cdots \cup (A_n \cap B)\big) \cup (A_{n+1} \cap B) \\ &\qquad \text{(by the inductive hypothesis)} \\ &= (A_1 \cap B) \cup (A_2 \cap B) \cup \cdots \cup (A_n \cap B) \cup (A_{n+1} \cap B) \end{aligned}$$

43. In order to prove this statement, we need to use one of De Morgan's laws from set theory: $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$ (see Section 2.2). Indeed, the proposition at hand is the generalization of this law, from two sets in the union to n sets in the union. We will also be using implicitly the associative laws for set union and intersection.

The basis step, $n = 1$, is the statement $\overline{A_1} = \overline{A_1}$ (since the union or intersection of just one set is the set itself), and this proposition is obviously true. Therefore we assume the inductive hypothesis that

$$\overline{\bigcup_{k=1}^{n} A_k} = \bigcap_{k=1}^{n} \overline{A_k}.$$

We wish to prove the similar statement for $n+1$, namely

$$\overline{\bigcup_{k=1}^{n+1} A_k} = \bigcap_{k=1}^{n+1} \overline{A_k}\,.$$

Starting with the left-hand side, we group, apply De Morgan's law for two sets, and then the inductive hypothesis:

$$\begin{aligned}
\overline{\bigcup_{k=1}^{n+1} A_k} &= \overline{(\bigcup_{k=1}^{n} A_k) \cup A_{n+1}} \\
&= \overline{\bigcup_{k=1}^{n} A_k} \cap \overline{A_{n+1}} \quad \text{(by DeMorgan's law)} \\
&= (\bigcap_{k=1}^{n} \overline{A_k}) \cap \overline{A_{n+1}} \quad \text{(by the inductive hypothesis)} \\
&= \bigcap_{k=1}^{n+1} \overline{A_k}
\end{aligned}$$

45. This proof will be similar to the proof in Example 10. The basis step is clear, since for $n = 2$, the set has exactly one subset containing exactly two elements, and $2(2-1)/2 = 1$. Assume the inductive hypothesis, that a set with n elements has $n(n-1)/2$ subsets with exactly two elements; we want to prove that a set S with $n+1$ elements has $(n+1)n/2$ subsets with exactly two elements. Fix an element a in S, and let T be the set of elements of S other than a. There are two varieties of subsets of S containing exactly two elements. First there are those that do not contain a. These are precisely the two-element subsets of T, and by the inductive hypothesis, there are $n(n-1)/2$ of them. Second, there are those that contain a together with one element of T. Since T has n elements, there are exactly n subsets of this type. Therefore the total number of subsets of S containing exactly two elements is $(n(n-1)/2) + n$, which simplifies algebraically to $(n+1)n/2$, as desired.

47. The hint gives the greedy algorithm. We reorder the locations if necessary so that $x_1 \le x_2 \le x_3 \le \cdots \le x_d$. The first tower is placed at position $t_1 = x_1 + 1$. It will serve the first building and any other buildings at locations no greater than $t_1 + 1$. Assume that we have placed tower k at t_k. Then place tower $k+1$ at position $t_{k+1} = x + 1$, where x is the smallest x_i greater than $t_k + 1$. Because all the buildings up to the one at position x were already serviced by the previous towers, and the building at position x is serviced by the new tower at t_{k+1}, all the buildings will be serviced once this process is completed.

49. The one and only flaw in this proof is in this statement, which is part of the inductive step: "the set of the first n horses and the set of the last n horses [in the collection of $n+1$ horses being considered] overlap." The only assumption made about the number n in this argument is that n is a positive integer. When $n = 1$, so that $n + 1 = 2$, the statement quoted is obviously nonsense: the set of the first one horse and the set of the last one horse, in this set of two horses, are disjoint.

51. The mistake is in applying the inductive hypothesis to look at $\max(x-1, y-1)$, because even though x and y are positive integers, $x-1$ and $y-1$ need not be (one or both could be 0). In fact, that is what happens if we let $x = 1$ and $y = 2$ when $k = 1$.

53. The base case ($n = 2$) is the old "I cut and you choose" approach. The first person cuts the cake into two portions that she thinks are each $1/2$ of the cake. The second person chooses the portion he thinks is at least $1/2$ of the cake (at least one of the pieces must satisfy that condition). For the inductive step, suppose there are $k+1$ people. By the inductive hypothesis, we can suppose that the first k people have divided the cake among themselves so that each person is satisfied that he got at least a fraction $1/k$ of the cake. Each of them now cuts his or her piece into $k+1$ pieces of equal size. The last person gets to choose one piece from each of the first k people's portions. After this is done, each of the first k people is satisfied that she still has $(1/k)(k/(k+1)) = 1/(k+1)$ of the cake. To see that the last person is satisfied, suppose that he thought that the i^{th} person $(1 \le i \le k)$ had a portion p_i of the cake, where $\sum_{i=1}^{k} p_i = 1$. By choosing what he thinks is the largest piece from each person, he is satisfied that he has at least $\sum_{i=1}^{k} p_i/(k+1) = (1/(k+1)) \sum_{i=1}^{k} p_i = 1/(k+1)$ of the cake.

55. We use the notation (i,j) to mean the square in row i and column j, where we number from the left and from the bottom, starting at $(0,0)$ in the lower left-hand corner. We use induction on $i+j$ to show that every square can be reached by the knight. There are six base cases, for the cases when $i+j \le 2$. The knight is already at $(0,0)$ to start, so the empty sequence of moves reaches that square. To reach $(1,0)$, the knight moves successively from $(0,0)$ to $(2,1)$ to $(0,2)$ to $(1,0)$. Similarly, to reach $(0,1)$, the knight moves successively from $(0,0)$ to $(1,2)$ to $(2,0)$ to $(0,1)$. Note that the knight has reached $(2,0)$ and $(0,2)$ in the process. For the last basis step, note this path to $(1,1)$: $(0,0)$ to $(1,2)$ to $(2,0)$ to $(0,1)$ to $(2,2)$ to $(0,3)$ to $(1,1)$. We now assume the inductive hypothesis, that the knight can reach any square (i,j) for which $i+j=k$, where k is an integer greater than 1, and we want to show how the knight can reach each square (i,j) when $i+j=k+1$. Since $k+1 \ge 3$, at least one of i and j is at least 2. If $i \ge 2$, then by the inductive hypothesis, there is a sequence of moves ending at $(i-2, j+1)$, since $i-2+j+1 = i+j-1 = k$; from there it is just one step to (i,j). Similarly, if $j \ge 2$, then by the inductive hypothesis, there is a sequence of moves ending at $(i+1, j-2)$, since $i+1+j-2 = i+j-1 = k$; from there it is again just one step to (i,j).

57. The base cases are $n=0$ and $n=1$, and it is a simple matter to evaluate, directly from the "limit of difference quotient" definition, the derivatives of $x^0 = 1$ and $x^1 = x$:

$$\frac{d}{dx}x^0 = \lim_{h\to 0}\frac{(x+h)^0 - x^0}{h} = \lim_{h\to 0}\frac{1-1}{h} = 0 = 0\cdot x^{-1}$$
$$\frac{d}{dx}x^1 = \lim_{h\to 0}\frac{(x+h)^1 - x^1}{h} = \lim_{h\to 0}\frac{h}{h} = 1 = 1\cdot x^0$$

We are told to assume that the product rule holds:

$$\frac{d}{dx}(f(x)\cdot g(x)) = f(x)\cdot g'(x) + g(x)\cdot f'(x)$$

So we work as follows, invoking the inductive hypothesis and the base cases:

$$\begin{aligned}\frac{d}{dx}x^{n+1} &= \frac{d}{dx}(x\cdot x^n) = x\cdot\frac{d}{dx}x^n + x^n\cdot\frac{d}{dx}x \\ &= x\cdot nx^{n-1} + x^n\cdot 1 = nx^n + x^n = (n+1)x^n\end{aligned}$$

59. We prove this by induction on k. The basis step $k=0$ is the trivial statement that $1 \equiv 1 \pmod{m}$. Suppose that the statement is true for k. We must show it for $k+1$. So let $a \equiv b \pmod{m}$. By the inductive hypothesis we know that $a^k \equiv b^k \pmod{m}$. Then we apply Theorem 5 from Section 4.1 to conclude that $a\cdot a^k \equiv b\cdot b^k \pmod{m}$, which by definition says that $a^{k+1} \equiv b^{k+1} \pmod{m}$, as desired.

61. Let $P(n)$ be the proposition

$$[(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \cdots \wedge (p_{n-1} \to p_n)] \to [(p_1 \wedge p_2 \wedge \cdots \wedge p_{n-1}) \to p_n].$$

We want to prove this proposition for all $n \ge 2$. The basis step, $(p_1 \to p_2) \to (p_1 \to p_2)$, is clearly true (a tautology), since every proposition implies itself. Now we assume $P(n)$ and want to show $P(n+1)$, namely

$$\begin{aligned}&[(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \cdots \wedge (p_{n-1} \to p_n) \wedge (p_n \to p_{n+1})] \to \\ &\qquad [(p_1 \wedge p_2 \wedge \cdots \wedge p_{n-1} \wedge p_n) \to p_{n+1}].\end{aligned}$$

To show this, we will assume that the hypothesis (everything in the first square brackets) is true and show that the conclusion (the conditional statement in the second square brackets) is also true.

So we assume $(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \cdots \wedge (p_{n-1} \to p_n) \wedge (p_n \to p_{n+1})$. By the associativity of $\wedge$, we can group this as $\big((p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \cdots \wedge (p_{n-1} \to p_n)\big) \wedge (p_n \to p_{n+1})$. By the simplification rule, we can conclude that the first group, $(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \cdots \wedge (p_{n-1} \to p_n)$, must be true. Now the inductive hypothesis allows us to conclude that $(p_1 \wedge p_2 \wedge \cdots \wedge p_{n-1}) \to p_n$. This together with the rest of the assumption, namely $p_n \to p_{n+1}$, yields, by the hypothetical syllogism rule, $(p_1 \wedge\ p_2 \wedge \cdots \wedge p_{n-1}) \to p_{n+1}$.

That is almost what we wanted to prove, but not quite. We wanted to prove that $(p_1 \wedge p_2 \wedge \cdots \wedge p_{n-1} \wedge p_n) \to p_{n+1}$. In order to prove this, let us assume its hypothesis, $p_1 \wedge p_2 \wedge \cdots \wedge p_{n-1} \wedge p_n$. Again using the simplification rule we obtain $p_1 \wedge\ p_2 \wedge \cdots \wedge p_{n-1}$. Now by modus ponens with the proposition $(p_1 \wedge\ p_2 \wedge \cdots \wedge p_{n-1}) \to p_{n+1}$, which we proved above, we obtain p_{n+1}. Thus we have proved $(p_1 \wedge\ p_2 \wedge \cdots \wedge p_{n-1} \wedge p_n) \to p_{n+1}$, as desired.

63. This exercise, as the double star indicates, is quite hard. The trick is to induct not on n itself, but rather on $\log_2 n$. In other words, we write $n = 2^k$ and prove the statement by induction on k. This will prove the statement for every n that is a power of 2; a separate argument is needed to extend to the general case.

We take the basis step to be $k = 1$ (the case $k = 0$ is trivially true, as well), so that $n = 2^1 = 2$. In this case the trick is to start with the true inequality $(\sqrt{a_1} - \sqrt{a_2})^2 \ge 0$. Expanding, we have $a_1 - 2\sqrt{a_1a_2} + a_2 \ge 0$, whence $(a_1 + a_2)/2 \ge (a_1a_2)^{1/2}$, as desired. For the inductive step, we assume that the inequality holds for $n = 2^k$ and prove that it also holds for $2n = 2^{k+1}$. What we need to show, then, is that

$$\frac{a_1 + a_2 + \cdots + a_{2n}}{2n} \ge (a_1a_2 \cdots a_{2n})^{1/(2n)}.$$

First we observe that

$$\frac{a_1 + a_2 + \cdots + a_{2n}}{2n} = \left(\frac{a_1 + a_2 + \cdots + a_n}{n} + \frac{a_{n+1} + a_{n+2} + \cdots + a_{2n}}{n}\right) \Big/ 2$$

and

$$(a_1a_2 \cdots a_{2n})^{1/(2n)} = \Big((a_1a_2 \cdots a_n)^{1/n}(a_{n+1}a_{n+2} \cdots a_{2n})^{1/n}\Big)^{1/2}.$$

Now to simplify notation, let $A(x, y, \ldots)$ denote the arithmetic mean and $G(x, y, \ldots)$ denote the geometric mean of the numbers $x, y, \ldots$. It is clear that if $x \le x'$, $y \le y'$, and so on, then $A(x, y, \ldots) \le A(x', y', \ldots)$ and $G(x, y, \ldots) \le G(x', y', \ldots)$. Now we have

$$\begin{aligned} A(a_1, \ldots, a_{2n}) &= A\big(A(a_1, \ldots, a_n), A(a_{n+1}, \ldots, a_{2n})\big) \quad \text{(by the first observation above)} \\ &\ge A\big(G(a_1, \ldots, a_n), G(a_{n+1}, \ldots, a_{2n})\big) \quad \text{(by the inductive hypothesis)} \\ &\ge G\big(G(a_1, \ldots, a_n), G(a_{n+1}, \ldots, a_{2n})\big) \quad \text{(this was the case } n = 2) \\ &= G(a_1, \ldots, a_{2n}) \quad \text{(by the second observation above)}. \end{aligned}$$

Having proved the inequality in the case in which n is a power of 2, we now turn to the case of n that is not a power of 2. Let m be the smallest power of 2 bigger than m. (For instance, if $n = 25$, then $m = 32$.) Denote the arithmetic mean $A(a_1, \ldots, a_n)$ by a, and set $a_{n+1} = a_{n+2} = \cdots = a_m$ all equal to a. One effect of this is that then $A(a_1, \ldots, a_m) = a$. Now we have

$$\left(\Big(\prod_{i=1}^{n} a_i\Big)a^{m-n}\right)^{1/m} \le A(a_1, \ldots, a_m)$$

by the case we have already proved, since m is a power of 2. Using algebra on the left-hand side and the observation that $A(a_1, \ldots, a_m) = a$ on the right, we obtain

$$\Big(\prod_{i=1}^{n} a_i\Big)^{1/m} a^{1-n/m} \le a$$

or

$$\left(\prod_{i=1}^{n} a_i\right)^{1/m} \leq a^{n/m}.$$

Finally we raise both sides to the power m/n to give

$$\left(\prod_{i=1}^{n} a_i\right)^{1/n} \leq a,$$

as desired.

65. Let us check the cases $n = 1$ and $n = 2$, both to establish the basis and to try to see what is going on. For $n = 1$ there is only one nonempty subset of $\{1\}$, so the left-hand side is just $\frac{1}{1}$, and that equals 1. For $n = 2$ there are three nonempty subsets: $\{1\}$, $\{2\}$, and $\{1,2\}$, so the left-hand side is $\frac{1}{1} + \frac{1}{2} + \frac{1}{1\cdot 2} = 2$. To prove the inductive step, assume that the statement is true for n, and consider it for $n+1$. Now the set of the first $n+1$ positive integers has many nonempty subsets, but they fall into three categories: a nonempty subset of the first n positive integers, a nonempty subset of the first n positive integers together with $n+1$, or just $\{n+1\}$. So we need to sum over these three categories. By the inductive hypothesis, the sum over the first category is n. For the second category, we can factor out $\frac{1}{n+1}$ from each term of the sum, note that the remaining factor again gives n by the inductive hypothesis, and so conclude that this part of the sum is $\frac{n}{n+1}$. Finally, the third category simply yields the value $\frac{1}{n+1}$. Therefore the entire summation is $n + \frac{n}{n+1} + \frac{1}{n+1} = n + 1$, as desired.

67. The basis step ($n = 2$) is clear, because if $A_1 \subseteq A_2$, then A_1 satisfies the condition of being a subset of each set in the collection, and otherwise A_2 does, because in that case, A_2 must be a subset of A_1 (by the stated assumptions). For the inductive step, assume the inductive hypothesis, that the conditional statement is true for k sets, and suppose we are given $k+1$ sets that satisfy the given conditions. By the inductive hypothesis, there must be a set A_i for some $i \leq k$ such that $A_i \subseteq A_j$ for $1 \leq j \leq k$. If $A_i \subseteq A_{k+1}$, then we are done. Otherwise, we know that $A_{k+1} \subseteq A_i$, and this tells us that A_{k+1} satisfies the condition of being a subset of A_j for $1 \leq j \leq k+1$.

69. Number the people 1, 2, 3, and 4, and let s_i be the scandal originally known only to person i. It is clear that $G(1) = 0$ and $G(2) = 1$. For three people, without loss of generality assume that 1 calls 2 first and 1 calls 3 next. At this point 1 and 3 know all three scandals, but it takes one more call to let 2 know s_3. Thus $G(3) = 3$. For four people, without loss of generality assume that 1 calls 2 first. If now 3 calls 4, then after two calls 1 and 2 both know s_1 and s_2, while 3 and 4 both know s_3 and s_4. It is clear that two more calls (between 1 and 3, and between 2 and 4, say) are necessary and sufficient to complete the exchange. This makes a total of four calls. The only other case to consider (to see whether $G(4)$ might be less than 4) is when the second call, without loss of generality, occurs between 1 and 3. At this point, both 2 and 4 still need to learn s_3, and talking to each other won't give them that information, so at least two more calls would be required. Thus $G(4) = 4$.

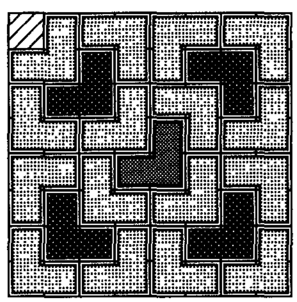
71. We need to show that $2n - 4$ calls are both necessary and sufficient to exchange all the gossip. Sufficiency is easier. Select four of the people, say 1, 2, 3, and 4, to be the central committee. Every person outside the central committee calls one person on the central committee. This takes $n - 4$ calls, and at this point the central committee members *as a group* know all the scandals. They then exchange information among themselves by making the calls 12, 34, 13, and 24 in that order (of course the first two can be done in parallel and the last two can be done in parallel). At this point, *every* central committee member knows all the scandals, and we have used $n - 4 + 4 = n$ calls. Finally, again every person outside the central committee calls one person on the central committee, at which point everyone knows all the scandals. This takes $n - 4$ more calls, for a total of $2n - 4$ calls.

That this cannot be done with fewer than $2n - 4$ calls is much harder to prove, and the proof will not be presented here. For more details, start with this survey article: Sandra M. Hedetniemi, Stephen T. Hedetniemi, and Arthur L. Liestman, "A survey of gossiping and broadcasting in communication networks," *Networks* **18** (1988), no. 4, 319–349.

73. We prove this by mathematical induction. The basis step ($n = 2$) is true tautologically (if $I_1 \cap I_2 \neq \emptyset$ then $I_1 \cap I_2 \neq \emptyset$). The heart of the argument occurs with three sets, so we will give the proof for $n = 3$ explicitly. Recall the notation $(u, v) = \{ x \mid u < x < v \}$. Suppose that the intervals are (a, b), (c, d), and (e, f), where without loss of generality we can assume that $a \leq c \leq e$. Because $(a, b) \cap (e, f) \neq \emptyset$, we must have $e < b$; for a similar reason, $e < d$. It follows that the number halfway between e and the smaller of b and d is common to all three intervals. Now for the inductive step, assume that whenever we have k intervals that have pairwise nonempty intersections then there is a point common to all the intervals, and suppose that we are given intervals I_1, I_2, $\ldots$, I_{k+1} that have pairwise nonempty intersections. For each i from 1 to k, let $J_i = I_i \cap I_{k+1}$. We claim that the collection J_1, J_2, $\ldots$, J_k satisfies the inductive hypothesis, that is, that $J_{i_1} \cap J_{i_2} \neq \emptyset$ for each choice of subscripts i_1 and i_2. This follows from the $n = 3$ case proved above, using the sets I_{i_1}, I_{i_2}, and I_{k+1}. We can now invoke the inductive hypothesis to conclude that there is a number common to all of the sets J_i for $i = 1, 2, \ldots, k$, which perforce is in the intersection of all the sets I_i for $i = 1, 2, \ldots, k + 1$.

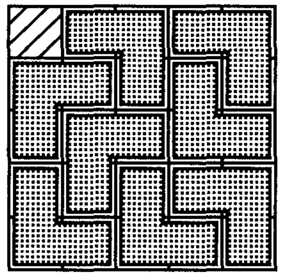
75. Pair up the people. Have the people stand at mutually distinct small distances from their partners but far away from everyone else. Then each person throws a pie at his or her partner, so everyone gets hit.

77. The proof in Example 14 guides us to one solution (it is certainly not unique). We begin by placing a right triomino in the center, with its gap in the same quadrant as the missing square in the upper left corner of the board (this piece is distinctively shaded in our solution below). This reduces the problem to four problems on 4×4 boards. Then we place triominoes in the centers of these four quadrants, using the same principle (shaded somewhat differently below). Finally, we place pieces in the remaining squares to fill up each quadrant.



