Evens, Odds, and Primes: A Taste of Number Theory

Figure 1.0.1. A double rainbow at Yellowstone National Park. Photo by Jingwei Xia.

Trinity: It's so beautiful. – From "The Matrix Resurrections"

Goals of this chapter: To demonstrate that we can, without much background, understand some elementary aspects of a deep subject: prime numbers. To see some of the pitfalls of inductive reasoning. To give examples of deductive reasoning leading to the proofs of results. After reading this chapter, the reader should be able to write some simple proofs such as in the exercises.

Figure 1.0.2. Euclid (fl. 300 BC). Detail from Raphael's *The School of Athens*. Wikimedia Commons, Public Domain.

In this introductory chapter, we take a closer look at something we are all familiar with: *even* and *odd* integers. Perhaps a bit less familiar, but still something we know about, are *prime* numbers. Do you know Euclid's Theorem that there are infinitely many prime numbers? If you know it, congratulations; you are truly knowledgeable.[1] If not, you will first learn the proof of this wonderful theorem in this book.[2]

On the other hand, do you know the proof that there are infinitely many *twin primes*? As of this writing, *nobody* knows whether this statement is true or false although remarkable progress has been made on this *conjecture* (see §1.9* below for the definition of "twin prime" and for the statement of the conjecture). The subject of prime numbers, while fascinating, at advanced levels can be not at all easy. So in this chapter we consider results that are either easy to state, easy to prove, or both.

Math, perhaps like life, is a game. Imagine beginning to play a video game with 40 levels. At the beginning, level 38 looks very, maybe impossibly, difficult. Math, like some video games, can be thought of as being built on levels. Our goal will be to get good at the *game of math*.

If we approach the game of math very formally, then proceeding through the levels of our game will necessarily take a lot of time and a lot of pages. So, typically, in a book we jump over some of the elementary levels. In this book, to make the discussion more lively, we give you, the reader, a sneak peak of the higher levels, including some famous unsolved conjectures!

Instead of beginning with a more formal treatment of the basics of logic, we will first learn how to prove theorems by example. Our philosophy is that the easiest way to learn how to prove statements is by seeing how it is done. We encourage you to think independently and to work out proofs with the minimum amount of help that you need to work it out in a reasonable amount of time. For example, while

[1] This type of sentence is patterned after the pattern of speech of chess Youtuber agadmator.

[2] That is, if you do not first click on the Wikipedia page link for this theorem! Euclid's Theorem is also Theorem 4.12 in this book.

you are reading a proof, you may have an aha moment, where you get the idea of the proof and feel that you can finish off the proof by yourself. When this happens, we hope that you try to do this. At least at the beginning, it may be helpful to check your proof with the proof in the book or any other source. Typically, the proofs will be rather similar. If they are not, then you have an independent proof!

In this chapter, as in every chapter, *exercises* are sprinkled throughout the text. We strongly suggest you work as many problems as you can. After straining for at least a few minutes, you may look at the hints at the end of the chapter.

Figure 1.0.3. Can you decode the color coding of the integers from 1 to 100? This image is from Dan Finkel's TEDx talk "Five Principles of Extraordinary Math Teaching".

1.1. A first excursion into prime numbers

Not all math puns are awful, just sum.

In this section we learn what a prime number is, we see all of the primes less than 100, and we formulate some naive conjectures on primes, which we prove are false.

1.1.1. Prime numbers. Let $\mathbb{Z}$ denote the set of integers, including the positive ones, the negative ones, and zero, denoted by 0. For example, -17 and 8 are

integers, but π, read as "pi", is not. On this set $\mathbb{Z}$ we have the operations of addition $+$ and multiplication $\cdot$ or $\times$. For example $2+2=2\cdot 2=4$ and $2\cdot 3=6$.

1.1.1.1. *Definition of prime number.* Let us consider positive integers. Primes are their multiplicative building blocks. We see that some numbers factor, such as $6=2\cdot 3$, $12=4\cdot 3$, and $35=5\cdot 7$. Other numbers don't factor, such as 17: we can write $17=1\cdot 17=17\cdot 1$, but there is no other way to write 17 as a product of two positive integers. With this in mind, we make the following:

Definition 1.1. We say that an integer $p\geq 2$ is **prime** if the only way to factor p as the product of two positive integers is

$$p=1\cdot p=p\cdot 1.$$

That is, the only way of "breaking up" p as the product of positive integers is the trivial way. In other words, an integer at least 2 is prime **if and only if** it is "indivisible" multiplicatively.

Remark 1.2. By "if and only if" we mean "exactly when". We will see a formal definition of "if and only if", which we do not need here, in Chapter 3 below. When the word "if" is used to make a *definition*, we actually mean "if and only if".

For example, 2 is prime since the only way to factor it as the product of positive integers is $2=1\cdot 2=2\cdot 1$. Similarly, we see that 3 is prime since the only way to factor it as the product of positive integers is $3=1\cdot 3=3\cdot 1$. One the other hand, even though the only way to factor 1 as the product of two positive integers is $1=1\cdot 1$, we have that 1 is not a prime simply because $1<2$. As will be evident later, one makes this choice that 1 is not a prime so that many results involving primes will be smoother to state. We see that 4 is not prime since $4=2\cdot 2$ and since the positive integers $2,2$ are not $1,4$, in either order. Next, 5 is prime as $5=1\cdot 5=5\cdot 1$ is the only way to factor 5 as the product of two positive integers. But 6 is not prime since $6=2\cdot 3$ and since the positive integers $2,3$ are not $1,6$, in either order.

Exercise 1.1. *Explain the color coding of the first one hundred positive integers in Figure* 1.0.3. *The topic of* §1.6 *is a hint! If you are having difficulty with this exercise, continue reading and come back to it.*

Certain elementary facts about integers will be useful.

Solved Problem 1.3. *Prove that if a is a positive integer satisfying $a\neq 1$, then $a>1$, and in fact $a\geq 2$.*

Solution. Firstly, for this proof, we assume the basic facts that 1 is the smallest positive integer and 2 is the next smallest positive integer. In particular, there are no integers strictly between 0 and 1, and there are no integers strictly between 1 and 2.

Let a be a positive integer satisfying $a\neq 1$. Since $a>0$ and a is an integer, we have $a\geq 1$. Indeed, there is no integer a satisfying $0<a<1$. Now, since $a\geq 1$ and $a\neq 1$, we obtain $a>1$. Now, since there is no integer a satisfying $1<a<2$, we conclude that $a\geq 2$. □

The □ symbol indicates the end of the solution or proof. That was a relatively easy proof. And it was indeed a proof. That is, it was

a logical argument which demonstrated the truth of a statement.

Part of the key to our success was that we clearly understood beforehand what it means to be an integer. As Polya said, "You have to understand the problem."

Exercise 1.2. *Let n be a positive integer, and suppose that a and b are integers such that $n = ab$. Prove:* ***If*** *a is equal to 1 or n,* ***then*** *b is equal to n* ***or*** *1, respectively. Hint: Show that if $a = 1$, then $b = n$. Similarly for 1 and n switched.*

Remark 1.4. In the above, we boldfaced the "if-then" and "or" natures of the statement. **If-then statements** are called *implications* (a.k.a. conditional statements), and **or** is an example of a logical connective, all of which is studied in more detail in Chapter 3 below. But we assume that since such statements are common, even in elementary mathematics, you are comfortable with their meanings.

The exercise above is a short proof, but there is logical reasoning going on here! Usually we give hints to the exercises at the end of the chapter. However, since this is our first "proof" exercise, we solve part of Exercise 1.2 here:

Suppose $a = 1$. Then $n = a \cdot b = 1 \cdot b = b$. This proves: If $a = 1$, then $b = n$.

Characterization of non-primes: So what does it mean for an integer n *not* to be prime? Firstly, if $n \leq 1$, then n is not prime. So let us assume that $n \geq 2$. The following is a tweak to the characterization of not being prime.

Lemma 1.5. *An integer $n \geq 2$ is not a prime if and only if there exist integers $a > 1$ and $b > 1$ such that $n = ab$.*

Proof. By Definition 1.1, n is not prime precisely when there is another way to factor n by positive integers besides $1 \cdot n$ and $n \cdot 1$; that is, there exist positive integers a and b such that

$$n = ab, \tag{1.1}$$

where a, b are not equal to $1, n$ in any order.

Claim. The condition above that a, b are not equal to $1, n$ in any order *is equivalent to* the condition

$$a \neq 1 \quad \text{and} \quad b \neq 1. \tag{1.2}$$

Proof of the claim. Firstly, if $a \neq 1$ and $b \neq 1$, then clearly a, b are not equal to $1, n$ in any order.

Secondly and conversely, suppose that a, b are not equal to $1, n$ in any order. **Then suppose for a contradiction that $a = 1$.** By Exercise 1.2, we have $b = n$, contradicting that a, b are not equal to $1, n$ in any order. Since we have arrived at a *contradiction* to our last assumption that $a = 1$, we must have that $a \neq 1$.

The proof that $b \neq 1$ is exactly analogous to the proof that $a \neq 1$ by switching the roles of a and b in the proof. So we have proved the claim.

Since a and b are positive, by Solved Problem 1.3, condition (1.2) is in turn equivalent to the condition that

$$a > 1 \quad \text{and} \quad b > 1. \tag{1.3}$$

This and the proved claim above complete the proof of the lemma. □

Remark 1.6. This was the first time we proved something by the method of *contradiction*. Namely, at one point in the proof we assumed that $a = 1$, and from this assumption we logically deduced a contradiction. This proves that the assumption $a = 1$ is false, so necessarily we have $a \neq 1$. We will discuss proof by contradiction in more detail in Chapter 3.

For Lemma 1.5 we walked the path of a proof. By going over the logic of the proof, you will know the path of the proof better. There is no single right balance of walking and knowing proofs. The way you choose is your path.

Exercise 1.3. *Given that $n = ab$, show that condition* (1.3) *on a and b is equivalent to the condition*

$$1 < a < n. \tag{1.4}$$

This is also equivalent to $1 < b < n$. Hint: Use some basic facts about inequalities.

1.1.1.2. *Composite numbers.* Non-prime integers greater than 1 are also called **composite numbers**. So, by Lemma 1.5, an integer $n > 1$ is composite if and only if there exist integers $a, b > 1$ such that $n = ab$.

If $n = ab$, where a and b are integers, then we say that a and b are **divisors** of n. Another way to say this is: An integer a is a *divisor* of an integer n if there is some integer b such that $n = ab$. We also say that a **divides** n. We can think of a dividing n as meaning that a is "contained" in n from the point of view of multiplication.

Example 1.7. (1) 7 is a divisor of 56 since $7 \cdot 8 = 56$ and 56 is a composite number.

(2) 1 is a divisor of any integer n since $1 \cdot n = n$.

Exercise 1.4. *Show that 0 is not a divisor of any non-zero integer.*

Lemma 1.8. *If a and n are positive integers and if a is a divisor of n, then*

$$1 \leq a \leq n. \tag{1.5}$$

Proof. Let a and n be positive integers such that a divides n. Since a is a positive integer, we have $a \geq 1$ (it is not possible that $0 < a < 1$). We also have that there exists a positive integer b such that $ab = n$. Since $b \geq 1$, this implies that $a = \frac{n}{b} \leq \frac{n}{1} = n$. □

Notice how most mathematical proofs, in contrast to computer programming, have (hopefully small) jumps in logic. For example, in the proof above, we used the "elementary" fact that since $n > 0$ and $b \geq 1 > 0$, we have $\frac{n}{b} \leq \frac{n}{1}$. For a justification of this fact, see (1.18) below.

Given a positive integer n, we call 1 and n **trivial divisors** of n. If $1 < a < n$ is a divisor of n, then we call a a **non-trivial divisor** of n.

Example 1.9. 1 and 15 are trivial divisors of 15, whereas 3 and 5 are non-trivial divisors of 15.

Exercise 1.5. *Let $n = ab$ be a positive integer. Prove that if a is a non-trivial divisor of n, then b is a non-trivial divisor of n.*

By Exercise 1.3, we have the following further tweak of the characterization of composite numbers.

Corollary 1.10. *Let $n \geq 2$ be an integer. The integer n is a composite number if and only if there exists a divisor a of n satisfying $1 < a < n$, that is, if and only if n has a non-trivial divisor.*

Proof. Let $n \geq 2$ be a composite number. By Lemma 1.5, this is equivalent to there existing integers $a > 1$ and $b > 1$ such that $n = ab$.

By Exercise 1.3, this implies that a is a non-trivial divisor of n.

Conversely, suppose that $n \geq 2$ has a non-trivial divisor a. Since a is a divisor of n, there exists an integer b such that $n = ab$. Since $1 < a < n$, by Exercise 1.3 again, this implies that $1 < b < n$. This proves that n is a composite number. □

So, a composite number is an integer at least 2 which has at least one non-trivial divisor. On the other hand, a prime is an integer at least 2 which has no non-trivial divisors. For example, to prove that 5 is prime (as we claimed earlier), we just need to check that none of $2, 3, 4$ divide 5. To reprove that 6 is a composite number, we just need to observe that 2 divides 6 and that $1 < 2 < 6$.

A visualization of prime versus composite number is given in Figure 1.1.1.

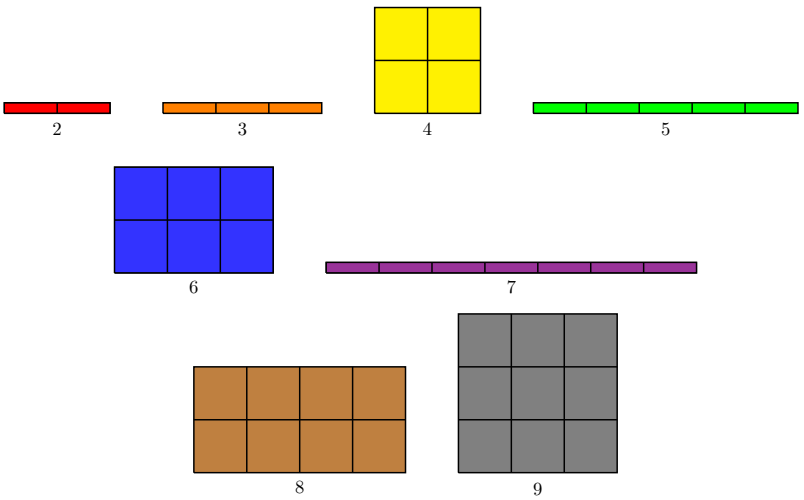

Figure 1.1.1. Visualizing the integers 2 through 9 as primes or composite numbers. The composite numbers are $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, $9 = 3 \cdot 3$.

