CHAPTER 10

Mathematical Induction

This chapter explains a powerful proof technique called **mathematical induction** (or just **induction** for short). To motivate the discussion, let's first examine the kinds of statements that induction is used to prove. Consider the following statement.

Conjecture. The sum of the first n odd natural numbers equals n^2.

The following table illustrates what this conjecture says. Each row is headed by a natural number n, followed by the sum of the first n odd natural numbers, followed by n^2.

n	sum of the first n odd natural numbers	n^2
1	$1 =$	1
2	$1+3 =$	4
3	$1+3+5 =$	9
4	$1+3+5+7 =$	16
5	$1+3+5+7+9 =$	25
⋮	⋮	⋮
n	$1+3+5+7+9+11+\cdots+(2n-1) =$	n^2
⋮	⋮	⋮

Note that in the first five lines of the table, the sum of the first n odd numbers really does add up to n^2. Notice also that these first five lines indicate that the nth odd natural number (the last number in each sum) is $2n-1$. (For instance, when $n=2$, the second odd natural number is $2\cdot 2-1=3$; when $n=3$, the third odd natural number is $2\cdot 3-1=5$, etc.)

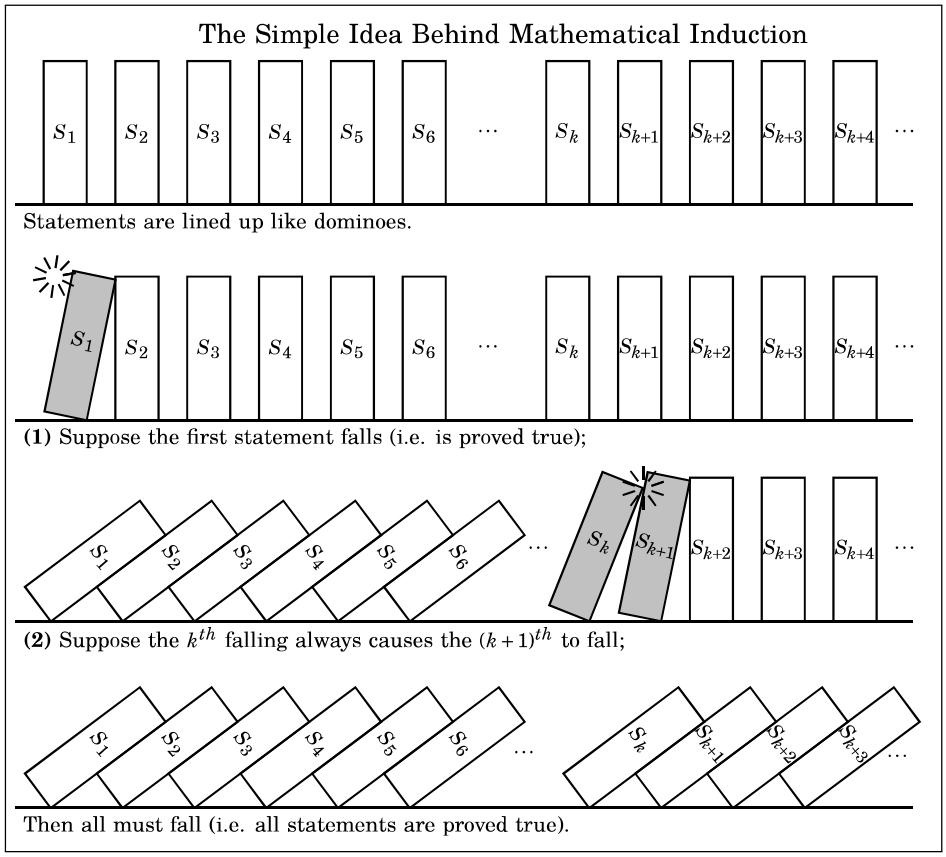
The table raises a question. Does the sum $1+3+5+7+\cdots+(2n-1)$ really always equal n^2? In other words, is the conjecture true?

Let's rephrase this as follows. For each natural number n (i.e., for each line of the table), we have a statement S_n, as follows:

$$S_1 : 1 = 1^2$$
$$S_2 : 1 + 3 = 2^2$$
$$S_3 : 1 + 3 + 5 = 3^2$$
$$\vdots$$
$$S_n : 1 + 3 + 5 + 7 + \cdots + (2n-1) = n^2$$
$$\vdots$$

Our question is: Are all of these statements true?

Mathematical induction is designed to answer just this kind of question. It is used when we have a set of statements $S_1, S_2, S_3, \ldots, S_n, \ldots$, and we need to prove that they are all true. The method is really quite simple. To visualize it, think of the statements as dominoes, lined up in a row. Imagine you can prove the first statement S_1, and symbolize this as domino S_1 being knocked down. Additionally, imagine that you can prove that any statement S_k being true (falling) forces the next statement S_{k+1} to be true (to fall). Then S_1 falls, and knocks down S_2. Next S_2 falls and knocks down S_3, then S_3 knocks down S_4, and so on. The inescapable conclusion is that all the statements are knocked down (proved true).



This picture gives our outline for *proof by mathematical induction.*

Outline for Proof by Induction

Proposition The statements $S_1, S_2, S_3, S_4, \ldots$ are all true.