79. This problem is very similar to Example 14; the only difficulty is in visualizing what's happening in three dimensions. The basis step ($n = 1$) is trivial, since one tile coincides with the solid to be tiled. To make this read a little easier, let us call a $1 \times 1 \times 1$ cube a "cubie"; and let us call the object we are tiling with, namely the $2 \times 2 \times 2$ cube with one cubie removed, a tile. For the inductive step, assume the inductive hypothesis, that the $2^n \times 2^n \times 2^n$ cube with one cubie removed can be covered with tiles, and suppose that a $2^{n+1} \times 2^{n+1} \times 2^{n+1}$ cube with one cubie removed is given. We must show how to cover it with tiles. Think of this large object as split into eight octants through its center, by planes parallel to the faces. The missing cubie occurs in one of these octants. Now position one tile with its center at the center of the large object, so that the missing cubie in the tile lies in the octant in which the large object is missing its cubie. This creates eight $2^n \times 2^n \times 2^n$ cubes, each missing exactly one cubie—one in each octant. By the inductive hypothesis, we can fill each of these smaller objects with tiles. Putting these tilings together gives us the desired tiling of the $2^{n+1} \times 2^{n+1} \times 2^{n+1}$ cube with one cubie removed, as desired.

81. For this specific tiling, the most straightforward proof consists of producing the desired picture. It can be discovered by playing around with the tiles (either make a set, or use paper and pencil).



83. Let $Q(n)$ be $P(n+b-1)$. Thus $Q(1)$ is $P(b)$, $Q(2)$ is $P(b+1)$, and so on. Therefore the statement that $P(n)$ is true for $n = b, b+1, b+2, \ldots$ is the same as the statement that $Q(m)$ is true for all positive integers m. We are given that $P(b)$ is true (i.e., that $Q(1)$ is true), and that $P(k) \to P(k+1)$ for all $k \geq b$ (i.e., that $Q(m) \to Q(m+1)$ for all positive integers m). Therefore by the principle of mathematical induction, $Q(m)$ is true for all positive integers m, as desired.

SECTION 5.2 Strong Induction and Well-Ordering

In this section we extend the technique of proof by mathematical induction by using a stronger inductive hypothesis. The inductive step is now to prove the proposition for $k+1$, assuming the inductive hypothesis that the proposition is true for all values less than or equal to k. Aside from that, the two methods are the same.

1. Let $P(n)$ be the statement that you can run n miles. We want to prove that $P(n)$ is true for all positive integers n. For the basis step we note that the given conditions tell us that $P(1)$ and $P(2)$ are true. For the inductive step, fix $k \geq 2$ and assume that $P(j)$ is true for all $j \leq k$. We want to show that $P(k+1)$ is true. Since $k \geq 2$, $k-1$ is a positive integer less than or equal to k, so by the inductive hypothesis, we know that $P(k-1)$ is true. That is, we know that you can run $k-1$ miles. We were told that "you can always run two more miles once you have run a specified number of miles," so we know that you can run $(k-1)+2 = k+1$ miles. This is $P(k+1)$.

Note that we didn't use strong induction exactly as stated in the text. Instead, we considered both $n = 1$ and $n = 2$ as part of the basis step. We could have more formally included $n = 2$ in the inductive step as a special case. Writing our proof this way, the basis step is just to note that we are told we can run one mile, so $P(1)$ is true. For the inductive step, if $k = 1$ then we are already told that we can run two miles. If $k > 1$, then the inductive hypothesis tells us that we can run $k-1$ miles, so we can run $(k-1)+2 = k+1$ miles.

3. a) $P(8)$ is true, because we can form 8 cents of postage with one 3-cent stamp and one 5-cent stamp. $P(9)$ is true, because we can form 9 cents of postage with three 3-cent stamps. $P(10)$ is true, because we can form 10 cents of postage with two 5-cent stamps.

b) The inductive hypothesis is the statement that using just 3-cent and 5-cent stamps we can form j cents postage for all j with $8 \leq j \leq k$, where we assume that $k \geq 10$.

c) In the inductive step we must show, assuming the inductive hypothesis, that we can form $k+1$ cents postage using just 3-cent and 5-cent stamps.

d) We want to form $k+1$ cents of postage. Since $k \geq 10$, we know that $P(k-2)$ is true, that is, that we can form $k-2$ cents of postage. Put one more 3-cent stamp on the envelope, and we have formed $k+1$ cents of postage, as desired.

e) We have completed both the basis step and the inductive step, so by the principle of strong induction, the statement is true for every integer n greater than or equal to 8.

5. a) We can form the following amounts of postage as indicated: $4 = 4$, $8 = 4+4$, $11 = 11$, $12 = 4+4+4$, $15 = 11+4$, $16 = 4+4+4+4$, $19 = 11+4+4$, $20 = 4+4+4+4+4$, $22 = 11+11$, $23 = 11+4+4+4$, $24 = 4+4+4+4+4+4$, $26 = 11+11+4$, $27 = 11+4+4+4+4$, $28 = 4+4+4+4+4+4+4$, $30 = 11+11+4+4$, $31 = 11+4+4+4+4+4$, $32 = 4+4+4+4+4+4+4+4$, $33 = 11+11+11$. By having considered all the combinations, we know that the gaps in this list cannot be filled. We claim that we can form all amounts of postage greater than or equal to 30 cents using just 4-cent and 11-cent stamps.

b) Let $P(n)$ be the statement that we can form n cents of postage using just 4-cent and 11-cent stamps. We want to prove that $P(n)$ is true for all $n \geq 30$. The basis step, $n = 30$, is handled above. Assume that we can form k cents of postage (the inductive hypothesis); we will show how to form $k+1$ cents of postage. If the k cents included an 11-cent stamp, then replace it by three 4-cent stamps ($3 \cdot 4 = 11 + 1$). Otherwise, k cents was formed from just 4-cent stamps. Because $k \geq 30$, there must be at least eight 4-cent stamps involved. Replace eight 4-cent stamps by three 11-cent stamps, and we have formed $k+1$ cents in postage ($3 \cdot 11 = 8 \cdot 4 + 1$).

c) $P(n)$ is the same as in part **(b)**. To prove that $P(n)$ is true for all $n \geq 30$, we note for the basis step that from part **(a)**, $P(n)$ is true for $n = 30, 31, 32, 33$. Assume the inductive hypothesis, that $P(j)$ is true for all j with $30 \leq j \leq k$, where k is a fixed integer greater than or equal to 33. We want to show that $P(k+1)$ is true. Because $k - 3 \geq 30$, we know that $P(k-3)$ is true, that is, that we can form $k-3$ cents of postage. Put one more 4-cent stamp on the envelope, and we have formed $k+1$ cents of postage, as desired. In this proof our inductive hypothesis included all values between 30 and k inclusive, and that enabled us to jump back four steps to a value for which we knew how to form the desired postage.

7. We can form the following amounts of money as indicated: $2 = 2$, $4 = 2+2$, $5 = 5$, $6 = 2+2+2$. By having considered all the combinations, we know that the gaps in this list (\$1 and \$3) cannot be filled. We claim that we can form all amounts of money greater than or equal to 5 dollars. Let $P(n)$ be the statement that we can form n dollars using just 2-dollar and 5-dollar bills. We want to prove that $P(n)$ is true for all $n \geq 5$. We already observed that the basis step is true for $n = 5$ and 6. Assume the inductive hypothesis, that $P(j)$ is true for all j with $5 \leq j \leq k$, where k is a fixed integer greater than or equal to 6. We want to show that $P(k+1)$ is true. Because $k - 1 \geq 5$, we know that $P(k-1)$ is true, that is, that we can form $k-1$ dollars. Add another 2-dollar bill, and we have formed $k+1$ dollars, as desired.

9. Following the hint, we let $P(n)$ be the statement that there is no positive integer b such that $\sqrt{2} = n/b$. For the basis step, $P(1)$ is true because $\sqrt{2} > 1 \geq 1/b$ for all positive integers b. For the inductive step, assume that $P(j)$ is true for all $j \leq k$, where k is an arbitrary positive integer; we must prove that $P(k+1)$ is true. So assume the contrary, that $\sqrt{2} = (k+1)/b$ for some positive integer b. Squaring both sides and clearing fractions, we have $2b^2 = (k+1)^2$. This tells us that $(k+1)^2$ is even, and so $k+1$ is even as well (the square of an odd number is odd, by Example 1 in Section 1.7). Therefore we can write $k+1 = 2t$ for some positive integer t. Substituting, we have $2b^2 = 4t^2$, so $b^2 = 2t^2$. By the same reasoning as before, b is even, so $b = 2s$ for some positive integer s. Then we have $\sqrt{2} = (k+1)/b = (2t)/(2s) = t/s$. But $t \leq k$, so this contradicts the inductive hypothesis, and our proof of the inductive step is complete.

11. There are four base cases. If $n = 1 = 4 \cdot 0 + 1$, then clearly the first player is doomed, so the second player wins. If there are two, three, or four matches ($n = 4 \cdot 0 + 2$, $n = 4 \cdot 0 + 3$, or $n = 4 \cdot 1$), then the first player can win by removing all but one match. Now assume the strong inductive hypothesis, that in games with k or fewer matches, the first player can win if $k \equiv 0$, 2 or, $3 \pmod 4$ and the second player can win if $k \equiv 1 \pmod 4$. Suppose we have a game with $k+1$ matches, with $k \geq 4$. If $k+1 \equiv 0 \pmod 4$, then the first player can remove three matches, leaving $k-2$ matches for the other player. Since $k-2 \equiv 1 \pmod 4$, by the inductive hypothesis, this is a game that the second player at that point (who is the first player in our game) can win. Similarly, if $k+1 \equiv 2 \pmod 4$, then the first player can remove one match, leaving k matches for the other player. Since $k \equiv 1 \pmod 4$, by the inductive hypothesis, this is a game that the second player at that point (who is the first player in our game) can win. And if $k+1 \equiv 3 \pmod 4$, then the first player can remove two matches, leaving $k-1$ matches for the other player. Since $k-1 \equiv 1 \pmod 4$, by the inductive hypothesis, this is again a game that the second player at that point (who is the first player in our game) can win. Finally, if $k+1 \equiv 1 \pmod 4$, then the first player must leave k, $k-1$, or $k-2$ matches for the other player. Since $k \equiv 0 \pmod 4$, $k-1 \equiv 3 \pmod 4$, and $k-2 \equiv 2 \pmod 4$, by the inductive hypothesis, this is a game that the first player at that point (who is the second player in our game) can win. Thus the first player in our game is doomed, and the proof is complete.

13. Let $P(n)$ be the statement that exactly $n-1$ moves are required to assemble a puzzle with n pieces. Now $P(1)$ is trivially true. Assume that $P(j)$ is true for all $j < n$, and consider a puzzle with n pieces. The final move must be the joining of two blocks, of size k and $n-k$ for some integer k, $1 \leq k \leq n-1$. By the inductive hypothesis, it required $k-1$ moves to construct the one block, and $n-k-1$ moves to construct the other. Therefore $1+(k-1)+(n-k-1) = n-1$ moves are required in all, so $P(n)$ is true. Notice that for variety here we proved $P(n)$ under the assumption that $P(j)$ was true for $j < n$; so n played the role that $k+1$ plays in the statement of strong induction given in the text. It is worthwhile to understand how all of these forms are saying the same thing and to be comfortable moving between them.

15. Let the Chomp board have n rows and n columns. We claim that the first player can win the game by making the first move to leave just the top row and left-most column. (He does this by selecting the cookie in the second column of the second row.) Let $P(n)$ be the statement that if a player has presented his opponent with a Chomp configuration consisting of just n cookies in the top row and n cookies in the left-most column (both of these including the poisoned cookie in the upper left corner), then he can win the game. We will prove $\forall n P(n)$ by strong induction. We know that $P(1)$ is true, because the opponent is forced to take the poisoned cookie at his first turn. Fix $k \geq 1$ and assume that $P(j)$ is true for all $j \leq k$. We claim that $P(k+1)$ is true. It is the opponent's turn to move. If she picks the poisoned cookie, then the game is over and she loses. Otherwise, assume that she picks the cookie in the top row in column j, or the cookie in the left column in row j, for some j with $2 \leq j \leq k+1$. The first player now picks the cookie in the left column in row j, or the cookie in the top row in column j, respectively. This leaves the position covered by $P(j-1)$ for his opponent, so by the inductive hypothesis, he can win.

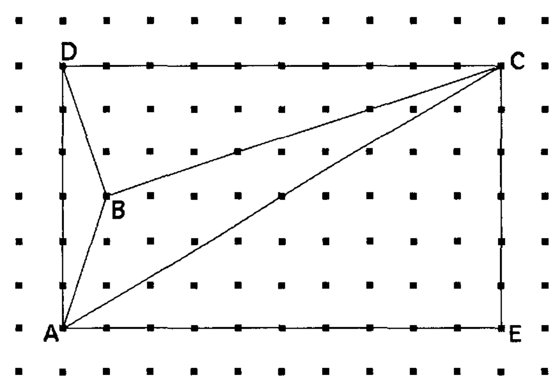
17. Let $P(n)$ be the statement that if a simple polygon with n sides is triangulated, then at least two of the triangles in the triangulation have two sides that border the exterior of the polygon. We will prove $\forall n \geq 4\, P(n)$. The statement is clearly true for $n = 4$, because there is only one diagonal, leaving two triangles with the desired property. Fix $k \geq 4$ and assume that $P(j)$ is true for all j with $4 \leq j \leq k$. Consider a polygon with $k+1$ sides, and some triangulation of it. Pick one of the diagonals in this triangulation. First suppose that this diagonal divides the polygon into one triangle and one polygon with k sides. Then the triangle has two sides that border the exterior. Furthermore, the k-gon has, by the inductive hypothesis, two triangles that have two sides that border the exterior of that k-gon, and only one of these triangles can fail to be a triangle that has two sides that border the exterior of the original polygon. The only other case is that this diagonal divides the polygon into two polygons with j sides and $k+3-j$ sides for some j with $4 \leq j \leq k-1$. By the inductive hypothesis, each of these two polygons has two triangles that have two sides that border their exterior, and in each case only one of these triangles can fail to be a triangle that has two sides that border the exterior of the original polygon.

19. Let $P(n)$ be the statement that the area of a simple polygon with n sides and vertices all at lattice points is given by $I + B/2 - 1$, where I and B are as defined in the exercise. We will prove $\forall n \geq 3\, P(n)$. We begin by proving an additivity lemma. If P is a simple polygon with all vertices at the lattice points, divided into polygons P_1 and P_2 by a diagonal, then $I(P)+B(P)/2-1 = (I(P_1)+B(P_1)/2-1)+(I(P_2)+B(P_2)/2-1)$. To see this, suppose there are k lattice points on the diagonal, not counting its endpoints. Then $I(P) = I(P_1) + I(P_2) + k$ and $B(P) = B(P_1) + B(P_2) - 2k - 2$; and the result follows by simple algebra. What this says in particular is that if Pick's formula gives the correct area for P_1 and P_2, then it must give the correct formula for P, whose area is the sum of the areas for P_1 and P_2; and similarly if Pick's formula gives the correct area for P and one of the P_i's, then it must give the correct formula for the other P_i.

Next we prove the theorem for rectangles whose sides are parallel to the coordinate axes. Such a rectangle necessarily has vertices at (a,b), (a,c), (d,b), and (d,c), where a, b, c, and d are integers with $b < c$ and $a < d$. Its area is clearly $(c-b)(d-a)$. By looking at the perimeter, we see that it has $B = 2(c-b+d-a)$, and we see also that it has $I = (c-b-1)(d-a-1) = (c-b)(d-a) - (c-b) - (d-a) + 1$. Therefore $I + B/2 - 1 = (c-b)(d-a) - (c-b) - (d-a) + 1 + (c-b+d-a) - 1 = (c-b)(d-a)$, which is the desired area.

Next consider a right triangle whose legs are parallel to the coordinate axes. This triangle is half a rectangle of the type just considered, for which Pick's formula holds, so by the additivity lemma, it holds for the triangle as well. (The values of B and I are the same for each of the two triangles, so if Pick's formula gave an answer that was either too small or too large, then it would give a correspondingly wrong answer for the rectangle.)

For the next step, consider an arbitrary triangle with vertices at the lattice points that is not of the type already considered. Embed it in as small a rectangle as possible. There are several possible ways this can happen, but in any case (and adding one more edge in one case), the rectangle will have been partitioned into the given triangle and two or three right triangles with sides parallel to the coordinate axes. See the figure for a typical case. Again by the additivity lemma, we are guaranteed that Pick's formula gives the correct area for the central triangle.



Note that we have now proved $P(3)$, the basis step in our strong induction proof. For the inductive step, given an arbitrary polygon, use Lemma 1 in the text to split it into two polygons. Then by the additivity lemma above and the inductive hypothesis, we know that Pick's formula gives the correct area for this polygon.

Here are some good websites for more details:

`planetmath.org/encyclopedia/ProofOfPicksTheorem.html`
`mathforum.org/library/drmath/view/65670.html`

21. **a)** Use the left figure. Angle abp is smallest for p, but the segment bp is not an interior diagonal.
b) Use the right figure. The vertex other than b with smallest x-coordinate is d, but the segment bd is not an interior diagonal.

c) Use the right figure. The vertex closest to b is d, but the segment bd is not an interior diagonal.

23. **a)** When we try to prove the inductive step and find a triangle in each subpolygon with at least two sides bordering the exterior, it may happen in each case that the triangle we are guaranteed in fact borders the diagonal (which is part of the boundary of that polygon). This leaves us with no triangles guaranteed to touch the boundary of the *original* polygon.

b) We proved $\forall n \geq 4\, T(n)$ in Exercise 17. Since we can always find two triangles that satisfy the property, perforce, at least one triangle does. Thus we have proved $\forall n \geq 4\, E(n)$.

25. **a)** The inductive step here allows us to conclude that $P(3)$, $P(5)$, ... are all true, but we can conclude nothing about $P(2)$, $P(4)$, ...

b) We can conclude that $P(n)$ is true for all positive integers n, using strong induction.

c) The inductive step here allows us to conclude that $P(2)$, $P(4)$, $P(8)$, $P(16)$, ... are all true, but we can conclude nothing about $P(n)$ when n is not a power of 2.

d) This is mathematical induction; we can conclude that $P(n)$ is true for all positive integers n.

27. Suppose, for a proof by contradiction, that there is some positive integer n such that $P(n)$ is not true. Let m be the smallest positive integer greater than n for which $P(m)$ *is* true; we know that such an m exists because $P(m)$ is true for infinitely many values of m, and therefore true for more than just $1, 2, \ldots, n-1$. But we are given that $P(m) \to P(m-1)$, so $P(m-1)$ is true. Thus $m-1$ cannot be greater than n, so $m-1=n$ and $P(n)$ is in fact true. This contradiction shows that $P(n)$ is true for all n.

29. The error is in going from the basis step $n=0$ to the next value, $n=1$. We cannot write 1 as the sum of two smaller natural numbers, so we cannot invoke the inductive hypothesis. In the notation of the "proof," when $k=0$, we cannot write $0+1=i+j$ where $0 \leq i \leq 0$ and $0 \leq j \leq 0$.

31. To show that strong induction is valid, let us suppose that we have a proposition $\forall n P(n)$ which has been proved using it. We must show that in fact $\forall n P(n)$ is true (to say that a principle of proof is valid means that it proves only true propositions). Let S be the set of counterexamples, i.e., $S = \{\, n \mid \neg P(n) \,\}$. We want to show that $S = \emptyset$. We argue by contradiction. Assume that $S \neq \emptyset$. Then by the well-ordering property, S has a smallest element. Since part of the method of strong induction is to show that $P(1)$ is true, this smallest counterexample must be greater than 1. Let us call it $k+1$. Since $k+1$ is the smallest element of S, it must be the case that $P(1) \wedge P(2) \wedge \cdots \wedge P(k)$ is true. But the rest of the proof using strong induction involved showing that $P(1) \wedge P(2) \wedge \cdots \wedge P(k)$ implied $P(k+1)$; therefore since the hypothesis is true, the conclusion must be true as well, i.e., $P(k+1)$ is true. This contradicts our assumption that $k+1 \in S$. Therefore we conclude that $S = \emptyset$, so $\forall n P(n)$ is true.

