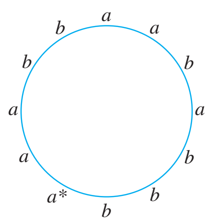
H 38. Suppose that n a's and n b's are distributed around the outside of a circle. Use mathematical induction to prove that for all integers $n \geq 1$, given any such arrangement, it is possible to find a starting point so that if one travels around the circle in a clockwise direction, the number of a's one has passed is never less than the number of b's one has passed. For example, in the diagram shown below, one could start at the a with an asterisk.



39. For a polygon to be **convex** means that all of its interior angles are less than 180 degrees. Use mathematical induction to prove that for all integers $n \geq 3$, the angles of any n-sided convex polygon add up to $180(n-2)$ degrees.

40. a. Prove that in an 8×8 checkerboard with alternating black and white squares, if the squares in the top right and bottom left corners are removed the remaining board cannot be covered with dominoes. (*Hint*: Mathematical induction is not needed for this proof.)

    b. Use mathematical induction to prove that for all integers n, if a $2n \times 2n$ checkerboard with alternating black and white squares has one white square and one black square removed anywhere on the board, the remaining squares can be covered with dominoes.

Answers for Test Yourself

1. deductive 2. prove

5.4 Strong Mathematical Induction and the Well-Ordering Principle for the Integers

Mathematics takes us still further from what is human into the region of absolute necessity, to which not only the actual world, but every possible world, must conform.
— Bertrand Russell, 1902

Strong mathematical induction is similar to ordinary mathematical induction in that it is a technique for establishing the truth of a sequence of statements about integers. Also, a proof by strong mathematical induction consists of a basis step and an inductive step. However, the basis step may contain proofs for several initial values, and in the inductive step the truth of the predicate $P(n)$ is assumed not just for one value of n but for *all* values through k, and then the truth of $P(k+1)$ is proved.

Principle of Strong Mathematical Induction

Let $P(n)$ be a property that is defined for integers n, and let a and b be fixed integers with $a \leq b$. Suppose the following two statements are true:

1. $P(a), P(a+1), \ldots,$ and $P(b)$ are all true. **(basis step)**
2. For any integer $k \geq b$, if $P(i)$ is true for all integers i from a through k, then $P(k+1)$ is true. **(inductive step)**

Then the statement

$$\text{for all integers } n \geq a, P(n)$$

is true. (The supposition that $P(i)$ is true for all integers i from a through k is called the **inductive hypothesis.** Another way to state the inductive hypothesis is to say that $P(a), P(a+1), \ldots, P(k)$ are all true.)

Any statement that can be proved with ordinary mathematical induction can be proved with strong mathematical induction. The reason is that given any integer $k \geq b$, if the truth of $P(k)$ alone implies the truth of $P(k+1)$, then certainly the truth of $P(a)$, $P(a+1), \ldots,$ and $P(k)$ implies the truth of $P(k+1)$. It is also the case that any statement that can be proved with strong mathematical induction can be proved with ordinary mathematical induction. A proof is sketched in exercise 27 at the end of this section.

Strictly speaking, the principle of strong mathematical induction can be written without a basis step if the inductive step is changed to "$\forall k \geq a-1$, if $P(i)$ is true for all integers i from a through k, then $P(k+1)$ is true." The reason for this is that the statement "$P(i)$ is true for all integers i from a through k" is vacuously true for $k = a-1$. Hence, if the implication in the inductive step is true, then the conclusion $P(a)$ must also be true,* which proves the basis step. However, in many cases the proof of the implication for $k > b$ does not work for $a \leq k \leq b$. So it is a good idea to get into the habit of thinking separately about the cases where $a \leq k \leq b$ by explicitly including a basis step.

The principle of strong mathematical induction is known under a variety of different names including the *second principle of induction*, the *second principle of finite induction*, and the *principle of complete induction*.

Applying Strong Mathematical Induction

The divisibility-by-a-prime theorem states that any integer greater than 1 is divisible by a prime number. We prove this theorem using strong mathematical induction.

Example 5.4.1 Divisibility by a Prime

Prove Theorem 4.3.4: Any integer greater than 1 is divisible by a prime number.

Solution The idea for the inductive step is this: If a given integer greater than 1 is not itself prime, then it is a product of two smaller positive integers, each of which is greater than 1. Since you are assuming that each of these smaller integers is divisible by a prime number, by transitivity of divisibility, those prime numbers also divide the integer you started with.

Proof (by strong mathematical induction):

Let the property $P(n)$ be the sentence

n is divisible by a prime number. $\leftarrow P(n)$

Show that P(2) is true:
To establish $P(2)$, we must show that

2 is divisible by a prime number. $\leftarrow P(2)$

But this is true because 2 is divisible by 2 and 2 is a prime number.

