Chapter 9

Direct Proof

A *proof* is a written verification that a mathematical statement is true.

The idea of a proof is paramount. In order to make true progress in mathematics, you must acquire the ability to read, write and understand proofs. Therefore, studying this topic is essential.

There are various strategies for writing proofs. This chapter introduces the most straightforward one, a method called *direct proof*. As we begin, it is important to keep in mind the meanings of three key terms: *Theorem*, *proof* and *definition*.

A **theorem** is a mathematical statement that is true and can be (and has been) verified as true. A **proof** of a theorem is a written verification that shows that the theorem is definitely and unequivocally true. A proof should be understandable and convincing to anyone who has the requisite background and knowledge. This knowledge includes an understanding of the meanings of the mathematical words, phrases and symbols that occur in the theorem and its proof. It is crucial that both the writer of the proof and the readers of the proof agree on the exact meanings of all the words, for otherwise there is an intolerable level of ambiguity. A **definition** is an exact, unambiguous explanation of the meaning of a mathematical word or phrase. We will elaborate on the terms *theorem* and *definition* in the next two sections, and then finally we will be ready to begin writing proofs.

9.1 Theorems

A **theorem** is a statement that is true and has been proved to be true. You have encountered many theorems in your mathematical education. Here are some theorems taken from an undergraduate calculus text. They will be familiar to you, though you may not have read all the proofs.

> **Theorem:** Let f be differentiable on an open interval I and let $c \in I$. If $f(c)$ is the maximum or minimum value of f on I, then $f'(c) = 0$.

> **Theorem:** If $\sum_{k=1}^{\infty} a_k$ converges, then $\lim_{k\to\infty} a_k = 0$.

> **Theorem:** Suppose f is continuous on the interval $[a, b]$. Then f is integrable on $[a, b]$.

Theorem: Every polynomial of odd degree has a real solution.

Observe that each of these theorems either has the conditional form *"If P, then Q,"* or can be put into that form. The first theorem has an initial sentence *"Let f be differentiable on an open interval I, and let $c \in I$,"* which sets up some notation, but a conditional statement follows it. The third theorem has form *"Suppose P. Then Q,"* but this means the same thing as *"If P, then Q."* The last theorem can be re-expressed as *"If a polynomial has odd degree, then it has a real solution."*

A theorem of form *"If P, then Q,"* can be regarded as a device that produces new information from P. Whenever we are dealing with a situation in which P is true, then the theorem guarantees that, in addition, Q is true. Since this kind of expansion of information is useful, theorems of form *"If P, then Q,"* are very common.

But not *every* theorem is a conditional statement. Some have the form of the biconditional $P \Leftrightarrow Q$, but, as we know, that can be expressed as *two* conditional statements. Other theorems simply state facts about specific things. For example, here is another theorem from your study of calculus.

Theorem: The number $\sqrt{2}$ is irrational.

It would be difficult (or at least awkward) to restate this as a conditional statement. Still, it is true that most theorems *are* conditional statements, so we will focus attention that type of theorem.

It is important to be aware that there are a number of words that mean essentially the same thing as the word "theorem," but are used in slightly different ways. In general the word "theorem" is reserved for a statement that is considered important or significant (the Pythagorean theorem, for example). A statement that is true but not as significant is sometimes called a **proposition**. A **lemma** is a theorem whose main purpose is to help prove another theorem. A **corollary** is a result that is an immediate consequence of a theorem or proposition. It is not important that you remember all these words now, for their meanings will become clear with usage.

Our main task is to learn how to prove theorems. As the above examples suggest, proving theorems requires a clear understanding of the conditional statement, and that is the primary reason we studied it so extensively in Chapters 3 and 5. It is also crucial to understand the role of definitions.

9.2 Definitions

A proof of a theorem should be absolutely convincing. Ambiguity must be avoided. Everyone must agree on the exact meaning of each mathematical term. Chapter 2 defined the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$ and $\emptyset$, as well as the meanings of the symbols $\in$ and $\subseteq$, and we shall make frequent use of these things. Here is another definition that we use often.

Definition 9.1. An integer n is **even** if $n = 2a$ for some integer $a \in \mathbb{Z}$.

Thus, for example, 10 is even because $10 = 2 \cdot 5$. Also, according to the definition, 7 is not even because there is no integer a for which $7 = 2a$. While there would be nothing wrong with defining an integer to be odd if it's not even, the following definition is more concrete.

Definition 9.2. An integer n is **odd** if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.

Thus 7 is odd because $7 = 2 \cdot 3 + 1$. We will use these definitions whenever the concept of even or odd numbers arises. If in a proof a certain number turns out to be even, the definition allows us to write it as $2a$ for an appropriate integer a. If some quantity has form $2b + 1$ where b is an integer, then the definition tells us the quantity is odd.

Definition 9.3. Two integers have the **same parity** if they are both even or they are both odd. Otherwise they have **opposite parity**.

Thus 6 and 4 have the same parity, but 3 and 4 have opposite parity.