33. In each case we will argue on the basis of a "smallest counterexample."

a) Suppose that there is a counterexample, that is, that there are values of n and k such that $P(n,k)$ is not true. Choose a counterexample with $n+k$ as small as possible. We cannot have $n=1$ and $k=1$, because we are given that $P(1,1)$ is true. Therefore either $n>1$ or $k>1$. In the former case, by our choice of counterexample, we know that $P(n-1,k)$ is true. But the inductive step then forces $P(n,k)$ to be true, a contradiction. The latter case is similar. So our supposition that there is a counterexample must be wrong, and $P(n,k)$ is true in all cases.

b) Suppose that there is a counterexample, that is, that there are values of n and k such that $P(n,k)$ is not true. Choose a counterexample with n as small as possible. We cannot have $n=1$, because we are given that $P(1,k)$ is true for all k. Therefore $n>1$. By our choice of counterexample, we know that $P(n-1,k)$

is true. But the inductive step then forces $P(n, k)$ to be true, a contradiction. So our supposition that there is a counterexample must be wrong, and $P(n, k)$ is true in all cases.

c) Suppose that there is a counterexample, that is, that there are values of n and k such that $P(n, k)$ is not true. Choose a counterexample with k as small as possible. We cannot have $k = 1$, because we are given that $P(n, 1)$ is true for all n. Therefore $k > 1$. By our choice of counterexample, we know that $P(n, k-1)$ is true. But the inductive step then forces $P(n, k)$ to be true, a contradiction. So our supposition that there is a counterexample must be wrong, and $P(n, k)$ is true in all cases.

35. We want to calculate the product $a_1 a_2 \cdots a_n$ by inserting parentheses to express the calculation as a sequence of multiplications of two quantities. For example, we can insert parentheses into $a_1 a_2 a_3 a_4 a_5$ to render it $(a_1(a_2a_3))(a_4a_5)$, and then the four multiplications are $a_2 \cdot a_3$, $a_4 \cdot a_5$, $a_1 \cdot (a_2a_3)$, and finally the product of these last two quantities. We must show that no matter how the parentheses are inserted, $n-1$ multiplications will be required. If $n = 1$, then clearly 0 multiplications are required, so the basis step is trivial. Now assume the strong inductive hypothesis, that for all $k < n$, no matter how parentheses are inserted into the product of k numbers, $k-1$ multiplications are required to compute the answer. Consider a parenthesized product of a_1 through a_n, and look at the last multiplication. Thus we have $(a_1 a_2 \cdots a_r) \cdot (a_{r+1} \cdots a_n)$, where we do not care how the parentheses are distributed within the pairs shown here. By the inductive hypothesis, it requires $r-1$ multiplications to obtain the first product in parentheses and $n-r-1$ to obtain the second (that second product has $n-r$ factors). Furthermore, 1 additional multiplication is needed to multiply these two answers together. This gives a total of $(r-1) + (n-r-1) + 1 = n-1$ multiplications for the given problem, exactly what we needed to show.

37. Suppose that we have two such pairs, say (q, r) and (q', r'), so that $a = dq + r = dq' + r'$, with $0 \le r, r' < d$. We will show that the pairs are really the same, that is, that $q = q'$ and $r = r'$. From $dq + r = dq' + r'$ we obtain $d(q - q') = r' - r$. Therefore $d \mid (r' - r)$. But $|r' - r| < d$ (since both r' and r are nonnegative integers less than d). The only multiple of d in that range is 0, so we are forced to conclude that $r' = r$. Then it easily follows that $q = q'$ as well, since $q = (a - r)/d = (a - r')/d = q'$.

39. This problem deals with a paradox caused by self-reference. First of all, the answer to the question is clearly "no," because there are a finite number of English words, and so only a finite number of strings of fifteen words or fewer; therefore only a finite number of positive integers can be so described, not all of them. On the other hand, we might offer the following "proof" that every positive integer *can* be so expressed. Clearly 1 can be so expressed (e.g., "one" or "the cardinality of the power set of the empty set"). By the well-ordering property, if there is a positive integer that cannot be expressed in fifteen words or fewer, then there is a smallest such, say s. Then the phrase "the smallest positive integer that cannot be described using no more than fifteen English words" is a description of s using no more than fifteen English words, a contradiction. Therefore no such s exists, and we seem to have proved that every positive integer can be so expressed, in obvious violation to common sense (and the argument presented above). Paradoxes like this are likely to arise whenever we try to use language to talk about itself; the use of language in this way, while seeming to be meaningful, is in fact nonsense.

41. We will prove this by contradiction. Suppose that the well-ordering property were false. Let S be a counterexample: a nonempty set of nonnegative integers that contains no smallest element. Let $P(n)$ be the statement "$i \notin S$ for all $i \le n$." We will show that $P(n)$ is true for all n (which will contradict the assertion that S is nonempty). Now $P(0)$ must be true, because if $0 \in S$ then clearly S would have a smallest element, namely 0. Suppose now that $P(n)$ is true, so that $i \notin S$ for $i = 0, 1, \ldots, n$. We must show that $P(n+1)$ is true, which amounts to showing that $n+1 \notin S$. If $n+1 \in S$, then $n+1$ would be the smallest element of S, and this would contradict our assumption. Therefore $n+1 \notin S$. Thus we have shown by the principle of mathematical induction that $P(n)$ is true for all n, which means that there can be no elements of S. This contradicts our assumption that $S \neq \emptyset$, and our proof by contradiction is complete.

43. First we claim that strong induction implies the principle of mathematical induction. Suppose we have proved $P(1)$ and proved for all $k \geq 1$ that $P(k) \to P(k+1)$ is true. This certainly implies that $[P(1) \wedge \cdots \wedge P(k)] \to P(k+1)$ is true (here we have a stronger hypothesis). Therefore by strong induction $P(n)$ is true for all n. By Exercise 41, the principle of mathematical induction implies the well-ordering property. Therefore by assuming strong induction as an axiom, we can prove the well-ordering property.

SECTION 5.3 Recursive Definitions and Structural Induction

The best way to approach a recursive definition is first to compute several instances. For example, if you are given a recursive definition of a function f, then compute $f(0)$ through $f(8)$ to get a feeling for what is happening. Most of the time it is necessary to prove statements about recursively defined objects using structural induction (or mathematical induction or strong induction), and the induction practically takes care of itself, mimicking the recursive definition.

1. In each case, we compute $f(1)$ by using the recursive part of the definition with $n = 0$, together with the given fact that $f(0) = 1$. Then we compute $f(2)$ by using the recursive part of the definition with $n = 1$, together with the given value of $f(1)$. We continue in this way to obtain $f(3)$ and $f(4)$.

a) $f(1) = f(0) + 2 = 1 + 2 = 3$; $f(2) = f(1) + 2 = 3 + 2 = 5$; $f(3) = f(2) + 2 = 5 + 2 = 7$; $f(4) = f(3) + 2 = 7 + 2 = 9$

b) $f(1) = 3f(0) = 3 \cdot 1 = 3$; $f(2) = 3f(1) = 3 \cdot 3 = 9$; $f(3) = 3f(2) = 3 \cdot 9 = 27$; $f(4) = 3f(3) = 3 \cdot 27 = 81$

c) $f(1) = 2^{f(0)} = 2^1 = 2$; $f(2) = 2^{f(1)} = 2^2 = 4$; $f(3) = 2^{f(2)} = 2^4 = 16$; $f(4) = 2^{f(3)} = 2^{16} = 65{,}536$

d) $f(1) = f(0)^2 + f(0) + 1 = 1^2 + 1 + 1 = 3$; $f(2) = f(1)^2 + f(1) + 1 = 3^2 + 3 + 1 = 13$; $f(3) = f(2)^2 + f(2) + 1 = 13^2 + 13 + 1 = 183$; $f(4) = f(3)^2 + f(3) + 1 = 183^2 + 183 + 1 = 33{,}673$

3. In each case we compute the subsequent terms by plugging into the recursive formula, using the previously given or computed values.

a) $f(2) = f(1) + 3f(0) = 2 + 3(-1) = -1$; $f(3) = f(2) + 3f(1) = -1 + 3 \cdot 2 = 5$; $f(4) = f(3) + 3f(2) = 5 + 3(-1) = 2$; $f(5) = f(4) + 3f(3) = 2 + 3 \cdot 5 = 17$

b) $f(2) = f(1)^2 f(0) = 2^2 \cdot (-1) = -4$; $f(3) = f(2)^2 f(1) = (-4)^2 \cdot 2 = 32$; $f(4) = f(3)^2 f(2) = 32^2 \cdot (-4) = -4096$; $f(5) = f(4)^2 f(3) = (-4096)^2 \cdot 32 = 536{,}870{,}912$

c) $f(2) = 3f(1)^2 - 4f(0)^2 = 3 \cdot 2^2 - 4 \cdot (-1)^2 = 8$; $f(3) = 3f(2)^2 - 4f(1)^2 = 3 \cdot 8^2 - 4 \cdot 2^2 = 176$; $f(4) = 3f(3)^2 - 4f(2)^2 = 3 \cdot 176^2 - 4 \cdot 8^2 = 92{,}672$; $f(5) = 3f(4)^2 - 4f(3)^2 = 3 \cdot 92672^2 - 4 \cdot 176^2 = 25{,}764{,}174{,}848$

d) $f(2) = f(0)/f(1) = (-1)/2 = -1/2$; $f(3) = f(1)/f(2) = 2/(-\frac{1}{2}) = -4$; $f(4) = f(2)/f(3) = (-\frac{1}{2})/(-4) = 1/8$; $f(5) = f(3)/f(4) = (-4)/\frac{1}{8} = -32$

5. a) This is not valid, since letting $n = 1$ we would have $f(1) = 2f(-1)$, but $f(-1)$ is not defined.

b) This is valid. The basis step tells us what $f(0)$ is, and the recursive step tells us how each subsequent value is determined from the one before. It is not hard to look at the pattern and conjecture that $f(n) = 1 - n$. We prove this by induction. The basis step is $f(0) = 1 = 1 - 0$; and if $f(k) = 1 - k$, then $f(k+1) = f(k) - 1 = 1 - k - 1 = 1 - (k+1)$.

c) The basis conditions specify $f(0)$ and $f(1)$, and the recursive step gives $f(n)$ in terms of $f(n-1)$ for $n \geq 2$, so this is a valid definition. If we compute the first several values, we conjecture that $f(n) = 4 - n$ if $n > 0$, but $f(0) = 2$. That is our "formula." To prove it correct by induction we need two basis steps: $f(0) = 2$, and $f(1) = 3 = 4 - 1$. For the inductive step (with $k \geq 1$), $f(k+1) = f(k) - 1 = (4 - k) - 1 = 4 - (k+1)$.

d) The basis conditions specify $f(0)$ and $f(1)$, and the recursive step gives $f(n)$ in terms of $f(n-2)$ for $n \geq 2$, so this is a valid definition. The sequence of function values is $1, 2, 2, 4, 4, 8, 8, \ldots$, and we can fit a formula to this if we use the floor function: $f(n) = 2^{\lfloor (n+1)/2 \rfloor}$. For a proof, we check the base cases: $f(0) = 1 = 2^{\lfloor (0+1)/2 \rfloor}$ and $f(1) = 2 = 2^{\lfloor (1+1)/2 \rfloor}$. For the inductive step: $f(k+1) = 2f(k-1) = 2 \cdot 2^{\lfloor k/2 \rfloor} = 2^{\lfloor k/2 \rfloor + 1} = 2^{\lfloor ((k+1)+1)/2 \rfloor}$.

e) The definition tells us explicitly what $f(0)$ is. The recursive step specifies $f(1)$, $f(3)$, ... in terms of $f(0)$, $f(2)$, ...; and it also gives $f(2)$, $f(4)$, ... in terms of $f(0)$, $f(2)$, ... So the definition is valid. We compute that $f(1) = 3$, $f(2) = 9$, $f(3) = 27$, and so conjecture that $f(n) = 3^n$. The basis step of the inductive proof is clear. For odd n greater than 0 we have $f(n) = 3f(n-1) = 3 \cdot 3^{n-1} = 3^n$, and for even n greater than 1 we have $f(n) = 9f(n-2) = 9 \cdot 3^{n-2} = 3^n$. Note that we used a slightly different notation here, letting n be the new value, rather than $k+1$, but the logic is the same.

7. There are many correct answers for these sequences. We will give what we consider to be the simplest ones.

a) Clearly each term in this sequence is 6 greater than the preceding term. Thus we can define the sequence by setting $a_1 = 6$ and declaring that $a_{n+1} = a_n + 6$ for all $n \geq 1$.

b) This is just like part **(a)**, in that each term is 2 more than its predecessor. Thus we have $a_1 = 3$ and $a_{n+1} = a_n + 2$ for all $n \geq 1$.

c) Each term is 10 times its predecessor. Thus we have $a_1 = 10$ and $a_{n+1} = 10a_n$ for all $n \geq 1$.

d) Just set $a_1 = 5$ and declare that $a_{n+1} = a_n$ for all $n \geq 1$.

9. We need to write $F(n+1)$ in terms of $F(n)$. Since $F(n)$ is the sum of the first n positive integers (namely 1 through n), and $F(n+1)$ is the sum of the first $n+1$ positive integers (namely 1 through $n+1$), we can obtain $F(n+1)$ from $F(n)$ by adding $n+1$. Therefore the recursive part of the definition is $F(n+1) = F(n)+n+1$. The initial condition is a specification of the value of $F(0)$; the sum of no positive integers is clearly 0, so we set $F(0) = 0$. (Alternately, if we assume that the argument for F is intended to be strictly positive, then we set $F(1) = 1$, since the sum of the first one positive integer is 1.)

11. We need to see how $P_m(n+1)$ relates to $P_m(n)$. Now $P_m(n+1) = m(n+1) = mn + m = P_m(n) + m$. Thus the recursive part of our definition is just $P_m(n+1) = P_m(n) + m$. The basis step is $P_m(0) = 0$, since $m \cdot 0 = 0$, no matter what value m has.

13. We prove this using the principle of mathematical induction. The base case is $n = 1$, and in that case the statement to be proved is just $f_1 = f_2$; this is true since both values are 1. Next we assume the inductive hypothesis, that

$$f_1 + f_3 + \cdots + f_{2n-1} = f_{2n},$$

and try to prove the corresponding statement for $n+1$, namely,

$$f_1 + f_3 + \cdots + f_{2n-1} + f_{2n+1} = f_{2n+2}.$$

We have

$$\begin{aligned} f_1 + f_3 + \cdots + f_{2n-1} + f_{2n+1} &= f_{2n} + f_{2n+1} \quad \text{(by the inductive hypothesis)} \\ &= f_{2n+2} \quad \text{(by the definition of the Fibonacci numbers).} \end{aligned}$$

15. We prove this using the principle of mathematical induction. The basis step is for $n = 1$, and in that case the statement to be proved is just $f_0 f_1 + f_1 f_2 = f_2^2$; this is true since $0 \cdot 1 + 1 \cdot 1 = 1^2$. Next we assume the inductive hypothesis, that

$$f_0 f_1 + f_1 f_2 + \cdots + f_{2n-1} f_{2n} = f_{2n}^2,$$

and try to prove the corresponding statement for $n+1$, namely,

$$f_0f_1 + f_1f_2 + \cdots + f_{2n-1}f_{2n} + f_{2n}f_{2n+1} + f_{2n+1}f_{2n+2} = f_{2n+2}^2 .$$

Note that *two* extra terms were added, since the final subscript has to be even. We have

$$\begin{aligned} f_0f_1 + f_1f_2 + \cdots + f_{2n-1}f_{2n} + f_{2n}f_{2n+1} + f_{2n+1}f_{2n+2} &= f_{2n}^2 + f_{2n}f_{2n+1} + f_{2n+1}f_{2n+2} \\ &\qquad \text{(by the inductive hypothesis)} \\ &= f_{2n}(f_{2n} + f_{2n+1}) + f_{2n+1}f_{2n+2} \\ &\qquad \text{(by factoring)} \\ &= f_{2n}f_{2n+2} + f_{2n+1}f_{2n+2} \\ &\qquad \text{(by the definition of the Fibonacci numbers)} \\ &= (f_{2n} + f_{2n+1})f_{2n+2} \\ &= f_{2n+2}f_{2n+2} = f_{2n+2}^2. \end{aligned}$$

17. Let d_n be the number of divisions used by Algorithm 1 in Section 4.3 (the Euclidean algorithm) to find $\gcd(f_{n+1}, f_n)$. We write the calculation in this order, since $f_{n+1} \geq f_n$. We begin by finding the values of d_n for the first few values of n, in order to find a pattern and make a conjecture as to what the answer is. For $n = 0$ we are computing $\gcd(f_1, f_0) = \gcd(1, 0)$. Without performing any divisions, we know immediately that the answer is 1, so $d_0 = 0$. For $n = 1$ we are computing $\gcd(f_2, f_1) = \gcd(1, 1)$. One division is used to show that $\gcd(1, 1) = \gcd(1, 0)$, so $d_1 = 1$. For $n = 2$ we are computing $\gcd(f_3, f_2) = \gcd(2, 1)$. One division is used to show that $\gcd(2, 1) = \gcd(1, 0)$, so $d_2 = 1$. For $n = 3$, the computation gives successively $\gcd(f_4, f_3) = \gcd(3, 2) = \gcd(2, 1) = \gcd(1, 0)$, for a total of 2 divisions; thus $d_3 = 2$. For $n = 4$, we have $\gcd(f_5, f_4) = \gcd(5, 3) = \gcd(3, 2) = \gcd(2, 1) = \gcd(1, 0)$, for a total of 3 divisions; thus $d_4 = 3$. At this point we see that each increase of 1 in n seems to add one more division, in order to reduce $\gcd(f_{n+1}, f_n)$ to $\gcd(f_n, f_{n-1})$. Perhaps, then, for $n \geq 2$, we have $d_n = n - 1$. Let us make that conjecture. We have already verified the basis step when we computed that $d_2 = 1$. Now assume the inductive hypothesis, that $d_n = n - 1$. We must show that $d_{n+1} = n$. Now d_{n+1} is the number of divisions used in computing $\gcd(f_{n+2}, f_{n+1})$. The first step in the algorithm is to divide f_{n+1} into f_{n+2}. Since $f_{n+2} = f_{n+1} + f_n$ (this is the key point) and $f_n < f_{n+1}$, we get a quotient of 1 and a remainder of f_n. Thus we have, after one division, $\gcd(f_{n+2}, f_{n+1}) = \gcd(f_{n+1}, f_n)$. Now by the inductive hypothesis we need exactly $d_n = n - 1$ more divisions, since the algorithm proceeds from this point exactly as it proceeded given the inputs for the case of n. Therefore $1 + (n - 1) = n$ divisions are used in all, and our proof is complete. The answer, then, is that $d_0 = 0$, $d_1 = 1$, and $d_n = n - 1$ for $n \geq 2$. (If we interpreted the problem as insisting that we compute $\gcd(f_n, f_{n+1})$, with that order of the arguments, then the analysis and the answer are slightly different: $d_0 = 1$, and $d_n = n$ for $n \geq 1$.)

19. The determinant of the matrix $\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, written $|\mathbf{A}|$, is by definition $ad - bc$; and the determinant has the multiplicative property that $|\mathbf{AB}| = |\mathbf{A}||\mathbf{B}|$. Therefore the determinant of the matrix $\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ in Exercise 16 is $1 \cdot 0 - 1 \cdot 1 = -1$, and $|\mathbf{A}^n| = |\mathbf{A}|^n = (-1)^n$. On the other hand, the determinant of the matrix $\begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}$ is by definition $f_{n+1}f_{n-1} - f_n^2$. In Exercise 18 we showed that $\mathbf{A}^n$ is this latter matrix. The identity in Exercise 14 follows.

