Introduction

What is mathematics? High school mathematics is concerned mostly with solving equations and computing answers to numerical questions. College mathematics deals with a wider variety of questions, involving not only numbers, but also sets, functions, and other mathematical objects. What ties them together is the use of *deductive reasoning* to find the answers to questions. When you solve an equation for x you are using the information given by the equation to *deduce* what the value of x must be. Similarly, when mathematicians solve other kinds of mathematical problems, they always justify their conclusions with deductive reasoning.

Deductive reasoning in mathematics is usually presented in the form of a *proof*. One of the main purposes of this book is to help you develop your mathematical reasoning ability in general, and in particular your ability to read and write proofs. In later chapters we'll study how proofs are constructed in detail, but first let's take a look at a few examples of proofs.

Don't worry if you have trouble understanding these proofs. They're just intended to give you a taste of what mathematical proofs are like. In some cases you may be able to follow many of the steps of the proof, but you may be puzzled about why the steps are combined in the way they are, or how anyone could have thought of the proof. If so, we ask you to be patient. Many of these questions will be answered later in this book, particularly in Chapter 3.

All of our examples of proofs in this introduction will involve prime numbers. Recall that an integer larger than 1 is said to be *prime* if it cannot be written as a product of two smaller positive integers. If it can be written as a product of two smaller positive integers, then it is *composite*. For example, 6 is a composite number, since $6 = 2 \cdot 3$, but 7 is a prime number.

Before we can give an example of a proof involving prime numbers, we need to find something to prove – some fact about prime numbers whose correctness can be verified with a proof. Sometimes you can find interesting

n	Is n prime?	$2^n - 1$	Is $2^n - 1$ prime?
2	yes	3	yes
3	yes	7	yes
4	no: $4 = 2 \cdot 2$	15	no: $15 = 3 \cdot 5$
5	yes	31	yes
6	no: $6 = 2 \cdot 3$	63	no: $63 = 7 \cdot 9$
7	yes	127	yes
8	no: $8 = 2 \cdot 4$	255	no: $255 = 15 \cdot 17$
9	no: $9 = 3 \cdot 3$	511	no: $511 = 7 \cdot 73$
10	no: $10 = 2 \cdot 5$	1023	no: $1023 = 31 \cdot 33$

Figure I.1.

patterns in mathematics just by trying out a calculation on a few numbers. For example, consider the table in Figure I.1. For each integer n from 2 to 10, the table shows whether or not both n and $2^n - 1$ are prime, and a surprising pattern emerges. It appears that $2^n - 1$ is prime in precisely those cases in which n is prime!

Will this pattern continue? It is tempting to guess that it will, but this is only a guess. Mathematicians call such guesses *conjectures*. Thus, we have the following two conjectures:

Conjecture 1. *Suppose n is an integer larger than 1 and n is prime. Then $2^n - 1$ is prime.*

Conjecture 2. *Suppose n is an integer larger than 1 and n is not prime. Then $2^n - 1$ is not prime.*

Unfortunately, if we continue the table in Figure I.1, we immediately find that Conjecture 1 is incorrect. It is easy to check that 11 is prime, but $2^{11} - 1 = 2047 = 23 \cdot 89$, so $2^{11} - 1$ is composite. Thus, 11 is a *counterexample* to Conjecture 1. The existence of even one counterexample establishes that the conjecture is incorrect, but it is interesting to note that in this case there are many counterexamples. If we continue checking numbers up to 30, we find two more counterexamples to Conjecture 1: both 23 and 29 are prime, but $2^{23} - 1 = 8{,}388{,}607 = 47 \cdot 178{,}481$ and $2^{29} - 1 = 536{,}870{,}911 = 2{,}089 \cdot 256{,}999$. However, no number up to 30 is a counterexample to Conjecture 2.