Two points about definitions are in order. First, in this book the word or term being defined appears in boldface type. Second, it is common to express definitions as conditional statements even though the biconditional would more appropriately convey the meaning. Consider the definition of an even integer. You understand full well that if n is even then $n = 2a$ (for $a \in \mathbb{Z}$), *and* if $n = 2a$, then n is even. Thus, technically the definition should read *"An integer n is even if and only if $n = 2a$ for some $a \in \mathbb{Z}$."* However, it is an almost-universal convention that definitions are phrased in the conditional form, even though they are interpreted as being in the biconditional form. There is really no good reason for this, other than economy of words. It is the standard way of writing definitions, and we have to get used to it.

Here is another definition that we will use often.

Definition 9.4. Suppose a and b are integers. We say a **divides** b, written $a \mid b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that a is a **divisor** of b, and that b is a **multiple** of a.

For example, 5 divides 15 because $15 = 5 \cdot 3$. We write this as $5 \mid 15$. Similarly $8 \mid 32$ because $32 = 8 \cdot 4$, and $-6 \mid 6$ because $6 = -6 \cdot -1$. However, 6 does not divide 9 because there is no integer c for which $9 = 6 \cdot c$. We express this as $6 \nmid 9$, which we read as *"6 does not divide 9."*

Be careful of your interpretation of the symbols. There is a big difference between the expressions $a \mid b$ and a/b. The expression $a \mid b$ is a *statement*, while a/b is a fraction. For example, $8 \mid 16$ is true and $8 \mid 20$ is false. By contrast, $8/16 = 0.5$ and $8/20 = 0.4$ are numbers, not statements. Be careful not to write one when you mean the other.

Every integer has a set of integers that divide it. The set of divisors of 6 is $\{a \in \mathbb{Z} : a \mid 6\} = \{-6, -3, -2, -1, 1, 2, 3, 6\}$. The set of divisors of 5 is $\{-5, -1, 1, 5\}$. The set of divisors of 0 is $\mathbb{Z}$. This brings us to the following definition, with which you are already familiar.

Definition 9.5. A natural number n is **prime** if and only if it has exactly two positive divisors, 1 and n.

For example, 2 is prime, as are 5 and 17. The definition implies that 1 is not prime, as it only has one (not two) positive divisor, namely 1. An integer n is **composite** if it factors as $n = ab$ where $a, b > 1$.

Definition 9.6. The **greatest common divisor** of integers a and b, denoted $\gcd(a, b)$, is the largest integer that divides both a and b.

The **least common multiple** of two non-zero integers a and b, denoted $\text{lcm}(a, b)$, is the smallest positive integer that is a multiple of both a and b.

So $\gcd(18, 24) = 6$, $\gcd(5, 5) = 5$ and $\gcd(32, -8) = 8$. Also $\gcd(50, 18) = 2$, but $\gcd(50, 9) = 1$. Note that $\gcd(0, 6) = 6$, because, although every integer divides 0, the largest divisor of 6 is 6.

The expression $\gcd(0, 0)$ is problematic. Every integer divides 0, so the only conclusion is that $\gcd(0, 0) = \infty$. We circumvent this irregularity by simply agreeing to consider $\gcd(a, b)$ only when a and b are not both zero.

Continuing our examples, $\text{lcm}(4, 6) = 12$, and $\text{lcm}(7, 7) = 7$.

Of course not all terms can be defined. If every word in a definition were defined, there would be separate definitions for the words that appeared in those definitions, and so on, until the chain of defined terms became circular. Thus we accept some ideas as being so intuitively clear that they require no definitions or verifications. For example, we will not find it necessary to define what an integer (or a real number) is. Nor will we define addition, multiplication, subtraction and division, though we will use these operations freely. We accept and use such things as the distributive and commutative properties of addition and multiplication, as well as other standard properties of arithmetic and algebra.

As mentioned in Section 2.9, we accept as fact the natural ordering of the elements of $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$, so that (for example) statements such as "$5 < 7$," and "$x < y$ implies $-x > -y$," do not need to be justified.

In addition, we accept the following fact without justification or proof.

Fact 9.1. Suppose a and b are integers. Then:

- $a + b \in \mathbb{Z}$
- $a - b \in \mathbb{Z}$
- $ab \in \mathbb{Z}$

These three statements can be combined. For example, we see that if a, b and c are integers, then $a^2b - ca + b$ is also an integer.

We will also accept as obvious the fact that any integer a can be divided by a non-zero integer b, resulting in a unique quotient q and remainder r. For example, $b = 3$ goes into $a = 17$ $q = 5$ times with remainder $r = 2$. In symbols, $17 = 5 \cdot 3 + 2$, or $a = qb + r$. This fact, called the *division algorithm*, was mentioned on page 215 (Fact 8.1).

(The Division Algorithm) Given integers a and b with $b > 0$, there exist unique integers q and r for which $a = qb + r$ and $0 \leq r < b$.