21. Assume that the definitions given in Exercise 20 were as follows: the max or min of one number is itself; $\max(a_1, a_2) = a_1$ if $a_1 \geq a_2$ and a_2 if $a_1 < a_2$, whereas $\min(a_1, a_2) = a_2$ if $a_1 \geq a_2$ and a_1 if $a_1 < a_2$; and for $n \geq 2$,

$$\max(a_1, a_2, \ldots, a_{n+1}) = \max(\max(a_1, a_2, \ldots, a_n), a_{n+1})$$

and

$$\min(a_1, a_2, \ldots, a_{n+1}) = \min(\min(a_1, a_2, \ldots, a_n), a_{n+1}).$$

We can then prove the three statements here by induction on n.

a) For $n = 1$, both sides of the equation equal $-a_1$. For $n = 2$, we must show that $\max(-a_1, -a_2) = -\min(a_1, a_2)$. There are two cases, depending on the relationship between a_1 and a_2. If $a_1 \le a_2$, then $-a_1 \ge -a_2$, so by our definition, $\max(-a_1, -a_2) = -a_1$. On the other hand our definition implies that $\min(a_1, a_2) = a_1$ in this case. Therefore $\max(-a_1, -a_2) = -a_1 = -\min(a_1, a_2)$. The other case, $a_1 > a_2$, is similar: $\max(-a_1, -a_2) = -a_2 = -\min(a_1, a_2)$. Now we are ready for the inductive step. Assume the inductive hypothesis, that

$$\max(-a_1, -a_2, \ldots, -a_n) = -\min(a_1, a_2, \ldots, a_n).$$

We need to show the corresponding equality for $n+1$. We have

$$\begin{aligned}
&\max(-a_1, -a_2, \ldots, -a_n, -a_{n+1}) \\
&\qquad = \max(\max(-a_1, -a_2, \ldots, -a_n), -a_{n+1}) \quad \text{(by definition)} \\
&\qquad = \max(-\min(a_1, a_2, \ldots, a_n), -a_{n+1}) \quad \text{(by the inductive hypothesis)} \\
&\qquad = -\min(\min(a_1, a_2, \ldots, a_n), a_{n+1}) \quad \text{(by the already proved case } n = 2) \\
&\qquad = -\min(a_1, a_2, \ldots, a_n, a_{n+1}) \quad \text{(by definition)}.
\end{aligned}$$

b) For $n = 1$, the equation is simply the identity $a_1 + b_1 = a_1 + b_1$. For $n = 2$, the situation is a little messy. Let us consider first the case that $a_1 + b_1 \ge a_2 + b_2$. Then $\max(a_1 + b_1, a_2 + b_2) = a_1 + b_1$. Also note that $a_1 \le \max(a_1, b_1)$, and $b_1 \le \max(b_1, b_2)$, so that $a_1 + b_1 \le \max(a_1, a_2) + \max(b_1, b_2)$. Therefore we have $\max(a_1 + b_1, a_2 + b_2) = a_1 + b_1 \le \max(a_1, a_2) + \max(b_1, b_2)$. The other case, in which $a_1 + b_1 < a_2 + b_2$, is similar. Now for the inductive step, we first need a lemma: if $u \le v$, then $\max(u, w) \le \max(v, w)$; this is easy to prove by looking at the three cases determined by the size of w relative to the sizes of u and v. Now assuming the inductive hypothesis, we have

$$\begin{aligned}
&\max(a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n, a_{n+1} + b_{n+1}) \\
&\qquad = \max(\max(a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n), a_{n+1} + b_{n+1}) \quad \text{(by definition)} \\
&\qquad \le \max(\max(a_1, a_2, \ldots, a_n) + \max(b_1, b_2, \ldots, b_n), a_{n+1} + b_{n+1}) \\
&\qquad\qquad \text{(by the inductive hypothesis and the lemma)} \\
&\qquad \le \max(\max(a_1, a_2, \ldots, a_n), a_{n+1}) + \max(\max(b_1, b_2, \ldots, b_n), b_{n+1}) \\
&\qquad\qquad \text{(by the already proved case } n = 2) \\
&\qquad = \max(a_1, a_2, \ldots, a_n, a_{n+1}) + \max(b_1, b_2, \ldots, b_n, b_{n+1}) \quad \text{(by definition)}.
\end{aligned}$$

c) The proof here is exactly dual to the proof in part **(b)**. We replace every occurrence of "max" by "min," and invert each inequality. The proof then reads as follows. For $n = 1$, the equation is simply the identity $a_1 + b_1 = a_1 + b_1$. For $n = 2$, the situation is a little messy. Let us consider first the case that $a_1 + b_1 \le a_2 + b_2$. Then $\min(a_1 + b_1, a_2 + b_2) = a_1 + b_1$. Also note that $a_1 \ge \min(a_1, a_2)$, and $b_1 \ge \min(b_1, b_2)$, so that $a_1 + b_1 \ge \min(a_1, a_2) + \min(b_1, b_2)$. Therefore we have $\min(a_1 + b_1, a_2 + b_2) = a_1 + b_1 \ge \min(a_1, a_2) + \min(b_1, b_2)$. The other case, in which $a_1 + b_1 > a_2 + b_2$, is similar. Now for the inductive step, we first need a lemma: if $u \ge v$, then $\min(u, w) \ge \min(v, w)$; this is easy to prove by looking at the three cases determined by the size of w relative to the sizes of u and v. Now assuming the inductive hypothesis, we have

$$\begin{aligned}
&\min(a_1+b_1, a_2+b_2, \ldots, a_n+b_n, a_{n+1}+b_{n+1}) \\
&\qquad = \min(\min(a_1+b_1, a_2+b_2, \ldots, a_n+b_n), a_{n+1}+b_{n+1}) \quad \text{(by definition)} \\
&\qquad \geq \min(\min(a_1, a_2, \ldots, a_n) + \min(b_1, b_2, \ldots, b_n), a_{n+1}+b_{n+1}) \\
&\qquad\qquad \text{(by the inductive hypothesis and the lemma)} \\
&\qquad \geq \min(\min(a_1, a_2, \ldots, a_n), a_{n+1}) + \min(\min(b_1, b_2, \ldots, b_n), b_{n+1}) \\
&\qquad\qquad \text{(by the already proved case } n=2\text{)} \\
&\qquad = \min(a_1, a_2, \ldots, a_n, a_{n+1}) + \min(b_1, b_2, \ldots, b_n, b_{n+1}) \quad \text{(by definition)}.
\end{aligned}$$

23. We can define the set $S = \{\, x \mid x \text{ is a positive integer and } x \text{ is a multiple of } 5 \,\}$ by the basis step requirement that $5 \in S$ and the recursive requirement that if $n \in S$, then $n+5 \in S$. Alternately we can mimic Example 5, making the recursive part of the definition that $x+y \in S$ whenever x and y are in S.

25. **a)** Since we can generate all the even integers by starting with 0 and repeatedly adding or subtracting 2, a simple recursive way to define this set is as follows: $0 \in S$; and if $x \in S$ then $x+2 \in S$ and $x-2 \in S$.
b) The smallest positive integer congruent to 2 modulo 3 is 2, so we declare $2 \in S$. All the others can be obtained by adding multiples of 3, so our inductive step is that if $x \in S$, then $x+3 \in S$.
c) The positive integers not divisible by 5 are the ones congruent to 1, 2, 3, or 4 modulo 5. Therefore we can proceed just as in part **(b)**, setting $1 \in S$, $2 \in S$, $3 \in S$, and $4 \in S$ as the base cases, and then declaring that if $x \in S$, then $x+5 \in S$.

27. **a)** If we apply each of the recursive step rules to the only element given in the basis step, we see that $(0,1)$, $(1,1)$, and $(2,1)$ are all in S. If we apply the recursive step to these we add $(0,2)$, $(1,2)$, $(2,2)$, $(3,2)$, and $(4,2)$. The next round gives us $(0,3)$, $(1,3)$, $(2,3)$, $(3,3)$, $(4,3)$, $(5,3)$, and $(6,3)$. And a fourth set of applications adds $(0,4)$, $(1,4)$, $(2,4)$, $(3,4)$, $(4,4)$, $(5,4)$, $(6,4)$, $(7,4)$, and $(8,4)$.
b) Let $P(n)$ be the statement that $a \leq 2b$ whenever $(a,b) \in S$ is obtained by n applications of the recursive step. For the basis step, $P(0)$ is true, since the only element of S obtained with no applications of the recursive step is $(0,0)$, and indeed $0 \leq 2 \cdot 0$. Assume the strong inductive hypothesis that $a \leq 2b$ whenever $(a,b) \in S$ is obtained by k or fewer applications of the recursive step, and consider an element obtained with $k+1$ applications of the recursive step. Since the final application of the recursive step to an element (a,b) must be applied to an element obtained with fewer applications of the recursive step, we know that $a \leq 2b$. So we just need to check that this inequality implies $a \leq 2(b+1)$, $a+1 \leq 2(b+1)$, and $a+2 \leq 2(b+1)$. But this is clear, since we just add $0 \leq 2$, $1 \leq 2$, and $2 \leq 2$, respectively, to $a \leq 2b$ to obtain these inequalities.
c) This holds for the basis step, since $0 \leq 0$. If this holds for (a,b), then it also holds for the elements obtained from (a,b) in the recursive step, since adding $0 \leq 2$, $1 \leq 2$, and $2 \leq 2$, respectively, to $a \leq 2b$ yields $a \leq 2(b+1)$, $a+1 \leq 2(b+1)$, and $a+2 \leq 2(b+1)$.

29. **a)** Since we are working with positive integers, the smallest pair in which the sum of the coordinates is even is $(1,1)$. So our basis step is $(1,1) \in S$. If we start with a point for which the sum of the coordinates is even and want to maintain this parity, then we can add 2 to the first coordinate, or add 2 to the second coordinate, or add 1 to each coordinate. Thus our recursive step is that if $(a,b) \in S$, then $(a+2,b) \in S$, $(a,b+2) \in S$, and $(a+1,b+1) \in S$. To prove that our definition works, we note first that $(1,1)$ has an even sum of coordinates, and if (a,b) has an even sum of coordinates, then so do $(a+2,b)$, $(a,b+2)$, and $(a+1,b+1)$, since we added 2 to the sum of the coordinates in each case. Conversely, we must show that if $a+b$ is even, then $(a,b) \in S$ by our definition. We do this by induction on the sum of the coordinates. If the sum is 2, then $(a,b) = (1,1)$, and the basis step put (a,b) into S. Otherwise the sum is at least 4, and at least one of $(a-2,b)$, $(a,b-2)$, and $(a-1,b-1)$ must have positive integer coordinates whose sum is an even number smaller than $a+b$, and therefore must be in S by our definition. Then one application of the recursive step shows that $(a,b) \in S$ by our definition.

b) Since we are working with positive integers, the smallest pairs in which there is an odd coordinate are $(1,1)$, $(1,2)$, and $(2,1)$. So our basis step is that these three points are in S. If we start with a point for which a coordinate is odd and want to maintain this parity, then we can add 2 to that coordinate. Thus our recursive step is that if $(a,b) \in S$, then $(a+2,b) \in S$ and $(a,b+2) \in S$. To prove that our definition works, we note first that $(1,1)$, $(1,2)$, and $(2,1)$ all have an odd coordinate, and if (a,b) has an odd coordinate, then so do $(a+2,b)$ and $(a,b+2)$, since adding 2 does not change the parity. Conversely (and this is the harder part), we must show that if (a,b) has at least one odd coordinate, then $(a,b) \in S$ by our definition. We do this by induction on the sum of the coordinates. If $(a,b)=(1,1)$ or $(a,b)=(1,2)$ or $(a,b)=(2,1)$, then the basis step put (a,b) into S. Otherwise either a or b is at least 3, so at least one of $(a-2,b)$ and $(a,b-2)$ must have positive integer coordinates whose sum is smaller than $a+b$, and therefore must be in S by our definition, since we haven't changed the parities. Then one application of the recursive step shows that $(a,b) \in S$ by our definition.

c) We use two basis steps here, $(1,6) \in S$ and $(2,3) \in S$. If we want to maintain the parity of $a+b$ and the fact that b is a multiple of 3, then we can add 2 to a (leaving b alone), or we can add 6 to b (leaving a alone). So our recursive step is that if $(a,b) \in S$, then $(a+2,b) \in S$ and $(a,b+6) \in S$. To prove that our definition works, we note first that $(1,6)$ and $(2,3)$ satisfy the condition, and if (a,b) satisfies the condition, then so do $(a+2,b)$ and $(a,b+6)$, since adding 2 or 6 does not change the parity of the sum, and adding 6 maintains divisibility by 3. Conversely (and this is the harder part), we must show that if (a,b) satisfies the condition, then $(a,b) \in S$ by our definition. We do this by induction on the sum of the coordinates. The smallest sums of coordinates satisfying the condition are 5 and 7, and the only points are $(1,6)$, which the basis step put into S, $(2,3)$, which the basis step put into S, and $(4,3)=(2+2,3)$, which is in S by one application of our recursive definition. For a sum greater than 7, either $a \geq 3$, or $a \leq 2$ and $b \geq 9$ (since $2+6$ is not odd). This implies that either $(a-2,b)$ or $(a,b-6)$ must have positive integer coordinates whose sum is smaller than $a+b$ and satisfy the condition for being in S, and hence are in S by our definition. Then one application of the recursive step shows that $(a,b) \in S$ by our definition.

31. The answer depends on whether we require fully parenthesized expressions. Assuming that we do not, then the following definition is the most straightforward. Let F be the required collection of formulae. The basis step is that all specific sets and all variables representing sets are to be in F. The recursive part of the definition is that if α and β are in F, then so are $\overline{\alpha}$, (α), $\alpha \cup \beta$, $\alpha \cap \beta$, and $\alpha - \beta$. If we insist on parentheses, then the recursive part of the definition is that if α and β are in F, then so are $\overline{\alpha}$, $(\alpha \cup \beta)$, $(\alpha \cap \beta)$, and $(\alpha - \beta)$.

33. Let $D=\{0,1,2,3,4,5,6,7,8,9\}$ be the set of decimal digits. We think of a string as either being an element of D or else coming from a shorter string by appending an element of D, as in Definition 1. This problem is somewhat like Example 7.

a) The basis step is for a string of length 1, i.e., an element of D. If $x \in D$, then $m(x)=x$. For the recursive step, if the string $s=tx$, where $t \in D^*$ and $x \in D$, then $m(s)=\min(m(s),x)$. In other words, if the last digit in the string is smaller than the minimum digit in the rest of the string, then the last digit is the smallest digit in the string; otherwise the smallest digit in the rest of the string is the smallest digit in the string.

b) Recall the definition of concatenation (Definition 2). The basis step does not apply, since s and t here must be nonempty. Let $t=wx$, where $w \in D^*$ and $x \in D$. If $w=\lambda$, then $m(st)=m(sx)=\min(m(s),x)=\min(m(s),m(x))$ by the recursive step and the basis step of the definition of m in part **(a)**. Otherwise, $m(st)=m((sw)x)=\min(m(sw),x)$ by the definition of m in part **(a)**. But $m(sw)=\min(m(s),m(w))$ by the inductive hypothesis of our structural induction, so $m(st)=\min(\min(m(s),m(w)),x)=\min(m(s),\min(m(w),x))$

by the meaning of min. But $\min(m(w), x) = m(wx) = m(t)$ by the recursive step of the definition of m in part **(a)**. Thus $m(st) = \min(m(s), m(t))$.

35. The string of length 0, namely the empty string, is its own reversal, so we define $\lambda^R = \lambda$. A string w of length $n+1$ can always be written as vy, where v is a string of length n (the first n symbols of w), and y is a symbol (the last symbol of w). To reverse w, we need to start with y, and then follow it by the first part of w (namely v), reversed. Thus we define $w^R = y(v^R)$. (Note that the parentheses are for our benefit—they are not part of the string.)

37. We set $w^0 = \lambda$ (the concatenation of no copies of w should be defined to be the empty string). For $i \geq 0$, we define $w^{i+1} = ww^i$, where this notation means that we first write down w and then follow it with w^i.

39. The recursive part of this definition tells us that the only way to modify a string in A to obtain another string in A is to tack a 0 onto the front and a 1 onto the end. Starting with the empty string, then, the only strings we get are λ, 01, 0011, 000111, ... In other words, $A = \{\, 0^n 1^n \mid n \geq 0 \,\}$.

41. The basis step is $i = 0$, where we need to show that the length of w^0 is 0 times the length of w. This is true, no matter what w is, since $l(w^0) = l(\lambda) = 0$. Assume the inductive hypothesis that $l(w^i) = i \cdot l(w)$. Then $l(w^{i+1}) = l(ww^i) = l(w) + l(w^i)$, this latter equality having been shown in Example 12. Now by the inductive hypothesis we have $l(w) + l(w^i) = l(w) + i \cdot l(w) = (i+1) \cdot l(w)$, as desired.

43. This is similar to Theorem 2. For the full binary tree consisting of just the root r the result is true since $n(T) = 1$ and $h(T) = 0$, and $1 \geq 2 \cdot 0 + 1$. For the inductive hypothesis we assume that $n(T_1) \geq 2h(T_1) + 1$ and $n(T_2) \geq 2h(T_2) + 1$ where T_1 and T_2 are full binary trees. By the recursive definitions of $n(T)$ and $h(T)$, we have $n(T) = 1 + n(T_1) + n(T_2)$ and $h(T) = 1 + \max(h(T_1), h(T_2))$. Therefore $n(T) = 1 + n(T_1) + n(T_2) \geq 1 + 2h(T_1) + 1 + 2h(T_2) + 1 \geq 1 + 2 \cdot \max(h(T_1), h(T_2)) + 2$ since the sum of two nonnegative numbers is at least as large as the larger of the two. But this equals $1 + 2(\max(h(T_1), h(T_2)) + 1) = 1 + 2h(T)$, and our proof is complete.

45. The basis step requires that we show that this formula holds when $(m, n) = (0, 0)$. The inductive step requires that we show that if the formula holds for all pairs smaller than (m, n) in the lexicographic ordering of $\mathbf{N} \times \mathbf{N}$, then it also holds for (m, n). For the basis step we have $a_{0,0} = 0 = 0 + 0$. For the inductive step, assume that $a_{m',n'} = m' + n'$ whenever (m', n') is less than (m, n) in the lexicographic ordering of $\mathbf{N} \times \mathbf{N}$. By the recursive definition, if $n = 0$ then $a_{m,n} = a_{m-1,n} + 1$; since $(m-1, n)$ is smaller than (m, n), the inductive hypothesis tells us that $a_{m-1,n} = m - 1 + n$, so $a_{m,n} = m - 1 + n + 1 = m + n$, as desired. Now suppose that $n > 0$, so that $a_{m,n} = a_{m,n-1} + 1$. Again we have $a_{m,n-1} = m + n - 1$, so $a_{m,n} = m + n - 1 + 1 = m + n$, and the proof is complete.

47. **a)** It is clear that $P_{m,m} = P_m$, since a number exceeding m can never be used in a partition of m.

b) We need to verify all five lines of this definition, show that the recursive references are to a smaller value of m or n, and check that they take care of all the cases and are mutually compatible. Let us do the last of these first. The first two lines take care of the case in which either m or n is equal to 1. They are consistent with each other in case $m = n = 1$. The last three lines are mutually exclusive and take care of all the possibilities for m and n if neither is equal to 1, since, given any two numbers, either they are equal or one is greater than the other. Note finally that the third line allows $m = 1$; in that case the value is defined to be $P_{1,1}$, which is consistent with line one, since $P_{1,n} = 1$.

Next let us make sure that the logic of the definition is sound, specifically that $P_{m,n}$ is being defined in terms of $P_{i,j}$ for $i \le m$ and $j \le n$, with at least one of the inequalities strict. There is no problem with the first two lines, since these are not recursive. The third line is okay, since $m < n$, and $P_{m,n}$ is being defined in terms of $P_{m,m}$. The fourth line is also okay, since here $P_{m,m}$ is being defined in terms of $P_{m,m-1}$. Finally, the last line is okay, since the subscripts satisfy the desired inequalities.

Finally, we need to check the content of each line. (Note that so far we have hardly even discussed what $P_{m,n}$ means!) The first line says that there is only one way to write the number 1 as the sum of positive integers, none of which exceeds n, and that is patently true, namely as $1 = 1$. The second line says that there is only one way to write the number m as the sum of positive integers, none of which exceeds 1, and that, too, is obvious, namely $m = 1 + 1 + \cdots + 1$. The third line says that the number of ways to write m as the sum of integers not exceeding n is the same as the number of ways to write m as the sum of integers not exceeding m as long as $m < n$. This again is true, since we could never use a number from $\{m+1, m+2, \ldots, n\}$ in such a sum anyway. Now we begin to get to the meat. The fourth line says that the number of ways to write m as the sum of positive integers not exceeding m is 1 plus the number of ways to write m as the sum of positive integers not exceeding $m-1$. Indeed, there is exactly one way to write m as the sum of positive integers not exceeding m that actually uses m, namely $m = m$; all the rest use only numbers less than or equal to $m-1$. This verifies line four. The real heart of the matter is line five. How can we write m as the sum of positive integers not exceeding n? We may use an n, or we may not. There are exactly $P_{m,n-1}$ ways to form the sum without using n, since in that case each summand is less than or equal to $n-1$. If we do use at least one n, then we have $m = n + (m-n)$. The number of ways this can be done, then, is the same as the number of ways to complete the partition by writing $(m-n)$ as the sum of positive integers not exceeding n. Thus there are $P_{m-n,n}$ ways to write m as the sum of numbers not exceeding n, at least one of which equals n. By the sum rule (see Chapter 6), we have $P_{m,n} = P_{m,n-1} + P_{m-n,n}$, as desired.

c) We expand each $P_{m,n}$ according to the definition. For the first problem we have (deleting the commas in the subscripts for readability) $P_5 = P_{55} = 1 + P_{54} = 1 + P_{53} + P_{14} = 1 + P_{52} + P_{23} + 1 = 1 + P_{51} + P_{32} + P_{22} + 1 = 1 + 1 + P_{31} + P_{12} + 1 + P_{21} + 1 = 1+1+1+1+1+1+1 = 7$. For the second problem we have $P_6 = P_{66} = 1 + P_{65} = 1 + P_{64} + P_{15} = 1 + P_{63} + P_{24} + 1 = 1 + P_{62} + P_{33} + P_{22} + 1 = 1 + P_{61} + P_{42} + 1 + P_{32} + 1 + P_{21} + 1 = 1 + 1 + P_{41} + P_{22} + 1 + P_{31} + P_{12} + 1 + 1 + 1 = 1 + 1 + 1 + 1 + P_{21} + 1 + 1 + 1 + 1 + 1 + 1 = 1+1+1+1+1+1+1+1+1+1+1 = 11$.

