

Chapter 1: Intuitive Proofs

The History of every major Galactic Civilization tends to pass through three distinct and recognizable phases, those of Survival, Inquiry and Sophistication, otherwise known as the How, Why, and Where phases. For instance, the first phase is characterized by the question “How can we eat?” the second by the question “Why do we eat?” and the third by the question “Where shall we have lunch?”

– Douglas Adams, *The Hitchhiker’s Guide to the Galaxy*

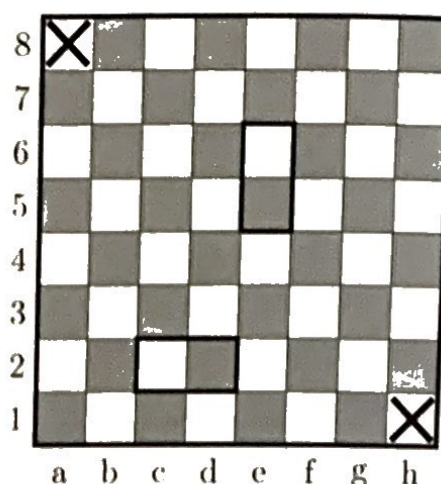
Your mathematics education will also pass through these phases. The first phase is characterized by the question, “How can I solve this integral?” The second phase by the question, “Why does my solution work?” And the third phase by the question, “Where should we explore next?”

Indeed, your previous “Phase 1” math classes were probably focused on computation, like how to use the fundamental theorem of calculus to solve a problem. In your future “Phase 2” math classes, you will seek to understand *why* the fundamental theorem of calculus is true.¹ In your earlier “Phase 1” math courses, you were taught to use the quadratic formula to solve second-degree polynomials. In your future “Phase 2” math courses, you will learn that there are similar formulas for third- and fourth-degree polynomials... but not for fifth-degree polynomials — and you will see precisely why that is the case. Your future courses will also introduce you to lots of topics that did not appear at all in your previous courses. In fact, I think the most interesting math topics are saved entirely for second-phase courses — so you have a lot to look forward to!

This book is the gateway to Phase 2. It will show you the techniques mathematicians use to understand our math (which we call *proof techniques*), and it will introduce you to new math topics that you will explore in detail in your future courses. So buckle up, because math is about to get a lot more interesting.

¹When your curiosities guide you to seek out new math and pursue your own original ideas — perhaps by engaging in mathematical research — you will enter Phase 3. Much more on this later!

and exactly one black square. Two examples are shown here:



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.¹⁰

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 helps 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.

¹⁰A 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.

1.2 Naming Results

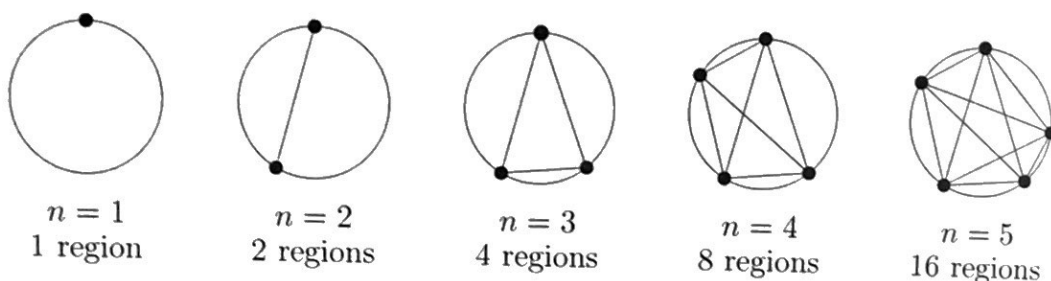
So far, all of our results have been called “propositions.” Here’s the run-down on the naming of results:

- A *theorem* is an important result¹² 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.¹³
- 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 it 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.



