CHAPTER

4 More Proof

Thus far we have used primarily one proof technique known as *direct* proof. In this method, we work from hypothesis to conclusion, showing how each statement follows from previous statements. The central idea is to unravel definitions and bridge the gap from what we have to what we want.

We are now ready for, and need, more sophisticated proof methods. In this chapter, we present two powerful methods: *proof by contradiction* and *proof by induction* (and its variant, *proof by smallest counterexample*).

20 Contradiction

Most theorems can be expressed in the if-then form. The usual way to prove "If A, then B" is to assume the conditions listed in A and then work to prove the conditions in B (see Proof Template 1). In this section, we present two alternatives to the direct proof method.

Proof by Contrapositive

The statement "If A, then B" is logically equivalent to the statement "If (not B), then (not A)." The statement "If (not B), then (not A)" is called the *contrapositive* of "If A, then B."

Why are a statement and its contrapositive logically equivalent? For "If A, then B" to be true, it must be the case that whenever A is true, B must also be true. If it ever should happen that B is false, then it must have been the case that A was false. In other words, if B is false, then A must be false. Thus we have "If (not B), then (not A)."

Here's another explanation. We know that "If A, then B" is logically equivalent to "(not A) or B" (see Exercise 4.4). By the same reasoning, "If (not B), then (not A)" is equivalent to "(not (not B)) or (not A)," but "not (not B)" is the same as B, so this becomes "B or (not A)," which is equivalent to "(not A) or B." In symbols,

$$a \to b \quad = \quad (\neg a) \vee b \quad = \quad (\neg(\neg b)) \vee (\neg a) \quad = \quad (\neg b) \to (\neg a).$$

If these explanations are difficult to follow, here is a mechanical way to proceed. We build a truth table for $a \to b$ and $(\neg b) \to (\neg a)$ and see the same results.

a	b	$a \to b$	$\neg b$	$\neg a$	$(\neg b) \to (\neg a)$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

The bottom line is this: To prove "If A, then B," it is acceptable to prove "If (not B), then (not A)." This is outlined in Proof Template 11.

Proof Template 11 Proof by contrapositive

To prove "If A, then B": Assume (not B) and work to prove (not A).

Let's work through an example.

Proposition 20.1 Let R be an equivalence relation on a set A and let $a, b \in A$. If $a \not R\, b$, then $[a] \cap [b] = \emptyset$.

We have essentially proved this already (see Proposition 15.12). Our purpose here is to illustrate proof by contrapositive. We set the proof up using Proof Template 11.

> Let R be an equivalence relation on a set A and let $a, b \in A$. We prove the contrapositive of the statement.
>
> Suppose $[a] \cap [b] \neq \emptyset$. ... Therefore $a\,R\,b$. ■

The key point to observe is that we suppose the negation of the conclusion (not $[a] \cap [b] = \emptyset$; i.e., $[a] \cap [b] \neq \emptyset$) and work toward proving the negation of the hypothesis (not $a \not R\, b$; i.e., $a\,R\,b$).

Notice that we alerted our reader that we are not using direct proof by announcing that we are going to prove the contrapositive.

To continue the proof, we observe that $[a] \cap [b] \neq \emptyset$ means there is an element in both $[a]$ and $[b]$. We put this into the proof.

> Let R be an equivalence relation on a set A and let $a, b \in A$. We prove the contrapositive of the statement.
>
> Suppose $[a] \cap [b] \neq \emptyset$. Thus there is an $x \in [a] \cap [b]$; that is, $x \in [a]$ and $x \in [b]$. ... Therefore $a\,R\,b$. ■

We use the definition of equivalence class to finish.

> Let R be an equivalence relation on a set A and let $a, b \in A$. We prove the contrapositive of the statement.
>
> Suppose $[a] \cap [b] \neq \emptyset$. Thus there is an $x \in [a] \cap [b]$; that is, $x \in [a]$ and $x \in [b]$. Hence $x\,R\,a$ and $x\,R\,b$. By symmetry $a\,R\,x$, and since $x\,R\,b$, by transitivity we have $a\,R\,b$. ■

Is there an advantage to proof by contrapositive? Yes. Try proving Proposition 20.1 by direct proof. We would assume $a \not R\, b$ and try to show $[a] \cap [b] = \emptyset$. How would we unravel the hypothesis $a \not R\, b$? How do we show that two sets have nothing in common? We don't have good ways of accomplishing these tasks; a direct proof here looks hard. By switching to the contrapositive, we have conditions that are easier for us to use.

Reductio Ad Absurdum

Proof by contradiction is also called *indirect proof*.

One mistake. Here is another way to think about proof by contradiction. We assume A and (not B) and then follow with valid reasoning until we reach an impossible situation. This means there must be a mistake. If all our reasoning is valid, and since we are allowed to assume A, the mistake *must* have been in supposing (not B). Since (not B) is the mistake, we must have B.

Proof by contrapositive is an alternative to direct proof. If you can't find a direct proof, try proving the contrapositive. Wouldn't it be nice if there were a proof technique that combined both direct proof and proof by contrapositive? There is! It is called *proof by contradiction* or, in Latin, *reductio ad absurdum*. Here is how it works.

We want to prove "If A, then B." To do this, we show that it is impossible for A to be true while B is false. In other words, we want to show that "A and (not B)" is impossible.

How do we prove that something is impossible? We suppose the impossible thing is true and prove that this supposition leads to an absurd conclusion. If a statement implies something clearly wrong, then that statement must have been false!

To prove "If A, then B," we make two assumptions. We assume the hypothesis A and we assume the opposite of the conclusion; that is, we assume (not B). From these two assumptions, we try to reach a clearly false statement. The general outline is given in Proof Template 12.

Proof Template 12 Proof by contradiction

To prove "If A, then B":
We assume the conditions in A.
Suppose, for the sake of contradiction, not B.
Argue until we reach a contradiction.
$\Rightarrow\Leftarrow$ ■

(The symbol $\Rightarrow\Leftarrow$ is an abbreviation for the following: Thus we have reached a contradiction. Therefore the supposition (not B) must be false. Hence B is true.)

Let us present a formal description of proof by contradiction and then give an example.

We want to prove a statement of the form "If A, then B." To do this, we assume A and (not B) and show this implies something false. Symbolically, we want to show $a \to b$. To do this, we prove $(a \wedge \neg b) \to \text{FALSE}$. These two are logically equivalent.

Proposition 20.2 The Boolean formulas $a \to b$ and $(a \wedge \neg b) \to \text{FALSE}$ are logically equivalent.

Proof. To see that these two are logically equivalent, we build a truth table.

a	b	$a \to b$	$a \wedge \neg b$	$(a \wedge \neg b) \to \text{FALSE}$
T	T	T	F	T
T	F	F	T	F
F	T	T	F	T
F	F	T	F	T

Therefore $a \to b = (a \wedge \neg b) \to \text{FALSE}$. ■

Let's apply this method to prove the following:

Proposition 20.3 No integer is both even and odd.

Re-expressed in if-then form, Proposition 20.3 reads, "If x is an integer, then x is not both even and odd."

Let's set up a proof by contradiction.

> Let x be an integer.
> Suppose, for the sake of contradiction, that x is both even and odd.
> ...
> That is impossible. Thus we have reached a contradiction, so our supposition (that x is both even and odd) is false. Therefore x is not both even and odd, and the proposition is proved. ■

Several comments are in order:

- The first sentence gives the hypothesis (let x be an integer).
- The second sentence serves two purposes.

  First, it announces to the reader that this is going to be a proof by contradiction using the phrase "for the sake of contradiction."

  Second, it supposes the opposite of the conclusion. The supposition is that x is both even and odd.

- The next sentence reads, "That is impossible." We don't know what the antecedent to "That" is! What is impossible? We don't know yet! As the proof develops, we hope to run into a contradiction.
- Given that we have reached a contradiction, here is how we finish the proof. We say that the supposition is impossible because it leads to an absurd statement. Therefore the supposition (not B) must be false. Hence the conclusion (B) must be true.

  The last few sentences of a proof by contradiction are almost always the same. Mathematicians use a special symbol to abbreviate a lot of words. The symbol is $\Rightarrow\Leftarrow$. The image is that two implications are crashing into one another.

  The symbol $\Rightarrow\Leftarrow$ is an abbreviation for "Thus we have reached a contradiction; therefore the supposition is false."

  The supposition is that which we have supposed—namely, (not B).

We don't know (yet) what contradiction we might reach. Let's just start working with what we have and hope for the best. We know that x is both even and odd, so we unravel.

> Let x be an integer.
> Suppose, for the sake of contradiction, that x is both even and odd.
> Since x is even, we know $2|x$; that is, there is an integer a such that $x = 2a$.
> Since x is odd, we know that there is an integer b such that $x = 2b + 1$.
> . . .
> $\Rightarrow\Leftarrow$ Therefore x is not both even and odd, and the proposition is proved. ■

No contradiction yet. The definitions are completely unraveled. What we have to work with is $x = 2a = 2b + 1$ where a and b are integers. Somehow, we need to manipulate these into something false. Let's try dividing the equation $x = 2a = 2b + 1$ through by 2 to give $\frac{x}{2} = a = b + \frac{1}{2}$, and this says that one integer is just $\frac{1}{2}$ bigger than another (i.e., $a - b = \frac{1}{2}$), but $a - b$ is an integer and $\frac{1}{2}$ is not! A number $(a - b)$ cannot be both an integer and not an integer! That's a contradiction. Hurray!! Let's put it into the proof. (Notice we didn't use $\frac{x}{2}$ in the contradiction, so we can simplify this a bit.)

> Let x be an integer.
> Suppose, for the sake of contradiction, that x is both even and odd.
> Since x is even, we know $2|x$; that is, there is an integer a such that $x = 2a$.
> Since x is odd, we know that there is an integer b such that $x = 2b + 1$.
> Therefore $2a = 2b + 1$. Dividing both sides by 2 gives $a = b + \frac{1}{2}$ so $a - b = \frac{1}{2}$.
> Note that $a - b$ is an integer (since a and b are integers) but $\frac{1}{2}$ is not an integer. $\Rightarrow\Leftarrow$
> Therefore x is *not* both even and odd, and the proposition is proved. ■

This completes the proof. We did not know when we began this proof that the absurdity we would reach is that $\frac{1}{2}$ is an integer. This is typical in a proof by contradiction; we begin with A and (not B) and see where the implications lead.

Proposition 20.3 can also be expressed as follows. Let

$$X = \{x \in \mathbb{Z} : x \text{ is even}\} \quad \text{and} \quad Y = \{x \in \mathbb{Z} : x \text{ is odd}\}.$$

Then $X \cap Y = \emptyset$.