49. We prove this by induction on m. The basis step is $m = 1$, so we need to compute $A(1,2)$. Line four of the definition tells us that $A(1,2) = A(0, A(1,1))$. Since $A(1,1) = 2$, by line three, we see that $A(1,2) = A(0,2)$. Now line one of the definition applies, and we see that $A(1,2) = A(0,2) = 2 \cdot 2 = 4$, as desired. For the inductive step, assume that $A(m-1,2) = 4$, and consider $A(m,2)$. Applying first line four of the definition, then line three, and then the inductive hypothesis, we have $A(m,2) = A(m-1, A(m,1)) = A(m-1,2) = 4$.

51. a) We use the results of Exercises 49 and 50: $A(2,3) = A(1, A(2,2)) = A(1,4) = 2^4 = 16$.

b) We have $A(3,3) = A(2, A(3,2)) = A(2,4)$ by Exercise 49. Now one can show by induction (using the result of Exercise 50) that $A(2,n)$ is equal to $2^{2^{\cdot^{\cdot^{2}}}}$, with n 2's in the tower. Therefore the answer is $2^{2^{2^2}} = 2^{16} = 65{,}536$.

53. It is often the case in proofs by induction that you need to prove something stronger than the given proposition, in order to have a stronger inductive hypothesis to work with. This is called **inductive loading** (see the preamble to Exercise 74 in Section 5.1). That is the case with our proof here. We will prove the statement "$A(m,k) > A(m,l)$ if $k > l$ for all m, k, and l," and we will use **double induction**, inducting first on m, and then within the inductive step for that induction, inducting on k (using strong induction). Note that this stronger statement implies the statement we are trying to prove—just take $k = l + 1$.

The basis step is $m = 0$, in which the statement at hand reduces (by line one of the definition) to the true conditional statement that if $k > l$, then $2k > 2l$. Next we assume the inductive hypothesis on m, namely that $A(m,x) > A(m,y)$ for *all* values of x and y with $x > y$. We want now to show that if $k > l$, then $A(m+1,k) > A(m+1,l)$. This we will do by induction on k. For the basis step, $k = 0$, there is nothing to prove, since the condition $k > l$ is vacuous. Similarly, if $k = 1$, then $A(m+1,k) = 2$ and $A(m+1,l) = 0$ (since necessarily $l = 0$), so the desired inequality holds. So assume the inductive hypothesis (using strong induction), that $A(m+1,r) > A(m+1,s)$ whenever $k > r > s$, where $k \geq 2$. We need to show that $A(m+1,k) > A(m+1,l)$ if $k > l$. Now $A(m+1,k) = A(m, A(m+1,k-1))$ by line four of the definition. Since $k - 1 \geq l$, we apply the inductive hypothesis on k to yield $A(m+1,k-1) > A(m+1,l-1)$, and therefore by the inductive hypothesis on m, we have $A(m, A(m+1,k-1)) > A(m, A(m+1,l-1))$. But this latter value equals $A(m+1,l)$, as long as $l \geq 2$. Thus we have shown that $A(m+1,k) > A(m+1,l)$ as long as $l \geq 2$. On the other hand, if $l = 0$ or 1, then $A(m+1,l) \leq 2$ (by lines two and three of the definition), whereas $A(m+1,2) = 4$ by Exercise 49. Therefore $A(m+1,k) \geq A(m+1,2) > A(m+1,l)$. This completes the proof.

55. We repeatedly invoke the result of Exercise 54, which says that $A(m+1,j) \geq A(m,j)$. Indeed, we have $A(i,j) \geq A(i-1,j) \geq \cdots \geq A(0,j) = 2j \geq j$.

57. Let $P(n)$ be the statement "F is well-defined at n; i.e., $F(n)$ is a well-defined number." We need to show that $P(n)$ is true for all n. We do this by strong induction. First $P(0)$ is true, since $F(0)$ is well-defined by the specification of $F(0)$. Next assume that $P(k)$ is true for all $k < n$. We want to show that $P(n)$ is also true, in other words that $F(n)$ is well-defined. Since the definition gave $F(n)$ in terms of $F(0)$ through $F(n-1)$, and since we are assuming that these are all well-defined (our inductive hypothesis), we conclude that $F(n)$ is well-defined, as desired.

59. **a)** This would be a proper definition if the recursive part were stated to hold for $n \geq 2$. As it stands, however, $F(1)$ is ambiguous.

b) This definition makes no sense as it stands; $F(2)$ is not defined, since $F(0)$ isn't.

c) For $n = 4$, the recursive part makes no sense, since we would have to know $F(4/3)$. Also, $F(3)$ is ambiguous.

d) The definition is ambiguous about $n = 1$, since both the second clause and the third clause seem to apply. If the second clause is restricted to odd $n \geq 3$, then the sequence is well-defined and begins 1, 2, 2, 3, 3, 3, 4, 4, 5, 4.

e) We note that $F(1)$ is defined explicitly, but we run into problems trying to compute $F(2)$:

$$F(2) = 1 + F(F(1)) = 1 + F(2).$$

This not only leaves us begging the question as to what $F(2)$ is, but is a contradiction, since $0 \neq 1$.

61. In each case we will apply the definition to compute $\log^{(0)}$, then $\log^{(1)}$, then $\log^{(2)}$, then $\log^{(3)}$ and so on. As soon as we get an answer no larger than 1 we stop; the last "exponent" is the answer. In other words $\log^* n$ is the number of times we need to apply the log function until we get a value less than or equal to 1. Note that $\log^{(1)} n = \log n$ for $n > 0$. Similarly, $\log^{(2)} n = \log(\log n)$ as long as it is defined ($n > 1$), $\log^{(3)} n = \log(\log(\log n))$ as long as it is defined ($n > 2$), and so on. Normally the parentheses are understood and omitted.

a) $\log^{(0)} 2 = 2$, $\log^{(1)} 2 = \log 2 = 1$; therefore $\log^* 2 = 1$, the last "exponent."

b) $\log^{(0)} 4 = 4$, $\log^{(1)} 4 = \log 4 = 2$, $\log^{(2)} 4 = \log 2 = 1$; therefore $\log^* 4 = 2$, the last "exponent." We had to take the log twice to get from 4 down to 1.

c) $\log^{(0)} 8 = 8$, $\log^{(1)} 8 = \log 8 = 3$, $\log^{(2)} 8 = \log 3 \approx 1.585$, $\log^{(3)} 8 \approx \log 1.585 \approx 0.664$; therefore $\log^* 8 = 3$, the last "exponent." We had to take the log three times to get from 8 down to something no bigger than 1.
d) $\log^{(0)} 16 = 16$, $\log^{(1)} 16 = \log 16 = 4$, $\log^{(2)} 16 = \log 4 = 2$, $\log^{(3)} 16 = \log 2 = 1$; therefore $\log^* 16 = 3$, the last "exponent." We had to take the log three times to get from 16 down to 1.
e) $\log^{(0)} 256 = 256$, $\log^{(1)} 256 = \log 256 = 8$; by part **(c)**, we need to take the log three more times in order to get from 8 down to something no bigger than 1, so we have to take the log four times in all to get from 256 down to something no bigger than 1. Thus $\log^* 256 = 4$.
f) $\log 65536 = 16$; by part **(d)**, we need to take the log three more times in order to get from 16 down to 1, so we have to take the log four times in all to get from 65536 down to 1. Thus $\log^* 65536 = 4$.
g) $\log 2^{2048} = 2048$; taking log four more times gives us, successively, 11, approximately 3.46, approximately 1.79, approximately 0.84. So $\log^* 2^{2048} = 5$.

63. Each application of the function f subtracts another a from the argument. Therefore iterating this function k times (which is what $f^{(k)}$ does) has the effect of subtracting ka. Therefore $f^{(k)}(n) = n - ka$. Now $f_0^*(n)$ is the smallest k such that $f^{(k)}(n) \le 0$, i.e., $n - ka \le 0$. Solving this for k easily yields $k \ge n/a$. Thus $f_0^*(n) = \lceil n/a \rceil$ (we need to take the ceiling function because k must be an integer).

65. Each application of the function f takes the square root of its argument. Therefore iterating this function k times (which is what $f^{(k)}$ does) has the effect of taking the $(2^k)^{\text{th}}$ root. Therefore $f^{(k)}(n) = n^{1/2^k}$. Now $f_2^*(n)$ is the smallest k such that $f^{(k)}(n) \le 2$, that is, $n^{1/2^k} \le 2$. Solving this for n easily yields $n \le 2^{2^k}$, so $k \ge \log\log n$, where logarithm is taken to the base 2. Thus $f_2^*(n) = \lceil \log\log n \rceil$ for $n \ge 2$ (we need to take the ceiling function because k must be an integer) and $f_2^*(1) = 0$.

SECTION 5.4 Recursive Algorithms

Recursive algorithms are important theoretical entities, but they often cause a lot of grief on first encounter. Sometimes it is helpful to "play computer" very carefully to see how a recursive algorithm works. Ironically, however, it is good to avoid doing that after you get the idea. Instead, convince yourself that if the recursive algorithm handles the base case correctly, and handles the recursive step correctly (gives the correct answer assuming that the correct answer was obtained on the recursive call), then the algorithm works. Let the computer worry about actually "recursing all the way down to the base case"!

1. First, we use the recursive step to write $5! = 5 \cdot 4!$. We then use the recursive step repeatedly to write $4! = 4 \cdot 3!$, $3! = 3 \cdot 2!$, $2! = 2 \cdot 1!$, and $1! = 1 \cdot 0!$. Inserting the value of $0! = 1$, and working back through the steps, we see that $1! = 1 \cdot 1 = 1$, $2! = 2 \cdot 1! = 2 \cdot 1 = 2$, $3! = 3 \cdot 2! = 3 \cdot 2 = 6$, $4! = 4 \cdot 3! = 4 \cdot 6 = 24$, and $5! = 5 \cdot 4! = 5 \cdot 24 = 120$.

3. With this input, the algorithm uses the **else** clause to find that $\gcd(8,13) = \gcd(13 \textbf{ mod } 8, 8) = \gcd(5,8)$. It uses this clause again to find that $\gcd(5,8) = \gcd(8 \textbf{ mod } 5, 5) = \gcd(3,5)$, then to get $\gcd(3,5) = \gcd(5 \textbf{ mod } 3, 3) = \gcd(2,3)$, then $\gcd(2,3) = \gcd(3 \textbf{ mod } 2, 2) = \gcd(1,2)$, and once more to get $\gcd(1,2) = \gcd(2 \textbf{ mod } 1, 1) = \gcd(0,1)$. Finally, to find $\gcd(0,1)$ it uses the first step with $a = 0$ to find that $\gcd(0,1) = 1$. Consequently, the algorithm finds that $\gcd(8,13) = 1$.

5. First, because $n = 11$ is odd, we use the **else** clause to see that

$$mpower(3, 11, 5) = (mpower(3, 5, 5)^2 \textbf{ mod } 5 \cdot 3 \textbf{ mod } 5) \textbf{ mod } 5 .$$

We next use the **else** clause again to see that

$$mpower(3, 5, 5) = (mpower(3, 2, 5)^2 \textbf{ mod } 5 \cdot 3 \textbf{ mod } 5) \textbf{ mod } 5 .$$

Then we use the **else if** clause to see that

$$mpower(3, 2, 5) = mpower(3, 1, 5)^2 \textbf{ mod } 5 .$$

Using the **else** clause again, we have

$$mpower(3, 1, 5) = (mpower(3, 0, 5)^2 \textbf{ mod } 5 \cdot 3 \textbf{ mod } 5) \textbf{ mod } 5 .$$

Finally, using the **if** clause, we see that $mpower(3, 0, 5) = 1$. Now we work backward: $mpower(3, 1, 5) = (1^2 \textbf{ mod } 5 \cdot 3 \textbf{ mod } 5) \textbf{ mod } 5 = 3$, $mpower(3, 2, 5) = 3^2 \textbf{ mod } 5 = 4$, $mpower(3, 5, 5) = (4^2 \textbf{ mod } 5 \cdot 3 \textbf{ mod } 5) \textbf{ mod } 5 = 3$, and finally that $mpower(3, 11, 5) = (3^2 \textbf{ mod } 5 \cdot 3 \textbf{ mod } 5) \textbf{ mod } 5 = 2$. We conclude that $3^{11} \textbf{ mod } 5 = 2$.

7. The key idea for this recursive procedure is that $nx = (n-1)x + x$. Thus we compute nx by calling the procedure recursively, with n replaced by $n-1$, and adding x. The base case is $1 \cdot x = x$.

procedure *product*(n : positive integer, x : integer)
if $n = 1$ **then return** x
else return $product(n-1, x) + x$

9. If we have already found the sum of the first $n-1$ odd positive integers, then we can find the sum of the first n positive integers simply by adding on the value of the n^{th} odd positive integer. We need to realize that the n^{th} odd positive integer is $2n-1$, and we need to note that the base case (in which $n = 1$) gives us a sum of 1. The algorithm is then straightforward.

procedure *sum of odds*(n : positive integer)
if $n = 1$ **then return** 1
else return *sum of odds*$(n-1) + 2n - 1$

11. We recurse on the size of the list. If there is only one element, then it is the smallest. Otherwise, we find the smallest element in the list consisting of all but the last element of our original list, and compare it with the last element of the original list. Whichever is smaller is the answer. (We assume that there is already a function min, defined for two arguments, which returns the smaller.)

procedure *smallest*($a_1, a_2, \ldots, a_n$: integers)
if $n = 1$ **then return** 1
else return $\min(smallest(a_1, a_2, \ldots, a_{n-1}), a_n)$

13. We basically just take the recursive algorithm for finding $n!$ and apply the **mod** operation at each step. Note that this enables us to calculate $n! \textbf{ mod } m$ without using excessively large numbers, even if $n!$ is very large.

procedure *modfactorial*(n, m : positive integers)
if $n = 1$ **then return** 1
else return $(n \cdot (modfactorial(n-1, m)) \textbf{ mod } m$

15. We need to worry about which of our arguments is the larger. Since we are given $a < b$ as input, we need to make sure always to call the algorithm with the first argument less than the second. There need to be two stopping conditions: when $a = 0$ (in which case the answer is b), and when the two arguments have become equal (in which case the answer is their common value). Otherwise we use the recursive condition that $\gcd(a, b) = \gcd(a, b - a)$, taking care to reverse the arguments if necessary.

procedure $gcd(a, b$: nonnegative integers with $a < b)$
if $a = 0$ **then return** b
else if $a = b - a$ **then return** a
else if $a < b - a$ **then return** $gcd(a, b - a)$
else return $gcd(b - a, a)$

17. We build the recursive steps into the algorithm.

procedure $multiply(x, y$: nonnegative integers)
if $y = 0$ **then return** 0
else if y is even **then return** $2 \cdot multiply(x, y/2)$
else return $2 \cdot multiply(x, (y - 1)/2) + x$

19. We use strong induction on a, starting at $a = 0$. If $a = 0$, we know that $\gcd(0, b) = b$ for all $b > 0$, so the **if** clause handles this basis case correctly. Now fix $k > 0$ and assume the inductive hypothesis—that the algorithm works correctly for all values of its first argument less than k. Consider what happens with input (k, b), where $k < b$. Since $k > 0$, the **else** clause is executed, and the answer is whatever the algorithm gives as output for inputs $(b \textbf{ mod } k, k)$. Note that $b \textbf{ mod } k < k$, so the input pair is valid. By our inductive hypothesis, this output is in fact $\gcd(b \textbf{ mod } k, k)$. By Lemma 1 in Section 4.3 (when the Euclidean algorithm was introduced), we know that $\gcd(k, b) = \gcd(b \textbf{ mod } k, k)$, and our proof is complete.

21. For the basis step, if $n = 1$, then $nx = x$, and the algorithm correctly returns x. For the inductive step, assume that the algorithm correctly computes kx, and consider what it does to compute $(k + 1)x$. The recursive clause applies, and it recursively computes the product of $k + 1 - 1 = k$ and x, and then adds x. By the inductive hypothesis, it computes that product correctly, so the answer returned is $kx + x = (k + 1)x$, which is the correct answer.

23. As usual with recursive algorithms, the algorithm practically writes itself.

procedure $square(n$: nonnegative integer)
if $n = 0$ **then return** 0
else return $square(n - 1) + 2(n - 1) + 1$

The proof of correctness, by mathematical induction, practically writes itself as well. Let $P(n)$ be the statement that this algorithm correctly computes n^2. Since $0^2 = 0$, the algorithm works correctly (using the **if** clause) if the input is 0. Assume that the algorithm works correctly for input k. Then for input $k + 1$ it gives as output (because of the **else** clause) its output when the input is k, plus $2(k + 1 - 1) + 1$. By the inductive hypothesis, its output at k is k^2, so its output at $k+1$ is $k^2 + 2(k+1-1) + 1 = k^2 + 2k + 1 = (k+1)^2$, exactly what it should be.

25. Algorithm 2 uses 2^n multiplications by a, one for each factor of a in the product a^{2^n}. The algorithm in Exercise 24, based on squaring, uses only n multiplications (each of which is a multiplication of a number by itself). For instance, to compute $a^{2^4} = a^{16}$, this algorithm will compute $a \cdot a = a^2$ (one multiplication), then $a^2 \cdot a^2 = a^4$ (a second multiplication), then $a^4 \cdot a^4 = a^8$ (a third), and finally $a^8 \cdot a^8 = a^{16}$ (a fourth multiplication).

27. Algorithm 2 uses n multiplications by a, one for each factor of a in the product a^n. The algorithm in Exercise 26 will use $O(\log n)$ multiplications as it computes squares. Furthermore, in addition to squaring, sometimes a multiplication by a is needed; this will add at most another $O(\log n)$ multiplications. Thus a total of $O(\log n)$ multiplications are used altogether.

29. This is very similar to the recursive procedure for computing the Fibonacci numbers. Note that we can combine the two base cases (stopping rules) into one.

procedure *sequence*(n : nonnegative integer)
if $n < 2$ **then return** $n + 1$
else return *sequence*$(n-1) \cdot$ *sequence*$(n-2)$

31. The iterative version is much more efficient. The analysis is exactly the same as that for the Fibonacci sequence given in this section. Indeed, the n^{th} term in this sequence is actually just 2^{f_n}, as is easily shown by induction.

33. This is essentially just Algorithm 8, with a different operation and with different (and more) initial conditions.

```
procedure iterative(n : nonnegative integer)
if n = 0 then return 1
else if n = 1 then return 2
else
    x := 1
    y := 2
    z := 3
    for i := 1 to n − 2
        w := x + y + z
        x := y
        y := z
        z := w
return z
```

35. These algorithms are very similar to the procedures for computing the Fibonacci numbers. Note that for the recursive version, we can combine the three base cases (stopping rules) into one.

procedure *recursive*(n : nonnegative integer)
if $n < 3$ **then return** $2n + 1$
else return *recursive*$(n-1) \cdot ($*recursive*$(n-2))^2 \cdot ($*recursive*$(n-3))^3$

```
procedure iterative(n : nonnegative integer)
if n = 0 then return 1
else if n = 1 then return 3
else
    x := 1
    y := 3
    z := 5
    for i := 1 to n − 2
        w := z · y^2 · x^3
        x := y
        y := z
        z := w
return z
```

The recursive version is much easier to write, but the iterative version is much more efficient. In doing the computation for the iterative version, we just need to go through the loop $n-2$ times in order to compute a_n, so it requires $O(n)$ steps. In doing the computation for the recursive version, we are constantly recalculating previous values that we've already calculated, just as was the case with the recursive version of the algorithm to calculate the Fibonacci numbers.

37. We use the recursive definition of the reversal of a string given in Exercise 35 of Section 5.3, namely that $(vy)^R = y(v^R)$, where y is the last symbol in the string and v is the substring consisting of all but the last symbol. The right-hand side of the last statement in this procedure means that we concatenate b_n with the output of the recursive call.

procedure $reverse(b_1b_2\ldots b_n$: bit string)
if $n = 0$ **then return** λ
else return $b_n reverse(b_1b_2\ldots b_{n-1})$

39. The procedure correctly gives the reversal of λ as λ (the basis step of our proof by mathematical induction on n), and because the reversal of a string consists of its last character followed by the reversal of its first $n-1$ characters (see Exercise 35 in Section 5.3), the algorithm behaves correctly when $n > 0$ by the inductive hypothesis.