1.1.1.3. *The primes under* 100. Having found which integers at most 6 are primes, if we continue in this way of checking for non-trivial divisors, then we can find the primes less than 100.

Exercise 1.6. *List all of the primes less than* 100. *Hint: We give the answer momentarily, but don't peek!*

By Corollary 1.10, an integer $p \geq 2$ is prime if and only if p does not have a divisor a satisfying $1 < a < p$.

It is cool to picture primes in red and non-primes in green as in Figure 1.1.2.

01	02	03	04	05	06	07	08	09	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Figure 1.1.2. The first 100 positive integers: primes are in red and composite numbers are in green.

Exercise 1.7. *We make the following observations about Figure* 1.1.2.

(1) *For the second, fourth, sixth, eighth, and tenth columns, all of the integers are composite except for the number* 2.

(2) *For the fifth and tenth columns, all of the integers are composite except for the number* 5.

(3) *All of the multiples of* 3, *except for* 3 *itself, are composite numbers.*

Explain the reason for why each of these observations is true.

Now we belatedly list the primes less than 100. They are, as pictured in Figure 1.1.2, in increasing order:

(1.6)

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

There are 25 in all, so assuming that you live to one hundred years old, on one quarter of your birthdays you will be a prime number of years old. So at age 97 you can say that you are in the prime of your life!

Although, we have listed the primes less than 100, it is a good exercise to give a *proof* that the first several in our list are actually primes.

Exercise 1.8. *Prove that each of the integers* $5, 7, 11, 13, 17$ *is a prime. That is, show that each of these integers does not have any non-trivial positive divisors. You may use Theorem* 1.34 *below.*

We remark that the prime 17 *is a rather interesting integer. The address of the Mathematical Sciences Research Institute (MSRI) is 17 Gauss Way in Berkeley.*

Remark 1.11. To see that 5 is not a prime, we calculate that $\frac{5}{2} = 2.5$, $\frac{5}{3} = 1 + \frac{2}{3}$, and $\frac{5}{4} = 1.25$, none of which are integers. (Namely, $2 < \frac{5}{2} < 3$, $1 < \frac{5}{3} < 2$, and $1 < \frac{5}{4} < 2$. Any real number strictly between two consecutive integers is not an integer.) Therefore, none of $2, 3, 4$ divide 5. This proves that 5 is prime.

1.1.2. Conjectures on primes—to prove or not to prove. That is the question!

To understand any concept, such as primes, we should ask questions and guess and check statements pertaining and related to this concept. A guessed statement is called a conjecture.

1.1.2.1. *Naive conjectures.* Let us make a "gonzo" conjecture based on wishful thinking.

An elementary fact is that all primes greater than 2 are odd; we will prove this in Theorem 1.19 (or Corollary 1.23) below, when we discuss even and odd in more detail. Moreover, positive powers of 2 are even, such as $2^1 = 2$, $2^2 = 4$, etc. So $2^n - 1$ is odd for every positive integer n. Naively, based on these observations we can ask:

Is $2^n - 1$ always prime for every positive integer n?

Let us try the first few cases. For $n = 1$, we have $2^n = 2 - 1 = 1$, which is not prime. So we add the hypothesis that $n \geq 2$. Now, for $n = 2$, we have $2^n - 1 = 3$, which is prime. For $n = 3$, we have $2^n - 1 = 7$, which is prime again.

So we are quick (perhaps too quick!) to pose the following.

Conjecture 1.12. *If $n \geq 2$ is an integer, then $2^n - 1$ is a prime.*

False conjectures are often easy to disprove. This statement is no exception! For $n = 4$, we have $2^n - 1 = 15$, which is not prime since $15 = 3 \cdot 5$. This suffices to disprove the conjecture, for there exists an integer at least 2, namely 4, for which the conjectured statement is false. In other words, if the conjecture were true, then 15 would be prime, but it isn't. So the conjecture is false.

So, by the logical argument above, which is not much of an argument(!), we have proved:

Proposition 1.13. Not all integers of the form $2^n - 1$ are prime, where $n \geq 2$ is an integer.

Moreover (we leave it to you to check this), not all integers of the form $2^n + 1$ are prime, where $n \geq 0$ is an integer.

One of the goals of the book by Fletcher and Patty [**FP96**] is to develop the reader's ability to "... distinguish mathematical thinking from wishful thinking." This is very important, and we would like to add to this statement that we would like to encourage wishful thinking (that is, conjecture making) with the qualification that the reader should logically check the wishful thinking to see if they can determine whether their conjecture is true or false.

Exercise 1.9. *Prove or disprove the following conjecture: For every non-negative integer n, $3^n + 2$ is a prime number.*

So, you have to decide whether the conjecture above is true or false. How did your thinking about the truth or falsehood of the statement evolve as you thought about the exercise?

In general, mathematical results and conjectures come from observation. In a sense, mathematics is an experimental science. We look at mathematical objects and structures, such as prime numbers, and we search for patterns. We then make hypotheses about the existence of patterns based on our observations. Before we prove or disprove them, these hypotheses may be true or false for all we know. To prove a conjecture, we need to come up with a logical argument that establishes the statement of the conjecture. Typically, to disprove a conjecture, we just need to find a **counterexample**, that is, an object that does not fit the pattern we conjectured. More precisely, a counterexample to a statement is an example (a.k.a. special case) for which the statement is false.

The previous paragraph exhibits a rational way of approaching conjectures. A less rational approach, as we saw in Conjecture 1.12, is what we describe as "gonzo mathematics": rather arbitrarily hypothesizing patterns based on only a small amount of observation. In other words, jumping to conclusions. Here, due to mostly wishful thinking with only a little empirical evidence, we hypothesize patterns usually guided by beauty and simplicity, which are subjective characteristics.

One advantage of making gonzo conjectures is that we gain experience and feedback. By determining whether they are true or false, we often are inspired to make better and less gonzo (i.e., less naive) conjectures.

Thing One to Thing Two: *Did you know that gullible isn't a word?*

As in the imagined conversation above (between two Dr. Seuss characters), it is perhaps just as important to know what is false as it is to know what is true!

1.1.2.2. *Less naive conjectures that are still false.* Going back to Conjecture 1.12, we may observe that 2 and 3 are primes, whereas 4 is a composite number. Is it possible that Conjecture 1.12 is true for n prime? Let's see. For n equal to the primes $2, 3, 5, 7$ we obtain for $2^n - 1$ the integers

$$3, 7, 31, 127,$$

which are all primes. (We show below that 127 is a prime.) In general, the larger the number, the harder it is to check whether or not it is a prime.

Despite the optimistic calculations above, can you disprove the following conjecture?

Conjecture 1.14. *If $p \geq 2$ is a prime, then $2^p - 1$ is a prime.*

To see if this conjecture has a chance to be true, we check the primeness of $2^p - 1$ for the next prime $p = 11$. We obtain the integer 2047, which is equal to $23 \cdot 89$.[3] So we conclude that Conjecture 1.14 is false! So, it was a bit harder to

[3]Indeed, $23 \times 100 = 2300$. So $23 \times 90 = 2300 - 230 = 2070$. Thus $23 \times 89 = 2070 - 23 = 2047$. Quick maths!

disprove this conjecture as compared to Conjecture 1.12, but by checking a few more primes we were able to do it.

Summarizing, we have proved:

Theorem 1.15. *The following statement is false:*

"If $p \geq 2$ is a prime, then $2^p - 1$ is a prime."

In other words, there exists a prime number p such that $2^p - 1$ is not a prime. In particular this is the case for $p = 11$.

Here are $2^p - 1$, color coded, for the the primes $p < 20$:

$$3, 7, 31, 127, 2047, 8191, 131071, 524287. \tag{1.7}$$

The moral of the story is that sometimes one aptly chosen example is enough to disprove a theorem, so it often makes sense to look for such an example. Even if you don't find one, often the work of checking several examples may lead you to a pattern that leads to a proof. So, having made a conjecture, it makes sense to check the validity of a number of examples of the stated conjecture. Many conjectures fall by the wayside simply from checking some examples!

1.1.2.3. *A true conjecture about primes.* Now that we have had so many misfires in formulating conjectures, it is nice to state true conjectures. A wonderful and true result is:

Theorem 1.16. *If n is a positive integer such that $2^n - 1$ is a prime, then n itself is prime!*

For the proof of this, see Exercise 1.10 or Theorem 3.40 below.

To analyze the implication in Theorem 1.16, we'll need some elementary logic, which we briefly discuss here and which will be discussed in more detail in Chapter 3. Consider an implication of the general form:

> If P, then Q.

This statement is equivalent to its **contrapositive** implication (see §3.7 below):

> If not Q, then not P.

For example, let p be an integer greater than 2, and consider the implication:

> If p is prime, then p is odd.

Then this implication is equivalent to its contrapositive:

> If p is not odd (that is, p is even), then p is not prime.

(Recall that we are assuming that $p > 2$.)

The special case of the logical equivalence above that we find useful is: The implication in Theorem 1.16 is equivalent to its "contrapositive":

> Let n be a positive integer. If n is a composite number, then $2^n - 1$ is a composite number.

Regarding this last statement, which we have not proved yet and leave as an exercise below, let us look at some examples. We have that $2^6 - 1 = 63$ and $63 = 3^2 \cdot 7$. We observe that the non-trivial divisors of 6 are 2 and 3 and that $2^2 - 1 = 3$ and $2^3 - 1 = 7$ are divisors of $63 = 2^6 - 1$. Next, let us consider the composite number 10 and we compute that $2^{10} - 1 = 1023$ and that $1023 = 3 \cdot 11 \cdot 31$. Again, we observe that the non-trivial divisors 2 and 5 of 10 have the property that $2^2 - 1 = 3$ and $2^5 - 1 = 31$ are divisors of $1023 = 2^{10} - 1$. We might as well try one more example to see the pattern more clearly: we compute that $2^{12} - 1 = 4095$ and that $4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$. The non-trivial divisors 2, 3, 4, and 6 of 12 satisfy

$$2^2 - 1 = 3, \quad 2^3 - 1 = 7, \quad 2^4 - 1 = 15 = 3 \cdot 5, \quad 2^6 - 1 = 63 = 3^2 \cdot 7,$$

which are all divisors of $4095 = 2^{12} - 1$. All of this leads us to:

Conjecture 1.17. *If we have positive integers a, b, n satisfying $n = ab$, then $2^a - 1$ and $2^b - 1$ both divide $2^n - 1$. Thus, if n is a composite number, then $2^n - 1$ is a composite number.*

Exercise 1.10. *Prove the conjecture. Hint: Apply polynomial long division, where the polynomial variable "x" is equal to 2^a. Namely, divide the polynomial $2^n - 1 = x^b - 1$ (explain why this equality is true) by the linear polynomial $2^a - 1 = x - 1$. Then explain why this proves the conjecture.*

Since the conjecture implies Theorem 1.16*, this exercise provides a proof of the theorem.*

1.2. Even and odd integers

What is more elementary than prime numbers, but nonetheless interesting, are the notions of even and odd. We discuss elementary properties of even and odd integers, including proving properties relating to addition, multiplication, and prime numbers.

1.2.1. Properties of even and odd integers.

Question: Do you know what's odd?
Answer: Numbers that aren't divisible by two.
Rebuttal: What are the odds you are even right?

Statements involve concepts. We discuss concepts by making definitions. Even though we all know what even and odd integers are, we now give their formal definitions.

Definition 1.18. An integer n is **even** if there exists an integer a such that $n = 2a$.

For example, 98 is even since $98 = 2 \cdot 49$. That is, the integer a that exists satisfying $98 = 2a$ is $a = 49$.

Two is the only even prime:

Theorem 1.19. *If $n > 2$ is an even integer, then n is not prime.*

Proof. Since n is even, there exists an integer b such that

$$n = 2b. \tag{1.8}$$

Since $2b = n > 2$, we have $b > 1$. This and $2 > 1$ imply that n is not prime (by Lemma 1.5). □

Mini-analysis of the proof above: The proof is an example of a "direct" proof. Our aim was to show that n is the product of two integers $a, b > 1$. Using our hypothesis, we were able to do this with $a = 2$.

Two mice, Mickey and Minnie, not quite satisfied with the mini-analysis (perhaps Mickey wasn't satisfied with the earlier proofs either!), have a long and sometimes silly Socratic dialogue about the proof: [4]

Mickey: How did you do that? It looked like magic. I'm not quite convinced.

Minnie: Well, I looked at the statement and saw that we have to prove that each even integer greater than 2 is not prime. So firstly, I took such an integer.

Mickey: How do you take such an integer? Is there a store where I can buy them?

Minnie: Actually, I conjured them out of thin air by using the word "let". So we started with:

Let $n > 2$ be an even integer.

This is our hypothesis.

Mickey: Seems impenetrable to me. How can you conjure something out of nothing?

Minnie: It is like conjuring anything. For example, assume that we have a unicorn. We can always assume this. However, the key is to *prove* something about the unicorn. Since unicorns are mythical objects, we won't get very far. So let's stick to math.

Mickey: I can agree to that!

Minnie: Now, please give me an even integer.

Mickey: Okay, how about the number 2?

Minnie: Sorry! We want an integer that is greater than 2.

Mickey: Okay, then, let's take 46.

Minnie: 46 is good. We have $46 = 2 \cdot 23$, so it is not prime since $2 > 1$ and $23 > 1$. Please give me another.

