Chapter 18
Mathematical Induction

Suppose that you want to show something is true for all positive integers. You could start by checking that the statement is true for $n = 1$, $n = 2$, and so on, but you would have to stop somewhere. Even if you check lots and lots of integers, you can run into problems. Consider the following:

Let us suppose that you are asked to prove that $n^2 + n + 41$ is prime for every positive integer n. You might think the following is good enough to convince someone: if $f(n) = n^2 + n + 41$, then $f(1) = 43$ (which is prime), $f(2) = 47$ (which is prime), $f(3) = 53$ (prime too), and so on. In fact, checking the first 39 integers reveals that $f(n)$ is indeed prime for $n = 1, \ldots, 39$. Is this enough evidence to prove that it is true for all positive integers n? Check $n = 40$: $f(40) = 1681$, which is divisible by 41. What's the moral of this story? That examples, even many, many examples, are not a method of proof. It can help us find counterexamples or it can motivate us to formulate a conjecture, but unless we can check every single case, it will never prove anything.

One mathematical technique to prove that a statement holds for all positive integers is to show that the statement is true for $n = 1$ and that whenever it is true for a positive integer n, it is true for the next positive integer $n + 1$. Then, since you have shown it is true for $n = 1$, it must be true for $n = 2$ (because it's always true for a successor). Now that the statement is true for $n = 2$, it has to be true for $n = 3$, because 3 is the integer after 2, and so on. This is called mathematical induction, and a more precise description of this method of proof is given below.

This method is sometimes compared to lining up dominoes and making them fall down (see H. Steinhaus [102]). What has to happen? The first one has to fall, and every time one falls the one after it must fall. Once this happens, all the dominoes do fall down.

Theorem 18.1 (Principle of mathematical induction). *For an integer n, let $P(n)$ denote an assertion. Suppose that*

(i) (The base step) $P(1)$ is true, and
(ii) (The induction step) for all positive integers n, if $P(n)$ is true, then $P(n+1)$ is true.

U. Daepp and P. Gorkin, *Reading, Writing, and Proving: A Closer Look at Mathematics*, Undergraduate Texts in Mathematics, DOI 10.1007/978-1-4419-9479-0_18,

Then $P(n)$ holds for all positive integers n.

The principle of mathematical induction is a direct consequence of the well-ordering principle of $\mathbb{N}$ we came across in Chapter 12. The proof of Theorem 18.1 will be by contradiction: were the induction principle false, then we could construct a nonempty subset of the natural numbers that would not have a minimum—a contradiction to the well-ordering principle. This is the main idea in the proof that follows.

Proof. Suppose the induction principle were false. Then there would exist an assertion P that would satisfy conditions (i) and (ii) of the theorem, but $P(n)$ would be false for some $n \in \mathbb{Z}^+$. So let $A = \{k \in \mathbb{Z}^+ : P(k) \text{ is false}\}$. Our supposition implies that A is nonempty. By the well-ordering principle [p. 125], the set A has a minimum. Let m denote this minimum. By condition (i), $m \neq 1$. Since $m \in \mathbb{Z}^+$, it follows that $m \geq 2$. Consider the integer $n = m-1 \geq 1$. Since $n < m$ and m is the minimum of A, we know that $n \notin A$. Thus $P(n)$ is true. By condition (ii), $P(n+1)$ is true too. But $P(n+1) = P(m)$, so $P(m)$ must also be true, a contradiction. □

Students often mistakenly believe condition (ii) says that $P(n)$ is true, and ask why we would state it again as a conclusion. Look carefully at condition (ii). Note that it is an implication. We are *not* saying that $P(n)$ is true. We *are* saying that *if* $P(n)$ is true, then $P(n+1)$ is true. The antecedent in this implication is called the induction hypothesis.

The next example is one that is associated with Carl Friedrich Gauss. As one version of the story goes, when Gauss was 10 years old, his teacher, Herr Büttner, asked the students to sum the integers from 1 to 100. Gauss did it almost instantly. It is believed that he did it by the following method.

Write the sum horizontally forwards and backwards as:

$$1 + \ \ 2 + \ \ 3 + \cdots + 99 + 100$$

$$100 + 99 + 98 + \cdots + \ \ 2 + \ \ 1.$$

Now add vertically. When you do this, you will get 101 one hundred times; in other words, you get $(101)(100)$. This is twice the sum that you needed, so the answer must be $(101)(100)/2$. There is nothing special about the integer 100. If you try this with a general positive integer n, you will see that $1+2+3+\cdots+n = n(n+1)/2$ for every positive integer n. What a nice formula! You will give it a rigorous proof using mathematical induction when you work Problem 18.1. Is something like this formula true for the sums of squares of the first n integers? Indeed it is.

Example 18.2. Using mathematical induction, show that

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

for every positive integer n.

Proof. Let $P(n)$ be the assertion that

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

First we check the base step: $P(1)$ is the statement that $1=(1(1+1)(2+1))/6$, and this is certainly true.