Proof by contradiction is usually the best technique for showing that a set is empty. This is worth codifying in a proof template.

Proof Template 13 Proving that a set is empty.

To prove a set is empty:
Assume the set is nonempty and argue to a contradiction.

Proof Template 13 is appropriate to prove statements of the form "There is no object that satisfies conditions."

Contradiction is also the proof technique of choice when proving *uniqueness* statements. Such statements assert that there can be only one object that satisfies the given conditions.

Mathspeak!

You would think that mathematicians, of all people, would use the word *two* correctly. So it may come as a surprise that when mathematicians say "two" they sometimes mean "one or two." Here is an example. Consider the following statement: Every positive even integer is the sum of two odd positive integers. Mathematicians consider this statement to be true despite the fact that the only way to write 2 as the sum of two positive odd numbers is $2 = 1 + 1$. The two odd numbers in this case are 1 and 1. The two numbers just happen to be the same.

The phrase "Let x and y be two integers ..." allows for the integers x and y to be the same. This is the convention, albeit a slightly dangerous one. It would be better simply to write, "Let x and y be integers ...."

Occasionally we truly wish to eliminate the possibility that $x = y$. In this case, we write, "Let x and y be two different integers ..." or "Let x and y be two distinct integers ...."

Proof Template 14 Proving uniqueness.

To prove there is at most one object that satisfies conditions:

Proof: Suppose there are two different objects, x and y, that satisfy conditions.
Argue to a contradiction.

Often the contradiction in a uniqueness proof is that the two allegedly different objects are in fact the same. Here is a simple example.

Proposition 20.4 Let a and b be numbers with $a \neq 0$. There is at most one number x with $ax + b = 0$.

Proof. Suppose there are two different numbers x and y such that $ax + b = 0$ and $ay + b = 0$. This gives $ax + b = ay + b$. Subtracting b from both sides gives $ax = ay$. Since $a \neq 0$, we can divide both sides by a to give $x = y$.$\Rightarrow\Leftarrow$ ■

Proof by Contradiction and Sudoku

If you solve *Sudoku* puzzles, you have undoubtedly used proof-by-contradiction reasoning. (For those who have not yet become addicted to this game, you can learn how to play on the web.)

For example, suppose the following diagram shows the top three rows of a *Sudoku* puzzle.

			4		9			8
					3		1	
5	6	7		2	8			

We ask: Where does the number 1 belong in the middle 3×3 box? (Take a moment to try to work this out before reading on.)

We claim that the 1 for the middle box must go to the left of the 2 in the bottom row. Here's the proof.

Suppose the 1 goes in the top row, between the 4 and the 9. Then the 1 for the left box cannot be in the top row (because of the 1 from the middle box between the 4 and the 9), cannot be in the middle row (because of the 1 in the right box), and cannot be in the bottom row (because there's no free cell available in the third row of the left box).$\Rightarrow\Leftarrow$ Therefore, the 1 cannot be between the 4 and the 9.

Suppose the 1 goes in the middle row (in one of the two cells to the left of the 3). But then we would have two 1s in the second row of the puzzle.$\Rightarrow\Leftarrow$ Therefore the middle box's 1 cannot be in the second row.

Therefore, the 1 for the middle box must be in the third row and there is only one open cell in that row to the left of the 2.

A Matter of Style

Proof by contradiction of "If A, then B" is often easier than direct proof because there are more conditions available. Instead of starting with only condition A and trying to demonstrate condition B, we start with both A and (not B) and hunt for a contradiction. This gives us more material with which to work.

Sometimes, when you elect to write a proof by contradiction, you may discover that proof by contradiction was not really required and a simpler sort of proof is possible. A proof is a proof, and you should be happy to have found a correct proof. Nonetheless, a simpler way to present your argument is always preferable. Here is how to tell whether you can simplify a proof of "If A, then B."

- You assumed A and (not B). You used only the hypothesis A, and the contradiction you reached was B and (not B).

  In this case, you really have a direct proof and you can remove the extraneous proof-by-contradiction apparatus.
- You assumed A and (not B). You used only the supposition (not B), and the contradiction you reached was A and (not A).

  In this case, you really have a proof by contrapositive. Rewrite it in that form.

Recap

We introduced two new proof techniques for statements of the form "If A, then B." In a proof by contrapositive, we assume (not B) and work to prove (not A). In a proof by contradiction, we assume both A and (not B) and work to produce a contradiction.

20 Exercises

20.1. Please state the contrapositive of each of the following statements:

a. If x is odd, then x^2 is odd.

b. If p is prime, then $2^p - 2$ is divisible by p.

c. If x is nonzero, then x^2 is positive.

d. If the diagonals of a parallelogram are perpendicular, then the parallelogram is a rhombus.

e. If the battery is fully charged, the car will start.

f. If A or B, then C.

20.2. What is the contrapositive of the contrapositive of an if-then statement?

20.3. A statement of the form "A if and only if B" is usually proved in two parts: one part to show $A \Rightarrow B$ and another to show $B \Rightarrow A$.

Explain why the following is also an acceptable structure for a proof. First prove $A \Rightarrow B$ and then prove $\neg A \Rightarrow \neg B$.

20.4. For each of the following statements, write the first sentences of a proof by contradiction (you should not attempt to complete the proofs). Please use the phrase "for the sake of contradiction."

a. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

b. The sum of two negative integers is a negative integer.

c. If the square of a rational number is an integer, then the rational number must also be an integer.

d. If the sum of two primes is prime, then one of the primes must be 2.

e. A line cannot intersect all three sides of a triangle.

f. Distinct circles intersect in at most two points.

g. There are infinitely many primes.

20.5. Prove by contradiction that consecutive integers cannot be both even.

20.6. Prove by contradiction that consecutive integers cannot be both odd.

20.7. Prove by contradiction: If the sum of two primes is prime, then one of the primes must be 2.

You may assume that every integer is either even or odd, but never both.

20.8. Prove by contradiction: If x is a real number, then x^2 is not negative.

20.9. Prove by contradiction: If a and b are real numbers and $ab = 0$, then $a = 0$ or $b = 0$.

20.10. Let a be a number with $a > 1$. Prove that $\sqrt{a}$ is strictly between 1 and a.

20.11. Prove by contradiction: Suppose n is an integer that is divisible by 4. Then $n + 2$ is not divisible by 4.

20.12. Prove by contradiction: A positive integer is divisible by 10 if and only if its last (one's) digit (when written in base ten) is a zero.

You may assume that every positive integer N can be expressed as follows:

$$N = d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_1 10 + d_0$$

where the numbers d_0 through d_k are in the set $\{0, 1, \ldots, 9\}$ and $d_k \neq 0$. In this notation, d_0 is the one's digit of N's base ten representation.

20.13. Let A and B be sets. Prove by contradiction that $(A - B) \cap (B - A) = \emptyset$.

20.14. Let A and B be sets. Prove $A \cap B = \emptyset$ if and only if $(A \times B) \cap (B \times A) = \emptyset$.

20.15. Prove the converse of the Addition Principle (Corollary 12.8). The *converse* of a statement "If A, then B" is the statement "If B, then A." In other words, your job is to prove the following:

Let A and B be finite sets. If $|A \cup B| = |A| + |B|$, then $A \cap B = \emptyset$.

20.16. Let A be a subset of the integers.

a. Write a careful definition for the *smallest element* of A.

b. Let E be the set of even integers; that is, $E = \{x \in \mathbb{Z} : 2|x\}$. Prove by contradiction that E has no smallest element.

c. Prove that if $A \subseteq \mathbb{Z}$ has a smallest element, it is unique.

21 Smallest Counterexample

Proof by contradiction as proof by lack of counterexample.

In Section 20 we developed the method of proof by contradiction. Here is another way we can think of this technique.

We want to prove a result of the form "If A, then B." Let's suppose this result were false. If that were the case, there would be a *counterexample* to the statement. That is, there would be an instance where A is true and B is false. We then analyze that alleged counterexample and produce a contradiction. Since the supposition that there is a counterexample leads to an absurd conclusion (a contradiction), that supposition must be wrong; there is no counterexample. Since there is no counterexample, the result must be true.

For example, we showed that no integer could be both even and odd. We can rephrase the argument as follows:

> Suppose the statement "No integer is both even and odd" were false. Then there would be a counterexample; let's say x were such an integer (i.e., x is both even and odd). Since x is even, there is an integer a such that $x = 2a$. Since x is odd, there is an integer b such that $x = 2b + 1$. Thus $2a = 2b + 1$, which implies $a - b = \frac{1}{2}$. Since a and b are integers, so is $a - b$, $\Rightarrow\Leftarrow$ ($\frac{1}{2}$ is not an integer). ■

In this section, we extend this idea by considering *smallest* counterexamples. It's a little idea that wields enormous power. The essence of the idea is that we not only consider an alleged counterexample to an if-then result, we consider a smallest counterexample. This needs to be done carefully, and we explore this idea at length.

We have not yet proved a fact you know well: Every integer is even or odd. We have shown that no integer can be both even and odd, but we have not yet ruled out the possibility that some integer is neither. It is sensible to try to prove this by contradiction. We would structure the proof as follows:

> Suppose, for the sake of contradiction, that there were an integer x that is neither even nor odd. . . . $\Rightarrow\Leftarrow$ Therefore every integer is either even or odd. ■

Next we could unravel definitions as follows:

> Suppose, for the sake of contradiction, that there were an integer x that is neither even nor odd. So there is no integer a with $x = 2a$ and there is no integer b with $x = 2b + 1$. . . . $\Rightarrow\Leftarrow$ Therefore every integer is either even or odd. ■

And now we're stuck. What do we do next? We need a new idea. The new idea is to consider a *smallest counterexample*. We begin with a restricted version of what we are trying to prove.

Proposition 21.1 Every natural number is either even or odd.

Why do we restrict the scope of Proposition 21.1 to natural numbers? If we were trying to prove that every *integer* is either even or odd, we could not rule out the possibility that there might be infinitely many counterexamples, marching off to $-\infty$. Then we could not talk sensibly about the *smallest* counterexample. It is akin to talking about the smallest odd integer; there is no such thing! The odd numbers descend forever $-3, -5, -7, \ldots$; there is no smallest odd integer.

On the other hand, the natural numbers do not descend forever; they "stop" at zero. It makes sense to speak of the smallest odd natural number, namely 1.

This is why we first prove Proposition 21.1 only for natural numbers. We extend this result to all integers after we complete the proof.

We begin the proof using the idea of smallest counterexample.