Mickey: Let's try 1363.

Minnie: That's not even.

Mickey: How do you know?

Minnie: Well, $1363 = 2 \cdot 681.5$, but 681.5 is not an integer, so 1363 is not even.

Mickey: Alright, I'm feeling bold, so now let's take n, where n is even and greater than 2.

Minnie: Great! Since n is even, by definition:

There is some integer b such that $n = 2b$.

[4] Silliness is not restricted to Socratic dialogues. For example, there is the Ministry of Silly Walks.

And not only that, since $n > 2$, we also get

$$b = \tfrac{n}{2} > 1.$$

Mickey: That is all fine and dandy. Now what?

Minnie: Now we need to observe that we are actually done with the proof! Why is that? Because we have proved that our hypothesized integer n is the product of two integers: $a = 2 > 1$ and $b > 1$. By the definition of prime number (more precisely, Lemma 1.5), we see that this implies that n is not a prime number!

Mickey: So I give you an integer that is greater than 2 and equal to 2 times *something*. You tell me that this *something* is greater than 1. Since both 2 and this *something* are greater than 1, my integer, which is their product, is not prime.

Minnie: You've got it, way to go!

Mickey: You are awesome! ♡

Minnie: Thanks, so are you! ♡

As in the joke quoted at the beginning of this subsection, we have:

Definition 1.20. An integer n is **odd** if n is not even. The **parity** of an integer refers to whether it is even or odd.

For example:

Lemma 1.21. *The integer* 3 *is odd.*

Proof. Suppose for a contradiction that 3 is even. Then $3 = 2a$ for some integer a. Then $a = 1.5$, which is not an integer.[5] So we have a contradiction to the supposition that 3 is even. Now, a contradiction cannot follow from a true statement. So we conclude that 3 is not even. □

The argument above can generalized as follows.

Lemma 1.22. *Any even integer plus* 1 *is odd. In other words, if n is even, then $n + 1$ is odd.*

Proof. Let n be an even integer. Then $n = 2k$ for some integer k. Suppose for a contradiction that $n + 1$ is not odd; that is, suppose $n + 1$ is even. Then there exists an integer ℓ such that $n + 1 = 2\ell$. We conclude that $2k + 1 = n + 1 = 2\ell$, which implies that

$$1 = 2\ell - 2k = 2(\ell - k).$$

Hence, since $\ell - k$ is an integer, we have that 1 is even, a contradiction. (Alternatively, $\ell - k = \frac{1}{2}$ is not an integer, a contradiction.) Therefore $n + 1$ is odd. □

Finally, we remark that we should be careful with how we state results. By Theorem 1.19, each of the statements in the following corollary, when interpreted correctly, is true!

Corollary 1.23. *All prime numbers are odd except one. Actually, all prime numbers are odd except two.*

[5] Alternatively, since $2 < 3 = 2a < 4$, we have $1 < a < 2$, so that a is not an integer.

Indeed, in the first sentence we mean "... except *one* of the prime numbers", while in the second sentence we mean "... except the prime number *two*"! So, in the statements of the corollary we were ambiguous. Having learned our lesson, from now on we will be more careful to write clear mathematical statements.

If you are not sure about the proof of this corollary, for a hint see Exercise 3.28 below in the chapter on implications and all that.

1.2.2. Even and odd and addition.

Question: How do you make seven an even number?
Answer: Remove the "s".

In this subsection and the next, we discuss the properties of even and odd with respect to the arithmetic operations of addition and multiplication. To wit, we answer the question: How does parity *interact* with addition and multiplication? Here are the answers.

Theorem 1.24. *The sum of two even integers is even. In other words, if a and b are even integers, then the integer $a + b$ is even.*

Proof. Suppose that a and b are even integers. Then there exist integers k and ℓ such that $a = 2k$ and $b = 2\ell$. We *calculate* that

$$a + b = 2k + 2\ell = 2(k + \ell). \tag{1.9}$$

Since $k+\ell$ is an integer (the sum of two integers is an integer), by (1.9) we conclude that $a + b$ is even. □

Regarding the proof of Theorem 1.24, if you prefer to think visually, we offer Figure 1.2.1.

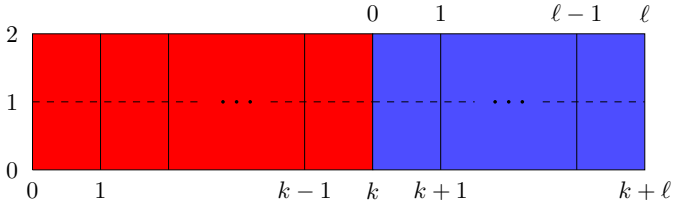

Figure 1.2.1. A visual proof that an even number plus an even number is even: $a = 2k$ and $b = 2\ell$ implies $a + b = 2(k + \ell)$.

Theorem 1.25. *The sum of an even integer and an odd integer is odd.*

Proof 1 of Theorem 1.25. This proof uses a fact which we will not prove until a fair bit later in the book. Thankfully, this fact is something you are most likely familiar with and take for granted as being true.

Fact 1.26. *If a is an odd integer, then there exists an integer k such that*

$$a = 2k + 1.$$

That is, any odd integer can be written as an even number plus 1.

As an example, 17 is odd, and $17 = 2 \cdot 8 + 1$. See Corollary 1.41 below for how this fact follows from the "Division Theorem" (Theorem 4.1 below). We now *boldly* proceed to prove the theorem.

> To boldly go where no person has gone before! – Star Trek

Let a be an odd integer and let b be an even integer. Since a is odd, by the fact above, there exists an integer k such that $a = 2k + 1$. Since b is even, there exists an integer ℓ such that $b = 2\ell$. We calculate that

$$a + b = (2k + 1) + 2\ell = 2(k + \ell) + 1. \tag{1.10}$$

Since $k + \ell$ is an integer, by (1.10) and Lemma 1.22, we have that $a + b$ is odd. □

Proof 2, by contradiction, of Theorem 1.25. By the commutativity of addition, we may assume that the first integer is even and the second integer is odd. So let a be an even integer and let b be an odd integer. Then there exists an integer k such that $a = 2k$.

Suppose for a contradiction that $a + b$ is not odd; that is, it is even. Then there exists an integer m such that $a + b = 2m$. We calculate that

$$b = (a + b) - a = 2m - 2k = 2(m - k). \tag{1.11}$$

Since $m - k$ is an integer (the difference of two integers is an integer), we conclude that b is even. This is a contradiction to our assumption. Therefore we conclude that $a + b$ is odd! □

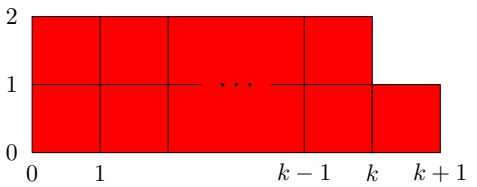

Figure 1.2.2. Visualization of an odd integer: a is odd implies that there exists an integer k such that $a = 2k + 1$.

Theorem 1.27. *The sum of two odd integers is even.*

Proof. Let a and b be odd integers. By this hypothesis and Fact 1.26, there exist integers k and ℓ such that $a = 2k + 1$ and $b = 2\ell + 1$. We calculate that

$$a + b = (2k + 1) + (2\ell + 1) = 2(k + \ell + 1). \tag{1.12}$$

Since $k + \ell + 1$ is an integer, we conclude from (1.12) that $a + b$ is even. □

Exercise 1.11. *Give visual proofs of Theorems* 1.25 *and* 1.27 *where the drawing is analogous to Figure* 1.2.1. *See also Figure* 1.2.2.

1.2.3. Even and odd and multiplication. Observe that 6 is an even integer, and for every integer b, we have that $6b = 2(3b)$. Since $3b$ is an integer, we conclude that $6b$ is an even integer for every integer b. In general, we have the following.

Theorem 1.28. *The product of any integer and an even integer is even.*

Proof. Without loss of generality, we assume that the first integer is even. Let a be an even integer and let b be an integer. Since a is even, there exists an integer k such that $a = 2k$. We calculate that

$$ab = (2k)b = 2(kb). \tag{1.13}$$

Of course, kb is an integer. So (1.13) proves that ab is even. □

Exercise 1.12. *Show that Theorem* 1.28 *may be restated as:*

If 2 *divides* a *and if* b *is an integer, then* 2 *divides* ab.

A visual proof of Theorem 1.28 is given by Figure 1.2.3.

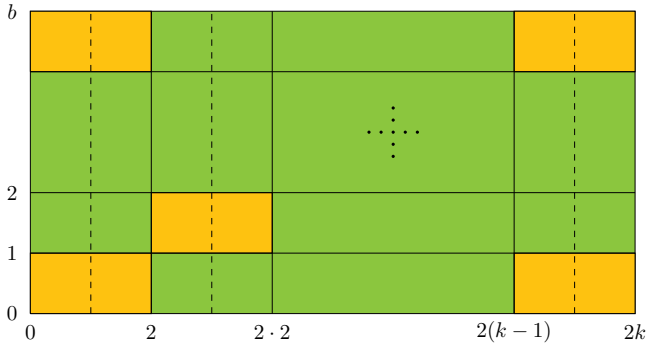

Figure 1.2.3. A visual proof of Theorem 1.28: Suppose $a = 2k$ for some integer k. We see that there are an even number of total squares in the rectangle representing the product. Can you think of an easier visual proof by dividing the $a \times b$ rectangle into only two subrectangles?

Theorem 1.29 (An odd fact)**.** *The product of two odd integers is odd.*

Proof. Let a and b be odd integers, by Fact 1.26 there exist integers k and ℓ such that $a = 2k + 1$ and $b = 2\ell + 1$. We calculate that

$$ab = (2k + 1)(2\ell + 1) = 2(2k\ell + k + \ell) + 1. \tag{1.14}$$

Since $2k\ell + k + \ell$ is an integer, from this we conclude that ab is odd. □

Exercise 1.13. *Give a visual proof of Theorem* 1.29.

By taking the two integers to be equal in each of the previous two theorems, we have:

Corollary 1.30. (1) *The square of an even integer is even.*

(2) *The square of an odd integer is odd.*

Direct proof of part (1) of Corollary 1.30. Let n be an even integer. By definition, $n = 2k$ for some $k \in \mathbb{Z}$. We compute that

$$n^2 = (2k)^2 = 2 \cdot 2k^2. \tag{1.15}$$

Since $2k^2 \in \mathbb{Z}$ (the product of integers is an integer), we conclude that n^2 is even. □

Exercise 1.14. *Prove: The cube of an even integer is even. The cube of an odd integer is odd.*

Exercise 1.15. *Prove that if the product of two integers is even, then at least one of the integers is even.*

1.3. Calculating primes and the sieve of Eratosthenes

Now we return to the subject of primes, our first love. Wouldn't it be nice to be able to rather easily figure out which numbers are primes? Fortunately, for numbers that are not too large, this is possible even if you are cast away on a deserted island with only food, water, pencil, and paper!

1.3.1. A shortcut for proving that an integer is a prime. To solve Exercise 1.8, for the prime 11 for example, you presumably checked for all divisors a with $1 < a < 11$ and came up empty. Interestingly, you only need to know that 2 and 3 do not divide 11 to show that 11 is not a prime. You will see why this is true from our discussion below.

Recall the following elementary fact about inequalities: Let a, b, c be real numbers and suppose that $c \geq 0$.

$$\text{If } b \geq a, \text{ then } cb \geq ca. \tag{1.16}$$

For example, if $b \geq a$, then $3b \geq 3a$. For another useful example, suppose that a and b are positive real numbers. By taking $c = \frac{1}{ab}$, we obtain:

$$\text{If } b \geq a > 0, \text{ then } \frac{1}{a} \geq \frac{1}{b} > 0. \tag{1.17}$$

By combining (1.16) and (1.17), we obtain:

$$\text{If } b \geq a > 0 \text{ and } m \geq 0, \text{ then } \frac{m}{a} \geq \frac{m}{b}. \tag{1.18}$$

Another result that we will find useful is:

Fact 1.31. *For every integer $n \geq 2$, there exists a prime p dividing n.*

This is Corollary 1.55 below. In particular, if n is a prime, then we simply take $p = n$. On the other hand, if n is a composite number, then this says that n has a prime divisor. For example, for $n = 24$ we may take $p = 2$ or $p = 3$.

We now return to the unfinished business from §1.1.2.2 of showing that 127 is a prime. Suppose that $127 = ab$, where a and b are positive integers. **Without loss of generality**, we may assume that $b \geq a$. We then get that (simply take $c = a$ in (1.16))

$$127 = ab \geq aa = a^2. \tag{1.19}$$

Since $a^2 \leq 127$, by taking square roots, we obtain

$$a \leq \sqrt{127}. \tag{1.20}$$

More generally, if $a^2 \leq b^2$ and $b \geq 0$, then $a \leq b$. In this paragraph we proved that **if** 127 is the product of two (non-trivial) factors, **then** the smaller of the two is at most the square root of 127.

From (1.20) we deduce that

$$a \leq \sqrt{127} < \sqrt{144} = 12. \tag{1.21}$$

Since $a < 12$ is an integer, we have that $a \leq 11$. To summarize, we have proved that if 127 is a composite number, then 127 has a divisor a satisfying $1 < a \leq 11$. In other words, if 127 does not have a divisor a satisfying $1 < a \leq 11$, then 127 is prime. Indeed this is the case and we leave it to you, the reader, to check this.

We can make the job of proving that 127 is a prime even easier. We have the following:

Fact 1.32. *If* 127 *is not prime, then* 127 *has a* **prime** *divisor* $1 < p \leq 11$. *Equivalently: If* 127 *does not have a* **prime** *divisor* $1 < p \leq 11$, *then* 127 *is prime.*

The reason this is true is as follows. As we have seen above, if 127 is not prime, then it has a divisor a satisfying $1 < a \leq 11$. Since $a > 1$, there exists a prime p dividing a (see Corollary 1.55 below). Since p divides a, we have $p \leq a \leq 11$. Also because p divides a and since a divides 127, we have that p divides 127 (by the "transitivity of division"). This proves Fact 1.32. □

For a more general and slightly more detailed version of this argument, see the proof of Theorem 1.34 below.

