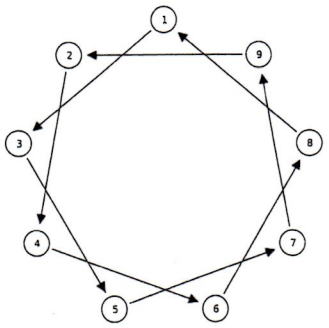

c. Let n be a positive integer. Draw n lines (no two of which are parallel) in the plane. How many regions are formed?

d. Place n points evenly around a circle. Starting at one point, draw a path to every other point around the circle until returning to start. In some instances, every point is visited and in some instances some are missed. Under what circumstances is every point visited (as in the figure with $n = 9$)?
Suppose instead of jumping to every second point, we jump to every third point. For what values of n does the path touch every point?
Finally, suppose we visit every k^{th} point (where k is between 1 and n). When does the path touch every point?

e. A school has a long hallway of lockers numbered 1, 2, 3, and so on up to 1000. In this problem we'll refer to *flipping* a locker to mean opening a closed locker or closing an open locker. That is, to *flip* a locker is to change its closed/open state.

- Student #1 walks down the hallway and closes all the lockers.
- Student #2 walks down the hallway and flips all the even numbered lockers. So now, the odd lockers are closed and the even lockers are open.
- Student #3 walks down the hall and flips all the lockers that are divisible by 3.
- Student #4 walks down the hall and flips all the lockers that are divisible by 4.
- Likewise students 5, 6, 7, and so on walk down the hall in turn, each flipping lockers divisible by their own number until finally student 1000 flips the (one and only) locker divisible by 1000 (the last locker).

Which lockers are open and which are closed? Generalize to any number of lockers.
Note: We ask you to prove your conjecture later; see Exercise 24.19. _____

5 Proof

We create mathematical concepts via definitions. We then posit assertions about mathematical notions, and then we try to prove our ideas are correct.

What is a *proof*?

In science, truth is borne out through experimentation. In law, truth is ascertained by a trial and decided by a judge and/or jury. In sports, the truth is the ruling of referees to the best of their ability. In mathematics, we have *proof*.

Truth in mathematics is not demonstrated through experimentation. This is not to say that experimentation is irrelevant for mathematics—quite the contrary! Trying out ideas and examples helps us to formulate statements we believe to be true (conjectures); we then try to prove these statements (thereby converting conjectures to theorems).

For example, recall the statement "All prime numbers are odd." If we start listing the prime numbers beginning with 3, we find hundreds and thousands of prime numbers, and they are all odd! Does this mean all prime numbers are odd? Of course not! We simply missed the number 2.

Let us consider a far less obvious example.

Conjecture 5.1 **(Goldbach)** Every even integer greater than two is the sum of two primes.

Let's see that this statement is true for the first few even numbers. We have

$$4 = 2 + 2 \qquad 6 = 3 + 3 \qquad 8 = 3 + 5 \qquad 10 = 3 + 7$$
$$12 = 5 + 7 \qquad 14 = 7 + 7 \qquad 16 = 11 + 5 \qquad 18 = 11 + 7.$$

Mathspeak! A proof is often called an *argument*. In standard English, the word *argument* carries a connotation of disagreement or controversy. No such negative connotation should be associated with a mathematical argument. Indeed, mathematicians are honored when their proofs are called "[illegible]"

One could write a computer program to verify that the first few billion even numbers (starting with 4) are each the sum of two primes. Does this imply Goldbach's Conjecture is true? No! The numerical evidence makes the conjecture believable, but it does not prove that it is true. To date, no proof has been found for Goldbach's Conjecture, so we simply do not know whether it is true or false.

A proof is an essay that incontrovertibly shows that a statement is true. Mathematical

and logical constructions appear frequently in proofs. In this and subsequent sections, we show how proofs are written.

The theorems we prove in this section are all rather simple. Indeed, you won't learn any facts about numbers you probably didn't already know quite well. The point in this section is not to learn new information about numbers; the point is to learn how to write proofs. So without further ado, let's start writing proofs!