Do you think that Conjecture 2 is correct? Having found counterexamples to Conjecture 1, we know that this conjecture is incorrect, but our failure to find a counterexample to Conjecture 2 does not show that it is correct. Perhaps there are counterexamples, but the smallest one is larger than 30. Continuing to check examples might uncover a counterexample, or, if it doesn't, it might

increase our confidence in the conjecture. But we can never be sure that the conjecture is correct if we only check examples. No matter how many examples we check, there is always the possibility that the next one will be the first counterexample. The only way we can be sure that Conjecture 2 is correct is to *prove* it.

In fact, Conjecture 2 *is* correct. Here is a proof of the conjecture:

Proof of Conjecture 2. Since n is not prime, there are positive integers a and b such that $a < n$, $b < n$, and $n = ab$. Let $x = 2^b - 1$ and $y = 1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}$. Then

$$\begin{aligned} xy &= (2^b - 1) \cdot (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) \\ &= 2^b \cdot (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) - (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) \\ &= (2^b + 2^{2b} + 2^{3b} + \cdots + 2^{ab}) - (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) \\ &= 2^{ab} - 1 \\ &= 2^n - 1. \end{aligned}$$

Since $b < n$, we can conclude that $x = 2^b - 1 < 2^n - 1$. Also, since $ab = n > a$, it follows that $b > 1$. Therefore, $x = 2^b - 1 > 2^1 - 1 = 1$, so $y < xy = 2^n - 1$. Thus, we have shown that $2^n - 1$ can be written as the product of two positive integers x and y, both of which are smaller than $2^n - 1$, so $2^n - 1$ is not prime. □

Now that the conjecture has been proven, we can call it a *theorem*. Don't worry if you find the proof somewhat mysterious. We'll return to it again at the end of Chapter 3 to analyze how it was constructed. For the moment, the most important point to understand is that if n is any integer larger than 1 that can be written as a product of two smaller positive integers a and b, then the proof gives a method (admittedly, a somewhat mysterious one) of writing $2^n - 1$ as a product of two smaller positive integers x and y. Thus, if n is not prime, then $2^n - 1$ must also not be prime. For example, suppose $n = 12$, so $2^n - 1 = 4095$. Since $12 = 3 \cdot 4$, we could take $a = 3$ and $b = 4$ in the proof. Then according to the formulas for x and y given in the proof, we would have $x = 2^b - 1 = 2^4 - 1 = 15$ and $y = 1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b} = 1 + 2^4 + 2^8 = 273$. And, just as the formulas in the proof predict, we have $xy = 15 \cdot 273 = 4095 = 2^n - 1$. Of course, there are other ways of factoring 12 into a product of two smaller integers, and these might lead to other ways of factoring 4095. For example, since $12 = 2 \cdot 6$, we could use the values $a = 2$ and $b = 6$. Try computing the corresponding values of x and y and make sure their product is 4095.

Although we already know that Conjecture 1 is incorrect, there are still interesting questions we can ask about it. If we continue checking prime numbers n to see if $2^n - 1$ is prime, will we continue to find counterexamples to the conjecture – examples for which $2^n - 1$ is not prime? Will we continue to find examples for which $2^n - 1$ is prime? If there were only finitely many prime numbers, then we might be able to investigate these questions by simply checking $2^n - 1$ for every prime number n. But in fact there are infinitely many prime numbers. Euclid (circa 300 BCE) gave a proof of this fact in Book IX of his *Elements*. His proof is one of the most famous in all of mathematics:[1]

Theorem 3. *There are infinitely many prime numbers.*

Proof. Suppose there are only finitely many prime numbers. Let $p_1, p_2, \ldots, p_n$ be a list of all prime numbers. Let $m = p_1 p_2 \cdots p_n + 1$. Note that m is not divisible by p_1, since dividing m by p_1 gives a quotient of $p_2 p_3 \cdots p_n$ and a remainder of 1. Similarly, m is not divisible by any of $p_2, p_3, \ldots, p_n$.