Exercise 1.16. *Prove that* 11 *is prime by showing that it is not divisible by* 2 *or by* 3. *Include a justification of why this suffices.*

Does this exact same method work for every integer strictly between 1 *and* 16*? Explain why or why not.*

As we have seen in the discussion above, taking square roots is useful.

> I poured root beer into a square cup. Now I have beer.

A mathematician translates this quote to the equation

$$(\sqrt{\text{beer}})^2 = \text{beer}. \ \text{☺}$$

Generalizing what we did for the number 127 above, we observe the following.

Lemma 1.33. *An integer* $n > 1$ *is composite if and only if there exists a divisor* a *of* n *satisfying* $1 < a \leq \sqrt{n}$.

Proof. An integer $n > 1$ is composite if and only if there exist integers $a > 1$ and $b > 1$ such that $ab = n$. Without loss of generality, we may assume that $a \leq b$. This implies that $a^2 \leq ab = n$, so that $a \leq \sqrt{n}$.

Conversely, suppose that $n > 1$ is an integer with a divisor a of n satisfying $1 < a \leq \sqrt{n}$. Since $n > 1$, we have $1 < a < n$. By Corollary 1.10, this proves that n is a composite number. □

In fact, we have an even nicer statement:

Theorem 1.34. *An integer $n > 1$ is composite if and only if there exists a prime divisor p of n satisfying $p \leq \sqrt{n}$.*

Equivalently, an integer $n > 1$ is prime if and only if for every prime $p \leq \sqrt{n}$, p does not divide n.

Proof. Let $a > 1$ be an integer. By Corollary 1.55, a has a prime divisor p; that is, there exists a prime p such that $a = pk$ for some integer k.

Now assume in addition that $a \leq \sqrt{n}$ and a is a divisor of n. Then there exists a positive integer b such that $n = ab$. Thus,

$$n = ab = pk \cdot b = p \cdot kb,$$

where p is prime and $p \leq kb$. Therefore, p is a prime divisor of n satisfying $p \leq \sqrt{n}$.

To summarize, we have proved: If $1 < a \leq \sqrt{n}$ is a divisor of n, then there exists a prime divisor p of n satisfying $p \leq \sqrt{n}$.

Conversely, clearly if there exists a prime divisor p of n satisfying $p \leq \sqrt{n}$, then there exists a divisor a of n satisfying $1 < a \leq \sqrt{n}$, namely $a = p$.

Finally, by Lemma 1.33, an integer $n > 1$ being composite is equivalent to there existing a divisor a of n satisfying $1 < a \leq \sqrt{n}$. So we are done. □

Remark 1.35. Regarding the equivalence of the two statements in the theorem above, we observe it is true by the following general fact, which will be proved in Chapter 3. A statement of the form "P if and only if Q" is equivalent to the statement "(not P) if and only if (not Q)".

Theorem 1.34 allows us to efficiently decide for example if integers less than $1024 = 2^{10}$ are prime, as we only need to see if they are divisible by the primes less than $32 = 2^5$.

We may also use Theorem 1.34 to help find the prime factorizations of numbers. For example, to find the prime factorization of 2074, by Theorem 1.34 we know that if 2074 is not prime, then it has a prime divisor at most $\sqrt{2074} \approx 45.5$. Indeed, since 2074 is even, 2 is a divisor of 2074. Dividing 2074 by 2 yields 1037. Now, if 1037 is not prime, then it has a prime divisor at most $\sqrt{1037} \approx 32.2$. It turns out that 17, which is less than $\sqrt{1037}$, is a prime divisor of 1037. Dividing 1037 by 17 yields 61. Finally, 61 is a prime, which can be verified by showing that it has no prime divisors at most $\sqrt{61}$. Since $\sqrt{61} < 8$, to show that 61 is prime, we just need to check that none of the primes $2, 3, 5, 7$ divide 61, which is true. By combining all of the above, we obtain

$$2074 = 2 \cdot 1037 = 2 \cdot 17 \cdot 61, \tag{1.22}$$

where the last equality gives the prime factorization of 2074.

Exercise 1.17. *Let a and b be positive real numbers satisfying $ab = 10000$. Prove that $a \leq 100$ or $b \leq 100$.*

Hint: Can you derive a contradiction if $a > 100$ and $b > 100$? Recall that we used proof by contradiction in the proof of Lemma 1.21.

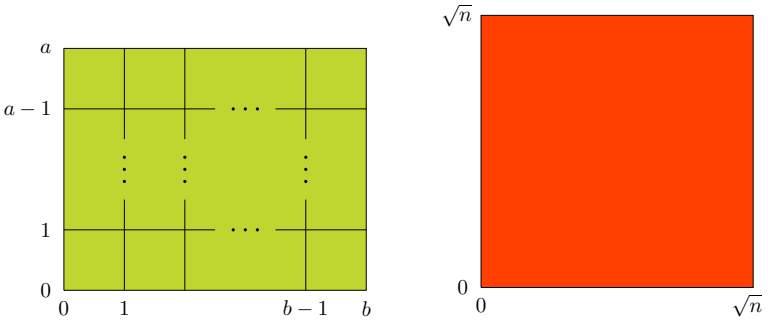

Figure 1.3.1. If $n = ab$ and $a \leq b$, then $a \leq \sqrt{n}$. The rectangle and the square have the same area n.

Commentary: You may have to use some (elementary) rules of logic, which you are likely familiar with. These logic rules are also discussed more formally later in the book. See, e.g., Chapter 3.

Exercise 1.18. *By the proof of Lemma* 1.33*, we have: If $n = ab$, where a, b are positive integers, then at least one of a, b is less than or equal to $\sqrt{n}$.*

Now, suppose that $n = abc$, where a, b, c are positive integers. Prove that at least one of a, b, c is less than or equal to $\sqrt[3]{n}$.

Example 1.36. If n is a positive integer less than or equal to 100, then by Theorem 1.34 we have that n is prime if and only if it is not divisible by any of $2, 3, 5, 7$ since these are the primes at most $10 = \sqrt{100}$.

If n is a positive integer less than 49, then n is prime if and only if it is not divisible by any of $2, 3, 5$.

If n is a positive integer less than 25, then n is prime if and only if it is not divisible by any of $2, 3$.

In this way, it is quite easy to come up with the list of primes in (1.6).

Figure 1.3.2. Eratosthenes (276 BC–194 BC). Wikimedia Commons, Public Domain.

Exercise 1.19. *Verify that the primes less than 100 are given by the list in* (1.6)*. A convenient way to carry this out is to use the sieve of Eratosthenes. Namely,*

cross out all the non-trivial (greater than 1*) multiples of* 2*. Look for the smallest integer greater than* 2 *that isn't crossed out, which is* 3*. Now cross out all the non-trivial multiples of* 3*. Look for the smallest integer greater than* 3 *that isn't crossed out, which is* 5*, and cross out all the non-trivial multiples of* 5*. Look for the smallest integer greater than* 5 *that isn't crossed out, which is* 7*, and cross out all the non-trivial multiples of* 7*. Since the smallest integer greater than* 7 *that isn't crossed out is* 11*, which is greater than* $\sqrt{100} = 10$*, we stop at* 7*. The remaining integers are primes (don't count* 1*). (Note that in this way we have actually verified that* $2, 3, 5, 7$ *are the primes less than or equal to* 10*.)*

01	02	03	04	05	06	07	08	09	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Figure 1.3.3. Cross out all of the multiples of 2, 3, 5, 7 between 1 and 100. Compare the integers remaining with a list of primes between 1 and 100. Are these two sets of integers the same?

Exercise 1.20. *Find the primes between* 101 *and* 200 *using the sieve of Eratosthenes (you can read about this at the "Sieve of Eratosthenes" Wikipedia link, but we give a brief description below). See also Figure* 1.6.1 *for the primes between* 1 *and* 100*. In short, the sieve works by crossing out all multiples of at least* 2 *or more of the primes starting with the lowest prime first. For example, for the prime* 2 *we cross out*

$$100, 102, 104, 106, 108, \ldots, 200.$$

For the prime 3*, we cross out*

$$102, 105, 108, 111, 114, \ldots, 198.$$

(Note that there are redundancies.) Did considering primes greater than 13 *help?*

Hints: See Figure 1.3.4 *and use Theorem* 1.34*.*

101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Figure 1.3.4. Cross out all of the multiples of 2, 3, 5, 7, 11, and 13 between 101 and 200. Compare the integers remaining with a list of primes between 101 and 200. Are these two sets of integers the same?

Exercise 1.21. *Disprove the following conjecture (i.e., prove that the statement is false): For every non-negative integer n, $F_n := 2^{2^n} + 1 := 2^{(2^n)} + 1$ is a prime. You may wish to use some sort of computer aid (instead of working it out with paper and pencil).*

Remarkably, F_n is known to be composite for all $5 \leq n \leq 32$. (Do not try to prove this full statement!) Why can we characterize this as extrapolation gone wrong?

1.4. Division

Primes are intimately related to multiplication and division. In this section we further consider division and some more of its elementary properties, and we also learn about some basic properties of the greatest common divisor of two integers.

1.4.1. Factoring 1.

"One and one make one." – From "Bargain" by The Who

The rock group, The Who, were evidently thinking about multiplication. And what can be simpler than the multiplicative identity? The following, which we could have proved earlier(!), says that there is no other way to make *one* via multiplication of positive integers. So a mathematician would amend The Who's lyrics by adding "uniquely"!

Theorem 1.37. *Suppose that a and b are positive integers satisfying $ab = 1$. Then $a = b = 1$.*

Proof. Let a and b be positive integers satisfying $ab = 1$. Suppose for a contradiction that $a > 1$. Then, since $b \geq 1$ and by (1.16), we have

$$1 = a \cdot b \geq a \cdot 1 = a > 1, \tag{1.23}$$

which is a contradiction. Thus $a \leq 1$, and hence $a = 1$ since $a > 0$. This implies that

$$b = \frac{1}{a} = 1. \tag{1.24}$$

□

Have you thought of any alternate proofs of Theorem 1.37? Figure 1.4.1 gives us an idea for one.

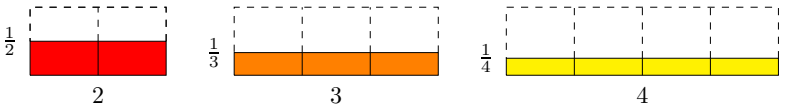

Figure 1.4.1. Visual idea for a proof of Theorem 1.37. The area of each colored region is equal to 1.

Alternate proof of Theorem 1.37. Suppose for a contradiction that $a > 1$. Since $\frac{1}{a}$ is a positive real number, we then have

$$1 = \frac{1}{a} \cdot a > \frac{1}{a} \cdot 1 = \frac{1}{a} = b > 0. \tag{1.25}$$

This is a contradiction since there is no integer strictly between 0 and 1. □

Given a result, it is usually interesting to consider special cases. In this case, for variety and to add a twist, we consider *negative* numbers instead of positive numbers in our special case:

Corollary 1.38. *There exists a unique negative integer n such that $n^2 = 1$. Namely, $n = -1$.*

Proof. Suppose that n is an integer satisfying $n^2 = 1$. Then $|n|$ is a non-negative integer satisfying

$$|n|^2 = n^2 = 1. \tag{1.26}$$

Suppose that $|n| = 0$. Then $0 = 0^2 = |n|^2 = 1$, which is a contradiction. Thus $|n|$ is a positive integer. So, by the preceding theorem, since $|n|\,|n| = 1$, we conclude that $|n| = |n| = 1$. Finally, this implies that $n = -1$ or $n = 1$. But since n is negative, we must have that $n = -1$. Since $(-1)^2 = 1$, we have proved that $n = -1$ is the unique negative integer with $n^2 = 1$. □

Here is an **Alternate proof of Corollary 1.38**, which implicitly assumes a couple of more facts but is shorter: By hypothesis, we have

$$1 = \sqrt{1} = \sqrt{n^2} = |n|. \tag{1.27}$$

This implies that $n = 1$ or $n = -1$. Since n is negative, $n = -1$. So we are done since $(-1)^2 = 1$.

Exercise 1.22. *Prove that there exists a unique positive integer n such that $n^2 = 1$.*

1.4.2. Division and its elementary properties. Recall that we say that an integer a **divides** an integer b if there exists an integer k such that

$$ak = b. \tag{1.28}$$

We also say that b is a **multiple** of a. Recall that we say that a is a **divisor** of b.

For example, 15 is a multiple of 3 since $3 \cdot 5 = 15$. And 3 is a divisor of 15.

By definition, an integer n is even if and only if n is a multiple of 2. An integer m is odd if and only if m is not a multiple of 2.

Figure 1.4.3 visualizes that 7 does not divide 139.

Theorem 1.37 says that the only positive divisor of 1 is 1 itself.

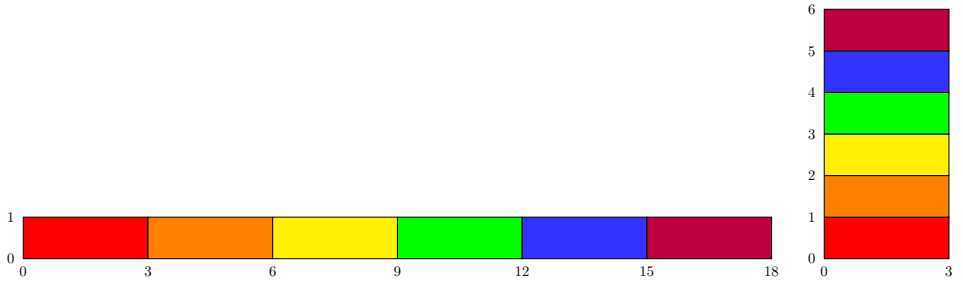

Figure 1.4.2. From these rectangles, we see that 18 is divisible by 3 and 6. The only other non-trivial way to factor 18 is as 2 times 9. So the positive divisors of 18 are $\mathrm{Div}(18) = \{1, 2, 3, 6, 9, 18\}$.