Now we verify the induction step. Let $n\in\mathbb{Z}^+$ and suppose $P(n)$ holds. Thus we suppose that for an $n\in\mathbb{Z}^+$ we have

$$1^2+2^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}. \tag{18.1}$$

We wish to show that $P(n+1)$ holds; that is, that

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

We start by grouping the left side of $P(n+1)$ and then simplify as follows:

$$\begin{aligned}
&1^2+2^2+\cdots+n^2+(n+1)^2\\
&=\left(1^2+2^2+\cdots+n^2\right)+(n+1)^2\\
&=\frac{n(n+1)(2n+1)}{6}+(n+1)^2 \quad \text{(by our induction hypothesis (18.1))}\\
&=(n+1)\left(\frac{n(2n+1)}{6}+(n+1)\right) \quad \text{(factor out } n+1\text{)}\\
&=(n+1)\left(\frac{2n^2+7n+6}{6}\right)\\
&=(n+1)\frac{(n+2)(2n+3)}{6}\\
&=\frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}.
\end{aligned}$$

By mathematical induction we conclude that the assertion holds for all positive integers. □

Induction proofs must contain certain steps. Look at the proof above and see if you can find each of the steps described below.

(1) You should indicate clearly what you are trying to prove. (2) There is always the base step, in which we check the first assertion. (This need not always begin with $n=1$; it can begin with $n=3$, $n=0$, or even at a negative integer! In fact, as long as what you say is true, it can begin at any integer you want it to begin at.) (3) Then we have the induction step, in which we show that for each $n\in\mathbb{Z}$ that is at least as big as the integer used in the base step, if $P(n)$ is true, then $P(n+1)$ is true.

Of course, you still need to write using complete sentences, and you still need to introduce every variable to the reader when the reader meets it (not after the reader has met it for the first time!). Finally, do tell the reader what the base step is ("First we show the assertion holds for $n = 1$"), what the induction step is ("We suppose that $P(n)$ holds for an $n \in \mathbb{Z}^+$; that is ... holds"), and what you will prove ("We will show that $P(n+1)$ holds; that is ... holds"). This is as much for your benefit as it is for the reader's. This step shows you where you will begin and where you will have to end. Then show what you said you will show and indicate clearly where you use the induction hypothesis. End your proof with a concluding sentence.

Many statements proved by induction involve sums or products. We remind you of the standard notation for this. In the following, $k \in \mathbb{Z}$ and $a_k \in \mathbb{R}$. The notation for sum is

$$a_1 + a_2 + a_3 + \cdots + a_n = \sum_{k=1}^{n} a_k\,,$$

and the notation for product is

$$a_1 \cdot a_2 \cdot a_3 \cdot \cdots \cdot a_n = \prod_{k=1}^{n} a_k\,.$$

This notation often saves space and makes a statement look neater. For instance, the result we proved in Example 18.2 is

$$\text{For } n \in \mathbb{Z}^+, \text{ we have } \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

If you are ever unsure about what such a statement says, you will almost certainly find it helpful to rewrite the expression the long way.

Exercise 18.3. Let $x_1, x_2, \ldots, x_n$ be real numbers. Prove that for $n \in \mathbb{Z}^+$, both of the following hold:

(a) $|\prod_{k=1}^{n} x_k| = \prod_{k=1}^{n} |x_k|$ and
(b) $|\sum_{k=1}^{n} x_k| \leq \sum_{k=1}^{n} |x_k|$. ○

The following exercise illustrates how induction can go awry. It's cute, but not very mathematical. A similar example, but a more mathematical one, appears in the problems. See if you can spot the error in that one.

Exercise 18.4. All people at Bucknell University have the same color hair.

Not a proof. Let $P(n)$ be the assertion that every group of n people has the same color hair (as each other). Then $P(1)$ is the statement that one person has the same color hair as herself. This is certainly true. So let $n \in \mathbb{Z}^+$ and suppose that $P(n)$ is true; that is, when we have n people, they all have the same color hair. We need to show that this implies that $n+1$ people in a group have the same color hair. So consider a group of $n+1$ people. If we look at the first n of them (people 1 through n in the group), by the induction hypothesis they all have the same color hair, which we may as well assume is black for right now. So the first n people all have black

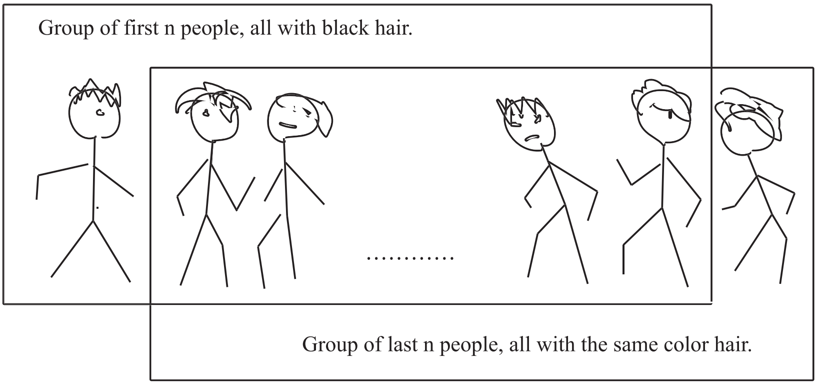
Group of first n people, all with black hair.
....
Group of last n people, all with the same color hair.