Proof. (Induction)
(1) Prove that the first statement S_1 is true.
(2) Given any integer $k \geq 1$, prove that the statement $S_k \Rightarrow S_{k+1}$ is true.
It follows by mathematical induction that every S_n is true. ■

In this setup, the first step (1) is called the **basis step**. Because S_1 is usually a very simple statement, the basis step is often quite easy to do. The second step (2) is called the **inductive step**. In the inductive step direct proof is most often used to prove $S_k \Rightarrow S_{k+1}$, so this step is usually carried out by assuming S_k is true and showing this forces S_{k+1} to be true. The assumption that S_k is true is called the **inductive hypothesis**.

Now let's apply this technique to our original conjecture that the sum of the first n odd natural numbers equals n^2. Our goal is to show that for each $n \in \mathbb{N}$, the statement $S_n : 1+3+5+7+\cdots+(2n-1) = n^2$ is true. Before getting started, observe that S_k is obtained from S_n by plugging k in for n. Thus S_k is the statement $S_k : 1+3+5+7+\cdots+(2k-1) = k^2$. Also, we get S_{k+1} by plugging in $k+1$ for n, so that $S_{k+1} : 1+3+5+7+\cdots+(2(k+1)-1) = (k+1)^2$.

Proposition If $n \in \mathbb{N}$, then $1+3+5+7+\cdots+(2n-1) = n^2$.

Proof. We will prove this with mathematical induction.

(1) Observe that if $n = 1$, this statement is $1 = 1^2$, which is obviously true.

(2) We must now prove $S_k \Rightarrow S_{k+1}$ for any $k \geq 1$. That is, we must show that if $1+3+5+7+\cdots+(2k-1) = k^2$, then $1+3+5+7+\cdots+(2(k+1)-1) = (k+1)^2$. We use direct proof. Suppose $1+3+5+7+\cdots+(2k-1) = k^2$. Then

$$\begin{aligned}
1+3+5+7+\cdots\cdots\cdots\cdots+(2(k+1)-1) &= \\
1+3+5+7+\cdots+(2k-1)+(2(k+1)-1) &= \\
\big(1+3+5+7+\cdots+(2k-1)\big)+(2(k+1)-1) &= \\
k^2 \quad +(2(k+1)-1) &= k^2+2k+1 \\
&= (k+1)^2.
\end{aligned}$$

Thus $1+3+5+7+\cdots+(2(k+1)-1) = (k+1)^2$. This proves that $S_k \Rightarrow S_{k+1}$.

It follows by induction that $1+3+5+7+\cdots+(2n-1) = n^2$ for every $n \in \mathbb{N}$. ■

In induction proofs it is usually the case that the first statement S_1 is indexed by the natural number 1, but this need not always be so. Depending on the problem, the first statement could be S_0, or S_m for any other integer m. In the next example the statements are $S_0, S_1, S_2, S_3, \ldots$ The same outline is used, except that the basis step verifies S_0, not S_1.

Proposition If n is a non-negative integer, then $5 \mid (n^5 - n)$.

Proof. We will prove this with mathematical induction. Observe that the first non-negative integer is 0, so the basis step involves $n = 0$.

(1) If $n = 0$, this statement is $5 \mid (0^5 - 0)$ or $5 \mid 0$, which is obviously true.

(2) Let $k \geq 0$. We need to prove that if $5 \mid (k^5 - k)$, then $5 \mid ((k+1)^5 - (k+1))$. We use direct proof. Suppose $5 \mid (k^5 - k)$. Thus $k^5 - k = 5a$ for some $a \in \mathbb{Z}$. Observe that

$$\begin{aligned}(k+1)^5 - (k+1) &= k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1 - k - 1 \\ &= (k^5 - k) + 5k^4 + 10k^3 + 10k^2 + 5k \\ &= 5a + 5k^4 + 10k^3 + 10k^2 + 5k \\ &= 5(a + k^4 + 2k^3 + 2k^2 + k).\end{aligned}$$

This shows $(k+1)^5 - (k+1)$ is an integer multiple of 5, so $5 \mid ((k+1)^5 - (k+1))$. We have now shown that $5 \mid (k^5 - k)$ implies $5 \mid ((k+1)^5 - (k+1))$.

It follows by induction that $5 \mid (n^5 - n)$ for all non-negative integers n. ■

As noted, induction is used to prove statements of the form $\forall n \in \mathbb{N}, S_n$. But notice the outline does *not* work for statements of form $\forall n \in \mathbb{Z}, S_n$ (where n is in $\mathbb{Z}$, not $\mathbb{N}$). The reason is that if you are trying to prove $\forall n \in \mathbb{Z}, S_n$ by induction, and you've shown S_1 is true and $S_k \Rightarrow S_{k+1}$, then it only follows from this that S_n is true for $n \geq 1$. You haven't proved that any of the statements $S_0, S_{-1}, S_{-2}, \ldots$ are true. If you ever want to prove $\forall n \in \mathbb{Z}, S_n$ by induction, you have to show that some S_a is true and $S_k \Rightarrow S_{k+1}$ **and** $S_k \Rightarrow S_{k-1}$.

Unfortunately, the term *mathematical induction* is sometimes confused with *inductive reasoning*, that is, the process of reaching the conclusion that something is likely to be true based on prior observations of similar circumstances. Please note that that mathematical induction, as introduced here, is a rigorous method that proves statements with absolute certainty.