> Suppose, for the sake of contradiction, that not all natural numbers are even or odd. Then there is a smallest natural number, x, that is neither even nor odd.
>
> . . . $\Rightarrow\Leftarrow$ ■

We add the next sentence to the proof, and let me warn you that the next sentence has an error! Read the sentence carefully and try to find the mistake.

> Suppose, for the sake of contradiction, that not all natural numbers are even or odd. Then there is a smallest natural number, x, that is neither even nor odd. Since $x - 1 < x$, we see that $x - 1$ is a smaller natural number and therefore is not a counterexample to Proposition 21.1.
>
> . . . $\Rightarrow\Leftarrow$ ■

Do you see the problem? It is subtle. Let's dissect the new sentence.

- Since $x - 1 < x$. . . . No problem here. Obviously $x - 1 < x$.
- . . . $x - 1$ . . . is not a counterexample to Proposition 21.1. No problem here either. We know x is the smallest counterexample. Because $x - 1$ is smaller than x, it is not a counterexample to Proposition 21.1.

  Where is the problem?
- . . . natural number. . . . How do we know $x - 1$ is a natural number? Here's the mistake. We do not know that $x - 1$ is a natural number because we have not ruled out the possibility that $x = 0$.

Now it is not hard to rule out $x = 0$; we simply haven't done it yet. Let's take care of this seemingly minor point.

> Suppose, for the sake of contradiction, that not all natural numbers are even or odd. Then there is a smallest natural number, x, that is neither even nor odd.
>
> We know $x \neq 0$ because 0 is even. Therefore $x \geq 1$.
>
> Since $0 \leq x - 1 < x$, we see that $x - 1$ is a smaller natural number and therefore is not a counterexample to Proposition 21.1.
>
> . . . $\Rightarrow\Leftarrow$ ■

We can now continue the proof. We know that $x - 1 \in \mathbb{N}$ and $x - 1$ is not a counterexample to the proposition. What does this mean? It means that since $x - 1$ is a natural number, it must be either even or odd. We don't know which of these might be true, so we consider both possibilities.

> Suppose, for the sake of contradiction, that not all natural numbers are even or odd. Then there is a smallest natural number, x, that is neither even nor odd.
>
> We know $x \neq 0$ because 0 is even. Therefore $x \geq 1$.
>
> Since $0 \leq x - 1 < x$, we see that $x - 1$ is a smaller natural number and therefore is not a counterexample to Proposition 21.1.
>
> Therefore $x - 1$ is either even or odd. We consider both possibilities.
>
> (1) Suppose $x - 1$ is odd. . . .
> (2) Suppose $x - 1$ is even. . . .
>
> $\ldots \Rightarrow\Leftarrow$ ■

Now we unravel definitions. In case (1), $x - 1$ is odd, so $x - 1 = 2a + 1$ for some integer a. In case (2), $x - 1$ is even, so $x - 1 = 2b$ for some integer b.

> Suppose, for the sake of contradiction, that not all natural numbers are even or odd. Then there is a smallest natural number, x, that is neither even nor odd.
>
> We know $x \neq 0$ because 0 is even. Therefore $x \geq 1$.
>
> Since $0 \leq x - 1 < x$, we see that $x - 1$ is a smaller natural number and therefore is not a counterexample to Proposition 21.1.
>
> Therefore $x - 1$ is either even or odd. We consider both possibilities.
>
> (1) Suppose $x - 1$ is odd. Therefore $x - 1 = 2a + 1$ for some integer a. . . .
> (2) Suppose $x - 1$ is even. Therefore $x - 1 = 2b$ for some integer b. . . .
>
> $\ldots \Rightarrow\Leftarrow$ ■

In case (1), we have $x - 1 = 2a + 1$, so $x = 2a + 2 = 2(a + 1)$, so x is even; this is a contradiction to the fact that x is neither even nor odd. In case (2), we get a similar contradiction.

> Suppose, for the sake of contradiction, that not all natural numbers are even or odd. Then there is a smallest natural number, x, that is neither even nor odd.
>
> We know $x \neq 0$ because 0 is even. Therefore $x \geq 1$.
>
> Since $0 \leq x - 1 < x$, we see that $x - 1$ is a smaller natural number and therefore is not a counterexample to Proposition 21.1.
>
> Therefore $x - 1$ is either even or odd. We consider both possibilities.
>
> (1) Suppose $x - 1$ is odd. Therefore $x - 1 = 2a + 1$ for some integer a. Thus $x = 2a + 2 = 2(a + 1)$, so x is even $\Rightarrow\Leftarrow$ (x is neither even nor odd).
> (2) Suppose $x - 1$ is even. Therefore $x - 1 = 2b$ for some integer b. Thus $x = 2b + 1$, so x is odd $\Rightarrow\Leftarrow$ (x is neither even nor odd).
>
> In every case, we have a contradiction, so the supposition is false and the proposition is proved. ■

Let us summarize the main points of this proof.

- It is a proof by contradiction.
- We consider a smallest counterexample to the result.
- We need to treat the *very* smallest possibility as a special case.
- We descend to a smaller case for which the theorem is true and work back.

Before we present another example, let us finish the job we set out to accomplish.

Corollary 21.2 Every integer is either even or odd.

The key idea is that either $x \geq 0$ (in which case we are finished by Proposition 21.1) or else $x < 0$ (in which case $-x \in \mathbb{N}$, and again we can use Proposition 21.1).

Proof. Let x be any integer.

If $x \geq 0$, then $x \in \mathbb{N}$, so by Proposition 21.1, x is either even or odd.

Otherwise, $x < 0$. In this case $-x > 0$, so $-x$ is either even or odd.

- If $-x$ is even, then $-x = 2a$ for some integer a. But then $x = -2a = 2(-a)$, so x is even.
- If $-x$ is odd, then $-x = 2b + 1$ for some integer b. From this we have $x = -2b - 1 = 2(-b - 1) + 1$, so x is odd.

In every case, x is either even or odd. ■

Proof Template 15 gives the general form of this technique.

Proof Template 15 Proof by smallest counterexample.

First, let x be a smallest counterexample to the result we are trying to prove. It must be clear that there can be such an x.

Second, rule out x being the *very* smallest possibility. This (usually easy) step is called the *basis* step.

Third, consider an instance x' of the result that is "just" smaller than x. Use the fact that the result for x' is true but the result for x is false to reach a contradiction $\Rightarrow\Leftarrow$.

Conclude that the result is true. ■

Here is another proposition we prove using the smallest-counterexample method.

Proposition 21.3 Let n be a positive integer. The sum of the first n odd natural numbers is n^2.

The first n odd natural numbers are $1, 3, 5, \ldots, 2n - 1$. The proposition claims that

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

or, in $\sum$ notation,

$$\sum_{k=1}^{n} (2k - 1) = n^2.$$

For example, with $n = 5$ we have $1 + 3 + 5 + 7 + 9 = 25 = 5^2$.

Proof. Suppose Proposition 21.3 is false. This means that there is a smallest positive integer x for which the statement is false (i.e., the sum of the first x odd numbers is not x^2); that is,

$$1 + 3 + 5 + \cdots + (2x - 1) \neq x^2. \tag{7}$$

Note that $x \neq 1$ because the sum of the first 1 odd numbers is $1 = 1^2$. (This is the basis step.)

So $x > 1$. Since x is the smallest number for which Proposition 21.3 fails and since $x > 1$, the sum of the first $x - 1$ odd numbers must equal $(x - 1)^2$; that is,

$$1 + 3 + 5 + \cdots + [2(x - 1) - 1] = (x - 1)^2. \tag{8}$$

(So far this proof has been on "autopilot." We are simply using Proof Template 15.)

Notice that the left-hand side of (8) is one term short of the sum of the first x odd numbers. We add one more term to both sides of this equation to give

$$1 + 3 + 5 + \cdots + [2(x - 1) - 1] + (2x - 1) = (x - 1)^2 + (2x - 1).$$

The right-hand side can be algebraically expanded; thus

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

contradicting (7).⇒⇐ ■

The absolute importance of the basis step.

In the two proofs we have considered thus far, there is a basis step. In the proof that all natural numbers are either even or odd, we first checked that 0 was not a counterexample. In the proof that the sum of the first n odd numbers is n^2, we first checked that 1 was not a counterexample. These steps are important. They show that the immediate smaller case of the result still makes sense. Perhaps the best way to convince you that this basis step is absolutely essential is to show how we can prove an erroneous result if we omit it.

Statement 21.4 **(false)** Every natural number is both even and odd.

Obviously Statement 21.4 is false! Here we give a bogus proof using the smallest-counterexample method, but omitting the basis step.

"Proof." Suppose Proposition 21.4 is false. Then there is a smallest natural number x that is not both even and odd. Consider $x-1$. Since $x-1<x$, $x-1$ is not a counterexample to Proposition 21.4. Therefore $x-1$ is both even and odd.

Since $x-1$ is even, $x-1=2a$ for some integer a, and so $x=2a+1$, so x is odd.

Since $x-1$ is odd, $x-1=2b+1$ for some integer b, and so $x=2b+2=2(b+1)$, so x is even.

Thus x is both even and odd, but x is not both even and odd.⇒⇐ ■

The proof is 99% correct. Where is the mistake? The error is in the sentence "Therefore $x-1$ is both even and odd." It is correct that $x-1$ is not a counterexample, but we do not know that $x-1$ is a natural number. We do not know this because we have not ruled out the possibility that $x-1=-1$ (i.e., $x=0$). Of course, no natural number is both even and odd. So the smallest natural number that is not both even and odd is zero (the exact problem case!).

Well-Ordering

Let us take a closer look at the proof-by-smallest-counterexample technique. We saw that it was appropriate to apply this technique to showing that all natural numbers are either even or odd, but the method is invalid for integers. The difference is that the integers contain infinitely descending negative numbers. However, consider the following statement and its bogus proof.

Statement 21.5 **(false)** Every nonnegative rational number is an integer.

Recall that a *rational number* is any number that can be expressed as a fraction a/b where $a,b\in\mathbb{Z}$ and $b\neq 0$. This statement is asserting that numbers such as $\frac{1}{4}$ are integers. Ridiculous! Notice, however, that the statement is restricted to nonnegative rational numbers; this is analogous to Proposition 21.1, which was restricted to nonnegative integers.

Let's look at the "proof."

"Proof." Suppose Statement 21.5 were false. Let x be a smallest counterexample.

Notice that $x=0$ is not a counterexample because 0 is an integer. (This is the basis step.)