Fig. 18.1 They must all have black hair

hair. Now consider the last n people in this group (people 2 through $n+1$ in the group). Again, by our induction hypothesis, they all have the same color hair. Those who are in both groups are also in the first group, and therefore have black hair. (See Figure 18.1.) Thus, since all people in the second group have the same color hair, everyone has black hair. By mathematical induction we conclude that all people at Bucknell have the same color hair. What a boring campus. □

There must be an error! Exactly where is it? ○

Exercise 18.5. Use induction to prove that for all natural numbers n, the expression $4^n - 1$ is a multiple of 3.

"Understanding the problem." Well, once again, it's probably a good idea to make sure that we know what everything means here. We need to show that $4^n - 1$ is a multiple of 3 for every natural number n. That means we need to show that there exists an integer k such that $4^n - 1 = 3k$.

"Devising a plan." The outline is presented to you below and the complete solution appears at the end of the chapter.

1. Say clearly what the assertion $P(n)$ is. (Most mathematicians write this out without labeling the assertion with $P(n)$ explicitly.)
2. Check the base step ($n = 0$).
3. Write out the induction step in the principle of mathematical induction clearly. Make sure you replace $P(n)$ by what it says, and replace $P(n+1)$ by what it says. This will help you figure out what you are supposing (you are supposing $P(n)$) and what you need to end with (you need to end with $P(n+1)$).
4. Write out the induction hypothesis; that is, write out what you are assuming to be true.
5. Having done all of the above, look at $4^{n+1} - 1$ and show that it is divisible by 3. Indicate clearly where you use the induction hypothesis.
6. State your conclusion clearly. ○

Induction can also be used to define functions. Perhaps the best known example of this technique is the definition of factorial: For $n \in \mathbb{N}$, we define n **factorial**, written as $n!$, as follows:

$$\begin{aligned} 0! &= 1 \\ (n+1)! &= (n+1) \cdot n! \text{ for } n \geq 0. \end{aligned}$$

What have we done? We defined a function $g : \mathbb{N} \to \mathbb{N}$, denoted $g(n) = n!$, by telling you that $g(0) = 1,\ g(1) = 1 \cdot g(0) = 1,\ g(2) = 2 \cdot g(1) = 2, g(3) = 3 \cdot g(2) = 6$, etc.

You might be thinking, "They say they've defined a function. Is it really well-defined?" If this is what you are, in fact, thinking, that's great. To prove that g is a function, we'll actually need a theorem. This theorem is often called the recursion theorem.

Theorem 18.6 (Recursion theorem). *Let X be a nonempty set, $f : X \to X$ a function, and $a \in X$. Then there is a unique function $g : \mathbb{N} \to X$ such that $g(0) = a$ and $g(n+1) = f(g(n))$ for all $n \in \mathbb{N}$.*

We usually begin by understanding the problem. In this case, understanding the theorem might also require some effort. What does it say? To define g, we say how to get started (that's what we are doing when we tell you $g(0) = a$). But that's only how you get started. To proceed from your starting point, we tell you how to compute $g(n+1)$. You have a rule (that's f) and the previous values of g (that's where $g(n)$ comes into play) and you compose them (that's $g(n+1) = f(g(n))$). And what we are saying is that this g that you get is a well-defined function.

"Understanding the problem" There are two parts to this proof. We will need to show that a function g exists and that at most one function g exists. If we can figure out how to show the function exists, we will try to show that uniqueness follows the way it often does. So, how can you show that something you don't have exists? Any function we define has to be a relation satisfying the conditions stated. But, on top of the conditions, we also want to obtain uniqueness. We will fall back on the definition of function as a relation and we'll try to find the smallest relation that does what we need. Being the smallest should make it unique, if we are lucky. Whatever object we end up constructing will also need to satisfy conditions (i) and (ii) of the definition of function. It might, at this point, be advisable to review our original function definition, Definition 14.1.

"Devising a plan." For the existence, we've decided that the smallest relation has a chance at satisfying the conditions. So we want a "small set" that "does certain things." Getting a small set suggests intersecting things that do what we want. So we will look at all relations from $\mathbb{N}$ to X; that is, all subsets A of $\mathbb{N} \times X$, with the property that $(0,a) \in A$ and whenever $(n,x) \in A$, then $(n+1, f(x)) \in A$. If we can show that there is at least one such relation, then we'll take the intersection of all of them and show that this is our function g.

To show uniqueness we will suppose that there is a second function h satisfying our needs and we will try to contradict something, most likely the minimal nature of g. Let us see whether we can turn this plan into a successful proof.

As you read this proof, you'll notice that the set $\mathscr{C}$ that we define comes up a lot. So you should write down, in some very handy place, what you have to do to get into the set $\mathscr{C}$.