To round out this section, we present four additional induction proofs.

Proposition If $n \in \mathbb{Z}$ and $n \geq 0$, then $\sum_{i=0}^{n} i \cdot i! = (n+1)! - 1$.

Proof. We will prove this with mathematical induction.

(1) If $n = 0$, this statement is

$$\sum_{i=0}^{0} i \cdot i! = (0+1)! - 1.$$

Since the left-hand side is $0 \cdot 0! = 0$, and the right-hand side is $1! - 1 = 0$, the equation $\sum_{i=0}^{0} i \cdot i! = (0+1)! - 1$ holds, as both sides are zero.

(2) Consider any integer $k \geq 0$. We must show that S_k implies S_{k+1}. That is, we must show that

$$\sum_{i=0}^{k} i \cdot i! = (k+1)! - 1$$

implies

$$\sum_{i=0}^{k+1} i \cdot i! = ((k+1)+1)! - 1.$$

We use direct proof. Suppose $\sum_{i=0}^{k} i \cdot i! = (k+1)! - 1$. Observe that

$$\begin{aligned}
\sum_{i=0}^{k+1} i \cdot i! &= \left(\sum_{i=0}^{k} i \cdot i!\right) + (k+1)(k+1)! \\
&= \Big((k+1)! - 1\Big) + (k+1)(k+1)! \\
&= (k+1)! + (k+1)(k+1)! - 1 \\
&= \big(1 + (k+1)\big)(k+1)! - 1 \\
&= (k+2)(k+1)! - 1 \\
&= (k+2)! - 1 \\
&= ((k+1)+1)! - 1.
\end{aligned}$$

Therefore $\sum_{i=0}^{k+1} i \cdot i! = ((k+1)+1)! - 1$.

It follows by induction that $\sum_{i=0}^{n} i \cdot i! = (n+1)! - 1$ for every integer $n \geq 0$. ■

The next example illustrates a trick that is occasionally useful. You know that you can add equal quantities to both sides of an equation without violating equality. But don't forget that you can add *unequal* quantities to both sides of an *inequality*, as long as the quantity added to the bigger side is bigger than the quantity added to the smaller side. For example, if $x \le y$ and $a \le b$, then $x + a \le y + b$. Similarly, if $x \le y$ and b is positive, then $x \le y + b$. This oft-forgotten fact is used in the next proof.

Proposition For each $n \in \mathbb{N}$, it follows that $2^n \le 2^{n+1} - 2^{n-1} - 1$.

Proof. We will prove this with mathematical induction.

(1) If $n = 1$, this statement is $2^1 \le 2^{1+1} - 2^{1-1} - 1$, which simplifies to $2 \le 4 - 1 - 1$, which is obviously true.

(2) Suppose $k \ge 1$. We need to show that $2^k \le 2^{k+1} - 2^{k-1} - 1$ implies $2^{k+1} \le 2^{(k+1)+1} - 2^{(k+1)-1} - 1$. We use direct proof. Suppose $2^k \le 2^{k+1} - 2^{k-1} - 1$, and reason as follows:

$$\begin{aligned}
2^k &\le 2^{k+1} - 2^{k-1} - 1 \\
2(2^k) &\le 2(2^{k+1} - 2^{k-1} - 1) \quad \text{(multiply both sides by 2)} \\
2^{k+1} &\le 2^{k+2} - 2^k - 2 \\
2^{k+1} &\le 2^{k+2} - 2^k - 2 + 1 \quad \text{(add 1 to the bigger side)} \\
2^{k+1} &\le 2^{k+2} - 2^k - 1 \\
2^{k+1} &\le 2^{(k+1)+1} - 2^{(k+1)-1} - 1.
\end{aligned}$$

It follows by induction that $2^n \le 2^{n+1} - 2^{n-1} - 1$ for each $n \in \mathbb{N}$. ■

We next prove that if $n \in \mathbb{N}$, then the inequality $(1+x)^n \ge 1 + nx$ holds for all $x \in \mathbb{R}$ with $x > -1$. Thus we will need to prove that the statement

$$S_n : (1+x)^n \ge 1 + nx \text{ for every } x \in \mathbb{R} \text{ with } x > -1$$

is true for every natural number n. This is (only) slightly different from our other examples, which proved statements of the form $\forall n \in \mathbb{N}, P(n)$, where $P(n)$ is a statement about the number n. This time we are proving something of form

$$\forall n \in \mathbb{N}, P(n, x),$$

where the statement $P(n, x)$ involves not only n, but also a second variable x. (For the record, the inequality $(1+x)^n \ge 1 + nx$ is known as *Bernoulli's inequality*.)

Proposition If $n \in \mathbb{N}$, then $(1+x)^n \geq 1+nx$ for all $x \in \mathbb{R}$ with $x > -1$.

Proof. We will prove this with mathematical induction.

(1) For the basis step, notice that when $n = 1$ the statement is $(1+x)^1 \geq 1+1\cdot x$, and this is true because both sides equal $1+x$.