Another fact that we will accept without proof (at least for now) is that every natural number greater than 1 has a unique factorization into primes. For example, the number 1176 can be factored into primes as $1176 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 \cdot 7 = 2^3 \cdot 3 \cdot 7^2$. By *unique* we mean that *any* factorization of 1176 into primes will have exactly the same factors (i.e., three 2's, one 3 and two 7's). Thus, for example, there is no valid factorization of 1176 that has a factor of 5, because the above factoring of 1176 does not have a factor of 5. You may be so used to factoring numbers into primes that it seems obvious that there cannot be different prime factorizations of the same number, but in fact this is a fundamental result whose proof is not transparent. Nonetheless, we will be content to assume that every natural number greater than 1 has a unique factorization into primes. (We will revisit the issue of a proof in Section 15.3.)

We will introduce other accepted facts, as well as definitions, as needed.

9.3 Direct Proof

This section explains a simple way to prove theorems or propositions that have the form of conditional statements. The technique is called **direct proof**. To simplify the discussion, our first examples will involve proving statements that are almost obviously true. Thus we will call the statements *propositions* rather than theorems. (Remember, a proposition is a statement that, although true, is not as significant as a theorem.)

To understand how the technique of direct proof works, suppose we have some proposition of the following form.

Proposition. If P, then Q.

This proposition is a conditional statement of form $P \Rightarrow Q$. Our goal is to show that this conditional statement is true. To see how to proceed, look at its truth table.

P	Q	$P \Rightarrow Q$
T	T	T
T	F	**F**
F	T	T
F	F	T

The table shows that if P is false, the statement $P \Rightarrow Q$ is automatically true. This means that if we are concerned with showing $P \Rightarrow Q$ is true, we don't have to worry about the situations where P is false (as in the last two lines of the table) because the statement $P \Rightarrow Q$ will be automatically true in those cases. But we must be very careful about the situations where P is true (as in the first two lines of the table). We must show that the condition of P being true forces Q to be true also, for that means the second line of the table cannot happen.

This gives a fundamental outline for proving statements of the form $P \Rightarrow Q$. Begin by assuming that P is true (remember, we don't need to worry about P being false) and show this forces Q to be true. We summarize this as follows.

Outline for Direct Proof

Proposition. If P, then Q.

Proof. Suppose P.

⋮

⋮

Therefore Q. □

So the setup for direct proof is remarkably simple. The first line of the proof is the sentence *"Suppose P."* The last line is the sentence *"Therefore Q."* Between the first and last line we use logic, definitions and standard math facts to transform the statement P to the statement Q. It is common to use the word "*Proof*" to indicate the beginning of a proof, and the symbol □ to indicate the end.

As our first example, let's prove that if x is odd then x^2 is also odd. (Granted, this is not a terribly impressive result, but we will move on to more significant things in due time.) The first step in the proof is to fill in the outline for direct proof. This is a lot like painting a picture, where the basic structure is sketched in first. We leave some space between the first and last line of the proof. The following series of frames indicates the steps you might take to fill in this space with a logical chain of reasoning.

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

Proof. Suppose x is odd.

Therefore x^2 is odd. □

Now that we have written the first and last lines, we need to fill in the space with a chain of reasoning that shows that x being odd forces x^2 to be odd.

In doing this it's always advisable to use any definitions that apply. The first line says x is odd, and by Definition 9.2 it must be that $x = 2a + 1$ for some $a \in \mathbb{Z}$, so we write this in as our second line.

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

Proof. Suppose x is odd.
Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by definition of an odd number.

Therefore x^2 is odd. □

Now jump down to the last line, which says x^2 is odd. Think about what the line immediately above it would have to be in order for us to conclude that x^2 is odd. By the definition of an odd number, we would have to have $x^2 = 2a+1$ for some $a \in \mathbb{Z}$. However, the symbol a now appears earlier in the proof in a different context, so we should use a different symbol, say b.

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

Proof. Suppose x is odd.
Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by definition of an odd number.

Thus $x^2 = 2b + 1$ for an integer b.
Therefore x^2 is odd, *by definition of an odd number.* □

We are almost there. We can bridge the gap as follows.

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

Proof. Suppose x is odd.
Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by definition of an odd number.
Thus $x^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$.
So $x^2 = 2b + 1$ where b is the integer $b = 2a^2 + 2a$.
Thus $x^2 = 2b + 1$ for an integer b.
Therefore x^2 is odd, by definition of an odd number. □

Finally, we may wish to clean up our work and write the proof in paragraph form. Here is our final version.

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

Proof. Suppose x is odd. Then $x = 2a+1$ for some $a \in \mathbb{Z}$, by definition of an odd number. Thus $x^2 = (2a+1)^2 = 4a^2+4a+1 = 2(2a^2+2a)+1$, so $x^2 = 2b+1$ where $b = 2a^2+2a \in \mathbb{Z}$. Therefore x^2 is odd, by definition of an odd number. □

At least initially, it's a good idea to write the first and last line of your proof first, and then fill the gap, jumping alternately between top and bottom until you meet in the middle, as we did above. This way you are constantly reminded that you are aiming for the statement at the bottom. Sometimes you will leave too much space, sometimes not enough. Sometimes you will get stuck before figuring out what to do. This is normal. Mathematicians do scratch work just as artists do sketches for paintings.