Observe that 7 divides 14 and that 5 divides 15, so the product $7 \cdot 5$ divides the product $14 \cdot 15$. More generally, we have the following.

Solved Problem 1.39 (Division and products)**.** *All quantities are integers. If a divides b and if c divides d, then ac divides bd.*

Solution. Since a divides b and c divides d, there exist integers k and ℓ such that

$$b = ka, \qquad d = \ell c. \tag{1.29}$$

Thus, multiplying these two integers, we obtain

$$bd = ka\ell c = k\ell ac \tag{1.30}$$

(where we used the commutativity of multiplication for the second equality). Since $k\ell$ is an integer, we conclude that ac divides bd by the definition of divides.

Exercise 1.23. *Show that if an integer a divides an integer b and if c is an integer, then a divides bc. Hint: You may pattern your proof after the proof of Theorem* 1.28.

Another way to say this is: If a divides b and if d is a multiple of b, then a divides d.

Show that, as a special case of this statement, we have: If a divides b, then a divides b^2.

Exercise 1.24. *Observe that* 3 *divides* 6*, and related to this,* 9 *(the square of* 3*) divides* 36 *(the square of* 6*).*

Generalizing this, prove: If 3 *divides* b*, then* 9 *divides* b^2*.*

Generalizing again, prove: If a *divides* b*, then* a^2 *divides* b^2*.*

Although the following has been observed earlier in this chapter, it is good for you to work it out again as an exercise.

Exercise 1.25. *Prove: If* a *divides* b *and if* b *divides* c*, then* a *divides* c*.*

1.4.3. The statement of the Division Theorem. Consider for example the problem of dividing 139 by 7 to get a remainder. That is, we are looking for the *largest* integer q, called the **quotient**, for which $7q \leq 139$. We then define the **remainder** to be

$$r = 139 - 7q; \quad \text{that is,} \quad 139 = 7q + r. \tag{1.31}$$

By a short calculation, we see that

$$q = 19 \quad \text{and} \quad r = 6.$$

Indeed, we have $139 = 7 \cdot 19 + 6$, whereas $q = 20$ would yield $7q = 140 > 139$ and hence produce a negative remainder. This can be visualized as in Figure 1.4.3. Observe that the remainder satisfies $r = 6 < 7$. On the other hand, if we took q to be smaller, e.g., $q = 18$, then we would obtain a remainder $r \geq 7$, e.g., in this case $r = 13$. To summarize, $q = 19$ and $r = 6$ are the unique integers satisfying

$$139 = 7q + r \quad \text{and} \quad 0 \leq r < 7.$$

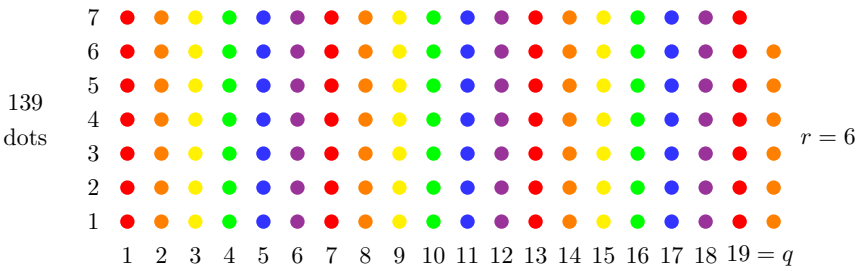

Figure 1.4.3. A visual rendering of the Division Theorem example that $139 = 7q + r$ has quotient $q = 19$ and remainder $r = 6$.

The general statement of the **Division Theorem**, which we prove in Chapter 4, is the following.

Theorem 1.40. *Let* a *be an integer and let* m *be a positive integer. Then there are unique integers* q *and* r *such that*

$$a = m\,q + r \quad \textit{and} \quad 0 \leq r < m. \tag{1.32}$$

That is, if we divide an integer a *by a positive integer* m*, then we get a unique quotient* q *and remainder* r*.*

By considering the special case $m = 2$ of the Division Theorem and since $0 \leq r < 2$ means the same thing as $r = 0$ or $r = 1$, we have:

Corollary 1.41. *Let a be an integer. Then there are unique integers q and r such that*

$$a = 2q + r \quad \text{and} \quad r = 0 \ \text{ or } \ r = 1. \tag{1.33}$$

Furthermore, $r = 0$ if and only if a is even, and $r = 1$ if and only if a is odd.

Example 1.42. We can use the Division Theorem to show that the integer 139 is a prime. To see this, we just need to check that none of the primes $2, 3, 5, 7, 11$ divide 139, since these are the primes less than 12, and $12^2 = 144 > 139$. We can see this as follows. By the Division Theorem, we may divide 139 by a prime p to get

$$139 = p \cdot q + r, \tag{1.34}$$

where the remainder r satisfies

$$0 \leq r < p.$$

Then the table in Figure 1.4.4 shows that none of the remainders r is equal to zero. Hence 139 is prime.

p	q	r
2	69	1
3	46	1
5	27	4
7	19	6
11	12	7

Figure 1.4.4. Table of values of primes $p \leq \sqrt{139}$, factors q, and remainders r, where $139 = p \cdot q + r$. Since the last column has no zeroes, 139 is a prime.

For example, the first row of Figure 1.4.4 is because $139 = 2 \cdot 69 + 1$ and $0 \leq 1 < 2$.

Remark 1.43. Without using the Division Theorem, one can show that 139 is prime by verifying that $\frac{139}{p}$ is not an integer for each of $p = 2, 3, 5, 7, 11$.

1.5. Greatest common divisor

Given two integers, what do they have in common from the point of view of *multiplication*? The answer is given by the greatest common divisor. We begin by discussing examples and then we give the formal definition of the greatest common divisor.

1.5.1. Definition of the greatest common divisor. What do the integers 51 and 68 have in common from the point of view of multiplication? Firstly, we observe that 17 divides 51 and 51 is a multiple of 17. This is because $17 \cdot 3 = 51$. By inspection, we see that the set of positive divisors of 51 is

$$\mathrm{Div}(51) := \{1, 3, 17, 51\}. \tag{1.35}$$

Secondly, we also observe that 17 divides 68. The set of positive divisors of 68 is

$$\text{Div}(68) := \{1, 2, 4, 17, 34, 68\}. \tag{1.36}$$

If we compare the lists of divisors for both 51 and 68, we see that the common divisors of 51 and 68 are 1 and 17. Thus, the *greatest common divisor* of 51 and 68 is the number 17. We write this as

$$\gcd(51, 68) = 17. \tag{1.37}$$

That is, the largest integer that divides both 51 and 68 is the number 17.

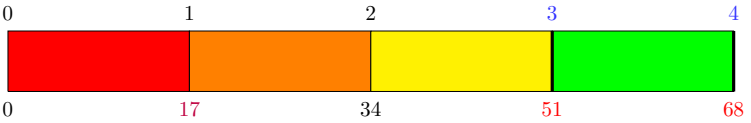

Figure 1.5.1. The gcd of 51 and 68 is 17: after factoring 51 and 68 by 17 we get 3 and 4, which are coprime.

From the examples of 51 and 68, you may have anticipated the following.

Exercise 1.26. *Prove that a divisor of a positive integer b that is not equal to b cannot be more than one-half of b.*

We will find the notion of the maximum of two (or sometimes more) numbers useful. We embark on a brief excursion regarding the maximum. The **maximum** of two real numbers a and b is defined by

$$\max\{a, b\} := \begin{cases} a & \text{if } a \geq b, \\ b & \text{if } a < b. \end{cases} \tag{1.38}$$

Similarly, we define the **minimum** of two real numbers a and b by

$$\min\{a, b\} := \begin{cases} b & \text{if } a \geq b, \\ a & \text{if } a < b. \end{cases} \tag{1.39}$$

Solved Problem 1.44 (Being bigger than the bigger of the two is the same as being bigger than both!)**.** *Let a and b be real numbers.*

(1) *Prove that* $\max\{a, b\} \geq a$ *and* $\max\{a, b\} \geq b$.

(2) *Prove that for every* $x \in \mathbb{R}$,

$$x \geq \max\{a, b\} \quad \textit{if and only if} \quad (x \geq a \textit{ and } x \geq b). \tag{1.40}$$

Solution. Let $m := \max\{a, b\}$.

(1) *Case i*: $a \geq b$. In this case, $m = a \geq b$, so $m \geq a$ and $m \geq b$.

Case ii: $a < b$. In this case, $m = b > a$, so again $m \geq a$ and $m \geq b$.

Since for every real number a and b, we have $a \geq b$ or $a < b$, we have proved (1). Aside: Two elementary facts which we have used are: $x = y$ implies $x \geq y$ and $x > y$ implies $x \geq y$.

(2) (**Only if**) Suppose $x \geq m$. Then, by part (1) we have $x \geq m \geq a$ and $x \geq m \geq b$. Thus, by the transitivity of the relation $\geq$, we conclude that $x \geq a$ and $x \geq b$.

(**If**) Suppose $x \geq a$ and $x \geq b$.

Case i: $a \geq b$. In this case, $m = a \leq x$, so $x \geq m$.

Case ii: $a < b$. In this case, $m = b \leq x$, so again $x \geq m$.

This proves (2). □

Exercise 1.27. *Let a and b be real numbers.*

(1) *Prove that* $\min\{a, b\} \leq a$ *and* $\min\{a, b\} \leq b$.

(2) *Prove that for every* $x \in \mathbb{R}$,

$$x \leq \min\{a, b\} \quad \textit{if and only if} \quad (x \leq a \text{ and } x \leq b). \tag{1.41}$$

Solved Problem 1.45. *Let a and b be positive odd integers greater than* 1. *Prove that*

$$ab \geq \max\{3a, 3b\}. \tag{1.42}$$

Solution. Since a is an odd integer and $a > 1$, we have $a \geq 3$. Indeed, 2 is even, and hence not odd. For the same reasons, $b \geq 3$. Thus by (1.16),

$$ab \geq 3b \quad \text{and} \quad ab \geq a3. \tag{1.43}$$

Since we have both $ab \geq 3b$ and $ab \geq 3a$, we conclude by Solved Problem 1.44(2) that $ab \geq \max\{3a, 3b\}$. □

Exercise 1.28. *Let a and b be positive integers. Prove that*

$$ab \geq \max\{a, b\}. \tag{1.44}$$

Hint: Any positive integer is at least 1.

Example 1.46 (Positive divisors of an integer)**.** If a positive integer a divides 1575, then $a \leq 1575$ by Lemma 1.8. One can also calculate (or at least verify!) that

$$1575 = 3^2 \cdot 5^2 \cdot 7. \tag{1.45}$$

In particular, the prime divisors of 1575 are 3, 5, and 7. One can check that the positive divisors of 1575 are

$$\begin{aligned} &1,\ 3,\ 3^2,\ 5,\ 3 \cdot 5,\ 3^2 \cdot 5,\ 5^2,\ 3 \cdot 5^2,\ 3^2 \cdot 5^2, \\ &7,\ 3 \cdot 7,\ 3^2 \cdot 7,\ 5 \cdot 7,\ 3 \cdot 5 \cdot 7,\ 3^2 \cdot 5 \cdot 7,\ 5^2 \cdot 7,\ 3 \cdot 5^2 \cdot 7,\ 3^2 \cdot 5^2 \cdot 7. \end{aligned} \tag{1.46}$$

Calculating the numerical values of this list of positive divisors yields

$$\begin{aligned} &1,\ 3,\ 9,\ 5,\ 15,\ 45,\ 25,\ 75,\ 225, \\ &7,\ 21,\ 63,\ 35,\ 105,\ 315,\ 175,\ 525,\ 1575. \end{aligned} \tag{1.47}$$

Observe that the integers in (1.46) are exactly of the form

$$3^a \cdot 5^b \cdot 7^c, \tag{1.48}$$

where $0 \leq a \leq 2$, $0 \leq b \leq 2$, and $0 \leq c \leq 1$. That is, the list of integers in (1.46) consists of $3^a \cdot 5^b \cdot 7^c$, where the triples (a, b, c) are given by

(1.49)
$(0,0,0),\ (1,0,0),\ (2,0,0),\ (0,1,0),\ (1,1,0),\ (2,1,0),\ (0,2,0),\ (1,2,0),\ (2,2,0),$

(1.50)
$(0,0,1),\ (1,0,1),\ (2,0,1),\ (0,1,1),\ (1,1,1),\ (2,1,1),\ (0,2,1),\ (1,2,1),\ (2,2,1).$

Exercise 1.29. *Can you come up with a conjecture about the relationship between factoring a number as a product of primes and the list of positive divisors of that number?*

Given a positive integer a, let $\mathrm{Div}(a)$ denote the set of positive divisors of a.

Given $m \in \mathbb{Z}^+$, let

$$\mathbb{N}_m := \{1, 2, 3, \ldots, m\} \tag{1.51}$$

be the set of the first m positive integers.

By Lemma 1.8, any positive divisor of a is an integer between 1 and a, inclusive, so that

$$\mathrm{Div}(a) \subset \mathbb{N}_a. \tag{1.52}$$

Given two non-zero integers a and b, the set of **common divisors** of a and b is

$$\mathrm{ComDiv}(a, b) = \mathrm{Div}(a) \cap \mathrm{Div}(b). \tag{1.53}$$

Here, the symbol $\cap$ is denotes "intersection". The **intersection** of two sets A and B is defined to be the set of elements that are in both sets.[6] So $\mathrm{ComDiv}(a, b)$ is the set of integers c such that c is a divisor of both a and b. For example, by (1.35) and (1.36), we see that

$$\mathrm{ComDiv}(51, 68) = \{1, 17\}$$

since 1 and 17 are the only integers in both $\mathrm{Div}(51)$ and $\mathrm{Div}(68)$.