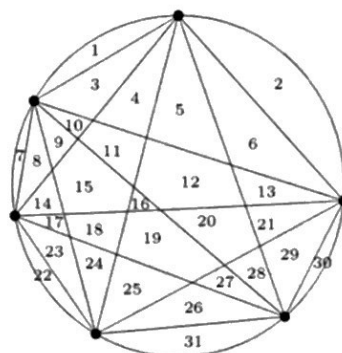
At this point, if you were to conjecture how many regions there will be for the $n = 6$ case, your guess would probably be 32 regions — the number of regions certainly seems to be doubling at every step. In fact, if it kept doubling, then with a little more thought you might even conjecture a general 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,

¹²By “result” we mean a sentence or mathematical expression that is true. We will discuss this in much more detail in Chapter 5.

¹³It’s like it’s saying “Yo, lemma help you prove that theorem.”

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:



$n = 6$
31 regions

This counterexample also underscores the reason why we prove things in math. Sometimes math is surprising.¹⁴ We need proofs to ensure that we aren't just guessing at what seems reasonable. Proofs ensure we are always on solid ground.¹⁵

Furthermore, 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.¹⁶ 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

¹⁴It looked like 2^{n-1} was going to be the formula. Actual formula: $\frac{1}{24}(n^4 - 6n^3 + 23n^2 - 18n + 24)$.

¹⁵Conjecture: 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!

¹⁶And if you are using this book in a course, then there's one final reason: *It's on the test!*

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.

Why do we prove things?

Now that you know the goal of this book, and have seen the first examples of proofs, it is reasonable to ask *why* we prove things. When you took algebra and geometry, you learned rules about solving equations and investigating geometric shapes. When you took linear algebra and differential equations, you learned deep results about systems of linear and differential equations. These results are really big deals, but they are not handed down to us from on high — mathematicians had to discover them.¹⁷ Meanwhile, mathematicians also have discovered things that seemed true but are not. How do we distinguish truth from lies? We use proofs.

In some sense, a proof is like a computer program. The program has to compile. It has to run. It must be logically sound in order for it to work. But a proof is also much more than that. It has to convince. We write proofs to communicate with each other, to justify our thoughts, and to know that we and others are correct. Thus, we must write proofs which are comprehensible and persuasive. Your proofs should convince your readers that you are correct.¹⁸

It is a wonderful thing about mathematics that we can *know* things to be true. A physicist or psychologist relies on theories that they can test, but without an axiomatic basis like in math, they can't know whether they have reached truth.

Proofs also help us not just know math, but *understand* math. They help show *why* something is true. This is the “Phase 2” mathematics we discussed on this book's first page. In calculus and pre-calculus, you learned mathematical rules and procedures. Each of those has a proof which can be verified and understood. A few of them will be proven in this book (like the Pythagorean theorem), while many more will be shown in your later courses.

You may have been taught that there are infinitely many primes, and that every positive integer (larger than 1) can be broken down as a product of prime numbers. How would you *know* that there are infinitely many primes without a proof? No experiment could verify such a thing. You may have heard that irrational numbers exist, and every integer can be written in binary. Perhaps you have heard that there is a deep result from number theory that is used to securely encrypt our digital transactions. Everything mentioned in this paragraph will be explained and proved later in this book.

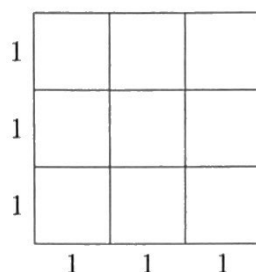
There is also so much more! We do not want to just verify that the boring calculations from pre-calc were correct — we want to explore new math, and prove that our discoveries are true. This is not just the beauty of math, it is the fun of math. We continue this endeavor with our second topic: the pigeonhole principle.

¹⁷Possible exception: Ramanujan.