Here is another example. Consider proving the following proposition.

Proposition. Let a, b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Let's apply the basic outline for direct proof. To clarify the procedure we will write the proof in stages again.

Proposition. Let a, b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Suppose $a \mid b$ and $b \mid c$.

Therefore $a \mid c$. □

Our first step is to apply Definition 9.4 to the first line. The definition says $a \mid b$ means $b = ac$ for some integer c, but since c already appears in a different context on the first line, we must use a different letter, say d. Similarly let's use a new letter e in the definition of $b \mid c$.

Proposition. Let a, b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Suppose $a \mid b$ and $b \mid c$.
By Definition 9.4, we know $a \mid b$ means there is an integer d with $b = ad$. Likewise, $b \mid c$ means there is an integer e for which $c = be$.

Therefore $a \mid c$. □

We have almost bridged the gap. The line immediately above the last line should show that $a \mid c$. According to Definition 9.4, this line should say that $c = ax$ for some integer x. We can get this equation from the lines at the top, as follows.

Proposition. Let a, b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Suppose $a \mid b$ and $b \mid c$.
By Definition 9.4, we know $a \mid b$ means there is an integer d with $b = ad$.
Likewise, $b \mid c$ means there is an integer e for which $c = be$.
Thus $c = be = (ad)e = a(de)$, *so* $c = ax$ *for the integer* $x = de$.
Therefore $a \mid c$. □

The next example is presented all at once rather than in stages.

Proposition. If x is an even integer, then $x^2 - 6x + 5$ is odd.

Proof. Suppose x is an even integer.
Then $x = 2a$ for some $a \in \mathbb{Z}$, by definition of an even integer.
So $x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5 = 4a^2 - 12a + 5 = 4a^2 - 12a + 4 + 1 = 2(2a^2 - 6a + 2) + 1$.
Therefore we have $x^2 - 6x + 5 = 2b + 1$, where $b = 2a^2 - 6a + 2 \in \mathbb{Z}$.
Consequently $x^2 - 6x + 5$ is odd, by definition of an odd number. □

One doesn't normally use a separate line for each sentence in a proof, but for clarity we will often do this for the next few chapters.

Our next example illustrates a standard technique for showing two quantities are equal. If we can show $m \leq n$ and $n \leq m$ then it follows that $m = n$. In general, the reasoning involved in showing $m \leq n$ can be quite different from that of showing $n \leq m$.

Recall Definition 9.6 of a least common multiple on page 242.

Proposition. If $a, b, c \in \mathbb{N}$, then $\text{lcm}(ca, cb) = c \cdot \text{lcm}(a, b)$.

Proof. Assume $a, b, c \in \mathbb{N}$. Let $m = \text{lcm}(ca, cb)$ and $n = c \cdot \text{lcm}(a, b)$. We will show $m = n$. By definition, $\text{lcm}(a, b)$ is a multiple of both a and b, so $\text{lcm}(a, b) = ax = by$ for some $x, y \in \mathbb{Z}$. From this we see that $n = c \cdot \text{lcm}(a, b) = cax = cby$ is a multiple of both ca and cb. But $m = \text{lcm}(ca, cb)$ is the *smallest* multiple of both ca and cb. Thus $m \leq n$.

On the other hand, as $m = \text{lcm}(ca, cb)$ is a multiple of both ca and cb, we have $m = cax = cby$ for some $x, y \in \mathbb{Z}$. Then $\frac{1}{c}m = ax = by$ is a multiple of both a and b. Therefore $\text{lcm}(a, b) \leq \frac{1}{c}m$, so $c \cdot \text{lcm}(a, b) \leq m$, that is, $n \leq m$.

We've shown $m \leq n$ and $n \leq m$, so $m = n$. The proof is complete. □

The examples we've looked at so far have all been proofs of statements about integers. In our next example, we are going to prove that if x and y are positive real numbers for which $x \leq y$, then $\sqrt{x} \leq \sqrt{y}$. You may feel that the proof is not as "automatic" as the proofs we have done so far. Finding the right steps in a proof can be challenging, and that is part of the fun.

Proposition. Let x and y be positive numbers. If $x \leq y$, then $\sqrt{x} \leq \sqrt{y}$.

Proof. Suppose $x \leq y$. Subtracting y from both sides gives $x - y \leq 0$.
This can be written as $\sqrt{x}^2 - \sqrt{y}^2 \leq 0$.
Factor this to get $(\sqrt{x} - \sqrt{y})(\sqrt{x} + \sqrt{y}) \leq 0$.
Dividing both sides by the positive number $\sqrt{x} + \sqrt{y}$ produces $\sqrt{x} - \sqrt{y} \leq 0$.
Adding $\sqrt{y}$ to both sides gives $\sqrt{x} \leq \sqrt{y}$. □

This proposition tells us that whenever $x \leq y$, we can take the square root of both sides and be assured that $\sqrt{x} \leq \sqrt{y}$. This can be useful, as we will see in our next proposition.