(2) Assume that for some $k \geq 1$, the statement $(1+x)^k \geq 1+kx$ is true for all $x \in \mathbb{R}$ with $x > -1$. From this we need to prove $(1+x)^{k+1} \geq 1+(k+1)x$. Now, $1+x$ is positive because $x > -1$, so we can multiply both sides of $(1+x)^k \geq 1+kx$ by $(1+x)$ without changing the direction of the $\geq$.

$$\begin{aligned} (1+x)^k(1+x) &\geq (1+kx)(1+x) \\ (1+x)^{k+1} &\geq 1+x+kx+kx^2 \\ (1+x)^{k+1} &\geq 1+(k+1)x+kx^2 \end{aligned}$$

The above term kx^2 is positive, so removing it from the right-hand side will only make that side smaller. Thus we get $(1+x)^{k+1} \geq 1+(k+1)x$. ■

Next, an example where the basis step involves more than routine checking. (It will be used later, so it is numbered for reference.)

Proposition 10.1 Suppose $a_1, a_2, \ldots, a_n$ are n integers, where $n \geq 2$. If p is prime and $p \mid (a_1 \cdot a_2 \cdot a_3 \cdots a_n)$, then $p \mid a_i$ for at least one of the a_i.

Proof. The proof is induction on n.

(1) The basis step involves $n = 2$. Let p be prime and suppose $p \mid (a_1 a_2)$. We need to show that $p \mid a_1$ or $p \mid a_2$, or equivalently, if $p \nmid a_1$, then $p \mid a_2$. Thus suppose $p \nmid a_1$. Since p is prime, it follows that $\gcd(p, a_1) = 1$. By Proposition 7.1 (on page 126), there are integers k and ℓ for which $1 = pk + a_1\ell$. Multiplying this by a_2 gives

$$a_2 = pka_2 + a_1a_2\ell.$$

As we are assuming that p divides a_1a_2, it is clear that p divides the expression $pka_2 + a_1a_2\ell$ on the right; hence $p \mid a_2$. We've now proved that if $p \mid (a_1a_2)$, then $p \mid a_1$ or $p \mid a_2$. This completes the basis step.

(2) Suppose that $k \geq 2$, and $p \mid (a_1 \cdot a_2 \cdots a_k)$ implies then $p \mid a_i$ for some a_i. Now let $p \mid (a_1 \cdot a_2 \cdots a_k \cdot a_{k+1})$. Then $p \mid \big((a_1 \cdot a_2 \cdots a_k) \cdot a_{k+1}\big)$. By what we proved in the basis step, it follows that $p \mid (a_1 \cdot a_2 \cdots a_k)$ or $p \mid a_{k+1}$. This and the inductive hypothesis imply that p divides one of the a_i. ■

Please test your understanding now by working a few exercises.

10.1 Proof by Strong Induction

This section describes a useful variation on induction.

Occasionally it happens in induction proofs that it is difficult to show that S_k forces S_{k+1} to be true. Instead you may find that you need to use the fact that some "lower" statements S_m (with $m < k$) force S_{k+1} to be true. For these situations you can use a slight variant of induction called strong induction. Strong induction works just like regular induction, except that in Step (2) instead of assuming S_k is true and showing this forces S_{k+1} to be true, we assume that *all* the statements $S_1, S_2, \ldots, S_k$ are true and show this forces S_{k+1} to be true. The idea is that if it always happens that the first k dominoes falling makes the $(k+1)$th domino fall, then all the dominoes must fall. Here is the outline.

Outline for Proof by Strong Induction

Proposition The statements $S_1, S_2, S_3, S_4, \ldots$ are all true.

Proof. (Strong induction)
(1) Prove the first statement S_1. (Or the first several S_n.)
(2) Given any integer $k \geq 1$, prove $(S_1 \wedge S_2 \wedge S_3 \wedge \cdots \wedge S_k) \Rightarrow S_{k+1}$. ■

Strong induction can be useful in situations where assuming S_k is true does not neatly lend itself to forcing S_{k+1} to be true. You might be better served by showing some other statement (S_{k-1} or S_{k-2} for instance) forces S_k to be true. Strong induction says you are allowed to use any (or all) of the statements $S_1, S_2, \ldots, S_k$ to prove S_{k+1}.

As our first example of strong induction, we are going to prove that $12 \mid (n^4 - n^2)$ for any $n \in \mathbb{N}$. But first, let's look at how regular induction would be problematic. In regular induction we would start by showing $12 \mid (n^4 - n^2)$ is true for $n = 1$. This part is easy because it reduces to $12 \mid 0$, which is clearly true. Next we would assume that $12 \mid (k^4 - k^2)$ and try to show this implies $12 \mid ((k+1)^4 - (k+1)^2)$. Now, $12 \mid (k^4 - k^2)$ means $k^4 - k^2 = 12a$ for some $a \in \mathbb{Z}$. Next we use this to try to show $(k+1)^4 - (k+1)^2 = 12b$ for some integer b. Working out $(k+1)^4 - (k+1)^2$, we get

$$\begin{aligned}(k+1)^4 - (k+1)^2 &= (k^4 + 4k^3 + 6k^2 + 4k + 1) - (k^2 + 2k + 1) \\ &= (k^4 - k^2) + 4k^3 + 6k^2 + 6k \\ &= 12a + 4k^3 + 6k^2 + 6k.\end{aligned}$$

At this point we're stuck because we can't factor out a 12. Now let's see how strong induction can get us out of this bind.