We leave it to you to check that

$$\mathrm{ComDiv}(18, 24) = \{1, 2, 3, 6\}, \tag{1.54}$$

and so $\gcd(18, 24) = 6$.

Observe that for all positive integers a and b,

$$\mathrm{ComDiv}(a, b) \subset \mathbb{N}_a \cap \mathbb{N}_b = \mathbb{N}_{\min\{a,b\}}. \tag{1.55}$$

For example, $\mathrm{ComDiv}(51, 68) \subset \mathbb{N}_{51}$.

If one of the integers, say a, is equal to zero, then we have the following:

$$\mathrm{Div}(0) = \mathbb{Z}, \qquad \mathrm{ComDiv}(0, b) = \mathrm{Div}(b). \tag{1.56}$$

In particular, for every two non-negative integers a and b, where at most one of them is zero, there always exists a **greatest common divisor**, which we denote by

$$\gcd(a, b). \tag{1.57}$$

Exercise 1.30. *Show that* $\gcd(5 \cdot 17, 23 \cdot 17) = 17$.

A potentially divisive conversation that ends up finding common ground:

> Alpha: What do we have in common?
> Beta: I don't know. What are your divisors?

And the conversation continues. Can you fill in how it might go?

[6] We will discuss set theory in more detail, including the notation of intersection, in Chapter 5.

Solved Problem 1.47 (Odd integers have nothing in common with 2 multiplicatively)**.** *Let n be an odd integer. Prove that* $\gcd(2, n) = 1$.

Solution. We have that $g := \gcd(2, n)$ is a positive integer dividing 2. Thus $g = 1$ or $g = 2$. Suppose for a contradiction that $g = 2$. Then 2 divides n, which implies that n is even, which contradicts the assumption that n is odd. Therefore $g \neq 2$, so that $g = 1$. □

Solved Problem 1.48 (The gcd and multiples)**.** *Prove that if a is a positive integer, then*

$$\gcd(a, 6) \leq \gcd(a, 30). \tag{1.58}$$

Solution. Let $g := \gcd(a, 6)$. Then g divides a, and g divides 6. Since 6 divides 30, this implies that g divides 30. Therefore g divides both a and 30, which implies that $g \leq \gcd(a, 30)$ by the definition of the greatest common divisor of a and 30. □

The property above generalizes as follows.

Exercise 1.31. *Let $\mathbb{Z}^+$ be the domain of discourse; that is, the variables a, b, d we discuss below are all assumed to be positive integers. Prove that if d divides a, then*

$$\gcd(d, b) \leq \gcd(a, b).$$

1.5.2. Rational numbers. So far, we have stayed in the universe of integers. It is time to expand this universe!

1.5.2.1. *The definition of a rational number.* We say that a real number r is a **rational number** if it can be expressed in the form

$$r = \frac{a}{b}, \tag{1.59}$$

where a and b are integers. For this to make sense, we assume that $b \neq 0$. For example, $-\frac{17}{3} = \frac{17}{-3}$ is a rational number.

Example 1.49. (1) Integers are rational numbers. Indeed, if a is an integer, then we may write it as $a = \frac{a}{1}$.

(2) Suppose that $a = mq + r$, where $0 < r < m$. Then $\frac{a}{m}$ is a rational number which is not an integer. Indeed, we have $q < \frac{a}{m} < q + 1$.

1.5.2.2. *Fractions in lowest terms.* We can understand rational numbers by using division. Let $g = \gcd(a, b)$. Given any rational number $\frac{a}{b}$, we define its **lowest terms** to be the fraction

$$\frac{a/g}{b/g}. \tag{1.60}$$

Here, we are considering a/g and b/g as integers. For example, the lowest terms of $\frac{51}{68}$ is $\frac{3}{4}$ since $51/17 = 3$ and $68/17 = 4$. Observe that $\gcd(3, 4) = 1$.

The following result explains why the lowest terms of a fraction has the gcd of the numerator and denominator equal to 1.

Theorem 1.50. *For all positive integers a and b, we have that*

$$\gcd\left(\frac{a}{g}, \frac{b}{g}\right) = 1, \tag{1.61}$$

where $g = \gcd(a, b)$.

Proof. Suppose that c is a common divisor of $\frac{a}{g}$ and $\frac{b}{g}$. By definition, this means that there exist integers k and ℓ such that

$$ck = \frac{a}{g}, \qquad c\ell = \frac{b}{g}. \tag{1.62}$$

By multiplying these equations by g, we may rewrite this as

$$(gc)k = a, \qquad (gc)\ell = b. \tag{1.63}$$

This tells us that gc is a common divisor of a and b. By the definition of g as the greatest common divisor of a and b, we obtain that

$$gc \leq g. \tag{1.64}$$

Since $g > 0$, **this implies that $c \leq 1$.** This proves that the greatest common divisor of $\frac{a}{g}$ and $\frac{b}{g}$ is 1. □

Figure 1.5.1 exhibits the fact that

$$\frac{51}{68} = \frac{3}{4}.$$

Exercise 1.32. *If $\frac{a}{b}$ is in lowest terms, can both a and b be even? Explain your answer.*

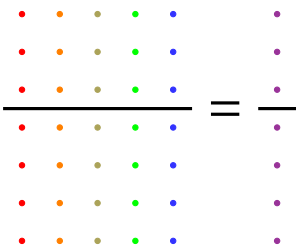

Figure 1.5.2. Visualizing Theorem 1.50: Imagining the rational number $\frac{15}{20}$ in lowest terms by dividing both the numerator and denominator by $\gcd(15, 20) = 5$ to obtain $\frac{3}{4}$, where $\gcd(3, 4) = 1$.

Exercise 1.33. *Find the lowest terms expressions for the following rational numbers:*

$$\frac{68}{51}, \frac{936}{324}, \frac{1748}{4199}, \frac{1139163}{987654321}. \tag{1.65}$$

1.5.3. Coprime integers. Just as it is interesting when two integers have something in common, it is interesting when two integers have nothing to do with each other, multiplicatively that is.

Definition 1.51. We say that integers a and b, not both zero, are **coprime** if $\gcd(a, b) = 1$.

In particular, two distinct primes are necessarily coprime. (For example, we have $\gcd(5, 17) = 1$.) Indeed, suppose that p and q are distinct (not equal) primes. Let $g = \gcd(p, q)$ be the greatest common divisor of p and q. Since g is a positive divisor of the prime p, we have $g = 1$ or $g = p$. Suppose for a contradiction that $g \neq 1$. Then $g = p$. Since g divides q, this implies that p divides q. Since q is a prime and since $p > 1$, we conclude that $p = q$, a contradiction. Therefore $g = 1$.

Exercise 1.34. *Let p and q be non-equal prime numbers. Prove that* $\gcd(p^2, q^2) = 1$.

More generally, it turns out that two integers are coprime if (and only if) they do not have any prime divisors in common. For example, the two integers

$$2^7 \cdot 3^4 \cdot 11 \quad \text{and} \quad 5^2 \cdot 7^8 \cdot 19$$

are coprime, for the prime divisors of the first integer are $2, 3, 11$ and the prime divisors of the second integer are $5, 7, 19$, and these two sets of primes contain no common primes. In other words, positive integers m and n are coprime means that if all the primes making up m disappeared from the list of all primes, then n would not be affected.

Flippantly, we may say that for molecules, water H_2O and salt NaCl are coprime, but carbon dioxide CO_2 and methane CH_4 are not coprime. ☺

Theorem 1.50 says that for every two integers a and b, where at most one of them is zero:

> The integers a/g and b/g are coprime, where g is the gcd of a and b.

See Chapter 4 for more discussion about coprime integers.

1.5.4. Division and integral linear combinations. So far, we have studied some elementary properties of division restricted to the realm of the binary operation of multiplication. It is time to add the binary operation of addition into the mix.

Regarding division, observe that 7 divides 21 and 7 divides 35. From this we can show 7 divides $21m + 35n$ for every pair of integers m, n. Indeed, let m and n be integers. We calculate that

$$21m + 35n = 7(3m + 5n).$$

Since $3m + 5n$ is an integer, we conclude that 7 divides $21m + 35n$.

We will find the following generalization of this rather useful. Why this is useful should not be immediately apparent to you!

Theorem 1.52. *Suppose that c is a common divisor of integers a and b. Then for all integers m and n, we have that c divides the* ***integral linear combination***

$$ma + nb$$

of a and b.

Proof. By hypothesis, there exist integers k and ℓ such that $ck = a$ and $c\ell = b$. Hence

$$ma + nb = m(ck) + n(c\ell) = c(mk + n\ell). \tag{1.66}$$

Since $mk + n\ell$ is an integer, by the definition of division this proves the desired conclusion. □

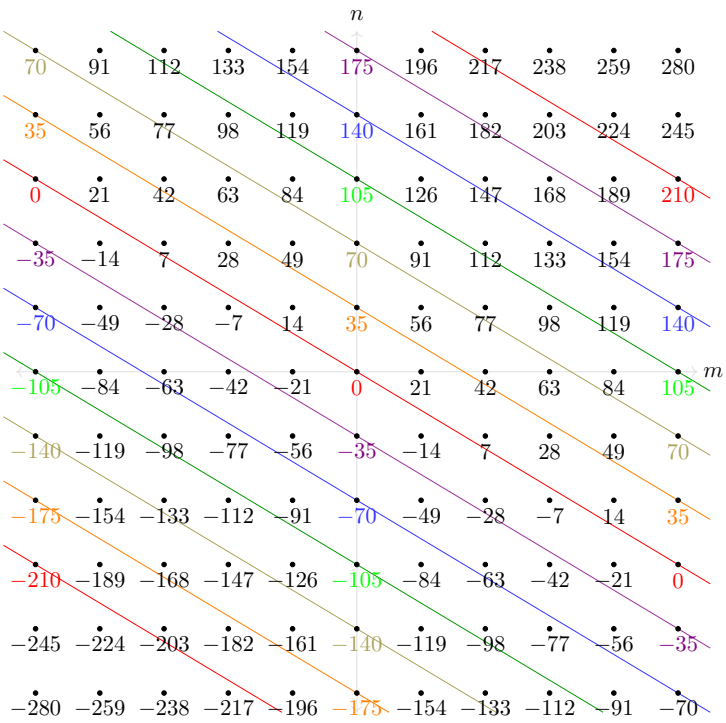

Figure 1.5.3. Visualizing Theorem 1.52: At each point (m, n) the integral linear combination $21m + 35n$ is displayed right below it. For example, $-133 = (-3)21 + (-2)35$ is displayed right below the point $(-3, -2)$. Since $\gcd(21, 35) = 7$, each integral linear combination is a multiple of 7. Horizontally we count by 21's and vertically we count by 35's.

1.5.5. Example of a linear Diophantine equation. It is easy to solve linear equations for real numbers. What about for integers? We consider this question in detail in Chapter 4. For now, we just consider an example.

Solved Problem 1.53 (Solving a linear Diophantine equation by hand)**.** *Find integers m and n such that*

$$9m + 11n = 1. \tag{1.67}$$

That is, find an integral linear combination of 9 *and* 11 *that is equal to* 1*.*

Solution. Here is a simple approach. Counting by 9's yields

$$9,\ 18,\ 27,\ 36,\ 45, \ldots, \tag{1.68}$$

while counting by 11's yields

$$11,\ 22,\ 33,\ 44, \ldots. \tag{1.69}$$

Noticing that 45 is one more than 44, we see that

$$9(5) + 11(-4) = 1, \tag{1.70}$$

so that $m = 5$, $n = -4$ gives a solution to $9m + 11n = 1$.

Since we were not asked to find *all* solutions to the equation, we just found a *particular* solution. See the following two exercises for examples of the more general question.

Exercise 1.35. *Verify that for every integer k,*

$$m = 5 + 11k, \qquad n = -4 - 9k \tag{1.71}$$

is a solution to (1.67)*. We will see in Chapter* 4 *below that this is the general solution (that is, there are no other solutions)!*

Exercise 1.36. *By trial and error, find integers m and n such that*

$$13m + 19n = 1. \tag{1.72}$$

Using the above, find an integer solution to

$$13m + 19n = 5. \tag{1.73}$$

Call your solution (m_0, n_0). Is $(m_0 + 19, n_0 - 13)$ also an integer solution? Can you find infinitely many integer solutions?

1.6. Statement of prime factorization

Have you answered the question in the caption for Figure 1.0.3 at the beginning of this chapter? If not, this section will help!

1.6.1. Atomic theory. Primes are the building blocks (dare we say atoms?) for the set of positive integers from the point of view of multiplication.

It turns out that (we prove this in later chapters):

Theorem 1.54. *Any integer $n \geq 2$ may be written (uniquely) as the product of primes.*

This is called the **prime factorization** of n, and this result is also known as the Fundamental Theorem of Arithmetic. Here are the prime factorizations of the integers from 2 to 19:

$$\begin{array}{llllll} 2 = 2^1, & 3 = 3^1, & 4 = 2^2, & 5 = 5^1, & 6 = 2 \cdot 3, & 7 = 7^1, \\ 8 = 2^3, & 9 = 3^2, & 10 = 2 \cdot 5, & 11 = 11^1, & 12 = 2^2 \cdot 3, & 13 = 13^1, \\ 14 = 2 \cdot 7, & 15 = 3 \cdot 5, & 16 = 2^4, & 17 = 17^1, & 18 = 2 \cdot 3^2, & 19 = 19^1. \end{array}$$

As a reminder (we've referred to this result earlier), we have:

Corollary 1.55. *For every integer $n \geq 2$, there exists a prime p divisor of n.*

Proof. Let $n \geq 2$ be an integer. By Theorem 1.54, there exist primes $p_1, p_2, \ldots, p_k$ (where the primes may not be distinct) such that

$$n = p_1 \cdot p_2 \cdots p_k. \tag{1.74}$$

So we have that p_1 is a prime divisor of n. □

Exercise 1.37. *Find the prime factorizations of all non-prime integers $2 \leq n \leq 100$. Hint: In §1.6 we have considered $n < 20$. So you may start with $n = 20$. Consider the green integers in Figure 1.1.2. Hint: We give the answer below, but again no peeking!*

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Figure 1.6.1. A partially drawn visualization of the prime factorization for the integers 1 to 100. (The filled squares are the integers 2 through 20, as well as the primes and squares less than 50.) The primes are framed in thick lines. Note that no prime greater than 50 is a divisor of a composite number less than or equal to 100.