Proof. We will first show that there exists a function $g : \mathbb{N} \to X$ satisfying the stated conditions. We let $\mathscr{C}$ be the set of all subsets A of $\mathbb{N} \times X$ with the condition that $(0,a) \in A$ and whenever $(n,x) \in A$, then $(n+1, f(x)) \in A$. Since $\mathbb{N} \times X \in \mathscr{C}$ we see that $\mathscr{C} \neq \emptyset$. Consequently, we can form the intersection of all elements of $\mathscr{C}$, which we call g. So $g = \bigcap_{A \in \mathscr{C}} A$. Obviously $g \subseteq \mathbb{N} \times X$. Since $(0,a) \in A$ for all $A \in \mathscr{C}$ we also have $(0,a) \in g$. If $(n,x) \in g$, then $(n,x) \in A$ for all $A \in \mathscr{C}$. This implies that $(n+1, f(x)) \in A$ for all $A \in \mathscr{C}$. Hence $(n+1, f(x)) \in g$. This shows that $g \in \mathscr{C}$ and g is a relation from $\mathbb{N}$ to X. We claim that, in fact, $g : \mathbb{N} \to X$ is a function. Since the domain and codomain are specified, we need only show that the two conditions of the function definition hold.

For condition (i) of the function definition we need to show that for each $n \in \mathbb{N}$ there exists $x \in X$ such that $(n,x) \in g$. We will prove this by induction on n. First the base step: Because $g \in \mathscr{C}$, we know that $(0,a) \in g$ where $a \in X$.

For the induction step, let $n \in \mathbb{N}$ and suppose that $(n,x) \in g$. Since $x \in X$, we know that $f(x) \in X$. Thus, since $g \in \mathscr{C}$ we conclude that $(n+1, f(x)) \in g$. So for $n+1$, the element $f(x)$ is the element of X that we were looking for; that is, by induction, we know that for each $n \in \mathbb{N}$ there exists $x \in X$ such that $(n,x) \in g$ and we conclude that condition (i) of the function definition holds.

For condition (ii), we need to show that for each $n \in \mathbb{N}$ if (n,x) and (n,y) are elements of g, then $x = y$. We will show this, again, by induction on n. For the base step, we have $(0,a) \in g$. Suppose that $(0,y) \in g$ with $y \neq a$. Define $h_1 = g \setminus \{(0,y)\}$. Then $h_1 \subset g$. Clearly, $(0,a) \in h_1$ since we haven't removed it from g. If for some $n \in \mathbb{N}$ we have $(n,x) \in h_1$, then the fact that $h_1 \subset g$ implies that $(n,x) \in g$. Therefore, $(n+1, f(x)) \in g$. Since $(n+1, f(x)) \neq (0,y)$ we conclude that $(n+1, f(x)) \in h_1$. Thus $h_1 \in \mathscr{C}$ and $h_1 \subset g$. This contradicts the construction of g and ensures that $y = a$. Thus we have handled the base case of the induction.

We now show the induction step. So, let $n \in \mathbb{N}$ and suppose that whenever (n,x) and (n,y) are elements of g, then $x = y$. We must show that whenever $(n+1,u)$ and $(n+1,v)$ are elelments of g, then $u = v$.

By condition (i) above there exists $z \in X$ with $(n,z) \in g$ and, since $g \in \mathscr{C}$, we know that $(n+1, f(z)) \in g$. Suppose that there exists $w \in X$ with $f(z) \neq w$ and $(n+1,w) \in g$. As before, we define $h_2 = g \setminus \{(n+1,w)\}$ and we claim that $h_2 \in \mathscr{C}$. To this end, note that $(0,a) \neq (n+1,w)$ and $(0,a) \in g$. Hence $(0,a) \in h_2$, so the first condition for admittance to $\mathscr{C}$ is satisfied. Furthermore, if $m \in \mathbb{N}$ and $(m,x) \in h_2$, we claim $(m+1, f(x)) \in h_2$.

To this end, note that $(m,x) \in h_2$ implies that $(m,x) \in g$. Because $g \in \mathscr{C}$ we have $(m+1, f(x)) \in g$. If $m \neq n$, then $(m+1, f(x)) \neq (n+1,w)$ and $(m+1, f(x)) \in h_2$. If $m = n$, then we have $(m,x) = (n,x) \in g$ and we chose z so that $(n,z) \in g$. Thus, by our induction hypothesis, $x = z$. Since $f(x) = f(z) \neq w$, we conclude that $(m+1, f(x)) \neq (n+1,w)$. This shows that $(m+1, f(x)) \in h_2$ and completes the proof that $h_2 \in \mathscr{C}$. So, we have constructed an element, h_2, of $\mathscr{C}$ that is strictly contained in g. This contradicts the minimality of g and shows that $w = f(z)$.

By induction, condition (ii) of the function definition also holds. Thus the intersection g is a well-defined function $g : \mathbb{N} \to X$.

To show the uniqueness of $g : \mathbb{N} \to X$ satisfying $g(0) = a$ and $g(n+1) = f(g(n))$ for all $n \in \mathbb{N}$, we suppose to the contrary that there is a different function $k : \mathbb{N} \to X$ that also satisfies $k(0) = a$ and $k(n+1) = f(k(n))$ for all $n \in \mathbb{N}$. We define the set $S = \{x \in \mathbb{N} : g(x) \neq k(x)\}$. Now we suppose that k and g are different functions, so $S \neq \emptyset$. By the well-ordering principle of $\mathbb{N}$ this set has a minimum, which we call $m = \min S$. So $g(m) \neq k(m)$. Since $g(0) = a = k(0)$ we know that $m > 0$. Therefore $m - 1 \in \mathbb{N}$ and $m - 1 \notin S$. Hence $g(m-1) = k(m-1)$. This implies that $g(m) = f(g(m-1)) = f(k(m-1)) = k(m)$. This is a contradiction and shows that our supposition is wrong. We conclude that $g = k$ and our function is unique. □

We now have a way of defining a function on the natural numbers: 1) We give the value of the function at the initial point (this may be at $n = 0, n = 1$, or it may be any other natural number) and 2) we give a rule about how to find the value of a natural number in terms of the function value of the previous number. A function defined in this manner is said to be defined recursively or defined by induction.