We now use the fact that every integer larger than 1 is either prime or can be written as a product of two or more primes. (We'll see a proof of this fact in Chapter 6 – see Theorem 6.4.2.) Clearly m is larger than 1, so m is either prime or a product of primes. Suppose first that m is prime. Note that m is larger than all of the numbers in the list $p_1, p_2, \ldots, p_n$, so we've found a prime number not in this list. But this contradicts our assumption that this was a list of *all* prime numbers.

Now suppose m is a product of primes. Let q be one of the primes in this product. Then m is divisible by q. But we've already seen that m is not divisible by any of the numbers in the list $p_1, p_2, \ldots, p_n$, so once again we have a contradiction with the assumption that this list included all prime numbers.

Since the assumption that there are finitely many prime numbers has led to a contradiction, there must be infinitely many prime numbers. □

Once again, you should not be concerned if some aspects of this proof seem mysterious. After you've read Chapter 3 you'll be better prepared to understand the proof in detail. We'll return to this proof then and analyze its structure.

We have seen that if n is not prime then $2^n - 1$ cannot be prime, but if n is prime then $2^n - 1$ can be either prime or composite. Because there are infinitely many prime numbers, there are infinitely many numbers of the form $2^n - 1$ that, based on what we know so far, *might* be prime. But how many of them *are* prime?

[1] Euclid phrased the theorem and proof somewhat differently. We have chosen to take a more modern approach in our presentation.

Prime numbers of the form $2^n - 1$ are called *Mersenne primes*, after Father Marin Mersenne (1588–1648), a French monk and scholar who studied these numbers. Although many Mersenne primes have been found, it is still not known if there are infinitely many of them. Many of the largest known prime numbers are Mersenne primes. As of this writing (February 2019), the largest known prime number is the Mersenne prime $2^{82,589,933} - 1$, a number with 24,862,048 digits.

Mersenne primes are related to perfect numbers, the subject of another famous unsolved problem of mathematics. A positive integer n is said to be *perfect* if n is equal to the sum of all positive integers smaller than n that divide n. (For any two integers m and n, we say that m *divides* n if n is divisible by m; in other words, if there is an integer q such that $n = qm$.) For example, the only positive integers smaller than 6 that divide 6 are 1, 2, and 3, and $1+2+3 = 6$. Thus, 6 is a perfect number. The next smallest perfect number is 28. (You should check for yourself that 28 is perfect by finding all the positive integers smaller than 28 that divide 28 and adding them up.)

Euclid proved that if $2^n - 1$ is prime, then $2^{n-1}(2^n - 1)$ is perfect. Thus, every Mersenne prime gives rise to a perfect number. Furthermore, about 2000 years after Euclid's proof, the Swiss mathematician Leonhard Euler (1707–1783), the most prolific mathematician in history, proved that every even perfect number arises in this way. (For example, note that $6 = 2^1(2^2 - 1)$ and $28 = 2^2(2^3 - 1)$.) Because it is not known if there are infinitely many Mersenne primes, it is also not known if there are infinitely many even perfect numbers. It is also not known if there are any odd perfect numbers. For proofs of the theorems of Euclid and Euler, see exercises 18 and 19 in Section 7.4.

Although there are infinitely many prime numbers, the primes thin out as we look at larger and larger numbers. For example, there are 25 primes between 1 and 100, 16 primes between 1001 and 1100, and only six primes between 1,000,001 and 1,000,100. As our last introductory example of a proof, we show that there are long stretches of consecutive positive integers containing no primes at all. In this proof, we'll use the following terminology: for any positive integer n, the product of all integers from 1 to n is called n *factorial* and is denoted $n!$. Thus, $n! = 1 \cdot 2 \cdot 3 \cdots n$. As with our previous two proofs, we'll return to this proof at the end of Chapter 3 to analyze its structure.

Theorem 4. *For every positive integer n, there is a sequence of n consecutive positive integers containing no primes.*

Proof. Suppose n is a positive integer. Let $x = (n+1)! + 2$. We will show that none of the numbers $x, x+1, x+2, \ldots, x+(n-1)$ is prime. Since this is a sequence of n consecutive positive integers, this will prove the theorem.