We prove the following:

Proposition 5.2 The sum of two even integers is even.

We write the proof here in full, and then discuss how this proof was created. In this proof, each sentence is numbered so we can examine the proof piece by piece. Normally we would write this short proof as a single paragraph and not number the sentences.

Proof Proposition 5.2

1. We show that if x and y are even integers, then $x + y$ is an even integer.
2. Let x and y be even integers.
3. Since x is even, we know by Definition 3.1 that x is divisible by 2 (i.e., $2|x$).
4. Likewise, since y is even, $2|y$.
5. Since $2|x$, we know, by Definition 3.2, that there is an integer a such that $x = 2a$.
6. Likewise, since $2|y$, there is an integer b such that $y = 2b$.
7. Observe that $x + y = 2a + 2b = 2(a + b)$.
8. Therefore there is an integer c (namely, $a + b$) such that $x + y = 2c$.
9. Therefore (Definition 3.2) $2|(x + y)$.
10. Therefore (Definition 3.1) $x + y$ is even. ■

Let us examine exactly how this proof was written.

Convert the statement to if-then form.

- The first step is to convert the statement of the proposition into the if-then form.

  The statement reads, "The sum of two even integers is even."

  We convert the statement into if-then form as follows:

  "If x and y are even integers, then $x + y$ is an even integer."

  Note that we introduced letters (x and y) to name the two even integers. These letters come in handy in the proof.

  Observe that the first sentence of the proof spells out the proposition in if-then form.

  Sentence 1 announces the structure of this proof. The hypothesis (the "if" part) tells the reader that we will assume that x and y are even integers, and the conclusion (the "then" part) tells the reader that we are working to prove that $x + y$ is even.

  Sentence 1 can be regarded as a preamble to the proof. The proof starts in earnest at sentence 2.

Write the first and last sentences using the hypothesis and conclusion of the statement.

- The next step is to write the very beginning and the very *end* of the proof.

  The hypothesis of sentence 1 tells us what to write next. It says, "...if x and y are even integers...," so we simply write, "Let x and y be even integers." (Sentence 2)

  Immediately after we write the first sentence, we write the very last sentence of the proof. The last sentence of the proof is a rewrite of the conclusion of the if-then form of the statement.

  "Therefore, $x + y$ is even." (Sentence 10)

  The basic skeleton of the proof has been constructed. We know where we begin (x and y are even), and we know where we are heading ($x + y$ is even).

Unravel definitions.

- The next step is to unravel definitions. We do this at both ends of the proof.

  Sentence 2 tells us that x is even. What does this mean? To find out, we check (or we remember) the definition of the word *even*. (Take a quick look at Definition 3.1 on page 4.) It says that an integer is even provided it is divisible by 2. So we know that x is divisible by 2, and we can also write that as $2|x$; this gives sentence 3.

  Sentence 4 does the same job as sentence 3. Since the reasoning in sentence 4 is identical to that of sentence 3, we use the word *likewise* to flag this parallel construction.

  We now unravel the definition of *divisible*. We consult Definition 3.2 to learn that $2|x$ means there is an integer—we need to give that integer a name and we call it a—so that

$x = 2a$. So sentence 5 just unravels sentence 3. Similarly (*likewise*!) sentence 6 unravels the fact that $2|y$ (sentence 4), and we know we have an integer b such that $y = 2b$.

At this point, we are stuck. We have unraveled all the definitions at the beginning of the proof, so now we return to the end of the proof and work backward!

We are still in the "unravel definitions" phase of writing this proof. The last sentence of the proof says, "Therefore $x + y$ is even." How do we prove an integer is even? We turn to the definition of *even*, and we see that we need to prove that $x + y$ is divisible by 2. So we know that the penultimate sentence (number 9) should say that $x + y$ is divisible by 2.

How do we get to sentence 9? To show that an integer (namely, $x + y$) is divisible by 2, we need to show there is an integer—let's call it c—such that $(x + y) = 2c$. This gives sentence 8.