Exercise 1.38. *Find the prime factorization of 3233. You can use an online applet.*

With the help of Figure 1.1.2, we give a table of prime factorizations of the integers from 2 to 100, inclusive:

(1.75)

	2	3	2^2	5	$2\cdot 3$	7	2^3	3^2	$2\cdot 5$
11	$2^2 3$	13	$2\cdot 7$	$3\cdot 5$	2^4	17	$2\cdot 3^2$	19	$2^2 5$
$3\cdot 7$	$2\cdot 11$	23	$2^3 3$	5^2	$2\cdot 13$	3^3	$2^2 7$	29	$2\cdot 3\cdot 5$
31	2^5	$3\cdot 11$	$2\cdot 17$	$5\cdot 7$	$2^2 3^2$	37	$2\cdot 19$	$3\cdot 13$	$2^3 5$
41	$2\cdot 3\cdot 7$	43	$2^2 11$	$3^2 5$	$2\cdot 23$	47	$2^4 3$	7^2	$2\cdot 5^2$
$3\cdot 17$	$2^2 13$	53	$2\cdot 3^3$	$5\cdot 11$	$2^3 7$	$3\cdot 19$	$2\cdot 29$	59	$2^2 3\cdot 5$
61	$2\cdot 31$	$3^2 7$	2^6	$5\cdot 13$	$2\cdot 3\cdot 11$	67	$2^2 17$	$3\cdot 23$	$2\cdot 5\cdot 7$
71	$2^3 3^2$	73	$2\cdot 37$	$3\cdot 5^2$	$2^2 19$	$7\cdot 11$	$2\cdot 3\cdot 13$	79	$2^4 5$
3^4	$2\cdot 41$	83	$2^2 3\cdot 7$	$5\cdot 17$	$2\cdot 43$	$3\cdot 29$	$2^3 11$	89	$2\cdot 3^2 5$
$7\cdot 13$	$2^2 23$	$3\cdot 31$	$2\cdot 47$	$5\cdot 19$	$2^5 3$	97	$2\cdot 7^2$	$3^2 11$	$2^2 5^2$

We prove the "existence" part of the Prime Factorization Theorem 1.54 (a.k.a. Fundamental Theorem of Arithmetic) in §2.4.3 below. The "uniqueness" part is proved in §4.8.

1.6.2. Euclid's theorem that there are infinitely many primes. Bountiful primes! We can use division and a clever idea (using the power of proof by contradiction!) to obtain the following result stated at the beginning of this chapter.

Theorem 1.56 (Euclid's Theorem)**.** *There are infinitely many primes.*

Proof. Suppose for a contradiction that there are only a finite number of primes in totality. Let n be the total number of primes, and denote the distinct primes by

$$p_1, p_2, \ldots, p_n. \tag{1.76}$$

Let

$$m = p_1 p_2 \cdots p_n + 1. \tag{1.77}$$

Since $m \geq 2$, by the Prime Factorization Theorem 1.54, there is some prime p_i, where $1 \leq i \leq n$, which divides m.

Since p_i also divides $p_1 p_2 \cdots p_n$, by Theorem 1.52 we obtain that p_i divides the difference

$$m - p_1 p_2 \cdots p_n = 1. \tag{1.78}$$

Since $p_i > 1$, this is a contradiction to Theorem 1.37. Hence there are infinitely many primes. □

1.6.3. How to make a quick buck. Primes have a number of important real-world applications. And they are fun to boot! Here is a game you can play. Choose two really large primes p and q, and multiply them together to get pq. Tell your friend the integer pq and also tell them that this integer is the product of two primes and ask them to find the two primes. If you can find two primes large enough so that they can never win the game, then you have a real world application: The RSA algorithm in cryptography is based on the difficulty of finding the prime

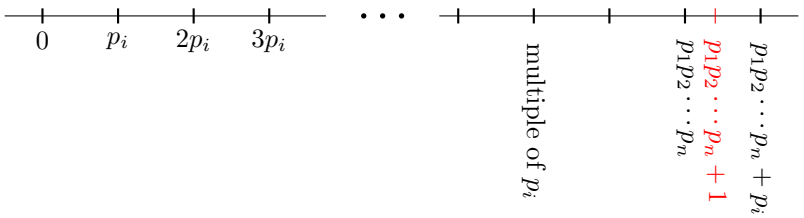

Figure 1.6.2. If there are only a finite number of primes, there exists an i such that $p_1p_2\cdots p_n+1$ divided by p_i has remainder both 0 and 1, which is a contradiction.

factorization for a large number that is the product of two large primes (called a semiprime). The basics of the RSA algorithm are discussed in §6.11* below.

If you are good at factoring semiprimes, you can make money: RSA Factoring Challenge. For example, the first RSA factoring challenge number is

$$\begin{aligned}&152260502792253336053561837813263742971806811496 13\\ &80688657908494580122963258952897654000350692006139.\end{aligned}$$

Sorry for writing a single number on two lines; it was too long to write on one line! This number was factored as

$$\begin{aligned}&3797522793694367392280887275544562785456553663819 9\\ &\times 4009469095092088103068373529276146838921489972406 1\end{aligned}$$

on April Fool's Day (of all days!) of 1991 by Arjen K. Lenstra.

You will make 200,000 USD if you can find the factorization of the following number (if it has not already been done by the time you read this):

25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357.

This number is indeed the product of two primes p and q. Presumably the presenters of the prize are the only ones who know the answer and they are bound to secrecy. Your challenge is to find p and q.

One of the difficulties is current computational power. This is related to Moore's Law.

1.7*. Perfect numbers

Question: What is the perfect number of hours to work per day?
Answer: Six! We will see why below.

Of course, primes are not the only natural numbers that have special properties. Observe that some numbers, like 36, have "lots" of divisors, whereas other numbers, like 39, have "few" divisors. Besides simply counting the number of positive divisors, we can sum the positive divisors of a number. For example, since the divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$, the sum of the positive divisors of 36 not counting 36 itself is "too much" in the sense that

$$1 + 2 + 3 + 4 + 6 + 9 + 12 + 18 = 55 > 36.$$

On the other hand, the divisors of 39 are $1, 3, 13, 39$, and their sum not counting 39 is "too little" in the sense that

$$1 + 3 + 13 = 17 < 39.$$

When something is neither too much nor too little, we say that is perfect, so:

Definition 1.57. We say that a positive integer n is a **perfect number** if n is equal to the sum of its positive divisors less than n.

For example, 6 is a perfect number since its positive divisors are $1, 2, 3, 6$ and

$$1 + 2 + 3 = 6. \tag{1.79}$$

Perfect! We also have that 28 is a perfect number since its positive divisors are $1, 2, 4, 7, 14, 28$ and

$$1 + 2 + 4 + 7 + 14 = 28. \tag{1.80}$$

Perfect again!

Here are the first few perfect numbers:

$$6, 28, 496, 8128, 33550336, 8589869056, 137438691328. \tag{1.81}$$

For example, the positive divisors of 496 are

$$1, 2, 4, 8, 16, 31, 62, 124, 248, 496, \tag{1.82}$$

and

$$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248. \tag{1.83}$$

Remarkably, it is unknown if there exist *odd* perfect numbers.

Conjecture 1.58 (Nicomachus)**.** *All perfect numbers are even.*

Exercise 1.39. (1) *Prove that if p is a prime, then p is not a perfect number.*

(2) *Prove that if p and q are primes, then pq is a perfect number if and only if $pq = 6$, i.e., one of p, q is 2 and one of p, q is 3.*

Exercise 1.40. *We know that 6 and 28 are perfect numbers. Prove that there are no perfect numbers n satisfying $6 < n < 28$.*

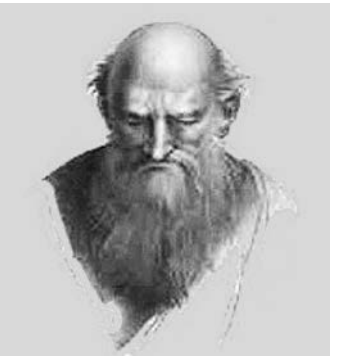

Figure 1.7*.1. Nichomachus. Line engraving by P. Ghigi after L. Agricola after Raphael. Wellcome Collection, https://wellcomecollection.org/works/v8swpwtt. Licensed under Creative Commons, https://creativecommons.org/publicdomain/mark/1.0. Public Domain.

1.8*. One of the Mersenne conjectures

It is cool to look at primes of various special forms. Remarkably, this topic is related to perfect numbers. A **Mersenne prime** is a prime p that is equal to one less than a power of two. That is, a prime of the form

$$p = 2^n - 1,$$

where n is some positive integer. Recall, by Theorem 1.16, n must be a prime for p to be a prime. For example, since 100 is not a prime, we know that $2^{100} - 1$ is not a prime.

The Mersenne primes corresponding to the integers

$$2, 3, 5, 7, 13, 17, 19, 31 \tag{1.84}$$

Figure 1.8*.1. Marin Mersenne (1588–1648). Wikimedia Commons, Public Domain.

are

$$3, 7, 31, 127, 8191, 131071, 524287, 2147483647, \tag{1.85}$$

respectively.

Exercise 1.41. *For n equal to the primes 11, 23, and 29, can you find the (non-trivial) prime factorizations of $p = 2^n - 1$? You may wish to use an online applet for this!*

Let q be a prime with the property that $M_q := 2^q - 1$ is a Mersenne prime. After the first 8 Mersenne primes in (1.85), the next 8 Mersenne primes are

$$M_{61}, M_{89}, M_{107}, M_{127}, M_{521}, M_{607}, M_{1279}, M_{2203}. \tag{1.86}$$

These integers get large quite quickly. For example, the sixteenth Mersenne prime M_{2203} has 664 digits! This particular Mersenne prime was found by Raphael Robinson in the year 1952.

According to Wikipedia, as of October 2020, only 51 Mersenne primes are known. The largest Mersenne prime known, which has 24862048 digits, is

$$M_{82589933} = 2^{82589933} - 1$$

(by the time you are reading this hopefully it is larger!). See the Great Internet Mersenne Prime Search.

It has been conjectured by Lenstra, Pomerance, and Wagstaff that:

Conjecture 1.59. *There are an infinite number of Mersenne primes.*

This conjecture is at present unsolved, and fame and glory await the solver!

We have the following beautiful result of Euclid and Euler (see Theorem 6.90 below for a proof):

Theorem 1.60.

An even positive integer n is a perfect number

if and only if

$n = (2^p - 1)2^{p-1}$, *where $2^p - 1$ is a Mersenne prime!*

For example, the first few perfect numbers can be written as the products (where the first factor is a Mersenne prime):

$$\begin{aligned} 6 &= 3 \cdot 2, \\ 28 &= 7 \cdot 4, \\ 496 &= 31 \cdot 16, \\ 8128 &= 127 \cdot 64, \\ 33550336 &= 8191 \cdot 4096. \end{aligned}$$

1.9*. Twin primes: An excursion into the unknown

Question: What did one twin prime say to the other?
Answer: We are close, but we are not identical.

There are certainly lots of things that we do not know about primes. This includes the following topic, although much amazing progress has been made. A twin prime pair is a pair of primes, one of which is equal to 2 plus the other. For example, the twin prime pairs of primes under 100 are

$$(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31),\ (41,43),\ (59,61),\ (71,73). \tag{1.87}$$

The largest twin prime pair under one thousand is

$$(881,883). \tag{1.88}$$

The largest twin prime pair under one million is

$$(999959,999961). \tag{1.89}$$

As of this writing, the largest known twin prime pair is

$$(2996863034895 \cdot 2^{1290000} - 1,\ 2996863034895 \cdot 2^{1290000} + 1). \tag{1.90}$$

This twin prime pair was found on September 14, 2016, by PrimeGrid using the Twin Prime Search.

The following is the Twin Prime Conjecture. As of this writing, this conjecture is still unsolved!

Conjecture 1.61. *There are an infinite number of twin prime pairs.*

A cousin prime pair is a pair of primes, one of which is equal to 4 plus the other. For example, the cousin prime pairs of primes under 100 are

$$(3,7),\ (7,11),\ (13,17),\ (19,23),\ (37,41),\ (43,47),\ (67,71),\ (79,83). \tag{1.91}$$

Currently, it is unknown whether there are an infinite number of cousin prime pairs.

Given a positive even integer k, let us say that a pair of primes is a **k-prime pair** if one of the primes is equal to k plus the other. Then twin and cousin prime pairs are the same as 2- and 4-prime pairs, respectively.

Yitang Zhang proved the following.[7]

[7] Zhang's work depends on a number of mathematicians' works including Bombieri, Deligne, Friedlander, Goldston, Heath-Brown, Iwaniec, Pintz, Vinogradov, and Yıldırım.

Theorem 1.62. *There exists a positive even integer k less than 70 million (yikes, that's a big number!) such that there are an infinite number of k-prime pairs.*

By the Polymath8 Project, this result has been improved to:

Theorem 1.63. *There exists a positive even integer $k \leq 246$ such that there are an infinite number of k-prime pairs.*

But, as of this writing, we do not know any *specific* such k, even though we know that such a k exists!

1.10*. Goldbach's conjecture

Primes greater than 2 are always odd. So the sum of two such primes is always even. This naturally leads to the following question:

Can we write each positive even integer as the sum of two prime numbers?