To see that x is not prime, note that

$$\begin{aligned} x &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + 2 \\ &= 2 \cdot (1 \cdot 3 \cdot 4 \cdots (n+1) + 1). \end{aligned}$$

Thus, x can be written as a product of two smaller positive integers, so x is not prime.

Similarly, we have

$$\begin{aligned} x + 1 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + 3 \\ &= 3 \cdot (1 \cdot 2 \cdot 4 \cdots (n+1) + 1), \end{aligned}$$

so $x + 1$ is also not prime. In general, consider any number $x + i$, where $0 \leq i \leq n - 1$. Then we have

$$\begin{aligned} x + i &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + (i+2) \\ &= (i+2) \cdot (1 \cdot 2 \cdot 3 \cdots (i+1) \cdot (i+3) \cdots (n+1) + 1), \end{aligned}$$

so $x + i$ is not prime. □

Theorem 4 shows that there are sometimes long stretches between one prime and the next prime. But primes also sometimes occur close together. Since 2 is the only even prime number, the only pair of consecutive integers that are both prime is 2 and 3. But there are lots of pairs of primes that differ by only two, for example, 5 and 7, 29 and 31, and 7949 and 7951. Such pairs of primes are called *twin primes*. It is not known whether there are infinitely many twin primes.

Recently, significant progress has been made on the twin primes question. In 2013, Yitang Zhang (1955–) proved that there is a positive integer $d \leq 70{,}000{,}000$ such that there are infinitely many pairs of prime numbers that differ by d. Work of many other mathematicians in 2013–14 narrowed down the possibilities for d to $d \leq 246$. Of course, if the statement holds with $d = 2$ then there are infinitely many twin primes.

Exercises

Note: Solutions or hints for exercises marked with an asterisk (*) are given in the appendix.

*1. (a) Factor $2^{15} - 1 = 32{,}767$ into a product of two smaller positive integers.

(b) Find an integer x such that $1 < x < 2^{32,767} - 1$ and $2^{32,767} - 1$ is divisible by x.

2. Make some conjectures about the values of n for which $3^n - 1$ is prime or the values of n for which $3^n - 2^n$ is prime. (You might start by making a table similar to Figure I.1.)

*3. The proof of Theorem 3 gives a method for finding a prime number different from any in a given list of prime numbers.
   (a) Use this method to find a prime different from 2, 3, 5, and 7.
   (b) Use this method to find a prime different from 2, 5, and 11.

4. Find five consecutive integers that are not prime.

5. Use the table in Figure I.1 and the discussion on p. 5 to find two more perfect numbers.

6. The sequence 3, 5, 7 is a list of three prime numbers such that each pair of adjacent numbers in the list differ by two. Are there any more such "triplet primes"?

7. A pair of distinct positive integers (m, n) is called *amicable* if the sum of all positive integers smaller than n that divide n is m, and the sum of all positive integers smaller than m that divide m is n. Show that $(220, 284)$ is amicable.

1

Sentential Logic

1.1. Deductive Reasoning and Logical Connectives

As we saw in the introduction, proofs play a central role in mathematics, and deductive reasoning is the foundation on which proofs are based. Therefore, we begin our study of mathematical reasoning and proofs by examining how deductive reasoning works.

Example 1.1.1. Here are three examples of deductive reasoning:

1. It will either rain or snow tomorrow.
   It's too warm for snow.
   Therefore, it will rain.
2. If today is Sunday, then I don't have to go to work today.
   Today is Sunday.
   Therefore, I don't have to go to work today.
3. I will go to work either tomorrow or today.
   I'm going to stay home today.
   Therefore, I will go to work tomorrow.

In each case, we have arrived at a *conclusion* from the assumption that some other statements, called *premises*, are true. For example, the premises in argument 3 are the statements "I will go to work either tomorrow or today" and "I'm going to stay home today." The conclusion is "I will go to work tomorrow," and it seems to be forced on us somehow by the premises.