Now we have unraveled definitions from both ends of the proof. Let's pause a moment to see what we have. The proof (written more tersely here) reads:

> We show that if x and y are even integers, then $x + y$ is an even integer.
>
> Let x and y be even integers. By definition of *even*, we know that $2|x$ and $2|y$. By definition of *divisibility*, we know there are integers a and b such that $x = 2a$ and $y = 2b$.
>
> ⋮
>
> Therefore there is an integer c such that $x + y = 2c$; hence $2|(x + y)$, and therefore $x + y$ is even.

What do we know? What do we need? Make the ends meet.

- The next step is to think. What do we know and what do we need?

  We know $x = 2a$ and $y = 2b$. We need an integer c such that $x + y = 2c$. So in this case, it is easy to see that we can take $c = a + b$ because the sum of two integers is an integer. We fill in the middle of the proof with sentence 7 and we are finished! To celebrate, and to mark the end of the proof, we append an end-of-proof symbol to the end of the proof: ■

This middle step—which was quite easy—is actually the hardest part of the proof. The translation of the statement of the proposition into if-then form and the unraveling of definitions are routine; once you have written several proofs, you will find these steps are easily produced. The hard part comes when you try to make ends meet!

The proof of Proposition 5.2 is the most basic type of proof; it is called a *direct* proof. The steps in writing a direct proof of an if-then statement are summarized in Proof Template 1.

Proof Template 1 Direct proof of an if-then theorem.

- Write the first sentence(s) of the proof by restating the hypothesis of the result. Invent suitable notation (e.g., assign letters to stand for variables).
- Write the last sentence(s) of the proof by restating the conclusion of the result.
- Unravel the definitions, working forward from the beginning of the proof and backward from the end of the proof.
- Figure out what you know and what you need. Try to forge a link between the two halves of your argument.

Let's use the direct proof technique to prove another result.

Proposition 5.3 Let a, b, and c be integers. If $a|b$ and $b|c$, then $a|c$.

The first step in creating the proof of this proposition is to write the first and last sentences based on the hypothesis and conclusion. This gives

> Suppose a, b, and c are integers with $a|b$ and $b|c$.
> ...
> Therefore $a|c$. ■

Next we unravel the definition of divisibility.

> Suppose a, b, and c are integers with $a|b$ and $b|c$. Since $a|b$, there is an integer x such that $b = ax$. Likewise there is an integer y such that $c = by$.
> ...
> Therefore there is an integer z such that $c = az$. Therefore $a|c$. ■

We have unraveled the definitions. Let's consider what we have and what we need.

We have a, b, c, x, and y such that: $b = ax$ and $c = by$.

We want to find z such that: $c = az$.

Now we have to think, but fortunately the problem is not too hard. Since $b = ax$, we can substitute ax for b in $c = by$ and get $c = axy$. So the z we need is $z = xy$. We can use this to finish the proof of Proposition 5.3.

> Suppose a, b, and c are integers with $a|b$ and $b|c$. Since $a|b$, there is an integer x such that $b = ax$. Likewise there is an integer y such that $c = by$. Let $z = xy$. Then $az = a(xy) = (ax)y = by = c$.
> Therefore there is an integer z such that $c = az$. Therefore $a|c$. ■

A More Involved Proof

Propositions 5.2 and 5.3 are rather simple and not particularly interesting. Here we develop a more interesting proposition and its proof.

One of the most intriguing and most difficult issues in mathematics is the pattern of prime and composite numbers. Here is one pattern for you to consider. Pick a positive integer, cube it, and then add one. Some examples:

$$3^3 + 1 = 27 + 1 = 28,$$
$$4^3 + 1 = 64 + 1 = 65,$$
$$5^3 + 1 = 125 + 1 = 126, \text{ and}$$
$$6^3 + 1 = 216 + 1 = 217.$$

Notice that the results are all composite. (Note that $217 = 7 \times 31$.) Try a few more examples on your own.

Let us try to convert this observation into a proposition for us to prove. Here's a first (but incorrect) draft: "If x is an integer, then $x^3 + 1$ is composite." This is a good start, but when we examine Definition 3.6, we note that the term *composite* applies only to positive integers. If x is negative, then $x^3 + 1$ is either negative or zero.