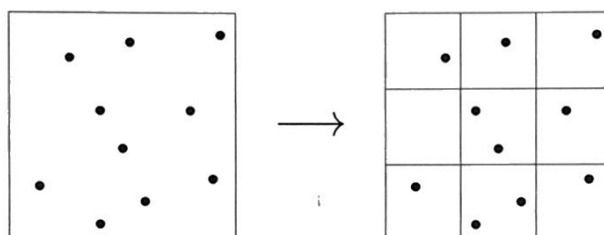
¹⁸Also, computer programs can have bugs. Especially long programs. We insist on rigor in our proofs to prevent bugs in our proofs. Especially our long proofs.

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 3×3 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 :



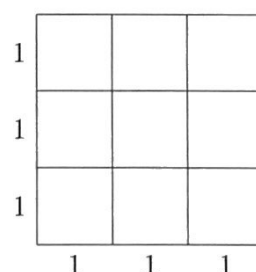
Then if you pick any 10 points from the 3×3 square, they will fall neatly into these boxes! For example:



Now, 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? As you can think about that, let's start the proof.

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



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

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.

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,

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

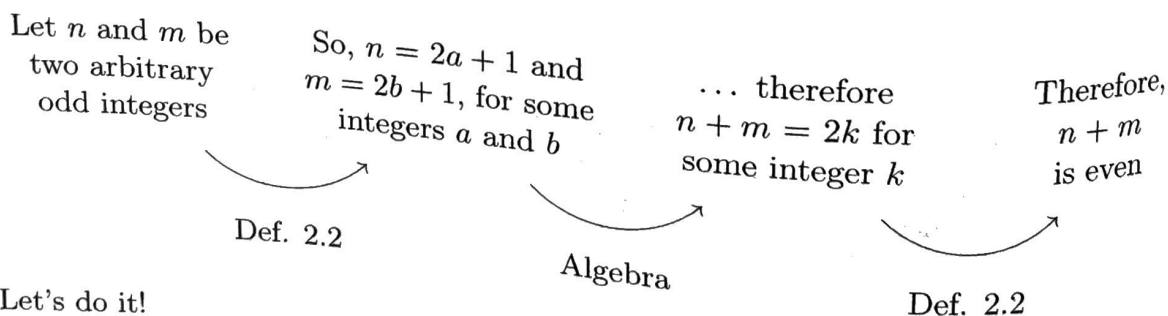
And since, by Fact 2.1, $a + b$ is an integer too, we have shown that $n + m = 2k$, where $k = a + b$ is an integer. Therefore, by Definition 2.2, this means that $n + m$ is even. \square

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'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.

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».

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 2.3.

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.”

Remember the general structure of a direct proof:

| | |
|---|--|
| <p>Proof. Assume P.</p> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 20px;"> <div style="text-align: center;"> <p>«An explanation of what P means»</p> <p>⋮ apply algebra, ⋮ logic, techniques</p> <p>«Hey look, that's what Q means»</p> <p>Therefore Q. □</p> </div> <div style="text-align: center; margin-top: 20px;"> <p>←</p> </div> <div style="text-align: right;"> <p>Apply definitions and/or other results.</p> </div> </div> | |
|---|--|

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 $c = ak$ for some integer k . Updating the above outline gives us this:

| | |
|---|--|
| <p>Proof. Assume that a, b and c are integers, and $a \mid b$ and $b \mid c$.</p> <p>Then by the definition of divisibility (Definition 2.8), $b = as$ for some integer s, and $c = bt$ for some integer t.</p> <div style="text-align: center; margin-top: 20px;"> <p>⋮ apply algebra, ⋮ logic, techniques</p> </div> <p>Therefore $c = ak$ for an integer k.</p> <p>Therefore $a \mid c$. □</p> | |
|---|--|

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 $a \mid c$. □

Proposition.