Since x is a nonnegative rational, so is $x/2$. Furthermore, since $x\neq 0$, we know that $x/2<x$, so $x/2$ is smaller than the smallest counterexample, x. Therefore $x/2$ is not a counterexample, so $x/2$ is an integer. Now $x=2(x/2)$, and 2 times an integer is an integer; therefore x is an integer.⇒⇐ ■

What is wrong with this proof? It looks like we followed Proof Template 15, and we even remembered to do a basis step (we considered $x=0$).

The problem is in the sentence "Let x be a smallest counterexample." There are infinitely many counterexamples to Statement 21.5, including $\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots$. These form an infinite descent of counterexamples, and so there can be no smallest counterexample!

We need to worry that we do not make subtle mistakes like the "proof" of Statement 21.5 when we use the proof-by-smallest-counterexample technique. The central issue is: When can we be certain to find a smallest counterexample?

The guiding principle is the following.

Statement 21.6 **(Well-Ordering Principle)** Every nonempty set of natural numbers contains a least element.

Example 21.7 Let $P = \{x \in \mathbb{N} : x \text{ is prime}\}$. This set is a nonempty subset of the natural numbers. By the Well-Ordering Principle, P contains a least element. Of course, the least element in P is 2.

Example 21.8 Consider the set

$$X = \{x \in \mathbb{N} : x \text{ is even and odd}\}.$$

We know that this set is empty because we have shown that no natural number is both even and odd (Proposition 21.1). But for the sake of contradiction, we suppose that $X \neq \emptyset$; then, by the Well-Ordering Principle, X would contain a smallest element. This is the central idea in the proof of Proposition 21.1.

The term *well-ordered* applies to an ordered set (i.e., a set X with a $<$ relation). The set X is called *well-ordered* if every nonempty subset of X contains a least element.

Example 21.9 In contradistinction, consider the set

$$Y = \{y \in \mathbb{Q} : y \geq 0,\ y \notin \mathbb{Z}\}.$$

The bogus proof of Statement 21.5 sought a least element of Y. We subsequently realized that Y has no least element, and that was the error in our "proof." The Well-Ordering Principle applies to $\mathbb{N}$, but not to $\mathbb{Q}$.

The Well-Ordering Principle is an *axiom* of the natural numbers.

Notice that we called the Well-Ordering Principle a *statement*; we did not call it a *theorem*. Why? The reason harks back to the beginning of this book. We could, but did not, define exactly what the integers are. Were we to go through the difficult task of writing a careful definition of the integers, we would begin by defining the natural numbers. The natural numbers are defined to be a set of "objects" that satisfy certain conditions; these defining conditions are called *axioms*. One of these defining axioms is the Well-Ordering Principle. So the natural numbers obey the Well-Ordering Principle by definition. There are other ways to define integers and natural numbers, and in those contexts one can prove the Well-Ordering Principle. If you are intrigued about how all this is done, I recommend you take a course in foundations of mathematics (such a course might be called Logic and Set Theory).

In any case, our approach has been to assume fundamental properties of the integers; we take the Well-Ordering Principle to be one of those fundamental properties.

The Well-Ordering Principle explains why the smallest-counterexample technique works to prove that natural numbers cannot be both even and odd, but it does not work to prove that nonnegative rationals are integers.

Proof Template 16 gives an alternative to Proof Template 15 that explicitly uses the Well-Ordering Principle.

Proof Template 16 Proof by the Well-Ordering Principle.

To prove a statement about natural numbers:

Proof. Suppose, for the sake of contradiction, that the statement is false. Let $X \subseteq \mathbb{N}$ be the set of counterexamples to the statement. (I like the letter X for eXceptions.) Since we have supposed the statement is false, $X \neq \emptyset$. By the Well-Ordering Principle, X contains a least element, x.

(Basis step.) We know that $x \neq 0$ because *show that the result holds for* 0*; this is usually easy.*

Consider $x - 1$. Since $x > 0$, we know that $x - 1 \in \mathbb{N}$ and the statement is true for $x - 1$ (because $x - 1 < x$). *From here we argue to a contradiction, often that x both is and is not a counterexample to the statement.*$\Rightarrow\Leftarrow$ ■

Here is an example of how to use Proof Template 16.

Proposition 21.10 Let $n \in \mathbb{N}$. If $a \neq 0$ and $a \neq 1$, then

$$a^0 + a^1 + a^2 + \cdots + a^n = \frac{a^{n+1} - 1}{a - 1}. \tag{9}$$

In fancy notation, we want to prove

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

We rule out $a = 1$ because the right-hand side would be $\frac{0}{0}$. We also rule out $a = 0$ to avoid worrying about 0^0. If we take $0^0 = 1$, then the formula still works.

Proof. We prove Proposition 21.10 using the Well-Ordering Principle.

Suppose, for the sake of contradiction, that Proposition 21.10 were false. Let X be the set of counterexamples—that is, those integers n for which Equation (9) does not hold. Hence

$$X = \left\{ n \in \mathbb{N} : \sum_{k=0}^{n} a^k \neq \frac{a^{n+1} - 1}{a - 1} \right\}.$$

As we have supposed that the proposition is false, there must be a counterexample, so $X \neq \emptyset$.

Since X is a nonempty subset of $\mathbb{N}$, by the Well-Ordering Principle, it contains a least element x.

Note that for $n = 0$, Equation (9) reduces to

$$1 = \frac{a^1 - 1}{a - 1}$$

and this is true. This means that $n = 0$ is not a counterexample to the proposition. Thus $x \neq 0$. (This is the basis step.)

Therefore $x > 0$. Now $x - 1 \in \mathbb{N}$ and $x - 1 \notin X$ because $x - 1$ is smaller than the least element of X. Therefore the proposition holds for $n = x - 1$, so we have

$$a^0 + a^1 + a^2 + \cdots + a^{x-1} = \frac{a^x - 1}{a - 1}.$$

We add a^x to both sides of this equation to get

$$a^0 + a^1 + a^2 + \cdots + a^{x-1} + a^x = \frac{a^x - 1}{a - 1} + a^x. \tag{10}$$

Putting the right-hand side of Equation (10) over a common denominator gives

$$\begin{aligned}\frac{a^x - 1}{a - 1} + a^x &= \frac{a^x - 1}{a - 1} + a^x \left(\frac{a - 1}{a - 1}\right)\\ &= \frac{a^x - 1 + a^{x+1} - a^x}{a - 1}\\ &= \frac{a^{x+1} - 1}{a - 1}\end{aligned}$$

and so

$$a^0 + a^1 + a^2 + \cdots + a^x = \frac{a^{x+1} - 1}{a - 1}.$$

This shows that x satisfies the proposition and is therefore not a counterexample, contradicting $x \in X$.$\Rightarrow\Leftarrow$ ■

Proof Template 16 is more rigidly specified than Proof Template 15. Often you will need to modify Proof Template 16 to suit a particular situation. For example, consider the following:

Proposition 21.11 For all integers $n \geq 5$, we have $2^n > n^2$.

Notice that the inequality $2^n > n^2$ is not true for a few small values of n:

n	0	1	2	3	4	5
2^n	1	2	4	8	16	32
n^2	0	1	4	9	16	25

Thus Proposition 21.11 does not apply to all of $\mathbb{N}$. We need to modify Proof Template 16 slightly. Here is the proof of Proposition 21.11:

Proof. Suppose, for the sake of contradiction, Proposition 21.11 were false. Let X be the set of counterexamples; that is,

$$X = \left\{n \in \mathbb{Z} : n \geq 5,\ 2^n \not> n^2\right\}.$$

Since our supposition is that the proposition is false, we have $X \neq \emptyset$. By the Well-Ordering Principle, X contains a least element x.

We claim that $x \neq 5$. Note that $2^5 = 32 > 25 = 5^2$, so 5 is not a counterexample to the proposition (i.e., $x \notin X$), and hence $x \neq 5$. Thus $x \geq 6$.

Now consider $x - 1$. Since $x \geq 6$, we have $x - 1 \geq 5$. Since x is the least element of X, we know that the proposition is true for $n = x - 1$; that is,

$$2^{x-1} > (x - 1)^2. \tag{11}$$

We know $2^{x-1} = \frac{1}{2} \cdot 2^x$ and $(x - 1)^2 = x^2 - 2x + 1$, so Equation (11) can be rewritten as

$$\frac{1}{2} \cdot 2^x > x^2 - 2x + 1.$$

Multiplying both sides by 2 gives

$$2^x > 2x^2 - 4x + 2. \tag{12}$$

We will be finished once we can prove

$$2x^2 - 4x + 2 \geq x^2. \tag{13}$$

To prove Equation (18), we just need to prove

$$x^2 - 4x + 4 \geq 2. \tag{14}$$

We got Equation (14) from Equation (13) by adding $2 - x^2$ to both sides. Notice that Equation (14) can be rewritten

$$(x - 2)^2 \geq 2. \tag{15}$$

So we have reduced the problem to proving Equation (15), and to prove that, it certainly is enough to prove

$$x - 2 \geq 2. \tag{16}$$

and that's true because $x \geq 6$ (all we need is $x \geq 4$). ■

The only modification to Proof Template 16 is that the basis case was $x = 5$ instead of $x = 0$.

We present another example where we need to modify slightly the Well-Ordering Principle method. This example involves the following celebrated sequence of numbers.

Definition 21.12 **(Fibonacci numbers)** The *Fibonacci numbers* are the list of integers $(1, 1, 2, 3, 5, 8, \ldots) = (F_0, F_1, F_2, \ldots)$ where

$$\begin{aligned} F_0 &= 1, \\ F_1 &= 1, \text{ and} \\ F_n &= F_{n-1} + F_{n-2}, \text{ for } n \geq 2. \end{aligned}$$

In words, the Fibonacci numbers are the sequence that begins $1, 1, 2, 3, 5, 8, \ldots$ and each successive term is produced by adding the two previous terms. We label these numbers F_n (starting with F_0).

Proposition 21.13 For all $n \in \mathbb{N}$, we have $F_n \leq 1.7^n$.

Proof. Suppose, for the sake of contradiction, that Proposition 21.13 were false. Let X be the set of counterexamples; that is,

$$X = \{n \in \mathbb{N} : F_n \not\leq 1.7^n\}.$$

Since we have supposed that the proposition is false, we know that $X \neq \emptyset$. Thus, by the Well-Ordering Principle, X contains a least element x.

Observe that $x \neq 0$ because $F_0 = 1 = 1.7^0$ and $x \neq 1$ because $F_1 = 1 \leq 1.7^1$.

Notice that we have considered two basis cases: $x \neq 0$ and $x \neq 1$. Why? We explain in just a moment.