Fortunately, it's easy to repair the draft statement; here is a second version: "If x is a positive integer, then $x^3 + 1$ is composite." This looks better, but we're in trouble already when $x = 1$ because, in this case, $x^3 + 1 = 1^3 + 1 = 2$, which is prime. This makes us worry about the entire idea, but we note that when $x = 2$, $x^3 + 1 = 2^3 + 1 = 9$, which is composite, and we can try many other examples with $x > 1$ and always meet with success.

The case $x = 1$ turns out to be the only positive exception, and this leads us to a third (and correct) version of the proposition we wish to prove.

Proposition 5.4 Let x be an integer. If $x > 1$, then $x^3 + 1$ is composite.

Let's write down the basic outline of the proof.

> Let x be an integer and suppose $x > 1$.
> ...
> Therefore $x^3 + 1$ is composite. ■

To reach the conclusion that $x^3 + 1$ is composite, we need to find a factor of $x^3 + 1$ that is strictly between 1 and $x^3 + 1$. With luck, the word *factor* makes us think about factoring the polynomial $x^3 + 1$ as a polynomial. Recall from basic algebra that

$$x^3 + 1 = (x + 1)(x^2 - x + 1).$$

You might have the following concern: "I forgot that $x^3 + 1$ factors. How would I ever come up with this proof?" One idea is to look for patterns in the factors. We saw that $6^3 + 1 = 7 \times 31$, so $6^3 + 1$ is divisible by 7. Trying more examples, you may notice that $7^3 + 1$ is divisible by 8, $8^3 + 1$ is divisible by 9, $9^3 + 1$ is divisible by 10, and so on. With luck, that will help you realize that $x^3 + 1$ is divisible by $x + 1$, and then you can complete the factorization $x^3 + 1 = (x + 1) \times ?$.

This is the "Aha!" insight we need. Both $x + 1$ and $x^2 - x + 1$ are factors of $x^3 + 1$. For example, when $x = 6$, the factors $x + 1$ and $x^2 - x + 1$ evaluate to 7 and 31, respectively. Let's add this insight to our proof.

> Let x be an integer and suppose $x > 1$. Note that $x^3 + 1 = (x + 1)(x^2 - x + 1)$.
> ...
> Since $x + 1$ is a divisor of $x^3 + 1$, we have that $x^3 + 1$ is composite. ■

To correctly say that $x + 1$ is a divisor of $x^3 + 1$, we need the fact that both $x + 1$ and $x^2 - x + 1$ are integers. This is clear, because x itself is an integer. Let's be sure we include this detail in our proof.

> Let x be an integer and suppose $x > 1$. Note that $x^3 + 1 = (x + 1)(x^2 - x + 1)$. Because x is an integer, both $x + 1$ and $x^2 - x + 1$ are integers. Therefore $(x + 1) | (x^3 + 1)$.
> ...
> Since $x + 1$ is a divisor of $x^3 + 1$, we have that $x^3 + 1$ is composite. ■

The proof isn't quite finished yet. Consult Definition 3.6; we need that the divisor be strictly between 1 and $x^3 + 1$, and we have not proved that yet. So let's figure out what we need to do. We must prove

$$1 < x + 1 < x^3 + 1.$$

The first part is easy. Since $x > 1$, adding 1 to both sides gives

$$x + 1 > 1 + 1 = 2 > 1.$$

Showing that $x + 1 < x^3 + 1$ is only slightly more difficult. Working backward, to show $x + 1 < x^3 + 1$, it will be enough if we can prove that $x < x^3$. Notice that since $x > 1$, multiplying both sides by x gives $x^2 > x$, and since $x > 1$, we have $x^2 > 1$. Multiplying both sides of this by x gives $x^3 > x$. Let's take these ideas and add them to the proof.

Let x be an integer and suppose $x > 1$. Note that $x^3+1 = (x+1)(x^2-x+1)$. Because x is an integer, both $x + 1$ and $x^2 - x + 1$ are integers. Therefore $(x + 1)|(x^3 + 1)$.

Since $x > 1$, we have $x + 1 > 1 + 1 = 2 > 1$.