Proposition 2.18 (*Modular cancellation law*). Let a, b, k and m be integers, with $k \neq 0$. 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.²⁶ 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 $ak - bk = m\ell$, for some integer ℓ . That is,

$$k(a - b) = m\ell. \quad (\heartsuit)$$

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

$$k \mid m\ell.$$

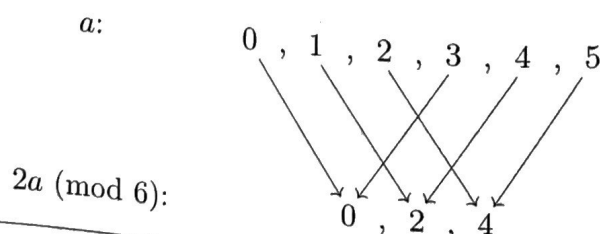
And since, by assumption, $\gcd(k, m) = 1$, by Lemma 2.17 part (ii) we must have $k \mid \ell$; by the definition of divisibility (Definition 2.8) this means that $\ell = kt$, for some integer t . This allows us to rewrite Equation (\heartsuit) :

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

where in the last line we used that $k \neq 0$. By the definition of modular congruence (Definition 2.14), this means that $m \mid (a - b)$. That is, $a \equiv b \pmod{m}$. \square

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:



²⁶“Yo, lemma help you prove that proposition.”

Introduction to Number Theory

Take a look at the following:

$$\begin{aligned}4 &= 2 + 2 \\6 &= 3 + 3 \\8 &= 5 + 3 \\10 &= 5 + 5 \\12 &= 7 + 5 \\14 &= 7 + 7 \\16 &= 11 + 5 \\18 &= 13 + 5 \\20 &= 17 + 3 \\22 &= 11 + 11.\end{aligned}$$

What do you notice about this? The numbers on the left are the even numbers larger than 2, and we have written each as a sum of two other numbers. Do you notice anything special about the numbers in the sums?

Each is written as a sum of two primes! Could it possibly be true that *every* even number larger than 2 can be written as a sum of two prime numbers? The data above is very little. The first ten cases work, but there are still infinitely many to go. Also, for small numbers, primes are everywhere! Take a look at the sequence of primes:³⁶

2 , 3 , 5 , 7 , 11 , 13 , 17 , 19 , 23 , 29 , 31 , 37 , 41 , ...

Among the ten odd numbers between 3 and 21, seven of them are prime! So the fact that we can write all the evens from 4 to 22 as a sum of two primes could very well be a coincidence — with 70% of the odds being prime, including the first three, *the odds seem in our favor*.³⁷ But could this result hold true even when the primes start thinning out? The density of the even numbers remains constant, so when the density of the primes starts dropping, perhaps there simply are not enough primes out there to give this pattern a fighting chance...

³⁶A fundamental fact: The sequence of primes is never-ending (we will prove this in Chapter 7).

³⁷Some say that puns make you numb. But this section's puns make you number.

Before Christian Goldbach discussed this problem with others in 1742, he presumably checked at least the first 100 cases, and sure enough, each of these can be written as a sum of two primes. Goldbach then told Leonhard Euler,³⁸ a master of numerical computation, who undoubtedly checked hundreds more. And so far, so good.

In 1938, Nils Pipping earned a spot in the math history books the hard way: he checked, by hand, all the even numbers up to 100,000 — and sure enough, he was able to write each and every one as a sum of two primes. Then, once computers were invented, Pipping's labor could be replicated in the blink of an eye, and could keep going at will.³⁹ As of this writing, the first 200,000,000,000,000 cases have been checked, and every single one is a sum of two primes.

But is it true forever? Or does there exist at least one even integer, way down the line, that is not the sum of two primes? And what do primes have to do with it anyways? It is common to think about multiplying primes together, since every natural number is a product of primes (a fact we will prove in Chapter 4); for example, $15 = 3 \cdot 5$, and $28 = 2 \cdot 2 \cdot 7$. But adding primes together completely loses their factorization; if p_1 and p_2 are different primes, then $p_1 + p_2$ is a product of primes other than p_1 and p_2 . So the main way in which we think about primes is failing us.

Goldbach's Conjecture states that every even number larger than 2 can be written as the sum of two primes.⁴⁰ But as of today, it remains a conjecture, meaning we still do not know whether it is true. Yet due to its age, its simplicity to understand, its difficulty to prove, and its relationship with prime numbers, whose study remains as important today as ever before, it stands as one of the most famous unsolved problems in all of mathematics.