Of course, 2 cannot be written as such since although $2 = 0 + 2$ and $2 = 1 + 1$, neither 0 nor 1 are prime numbers. So we should start with the number 4. As the first few cases, we have

$$4 = 2 + 2,\ 6 = 3 + 3,\ 8 = 3 + 5,\ 10 = 3 + 7,\ 12 = 5 + 7,\ 14 = 7 + 7. \tag{1.92}$$

Here are a few more:

$$16 = 3 + 13,\ 18 = 5 + 13,\ 20 = 3 + 17,\ 22 = 3 + 19,\ 24 = 5 + 19. \tag{1.93}$$

Skipping a few to 100, we have

$$100 = 11 + 89,\ 102 = 5 + 97,\ 104 = 7 + 97,\ 106 = 17 + 89,\ 108 = 19 + 89. \tag{1.94}$$

A longstanding and tantalizing conjecture is the following.

Conjecture 1.64 (Goldbach's conjecture)**.** *Every even integer greater than 2 is the sum of two primes.*

Here are some more examples of even integers which are the sums of two prime numbers:

$$1000 = 3 + 997 = 17 + 983 = 23 + 977 = \cdots = 491 + 509, \tag{1.95}$$

where there are in total 28 ways to write 1000 as the sum of two primes. For each

of the next powers of 10, we just give one sum of primes, likely of very many:

$$10^4 = 59 + 9941,$$
$$10^5 = 11 + 99989,$$
$$10^6 = 17 + 999983,$$
$$10^7 = 29 + 9999971,$$
$$10^8 = 11 + 99999989.$$

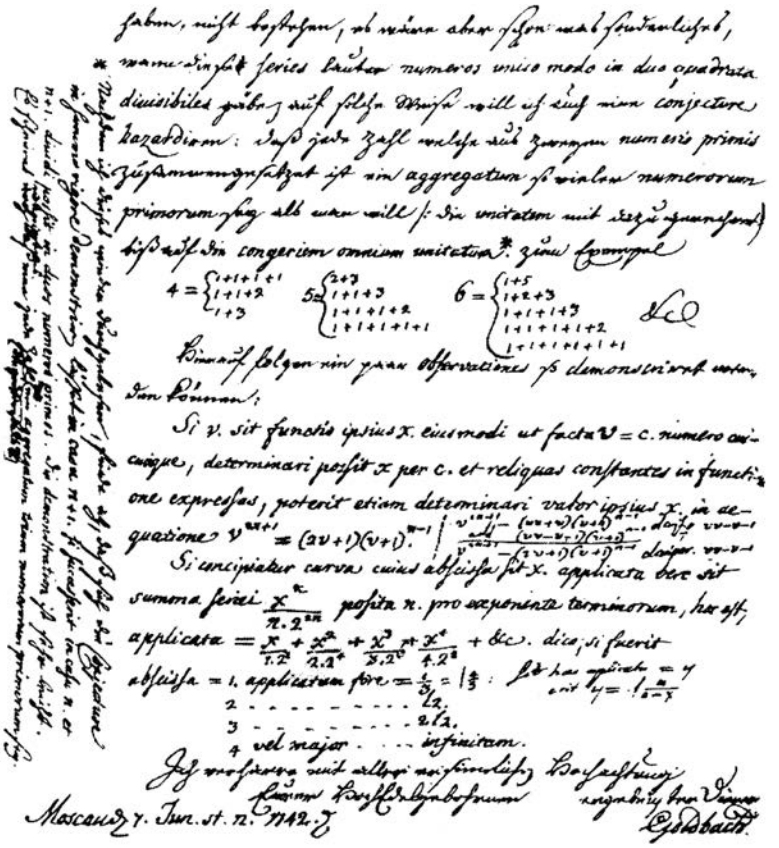

Figure 1.10*.1. Letter from Goldbach to Euler stating his conjecture, dated 1742. Wikimedia Commons, Public Domain.

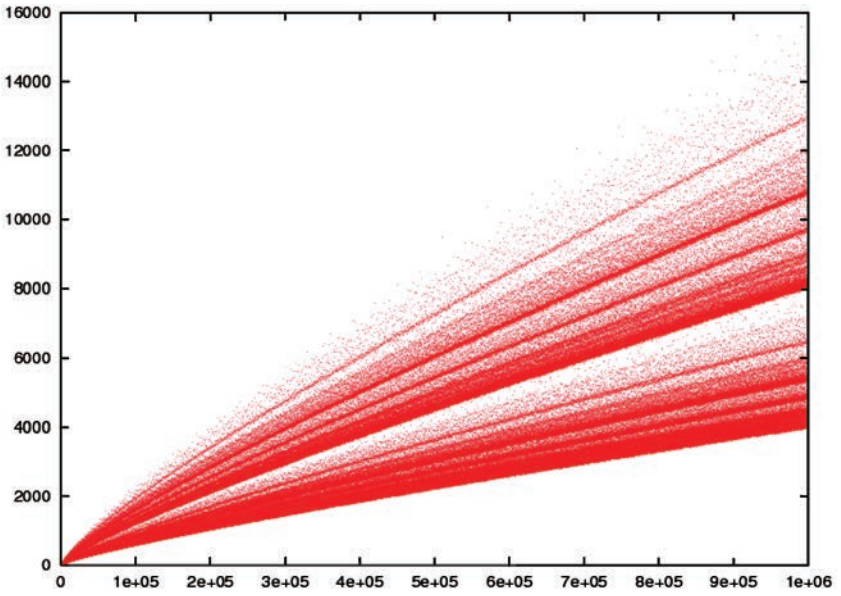

Figure 1.10*.2. A plot of points when the horizontal coordinate is a positive even integer n and the vertical coordinate is the number of ways n can be written as the sum of two primes. This plot gives us confidence that Goldbach's conjecture is true! Credit: Wikimedia Commons, author: Reddish at the English-language Wikipedia, licensed under the GNU Free Documentation license, version 1.2 or any later version, and the Creative Commons Attribution 3.0 Unported (https://creativecommons.org/licenses/by-sa/3.0/deed.en) license.

At the time of this writing, the following is known.

Theorem 1.65. *Every even integer greater than* 2 *and less that* 4×10^{18} *is the sum of two primes.*

So, unless you have access to a powerful computer and lots of time on your hands, we don't suggest that you look for counterexamples to Goldbach's conjecture!

1.11. Hints and partial solutions for the exercises

Hint for Exercise 1.1. The color coding in Figure 1.0.3 starts as follows. 1 is gray. 2 is orange. 3 is green. 4 since it is $2^2 = 2 \cdot 2$ is two oranges, 5 is blue, 6 since it is $2 \cdot 3$ is an orange and a green. 7 is purple. 8 since it is 2^3 is three oranges. Etc. See §1.6 on prime factorization for more food for thought on this.

Hint for Exercise 1.2. Suppose $a = n$. Then $n = a \cdot b = n \cdot b$. Now divide this equality by n.

Hint for Exercise 1.3. Since we are proving an equivalence (a.k.a. a biconditional), we prove two implications. Suppose that $n = ab$.

(1) Suppose $a > 1$ and $b > 1$. Prove that $1 < a < n$.

(2) Suppose that $1 < a < n$. Prove that $b > 1$.

Hint for Exercise 1.4. Suppose that 0 divides an integer n. Show that $n = 0$. Then explain why this solves the exercise.

Hint for Exercise 1.5. Suppose that $1 < a < n$. Prove that $1 < b < n$ using elementary properties about inequalities.

Hint for Exercise 1.6. The answer is given in each of Figure 1.1.2 and (1.6).

Hint for Exercise 1.7. The second, fourth, sixth, eighth, and tenth columns comprise the even integers.

Hint for Exercise 1.8. We just need to check for divisors less than or equal to the square root of each number.

Hint for Exercise 1.9. Our first impression is that the conjecture is false. This is from our knowing the falsehood of the conjectures about the primeness of integers of the form $2^n - 1$, $n \geq 2$, or even of the form $2^p - 1$, where p is a prime.

Hint for Exercise 1.10. Make the substitution $x = 2^a$. Then $2^n - 1 = x^b - 1$ by $2^a - 1 = x - 1$. Apply polynomial long division to dividing $x^b - 1$ by $x - 1$ (or you may already know what this ratio is having seen it somewhere).

Hint for Exercise 1.11. The key is to mimic Figures 1.2.1 and 1.2.2.

Hint for Exercise 1.12. Theorem 1.28 says that "The product of any integer and an even integer is even." Recast this statement as an "if-then" statement, and use the definition of even.

Hint for Exercise 1.13. Draw a $2k + 1$ by $2\ell + 1$ rectangle and consider the 4 "subrectangles" of dimensions $2k \times 2\ell$, $2k \times 1$, $1 \times 2\ell$, and 1×1.

Hint for Exercise 1.14. Let a be an even integer. Apply the result that the product of an even integer and any integer is even to the product $a^3 = a \cdot a^2$.

Hint for Exercise 1.15. Suppose that the product of two integers a and b is even. Assume for a contradiction that not at least one of the integers a, b is even. This means that both a and b are odd. Use a result in the book.

Hint for Exercise 1.16. Use that $\sqrt{11} < 4$.

Hint for Exercise 1.17. Assume for a contradiction that it is not true that $a \leq 100$ or $b \leq 100$. Then $a > 100$ and $b > 100$. Can you derive a contradiction from this assumption?

Hint for Exercise 1.18. Without loss of generality, we may assume that

$$0 < a \leq b \leq c. \tag{1.96}$$

Then show that

$$a^3 \leq n. \tag{1.97}$$

Hint for Exercise 1.19. We cross out all of the composite numbers from 2 to 100, inclusive. Any such composite number is the product of a prime p less than or equal to $\sqrt{100} = 10$ with an integer greater than 1. We call these products non-trivial multiples of p. These primes p are $2, 3, 5, 7$.

Observe that having crossed out all of the non-trivial multiples of primes, for primes less than or equal to p, the next uncrossed out integer is the next prime after p. For example, having crossed out all the non-trivial multiples of 2, 3, and 5, the next uncrossed out integer is 7. This in part explains why the process works.

Having crossed out all of the non-trivial multiples of $2, 3, 5, 7$, the remaining integers are 1 (which is not a prime) and the exact list of primes less than or equal to 100.

Hint for Exercise 1.20. We only need to consider primes less than or equal to $\sqrt{200}$, which is less than 15. So we cross out the (non-trivial) multiples of $2, 3, 5, 7, 11, 13$.

Hint for Exercise 1.21. Follow the advice of the exercise and check the fifth Fermat number. Use a computer and an online factorization applet.

Hint for Exercise 1.22. We simply apply Theorem 1.37 to the special case where $a = b = n$.

Hint for Exercise 1.23. Suppose a divides b. Then there exists an integer k such that $b = ka$. Square this equation.

Hint for Exercise 1.24. Suppose that 3 divides b. Then there exists an integer k such that $b = 3k$. Square this equation. For the second part of the exercise, replace 3 by a.

Hint for Exercise 1.25. Suppose that a divides b and that b divides c. Then there exist integers k and ℓ such that

$$b = ka, \qquad c = \ell b. \tag{1.98}$$

Continue.

Hint for Exercise 1.26. Let a be a positive divisor of a positive integer b with the property that $a \neq b$. Then $a < b$ (why?). There exists a positive integer k such that $ak = b$ (why?). We have $k \geq 2$ (why?). Continue.

Hint for Exercise 1.27. This is very similar to Solved Problem 1.44, so mimic the proof thereof.

Hint for Exercise 1.28. We have $a \geq 1$ and $b \geq 1$. Use a basic fact about inequalities, multiplication, and the maximum.

Hint for Exercise 1.29. For example, suppose that an integer n is equal to $p_1^{k_1} p_2^{k_2} p_3^{k_3}$, where p_1, p_2, p_3 are distinct primes and k_1, k_2, k_3 are positive integers. Then the positive divisors of n are given by

$$p_1^{j_1} p_2^{j_2} p_3^{j_3}, \quad \text{where } 0 \leq j_1 \leq k_1,\ 0 \leq j_2 \leq k_2,\ 0 \leq j_3 \leq k_3. \tag{1.99}$$

Hint for Exercise 1.30. Use that 5, 17, and 23 are prime to find all of the positive divisors of $5 \cdot 17$ and $23 \cdot 17$.

Hint for Exercise 1.31. Let c be a common divisor of d and b. Use that d divides a and the transitivity of division.

Hint for Exercise 1.32. Is 2 a common divisor of both a and b?

Hint for Exercise 1.33. We have $\frac{68}{51} = \frac{4}{3}$.

Hint for Exercise 1.34. Let p and q be non-equal prime numbers. Let $g := \gcd(p^2, q^2)$. Use that g is a positive integer dividing both p^2 and q^2 and that p and q are primes. You may use that the only positive divisors of p^2 are 1, p, and p^2, and similarly for p replaced by q.

Hint for Exercise 1.35. Let k be an integer. Substitute $m = 5 + 11k$ and $n = -4 - 9k$ into the expression $9m + 11n$ and verify that the answer is equal to 1.

Hint for Exercise 1.36. Counting by 13's yields

(1.100) $$13, 26, 39, 52, 65, \ldots,$$

while counting by 19's yields

(1.101) $$19, 38, 57, 76, 95, \ldots.$$

By comparing the integers on these two lists, can you find a solution to the linear Diophantine equation (1.72)?

For the second part of the exercise, multiply by 5.

For the third part of the exercise, let k be any integer and calculate $13(m_0 + 19k) + 19(n_0 - 13k)$.

Hint for Exercise 1.37. The answer is given by (1.75).

Hint for Exercise 1.38. One of the divisors is 53.

Hint for Exercise 1.39. (1) The only divisors of p are 1 and p.

(2) The only divisors of pq are $1, p, q, pq$. Note that it is hypothetically possible that $p = q$.

Hint for Exercise 1.40. By the previous exercise, we only need to show that the composite numbers strictly between 6 and 28 are all not perfect. To do this, one simply computes the sum of the positive divisors not equal to the composite number.

Hint for Exercise 1.41. We have that $2^{11} - 1 = 2047$. An online applet factors this as $2047 = 23 \cdot 89$.