Exercise 18.7. We define $g : \mathbb{N} \to \mathbb{N}$ recursively by

$$g(0) = 1 \text{ and } g(n+1) = 5g(n).$$

(a) Find $g(1)$ and $g(8)$.
(b) For this example describe the value a, the set X, and the function f in the recursion theorem. Why is the recursion theorem needed here? ○

We return to our motivating example, the factorial function. It's a function you've known for years, most likely, and yet it is more complicated than it appears—more complicated than most of the other examples in this section. For example, the recursion theorem uses $g(n+1) = f(g(n))$. But we need $g(n+1) = (n+1)g(n)$ and it's difficult to imagine how to express this as $g(f(n))$. It feels more like a rule combining two functions, $(n+1)$ and $g(n)$. We exploit this observation below.

Example 18.8. We defined the factorial function above. Explain how the recursion theorem can be used to show that this definition describes a unique function.

For this example, let $a = (0,1)$, $X = \mathbb{N} \times \mathbb{N}$, and let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ be defined by $f(x,y) = (x+1, (x+1)y)$. The recursion theorem tells us that there is a unique function $g : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ with $g(0) = (0,1)$ and $g(n+1) = f(g(n))$.[1] Well, we aren't interested in the first coordinate; only the second one (why?). So we compose g with the well-defined function $\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ where $\pi(x,y) = y$. If each function is well-defined and unique, then their composition $\pi \circ g : \mathbb{N} \to \mathbb{N}$ is too. Before going

[1] At this point, you probably know that you should write out $g(0), g(1), g(2)$, etc., until you understand what's happening.

on, check that the first coordinate of $g(n)$ is n, and note that the second coordinate of $g(n)$ is $\pi(g(n))$. Now we get

$$\begin{aligned}&(\pi \circ g)(0) = \pi(0,1) = 1 \text{ and}\\ &(\pi \circ g)(n+1) = \pi(f(g(n))) = \pi(n+1,(n+1)\pi(g(n))) = (n+1)(\pi \circ g)(n).\end{aligned}$$

If we write $(\pi \circ g)(n) = n!$, then we have the familiar definition. ○

Definitions

Definition 18.1. For $n \in \mathbb{N}$, we define n **factorial**, written as $n!$, as follows:

$$\begin{aligned}0! &= 1\\ (n+1)! &= (n+1)\cdot n! \quad \text{for } n \geq 0.\end{aligned}$$

Definition 18.2 (for Problem 18.22). A subset S of $\mathbb{R}^2$ is **convex** if for every two points $x, y \in S$, the line segment joining x and y again lies in S.

Definition 18.3 (for Problem 18.24). A **triangular number**, T_n, is the number of equally spaced points that can be used to form an equilateral triangle with sides built of n equally spaced points (see Figure 18.2).

Definition 18.4 (for Problem 18.25). For $k, n \in \mathbb{N}$ with $k \leq n$ we define the **binomial coefficient** as

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Solutions to Exercises

Solution (18.3).

Proof. [Proof of (a)] The base step $n = 1$ is trivial.

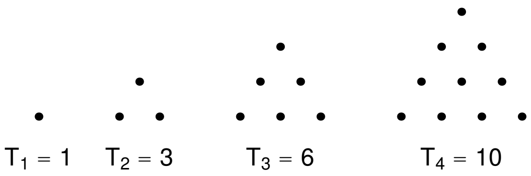

Fig. 18.2 Triangular numbers

For the induction step, let $n \in \mathbb{Z}^+$ and suppose that $|\prod_{k=1}^{n} x_k| = \prod_{k=1}^{n} |x_k|$. Then

$$\begin{aligned}
\left|\prod_{k=1}^{n+1} x_k\right| &= \left|\left(\prod_{k=1}^{n} x_k\right) x_{n+1}\right| \\
&= \left|\prod_{k=1}^{n} x_k\right| |x_{n+1}| \quad \text{(by Theorem 5.3)} \\
&= \left(\prod_{k=1}^{n} |x_k|\right) |x_{n+1}| \quad \text{(by induction hypothesis)} \\
&= \prod_{k=1}^{n+1} |x_k| \, .
\end{aligned}$$

The result follows from the principle of mathematical induction. □

Proof. [Proof of (b)] We will use the triangle inequality (Theorem 5.8), which has been proven (by you) in Problem 5.14. Our proof will be by induction on n. For $n \in \mathbb{Z}^+$, let $P(n)$ denote the assertion that $|\sum_{k=1}^{n} x_k| \leq \sum_{k=1}^{n} |x_k|$.

The validity of the base step, $n = 1$, is clear.