Also $x > 1$ implies $x^2 > x$, and since $x > 1$, we have $x^2 > 1$. Multiplying both sides by x again yields $x^3 > x$. Adding 1 to both sides gives $x^3 + 1 > x + 1$.

Thus $x + 1$ is an integer with $1 < x + 1 < x^3 + 1$.

Since $x + 1$ is a divisor of $x^3 + 1$ and $1 < x + 1 < x^3 + 1$, we have that $x^3 + 1$ is composite. ■

Proving If-and-Only-If Theorems

The basic technique for proving a statement of the form "A iff B" is to prove two if-then statements. We prove both "If A, then B" and "If B, then A." Here is an example:

Proposition 5.5 Let x be an integer. Then x is even if and only if $x + 1$ is odd.

The basic skeleton of the proof is as follows:

Let x be an integer.

($\Rightarrow$) Suppose x is even. . . . Therefore $x + 1$ is odd.

($\Leftarrow$) Suppose $x + 1$ is odd. . . . Therefore x is even. ■

Notice that we flag the two sections of the proof with the symbols ($\Rightarrow$) and ($\Leftarrow$). This lets the reader know which section of the proof is which.

Now we unravel the definitions at the front of each part of the proof. (Recall the definition of *odd*; see Definition 3.4 on page 5.)

Let x be an integer.

($\Rightarrow$) Suppose x is even. This means that $2|x$. Hence there is an integer a such that $x = 2a$. . . . Therefore $x + 1$ is odd.

($\Leftarrow$) Suppose $x + 1$ is odd. So there is an integer b such that $x + 1 = 2b + 1$. . . . Therefore x is even. ■

The next steps are clear. In the first part of the proof, we have $x = 2a$, and we want to prove $x + 1$ is odd. We just add 1 to both sides of $x = 2a$ to get $x + 1 = 2a + 1$, and that shows that $x + 1$ is odd.

In the second part of the proof, we know $x + 1 = 2b + 1$, and we want to prove that x is even. We subtract 1 from both sides and we are finished.

Let x be an integer.

($\Rightarrow$) Suppose x is even. This means that $2|x$. Hence there is an integer a such that $x = 2a$. Adding 1 to both sides gives $x + 1 = 2a + 1$. By the definition of *odd*, $x + 1$ is odd.

($\Leftarrow$) Suppose $x + 1$ is odd. So there is an integer b such that $x + 1 = 2b + 1$. Subtracting 1 from both sides gives $x = 2b$. This shows that $2|x$ and therefore x is even. ■

Proof Template 2 shows the basic method for proving an if-and-only-if theorem.

Proof Template 2 Direct proof of an if-and-only-if theorem.

To prove a statement of the form "A iff B":

- ($\Rightarrow$) Prove "If A, then B."
- ($\Leftarrow$) Prove "If B, then A."

When is it safe to skip steps?

As you become more comfortable writing proofs, you may find yourself getting bored writing the same steps over and over again. We have seen the sequence (1) x is even, so (2) x is divisible by 2, so (3) there is an integer a such that $x = 2a$ several times already. You may be tempted to skip step (2) and just write "x is even, so there is an integer a such that $x = 2a$." The decision about skipping steps requires some careful judgment, but here are some guidelines.

- Would it be easy (and perhaps boring) for you to fill in the missing steps? Are the missing steps obvious? If you answer yes, then omit the steps.
- Does the same sequence of steps appear several times in your proof(s), but the sequence of steps is not very easy to reconstruct? Here you have two choices:
  - Write the sequence of steps out once, and the next time the same sequence appears, use an expression such as "as we saw before" or "likewise."
  - Alternatively, if the consequence of the sequence of steps can be described in a statement, first prove that statement, calling it a *lemma*. Then invoke (refer to) your lemma whenever you need to repeat those steps.
- When in doubt, write it out.

Let us illustrate the idea of explicitly separating off a portion of a proof into a lemma. Consider the following statement.

Proposition 5.6 Let a, b, c, and d be integers. If $a|b$, $b|c$, and $c|d$, then $a|d$.