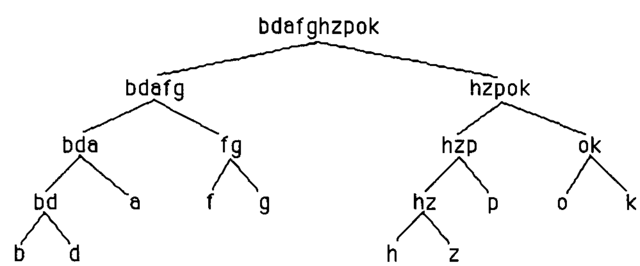
41. The algorithm merely implements the idea of Example 14 in Section 5.1. If $n = 1$ (the basis step here), we simply place the one right triomino so that its armpit corresponds to the hole in the 2×2 board. If $n > 1$, then we divide the board into four boards, each of size $2^{n-1} \times 2^{n-1}$, notice which quarter the hole occurs in, position one right triomino at the center of the board with its armpit in the quarter where the missing square is (see Figure 7 in Section 5.1), and invoke the algorithm recursively four times—once on each of the $2^{n-1} \times 2^{n-1}$ boards, each of which has one square missing (either because it was missing to begin with, or because it is covered by the central triomino).

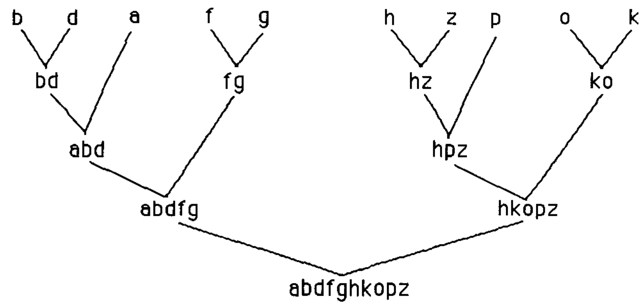
43. Essentially all we do is write down the definition as a procedure.

procedure $ackermann(m, n$: nonnegative integers)
if $m = 0$ **then return** $2 \cdot n$
else if $n = 0$ **then return** 0
else if $n = 1$ **then return** 2
else return $ackermann(m-1, ackermann(m, n-1))$

45. We assume that sorting is to be done into alphabetical order. First the list is split into the two lists b, d, a, f, g and h, z, p, o, k, and each of these is sorted by merge sort. Let us assume for a moment that this has been done, so the two lists are a, b, d, f, g and h, k, o, p, z. Then these two lists are merged into one sorted list, as follows. We compare a with h and find that a is smaller; thus a comes first in the merged list, and we pass on to b. Comparing b with h, we find that b is smaller, so b comes next in the merged list, and we pass on to d. We repeat this process (using Algorithm 10) until the lists are merged into one sorted list, $a, b, d, f, g, h, k, o, p, z$. (It was just a coincidence that every element in the first of these two lists came before every element in the second.)

Let us return to the question of how each of the 5-element lists was sorted. For the list b, d, a, f, g, we divide it into the sublists b, d, a and f, g. Again we sort each piece by the same algorithm, producing a, b, d and f, g, and we merge them into the sorted list a, b, d, f, g. Going one level deeper into the recursion, we see that sorting b, d, a was accomplished by splitting it into b, d and a, and sorting each piece by the same algorithm. The first of these required further splitting into b and d. One element lists are already sorted, of course. Similarly, the other 5-element list was sorted by a similar recursive process. A tree diagram for this problem is displayed below. The top half of the picture is a tree showing the splitting part of the algorithm. The bottom half shows the merging part as an upside-down tree.





47. All we have to do is to make sure that one of the lists is exhausted only when the other list has only one element left in it. In this case, a comparison is needed to place every element of the merged list into place, except for the last element. Clearly this condition is met if and only if the largest element in the combined list is in one of the initial lists and the second largest element is in the other. One such pair of lists is $\{1, 2, \ldots, m-1, m+n\}$ and $\{m, m+1, \ldots, m+n-1\}$.

49. We use strong induction on n, showing that the algorithm works correctly if $n = 1$, and that if it works correctly for $n = 1$ through $n = k$, then it also works correctly for $n = k + 1$. If $n = 1$, then the algorithm does nothing, which is correct, since a list with one element is already sorted. If $n = k + 1$, then the list is split into two lists, L_1 and L_2. By the inductive hypothesis, *mergesort* correctly sorts each of these sublists, and so it remains only to show that *merge* correctly merges two sorted lists into one. This is clear, from the code given in Algorithm 10, since with each comparison, the smallest element in $L_1 \cup L_2$ not yet put into L is put there.

51. We need to compare every other element with a_1. Thus at least $n-1$ comparisons are needed (we will assume for Exercises 53 and 55 that the answer is exactly $n - 1$). The actual number of comparisons depends on the actual encoding of the algorithm. With any reasonable encoding, it should be $O(n)$.

53. In our analysis we assume that a_1 is considered to be put between the two sublists, not as the last element of the first sublist (which would require an extra pass in some cases). In the worst case, the original list splits into lists of length 3 and 0 (with a_1 between them); by Exercise 51, this requires $4 - 1 = 3$ comparisons. No comparisons are needed to sort the second of these lists (since it is empty). To sort the first, we argue in the same way: the worst case is for a splitting into lists of length 2 and 0, requiring $3 - 1 = 2$ comparisons. Similarly, $2 - 1 = 1$ comparison is needed to split the list of length 2 into lists of length 1 and 0. In all, then, $3 + 2 + 1 = 6$ comparisons are needed in this worst case. (One can prove that this discussion really does deal with the worst case by looking at what happens in the various other cases.)

55. In our analysis we assume that a_1 is considered to be put between the two sublists, not as the last element of the first sublist (which would require an extra pass in some cases). We claim that the worst case complexity is $n(n-1)/2$ comparisons, and we prove this by induction on n. This is certainly true for $n = 1$, since no comparisons are needed. Otherwise, suppose that the initial split is into lists of size k and $n - k - 1$. By the inductive hypothesis, it will require $\big(k(k-1)/2\big) + \big((n-k-1)(n-k-2)/2\big)$ comparisons in the worst case to finish the algorithm. This quadratic function of k attains its maximum value if $k = 0$ (or $k = n - 1$), namely the value $(n-1)(n-2)/2$. Also, it took $n - 1$ comparisons to perform the first splitting. If we add these two quantities ($(n-1)(n-2)/2$ and $n - 1$) and do the algebra, then we obtain $n(n-1)/2$, as desired. Thus in the worst case the complexity is $O(n^2)$.

SECTION 5.5 Program Correctness

Entire books have been written on program verification; obviously here we barely scratch the surface. In some sense program verification is just a very careful stepping through a program to prove that it works correctly. There should be no problem verifying anything except loops; indeed it may seem that there is nothing to prove. Loops are harder to deal with. The trick is to find the right invariant. Once you have the invariant, it again is really a matter of stepping through one pass of the loop to make sure that the invariant is satisfied at the end of that pass, given that it was satisfied at the beginning. Analogous to our remark in the comments for Section 1.7, there is a deep theorem of logic (or theoretical computer science) that says essentially that there is no algorithm for proving correct programs correct, so the task is much more an art than a science.

Your proofs must be valid proofs, of course. You may use the rules of inference discussed in Section 1.6. What is special about proofs of program correctness is the addition of some special rules for this setting. These exercises (and the examples in the text) may seem overly simple, but unfortunately it is extremely hard to prove all but the simplest programs correct.

1. We suppose that initially $x = 0$. The segment causes two things to happen. First y is assigned the value of 1. Next the value of $x+y$ is computed to be $0+1=1$, and so z is assigned the value 1. Therefore at the end z has the value 1, so the final assertion is satisfied.

3. We suppose that initially $y = 3$. The effect of the first two statements is to assign x the value 2 and z the value $2+3=5$. Next, when the **if**...**then** statement is encountered, since the value of y is 3, and $3>0$ is true, the statement $z := z+1$ assigns the value $5+1=6$ to z (and the **else** clause is not executed). Therefore at the end, z has the value 6, so the final assertion $z=6$ is true.

5. We generalize the rule of inference for the **if**...**then**...**else** statement, given before Example 3. Let p be the initial assertion, and let q be the final assertion. If *condition* 1 is true, then S_1 will get executed, so we need $(p \wedge \textit{condition } 1)\{S_1\}q$. Similarly, if *condition* 2 is true, but *condition* 1 is false, then S_2 will get executed, so we need $(p \wedge \neg(\textit{condition } 1) \wedge \textit{condition } 2)\{S_2\}q$. This pattern continues, until the last statement we need is $\big(p \wedge \neg(\textit{condition } 1) \wedge \neg(\textit{condition } 2) \wedge \cdots \wedge \neg(\textit{condition } n-1)\big)\{S_n\}q$. Given all of these, we can conclude that pTq, where T is the entire statement. In symbols, we have

$$\begin{array}{l}
(p \wedge \textit{condition } 1)\{S_1\}q \\
(p \wedge \neg(\textit{condition } 1) \wedge \textit{condition } 2)\{S_2\}q \\
\quad\vdots \\
\big(p \wedge \neg(\textit{condition } 1) \wedge \neg(\textit{condition } 2) \wedge \cdots \wedge \neg(\textit{condition } n-1)\big)\{S_n\}q \\
\hline
\therefore\ p\{\textbf{if } \textit{condition } 1 \textbf{ then } S_1 \textbf{ else if } \textit{condition } 2 \textbf{ then } S_2 \ \ldots \textbf{else } S_n\}q.
\end{array}$$

7. The problem is similar to Example 4. We will use the loop invariant p: "$\textit{power} = x^{i-1}$ and $i \le n+1$." Now p is true initially, since before the loop starts, $i=1$ and $\textit{power} = 1 = x^0 = x^{1-1}$. (There is a technicality here: we define 0^0 to equal 1 in order for this to be correct if $x=0$. There is no harm in this, since $n>0$, so if $x=0$, then the program certainly computes the correct answer $x^n=0$.) We must now show that if p is true and $i \le n$ before some pass through the loop, then p remains true after that pass. The loop increments i by one. Hence since $i \le n$ before this pass through the loop, $i \le n+1$ after this pass. Also the loop assigns $\textit{power} \cdot x$ to $\textit{power}$. By the inductive hypothesis, $\textit{power}$ started with the value x^{i-1} (the old value of i). Therefore its new value is $x^{i-1} \cdot x = x^i = x^{(i+1)-1}$. But since $i+1$ is the new value of i, the statement $\textit{power} = x^{i-1}$ is true at the completion of this pass through the loop. Hence p remains true, so p is a loop invariant. Furthermore, the loop terminates after n traversals, with $i=n+1$, since i is assigned the value 1 prior to entering the loop, i is incremented by 1 on each pass, and the loop terminates when $i>n$. At termination we have $(i \le n+1) \wedge \neg(i \le n)$, so $i=n+1$. Hence $\textit{power} = x^{(n+1)-1} = x^n$, as desired.

9. We will break the problem up into the various statements that are left unproved in Example 5.

We must show that $p\{S_1\}q$, where p is the assertion that m and n are integers, and q is the proposition $p \wedge (a = |n|)$. This follows from Example 3 and the fact that the values of m and n have not been tampered with.

We must show that $q\{S_2\}r$, where r is the proposition $q \wedge (k = 0) \wedge (x = 0)$. This is clear, since in S_2, none of m, n, or a have been altered, but k and x have been assigned the value 0.

We must show that $(x = mk) \wedge (k \leq a)$ is an invariant for the loop in S_3. Assume that this statement is true before a pass through the loop. In the loop, k is incremented by 1. If $k < a$ (the condition of the loop), then at the end of the pass, $k < a + 1$, so $k \leq a$. Furthermore, since $x = mk$ at the beginning of the pass, and x is incremented by m inside the loop, we have $x = mk + m = m(k+1)$ at the end of the pass, which is precisely the statement that $x = mk$ for the updated value of k. When the loop terminates (which it clearly does after a iterations), $k = a$ (since $(k \leq a) \wedge \neg(k < a)$), and so $x = ma$ at this point.

Finally we must show that $s\{S_4\}t$, where s is the proposition $(x = ma) \wedge (a = |n|)$, and t is the proposition $\mathit{product} = mn$. The program segment S_4 assigns the value x or $-x$ to $\mathit{product}$, depending on the sign of n. We need to consider the two cases. If $n < 0$, then since $a = |n|$ we know that $a = -n$. Therefore $\mathit{product} = -x = -(ma) = -m(-n) = mn$. If $n \not< 0$, then since $a = |n|$ we know that $a = n$. Therefore $\mathit{product} = x = ma = mn$.

11. To say that the program assertion $p\{S\}q_1$ is true is to say that if p is true before S is executed, then q_1 is true after S is executed. To prove this, let us assume that p is true and then S is executed. Since $p\{S\}q_0$, we know that after S is executed q_0 is true. By modus ponens, since q_0 is true and $q_0 \rightarrow q_1$ is true, we know that q_1 is true, as desired.

13. Our loop invariant p is the proposition "$\gcd(a,b) = \gcd(x,y)$ and $y \geq 0$." First note that p is true before the loop is entered, since at that point $x = a$, $y = b$, and y is a positive integer (we use the initial assertion here). Now assume that p is true and $y > 0$; then the loop will be executed again. Within the loop x and y are replaced by y and $x \textbf{ mod } y$, respectively. According to Lemma 1 in Section 4.3, $\gcd(x,y) = \gcd(y, x \textbf{ mod } y)$. Therefore after the execution of the loop, the value of $\gcd(x,y)$ remains what it was before. Furthermore, since y is a remainder, it is still greater than or equal to 0. Hence p remains true—it is a loop invariant. Furthermore, if the loop terminates, then it must be the case that $y = 0$. In this case we know that $\gcd(x,y) = x$, the desired final assertion. Therefore the program, which gives x as its output, has correctly computed $\gcd(a,b)$. Finally (although this is not necessary to establish *partial* correctness), we can prove that the loop must terminate, since each iteration causes the value of y to decrease by at least 1 (by the definition of **mod**). Thus the loop can be iterated at most b times.

GUIDE TO REVIEW QUESTIONS FOR CHAPTER 5

1. **a)** no

b) Sometimes yes. If the given formula is correct, then it is often possible to prove it using the principle of mathematical induction (although it would be wishful thinking to believe that *every* such true formula could be so proved). If the formula is incorrect, then induction would not work, of course; thus an incorrect formula could not be shown to be incorrect using the principle.

c) See Exercise 9 in Section 5.1.

2. a) $n \geq 7$

b) For the basis step we just check that $11 \cdot 7 + 17 \leq 2^7$. Fix $n \geq 7$, and assume the inductive hypothesis, that $11n + 17 \leq 2^n$. Then $11(n+1) + 17 = (11n + 17) + 11 \leq 2^n + 11 < 2^n + 2^n = 2^{n+1}$. The strict inequality here follows from the fact that $n \geq 4$.

3. a) Carefully considering all the possibilities shows that the amounts of postage less than 32 cents that can be achieved are 0, 5, 9, 10, 14, 15, 18, 19, 20, 23, 24, 25, 27, 28, 29, and 30. All amounts greater than or equal to 32 cents can be achieved.

b) To prove this latter statement, we check the basis step by noting that $32 = 9 + 9 + 9 + 5$. Assume that we can achieve n cents, and consider $n+1$ cents, where $n \geq 32$. If the stamps used for n cents included a 9-cent stamp, then replacing it by two 5-cent stamps gives us $n+1$ cents, as desired. Otherwise only 5-cent stamps were used to achieve n cents, and since $n > 30$, there must be at least seven such stamps. Replace seven of the 5-cent stamps by four 9-cent stamps; this increases the amount of postage by $4 \cdot 9 - 7 \cdot 5 = 1$ cent, again as desired.

c) We check the base cases $32 = 3 \cdot 9 + 5$, $33 = 2 \cdot 9 + 3 \cdot 5$, $34 = 9 + 5 \cdot 5$, $35 = 7 \cdot 5$, and $36 = 4 \cdot 9$. Fix $n \geq 37$ and assume that all amounts from 32 to $n-1$ can be achieved. To achieve n cents postage, take the stamps used for $n-5$ cents (since $n \geq 37$, $n - 5 \geq 32$, so the inductive hypothesis applies) and adjoin a 5-cent stamp.

d) Let n be an integer greater than or equal to 32. We want to express n as a sum of a nonnegative multiple of 5 and a nonnegative multiple of 9. Divide n by 5 to obtain a quotient q and remainder r such that $n = 5q + r$ and $0 \leq r \leq 4$. Note that since $n \geq 32$, $q \geq 6$. If $r = 0$, then we already have n expressed in the desired form. If $r = 1$, then $n \geq 36$, so $q \geq 7$; thus we can write $n = 5q + 1 = 5(q-7) + 4 \cdot 9$ to get the desired decomposition. If $r = 2$, then we rewrite $n = 5q + 2 = 5(q-5) + 3 \cdot 9$. If $r = 3$, then we rewrite $n = 5q + 3 = 5(q-3) + 2 \cdot 9$. And if $r = 4$, then we rewrite $n = 5q + 4 = 5(q-1) + 9$. In each case we have the desired sum.

4. See Examples 2 and 3 in Section 5.2.

5. a) See p. 314 and Appendix 1 (Axiom 4 for the positive integers).

b) Let S be the set of positive integers that cannot be written as the product of primes. If $S \neq \emptyset$, then S has a least element, c. Clearly $c \neq 1$, since 1 is the product of no primes. Thus c is greater than 1. Now c cannot be prime, since as such it would already be written as the product of primes (namely itself). Therefore c is a composite number, say $c = ab$, where a and b are both positive integers less than c. Since c is the smallest element of S, neither a nor b is in S. Therefore both a and b *can* be written as the product of primes. But multiplying these products together patently shows that c is the product of primes. This is a contradiction to the choice of c. Therefore our assumption that $S \neq \emptyset$ was wrong, and the theorem is proved.

6. a) See Exercise 56 in Section 5.3. **b)** $f(1) = 2$, and $f(n) = (n+1)f(n-1)$ for all $n \geq 2$

7. a) See the top of p. 347. **b)** See Example 4 in Section 5.3.

8. a) See Exercise 57 in Section 5.3. **b)** $a_n = 3 \cdot 2^{n-3}$ for $n \geq 3$

9. See Examples 8 and 9 in Section 5.3.

10. a) See Example 7 in Section 5.3. **b)** See Example 12 in Section 5.3.

11. a) See the beginning of Section 5.4.

b) Call the sequence $a_1, a_2, \ldots, a_n$. If $n = 1$, then the $sum(a_1) = a_1$. Otherwise $sum(a_1, a_2, \ldots, a_n) = a_n + sum(a_1, a_2, \ldots, a_{n-1})$.

12. See Example 3 in Section 5.4.

13. **a)** See p. 367.

b) We split the list into the two halves: $4, 10, 1, 5, 3$ and $8, 7, 2, 6, 9$. We then merge sort each half by applying this algorithm recursively and merging the results. For the first half, for example, this means splitting $4, 10, 1, 5, 3$ into the two halves $4, 10, 1$ and $5, 3$, recursively sorting each half, and merging. For the second half of this, for example, it means splitting into 5 and 3, recursively sorting each half, and merging. Since these two halves are already sorted, we just merge, into the sorted list $3, 5$. Similarly, we will get $1, 4, 10$ for the result of merge sort applied to $4, 10, 1$. When we merge $1, 4, 10$ and $3, 5$, we get $1, 3, 4, 5, 10$. Finally, we merge this with the sorted second half, $2, 6, 7, 8, 9$, to obtain the completely sorted list $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$.

c) $O(n \log n)$; see pp. 369–370.

14. **a)** no

b) No—you also need to show that it halts for all inputs, and the initial and final assertions for which you provide a proof of partial correctness need to be appropriate ones (i.e., relevant to the question of whether the program produces the correct output).

15. See the rules displayed in Section 5.5.

16. See p. 375.

SUPPLEMENTARY EXERCISES FOR CHAPTER 5

1. Let $P(n)$ be the statement that this equation holds. The basis step consists of verifying that $P(1)$ is true, which is trivial because $2/3 = 1 - (1/3^1)$. For the inductive step we assume that $P(k)$ is true and try to prove $P(k+1)$. We have

$$\begin{aligned} \frac{2}{3} + \frac{2}{9} + \frac{2}{27} + \cdots + \frac{2}{3^n} + \frac{2}{3^{n+1}} &= 1 - \frac{1}{3^n} + \frac{2}{3^{n+1}} \quad \text{(by the inductive hypothesis)} \\ &= 1 - \frac{3}{3^{n+1}} + \frac{2}{3^{n+1}} \\ &= 1 - \frac{1}{3^{n+1}}, \end{aligned}$$

as desired.

3. We prove this by induction on n. If $n = 1$ (basis step), then the equation reads $1 \cdot 2^0 = (1-1) \cdot 2^1 + 1$, which is the true statement $1 = 1$. Assume that the statement is true for n:

$$1 \cdot 2^0 + 2 \cdot 2^1 + 3 \cdot 2^2 + \cdots + n \cdot 2^{n-1} = (n-1) \cdot 2^n + 1$$

We must show that it is true for $n+1$. Thus we have

$$\begin{aligned} &1 \cdot 2^0 + 2 \cdot 2^1 + 3 \cdot 2^2 + \cdots + n \cdot 2^{n-1} + (n+1) \cdot 2^n \\ &\qquad = (n-1) \cdot 2^n + 1 + (n+1) \cdot 2^n \quad \text{(by the inductive hypothesis)} \\ &\qquad = (2n) \cdot 2^n + 1 \\ &\qquad = n \cdot 2^{n+1} + 1 \\ &\qquad = \big((n+1) - 1\big) \cdot 2^{n+1} + 1, \end{aligned}$$

exactly as desired.