Show that for all integers $k \geq 2$, if P(i) is true for all integers i from 2 through k, then P(k + 1) is also true:

continued on page 270

*If you have proved that a certain if-then statement is true and if you also know that the hypothesis is true, then the conclusion must be true.

Let k be any integer with $k \geq 2$ and suppose that

i is divisible by a prime number for all integers
i from 2 through k. ← inductive hypothesis

We must show that

$k + 1$ is divisible by a prime number. $\leftarrow P(k+1)$

Case 1 (k + 1 is prime): In this case $k + 1$ is divisible by a prime number, namely itself.

Case 2 (k + 1 is not prime): In this case $k + 1 = ab$ where a and b are integers with $1 < a < k + 1$ and $1 < b < k + 1$. Thus, in particular, $2 \leq a \leq k$, and so by inductive hypothesis, a is divisible by a prime number p. In addition because $k + 1 = ab$, we have that $k + 1$ is divisible by a. Hence, since $k + 1$ is divisible by a and a is divisible by p, by transitivity of divisibility, $k + 1$ is divisible by the prime number p.

Therefore, regardless of whether $k + 1$ is prime or not, it is divisible by a prime number *[as was to be shown]*.

[Since we have proved both the basis and the inductive step of the strong mathematical induction, we conclude that the given statement is true.]

■

Both ordinary and strong mathematical induction can be used to show that the terms of certain sequences satisfy certain properties. The next example shows how this is done using strong induction.

Example 5.4.2 Proving a Property of a Sequence with Strong Induction

Define a sequence $s_0, s_1, s_2, \ldots$ as follows:

$$s_0 = 0, \quad s_1 = 4, \quad s_k = 6a_{k-1} - 5a_{k-2} \quad \text{for all integers } k \geq 2.$$

a. Find the first four terms of this sequence.

b. It is claimed that for each integer $n \geq 0$, the nth term of the sequence has the same value as that given by the formula $5^n - 1$. In other words, the claim is that all the terms of the sequence satisfy the equation $s_n = 5^n - 1$. Prove that this is true.

Solution

a. $s_0 = 0, \qquad s_1 = 4, \qquad s_2 = 6s_1 - 5s_0 = 6 \cdot 4 - 5 \cdot 0 = 24,$
$s_3 = 6s_2 - 5s_1 = 6 \cdot 24 - 5 \cdot 4 = 144 - 20 = 124$

b. To use strong mathematical induction to show that every term of the sequence satisfies the equation, the basis step must show that the first two terms satisfy it. This is necessary because, according to the definition of the sequence, computing values of later terms requires knowing the values of the *two* previous terms. So if the basis step only shows that the first term satisfies the equation, it would not be possible to use the inductive step to deduce that the second term satisfies the equation. In the inductive step you suppose that for an arbitrarily chosen integer $k \geq 1$, all the terms of the sequence from s_0 through s_k satisfy the given equation and you then deduce that s_{k+1} must also satisfy the equation.

Proof:

Let $s_0, s_1, s_2, \ldots$ be the sequence defined by specifying that $s_0 = 0$, $s_1 = 4$, and $s_k = 6a_{k-1} - 5a_{k-2}$ for all integers $k \geq 2$, and let the property $P(n)$ be the formula

$$s_n = 5^n - 1 \qquad \leftarrow P(n)$$

We will use strong mathematical induction to prove that for all integers $n \geq 0$, $P(n)$ is true.

Show that P*(0) *and P*(1) *are true:
To establish $P(0)$ and $P(1)$, we must show that

$$s_0 = 5^0 - 1 \quad \text{and} \quad s_1 = 5^1 - 1. \qquad \leftarrow P(0) \quad \text{and} \quad P(1)$$

But, by definition of $s_0, s_1, s_2, \ldots$, we have that $s_0 = 0$ and $s_1 = 4$. Since $5^0 - 1 = 1 - 1 = 0$ and $5^1 - 1 = 5 - 1 = 4$, the values of s_0 and s_1 agree with the values given by the formula.