Thus $x \geq 2$. Now we know that

$$F_x = F_{x-1} + F_{x-2} \tag{17}$$

and we know, since $x - 1$ and $x - 2$ are natural numbers less than x, that

$$F_{x-2} \leq 1.7^{x-2} \quad \text{and} \quad F_{x-1} \leq 1.7^{x-1}. \tag{18}$$

This is why! We want to use the fact that the proposition is true for $x - 1$ and $x - 2$ in the proof. We cannot do this unless we are sure that $x - 1$ and $x - 2$ are natural numbers; that is why we must rule out both $x = 0$ and $x = 1$.

Combining Equations (17) and (18), we have

$$\begin{aligned} F_x &= F_{x-1} + F_{x-2} \\ &\leq 1.7^{x-1} + 1.7^{x-2} \\ &= 1.7^{x-2}(1.7 + 1) \\ &= 1.7^{x-2}(2.7) \\ &< 1.7^{x-2}(2.89) \\ &= 1.7^{x-2}(1.7^2) \\ &= 1.7^x. \end{aligned}$$

(The trick was recognizing $2.7 < 2.89 = 1.7^2$.)

Therefore Proposition 21.13 is true for $n = x$, contradicting $x \in X$. $\Rightarrow\Leftarrow$ ■

Recap

In this section, we extended the proof-by-contradiction method to proof by smallest counterexample. We refined this method by explicit use of the Well-Ordering Principle. We underscored the vital importance of the (usually easy) basis case.

21 Exercises

21.1. What is the smallest positive real number?

21.2. Prove by the techniques of this section that $1 + 2 + 3 + \cdots + n = \frac{1}{2}(n)(n + 1)$ for all positive integers n.

21.3. Prove by the techniques of this section that $n < 2^n$ for all $n \in \mathbb{N}$.

21.4. Prove by the techniques of this section that $n! \le n^n$ for all positive integers n.

21.5. Prove by the techniques of this section that $\binom{2n}{n} \le 4^n$ for all natural numbers n.

21.6. Recall Proposition 13.2 that for all positive integers n we have

$$1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n + 1)! - 1.$$

Prove this using the techniques of this section.

21.7. The inequality $F_n > 1.6^n$ is true once n is big enough. Do some calculations to find out from what value n this inequality holds. Prove your assertion.

21.8. Calculate the sum of the first n Fibonacci numbers for $n = 0, 1, 2, \ldots, 5$. In other words, calculate

$$F_0 + F_1 + \cdots + F_n$$

for several values of n.

Formulate a conjecture about these sums and prove it.

21.9. Criticize the following statement and proof:

Statement. All natural numbers are divisible by 3.

Proof. Suppose, for the sake of contradiction, the statement were false. Let X be the set of counterexamples (i.e., $X = \{x \in \mathbb{N} : x \text{ is not divisible by } 3\}$). The supposition that the statement is false means that $X \ne \emptyset$. Since X is a nonempty set of natural numbers, it contains a least element x.

Note that $0 \notin X$ because 0 is divisible by 3. So $x \ne 0$.

Now consider $x - 3$. Since $x - 3 < x$, it is not a counterexample to the statement. Therefore $x - 3$ is divisible by 3; that is, there is an integer a such that $x - 3 = 3a$. So $x = 3a + 3 = 3(a + 1)$ and x is divisible by 3, contradicting $x \in X$.⇒⇐ ■

21.10. In Section 17 we discussed that Pascal's triangle and the triangle of binomial coefficients are the same, and we explained why. Rewrite that discussion as a careful proof using the method of smallest counterexample. Your proof should contain a sentence akin to "Consider the first row where Pascal's triangle and the binomial coefficient triangle are not the same."

21.11. Prove the generalized Addition Principle by use of the Well-Ordering Principle. That is, please prove the following:

Suppose $A_1, A_2, \ldots, A_n$ are pairwise disjoint finite sets. Then

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

And Finally

Theorem 21.14 **(Interesting)** Every natural number is interesting.

Proof. Suppose, for the sake of contradiction, that Theorem 21.14 were false. Let X be the set of counterexamples (i.e., X is the set of those natural numbers that are *not* interesting). Because we have supposed the theorem to be false, we have $X \ne \emptyset$. By the Well-Ordering Principle, let x be the smallest element of X.

Of course, 0 is an interesting number: It is the identity element for addition, it is the first natural number, any number multiplied by 0 is 0, and so on. So $x \ne 0$. Similarly, $x \ne 1$

because 1 is the only unit in $\mathbb{N}$, it is the identity element for multiplication, and so on. And $x \neq 2$ because 2 is the only even prime. These are interesting numbers!

What is x? It is the first natural number that isn't interesting. That makes it very interesting! $\Rightarrow\Leftarrow$ ■

22 Induction

In this section, we present an alternative to proof by smallest counterexample. This method is called *mathematical induction*, or *induction* for short.

Mathspeak!

In standard English, the word *induction* refers to drawing general conclusions from examining several particular facts. For example, the general principle that the sun always rises in the east follows by induction from the observations that every sunrise ever seen has been in the east. This, of course, does not prove the sun will rise in the east tomorrow, but even a mathematician would not bet against it! The mathematician's use of the word *induction* is quite different and is explained in this section.

It's a great deal of fun to stand up a bunch of dominoes on their ends and then set off a chain reaction to knock them all down. The picture on the cover of this book illustrates this.

What conditions need to be met so that all the dominoes will fall? We need two things to hold: First, we need to be able to tip over the first domino in the line. Second, we need to be sure that whenever a domino falls, it knocks over the next domino in the line. If these two criteria are met, then all the dominoes will fall!

Keep this in mind and read on . . .

The Induction Machine

Imagine: Sitting before you is a statement to be proved. Rather than prove it yourself, suppose you could build a machine to prove it for you. Although progress has been made by computer scientists to create theorem-proving programs, the dream of a personal theorem-proving robot is still the stuff of science fiction.

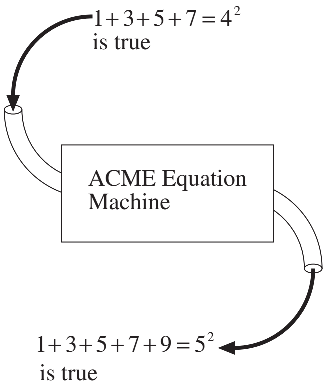
Nevertheless, some statements can be proved by an imaginary theorem-proving machine. Let us illustrate with an example.

Proposition 22.1 Let n be a positive integer. The sum of the first n odd natural numbers is n^2.

This is Proposition 21.3, repeated here for our reconsideration.

We can think of Proposition 22.1 as an assertion that infinitely many equations are true:

$$\begin{aligned} 1 &= 1^2 \\ 1+3 &= 2^2 \\ 1+3+5 &= 3^2 \\ 1+3+5+7 &= 4^2 \\ &\vdots \end{aligned}$$



It is neither difficult nor particular interesting to verify any one of these equations; we just need to add some numbers and check that we get the promised answer.

We could write a computer program to check these equations, but we cannot wait for the program to run forever to verify the entire list. Instead, we are going to build a different sort of machine. Here is how the machine works.

We give the machine one of the equations that has already been proved, say $1+3+5 = 3^2$. The machine takes this equation and uses it to prove the next equation on the list, say $1+3+5+7 = 4^2$. That's all the machine does. When we give the machine one equation, it uses that equation to prove the next equation on the list.

Suppose such a machine has been built and is ready to work. We drop in $1+3+5+7 = 4^2$ and out pops $1+3+5+7+9 = 5^2$. Then we push in $1+3+5+7+9 = 5^2$ and out comes $1+3+5+7+9+11 = 6^2$. Amazing! But it gets tiring feeding the machine these equations, so let's attach a pipe from the "out" tube of the machine around to the "in" tube of the machine. As verified equations pop out of the machine, they are immediately shuttled over to the machine's intake to produce the next equation, and the whole cycle repeats *ad infinitum*.

Our machine is all ready to work. To start it off, we put in the first equation, $1 = 1^2$, switch on the machine and let it run. Out pops $1 + 3 = 2^2$, and then $1 + 3 + 5 = 3^2$, and so on. Marvelous!

Would such a machine be able to prove Proposition 22.1? Won't we need to wait forever for the machine to prove all the equations? Certainly the machine is fun to watch, but who has all eternity to wait?

We need one more idea. Suppose we could prove that the machine is 100% reliable. Whenever one equation on the list is fed into the machine, we are absolutely guaranteed that the machine will verify the next equation on the list. If we had such a guarantee, then we would know that every equation on the list will eventually be proved, so they all must be correct.

Let's see how this is possible. The machine takes an equation that has already been proved, say $1+3+5+7 = 4^2$. The machine is now required to prove that $1+3+5+7+9 = 5^2$. The machine could simply add up 1, 3, 5, 7, and 9 to get 25 and then check that $25 = 5^2$. But that is rather inefficient. The machine already knows that $1 + 3 + 5 + 7 = 4^2$, so it is faster and simpler to add 9 to both sides of the equation: $1 + 3 + 5 + 7 + 9 = 4^2 + 9$. Now the machine just has to calculate $4^2 + 9 = 16 + 9 = 25 = 5^2$.

Here are the blueprints for the machine:

1. The machine receives an equation of the form
$$1 + 3 + 5 + \cdots + (2k - 1) = k^2$$
through its intake tube.
Note: We are allowed to insert only equations that have already been proved, so we trust that this particular equation is correct.
2. The next odd number after $2k - 1$ is $(2k - 1) + 2 = 2k + 1$. The machine adds $2k + 1$ to both sides of the equation. The equation now looks like this:
$$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = k^2 + (2k + 1).$$
3. The machine calculates $k^2 + (2k + 1)$ and checks to see whether it equals $(k + 1)^2$. If so, it is happy and ejects the newly proved equation
$$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = (k + 1)^2$$
through its output tube.

To be sure this machine is reliable, we need to check that whenever we feed the machine a valid equation, the machine will always verify that the next equation on this list is valid.

As we examine the inner workings of the machine carefully, the only place the machine's gears might jam is when it checks whether $k^2 + (2k + 1)$ is equal to $(k + 1)^2$. If we can be sure that step always works, then we can have complete confidence in the machine. Of course, we know from basic algebra that $k^2 + 2k + 1 = (k + 1)^2$, and so we know with complete certainty that this machine will perform its job flawlessly!

The proof boils down to this. It is easy to check the first equation: $1 = 1^2$. We now imagine this equation being fed into the machine (which we proved is flawless) and the machine will prove all the equations on the list. We don't need to wait for the machine to run forever; we know that every equation on the list is going to be proved. Therefore, Proposition 22.1 must be true.

Theoretical Underpinnings

The essence of proof by mathematical induction is embedded in the metaphor of the equation-proving machine. The method is embodied in the following theorem.