5. We prove this by induction on n. If $n=1$ (basis step), then the equation reads $1/(1\cdot 4)=1/4$, which is true. Assume that the statement is true for n:

$$\frac{1}{1\cdot 4}+\frac{1}{4\cdot 7}+\cdots+\frac{1}{(3n-2)(3n+1)}=\frac{n}{3n+1}$$

We must show that it is true for $n+1$. Thus we have

$$\begin{aligned}
\frac{1}{1\cdot 4}+\frac{1}{4\cdot 7}+\cdots+\frac{1}{(3n-2)(3n+1)}&+\frac{1}{\big(3(n+1)-2\big)\big(3(n+1)+1\big)}\\
&=\frac{n}{3n+1}+\frac{1}{\big(3(n+1)-2\big)\big(3(n+1)+1\big)} \quad \text{(by the inductive hypothesis)}\\
&=\frac{n}{3n+1}+\frac{1}{(3n+1)(3n+4)}\\
&=\frac{1}{3n+1}\left(n+\frac{1}{3n+4}\right)\\
&=\frac{1}{3n+1}\left(\frac{3n^2+4n+1}{3n+4}\right)\\
&=\frac{1}{3n+1}\left(\frac{(3n+1)(n+1)}{3n+4}\right)\\
&=\frac{n+1}{3n+4}\\
&=\frac{n+1}{3(n+1)+1},
\end{aligned}$$

exactly as desired.

7. Let $P(n)$ be the statement $2^n>n^3$. We want to prove that $P(n)$ is true for all $n>9$. The basis step is $n=10$, in which we have $2^{10}=1024>1000=10^3$. Assume $P(n)$; we want to show $P(n+1)$. Then we have

$$\begin{aligned}
(n+1)^3&=n^3+3n^2+3n+1\\
&\le n^3+3n^2+3n^2+3n^2 \quad (\text{since } n\ge 1)\\
&=n^3+9n^2\\
&<n^3+n^3 \quad (\text{since } n>9)\\
&=2n^3<2\cdot 2^n \quad \text{(by the inductive hypothesis)}\\
&=2^{n+1},
\end{aligned}$$

as desired.

9. This problem deals with factors in algebra. We have to be just a little clever. Let $P(n)$ be the statement that $a-b$ is a factor of a^n-b^n. We want to show that $P(n)$ is true for all positive integers n, and of course we will do so by induction. If $n=1$, then we have the trivial statement that $a-b$ is a factor of $a-b$. Next assume the inductive hypothesis, that $P(n)$ is true. We want to show $P(n+1)$, that $a-b$ is a factor of $a^{n+1}-b^{n+1}$. The trick is to rewrite $a^{n+1}-b^{n+1}$ by subtracting and adding ab^n (and hence not changing its value). We obtain $a^{n+1}-b^{n+1}=a^{n+1}-ab^n+ab^n-b^{n+1}=a(a^n-b^n)+b^n(a-b)$. Now this expression contains two terms. By the inductive hypothesis, $a-b$ is a factor of the first term. Obviously $a-b$ is a factor of the second. Therefore $a-b$ is a factor of the entire expression, and we are done.

11. This should be similar to Example 9 in Section 5.1. First we check the basis step: When $n=1$, $6^{n+1}+7^{2n-1}=36+7=43$, which is certainly divisible by 43. Assume the inductive hypothesis, that 43 divides $6^{n+1}+7^{2n-1}$; we must show that 43 divides $6^{n+2}+7^{2n+1}$. We have $6^{n+2}+7^{2n+1}=6\cdot 6^{n+1}+49\cdot 7^{2n-1}=6\cdot 6^{n+1}+6\cdot 7^{2n-1}+43\cdot 7^{2n-1}=6(6^{n+1}+7^{2n-1})+43\cdot 7^{2n-1}$. Now the first term is divisible by 43 because the inductive hypothesis guarantees that its second factor is divisible by 43. The second term is patently divisible by 43. Therefore the sum is divisible by 43, and our proof by mathematical induction is complete.

13. Let $P(n)$ be the given equation. It is certainly true for $n = 0$, since it reads $a = a$ in that case. Assume that $P(n)$ is true:

$$a + (a + d) + \cdots + (a + nd) = \frac{(n + 1)(2a + nd)}{2}$$

Then

$$\begin{aligned}
&a + (a + d) + \cdots + (a + nd) + \big(a + (n + 1)d\big) \\
&\quad = \frac{(n + 1)(2a + nd)}{2} + \big(a + (n + 1)d\big) \quad \text{(by the inductive hypothesis)} \\
&\quad = \frac{(n + 1)(2a + nd) + 2\big(a + (n + 1)d\big)}{2} \\
&\quad = \frac{(n + 1)(2a + nd) + 2a + nd + nd + 2d}{2} \\
&\quad = \frac{(n + 2)(2a + nd) + (n + 2)d}{2} \\
&\quad = \frac{(n + 2)\big(2a + (n + 1)d\big)}{2},
\end{aligned}$$

which is exactly $P(n + 1)$.

15. We use induction. If $n = 1$, then the left-hand side has just one term, namely $5/6$, and the right-hand side is $10/12$, which is the same number. Assume that the equation holds for $n = k$, and consider $n = k+1$. (Do not get confused by the choice of letters here! The index of summation in the problem as stated is just a dummy variable, and since we want to use k in the inductive hypothesis, we have changed the dummy summation index to i.) Then we have

$$\begin{aligned}
\sum_{i=1}^{k+1} \frac{i + 4}{i(i + 1)(i + 2)} &= \sum_{i=1}^{k} \frac{i + 4}{i(i + 1)(i + 2)} + \frac{k + 5}{(k + 1)(k + 2)(k + 3)} \\
&= \frac{k(3k + 7)}{2(k + 1)(k + 2)} + \frac{k + 5}{(k + 1)(k + 2)(k + 3)} \quad \text{(by the inductive hypothesis)} \\
&= \frac{1}{(k + 1)(k + 2)} \cdot \left(\frac{k(3k + 7)}{2} + \frac{k + 5}{k + 3}\right) \\
&= \frac{1}{2(k + 1)(k + 2)(k + 3)} \cdot (k(3k + 7)(k + 3) + 2(k + 5)) \\
&= \frac{1}{2(k + 1)(k + 2)(k + 3)} \cdot (3k^3 + 16k^2 + 23k + 10) \\
&= \frac{1}{2(k + 1)(k + 2)(k + 3)} \cdot (3k + 10)(k + 1)^2 \\
&= \frac{1}{2(k + 2)(k + 3)} \cdot (3k + 10)(k + 1) \\
&= \frac{(k + 1)(3(k + 1) + 7)}{2((k + 1) + 1)((k + 1) + 2)},
\end{aligned}$$

as desired.

17. When $n = 1$, we are looking for the derivative of $g(x) = xe^x$, which, by the product rule, is $x \cdot e^x + e^x = (x + 1)e^x$, so the statement is true for $n = 1$. Assume that the statement is true for $n = k$, that is, the k^{th} derivative is given by $g^{(k)} = (x + k)e^x$. Differentiating by the product rule gives us the $(k + 1)^{\text{st}}$ derivative: $g^{(k+1)} = (x + k)e^x + e^x = (x + (k + 1))e^x$, as desired.

19. We look at the first few Fibonacci numbers to see if there is a pattern: $f_0 = 0$ (even), $f_1 = 1$ (odd), $f_2 = 1$ (odd), $f_3 = 2$ (even), $f_4 = 3$ (odd), $f_5 = 5$ (odd), ... The pattern seems to be even-odd-odd, repeated forever. Since the pattern has period 3, we can formulate our conjecture as follows: f_n is even if

$n \equiv 0 \pmod 3$, and is odd in the other two cases. Let us prove this by mathematical induction. There are two base cases, $n = 0$ and $n = 1$. The conjecture is certainly true in each of them, since $0 \equiv 0 \pmod 3$ and f_0 is even, and $1 \not\equiv 0 \pmod 3$ and f_0 is odd. So we assume the inductive hypothesis and consider a given $n+1$. There are three cases to consider, depending on the value of $(n+1) \mathbf{~mod~} 3$. If $n+1 \equiv 0 \pmod 3$, then $n-1$ and n are congruent to 1 and 2 modulo 3, respectively. By the inductive hypothesis, both f_{n-1} and f_n are odd. Therefore f_{n+1}, which is the sum of these two numbers, is even, as desired. The other two cases are similar. If $n+1 \equiv 1 \pmod 3$, then $n-1$ and n are congruent to 2 and 0 modulo 3, respectively. By the inductive hypothesis, f_{n-1} is odd and f_n is even. Therefore f_{n+1}, which is the sum of these two numbers, is odd, as desired. On the other hand, if $n+1 \equiv 2 \pmod 3$, then $n-1$ and n are congruent to 0 and 1 modulo 3, respectively. By the inductive hypothesis, f_{n-1} is even and f_n is odd. Therefore f_{n+1}, which is the sum of these two numbers, is odd, as desired.

21. The important point to note here is that k can be thought of as a universally quantified variable for each n. Thus the statement we wish to prove is $P(n)$: for every k, $f_k f_n + f_{k+1} f_{n+1} = f_{n+k+1}$. We use mathematical induction. If $n = 0$ (the first base case), then we want to prove $P(0)$: for every k, $f_k f_0 + f_{k+1} f_1 = f_{0+k+1}$, which reduces to the identity $f_{k+1} = f_{k+1}$, since $f_0 = 0$ and $f_1 = 1$. If $n = 1$ (the second base case), then we want to prove $P(1)$: for every k, $f_k f_1 + f_{k+1} f_2 = f_{1+k+1}$, which reduces to the defining recurrence $f_k + f_{k+1} = f_{k+2}$, since $f_1 = 1$ and $f_2 = 1$. Now we assume the inductive hypothesis $P(n)$ and try to prove $P(n+1)$. It is a straightforward calculation, using the inductive hypothesis and the recursive definition of the Fibonacci numbers:

$$\begin{aligned} f_k f_{n+1} + f_{k+1} f_{n+2} &= f_k(f_{n-1} + f_n) + f_{k+1}(f_n + f_{n+1}) \\ &= f_k f_{n-1} + f_k f_n + f_{k+1} f_n + f_{k+1} f_{n+1} \\ &= (f_k f_{n-1} + f_{k+1} f_n) + (f_k f_n + f_{k+1} f_{n+1}) \\ &= f_{n-1+k+1} + f_{n+k+1} = f_{n+k+2}\,, \end{aligned}$$

as desired.

23. Let $P(n)$ be the statement $l_0^2 + l_1^2 + \cdots + l_n^2 = l_n l_{n+1} + 2$. We easily verify the two base cases, $P(0)$ and $P(1)$, since $2^2 = 2 \cdot 1 + 2$ and $2^2 + 1^2 = 1 \cdot 3 + 2$. Next assume the inductive hypothesis and consider $P(n+1)$. We have

$$\begin{aligned} l_0^2 + l_1^2 + \cdots + l_n^2 + l_{n+1}^2 &= l_n l_{n+1} + 2 + l_{n+1}^2 \\ &= l_{n+1}(l_n + l_{n+1}) + 2 \\ &= l_{n+1} l_{n+2} + 2\,, \end{aligned}$$

which is exactly what we wanted.

25. The identity is clearly true for $n = 1$. Let us expand the right-hand side for $n+1$, invoking the inductive hypothesis at the appropriate point (and using the suggested trigonometric identities as well as the fact that $i^2 = -1$):

$$\begin{aligned} \cos(n+1)x + i\sin(n+1)x &= \cos(nx + x) + i\sin(nx + x) \\ &= \cos nx \cos x - \sin nx \sin x + i(\sin nx \cos x + \cos nx \sin x) \\ &= \cos x(\cos nx + i\sin nx) + \sin x(-\sin nx + i\cos nx) \\ &= \cos x(\cos nx + i\sin nx) + i\sin x(i\sin nx + \cos nx) \\ &= (\cos nx + i\sin nx)(\cos x + i\sin x) \\ &= (\cos x + i\sin x)^n(\cos x + i\sin x) \\ &= (\cos x + i\sin x)^{n+1} \end{aligned}$$

27. First let's rewrite the right-hand side to make it simpler to work with, namely as $2^{n+1}(n^2-2n+3)-6$. We use induction. If $n=1$, then the left-hand side has just one term, namely 2, and the right-hand side is $4\cdot 2-6=2$ as well. Assume that the equation holds for $n=k$, and consider $n=k+1$. Then we have

$$\begin{aligned}
\sum_{j=1}^{k+1} j^2 2^j &= \sum_{j=1}^{k} j^2 2^j + (k+1)^2 2^{k+1}\\
&= 2^{k+1}(k^2-2k+3)-6+(k^2+2k+1)2^{k+1} \quad \text{(by the inductive hypothesis)}\\
&= 2^{k+1}(2k^2+4)-6\\
&= 2^{k+2}(k^2+2)-6\\
&= 2^{k+2}((k+1)^2-2(k+1)+3)-6,
\end{aligned}$$

as desired.

29. One solution here is to use partial fractions and telescoping. First note that

$$\frac{1}{j^2-1}=\frac{1}{2}\left(\frac{1}{j-1}-\frac{1}{j+1}\right).$$

Therefore when summing from 1 to n, the terms being added and the terms being subtracted all cancel out except for $1/(j-1)$ when $j=2$ and 3, and $1/(j+1)$ when $j=n-1$ and n. Thus the sum is just

$$\frac{1}{2}\left(\frac{1}{1}+\frac{1}{2}-\frac{1}{n}-\frac{1}{n+1}\right).$$

which simplifies, with a little algebra, to the expression given on the right-hand side of the formula in the exercise.

In the spirit of this chapter, however, we also give a proof by mathematical induction. Let $P(n)$ be the formula in the exercise. The basis step is for $n=2$, in which case both sides reduce to $1/3$. For the inductive step assume that the equation holds for $n=k$, and consider $n=k+1$. Then we have

$$\begin{aligned}
\sum_{j=1}^{k+1}\frac{1}{j^2-1} &= \sum_{j=1}^{k}\frac{1}{j^2-1}+\frac{1}{(k+1)^2-1}\\
&= \frac{(k-1)(3k+2)}{4k(k+1)}+\frac{1}{(k+1)^2-1} \quad \text{(by the inductive hypothesis)}\\
&= \frac{(k-1)(3k+2)}{4k(k+1)}+\frac{1}{k^2+2k}=\frac{(k-1)(3k+2)}{4k(k+1)}+\frac{1}{k(k+2)}\\
&= \frac{(k-1)(3k+2)(k+2)+4(k+1)}{4k(k+1)(k+2)}\\
&= \frac{3k^3+5k^2}{4k(k+1)(k+2)}=\frac{3k^2+5k}{4(k+1)(k+2)}\\
&= \frac{k(3k+5)}{4(k+1)(k+2)}=\frac{((k+1)-1)(3(k+1)+2)}{4(k+1)(k+2)},
\end{aligned}$$

which is exactly what $P(k+1)$ asserts.

31. Let $P(n)$ be the assertion that at least $n+1$ lines are needed to cover the lattice points in the given triangular region. Clearly $P(0)$ is true, because we need at least one line to cover the one point at $(0,0)$. Assume the inductive hypothesis, that at least $k+1$ lines are needed to cover the lattice points with $x\ge 0$, $y\ge 0$, and $x+y\le k$. Consider the triangle of lattice points defined by $x\ge 0$, $y\ge 0$, and $x+y\le k+1$. Because this set includes the previous set, at least $k+1$ lines are required just to cover the smaller set (by the inductive hypothesis). By way of contradiction, assume that $k+1$ lines could cover this larger set as well. Then these lines must also cover the $k+2$ points on the line $x+y=k+1$, namely $(0,k+1)$, $(1,k)$, $(2,k-1)$, …, $(k,1)$, $(k+1,0)$. But only the line $x+y=k+1$ itself can cover more than one of these points, because two distinct lines intersect in at most one point, and this line does nothing toward covering the lattice points in the smaller triangle. Therefore none of the $k+1$ lines that are needed to cover the lattice points in the smaller triangle can cover more than one of the points on the line $x+y=k+1$, and this leaves at least one point uncovered. Therefore our assumption that $k+1$ line could cover the larger set is wrong, and our proof is complete.

33. The basis step is the given statement defining $\mathbf{B}$. Assume the inductive hypothesis, that $\mathbf{B}^k = \mathbf{M}\mathbf{A}^k\mathbf{M}^{-1}$. We want to prove that $\mathbf{B}^{k+1} = \mathbf{M}\mathbf{A}^{k+1}\mathbf{M}^{-1}$. By definition $\mathbf{B}^{k+1} = \mathbf{B}\mathbf{B}^k = \mathbf{M}\mathbf{A}\mathbf{M}^{-1}\mathbf{B}^k = \mathbf{M}\mathbf{A}\mathbf{M}^{-1}\mathbf{M}\mathbf{A}^k\mathbf{M}^{-1}$ by the inductive hypothesis. But this simplifies, using rules for matrices, to $\mathbf{M}\mathbf{A}\mathbf{I}\mathbf{A}^k\mathbf{M}^{-1} = \mathbf{M}\mathbf{A}\mathbf{A}^k\mathbf{M}^{-1} = \mathbf{M}\mathbf{A}^{k+1}\mathbf{M}^{-1}$, as desired.

35. It takes some luck to be led to the solution here. We see that we can write $3! = 3+2+1$. We also have a recursive definition of factorial, that $(n+1)! = (n+1)n!$, so we might hope to multiply each of the divisors we got at the previous stage by $n+1$ to get divisors at this stage. Thus we would have $4! = 4\cdot 3! = 4(3+2+1) = 12+8+4$, but that gives us only three divisors in the sum, and we want four. That last divisor, which is $n+1$ can, however, be rewritten as the sum of n and 1, so our sum for $4!$ is $12+8+3+1$. Let's see if we can continue this. We have $5! = 5\cdot 4! = 5(12+8+3+1) = 50+40+15+5 = 50+40+15+4+1$. It seems to be working. The basis step $n=3$ is already done, so let's see if we can prove the inductive step. Assume that we can write $k!$ as a sum of the desired form, say $k! = a_1 + a_2 + \cdots + a_k$, where each a_i is a divisor of $k!$ and the divisors are listed in strictly decreasing order, and consider $(k+1)!$. Then we have $(k+1)! = (k+1)k! = (k+1)(a_1+a_2+\cdots+a_k) = (k+1)a_1 + (k+1)a_2 + \cdots + (k+1)a_k = (k+1)a_1 + (k+1)a_2 + \cdots + k\cdot a_k + a_k$. Because each a_i was a divisor of $k!$, each $(k+1)a_i$ is a divisor of $(k+1)!$, but what about those last two terms? We don't seem to have any way to know that $k\cdot a_k$ is a factor of $(k+1)!$. Hold on, in our exploration we always had the last divisor in our sum being 1. If so, then $k\cdot a_k = k$, which is a divisor of $(k+1)!$, and $a_k = 1$, so the new last summand is again 1. (Notice also that our list of summands is still in strictly decreasing order.) So our proof by mathematical induction needs to be of the following stronger result: For every $n \geq 3$, we can write $n!$ as the sum of n of its distinct positive divisors, one of which is 1. The argument we have just given proves this by mathematical induction.

37. When $n=1$ the statement is vacuously true. If $n=2$ there must be a woman first and a man second, so the statement is true. Assume that the statement is true for $n=k$, where $k \geq 2$, and consider $k+1$ people standing in a line, with a woman first and a man last. If the k^{th} person is a woman, then we have that woman standing in front of the man at the end, and we are done. If the k^{th} person is a man, then the first k people in line satisfy the conditions of the inductive hypothesis for the first k people in line, so again we can conclude that there is a woman directly in front of a man somewhere in the line.

39. (It will be helpful for the reader to draw a diagram to help in following this proof.) When $n=1$ there is one circle, and we can color the inside blue and the outside red to satisfy the conditions. Assume the inductive hypothesis that if there are k circles, then the regions can be 2-colored such that no regions with a common boundary have the same color, and consider a situation with $k+1$ circles. Remove one of the circles, producing a picture with k circles, and invoke the inductive hypothesis to color it in the prescribed manner. Then replace the removed circle and change the color of every region inside this circle (from red to blue, and from blue to red). It is clear that the resulting figure satisfies the condition, since if two regions have a common boundary, then either that boundary was an arc of the new circle, in which case the regions on either side used to be the same region and now the inside portion is colored differently from the outside, or else the boundary did not involve the new circle, in which case the regions are colored differently because they were colored differently before the new circle was restored.