The Prime Number Theorem

The study of formal mathematics began with the study of geometry and number theory. And from early on, mathematicians realized that in order to understand numbers, one must study the primes. In Chapter 2, we recalled that a prime is an integer p which is at least 2 and whose only positive divisors are 1 and p . If a positive integer is at least 2 and is not prime, then it is called *composite*. Not only do the primes thin out as you reach higher and higher portions of the natural numbers, but the *rate* at which the primes thin out is pretty steady. Indeed, if we let $\pi(N)$ denote the number of primes up to an integer N (e.g., $\pi(10) = 4$, since there are four primes in $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$), then we know exactly how fast $\pi(N)$ is growing as N gets larger and larger. The answer:

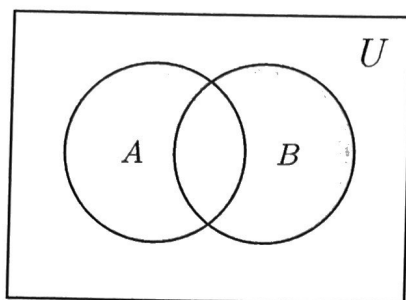
$$\pi(N) \sim \frac{N}{\log(N)}.$$

³⁸Pro-Tip: "Euler" is pronounced "Oiler."

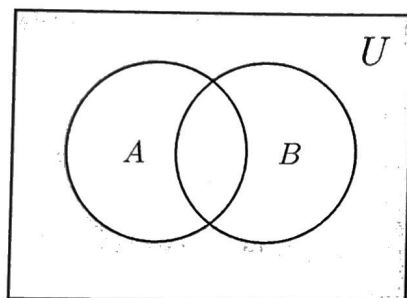
³⁹And a computer can do so without his wife getting mad at him because he won't put down the damn pencil. I mean, seriously Nils, 50,000 ain't enough? You live in Finland in the 1930s for God's sake. Pick up an ax already; your house won't heat itself!

⁴⁰..... And puns about Goldbach's conjecture make you *even number*.

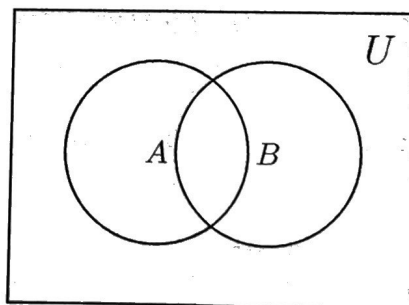
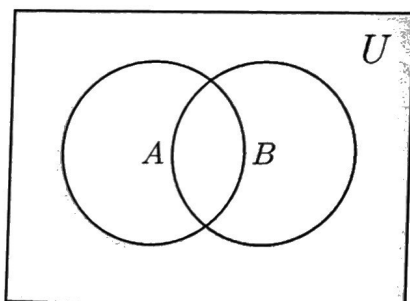
the set $A \cup B$, inside the set U :



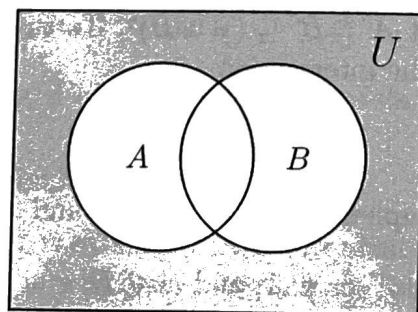
Taking the complement,²¹ this is $(A \cup B)^c$:



Meanwhile, here are A^c and B^c :