Now let n be a positive integer and suppose that $P(n)$ holds; that is, we let $n \in \mathbb{Z}^+$ and suppose that $|\sum_{k=1}^{n} x_k| \leq \sum_{k=1}^{n} |x_k|$. We must show that $P(n+1)$ holds; in other words, we must show that $|\sum_{k=1}^{n+1} x_k| \leq \sum_{k=1}^{n+1} |x_k|$. But

$$\begin{aligned}
\left|\sum_{k=1}^{n+1} x_k\right| &= |(x_1 + \cdots + x_n) + x_{n+1}| \\
&\leq |x_1 + \cdots + x_n| + |x_{n+1}| \quad \text{(by the triangle inequality)} \\
&= \left|\sum_{k=1}^{n} x_k\right| + |x_{n+1}| \\
&\leq \sum_{k=1}^{n} |x_k| + |x_{n+1}| \quad \text{(by the induction hypothesis)} \\
&= \sum_{k=1}^{n+1} |x_k| ,
\end{aligned}$$

and the result now follows from the principle of mathematical induction. □

Solution (18.4). If the base step is for $n = 1$, then the induction step, $P(n)$ implies $P(n+1)$, needs to be valid *for all* $n \geq 1$. We made the following argument: “Those who are in both groups are also in the first group and therefore they have black hair.” This argument is not valid if $n = 1$. In that case, the group of the first n people is disjoint from the group of the last n people. However, our argument requires that some person be in both groups. Hence the reasoning falls apart right where it should: If a second person joins a black-haired person, there is no guarantee that he or she will also have black hair.

Solution (18.5).

Proof. For $n \in \mathbb{N}$, let $P(n)$ denote the assertion that $4^n - 1$ is a multiple of 3; that is, there is $k \in \mathbb{Z}$ such that $4^n - 1 = 3k$. We will prove this by induction on n.

We check the *base step*. For $n = 0$ the statement becomes $4^0 - 1 = 0$ is divisible by 3. This is obviously true.

Now we check the *induction step*. Let $n \in \mathbb{N}$ and suppose that there exists $k \in \mathbb{Z}$ such that $4^n - 1 = 3k$. We need to show that there exists $l \in \mathbb{Z}$ such that $4^{n+1} - 1 = 3l$. Consider the following calculation:

$$4^{n+1} - 1 = 4 \cdot 4^n - 1 = 3 \cdot 4^n + (4^n - 1) = 3 \cdot 4^n + 3k = 3(4^n + k),$$

where the second-to-last equality is justified by the induction hypothesis. Now set $l = 4^n + k$. Then $l \in \mathbb{Z}$ and $4^{n+1} - 1 = 3l$. Hence the induction step is established.

By the principle of mathematical induction, $4^n - 1$ is divisible by 3 for all $n \in \mathbb{N}$.

□

Solution (18.7).

(a) $g(1) = 5g(0) = 5 \cdot 1 = 5$.
$g(8) = 5g(7) = 5^2 g(6) = 5^3 g(5) = 5^4 g(4) = 5^5 g(3) = 5^6 g(2) = 5^7 g(1) = 5^8$.

(b) In the theorem, we set $a = 1$, $X = \mathbb{N}$, and $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = 5x$. We can now verify that $g(0) = 1$ and $g(n+1) = f(g(n)) = 5g(n)$. The theorem tells us that the function g is well-defined and unique. Without this theorem, we wouldn't be able to conclude that this is true!

Problems

Problem 18.1. Prove that $1 + 2 + \cdots + n = n(n+1)/2$ for every positive integer n, using the principle of mathematical induction.

Problem 18.2. Prove that $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ for every positive integer n, using the principle of mathematical induction.

Problem 18.3. Prove that $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$ for every positive integer n, using the principle of mathematical induction.

Problem 18.4. Prove that if $n \in \mathbb{Z}^+$ and r is a real number such that $r \neq 1$, then

$$\sum_{k=0}^{n-1} r^k = \frac{1 - r^n}{1 - r}.$$

Problem 18.5. Show that $2^n \leq n!$ for all integers with $n \geq 5$.

Problem 18.6. Use induction to prove Bernoulli's inequality: For $x \in \mathbb{R}$, if $1 + x > 0$, then $(1 + x)^n \geq 1 + nx$ for all $n \in \mathbb{N}$.

Problem 18.7. Show that for every positive integer n,

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{2^n}\geq 1+\frac{n}{2}.$$

(This can be used to show that the harmonic series $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}+\cdots$ diverges.)

Problem 18.8. Show that $2^n > n^2$ for all integers n with $n \geq 5$.

Problem 18.9. Prove that 8 divides $5^{2n}-1$ for all $n \in \mathbb{N}$.

Problem 18.10. Suppose that $g : \mathbb{N} \to \mathbb{N}$ satisfies $g(n+1) = g(n) + g(1)$ for all $n \in \mathbb{N}$.

(a) Find $g(0)$.
(b) Show that $g(n+m) = g(n) + g(m)$ for all $n, m \in \mathbb{N}$.

Problem 18.11. Let $g : \mathbb{N} \to \mathbb{R}^+$ and let a be a positive real number. Suppose that g has the properties that $g(1) = a$ and $g(m+n) = g(m)g(n)$ for all natural numbers n and m.