Here is the proof as suggested by Proof Template 1.

Let a, b, c, and d be integers with $a|b$, $b|c$, and $c|d$.
Since $a|b$, there is an integer x such that $ax = b$.
Since $b|c$, there is an integer y such that $by = c$.
Since $c|d$, there is an integer z such that $cz = d$.
Note that $a(xyz) = (ax)(yz) = b(yz) = (by)z = cz = d$.
Therefore there is an integer $w = xyz$ such that $aw = d$.
Therefore $a|d$. ■

There is nothing wrong with this proof, but there is a simpler, less verbose way to handle it. We have already shown that $a|b,\ b|c \Rightarrow a|c$ in Proposition 5.3. Let us use this proposition to prove Proposition 5.6.

Here is the alternative proof.

Let a, b, c, and d be integers with $a|b$, $b|c$, and $c|d$.
Since $a|b$ and $b|c$, by Proposition 5.3 we have $a|c$.
Now, since $a|c$ and $c|d$, again by Proposition 5.3 we have $a|d$. ■

The key idea is to use Proposition 5.3 twice. Once it was applied to a, b, and c to get $a|c$. When we have established that $a|c$, we can use Proposition 5.3 again on the integers a, c, and d to finish the proof.

Proposition 5.3 serves as a lemma in the proof of Proposition 5.6.

Proving Equations and Inequalities

The basic algebraic manipulations you already know are valid steps in a proof. It is not necessary for you to prove that $x + x = 2x$ or that $x^2 - y^2 = (x - y)(x + y)$. In your proofs, feel free to use standard algebraic steps without detailed comment.

However, even these simple facts can be proved using the fundamental properties of numbers and operations (see Appendix D). We show how here, simply to illustrate that algebraic manipulations can be justified in terms of more basic principles.

For $x + x = 2x$:

$$\begin{aligned} x + x &= 1 \cdot x + 1 \cdot x && \text{1 is the identity element for multiplication} \\ &= (1 + 1)x && \text{distributive property} \\ &= 2x && \text{because } 1 + 1 = 2. \end{aligned}$$

For $(x - y)(x + y) = x^2 - y^2$:

$$\begin{aligned} (x - y)(x + y) &= x(x + y) - y(x + y) && \text{distributive property} \\ &= x^2 + xy - yx - y^2 && \text{distributive property} \\ &= x^2 + xy - xy - y^2 && \text{commutative property for multiplication} \\ &= x^2 + 1xy - 1xy - y^2 && \text{1 is the identity element for multiplication} \\ &= x^2 + (1 - 1)xy - y^2 && \text{distributive property} \\ &= x^2 + 0xy - y^2 && \text{because } 1 - 1 = 0 \\ &= x^2 + 0 - y^2 && \text{because anything multiplied by 0 is 0} \\ &= x^2 - y^2 && \text{0 is the identity element for addition.} \end{aligned}$$

Working with inequalities may be less familiar, but the basic steps are the same. For example, suppose you are asked to prove the following statement: If $x > 2$ then $x^2 > x + 1$. Here is a proof:

We need to comment that x is positive because multiplying both sides of an inequality by a negative number reverses the inequality.

Proof. We are given that $x > 2$. Since x is positive, multiplying both sides by x gives $x^2 > 2x$. So we have

$$\begin{aligned} x^2 &> 2x \\ &= x + x \\ &> x + 2 && \text{because } x > 2 \\ &> x + 1 && \text{because } 2 > 1. \end{aligned}$$

Therefore, by transitivity, $x^2 > x + 1$. ■

See the discussion of Ordering in Appendix D for a review of *transitivity*.

Recap

We introduced the concept of proof and presented the basic technique of writing a direct proof for an if-then statement. For if-and-only-if statements, we apply this basic technique to both the forward ($\Rightarrow$) and the backward ($\Leftarrow$) implications.