Show that for all integers k* ≥ 1, *if P(i) is true for all integers i from* 0 *through k, then P(k* + 1*) is also true:
Let k be any integer with $k \geq 1$ and suppose that

$$s_i = 5^i - 1 \text{ for all integers } i \text{ with } 0 \leq i \leq k. \qquad \leftarrow \text{inductive hypothesis}$$

We must show that

$$s_{k+1} = 5^{k+1} - 1. \qquad \leftarrow P(k+1)$$

But since $k \geq 1$, we have that $k + 1 \geq 2$, and so

$$\begin{aligned}
s_{k+1} &= 6s_k - 5s_{k-1} && \text{by definition of } s_0, s_1, s_2, \ldots \\
&= 6(5^k - 1) - 5(5^{k-1} - 1) && \text{by definition hypothesis} \\
&= 6 \cdot 5^k - 6 - 5^k + 5 && \text{by multiplying out and applying} \\
& && \text{a law of exponents} \\
&= (6 - 1)5^k - 1 && \text{by factoring out 6 and arithmetic} \\
&= 5 \cdot 5^k - 1 && \text{by arithmetic} \\
&= 5^{k+1} - 1 && \text{by applying a law of exponents,}
\end{aligned}$$

[as was to be shown].

[Since we have proved both the basis and the inductive step of the strong mathematical induction, we conclude that the given statement is true.]

Another use of strong induction concerns the computation of products. A product of four numbers may be computed in a variety of different ways as indicated by the placement of parentheses. For instance,

> $((x_1x_2)x_3)x_4$ means multiply x_1 and x_2, multiply the result by x_3, and then multiply that number by x_4.

And

> $(x_1x_2)(x_3x_4)$ means multiply x_1 and x_2, multiply x_3 and x_4, and then take the product of the two.

Note that in both examples above, although the factors are multiplied in a different order, the number of multiplications—three—is the same. Strong mathematical induction is used to prove a generalization of this fact.

Note Like many definitions, for extreme cases this may look strange but it makes things work out nicely.

Convention

Let us agree to say that a single number x_1 is a product with one factor and can be computed with zero multiplications.

Example 5.4.3 The Number of Multiplications Needed to Multiply n Numbers

Prove that for any integer $n \geq 1$, if $x_1, x_2, \ldots, x_n$ are n numbers, then no matter how the parentheses are inserted into their product, the number of multiplications used to compute the product is $n - 1$.

Solution The truth of the basis step follows immediately from the convention about a product with one factor. The inductive step is based on the fact that when several numbers are multiplied together, each step of the process involves multiplying two individual quantities. For instance, the final step for computing $((x_1x_2)x_3)(x_4x_5)$ is to multiply $(x_1x_2)x_3$ and x_4x_5. In general, if $k + 1$ numbers are multiplied, the two quantities in the final step each consist of fewer than $k + 1$ factors. This is what makes it possible to use the inductive hypothesis.

Proof (by strong mathematical induction):

Let the property $P(n)$ be the sentence

> If $x_1, x_2, \ldots, x_n$ are n numbers, then no matter how parentheses are inserted into their product, the number of multiplications used to compute the product is $n - 1$. $\leftarrow P(n)$

Show that $P(1)$ is true:
To establish $P(1)$, we must show that

> The number of multiplications needed to compute the product of x_1 is $1 - 1$. $\leftarrow P(1)$

This is true because, by convention, x_1 is a product that can be computed with 0 multiplications, and $0 = 1 - 1$.

Show that for all integers $k \geq 1$, if $P(i)$ is true for all integers i from 1 through k, then $P(k+1)$ is also true:
Let k by any integer with $k \geq 1$ and suppose that

> For all integers i from 1 through k, if $x_1, x_2, \ldots, x_i$ are numbers, then no matter how parentheses are inserted into their product, the number of multiplications used to compute the product is $i - 1$. $\leftarrow$ inductive hypothesis

We must show that

> If $x_1, x_2, \ldots, x_{k+1}$ are $k + 1$ numbers, then no matter how parentheses are inserted into their product, the number of multiplications used to compute the product is $(k + 1) - 1 = k$. $\leftarrow P(k + 1)$

Consider a product of $k + 1$ factors: $x_1, x_2 \ldots, x_{k+1}$. When parentheses are inserted in order to compute the product, some multiplication is the final one and each of the two factors making up the final multiplication is a product of fewer than $k+1$ factors. Let L be the product of the left-hand factors and R be the product of the right-hand factors, and suppose that L is composed of l factors and R is composed of r factors. Then $l+r=k+1$, the total number of factors in the product, and

$$1 \le l \le k \quad \text{and} \quad 1 \le r \le k.$$

By inductive hypothesis, evaluating L takes $l-1$ multiplications and evaluating R takes $r-1$ multiplications. Because one final multiplication is needed to evaluate $L \cdot R$, the number of multiplications needed to evaluate the product of all $k+1$ factors is

$$(l-1)+(r-1)+1=(l+r)-1=(k+1)-1=k.$$

[This is what was to be shown.]
[Since we have proved the basis step and the inductive step of the strong mathematical induction, we conclude that the given statement is true.]