Theorem 22.2 **(Principle of Mathematical Induction)** Let A be a set of natural numbers. If

- $0 \in A$, and
- $\forall k \in \mathbb{N},\ k \in A \Longrightarrow k + 1 \in A$,

then $A = \mathbb{N}$.

The two conditions say that (a) 0 is in the set A and (b) whenever a natural number k is in A, it must be the case that $k + 1$ is also in A. The only way these two conditions can be met is if A is the full set of natural numbers.

First we prove this result, and then we explain how to use it as the central tool of a proof technique.

Proof. Suppose, for the sake of contradiction, that $A \neq \mathbb{N}$. Let $X = \mathbb{N} - A$ (i.e., X is the set of natural numbers not in A). Our supposition that $A \neq \mathbb{N}$ means there is some natural number not in A (i.e., $X \neq \emptyset$).

Since X is a nonempty set of natural numbers, we know that X contains a least element x (Well-Ordering Principle). So x is the smallest natural number not in A.

Note that $x \neq 0$ because we are given that $0 \in A$, so $0 \notin X$. Therefore $x \geq 1$. Thus $x - 1 \geq 0$, so $x - 1 \in \mathbb{N}$. Furthermore, since x is the smallest element not in A, we have $x - 1 \in A$.

Now the second condition of the theorem says that whenever a natural number is in A, so is the next larger natural number. Since $x - 1 \in A$, we know that $(x - 1) + 1 = x$ is in A. But $x \notin A$.$\Rightarrow\Leftarrow$ ■

Proof by Induction

We can use Theorem 22.2 as a proof technique. The general kind of statement we prove by induction can be expressed in the form "Every natural number has a certain property." For example, consider the following.

Proposition 22.3 Let n be a natural number. Then

$$0^2 + 1^2 + 2^2 + \cdots + n^2 = \frac{(2n + 1)(n + 1)(n)}{6}. \tag{19}$$

The overall outline of the proof is summarized in Proof Template 17. We use this method to prove Proposition 22.3.

Proof Template 17 Proof by induction.

To prove every natural number has *some property*.

Proof.

- Let A be the set of natural numbers for which the result is true.
- Prove that $0 \in A$. This is called the *basis step*. It is usually easy.
- Prove that if $k \in A$, *then* $k + 1 \in A$. This is called the *inductive step*. To do this we
  - Assume that the result is true for $n = k$. This is called the *induction hypothesis*.
  - Use the induction hypothesis to prove the result is true for $n = k + 1$.
- We invoke Theorem 22.2 to conclude $A = \mathbb{N}$.
- Therefore the result is true for all natural numbers. ■

Proof (of Proposition 22.3)

We prove this result by induction on n. Let A be the set of natural numbers for which Proposition 22.3 is true—that is, those n for which Equation (19) holds.

- **Basis step**: Note that the theorem is true for $n = 0$ because both sides of Equation (19) evaluate to 0.
- **Induction hypothesis**: Suppose the result is true for $n = k$; that is, we may assume
$$0^2 + 1^2 + 2^2 + \cdots + k^2 = \frac{(2k+1)(k+1)(k)}{6}. \tag{20}$$
- Now we need to prove that Equation (19) holds for $n = k + 1$; that is, we need to prove
$$0^2 + 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = \frac{[2(k+1)+1][(k+1)+1][k+1]}{6}. \tag{21}$$
- To prove Equation (21) from Equation (20), we add $(k+1)^2$ to both sides of Equation (20):
$$0^2 + 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = \frac{(2k+1)(k+1)(k)}{6} + (k+1)^2. \tag{22}$$
To complete the proof, we need to show that the right-hand side of Equation (21) equals the right-hand side of Equation (22); that is, we have to prove
$$\frac{(2k+1)(k+1)(k)}{6} + (k+1)^2 = \frac{[2(k+1)+1][(k+1)+1][k+1]}{6}. \tag{23}$$
The verification of Equation (23) is a simple, if mildly painful, algebra exercise that we leave to you (Exercise 22.3).
- We have shown $0 \in A$ and $k \in A \implies (k+1) \in A$. Therefore, by induction (Theorem 22.2), we know that $A = \mathbb{N}$; that is, the proposition is true for all natural numbers. ■

This proof can be described using the machine metaphor. We want to prove all of the following equations:

$$\begin{aligned}
0^2 &= \frac{(2\cdot 0+1)(0+1)(0)}{6}\\
0^2+1^2 &= \frac{(2\cdot 1+1)(1+1)(1)}{6}\\
0^2+1^2+2^2 &= \frac{(2\cdot 2+1)(2+1)(2)}{6}\\
0^2+1^2+2^2+3^2 &= \frac{(2\cdot 3+1)(3+1)(3)}{6}\\
0^2+1^2+2^2+3^2+4^2 &= \frac{(2\cdot 4+1)(4+1)(4)}{6}\\
&\vdots
\end{aligned}$$

So we build a machine that accepts one of these equations in its input tube; the equation entering the machine is assumed to have been proved already. The machine then uses that known equation to verify the next equation on the list. Suppose we know that the machine is absolutely reliable, and whenever one equation is fed into the machine, the next equation on the list will emerge from the machine as verified.

So if we can prove that the machine is completely reliable, all we need to do is feed in the first equation on the list and let the machine churn through the rest. Our job reduces to this: Prove the first equation (which is easy), design the machine, and prove it works.

The design of the machine is not particularly difficult. It simply adds the next term in the long sum to both sides of the equation and checks for equality.

The challenging part is to verify that the machine will always work. For this, we must have to check an algebraic identity, namely
$$\frac{(2k+1)(k+1)(k)}{6} + (k+1)^2 = \frac{[2(k+1)+1][(k+1)+1][k+1]}{6}.$$

In the proof of Proposition 22.3, we explicitly referred to the set A of all natural numbers for which the result is true. As you become more comfortable with proofs by induction, you can omit explicit mention of this set. The important steps in a proof by induction are these:

- Prove the basis case; that is, prove the result is true for $n = 0$.
- Assume the induction hypothesis; that is, assume the result for $n = k$.
- Use the induction hypothesis to prove the next case (i.e., for $n = k + 1$).

Note that in proving the case $n = k + 1$, you should use the fact that the result is true in case $n = k$. If you do not use the induction hypothesis, then either (1) you can write a simpler proof of the result without induction or (2) you have made a mistake.

The basis case is always essential and, thankfully, usually easy. If the result you wish to prove does not cover all natural numbers—say, it covers just the positive integers—then the basis step may begin at a value other than 0.

The induction hypothesis is a seemingly magical tool that makes proving theorems easier. To prove the case $n = k + 1$, not only may you assume the hypotheses of the theorem, but you also may assume the induction hypothesis; this gives you more with which to work.

Proving Equations and Inequalities

Proof by induction takes practice. One common application of this technique is to prove equations and inequalities. Here we present some examples for you to study. You will find that the general outlines of the proofs are the same; the only difference is in some of the algebra. The first two examples are results also proved in Section 13 by the combinatorial method (see Propositions 13.1 and 13.2).

Proposition 22.4 Let n be a positive integer. Then

$$2^0 + 2^1 + \cdots + 2^{n-1} = 2^n - 1.$$

Note that this induction proof begins with $n = 1$ because the Proposition is asserted for positive integers.

Proof. We prove this by induction on n.

Basis step: The case $n = 1$ is true because both sides of the equation, 2^0 and $2^1 - 1$, evaluate to 1.

Induction hypothesis: Suppose the result is true when $n = k$; that is, we assume

$$2^0 + 2^1 + \cdots + 2^{k-1} = 2^k - 1. \tag{24}$$

We must prove that the Proposition is true when $n = k + 1$; that is, we must use Equation (24) to prove

$$2^0 + 2^1 + \cdots + 2^{(k+1)-1} = 2^{k+1} - 1. \tag{25}$$

Note that the left-hand side of Equation (25) can be formed from the left-hand side of Equation (24) by adding the term 2^k. So we add 2^k to both sides of Equation (24) to get

$$2^0 + 2^1 + \cdots + 2^{k-1} + 2^k = 2^k - 1 + 2^k. \tag{26}$$

We need to show that the right-hand side of Equation (26) equals the right-hand side of Equation (25). Fortunately, this is easy:

$$2^k - 1 + 2^k = 2 \cdot 2^k - 1 = 2^{k+1} - 1. \tag{27}$$

Using Equations (25) and (27) gives

$$2^0 + 2^1 + \cdots + 2^{(k+1)-1} = 2^{k+1} - 1$$

which is what we needed to show. ■

As our comfort and confidence in writing proofs by induction grow, we can be a bit terser. The next proof is written in a more compact style.

Proposition 22.5 Let n be a positive integer. Then

$$1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n + 1)! - 1.$$

Proof. We prove the result by induction on n.

Basis case: The Proposition is true in the case $n = 1$, because both sides of the equation, $1! \cdot 1$ and $2! - 1$, evaluate to 1.

Induction hypothesis: Suppose the Proposition is true in case $n = k$; that is, we have that

$$1 \cdot 1! + 2 \cdot 2! + \cdots + k \cdot k! = (k + 1)! - 1. \tag{28}$$

We need to prove the Proposition for the case $n = k + 1$. To this end, we add $(k + 1) \cdot (k + 1)!$ to both sides of Equation (28) to give

$$1 \cdot 1! + 2 \cdot 2! + \cdots + k \cdot k! + (k + 1) \cdot (k + 1)! = (k + 1)! - 1 + (k + 1) \cdot (k + 1)!. \tag{29}$$

The right-hand side of Equation (29) can be manipulated as follows:

$$\begin{aligned}(k + 1)! - 1 + (k + 1) \cdot (k + 1)! &= (1 + k + 1) \cdot (k + 1)! - 1 \\ &= (k + 2) \cdot (k + 1)! - 1 \\ &= (k + 2)! - 1 = [(k + 1) + 1]! - 1.\end{aligned}$$

Substituting this into Equation (29) gives

$$1 \cdot 1! + 2 \cdot 2! + \cdots + k \cdot k! + (k + 1) \cdot (k + 1)! = [(k + 1) + 1]! - 1.$$

■

Inequalities can be proved by induction as well. Here is a simple example whose proof is a bit terser still.

Proposition 22.6 Let n be a natural number. Then

$$10^0 + 10^1 + \cdots + 10^n < 10^{n+1}.$$

Proof. The proof is by induction on n. The basis case, when $n = 0$, is clear because $10^0 < 10^1$.