5 Exercises

5.1. Prove that the sum of two odd integers is even.
5.2. Prove that the sum of an odd integer and an even integer is odd.
5.3. Prove that if n is an odd integer, then $-n$ is also odd.
5.4. Prove that the product of two even integers is even.
5.5. Prove that the product of an even integer and an odd integer is even.
5.6. Prove that the product of two odd integers is odd.
5.7. Prove that the square of an odd integer is odd.
5.8. Prove that the cube of an odd integer is odd.
5.9. Suppose a, b, and c are integers. Prove that if $a|b$ and $a|c$, then $a|(b + c)$.
5.10. Suppose a, b, and c are integers. Prove that if $a|b$, then $a|(bc)$.
5.11. Suppose a, b, d, x, and y are integers. Prove that if $d|a$ and $d|b$, then $d|(ax + by)$.
5.12. Suppose a, b, c, and d are integers. Prove that if $a|b$ and $c|d$, then $(ac)|(bd)$.

Note that Exercise 5.14 provides an alternative to Definition 3.4. To show that a number x is odd we can either look for an integer a so that $x = 2a + 1$ (using the definition) or we can look for an integer b so that $x = 2b - 1$ (using the result you prove here).

5.13. Let x be an integer. Prove that x is odd if and only if $x + 1$ is even.

5.14. Let x be an integers. Prove that x is odd if and only if there is an integer b such that $x = 2b - 1$.

5.15. Let x be an integer. Prove that $0|x$ if and only if $x = 0$.

5.16. Let a and b be integers. Prove that $a < b$ if and only if $a \leq b - 1$.

5.17. Let a be a number with $a > 1$. Prove that a number x is strictly between 1 and $\sqrt{a}$ if and only if a/x is strictly between $\sqrt{a}$ and a.

You may assume that $1 < \sqrt{a} < a$. (We ask you to prove this later; see Exercise 20.10.)

By *consecutive perfect squares* we mean numbers such as 3^2 and 4^2 or 12^2 and 13^2.

5.18. Prove that the difference between consecutive perfect squares is odd.

5.19. Let a be a perfect square. Prove that a is the square on a nonnegative integer.

5.20. For real numbers a and b, prove that if $0 < a < b$, then $a^2 < b^2$.

5.21. Prove that the difference between distinct, nonconsecutive perfect squares is composite.

5.22. Prove that an integer is odd if and only if it is the sum of two consecutive integers.

5.23. Suppose you are asked to prove a statement of the form "If A or B, then C." Explain why you need to prove (a) "If A, then C" and also (b) "If B, then C." Why is it not enough to prove only one of (a) and (b)?

5.24. Suppose you are asked to prove a statement of the form "A iff B." The standard method is to prove both $A \Rightarrow B$ and $B \Rightarrow A$.

Consider the following alternative proof strategy: Prove both $A \Rightarrow B$ and (not A) $\Rightarrow$ (not B). Explain why this would give a valid proof.

6 Counterexample

In the previous section, we developed the notion of proof: a technique to demonstrate irrefutably that a given statement is true. Not all statements about mathematics are true! Given a statement, how do we show that it is false? Disproving false statements is often simpler than proving theorems. The typical way to disprove an if-then statement is to create a *counterexample*. Consider the statement "If A, then B." A counterexample to such a statement would be an instance where A is true but B is false.

For example, consider the statement "If x is a prime, then x is odd." This statement is false. To prove that it is false, we just have to give an example of an integer that is prime but is not odd. The integer 2 has the requisite properties.

Let's consider another false statement.

Statement 6.1 **(false)** Let a and b be integers. If $a|b$ and $b|a$, then $a = b$.

This statement appears plausible. It seems that if $a|b$, then $a \leq b$, and if $b|a$, then $b \leq a$, and so $a = b$. But this reasoning is incorrect.

To disprove Statement 6.1, we need to find integers a and b that, on the one hand, satisfy $a|b$ and $b|a$ but, on the other hand, do not satisfy $a = b$.

Here is a counterexample: Take $a = 5$ and $b = -5$. To check that this is a counterexample, we simply note that, on the one hand, $5|-5$ and $-5|5$ but, on the other hand, $5 \neq -5$.

Proof Template 3 Refuting a false if-then statement via a counterexample.

To disprove a statement of the form "If A, then B":

Find an instance where A is true but B is false.