Strong mathematical induction makes possible a proof of the fact used frequently in computer science that every positive integer n has a unique binary integer representation. The proof looks complicated because of all the notation needed to write down the various steps. But the idea of the proof is simple. It is that if smaller integers than n have unique representations as sums of powers of 2, then the unique representation for n as a sum of powers of 2 can be found by taking the representation for $n/2$ (or for $(n-1)/2$ if n is odd) and multiplying it by 2.

Theorem 5.4.1 Existence and Uniqueness of Binary Integer Representations

Given any positive integer n, n has a unique representation in the form

$$n \;=\; c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0,$$

where r is a nonnegative integer, $c_r = 1$, and $c_j = 1$ or 0 for all $j = 0, 1, 2, \ldots, r-1$.

Proof:

We give separate proofs by strong mathematical induction to show first the existence and second the uniqueness of the binary representation.

Existence (proof by strong mathematical induction): Let the property $P(n)$ be the equation

$$n \;=\; c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0, \qquad \leftarrow P(n)$$

where r is a nonnegative integer, $c_r = 1$, and $c_j = 1$ or 0 for all $j = 0, 1, 2, \ldots, r-1$.

Show that $P(1)$ is true:
Let $r=0$ and $c_0=1$. Then $1 = c_r \cdot 2^r$, and so $n=1$ can be written in the required form.

Show that for all integers $k \ge 1$, if $P(i)$ is true for all integers i from 1 through k, then $P(k+1)$ is also true:

continued on page 274

Let k be an integer with $k \geq 1$. Suppose that for all integers i from 1 through k,

$$i = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0, \qquad \leftarrow \text{inductive hypothesis}$$

where r is a nonnegative integer, $c_r = 1$, and $c_j = 1$ or 0 for all $j = 0, 1, 2, \ldots, r-1$. We must show that $k+1$ can be written as a sum of powers of 2 in the required form.

Case 1 ($k + 1$ is even): In this case $(k+1)/2$ is an integer, and by inductive hypothesis, since $1 \leq (k+1)/2 \leq k$, then,

$$\frac{k+1}{2} = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0,$$

where r is a nonnegative integer, $c_r = 1$, and $c_j = 1$ or 0 for all $j = 0, 1, 2, \ldots, r-1$. Multiplying both sides of the equation by 2 gives

$$k+1 = c_r \cdot 2^{r+1} + c_{r-1} \cdot 2^r + \cdots + c_2 \cdot 2^3 + c_1 \cdot 2^2 + c_0 \cdot 2,$$

which is a sum of powers of 2 of the required form.

Case 2 ($k + 1$ is odd): In this case $k/2$ is an integer, and by inductive hypothesis, since $1 \leq k/2 \leq k$, then

$$\frac{k}{2} = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0,$$

where r is a nonnegative integer, $c_r = 1$, and $c_j = 1$ or 0 for all $j = 0, 1, 2, \ldots, r-1$. Multiplying both sides of the equation by 2 and adding 1 gives

$$k+1 = c_r \cdot 2^{r+1} + c_{r-1} \cdot 2^r + \cdots + c_2 \cdot 2^3 + c_1 \cdot 2^2 + c_0 \cdot 2 + 1,$$

which is also a sum of powers of 2 of the required form.

The preceding arguments show that regardless of whether $k+1$ is even or odd, $k+1$ has a representation of the required form. *[Or, in other words, $P(k+1)$ is true as was to be shown.]*

[Since we have proved the basis step and the inductive step of the strong mathematical induction, the existence half of the theorem is true.]

***Uniqueness*:** To prove uniqueness, suppose that there is an integer n with two different representations as a sum of nonnegative integer powers of 2. Equating the two representations and canceling all identical terms gives

$$2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_1 \cdot 2 + c_0 = 2^s + d_{s-1} \cdot 2^{s-1} + \cdots + d_1 \cdot 2 + d_0 \qquad 5.4.1$$

where r and s are nonnegative integers, and each c_i and each d_i equal 0 or 1. Without loss of generality, we may assume that $r < s$. But by the formula for the sum of a geometric sequence (Theorem 5.2.3) and because $r < s$,

$$\begin{aligned} 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_1 \cdot 2 + c_0 \leq 2^r + 2^{r-1} + \cdots + 2 + 1 &= 2^{r+1} - 1 \\ &< 2^s. \end{aligned}$$

Thus

$$2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_1 \cdot 2 + c_0 < 2^s + d_{s-1} \cdot 2^{s-1} + \cdots + d_1 \cdot 2 + d_0,$$

which contradicts equation (5.4.1). Hence the supposition is false, so any integer n has only one representation as a sum of nonnegative integer powers of 2.