41. We use induction. If $n = 1$ then the equation reads $1 \cdot 1 = 1 \cdot 2/2$, which is true. Assume that the equation is true for n and consider it for $n+1$. (We use the letter n rather than k, because k is used for something else here.) Then we have, with some messy algebra (including an application of Example 2 in Section 5.1 in line 4),

$$\begin{aligned}
\sum_{j=1}^{n+1}(2j-1)\left(\sum_{k=j}^{n+1}\frac{1}{k}\right) &= \sum_{j=1}^{n}(2j-1)\left(\sum_{k=j}^{n+1}\frac{1}{k}\right) + (2(n+1)-1)\cdot\frac{1}{n+1} \\
&= \sum_{j=1}^{n}(2j-1)\left(\frac{1}{n+1}+\sum_{k=j}^{n}\frac{1}{k}\right) + \frac{2n+1}{n+1} \\
&= \left(\frac{1}{n+1}\sum_{j=1}^{n}(2j-1)\right) + \left(\sum_{j=1}^{n}(2j-1)\left(\sum_{k=j}^{n}\frac{1}{k}\right)\right) + \frac{2n+1}{n+1} \\
&= \left(\frac{1}{n+1}\cdot n^2\right) + \frac{n(n+1)}{2} + \frac{2n+1}{n+1} \quad \text{(by the inductive hypothesis)} \\
&= \frac{2n^2 + n(n+1)^2 + (4n+2)}{2(n+1)} \\
&= \frac{2(n+1)^2 + n(n+1)^2}{2(n+1)} \\
&= \frac{(n+1)(n+2)}{2},
\end{aligned}$$

as desired.

43. Let $T(n)$ be the statement that the sequence of towers of 2 is eventually constant modulo n. We will use strong induction to prove that $T(n)$ is true for all positive integers n. Basis step: When $n = 1$ (and $n = 2$), the sequence of towers of 2 modulo n is the sequence of all 0's. Inductive step: Suppose that k is an integer with $k \geq 2$. Suppose that $T(j)$ is true for $1 \leq j \leq k-1$. In the proof of the inductive step we denote the r^{th} term of the sequence modulo n by a_r. We will split the proof of the inductive step into two cases, based on the parity of k.

Suppose k is even. Let $k = 2^s q$ where $s \geq 1$ and $q < k$ is odd. When j is large enough, $a_{j-2} \geq s$, and for such j, $a_j = 2^{2^{a_{j-2}}}$ is a multiple of 2^s. It follows that for sufficiently large j, $a_j \equiv 0 \pmod{2^s}$. Hence, for large enough i, 2^s divides $a_{i+1} - a_i$. By the inductive hypothesis $T(q)$ is true, so the sequence $a_1, a_2, a_3, \ldots$ is eventually constant modulo q. This implies that for large enough i, q divides $a_{i+1} - a_i$. Because $\gcd(q, 2^s) = 1$ and for sufficiently large i both q and 2^s divide $a_{i+1} - a_i$, $k = 2^s q$ divides $a_{i+1} - a_i$ for sufficiently large i. Hence, for sufficiently large i, $a_{i+1} - a_i \equiv 0 \pmod{k}$. This means that the sequence is eventually constant modulo k.

Finally, suppose k is odd. Then $\gcd(2, k) = 1$, so by Euler's theorem (found in elementary number theory books, such as the author's), we know that $2^{\phi(k)} \equiv 1 \pmod{k}$, where ϕ is Euler's phi function (see preamble to Exercise 21 in Section 4.3). Let $r = \phi(k)$. Because $r < k$, by the inductive hypothesis $T(r)$, the sequence $a_1, a_2, a_3, \ldots$ is eventually constant modulo r, say equal to c. Hence for large enough i, for some integer t_i, $a_i = t_i r + c$. Hence $a_{i+1} = 2^{a_i} = 2^{t_i r + c} = (2^r)^{t_i} 2^c \equiv 2^c \pmod{k}$. This shows that $a_1, a_2, \ldots$ is eventually constant modulo k.

45. **a)** $M(102) = 102 - 10 = 92$ **b)** $M(101) = 101 - 10 = 91$
c) $M(99) = M(M(99+11)) = M(M(110)) = M(100) = M(M(111)) = M(101) = 91$
d) $M(97) = M(M(108)) = M(98) = M(M(109)) = M(99) = 91$ (using part **(c)**)

e) This one is too long to show in its entirety here, but here is what is involved. First, $M(87) = M(M(98)) = M(91)$, using part **(d)**. Then $M(91) = M(M(102)) = M(92)$ from part **(a)**. In a similar way, we find that $M(92) = M(93)$, and so on, until it equals $M(97)$, which we found in part **(d)** to be 91. Hence the answer is 91.

f) Using what we learned from part **(e)**, we have $M(76) = M(M(87)) = M(91) = 91$.

47. The basis step is wrong. The statement makes no sense for $n = 1$, since the last term on the left-hand side would then be $1/(0 \cdot 1)$, which is undefined. The first n for which it makes sense is $n = 2$, when it reads

$$\frac{1}{1 \cdot 2} = \frac{3}{2} - \frac{1}{2}.$$

Of course this statement is false, since $\frac{1}{2} \neq 1$. Therefore the basis step fails, and so the "theorem" is not true.

49. We will prove by induction that n circles divide the plane into $n^2 - n + 2$ regions. One circle certainly divides the plane into two regions (the inside and the outside), and $1^2 - 1 + 2 = 2$. Thus the statement is correct for $n = 1$. We assume that the statement is true for n circles, and consider it for $n + 1$ circles. Let us imagine an arrangement of $n + 1$ circles in the plane, each pair intersecting in exactly two points, no point common to three circles. If we remove one circle, then we are left with n circles, and by the inductive hypothesis they divide the plane into $n^2 - n + 2$ regions. Now let us draw the circle that we removed, starting at a point at which it intersects another circle. As we proceed around the circle, every time we encounter a point on one of the circles that was already there, we cut off a new region (in other words, we divide one old region into two). Therefore the number of regions that are added on account of this circle is equal to the number of points of intersection of this circle with the other n circles. We are told that each other circle intersects this one in exactly two points. Therefore there are a total of $2n$ points of intersection, and hence $2n$ new regions. Therefore the number of regions determined by $n+1$ circles is $n^2 - n + 2 + 2n = n^2 + n + 2 = (n+1)^2 - (n+1) + 2$ (the last equality is just algebra). Thus we have derived that the statement is also true for $n + 1$, and our proof is complete.

51. We will give a proof by contradiction. Let us consider the set $B = \{\, b\sqrt{2} \mid b \text{ and } b\sqrt{2} \text{ are positive integers} \,\}$. Clearly B is a subset of the set of positive integers. Now if $\sqrt{2}$ is rational, say $\sqrt{2} = p/q$, then $B \neq \emptyset$, since $q\sqrt{2} = p \in B$. Therefore by the well-ordering property, B contains a smallest element, say $a = b\sqrt{2}$. Then $a\sqrt{2} - a = a\sqrt{2} - b\sqrt{2} = (a-b)\sqrt{2}$. Since $a\sqrt{2} = 2b$ and a are both integers, so is this quantity. Furthermore, it is a positive integer, since it equals $a(\sqrt{2} - 1)$ and $\sqrt{2} - 1 > 0$. Therefore $a\sqrt{2} - a \in B$. But clearly $a\sqrt{2} - a < a$, since $\sqrt{2} < 2$. This contradicts our choice of a to be the smallest element of B. Therefore our original assumption that $\sqrt{2}$ is rational is false.

53. a) We use the following lemma: A positive integer d is a common divisor of a_1, a_2, $\ldots$, a_n if and only if d is a divisor of $\gcd(a_1, a_2, \ldots, a_n)$. [Proof: The prime factorization of $\gcd(a_1, a_2, \ldots, a_n)$ is $\prod p_i^{e_i}$, where e_i is the minimum exponent of p_i among a_1, a_2, $\ldots$, a_n. Clearly d divides every a_j if and only if the exponent of p_i in the prime factorization of d is less than or equal to e_i for every i, which happens if and only if $d \mid \gcd(a_1, a_2, \ldots, a_n)$.] Now let $d = \gcd(a_1, a_2, \ldots, a_n)$. Then d must be a divisor of each a_i, and hence must be a divisor of $\gcd(a_{n-1}, a_n)$ as well. Therefore d is a common divisor of $a_1, a_2, \ldots, a_{n-2}, \gcd(a_{n-1}, a_n)$. To show that it is the greatest common divisor of these numbers, suppose that e is any common divisor of these numbers. Then e is a divisor of each a_i for $1 \leq i \leq n-2$, and, being a divisor of $\gcd(a_{n-1}, a_n)$, it is also a divisor of a_{n-1} and a_n. Therefore e is a common divisor of *all* the a_i and hence a divisor of their common divisor, d. This shows that d is the greatest common divisor of $a_1, a_2, \ldots, a_{n-2}, \gcd(a_{n-1}, a_n)$.

b) If $n = 2$, then we just apply the Euclidean algorithm to a_1 and a_2. Otherwise, we apply the Euclidean algorithm to a_{n-1} and a_n, obtaining an answer d, and then apply this algorithm recursively to $a_1, a_2, \ldots, a_{n-2}, d$. Note that this last sequence has only $n - 1$ numbers in it.

55. We begin by computing $f(n)$ for the first few values of n, using the recursive definition. Thus we have $f(1) = 1$, $f(2) = f(1)+4-1 = 1+4-1 = 4$, $f(3) = f(2)+6-1 = 4+6-1 = 9$, $f(4) = f(3)+8-1 = 9+8-1 = 16$. The pattern seems clear, so we conjecture that $f(n) = n^2$. Now we prove this by induction. The base case we have already verified. So assume that $f(n) = n^2$. All we have to do is show that $f(n+1) = (n+1)^2$. By the recursive definition we have $f(n+1) = f(n) + 2(n+1) - 1$. This equals $n^2 + 2(n+1) - 1$ by the inductive hypothesis, and by algebra we have $n^2 + 2(n+1) - 1 = (n+1)^2$, as desired.

57. The recursive definition says that we can "grow" strings in S by appending 0's on the left and 1's on the right, as many as we wish.

a) The only string of length 0 in S is λ. There are two strings of length 1 in S, obtained either by appending a 0 to the front of λ or a 1 to the end of λ, namely the strings 0 and 1. The strings of length 2 in S come from the strings of length 1 by appending either a 0 to the front or a 1 to the end; they are 00, 01, and 11. Similarly, we can append a 0 to the front or a 1 to the end of any of these strings to get the strings of length 3 in S, namely 000, 001, 011, and 111. Continuing in this manner, we see that the other strings in S of length less than or equal to 5 are 0000, 0001, 0011, 0111, 1111, 00000, 00001, 00011, 00111, 01111, and 11111.

b) The simplest way to describe these strings is $\{\, 0^m 1^n \mid m \text{ and } n \text{ are nonnegative integers} \,\}$.

59. Applying the first recursive step once to λ tells us that $() \in B$. Then applying the second recursive step to this string tells us that $()() \in B$. Finally, we apply the first recursive step once more to get $(()()) \in B$. To see that $(()))$ is not in B, we invoke Exercise 62. Since the number of left parentheses does not equal the number of right parentheses, this string is not balanced.

61. There is of course the empty string, with 0 symbols. By the first recursive rule, we get the string $()$. If we apply the first recursive rule to this string, then we get $(())$, and if we apply the second recursive rule, then we get $()()$. These are the only strings in B with four or fewer symbols.

63. The definition simply says that N of a string is a count of the parentheses, with each left parenthesis counting $+1$ and each right parenthesis counting -1.

a) There is one left parenthesis and one right parenthesis, so $N(()) = 1 - 1 = 0$.

b) There are 3 left parentheses and 5 right parentheses, so $N()))())(() = 3 - 5 = -2$.

c) There are 4 left parentheses and 2 right parentheses, so $N((()(()) = 4 - 2 = 2$.

d) There are 6 left parentheses and 6 right parentheses, so $N(()((()))(())) = 6 - 6 = 0$.

65. The basic idea, of course, is to turn the definition into a procedure. The recursive part of the definition tells us how to find elements of B from shorter elements of B. The naive approach, however, is not very good, because we end up adding to B strings that already are there. For example, the string $()()()$ occurs in two different ways from the rule "$xy \in B$ if $x, y \in B$": by letting $x = ()()$ and $y = ()$, and by letting $x = ()$ and $y = ()()$.

To avoid this problem, we will keep two lists of strings, whose union is the set $B(n)$ of balanced strings of parentheses of length not exceeding n. The set $S(n)$ will be those balanced strings w of length at most n such that $w = uv$, where $u, v \neq \lambda$ and u and v are balanced. The set $T(n)$ will be all other balanced strings of length at most n. Note that, for example, $\lambda \in T$, $() \in T$, $(()) \in T$, but $()() \in S$. Since all the strings in B are of even length, we really only need to work with even values of n, dragging the odd values along for the ride.

```
procedure generate(n : nonnegative integer)
if n is odd then
        S := S(n − 1)  {the S constructed by generate(n − 1)}
        T := T(n − 1)  {the T constructed by generate(n − 1)}
else if n = 0 then
        S := ∅
        T := {λ}
else
        S' := S(n − 2)  {the S constructed by generate(n − 2)}
        T' := T(n − 2)  {the T constructed by generate(n − 2)}
        T := T' ∪ { (x) | x ∈ T' ∪ S' ∧ length(x) = n − 2 }
        S := S' ∪ { xy | x ∈ T' ∧ y ∈ T' ∪ S' ∧ length(xy) = n }
{ T ∪ S is the set of balanced strings of length at most n }
```

67. There are two cases. If $x \le y$ initially, then the statement $x := y$ is not executed, so x and y remain unchanged and $x \le y$ is a true final assertion. If $x > y$ initially, then the statement $x := y$ is executed, so $x = y$ at the end, and thus $x \le y$ is again a true final assertion. These are the only two possibilities associated with the initial condition **T** (true), so our proof is complete.

69. If the list has just one element in it, then the number of 0's is 1 if the element is 0 and is 0 otherwise. That forms the basis step of our algorithm. For the recursive step, the number of occurrences of 0 in a list L is the same as the number of occurrences in the list L without its last term if that last term is not a 0, and is one more than this value if it is. We can write this in pseudocode as follows.

```
procedure zerocount(a_1, a_2, ..., a_n : list of integers)
if n = 1 then
        if a_1 = 0 then return 1
        else return 0
else
        if a_n = 0 then return zerocount(a_1, a_2, ..., a_{n-1}) + 1
        else return zerocount(a_1, a_2, ..., a_{n-1})
```

71. From the numerical evidence in Exercise 70, it appears that $a(n)$ is a natural number and $a(n) \le n$ for all n. We prove that a is well-defined by showing that this observation is in fact true. Obviously the proof is by mathematical induction. The basis step is $n = 0$, for which the statement is obviously true, since $a(0) = 0$. Now assume that $a(n-1)$ is a natural number and $a(n-1) \le n-1$. Then $a(a(n-1))$ is a applied to some natural number less than or equal to $n-1$; by the inductive hypothesis this value is some natural number less than or equal to $n-1$. Therefore $a(a(n-1))$ is also some natural number less than or equal to $n-1$ (again by the inductive hypothesis). Therefore $n - a(a(n-1))$ is n minus some natural number less than or equal to $n-1$, which is some natural number less than or equal to n, and we are done.

73. From Exercise 72 we know that $a(n) = \lfloor (n+1)\mu \rfloor$ and that $a(n-1) = \lfloor n\mu \rfloor$. Since μ is less than 1, these two values are either equal or they differ by 1. First suppose that $\mu n - \lfloor \mu n \rfloor < 1 - \mu$. This is equivalent to $\mu(n+1) < 1 + \lfloor \mu n \rfloor$. If this is true, then clearly $\lfloor \mu(n+1) \rfloor = \lfloor \mu n \rfloor$. On the other hand, if $\mu n - \lfloor \mu n \rfloor \ge 1 - \mu$, then $\mu(n+1) \ge 1 + \lfloor \mu n \rfloor$, so $\lfloor \mu(n+1) \rfloor = \lfloor \mu n \rfloor + 1$, as desired.

75. We apply the definition:

$$\begin{aligned}
m(0) &= 0 & f(0) &= 1\\
m(1) &= 1 - f(m(0)) = 1 - f(0) = 1 - 1 = 0 & f(1) &= 1 - m(f(0)) = 1 - m(1) = 1 - 0 = 1\\
m(2) &= 2 - f(m(1)) = 2 - f(0) = 2 - 1 = 1 & f(2) &= 2 - m(f(1)) = 2 - m(1) = 2 - 0 = 2\\
m(3) &= 3 - f(m(2)) = 3 - f(1) = 3 - 1 = 2 & f(3) &= 3 - m(f(2)) = 3 - m(2) = 3 - 1 = 2\\
m(4) &= 4 - f(m(3)) = 4 - f(2) = 4 - 2 = 2 & f(4) &= 4 - m(f(3)) = 4 - m(2) = 4 - 1 = 3\\
m(5) &= 5 - f(m(4)) = 5 - f(2) = 5 - 2 = 3 & f(5) &= 5 - m(f(4)) = 5 - m(3) = 5 - 2 = 3\\
m(6) &= 6 - f(m(5)) = 6 - f(3) = 6 - 2 = 4 & f(6) &= 6 - m(f(5)) = 6 - m(3) = 6 - 2 = 4\\
m(7) &= 7 - f(m(6)) = 7 - f(4) = 7 - 3 = 4 & f(7) &= 7 - m(f(6)) = 7 - m(4) = 7 - 2 = 5\\
m(8) &= 8 - f(m(7)) = 8 - f(4) = 8 - 3 = 5 & f(8) &= 8 - m(f(7)) = 8 - m(5) = 8 - 3 = 5\\
m(9) &= 9 - f(m(8)) = 9 - f(5) = 9 - 3 = 6 & f(9) &= 9 - m(f(8)) = 9 - m(5) = 9 - 3 = 6
\end{aligned}$$

77. By Exercise 76 the sequence starts out 1, 2, 2, 3, 3, 4, 4, 4, 5, 5, 5, 6, 6, 6, 6, 7, 7, 7, 7, 8, ..., and we see that $f(1) = 1$ (since the last occurrence of 1 is in position 1), $f(2) = 3$ (since the last occurrence of 2 is in position 3), $f(3) = 5$ (since the last occurrence of 3 is in position 5), $f(4) = 8$ (since the last occurrence of 4 is in position 8), and so on. Since the sequence is nondecreasing, the last occurrence of n must be in the position for which the total number of 1s, 2s, 3s, ..., n's all together is that position number. But since a_k gives the number of occurrences of k, this is just $\sum_{k=1}^{n} a_k$, as desired. For example,

$$\sum_{k=1}^{6} a_k = 1 + 2 + 2 + 3 + 3 + 4 = 15 = f(6),$$

the position where the last 6 occurs.

Since we just saw that $f(n)$ is the sum of the first n terms of the sequence, $f(f(n))$ must be the sum of the first $f(n)$ terms of the sequence. But since $f(n)$ is the last term whose value is n, this means the sum of all the terms of the sequence whose value is at most n. Since there are a_k terms of the sequence whose value is k, this sum must be $\sum_{k=1}^{n} k \cdot a_k$, as desired. For example,

$$\sum_{k=1}^{3} k \cdot a_k = 1 \cdot 1 + 2 \cdot 2 + 2 \cdot 3 = 11 = f(f(3)) = f(5),$$

the position where the last 5 occurs.

WRITING PROJECTS FOR CHAPTER 5

Books and articles indicated by bracketed symbols below are listed near the end of this manual. You should also read the general comments and advice you will find there about researching and writing these essays.

1. Start with the historical footnote in the text. The standard history of mathematics references, such as [Bo4] and [Ev3], might have something or might provide a hint of where to look next.

2. There is a nice chapter on this in [He]. A Web search should also turn up useful pages, such as this one: `www-cgrl.cs.mcgill.ca/~godfried/teaching/cg-projects/97/Octavian/compgeom.html`

3. There are several textbooks on computational geometry, such as [O'R]. A comprehensive website on the subject can be found here: `compgeom.cs.uiuc.edu/~jeffe/compgeom/`

4. The ratio of successive Fibonacci numbers approaches a value known as the "golden ratio," so it would be useful to search for this topic as well. A recent and somewhat controversial book on the subject [Li] debunks some of the more outrageous claimed applications. This website seems to have a wealth of information on applications of Fibonacci numbers: `www.cs.rit.edu/~pga/Fibo/fact_sheet.html`

5. You can find some references, as well as an historical discussion of the Ackermann function and an iterative algorithm for computing it, in [GrZe].

6. Try searching your library's on-line catalog or the Web under keywords like *program correctness* or *verification.* Or look at [Ba1], [Di], or [Ho1].

7. As in Writing Project 6, a key-word search might turn up something. One book to look at is [De1].