Refuting false statements is usually easier than proving true statements. However, finding counterexamples can be tricky. To create a counterexample, I recommend you try creating several instances where the hypothesis of the statement is true and check each to see whether or not the conclusion holds. All it takes is one counterexample to disprove a statement.

Unfortunately, it is easy to get stuck in a thinking rut. For Statement 6.1, we might consider $3|3$ and $4|4$ and $5|5$ and never think about making one number positive and the other negative.

Try to break out of such a rut by creating strange examples. Don't forget about the number 0 (which acts strangely) and negative numbers. Of course, following that advice, we might still be stuck in the rut $0|0, -1|-1, -2|-2$, and so on.

A strategy for finding counterexamples.

Here is a strategy for finding counterexamples. Begin by trying to prove the statement; when you get stuck, try to figure out what the problem is and look there to build a counterexample.

Let's apply this technique to Statement 6.1. We start, as usual, by converting the hypothesis and conclusion of the statement into the beginning and end of the proof.

> Let a and b be integers with $a|b$ and $b|a$. . . . Therefore $a = b$. ■

Next we unravel definitions.

> Let a and b be integers with $a|b$ and $b|a$. Since $a|b$, there is an integer x such that $b = ax$. Since $b|a$, there is an integer y such that $a = by$. . . . Therefore $a = b$. ■

Now we ask: What do we know? What do we need? We know

$$b = ax \qquad \text{and} \qquad a = by$$

and we want to show $a = b$. To get there, we can try to show that $x = y = 1$. Let's try to solve for x or y.

Since we have two expressions in terms of a and b, we can try substituting one in the other. We use the fact that $b = ax$ to eliminate b from $a = by$. We get

$$a = by \quad \Rightarrow \quad a = (ax)y \quad \Rightarrow \quad a = (xy)a.$$

It now looks quite tempting to divide both sides of the last equation by a, but we need to worry that perhaps, $a = 0$. Let's ignore the possibility of $a = 0$ for just a moment and go ahead and write $xy = 1$. We see that we have two integers whose product is 1. And we realize at this point that there are two ways that can happen: either $1 = 1 \times 1$ or $1 = -1 \times -1$. So although we know $xy = 1$, we can't conclude that $x = y = 1$ and finish the proof. We're stuck and now we consider the possibility that Statement 6.1 is false. We ask: What if $x = y = -1$? We see that this would imply that $a = -b$; for example, $a = 5$ and $b = -5$. And then we realize that in such a case, $a|b$ and $b|a$ but $a \neq b$. We have found a counterexample. Do we need to go back to our worry that perhaps $a = 0$? No! We have refuted the statement with our counterexample. The attempted proof served only to help us find a counterexample.

Recap

This section showed how to disprove an if-then statement by finding an example that satisfies the hypothesis of the statement but not the conclusion.

6 Exercises

6.1. Disprove: If a and b are integers with $a|b$, then $a \leq b$.

6.2. Disprove: If a and b are nonnegative integers with $a|b$, then $a \leq b$.
Note: A counterexample to this statement would also be a counterexample for the previous problem, but not necessarily vice versa.

6.3. Disprove: If a, b, and c are positive integers with $a|(bc)$, then $a|b$ or $a|c$.

6.4. Disprove: If a, b, and c are positive integers, then $a^{(b^c)} = (a^b)^c$.

6.5. Disprove: If p and q are prime, then $p + q$ is composite.

6.6. Disprove: If p is prime, then $2^p - 1$ is also prime.

6.7. Disprove: If n is a nonnegative integer, then $2^{(2^n)} + 1$ is prime.

6.8. An integer is a *palindrome* if it reads the same forwards and backwards when expressed in base-10. For example, 1331 is a palindrome.
Disprove: All palindromes with two or more digits are divisible by 11.

6.9. Consider the polynomial $n^2 + n + 41$.
(a) Calculate the value of this polynomial for $n = 1, 2, 3, \ldots, 10$.
Notice that all the numbers you computed are prime.
(b) Disprove: If n is a positive integer, then $n^2 + n + 41$ is prime.