The Well-Ordering Principle for the Integers

The well-ordering principle for the integers looks very different from both the ordinary and the strong principles of mathematical induction, but it can be shown that all three principles are equivalent. That is, if any one of the three is true, then so are both of the others.

Well-Ordering Principle for the Integers

Let S be a set of integers containing one or more integers all of which are greater than some fixed integer. Then S has a least element.

Note that when the context makes the reference clear, we will write simply "the well-ordering principle" rather than "the well-ordering principle for the integers."

Example 5.4.4 Finding Least Elements

In each case, if the set has a least element, state what it is. If not, explain why the well-ordering principle is not violated.

a. The set of all positive real numbers.

b. The set of all nonnegative integers n such that $n^2 < n$.

c. The set of all nonnegative integers of the form $46 - 7k$, where k is an integer.

Solution

a. There is no least positive real number. For if x is any positive real number, then $x/2$ is a positive real number that is less than x. No violation of the well-ordering principle occurs because the well-ordering principle refers only to sets of integers, and this set is not a set of integers.

b. There is no *least* nonnegative integer n such that $n^2 < n$ because there is *no* nonnegative integer that satisfies this inequality. The well-ordering principle is not violated because the well-ordering principle refers only to sets that contain at least one element.

c. The following table shows values of $46 - 7k$ for various values of k.

k	0	1	2	3	4	5	6	7	$\cdots$	-1	-2	-3	$\cdots$
$46 - 7k$	46	39	32	25	18	11	4	-3	$\cdots$	53	60	67	$\cdots$

The table suggests, and you can easily confirm, that $46 - 7k < 0$ for $k \geq 7$ and that $46 - 7k \geq 46$ for $k \leq 0$. Therefore, from the other values in the table it is clear that 4 is the least nonnegative integer of the form $46 - 7k$. This corresponds to $k = 6$. ■

Another way to look at the analysis of Example 5.4.4(c) is to observe that subtracting six 7's from 46 leaves 4 left over and this is the least nonnegative integer obtained by repeated subtraction of 7's from 46. In other words, 6 is the quotient and 4 is the remainder for the division of 46 by 7. More generally, in the division of any integer n by any positive integer d, the remainder r is the least nonnegative integer of the form $n - dk$. This is the heart of the following proof of the existence part of the quotient-remainder theorem (the part that guarantees the existence of a quotient and a remainder of the division of an integer by a positive integer). For a proof of the uniqueness of the quotient and remainder, see exercise 18 of Section 4.6.

Quotient-Remainder Theorem (Existence Part)

Given any integer n and any positive integer d, there exist integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \le r < d.$$

Proof:

Let S be the set of all nonnegative integers of the form

$$n - dk,$$

where k is an integer. This set has at least one element. *[For if n is nonnegative, then*

$$n - 0 \cdot d = n \ge 0,$$

and so $n - 0 \cdot d$ is in S. And if n is negative, then

$$n - nd = \underset{<0}{n}\underbrace{(1-d)}_{\le 0 \text{ since } d \text{ is a positive integer}} \ge 0,$$

and so $n - nd$ is in S.] It follows by the well-ordering principle for the integers that S contains a least element r. Then, for some specific integer $k = q$,

$$n - dq = r$$

[because every integer in S can be written in this form]. Adding dq to both sides gives

$$n = dq + r.$$

Furthermore, $r < d$. *[For suppose $r \ge d$. Then*

$$n - d(q+1) = n - dq - d = r - d \ge 0,$$

and so $n - d(q+1)$ would be a nonnegative integer in S that would be smaller than r. But r is the smallest integer in S. This contradiction shows that the supposition $r \ge d$ must be false.] The preceding arguments prove that there exist integers r and q for which

$$n = dq + r \quad \text{and} \quad 0 \le r < d.$$

[This is what was to be shown.]

Another consequence of the well-ordering principle is the fact that any strictly decreasing sequence of nonnegative integers is finite. That is, if $r_1, r_2, r_3, \ldots$ is a sequence of nonnegative integers satisfying

$$r_i > r_{i+1}$$

for all $i \ge 1$, then $r_1, r_2, r_3, \ldots$ is a finite sequence. *[For by the well-ordering principle such a sequence would have to have a least element r_k. It follows that r_k must be the final term of the sequence because if there were a term r_{k+1}, then since the sequence is strictly decreasing, $r_{k+1} < r_k$, which would be a contradiction.]* This fact is frequently used in computer science to prove that algorithms terminate after a finite number of steps.