That proposition will concern the expression $2\sqrt{xy} \leq x + y$. Notice when you substitute random positive values for the variables, the expression is true. For example, for $x = 6$ and $y = 4$, the left side is $2\sqrt{6 \cdot 4} = 4\sqrt{6} \approx 9.79$, which is less than the right side $6 + 4 = 10$. Is it true that $2\sqrt{xy} \leq x + y$ for any positive x and y? How could we prove it?

To see how, let's first cast this into the form of a conditional statement: If x and y are positive real numbers, then $2\sqrt{xy} \leq x + y$. The proof begins with the assumption that x and y are positive, and ends with $2\sqrt{xy} \leq x + y$. In mapping out a strategy, it can be helpful to work backwards, working from $2\sqrt{xy} \leq x + y$ to something that is obviously true. Then the steps can be reversed in the proof. In this case, squaring both sides of $2\sqrt{xy} \leq x + y$ gives us

$$4xy \leq x^2 + 2xy + y^2.$$

Now subtract $4xy$ from both sides and factor.

$$0 \leq x^2 - 2xy + y^2$$
$$0 \leq (x - y)^2$$

But this last line is clearly true, since the square of $x - y$ cannot be negative! This gives us a strategy for the proof, which follows.

Proposition. If x and y are positive real numbers, then $2\sqrt{xy} \leq x + y$.

Proof. Suppose x and y are positive real numbers.
Then $0 \leq (x - y)^2$, that is, $0 \leq x^2 - 2xy + y^2$.
Adding $4xy$ to both sides gives $4xy \leq x^2 + 2xy + y^2$.
Factoring yields $4xy \leq (x + y)^2$.
Previously we proved that such an inequality still holds after taking the square root of both sides; doing so produces $2\sqrt{xy} \leq x + y$. □

Notice that in the last step of the proof we took the square root of both sides of $4xy \leq (x+y)^2$ and got $\sqrt{4xy} \leq \sqrt{(x+y)^2}$, and the fact that this did not reverse the symbol $\leq$ followed from our previous proposition. This is an important point. Often the proof of a proposition or theorem uses another proposition or theorem (that has already been proved).

9.4 Using Cases

In proving a statement is true, we sometimes have to examine multiple cases before showing the statement is true in all possible scenarios. This section illustrates a few examples.

Our examples will concern the expression $1 + (-1)^n(2n-1)$. Here is a table showing its value for various integers for n. Notice that $1 + (-1)^n(2n-1)$ is a multiple of 4 in every line.

n	$1 + (-1)^n(2n-1)$
1	0
2	4
3	-4
4	8
5	-8

Is $1 + (-1)^n(2n-1)$ always a multiple of 4? We prove the answer is "yes" in our next example. Notice, however, that the expression $1 + (-1)^n(2n-1)$ behaves differently depending on whether n is even or odd, for in the first case $(-1)^n = 1$, and in the second $(-1)^n = -1$. Thus the proof must examine these two possibilities separately.

Proposition. If $n \in \mathbb{N}$, then $1 + (-1)^n(2n-1)$ is a multiple of 4.

Proof. Suppose $n \in \mathbb{N}$.
Then n is either even or odd. Let's consider these two cases separately.

Case 1. Suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$, and $(-1)^n = 1$.
Thus $1 + (-1)^n(2n-1) = 1 + (1)(2 \cdot 2k - 1) = 4k$, which is a multiple of 4.

Case 2. Suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$, and $(-1)^n = -1$.
Thus $1 + (-1)^n(2n-1) = 1 - (2(2k+1) - 1) = -4k$, which is a multiple of 4.

These cases show that $1 + (-1)^n(2n-1)$ is always a multiple of 4. □

Now let's examine the flip side of the question. We just proved $1+(-1)^n(2n-1)$ is always a multiple of 4, but can we get *every* multiple of 4 this way? The following proposition and proof give an affirmative answer.

Proposition. Every multiple of 4 equals $1 + (-1)^n(2n-1)$ for some $n \in \mathbb{N}$.

Proof. In conditional form, the proposition is as follows:
If k is a multiple of 4, then there is an $n \in \mathbb{N}$ for which $1 + (-1)^n(2n-1) = k$.
What follows is a proof of this conditional statement.
Suppose k is a multiple of 4. This means $k = 4a$ for some integer a.
We must produce an $n \in \mathbb{N}$ for which $1 + (-1)^n(2n-1) = k$.
This is done by cases, depending on whether a is zero, positive or negative.
Case 1. Suppose $a = 0$. If $n = 1$, then $1 + (-1)^n(2n-1) = 1 + (-1)^1(2-1) = 0 = 4{\cdot}0 = 4a = k$.
Case 2. Suppose $a > 0$. Let $n = 2a$, which is in $\mathbb{N}$ because a is positive. Also n is even, so $(-1)^n = 1$. Thus $1 + (-1)^n(2n-1) = 1 + (2n-1) = 2n = 2(2a) = 4a = k$.
Case 3. Suppose $a < 0$. Let $n = 1 - 2a$, which is an element of $\mathbb{N}$ because a is negative, making $1 - 2a$ positive. Also n is odd, so $(-1)^n = -1$. Thus $1 + (-1)^n(2n-1) = 1 - (2n-1) = 1 - (2(1-2a)-1) = 4a = k$.