(a) Find $g(0)$. Justify your answer.
(b) Define g recursively.
(c) Prove that $g(n) = a^n$ for all $n \in \mathbb{N}$.

Problem 18.12. Let $a_1, a_2, \ldots, a_n$ be real numbers that satisfy $|a_j| \leq 1$ for all $j = 1, 2, \ldots, n$. Prove that for all $n \in \mathbb{Z}^+$ the following holds:

$$\left|\left(\prod_{j=1}^{n} a_j\right) - 1\right| \leq \sum_{j=1}^{n} |a_j - 1|.$$

Problem 18.13. Show that for all positive integers n,

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

Problem 18.14. Show that for all integers $n \geq 2$,

$$\prod_{k=2}^{n}\left(1-\frac{1}{\sqrt{k}}\right) < \frac{2}{n^2}.$$

Problem 18.15. Find the error in the *Not a proof* below. (See Problem 10.13 for the definition of the degree of a polynomial.)

Nontheorem. *Let p be a polynomial of positive degree n such that p is a product of degree-one polynomials and $p(0) = 0$. If $c \in \mathbb{R}$ satisfies $p(c) = 0$, then $c = 0$.*

In other words, our claim is that if $p(x) = ax(a_1x+b_1)\cdots(a_{n-1}x+b_{n-1})$, where $a, a_1, \ldots, a_{n-1}, b_1, \ldots, b_{n-1} \in \mathbb{R}$ and $a, a_1, \ldots, a_{n-1} \neq 0$, then the only root of p is 0.

Not a proof. We will prove this statement by induction on the degree n of the polynomial p.

For the base step, we let $n = 1$. Since $p(0) = 0$, we can write $p(x) = ax$ for some $a \in \mathbb{R}$ and $a \neq 0$. If $p(c) = 0$, then $p(c) = ac = 0$. Since $a \neq 0$, we conclude that $c = 0$.

For the induction step, let $n \in \mathbb{Z}^+$ and suppose that if p is a polynomial of degree n that is a product of degree-one polynomials and satisfies $p(0) = 0$, then $p(c) = 0$ implies that $c = 0$. Let p be a polynomial of degree $n+1$ that factors into $n+1$ degree-one polynomials and satisfies $p(0) = 0$. We need to show that $p(c) = 0$ implies that $c = 0$. Write $p(x) = ax(a_1x+b_1)\cdots(a_nx+b_n)$, where $a, a_1, \ldots, a_n$ are nonzero real numbers and $b_1, \ldots, b_n \in \mathbb{R}$. Suppose that $p(c) = 0$. Then

$$0 = p(c) = ac(a_1c+b_1)\cdots(a_nc+b_n).$$

One of the factors, $ac, a_1c+b_1, \ldots, a_nc+b_n$, must vanish. Rearranging terms if necessary, we may assume that the factor ac or the factor a_1c+b_1 vanishes. Now,

$$q(x) = ax(a_1x+b_1)\cdots(a_{n-1}x+b_{n-1})$$

is a polynomial of degree n that is a product of degree-one polynomials and satisfies $q(0) = 0$. Since $ac(a_1c+b_1) = 0$, we have $q(c) = 0$. Since our induction hypothesis applies to q, we conclude that $c = 0$. Therefore, $p(c) = 0$ implies that $c = 0$, and the nontheorem follows from mathematical induction. $\boxed{?}$

Problem 18.16. We define the function $g : \mathbb{N} \to \mathbb{R}^+$ recursively by $g(0) = 1$ and $g(n+1) = \frac{g(n)^2+5}{g(n)}$ for $n \in \mathbb{N}$.

(a) Calculate $g(3)$.
(b) Find the value of a, the set X, and the function f used in the recursion theorem to justify the recursive definition of this particular function g.

Problem 18.17. Let $X = \{(x,y) \in \mathbb{R}^2 : x \geq 0, y \geq 0, \text{ and } x+y \leq 1\}$. We define the function $g : \mathbb{N} \to \mathscr{P}(X)$ recursively as follows:

$g(0) = X$ and for $n \in \mathbb{N}$,

$$\begin{aligned} &g(n+1) = \\ &\quad \{(x/2, y/2) : (x,y) \in g(n)\} \cup \{((x+1)/2, y/2) : (x,y) \in g(n)\} \\ &\quad \cup \{(x/2, (y+1)/2) : (x,y) \in g(n)\}. \end{aligned}$$

Sketch $g(0), g(1), g(2)$, and $g(3)$. What kind of object is this function building?

Problem 18.18. Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ be defined by $f(x,y) = (x+1, y^2/x)$ and choose $(1,5) \in \mathbb{N} \times \mathbb{N}$. According to the recursion theorem, there is a unique function $g : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ such that $g(0) = (1,5)$ and $g(n+1) = f(g(n))$ for $n \in \mathbb{N}$. Let $\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined by $\pi(x,y) = y$ and let $h = \pi \circ g : \mathbb{N} \to \mathbb{N}$.

(a) Calculate $h(2)$.

(b) Define h recursively by giving $h(0)$ and $h(n+1)$ in terms of $h(n)$ and n.

Problem 18.19. Write recursive functions for the following, identifying the point a, the set X, and the functions f and g in the recursion theorem. Prove that your answers are correct.