Test Yourself

1. In a proof by strong mathematical induction the basis step may require checking a property $P(n)$ for more _____ value of n.

2. Suppose that in the basis step for a proof by strong mathematical induction the property $P(n)$ was checked for all integers n from a through b. Then in the inductive step one assumes that for any integer $k \geq b$, the property $P(n)$ is true for all values of i from _____ through _____ and one shows that _____ is true.

3. According to the well-ordering principle for the integers, if a set S of integers contains at least _____ and if there is some integer that is less than or equal to every _____, then _____.

Exercise Set 5.4

1. Suppose $a_1, a_2, a_3, \ldots$ is a sequence defined as follows:

$$a_1 = 1, \; a_2 = 3,$$
$$a_k = a_{k-2} + 2a_{k-1} \quad \text{for all integers } k \geq 3.$$

Prove that a_n is odd for all integers $n \geq 1$.

2. Suppose $b_1, b_2, b_3, \ldots$ is a sequence defined as follows:

$$b_1 = 4, \; b_2 = 12$$
$$b_k = b_{k-2} + b_{k-1} \quad \text{for all integers } k \geq 3.$$

Prove that b_n is divisible by 4 for all integers $n \geq 1$.

3. Suppose that $c_0, c_1, c_2, \ldots$ is a sequence defined as follows:

$$c_0 = 2, \; c_1 = 2, \; c_2 = 6,$$
$$c_k = 3c_{k-3} \quad \text{for all integers } k \geq 3.$$

Prove that c_n is even for all integers $n \geq 0$.

4. Suppose that $d_1, d_2, d_3, \ldots$ is a sequence defined as follows:

$$d_1 = \frac{9}{10}, \; d_2 = \frac{10}{11},$$
$$d_k = d_{k-1} \cdot d_{k-2} \quad \text{for all integers } k \geq 3.$$

Prove that $0 < d_n \leq 1$ for all integers $n \geq 0$.

5. Suppose that $e_0, e_1, e_2, \ldots$ is a sequence defined as follows:

$$e_0 = 12, \; e_1 = 29$$
$$e_k = 5e_{k-1} - 6e_{k-2} \quad \text{for all integers } k \geq 2.$$

Prove that $e_n = 5 \cdot 3^n + 7 \cdot 2^n$ for all integers $n \geq 0$.

6. Suppose that $f_0, f_1, f_2, \ldots$ is a sequence defined as follows:

$$f_0 = 5, \; f_1 = 16$$
$$f_k = 7f_{k-1} - 10f_{k-2} \quad \text{for all integers } k \geq 2.$$

Prove that $f_n = 3 \cdot 2^n + 2 \cdot 5^n$ for all integers $n \geq 0$.

7. Suppose that $g_1, g_2, g_3, \ldots$ is a sequence defined as follows:

$$g_1 = 3, \; g_2 = 5$$
$$g_k = 3g_{k-1} - 2g_{k-2} \quad \text{for all integers } k \geq 3.$$

Prove that $g_n = 2^n + 1$ for all integers $n \geq 1$.

8. Suppose that $h_0, h_1, h_2, \ldots$ is a sequence defined as follows:

$$h_0 = 1, \; h_1 = 2, \; h_2 = 3,$$
$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \quad \text{for all integers } k \geq 3.$$

a. Prove that $h_n \leq 3^n$ for all integers $n \geq 0$.
b. Suppose that s is any real number such that $s^3 \geq s^2 + s + 1$. (This implies that $s > 1.83$.) Prove that $h_n \leq s^n$ for all $n \geq 2$.

9. Define a sequence $a_1, a_2, a_3, \ldots$ as follows: $a_1 = 1, a_2 = 3$, and $a_k = a_{k-1} + a_{k-2}$ for all integers $k \geq 3$. (This sequence is known as the Lucas sequence.) Use strong mathematical induction to prove that $a_n \leq \left(\frac{7}{4}\right)^n$ for all integers $n \geq 1$.

H **10.** The problem that was used to introduce ordinary mathematical induction in Section 5.2 can also be solved using strong mathematical induction. Let $P(n)$ be "any collection of n coins can be obtained using a combination of 3¢ and 5¢ coins." Use strong mathematical induction to prove that $P(n)$ is true for all integers $n \geq 14$.

11. You begin solving a jigsaw puzzle by finding two pieces that match and fitting them together. Each subsequent step of the solution consists of fitting together two blocks made up of one or more pieces that have previously been assembled. Use strong mathematical induction to prove that the number of steps required to put together all n pieces of a jigsaw puzzle is $n - 1$.