Strong induction involves assuming each of statements $S_1, S_2, \ldots, S_k$ is true, and showing that this forces S_{k+1} to be true. In particular, if S_1 through S_k are true, then certainly S_{k-5} is true, provided that $1 \le k-5 < k$. The idea is then to show $S_{k-5} \Rightarrow S_{k+1}$ instead of $S_k \Rightarrow S_{k+1}$. For this to make sense, our basis step must involve checking that $S_1, S_2, S_3, S_4, S_5, S_6$ are all true. Once this is established, $S_{k-5} \Rightarrow S_{k+1}$ will imply that the other S_k are all true. For example, if $k = 6$, then $S_{k-5} \Rightarrow S_{k+1}$ is $S_1 \Rightarrow S_7$, so S_7 is true; for $k = 7$, then $S_{k-5} \Rightarrow S_{k+1}$ is $S_2 \Rightarrow S_8$, so S_8 is true, etc.

Proposition If $n \in \mathbb{N}$, then $12 \mid (n^4 - n^2)$.

Proof. We will prove this with strong induction.

(1) First note that the statement is true for the first six positive integers:

If $n = 1$, 12 divides $n^4 - n^2 = 1^4 - 1^2 = 0$.

If $n = 2$, 12 divides $n^4 - n^2 = 2^4 - 2^2 = 12$.

If $n = 3$, 12 divides $n^4 - n^2 = 3^4 - 3^2 = 72$.

If $n = 4$, 12 divides $n^4 - n^2 = 4^4 - 4^2 = 240$.

If $n = 5$, 12 divides $n^4 - n^2 = 5^4 - 5^2 = 600$.

If $n = 6$, 12 divides $n^4 - n^2 = 6^4 - 6^2 = 1260$.

(2) Let $k \ge 6$ and assume $12 \mid (m^4 - m^2)$ for $1 \le m \le k$. (That is, assume statements $S_1, S_2, \ldots, S_k$ are all true.) We must show $12 \mid \big((k+1)^4 - (k+1)^2\big)$. (That is, we must show that S_{k+1} is true.) Since S_{k-5} is true, we have $12 \mid ((k-5)^4 - (k-5)^2)$. For simplicity, let's set $\boxed{m = k-5,}$ so we know $12 \mid (m^4 - m^2)$, meaning $\boxed{m^4 - m^2 = 12a}$ for some integer a. Observe that:

$$\begin{aligned}
(k+1)^4 - (k+1)^2 &= (m+6)^4 - (m+6)^2 \\
&= m^4 + 24m^3 + 216m^2 + 864m + 1296 - (m^2 + 12m + 36) \\
&= (m^4 - m^2) + 24m^3 + 216m^2 + 852m + 1260 \\
&= 12a + 24m^3 + 216m^2 + 852m + 1260 \\
&= 12\big(a + 2m^3 + 18m^2 + 71m + 105\big).
\end{aligned}$$

As $(a + 2m^3 + 18m^2 + 71m + 105)$ is an integer, we get $12 \mid ((k+1)^4 - (k+1)^2)$.

This shows by strong induction that $12 \mid (n^4 - n^2)$ for every $n \in \mathbb{N}$. ■

Our next example involves mathematical objects called *graphs*. In mathematics, the word *graph* is used in two contexts. One context involves the graphs of equations and functions from algebra and calculus. In the other context, a **graph** is a configuration consisting of points (called **vertices**) and **edges** which are lines connecting the vertices. Following are some pictures of graphs. Let's agree that all of our graphs will be in "one piece," that is, you can travel from any vertex of a graph to any other vertex by traversing a route of edges from one vertex to the other.

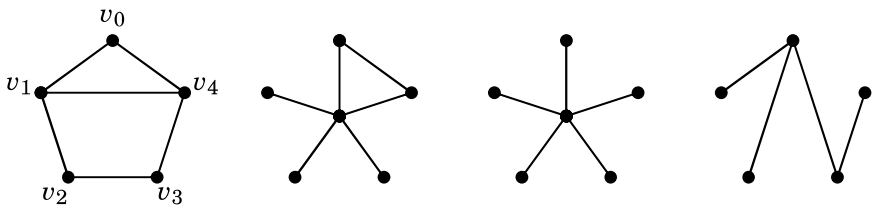


Figure 10.1. Examples of Graphs

A **cycle** in a graph is a sequence of distinct edges in the graph that form a route that ends where it began. For example, the graph on the far left of Figure 10.1 has a cycle that starts at vertex v_1, then goes to v_2, then to v_3, then v_4 and finally back to its starting point v_1. You can find cycles in both of the graphs on the left, but the two graphs on the right do not have cycles. There is a special name for a graph that has no cycles; it is called a **tree**. Thus the two graphs on the right of Figure 10.1 are trees, but the two graphs on the left are not trees.

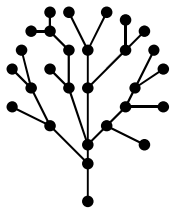


Figure 10.2. A tree

Note that the trees in Figure 10.1 both have one fewer edge than vertex. The tree on the far right has 5 vertices and 4 edges. The one next to it has 6 vertices and 5 edges. Draw any tree; you will find that if it has n vertices, then it has $n-1$ edges. We now prove that this is always true.

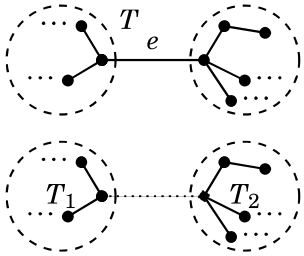
Proposition If a tree has n vertices, then it has $n-1$ edges.