The above cases show that no matter whether a multiple $k = 4a$ of 4 is zero, positive or negative, $k = 1 + (-1)^n(2n-1)$ for some $n \in \mathbb{N}$. □

9.5 Treating Similar Cases

Occasionally two or more cases in a proof will be so similar that writing them separately seems tedious or unnecessary. Here is an example.

Proposition. If two integers have opposite parity, then their sum is odd.

Proof. Suppose m and n are two integers with opposite parity.
We need to show that $m + n$ is odd. This is done in two cases, as follows.
Case 1. Suppose m is even and n is odd. Thus $m = 2a$ and $n = 2b + 1$ for some $a, b \in \mathbb{Z}$. So $m + n = 2a + 2b + 1 = 2(a + b) + 1$, which is odd (by Definition 9.2).
Case 2. Suppose m is odd and n is even. Thus $m = 2a + 1$ and $n = 2b$ for some $a, b \in \mathbb{Z}$. So $m + n = 2a + 1 + 2b = 2(a + b) + 1$, which is odd (by Definition 9.2).

In either case, $m + n$ is odd. □

The two cases in this proof are entirely alike except for the order in which the even and odd terms occur. It is appropriate to just do one case and say that the other case is nearly identical. The phrase "*Without loss of generality...*" is a common way of signaling that the proof is treating just one of several nearly identical cases. Here is a second version of the above example.

Proposition. If two integers have opposite parity, then their sum is odd.

Proof. Suppose m and n are two integers with opposite parity. We need to show that $m+n$ is odd. Without loss of generality, suppose m is even and n is odd. Thus $m = 2a$ and $n = 2b+1$ for some integers a and b. Therefore $m + n = 2a + 2b + 1 = 2(a + b) + 1$, which is odd (by Definition 9.2). □

In reading proofs in other texts, you may sometimes see the phrase "Without loss of generality" abbreviated as "WLOG." However, in the interest of transparency we will avoid writing it this way. In a similar spirit, it is advisable—at least until you become more experienced in proof writing—that you write out all cases, no matter how similar they appear to be.

Please check your understanding by doing the following exercises. The odd numbered problems are proved in the Solutions section in the back of the text.

Exercises for Chapter 9

Use the method of direct proof to prove the following statements.

1. If x is an even integer, then x^2 is even.

2. If x is an odd integer, then x^3 is odd.

3. If a is an odd integer, then $a^2 + 3a + 5$ is odd.

4. Suppose $x, y \in \mathbb{Z}$. If x and y are odd, then xy is odd.

5. Suppose $x, y \in \mathbb{Z}$. If x is even, then xy is even.

6. Suppose $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

7. Suppose $a, b \in \mathbb{Z}$. If $a \mid b$, then $a^2 \mid b^2$.

8. Suppose a is an integer. If $5 \mid 2a$, then $5 \mid a$.

9. Suppose a is an integer. If $7 \mid 4a$, then $7 \mid a$.

10. Suppose a and b are integers. If $a \mid b$, then $a \mid (3b^3 - b^2 + 5b)$.

11. Suppose $a, b, c, d \in \mathbb{Z}$. If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

12. If $x \in \mathbb{R}$ and $0 < x < 4$, then $\frac{4}{x(4-x)} \geq 1$.

13. Suppose $x, y \in \mathbb{R}$. If $x^2 + 5y = y^2 + 5x$, then $x = y$ or $x + y = 5$.

14. If $n \in \mathbb{Z}$, then $5n^2 + 3n + 7$ is odd. (Try cases.)

15. If $n \in \mathbb{Z}$, then $n^2 + 3n + 4$ is even. (Try cases.)

16. If two integers have the same parity, then their sum is even. (Try cases.)

17. If two integers have opposite parity, then their product is even.

18. Suppose x and y are positive real numbers. If $x < y$, then $x^2 < y^2$.

19. Suppose a, b and c are integers. If $a^2 \mid b$ and $b^3 \mid c$, then $a^6 \mid c$.

20. If a is an integer and $a^2 \mid a$, then $a \in \{-1, 0, 1\}$.

21. If p is prime and k is an integer for which $0 < k < p$, then p divides $\binom{p}{k}$.

22. If $n \in \mathbb{N}$, then $n^2 = 2\binom{n}{2} + \binom{n}{1}$. (You may need a separate case for $n = 1$.)

23. If $n \in \mathbb{N}$, then $\binom{2n}{n}$ is even.

24. If $n \in \mathbb{N}$ and $n \geq 2$, then the numbers $n! + 2$, $n! + 3$, $n! + 4$, $n! + 5$, $\ldots$, $n! + n$ are all composite. (Thus for any $n \geq 2$, one can find n consecutive composite numbers. This means there are arbitrarily large "gaps" between prime numbers.)