H **12.** The sides of a circular track contain a sequence of cans of gasoline. The total amount in the cans is sufficient to enable a certain car to make one complete circuit of the track, and it could all fit into the car's gas tank at one time. Use mathematical induction to prove that it is possible to find an initial location for placing the car so that it will be able to traverse the entire track by using the various amounts of gasoline in the cans that it encounters along the way.

H **13.** Use strong mathematical induction to prove the existence part of the unique factorization of integers (Theorem 4.3.5): Every integer greater than 1 is either a prime number or a product of prime numbers.

14. Any product of two or more integers is a result of successive multiplications of two integers at a time. For instance, here are a few of the ways in which $a_1a_2a_3a_4$ might be computed: $(a_1a_2)(a_3a_4)$ or $((a_1a_2)a_3)a_4)$ or $a_1((a_2a_3)a_4)$. Use strong mathematical induction to prove that any product of two or more odd integers is odd.

15. Any sum of two or more integers is a result of successive additions of two integers at a time. For instance, here are a few of the ways in which $a_1 + a_2 + a_3 + a_4$ might be computed: $(a_1 + a_2) + (a_3 + a_4)$ or $((a_1 + a_2) + a_3) + a_4)$ or $a_1 + ((a_2 + a_3) + a_4)$. Use strong mathematical induction to prove that any sum of two or more even integers is even.

H **16.** Use strong mathematical induction to prove that for any integer $n \geq 2$, if n is even, then any sum of n odd integers is even, and if n is odd, then any sum of n odd integers is odd.

17. Compute $4^1, 4^2, 4^3, 4^4, 4^5, 4^6, 4^7$, and 4^8. Make a conjecture about the units digit of 4^n where n is a positive integer. Use strong mathematical induction to prove your conjecture.

18. Compute $9^0, 9^1, 9^2, 9^3, 9^4$, and 9^5. Make a conjecture about the units digit of 9^n where n is a positive integer. Use strong mathematical induction to prove your conjecture.

19. Find the mistake in the following "proof" that purports to show that every nonnegative integer power of every nonzero real number is 1.

"**Proof:** Let r be any nonzero real number and let the property $P(n)$ be the equation $r^n = 1$.

Show that P(0) is true: $P(0)$ is true because $r^0 = 1$ by definition of zeroth power.

Show that for all integers k ≥ 0, if P(i) is true for all integers i from 0 through k, then P(k + 1) is also true: Let k be any integer with $k \geq 0$ and suppose that $r^i = 1$ for all integers i from 0 through k. This is the inductive hypothesis. We must show that $r^{k+1} = 1$. Now

$$\begin{aligned}
r^{k+1} &= r^{k+k-(k-1)} && \text{because } k + k - (k-1) = k + k - k + 1 = k + 1 \\
&= \frac{r^k \cdot r^k}{r^{k-1}} && \text{by the laws of exponents} \\
&= \frac{1 \cdot 1}{1} && \text{by inductive hypothesis} \\
&= 1.
\end{aligned}$$

Thus $r^{k+1} = 1$ *[as was to be shown].*

[Since we have proved the basis step and the inductive step of the strong mathematical induction, we conclude that the given statement is true.]"

20. Use the well-ordering principle for the integers to prove Theorem 4.3.4: Every integer greater than 1 is divisible by a prime number.

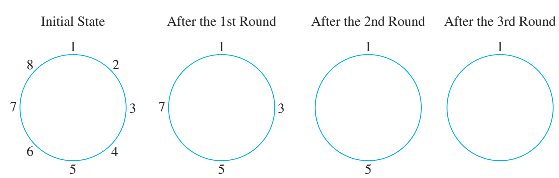
21. Use the well-ordering principle for the integers to prove the existence part of the unique factorization of integers theorem: Every integer greater than 1 is either prime or a product of prime numbers.

22. **a.** The Archimedean property for the rational numbers states that for all rational numbers r, there is an integer n such that $n > r$. Prove this property.
b. Prove that given any rational number r, the number $-r$ is also rational.
c. Use the results of parts (a) and (b) to prove that given any rational number r, there is an integer m such that $m < r$.

H **23.** Use the results of exercise 22 and the well-ordering principle for the integers to show that given any rational number r, there is an integer m such that $m \leq r < m + 1$.

24. Use the well-ordering principle to prove that given any integer $n \geq 1$, there exists an odd integer m and a nonnegative integer k such that $n = 2^k \cdot m$.