Proof. Notice that this theorem asserts that for any $n \in \mathbb{N}$, the following statement is true: S_n : *A tree with n vertices has* $n-1$ *edges.* We use strong induction to prove this.

(1) Observe that if a tree has $n = 1$ vertex then it has no edges. Thus it has $n-1=0$ edges, so the theorem is true when $n=1$.

(2) Now take an integer $k \geq 1$. We must show $(S_1 \wedge S_2 \wedge \cdots \wedge S_k) \Rightarrow S_{k+1}$. In words, we must show that if it is true that any tree with m vertices has $m-1$ edges, where $1 \leq m \leq k$, then any tree with $k+1$ vertices has $(k+1)-1=k$ edges. We will use direct proof.

Suppose that for each integer m with $1 \leq m \leq k$, any tree with m vertices has $m-1$ edges. Now let T be a tree with $k+1$ vertices. Single out an edge of T and label it e, as illustrated below.



Now remove the edge e from T, but leave the two endpoints of e. This leaves two smaller trees that we call T_1 and T_2. Let's say T_1 has x vertices and T_2 has y vertices. As each of these two smaller trees has fewer than $k+1$ vertices, our inductive hypothesis guarantees that T_1 has $x-1$ edges, and T_2 has $y-1$ edges. Think about our original tree T. It has $x+y$ vertices. It has $x-1$ edges that belong to T_1 and $y-1$ edges that belong to T_2, *plus* it has the additional edge e that belongs to neither T_1 nor T_2. Thus, all together, the number of edges that T has is $(x-1)+(y-1)+1=(x+y)-1$. In other words, T has one fewer edges than it has vertices. Thus it has $(k+1)-1=k$ edges.

It follows by strong induction that a tree with n vertices has $n-1$ edges. ■

Notice that it was absolutely essential that we used strong induction in the above proof because the two trees T_1 and T_2 will not both have k vertices. At least one will have fewer than k vertices. Thus the statement S_k is not enough to imply S_{k+1}. We need to use the assumption that S_m will be true whenever $m \leq k$, and strong induction allows us to do this.

10.2 Proof by Smallest Counterexample

This section introduces yet another proof technique, called **proof by smallest counterexample**. It is a hybrid of induction and proof by contradiction. It has the nice feature that it leads you straight to a contradiction. It is therefore more "automatic" than the proof by contradiction that was introduced in Chapter 6. Here is the outline:

Outline for Proof by Smallest Counterexample

Proposition The statements $S_1, S_2, S_3, S_4, \ldots$ are all true.

Proof. (Smallest counterexample)
(1) Check that the first statement S_1 is true.
(2) For the sake of contradiction, suppose not every S_n is true.
(3) Let $k > 1$ be the smallest integer for which S_k is **false**.
(4) Then S_{k-1} is true and S_k is false. Use this to get a contradiction. ■

Notice that this setup leads you to a point where S_{k-1} is true and S_k is false. It is here, where true and false collide, that you will find a contradiction. Let's do an example.

Proposition If $n \in \mathbb{N}$, then $4 \mid (5^n - 1)$.

Proof. We use proof by smallest counterexample. (We will number the steps to match the outline, but that is not usually done in practice.)

(1) If $n = 1$, then the statement is $4 \mid (5^1 - 1)$, or $4 \mid 4$, which is true.

(2) For sake of contradiction, suppose it's not true that $4 \mid (5^n - 1)$ for all n.

(3) Let $k > 1$ be the smallest integer for which $4 \nmid (5^k - 1)$.

(4) Then $4 \mid (5^{k-1} - 1)$, so there is an integer a for which $5^{k-1} - 1 = 4a$. Then:

$$\begin{aligned} 5^{k-1} - 1 &= 4a \\ 5(5^{k-1} - 1) &= 5 \cdot 4a \\ 5^k - 5 &= 20a \\ 5^k - 1 &= 20a + 4 \\ 5^k - 1 &= 4(5a + 1) \end{aligned}$$

This means $4 \mid (5^k - 1)$, a contradiction, because $4 \nmid (5^k - 1)$ in Step 3. Thus, we were wrong in Step 2 to assume that it is untrue that $4 \mid (5^n - 1)$ for every n. Therefore $4 \mid (5^n - 1)$ is true for every n. ■

We next prove the **fundamental theorem of arithmetic**, which says any integer greater than 1 has a unique prime factorization. For example, 12 factors into primes as $12 = 2 \cdot 2 \cdot 3$, and moreover *any* factorization of 12 into primes uses exactly the primes 2, 2 and 3. Our proof combines the techniques of induction, cases, minimum counterexample and the idea of uniqueness of existence outlined at the end of Section 7.3. We dignify this fundamental result with the label of "Theorem."

Theorem 10.1 (Fundamental Theorem of Arithmetic) Any integer $n > 1$ has a unique prime factorization. That is, if $n = p_1 \cdot p_2 \cdot p_3 \cdots p_k$ and $n = a_1 \cdot a_2 \cdot a_3 \cdots a_\ell$ are two prime factorizations of n, then $k = \ell$, and the primes p_i and a_i are the same, except that they may be in a different order.