But is this conclusion really correct? After all, isn't it possible that I'll stay home today, and then wake up sick tomorrow and end up staying home again? If that happened, the conclusion would turn out to be false. But notice that in that case the first premise, which said that I would go to work either tomorrow

or today, would be false as well! Although we have no guarantee that the conclusion is true, it can only be false if at least one of the premises is also false. *If* both premises are true, we can be sure that the conclusion is also true. This is the sense in which the conclusion is forced on us by the premises, and this is the standard we will use to judge the correctness of deductive reasoning. We will say that an argument is *valid* if the premises cannot all be true without the conclusion being true as well. All three of the arguments in our example are valid arguments.

Here's an example of an invalid deductive argument:

Either the butler is guilty or the maid is guilty.
Either the maid is guilty or the cook is guilty.
Therefore, either the butler is guilty or the cook is guilty.

The argument is invalid because the conclusion could be false even if both premises are true. For example, if the maid were guilty, but the butler and the cook were both innocent, then both premises would be true and the conclusion would be false.

We can learn something about what makes an argument valid by comparing the three arguments in Example 1.1.1. On the surface it might seem that arguments 2 and 3 have the most in common, because they're both about the same subject: attendance at work. But in terms of the reasoning used, arguments 1 and 3 are the most similar. They both introduce two possibilities in the first premise, rule out the second one with the second premise, and then conclude that the first possibility must be the case. In other words, both arguments have the form:

P or Q.
Not Q.
Therefore, P.

It is this form, and not the subject matter, that makes these arguments valid. You can see that argument 1 has this form by thinking of the letter P as standing for the statement "It will rain tomorrow," and Q as standing for "It will snow tomorrow." For argument 3, P would be "I will go to work tomorrow," and Q would be "I will go to work today."

Replacing certain statements in each argument with letters, as we have in stating the form of arguments 1 and 3, has two advantages. First, it keeps us from being distracted by aspects of the arguments that don't affect their validity. You don't need to know anything about weather forecasting or work habits to recognize that arguments 1 and 3 are valid. That's because both arguments have the form shown earlier, and you can tell that this argument

form is valid without even knowing what P and Q stand for. If you don't believe this, consider the following argument:

> Either the framger widget is misfiring, or the wrompal mechanism is out of alignment.
> I've checked the alignment of the wrompal mechanism, and it's fine.
> Therefore, the framger widget is misfiring.

If a mechanic gave this explanation after examining your car, you might still be mystified about why the car won't start, but you'd have no trouble following his logic!

Perhaps more important, our analysis of the forms of arguments 1 and 3 makes clear what *is* important in determining their validity: the words *or* and *not*. In most deductive reasoning, and in particular in mathematical reasoning, the meanings of just a few words give us the key to understanding what makes a piece of reasoning valid or invalid. (Which are the important words in argument 2 in Example 1.1.1?) The first few chapters of this book are devoted to studying those words and how they are used in mathematical writing and reasoning.

In this chapter, we'll concentrate on words used to combine statements to form more complex statements. We'll continue to use letters to stand for statements, but only for unambiguous statements that are either true or false. Questions, exclamations, and vague statements will not be allowed. It will also be useful to use symbols, sometimes called *connective symbols*, to stand for some of the words used to combine statements. Here are our first three connective symbols and the words they stand for:

Symbol	Meaning
$\vee$	or
$\wedge$	and
$\neg$	not

Thus, if P and Q stand for two statements, then we'll write $P \vee Q$ to stand for the statement "P or Q," $P \wedge Q$ for "P and Q," and $\neg P$ for "not P" or "P is false." The statement $P \vee Q$ is sometimes called the *disjunction* of P and Q, $P \wedge Q$ is called the *conjunction* of P and Q, and $\neg P$ is called the *negation* of P.

Example 1.1.2. Analyze the logical forms of the following statements:

1. Either John went to the store, or we're out of eggs.
2. Joe is going to leave home and not come back.
3. Either Bill is at work and Jane isn't, or Jane is at work and Bill isn't.