25. Imagine a situation in which eight people, numbered consecutively 1–8, are arranged in a circle. Starting from person #1, every second person in the circle is eliminated. The elimination process continues until only one person remains. In the first round the people numbered 2, 4, 6, and 8 are eliminated, in the second round the people numbered 3 and 7 are eliminated, and in the third round person #5 is eliminated. So after the third round only person #1 remains, as shown below.



a. Given a set of sixteen people arranged in a circle and numbered, consecutively 1–16, list the numbers of the people who are eliminated in each round if every second person is eliminated and the elimination process continues until only one person remains. Assume that the starting point is person #1.
b. Use mathematical induction to prove that for all integers $n \geq 1$, given any set of 2^n people arranged in a circle and numbered consecutively 1 through 2^n, if one starts from person #1 and goes repeatedly around the circle successively eliminating every second person, eventually only person #1 will remain.
c. Use the result of part (b) to prove that for any nonnegative integers n and m with $2^n \leq 2^n + m < 2^{n+1}$, if $r = 2^n + m$, then given any set of r people arranged in a circle and numbered consecutively 1 through r, if one starts from person #1 and goes repeatedly around the circle successively eliminating every second person, eventually only person #$(2m + 1)$ will remain.

26. Suppose $P(n)$ is a property such that
    1. $P(0)$, $P(1)$, $P(2)$ are all true,
    2. for all integers $k \geq 0$, if $P(k)$ is true, then $P(3k)$ is true.

    Must it follow that $P(n)$ is true for all integers $n \geq 0$? If yes, explain why; if no, give a counterexample.

27. Prove that if a statement can be proved by strong mathematical induction, then it can be proved by ordinary mathematical induction. To do this, let $P(n)$ be a property that is defined for integers n, and suppose the following two statements are true:
    1. $P(a)$, $P(a+1)$, $P(a+2)$, $\ldots$, $P(b)$.
    2. For any integer $k \geq b$, if $P(i)$ is true for all integers i from a through k, then $P(k+1)$ is true.

    The principle of strong mathematical induction would allow us to conclude immediately that $P(n)$ is true for all integers $n \geq a$. Can we reach the same conclusion using the principle of ordinary mathematical induction? Yes! To see this, let $Q(n)$ be the property

    $$P(j) \text{ is true for all integers } j \text{ with } a \leq j \leq n.$$

    Then use ordinary mathematical induction to show that $Q(n)$ is true for all integers $n \geq b$. That is, prove
    1. $Q(b)$ is true.
    2. For any integer $k \geq b$, if $Q(k)$ is true then $Q(k+1)$ is true.

28. Give examples to illustrate the proof of Theorem 5.4.1.

H 29. It is a fact that every integer $n \geq 1$ can be written in the form

$$c_r \cdot 3^r + c_{r-1} \cdot 3^{r-1} + \cdots + c_2 \cdot 3^2 + c_1 \cdot 3 + c_0,$$

where $c_r = 1$ or 2 and $c_i = 0, 1,$ or 2 for all integers $i = 0, 1, 2, \ldots, r-1$. Sketch a proof of this fact.

H✶30. Use mathematical induction to prove the existence part of the quotient-remainder theorem for integers $n \geq 0$.

H✶31. Prove that if a statement can be proved by ordinary mathematical induction, then it can be proved by the well-ordering principle.

H 32. Use the principle of ordinary mathematical induction to prove the well-ordering principle for the integers.

Answers for Test Yourself

1. than one 2. a; k; $P(k+1)$ 3. one integer; integer in S; S contains a least element

5.5 Application: Correctness of Algorithms

[P]rogramming reliably—must be an activity of an undeniably mathematical nature . . . . You see, mathematics is about thinking, and doing mathematics is always trying to think as well as possible. — Edsger W. Dijkstra (1981)

The University of Texas at Austin

Edsger W. Dijkstra (1930–2002)

What does it mean for a computer program to be correct? Each program is designed to do a specific task—calculate the mean or median of a set of numbers, compute the size of the paychecks for a company payroll, rearrange names in alphabetical order, and so forth. We will say that a program is correct if it produces the output specified in its accompanying documentation for each set of input data of the type specified in the documentation.*

Most computer programmers write their programs using a combination of logical analysis and trial and error. In order to get a program to run at all, the programmer must first fix all syntax errors (such as writing **ik** instead of **if,** failing to declare a variable, or using a restricted keyword for a variable name). When the syntax errors have been removed, however, the program may still contain logical errors that prevent it from producing correct output. Frequently, programs are tested using sets of sample data for which the correct output is known in advance. And often the sample data are deliberately chosen to test the correctness of the program under extreme circumstances. But for most programs the number of possible sets of input data is either infinite or unmanageably large, and so no amount of program testing can give perfect confidence that the program will be correct for all possible sets of legal input data.

*Consumers of computer programs want an even more stringent definition of correctness. If a user puts in data of the wrong type, the user wants a decent error message, not a system crash.