Proof. Suppose $n > 1$. We first use strong induction to show that n has a prime factorization. For the basis step, if $n = 2$, it is prime, so it is already its own prime factorization. Let $n \geq 2$ and assume every integer between 2 and n (inclusive) has a prime factorization. Consider $n+1$. If it is prime, then it is its own prime factorization. If it is not prime, then it factors as $n+1 = ab$ with $a, b > 1$. Because a and b are both less than $n+1$ they have prime factorizations $a = p_1 \cdot p_2 \cdot p_3 \cdots p_k$ and $b = p'_1 \cdot p'_2 \cdot p'_3 \cdots p'_\ell$. Then

$$n+1 = ab = (p_1 \cdot p_2 \cdot p_3 \cdots p_k)(p'_1 \cdot p'_2 \cdot p'_3 \cdots p'_\ell)$$

is a prime factorization of $n+1$. This competes the proof by strong induction that every integer greater than 1 has a prime factorization.

Next we use proof by smallest counterexample to prove that the prime factorization of any $n \geq 2$ is unique. If $n = 2$, then n clearly has only one prime factorization, namely itself. Assume for the sake of contradiction that there is an $n > 2$ that has different prime factorizations $n = p_1 \cdot p_2 \cdot p_3 \cdots p_k$ and $n = a_1 \cdot a_2 \cdot a_3 \cdots a_\ell$. Assume n is the smallest number with this property. From $n = p_1 \cdot p_2 \cdot p_3 \cdots p_k$, we see that $p_1 \mid n$, so $p_1 \mid (a_1 \cdot a_2 \cdot a_3 \cdots a_\ell)$. By Proposition 10.1 (page 160), p_1 divides one of the primes a_i. As a_i is prime, we have $p_1 = a_i$. Dividing $n = p_1 \cdot p_2 \cdot p_3 \cdots p_k = a_1 \cdot a_2 \cdot a_3 \cdots a_\ell$ by $p_1 = a_i$ yields

$$p_2 \cdot p_3 \cdots p_k = a_1 \cdot a_2 \cdot a_3 \cdots a_{i-1} \cdot a_{i+1} \cdots a_\ell.$$

These two factorizations are different, because the two prime factorizations of n were different. (Remember: the primes p_1 and a_i are equal, so the difference appears in the remaining factors, displayed above.) But also the above number $p_2 \cdot p_3 \cdots p_k$ is smaller than n, and this contradicts the fact that n was the smallest number with two different prime factorizations. ■

One word of warning about proof by smallest counterexample. In proofs in other textbooks or in mathematical papers, it often happens that the writer doesn't tell you up front that proof by smallest counterexample is being used. Instead, you will have to read through the proof to glean from context that this technique is being used. In fact, the same warning applies to *all* of our proof techniques. If you continue with mathematics, you will gradually gain through experience the ability to analyze a proof and understand exactly what approach is being used when it is not stated explicitly. Frustrations await you, but do not be discouraged by them. Frustration is a natural part of anything that's worth doing.

10.3 Fibonacci Numbers

Leonardo Pisano, now known as Fibonacci, was a mathematician born around 1175 in what is now Italy. His most significant work was a book *Liber Abaci*, which is recognized as a catalyst in medieval Europe's slow transition from Roman numbers to the Hindu-Arabic number system. But he is best known today for a number sequence that he described in his book and that bears his name. The **Fibonacci sequence** is

$$1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,\ 233,\ 377,\ldots$$

The numbers that appear in this sequence are called **Fibonacci numbers**. The first two numbers are 1 and 1, and thereafter any entry is the sum of the previous two entries. For example $3+5=8$, and $5+8=13$, etc. We denote the nth term of this sequence as F_n. Thus $F_1=1$, $F_2=1$, $F_3=2$, $F_4=3$, $F_7=13$ and so on. Notice that the Fibonacci Sequence is entirely determined by the rules $F_1=1$, $F_2=1$, and $F_n=F_{n-1}+F_{n-2}$.

We introduce Fibonacci's sequence here partly because it is something everyone should know about, but also because it is a great source of induction problems. This sequence, which appears with surprising frequency in nature, is filled with mysterious patterns and hidden structures. Some of these structures will be revealed to you in the examples and exercises.

We emphasize that the condition $F_n=F_{n-1}+F_{n-2}$ (or equivalently $F_{n+1}=F_n+F_{n-1}$) is the perfect setup for induction. It suggests that we can determine something about F_n by looking at earlier terms of the sequence. In using induction to prove something about the Fibonacci sequence, you should expect to use the equation $F_n=F_{n-1}+F_{n-2}$ somewhere.

For our first example we will prove that $F_{n+1}^2-F_{n+1}F_n-F_n^2=(-1)^n$ for any natural number n. For example, if $n=5$ we have $F_6^2-F_6F_5-F_5^2=8^2-8\cdot5-5^2=64-40-25=-1=(-1)^5$.

Proposition The Fibonacci sequence obeys $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$.

Proof. We will prove this with mathematical induction.

(1) If $n = 1$ we have $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = F_2^2 - F_2F_1 - F_1^2 = 1^2 - 1\cdot 1 - 1^2 = -1 = (-1)^1 = (-1)^n$, so indeed $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$ is true when $n = 1$.