Assume (induction hypothesis) that the result holds for $n = k$; that is, we have

$$10^0 + 10^1 + \cdots + 10^k < 10^{k+1}.$$

To show that the Proposition is true when $n = k + 1$, we add 10^{k+1} to both sides and find

$$\begin{aligned}10^0 + 10^1 + \cdots + 10^k + 10^{k+1} &< 10^{k+1} + 10^{k+1} \\ &= 2 \cdot 10^{k+1} < 10 \cdot 10^{k+1} = 10^{k+1}.\end{aligned}$$

Therefore the result holds when $n = k + 1$. ■

Other Examples

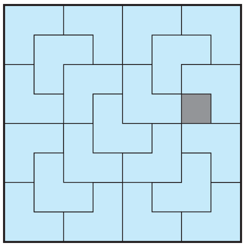
With a bit of practice, proving equations and inequalities by induction will become routine. Generally, we manipulate both sides of the given equation (assumed by the induction hypothesis, $n = k$) to demonstrate the next equation ($n = k + 1$). However, other kinds of results can be proved by induction. For example, consider the following:

Proposition 22.7 Let n be a natural number. Then $4^n - 1$ is divisible by 3.

Proof. The proof is by induction on n. The basis case, $n = 0$, is clear since $4^0 - 1 = 1 - 1 = 0$ is divisible by 3.

Suppose (induction hypothesis) that the Proposition is true for $n = k$; that is, $4^k - 1$ is divisible by 3. We must show that $4^{k+1} - 1$ is also divisible by 3.

Note that $4^{k+1} - 1 = 4 \cdot 4^k - 1 = 4(4^k - 1) + 4 - 1 = 4(4^k - 1) + 3$. Since $4^k - 1$ and 3 are both divisible by 3, it follows that $4(4^k - 1) + 3$ is divisible by 3 hence $4^{k+1} - 1$ is divisible by 3. ■

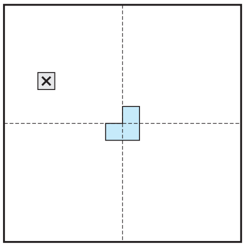


The next example involves some geometry. We wish to cover a chess board with special tiles called *L-shaped triominoes*, or *L-triominoes* for short. These are tiles formed from three 1×1 squares joined at their edges to form an L shape.

It is not possible to tile a standard 8×8 chess board with L-triominoes because there are 64 squares on the chess board and 64 is not divisible by 3. However, it is possible to cover all but one square of the chess board, and such a tiling is shown in the figure.

Is it possible to tile larger chess boards? A $2^n \times 2^n$ chess board has 4^n squares, so, applying Proposition 22.7, we know that $4^n - 1$ is divisible by 3. Hence there is a hope that we may be able to cover all but one of the squares.

Proposition 22.8 Let n be a positive integer. For every square on a $2^n \times 2^n$ chess board, there is a tiling by L-triominoes of the remaining $4^n - 1$ squares.



Proof. The proof is by induction on n. The basis case, $n = 1$, is obvious since placing an L-triomino on a 2×2 chess board covers all but one of the squares, and by rotating the triomino we can select which square is missed.

Suppose (induction hypothesis) that the Proposition has been proved for $n = k$.

We are given a $2^{k+1} \times 2^{k+1}$ chess board with one square selected. Divide the board into four $2^n \times 2^n$ subboards (as shown); the selected square must lie in one of these subboards. Place an L-triomino overlapping three corners from the remaining subboards as shown in the diagram.

We now have four $2^k \times 2^k$ subboards each with one square that does not need to be covered. By induction, the remaining squares in the subboards can be tiled by L-triominoes. ■

Strong Induction

Here is a variation on Theorem 22.2.

Theorem 22.9 **(Principle of Mathematical Induction—strong version)** Let A be a set of natural numbers. If

- $0 \in A$ and
- for all $k \in \mathbb{N}$, if $0, 1, 2, \ldots, k \in A$, then $k + 1 \in A$

then $A = \mathbb{N}$.

The proof of this theorem is left to you (see Exercise 22.23).

Why is this called *strong* induction? Suppose you are using induction to prove a proposition. In both standard and strong induction, you begin by showing the basis case ($0 \in A$). In standard induction, you assume the induction hypothesis ($k \in A$; i.e., the proposition is true for $n = k$) and then use that to prove $k + 1 \in A$ (i.e., the proposition is true for $n = k + 1$). Strong induction gives you a stronger induction hypothesis. In strong induction, you may assume $0, 1, 2, \ldots, k \in A$ (the proposition is true for all n from 0 to k) and use that to prove $k + 1 \in A$ (the proposition is true for $n = k + 1$).

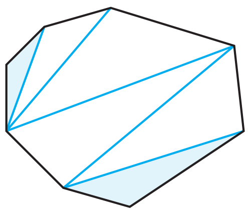
This method is outlined in Proof Template 18.

Proof Template 18 Proof by strong induction.

To prove every natural number has *some property*:

Proof.

- Let A be the set of natural numbers for which the result is true.
- Prove that $0 \in A$. This is called the *basis step*. It is usually easy.
- Prove that *if* $0, 1, 2, \ldots, k \in A$, *then* $k + 1 \in A$. This is called the *inductive step*. To do this we
  - Assume that the result is true for $n = 0, 1, 2, \ldots, k$. This is called the *strong induction hypothesis*.
  - Use the strong induction hypothesis to prove the result is true for $n = k + 1$.
- Invoke Theorem 22.9 to conclude $A = \mathbb{N}$.
- Therefore the result is true for all natural numbers. ■



Let us see how to use strong induction and why it gives us more flexibility than standard induction. We illustrate proof by strong induction on a geometry problem.

Let P be a polygon in the plane. To *triangulate* a polygon is to draw diagonals through the interior of the polygon so that (1) the diagonals do not cross each other and (2) every region created is a triangle (see the figure). Notice that we have shaded two of the triangles. These triangles are called *exterior* triangles because two of their three sides are on the exterior of the original polygon.

We prove the following result using strong induction.

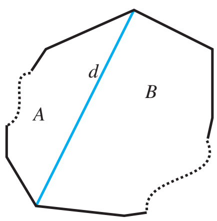
Proposition 22.10 If a polygon with four or more sides is triangulated, then at least two of the triangles formed are exterior.

Proof. Let n denote the number of sides of the polygon. We prove Proposition 22.10 by strong induction on n.

Basis case: Since this result makes sense only for $n \geq 4$, the basis case is $n = 4$. The only way to triangulate a quadrilateral is to draw in one of the two possible diagonals. Either way, the two triangles formed must be exterior.

Strong induction hypothesis: Suppose Proposition 22.10 has been proved for all polygons on $n = 4, 5, \ldots, k$ sides.

Let P be any triangulated polygon with $k + 1$ sides. We must prove that at least two of its triangles are exterior.



Let d be one of the diagonals. This diagonal separates P into two polygons A and B where (this is the key comment) A and B are triangulated polygons with fewer sides than P. It is possible that one or both of A and B are triangles themselves. We consider the cases where neither, one, or both A and B are triangles.

- *If A is not a triangle*: Then, since A has at least four, but at most k sides, by strong induction we know that two or more of A's triangles are exterior. Now we need to worry: Are the exterior triangles of A really exterior triangles of P? Not necessarily. If one of A's exterior triangles uses the diagonal d, then it is not an exterior triangle of P. Nonetheless, the other exterior triangle of A can't also use the diagonal d, and so at least one exterior triangle of A is also an exterior triangle of P.
- *If B is not a triangle*: As in the previous case, B contributes at least one exterior triangle to P.
- *If A is a triangle*: Then A is an exterior triangle of P.
- *If B is a triangle*: Then B is an exterior triangle of P.

In every case, both A and B contribute at least one exterior triangle to P, and so P has at least two exterior triangles. ■

Strong induction helped us enormously in this proof. When we considered the diagonal d, we did not know the number of sides of the two polygons A and B. All we knew for sure was that they had fewer sides than P. To use ordinary induction, we would need to have chosen a diagonal such that A had k sides and B had three; in other words, we would have to select B to be an exterior triangle. The problem is that we had not yet proved that a triangulated polygon has an exterior triangle!

Curiously, it is harder to prove that a triangulated polygon has one exterior triangle than to prove that a triangulated polygon has two exterior triangles! See Exercise 22.21.

Strong induction gives more flexibility than standard induction because the induction hypothesis lets you assume more. It is probably best not to write your proof in the style of strong induction when standard induction suffices. In the cases where you need to use strong induction, you also have proof by smallest counterexample as an alternative.

A More Complicated Example

Fibonacci numbers were introduced in Definition 21.12. Recall that $F_0 = F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for all $n \geq 2$.

We prove the following result by strong induction. The hard part of this example is keeping track of the many binomial coefficients. The overall structure of the proof is no different from the proof of Proposition 22.10. We follow Proof Template 18.

Proposition 22.11 Let $n \in \mathbb{N}$ and let F_n denote the n^{th} Fibonacci number. Then

$$\binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots + \binom{0}{n} = F_n. \tag{30}$$

Note that the last several terms in the sum are all zero. Eventually the lower index in the binomial coefficient will exceed the upper index, and all terms from that point on are zero. For example,

$$\tbinom{7}{0} + \tbinom{6}{1} + \tbinom{5}{2} + \tbinom{4}{3} + \tbinom{3}{4} + \tbinom{2}{5} + \tbinom{1}{6} + \tbinom{0}{7} = 1+6+10+4+0+0+0+0 = 21 = F_7.$$

In fancy notation,

$$\sum_{j=0}^{n} \binom{n-j}{j} = F_n.$$

Before we present the formal proof of Proposition 22.11, let us look to see why this might be true and why we need strong induction.

In general, to prove that some expression gives a Fibonacci number, we use the fact that $F_n = F_{n-1} + F_{n-2}$. If we know that the expression works for F_{n-1} and F_{n-2}, then we can add the appropriate expressions and hope we get F_n. In ordinary induction, we can assume only the immediate smaller case of the result; here we need the two previous values, and strong induction allows us to do this.