(a) Given a real number $r > 0$, write a recursive function that computes r^n to every $n \in \mathbb{N}$;
(b) Write a recursive function that computes the sum of the first n positive integers.

There is an equivalent form of the principle of mathematical induction, namely:

Theorem 18.9 (Second principle of mathematical induction). *For an integer n, let $Q(n)$ denote an assertion. Suppose that*

(i) $Q(1)$ is true and
(ii) for all positive integers n, if $Q(1), \ldots, Q(n)$ are true, then $Q(n+1)$ is true.

Then $Q(n)$ holds for all positive integers n.

Problem 18.20. Prove that the first principle of mathematical induction (Theorem 18.1) implies the second one (Theorem 18.9). To do so, let $P(n)$ be the assertion "$Q(1), \ldots, Q(n)$ are true."

Problem 18.21. Prove that every integer n, where $n \geq 2$, is a prime or the product of prime numbers. (We have used this before; this shows that every integer $n \geq 2$ can be factored as a product of primes. If you also prove the uniqueness of this factorization, you will have proved the fundamental theorem of arithmetic.)

Problem 18.22. A subset S of $\mathbb{R}^2$ is **convex** if for every two points $x, y \in S$, the line segment joining x and y again lies in S. Recall that an interior angle at a vertex of a convex polygon is the smaller of the two angles formed by the edges at that vertex.

Prove that for an integer n, where $n \geq 3$, the sum of all the interior angles of a convex polygon with n vertices is $(n-2)180$ degrees. (See Figure 18.3.)

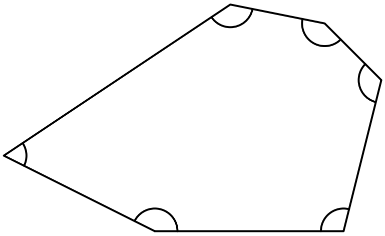

Fig. 18.3 The sum of all the interior angles in this convex polygon is $4 \cdot 180°$

Problem 18.23. Let p_n be a polynomial with real coefficients and of positive degree n. (See Problem 10.13 for the definitions.)

(a) Suppose $p_n(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. For a real number a, what is the largest the degree of q_n, defined by $q_n(x) = p_n(x) - (x-a)a_n x^{n-1}$, can be?

(b) Let $a \in \mathbb{R}$ and $n \in \mathbb{Z}^+$. Prove that $p_n(a) = 0$ if and only if $(x-a)$ is a factor of $p_n(x)$.

Problem 18.24. A **triangular number**, T_n, is the number of equally spaced points that can be used to form an equilateral triangle with sides built of n equally spaced points (see Figure 18.2 on page 201).

(a) Find a formula for the nth triangular number, and prove that your formula is correct.

(b) Can you think of a (familiar) game that uses T_4? T_5?

For $k, n \in \mathbb{N}$ with $k \leq n$ we define the **binomial coefficient** as

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Because the binomial coefficient is the number of ways that we can choose k different elements from a set of n elements, we read $\binom{n}{k}$ as "n choose k."

Theorem 18.10 (Binomial theorem). *Let $a, b \in \mathbb{R} \setminus \{0\}$ and $n \in \mathbb{Z}^+$. Then*

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

Problem 18.25. This problem refers to the notation and theorem above.

(a) Compute each of the following:

$$5!\,,\ \binom{8}{3},\ \binom{8}{5},\ \binom{5}{2},\ \binom{5}{3},\ \binom{7}{0},\ \text{and}\ \binom{7}{7}.$$

(b) Consider the special case of Theorem 18.10 in which $(m+1)^2 = m^2 + 2m + 1$, where $m \in \mathbb{N}$. A "picture proof" is presented in Figure 18.4. Explain the picture proof.

(c) Prove that for all $k, n \in \mathbb{N}$ with $1 \leq k \leq n$, we get

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

(If you write out what it means, life will be a lot easier.)

(d) Use part (c) to prove Theorem 18.10. (See Project 29.8, on Pascal's triangle.)

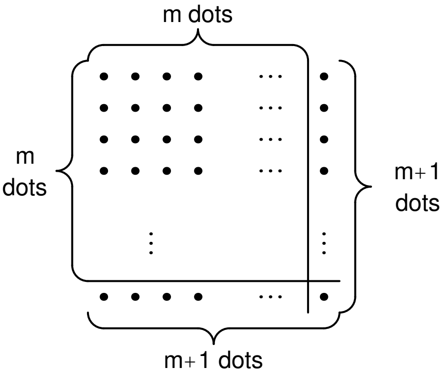

Fig. 18.4 "Proof" of $(m+1)^2 = m^2 + 2m + 1$

(e) Prove that

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0 \text{ for all } n \in \mathbb{Z}^+.$$

Problem 18.26. Deduce the well-ordering principle of $\mathbb{N}$, stated in Chapter 12, from Theorem 18.9 stated on page 206.

Recall that we used the well-ordering principle of $\mathbb{N}$ to prove Theorem 18.1 and that Theorem 18.1 implies Theorem 18.9 (as shown in Problem 18.20). So this problem shows that the principle of mathematical induction, the second principle of mathematical induction, and the well-ordering principle of $\mathbb{N}$ are all equivalent.