(2) Take any integer $k \geq 1$. We must show that if $F_{k+1}^2 - F_{k+1}F_k - F_k^2 = (-1)^k$, then $F_{k+2}^2 - F_{k+2}F_{k+1} - F_{k+1}^2 = (-1)^{k+1}$. We use direct proof. Suppose $F_{k+1}^2 - F_{k+1}F_k - F_k^2 = (-1)^k$. Now we are going to carefully work out the expression $F_{k+2}^2 - F_{k+2}F_{k+1} - F_{k+1}^2$ and show that it really does equal $(-1)^{k+1}$. In so doing, we will use the fact that $F_{k+2} = F_{k+1} + F_k$.

$$\begin{aligned}
F_{k+2}^2 - F_{k+2}F_{k+1} - F_{k+1}^2 &= (F_{k+1} + F_k)^2 - (F_{k+1} + F_k)F_{k+1} - F_{k+1}^2 \\
&= F_{k+1}^2 + 2F_{k+1}F_k + F_k^2 - F_{k+1}^2 - F_kF_{k+1} - F_{k+1}^2 \\
&= -F_{k+1}^2 + F_{k+1}F_k + F_k^2 \\
&= -(F_{k+1}^2 - F_{k+1}F_k - F_k^2) \\
&= -(-1)^k \qquad \text{(inductive hypothesis)} \\
&= (-1)^1(-1)^k \\
&= (-1)^{k+1}
\end{aligned}$$

Therefore $F_{k+2}^2 - F_{k+2}F_{k+1} - F_{k+1}^2 = (-1)^{k+1}$.

It follows by induction that $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$ for every $n \in \mathbb{N}$. ■

Let's pause for a moment and think about what the result we just proved means. Dividing both sides of $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$ by F_n^2 gives

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

For large values of n, the right-hand side is very close to zero, and the left-hand side is F_{n+1}/F_n plugged into the polynomial $x^2 - x - 1$. Thus, as n increases, the ratio F_{n+1}/F_n approaches a root of $x^2 - x - 1 = 0$. By the quadratic formula, the roots of $x^2 - x - 1$ are $\frac{1\pm\sqrt{5}}{2}$. As $F_{n+1}/F_n > 1$, this ratio must be approaching the *positive* root $\frac{1+\sqrt{5}}{2}$. Therefore

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \frac{1+\sqrt{5}}{2}. \tag{10.1}$$

For a quick spot check, note that $F_{13}/F_{12} \approx 1.618025$, while $\frac{1+\sqrt{5}}{2} \approx 1.618033$. Even for the small value $n = 12$, the numbers match to four decimal places.

The number $\Phi = \frac{1+\sqrt{5}}{2}$ is sometimes called the **golden ratio**, and there has been much speculation about its occurrence in nature as well as in classical art and architecture. One theory holds that the Parthenon and the Great Pyramids of Egypt were designed in accordance with this number.

But we are here concerned with things that can be proved. We close by observing how the Fibonacci sequence in many ways resembles a geometric sequence. Recall that a **geometric sequence** with first term a and common ratio r has the form

$$a,\ ar,\ ar^2,\ ar^3,\ ar^4,\ ar^5,\ ar^6,\ ar^7,\ ar^8,\ldots$$

where any term is obtained by multiplying the previous term by r. In general its nth term is $G_n = ar^n$, and $G_{n+1}/G_n = r$. Equation (10.1) tells us that $F_{n+1}/F_n \approx \Phi$. Thus even though it is not a geometric sequence, the Fibonacci sequence tends to behave like a geometric sequence with common ratio Φ, and the further "out" you go, the higher the resemblance.

Exercises for Chapter 10

Prove the following statements with either induction, strong induction or proof by smallest counterexample.

1. For every integer $n \in \mathbb{N}$, it follows that $1+2+3+4+\cdots+n = \dfrac{n^2+n}{2}$.

2. For every integer $n \in \mathbb{N}$, it follows that $1^2+2^2+3^2+4^2+\cdots+n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

3. For every integer $n \in \mathbb{N}$, it follows that $1^3+2^3+3^3+4^3+\cdots+n^3 = \dfrac{n^2(n+1)^2}{4}$.

4. If $n \in \mathbb{N}$, then $1\cdot 2+2\cdot 3+3\cdot 4+4\cdot 5+\cdots+n(n+1) = \dfrac{n(n+1)(n+2)}{3}$.

5. If $n \in \mathbb{N}$, then $2^1+2^2+2^3+\cdots+2^n = 2^{n+1}-2$.

6. For every natural number n, it follows that $\sum_{i=1}^{n}(8i-5) = 4n^2-n$.

7. If $n \in \mathbb{N}$, then $1\cdot 3+2\cdot 4+3\cdot 5+4\cdot 6+\cdots+n(n+2) = \dfrac{n(n+1)(2n+7)}{6}$.

8. If $n \in \mathbb{N}$, then $\dfrac{1}{2!}+\dfrac{2}{3!}+\dfrac{3}{4!}+\cdots+\dfrac{n}{(n+1)!} = 1-\dfrac{1}{(n+1)!}$

9. For any integer $n \geq 0$, it follows that $24 \mid (5^{2n}-1)$.

10. For any integer $n \geq 0$, it follows that $3 \mid (5^{2n}-1)$.

11. For any integer $n \geq 0$, it follows that $3 \mid (n^3+5n+6)$.

12. For any integer $n \geq 0$, it follows that $9 \mid (4^{3n}+8)$.