Let's see how we can apply this to Proposition 22.11 by examining the case $n = 8$. We want to prove

$$F_8 = \binom{8}{0} + \binom{7}{1} + \cdots + \binom{4}{4}.$$

We do this by assuming

$$F_6 = \binom{6}{0} + \binom{5}{1} + \binom{4}{2} + \binom{3}{3} \quad \text{and}$$

$$F_7 = \binom{7}{0} + \binom{6}{1} + \binom{5}{2} + \binom{4}{3}.$$

We want to add these equations because $F_8 = F_7 + F_6$. The idea is to interleave the terms from the two expressions:

$$F_7 + F_6 = \binom{7}{0} + \binom{6}{0} + \binom{6}{1} + \binom{5}{1} + \binom{5}{2} + \binom{4}{2} + \binom{4}{3} + \binom{3}{3}$$

Now we can use Pascal's identity (Theorem 17.10) to combine pairs of terms:

$$\binom{6}{0}+\binom{6}{1}=\binom{7}{1} \qquad \binom{5}{1}+\binom{5}{2}=\binom{6}{2} \qquad \binom{4}{2}+\binom{4}{3}=\binom{5}{3}$$

We can therefore combine every other term to get

$$\begin{aligned} F_7+F_6 &= \binom{7}{0}+\left[\binom{6}{0}+\binom{6}{1}\right]+\left[\binom{5}{1}+\binom{5}{2}\right]+\left[\binom{4}{2}+\binom{4}{3}\right]+\binom{3}{3} \\ &= \binom{7}{0}+\binom{7}{1}+\binom{6}{2}+\binom{5}{3}+\binom{3}{3}. \end{aligned}$$

We are nearly finished. Notice that the $\binom{7}{0}$ term should be $\binom{8}{0}$ and the $\binom{3}{3}$ term should be $\binom{4}{4}$. The good news is that these terms both equal 1, so we can replace what we have by what we want to finish this example:

$$\begin{aligned} F_7+F_6 &= \binom{7}{0}+\binom{6}{0}+\binom{6}{1}+\binom{5}{1}+\binom{5}{2}+\binom{4}{2}+\binom{4}{3}+\binom{3}{3} \\ &= \binom{7}{0}+\binom{7}{1}+\binom{6}{2}+\binom{5}{3}+\binom{3}{3} \\ &= \binom{8}{0}+\binom{7}{1}+\binom{6}{2}+\binom{5}{3}+\binom{4}{4}. \end{aligned}$$

The case $F_9 = F_8 + F_7$ is similar, but there are some minor differences. It is important that you write out the steps for this case yourself before reading the proof. Be sure you see what the differences are between these two cases.

Proof (of Proposition 22.11)

We use strong induction.

Basis case: The result is true for $n = 0$; Equation (30) reduces to $\binom{0}{0} = 1 = F_0$, which is true. Notice that the result is also true for $n = 1$ since $\binom{1}{0}+\binom{0}{1} = 1 + 0 = 1 = F_1$.

Strong induction hypothesis: Proposition 22.11 is true for all values of n from 0 to k. (We may also assume $k \geq 1$ since we have already proved the result for $n = 0$ and $n = 1$.)

We seek to prove Equation (30) in the case $n = k + 1$; that is, we want to prove

$$F_{k+1} = \binom{k+1}{0}+\binom{k}{1}+\binom{k-1}{2}+\cdots.$$

By the strong induction hypothesis, we know the following two equations are true:

$$\begin{aligned} F_{k-1} &= \binom{k-1}{0}+\binom{k-2}{1}+\binom{k-3}{2}+\cdots \\ F_k &= \binom{k}{0}+\binom{k-1}{1}+\binom{k-2}{2}+\cdots. \end{aligned}$$

We add these two lines to get

$$\begin{aligned} F_{k+1} &= F_k + F_{k-1} \\ &= \binom{k}{0}+\binom{k-1}{0}+\binom{k-1}{1}+\binom{k-2}{1}+\binom{k-2}{2}+\binom{k-3}{2}+\cdots. \end{aligned}$$

The next step is to combine terms with the same upper index using Pascal's identity (Theorem 17.10). First, we are going to worry about where this long sum ends.

In the case k is even, the sum ends

$$F_{k+1} = \cdots + \binom{\frac{k}{2}+1}{\frac{k}{2}-2}+\binom{\frac{k}{2}+1}{\frac{k}{2}-1}+\binom{\frac{k}{2}}{\frac{k}{2}-1}+\binom{\frac{k}{2}}{\frac{k}{2}}$$

and in the case k is odd, it ends

$$F_{k+1} = \cdots + \binom{\frac{1}{2}(k-1)+1}{\frac{1}{2}(k-1)-1} + \binom{\frac{1}{2}(k-1)+1}{\frac{1}{2}(k-1)} + \binom{\frac{1}{2}(k-1)}{\frac{1}{2}(k-1)}.$$

Now we apply Pascal's identity, combining those pairs of terms with the same upper entry (each black term and the color term that follows).

In the case k is even, we have

$$\begin{aligned} F_{k+1} &= \binom{k}{0} + \left[\binom{k}{1} + \binom{k-1}{2} + \cdots + \binom{\frac{k}{2}+2}{\frac{k}{2}-1} + \binom{\frac{k}{2}+1}{\frac{k}{2}}\right] \\ &= \binom{k+1}{0} + \left[\binom{k}{1} + \binom{k-1}{2} + \cdots + \binom{\frac{k}{2}+2}{\frac{k}{2}-1} + \binom{\frac{k}{2}+1}{\frac{k}{2}}\right] \end{aligned}$$

and in the case k is odd, we have

$$\begin{aligned} F_{k+1} &= \binom{k}{0} + \left[\binom{k}{1} + \binom{k-1}{2} + \cdots + \binom{\frac{1}{2}(k-1)+2}{\frac{1}{2}(k-1)}\right] + \binom{\frac{1}{2}(k-1)}{\frac{1}{2}(k-1)} \\ &= \binom{k+1}{0} + \left[\binom{k}{1} + \binom{k-1}{2} + \cdots + \binom{\frac{1}{2}(k-1)+2}{\frac{1}{2}(k-1)}\right] + \binom{\frac{1}{2}(k+1)}{\frac{1}{2}(k+1)}. \end{aligned}$$

In both cases, we have verified Equation (30) with $n = k + 1$, completing the proof. ■

The most difficult part of this proof was dealing with the upper and lower indices of the binomial coefficients.

A Matter of Style

Proof by induction and proof by smallest counterexample are usually interchangeable. I prefer, however, proof by smallest counterexample. This is mostly a stylistic preference, but there is a mathematical reason to prefer the smallest-counterexample technique. When mathematicians try to prove statements, they may believe that the statement is true, but they don't *know*—until they have a proof—whether or not the statement is true. We often alternate between trying to prove the statement and trying to find a counterexample. One way to do both activities simultaneously is to try to deduce properties a smallest counterexample might have. In this way, we either reach a contradiction (and then we have a proof of the statement) or we learn enough about how the counterexample should behave to construct a counterexample.

Recap

Proof by induction is an alternative method to proof by smallest counterexample. The first step in a proof by induction is to prove a basis case (often that the result you want to prove is true for $n = 0$). In standard induction, we make an induction hypothesis (the proposition is true when $n = k$) and use it to prove the next case (the proposition is true when $n = k + 1$). Strong induction is similar, but the strong-induction hypothesis is that the proposition is true for $n = 0, 1, 2, \ldots, k$.

Any result you prove by induction (standard or strong) can just as well be proved using the smallest-counterexample method. Induction proofs are more popular.

22 Exercises

22.1. Induction is often likened to climbing a ladder. If you can master the following two skills, then you can climb a ladder: (1) get your foot on the first rung and (2) advance from one rung to the next.

Explain why both parts (1) and (2) are necessary, and explain what this has to do with induction.

22.2. Give a "mathematical proof" that you can topple an entire line of dominoes provided (a) you can tip over the first domino in the line and (b) whenever a domino falls, it knocks over the next domino in the line.

22.3. Prove Equation (23).

22.4. Prove the following equations by induction. In each case, n is a positive integer.

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

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

c. $9 + 9 \times 10 + 9 \times 100 + \cdots + 9 \times 10^{n-1} = 10^n - 1$.

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

e. $1 + x + x^2 + x^3 + \cdots + x^n = (1 - x^{n+1})/(1 - x)$. You should assume $x \neq 1$. What is the correct right hand side when $x = 1$?

The next parts are for those who have studied calculus.

f.

$$\lim_{x\to\infty} \frac{x^n}{e^x} = 0.$$

g.

$$n! = \int_0^\infty x^n e^{-x}\, dx.$$

h. The nth derivative of x^n is $n!$; that is

$$\frac{d^n}{dx^n} x^n = n!.$$

22.5. Prove the following inequalities by induction. In each case, n is a positive integer.

a. $2^n \le 2^{n+1} - 2^{n-1} - 1$.

b. $(1 - \frac{1}{2})(1 - \frac{1}{4})(1 - \frac{1}{8}) \cdots (1 - \frac{1}{2^n}) \ge \frac{1}{4} + \frac{1}{2^{n+1}}$.

c. $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{2^n} \ge 1 + \frac{n}{2}$.

d. $\binom{2n}{n} < 4^n$.

e. $n! \le n^n$.

f. $1 + 2 + 3 + 4 + \cdots + n \le n^2$.

22.6. Let F_k denote the k^{th} Fibonacci number (see Definition 21.12). Find a formula for

$$\sum_{k=0}^{n} (-1)^k F_k$$

and prove by induction that your formula is correct for all $n > 0$.

22.7. This problem is motivated by the infinite sum

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots.$$

You are going to show that the value of this sum is between 1 and 2 with the help of Exercise 22.4(d). This sum is known as $\zeta(2)$ (where ζ is the Greek letter *zeta* and stands for the *Riemann zeta function*).

For your first step, please prove (by induction) that the following inequality holds for all positive integers n:

$$\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{n^2} > \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)}. \qquad (*)$$

For the second step, prove (by induction) this variation of $(*)$ is true for all positive integers n:

$$\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{n^2} \le 1 + \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{(n-1)n}. \qquad (**)$$

Finally, use $(*)$, $(**)$, and Exercise 22.4(d) to show that $1 \le \zeta(2) \le 2$.

22.8. Let A be the matrix

$$A = \begin{bmatrix} 2 & 2 \\ -1 & 5 \end{bmatrix}$$

Prove, by induction, that for a positive integer n we have

$$A^n = \begin{bmatrix} 2\cdot 3^n - 4^n & 2\cdot 4^n - 2\cdot 3^n \\ 3^n - 4^n & 2\cdot 4^n - 3^n \end{bmatrix} = 4^n \begin{bmatrix} -1 & 2 \\ -1 & 2 \end{bmatrix} + 3^n \begin{bmatrix} 2 & -2 \\ 1 & -1 \end{bmatrix}.$$

This problem involves matrix multiplication. Here A^n means A matrix multiplied by itself n times. For 2×2-matrices we have

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} aw+by & ax+bz \\ cw+dy & cx+dz \end{bmatrix}$.

So for the matrix in this problem $A^2 = \begin{bmatrix} 2 & 14 \\ -7 & 23 \end{bmatrix}$.