25. If $a, b, c \in \mathbb{N}$ and $c \leq b \leq a$, then $\binom{a}{b}\binom{b}{c} = \binom{a}{b-c}\binom{a-b+c}{c}$.

26. Every odd integer is a difference of two squares. (Example $7 = 4^2 - 3^2$, etc.)

27. Suppose $a, b \in \mathbb{N}$. If $\gcd(a, b) > 1$, then $b \mid a$ or b is not prime.

28. If $a, b, c \in \mathbb{Z}$, then $c \cdot \gcd(a, b) \leq \gcd(ca, cb)$.

Solutions for Chapter 9

1. If x is an even integer, then x^2 is even.

Proof. Suppose x is even. Thus $x = 2a$ for some $a \in \mathbb{Z}$.
Consequently $x^2 = (2a)^2 = 4a^2 = 2(2a^2)$.
Therefore $x^2 = 2b$, where b is the integer $2a^2$.
Thus x^2 is even by definition of an even number. □

3. If a is an odd integer, then $a^2 + 3a + 5$ is odd.

Proof. Suppose a is odd.
Thus $a = 2c + 1$ for some integer c, by definition of an odd number.
Then $a^2+3a+5 = (2c+1)^2+3(2c+1)+5 = 4c^2+4c+1+6c+3+5 = 4c^2+10c+9$
$= 4c^2 + 10c + 8 + 1 = 2(2c^2 + 5c + 4) + 1$.
This shows $a^2 + 3a + 5 = 2b + 1$, where $b = 2c^2 + 5c + 4 \in \mathbb{Z}$.
Therefore $a^2 + 3a + 5$ is odd. □

5. Suppose $x, y \in \mathbb{Z}$. If x is even, then xy is even.

Proof. Suppose $x, y \in \mathbb{Z}$ and x is even.
Then $x = 2a$ for some integer a, by definition of an even number.
Thus $xy = (2a)(y) = 2(ay)$.
Therefore $xy = 2b$ where b is the integer ay, so xy is even. □

7. Suppose $a, b \in \mathbb{Z}$. If $a \mid b$, then $a^2 \mid b^2$.

Proof. Suppose $a \mid b$.
By definition of divisibility, this means $b = ac$ for some integer c.
Squaring both sides of this equation produces $b^2 = a^2c^2$.
Then $b^2 = a^2d$, where $d = c^2 \in \mathbb{Z}$.
By definition of divisibility, this means $a^2 \mid b^2$. □

9. Suppose a is an integer. If $7 \mid 4a$, then $7 \mid a$.

Proof. Suppose $7 \mid 4a$.
By definition of divisibility, this means $4a = 7c$ for some integer c.
Since $4a = 2(2a)$ it follows that $4a$ is even, and since $4a = 7c$, we know $7c$ is even.
But then c can't be odd, because that would make $7c$ odd, not even.
Thus c is even, so $c = 2d$ for some integer d.
Now go back to the equation $4a = 7c$ and plug in $c = 2d$. We get $4a = 14d$.
Dividing both sides by 2 gives $2a = 7d$.
Now, since $2a = 7d$, it follows that $7d$ is even, and thus d cannot be odd.
Then d is even, so $d = 2e$ for some integer e.
Plugging $d = 2e$ back into $2a = 7d$ gives $2a = 14e$.
Dividing both sides of $2a = 14e$ by 2 produces $a = 7e$.
Finally, the equation $a = 7e$ means that $7 \mid a$, by definition of divisibility. □

11. Suppose $a, b, c, d \in \mathbb{Z}$. If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

Proof. Suppose $a \mid b$ and $c \mid d$.
As $a \mid b$, the definition of divisibility means there is an integer x for which $b = ax$.
As $c \mid d$, the definition of divisibility means there is an integer y for which $d = cy$.
Since $b = ax$, we can multiply one side of $d = cy$ by b and the other by ax.
This gives $bd = axcy$, or $bd = (ac)(xy)$.
Since $xy \in \mathbb{Z}$, the definition of divisibility applied to $bd = (ac)(xy)$ gives $ac \mid bd$. □

13. Suppose $x, y \in \mathbb{R}$. If $x^2 + 5y = y^2 + 5x$, then $x = y$ or $x + y = 5$.

Proof. Suppose $x^2 + 5y = y^2 + 5x$.
Then $x^2 - y^2 = 5x - 5y$, and factoring gives $(x - y)(x + y) = 5(x - y)$.
Now consider two cases.
Case 1. If $x - y \neq 0$ we can divide both sides of $(x - y)(x + y) = 5(x - y)$ by the non-zero quantity $x - y$ to get $x + y = 5$.
Case 2. If $x - y = 0$, then $x = y$. (By adding y to both sides.)
Thus $x = y$ or $x + y = 5$. □

15. If $n \in \mathbb{Z}$, then $n^2 + 3n + 4$ is even.

Proof. Suppose $n \in \mathbb{Z}$. We consider two cases.
Case 1. Suppose n is even. Then $n = 2a$ for some $a \in \mathbb{Z}$.
Therefore $n^2 + 3n + 4 = (2a)^2 + 3(2a) + 4 = 4a^2 + 6a + 4 = 2(2a^2 + 3a + 2)$.
So $n^2 + 3n + 4 = 2b$ where $b = 2a^2 + 3a + 2 \in \mathbb{Z}$, so $n^2 + 3n + 4$ is even.
Case 2. Suppose n is odd. Then $n = 2a + 1$ for some $a \in \mathbb{Z}$.
Therefore $n^2+3n+4 = (2a+1)^2+3(2a+1)+4 = 4a^2+4a+1+6a+3+4 = 4a^2+10a+8$ $= 2(2a^2 + 5a + 4)$. So $n^2 + 3n + 4 = 2b$ where $b = 2a^2 + 5a + 4 \in \mathbb{Z}$, so $n^2 + 3n + 4$ is even.

In either case $n^2 + 3n + 4$ is even. □

17. If two integers have opposite parity, then their product is even.

Proof. Suppose a and b are two integers with opposite parity. Thus one is even and the other is odd. Without loss of generality, suppose a is even and b is odd. Therefore there are integers c and d for which $a = 2c$ and $b = 2d + 1$. Then the product of a and b is $ab = 2c(2d + 1) = 2(2cd + c)$. Therefore $ab = 2k$ where $k = 2cd + c \in \mathbb{Z}$. Therefore the product ab is even. □

19. Suppose $a, b, c \in \mathbb{Z}$. If $a^2 \mid b$ and $b^3 \mid c$ then $a^6 \mid c$.

Proof. Since $a^2 \mid b$ we have $b = ka^2$ for some $k \in \mathbb{Z}$. Since $b^3 \mid c$ we have $c = hb^3$ for some $h \in \mathbb{Z}$. Thus $c = h(ka^2)^3 = hk^3a^6$. Hence $a^6 \mid c$. □

21. If p is prime and $0 < k < p$ then $p \mid \binom{p}{k}$.

Proof. From the formula $\binom{p}{k} = \frac{p!}{(p-k)!k!}$, we get $p! = \binom{p}{k}(p-k)!k!$. Now, since the prime number p is a factor of $p!$ on the left, it must also be a factor of $\binom{p}{k}(p-k)!k!$ on the right. Thus the prime number p appears in the prime factorization of $\binom{p}{k}(p-k)!k!$.

Now, $k!$ is a product of numbers smaller than p, so its prime factorization contains no p's. Similarly the prime factorization of $(p-k)!$ contains no p's. But we noted

that the prime factorization of $\binom{p}{k}(p-k)!k!$ must contain a p, so it follows that the prime factorization of $\binom{p}{k}$ contains a p. Thus $\binom{p}{k}$ is a multiple of p, so p divides $\binom{p}{k}$. □

23. If $n \in \mathbb{N}$ then $\binom{2n}{n}$ is even.

Proof. By definition, $\binom{2n}{n}$ is the number of n-element subsets of a set A with $2n$ elements. For each subset $X \subseteq A$ with $|X| = n$, the complement $\overline{X}$ is a different set, but it also has $2n - n = n$ elements. Imagine listing out all the n-elements subset of a set A. It could be done in such a way that the list has form

$$X_1,\ \overline{X_1},\quad X_2,\ \overline{X_2},\quad X_3,\ \overline{X_3},\quad X_4,\ \overline{X_4},\quad X_5,\ \overline{X_5}\ldots$$

This list has an even number of items, for they are grouped in pairs. Thus $\binom{2n}{n}$ is even. □

25. If $a, b, c \in \mathbb{N}$ and $c \leq b \leq a$ then $\binom{a}{b}\binom{b}{c} = \binom{a}{b-c}\binom{a-b+c}{c}$.

Proof. Assume $a, b, c \in \mathbb{N}$ with $c \leq b \leq a$. Then we have $\binom{a}{b}\binom{b}{c} = \frac{a!}{(a-b)!b!}\frac{b!}{(b-c)!c!} = \frac{a!}{(a-b+c)!(a-b)!}\frac{(a-b+c)!}{(b-c)!c!} = \frac{a!}{(b-c)!(a-b+c)!}\frac{(a-b+c)!}{(a-b)!c!} = \binom{a}{b-c}\binom{a-b+c}{c}$. □

27. Suppose $a, b \in \mathbb{N}$. If $\gcd(a, b) > 1$, then $b \mid a$ or b is not prime.

Proof. Suppose $\gcd(a, b) > 1$. Let $c = \gcd(a, b) > 1$. Then since c is a divisor of both a and b, we have $a = cx$ and $b = cy$ for integers x and y. We divide into two cases according to whether or not b is prime.
Case I. Suppose b is prime. Then the above equation $b = cy$ with $c > 1$ forces $c = b$ and $y = 1$. Then $a = cx$ becomes $a = bx$, which means $b \mid a$. We conclude that the statement "$b \mid a$ *or* b *is not prime,*" is true.
Case II. Suppose b is not prime. Then the statement "$b \mid a$ *or* b *is not prime,*" is automatically true. □