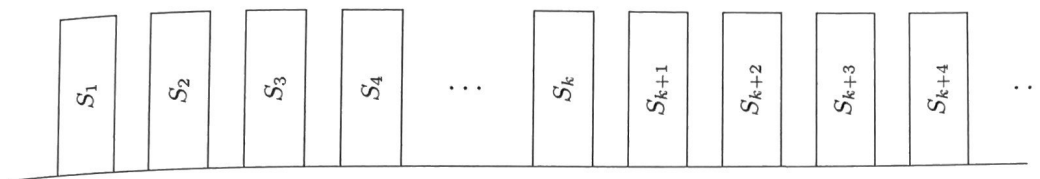
Since these are A^c and B^c , the Venn diagram of $A^c \cap B^c$ is the set of all points which are shaded in *both* of the above diagrams. Which is this:



The Venn diagram for $(A \cup B)^c$ is the same as the Venn diagram for $A^c \cap B^c$!

²¹There are two types of people in this world. Those who understand complements and (those who understand complements)^c.

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. \square

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.

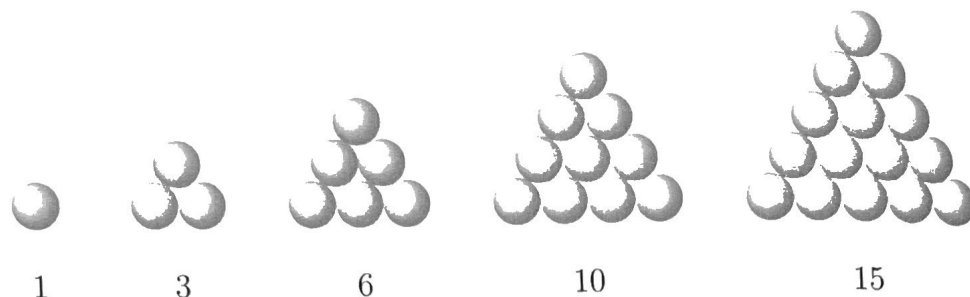
Assume there is a ladder that rests on the ground but climbs upwards forever. Assuming you can step on the first rung, and assuming that you can always step from one rung to the next, then sky's (not even) the limit! You can climb upward forever!³

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 $1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 = \frac{8(8+1)}{2}$. We aim to prove all S_n are true.

Proof Idea. Since we are aiming to prove something for all $n \in \mathbb{N}$, it makes sense to consider 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 (S_k) 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 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 " $1 + 2 + \cdots + 6 + 7$." These are certainly 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!

$$1 + 2 + 3 + \cdots + (k+1) = \underbrace{1 + 2 + 3 + \cdots + k}_{= \frac{k(k+1)}{2}, \text{ by induc. hyp.}} + (k+1)$$

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

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}.$$

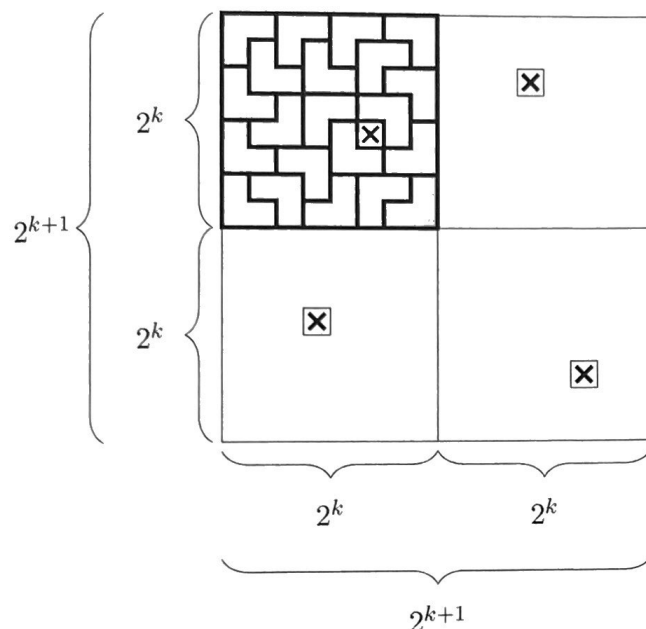
Induction Step. We aim to prove that the result holds for $k+1$. That is, we wish to show that

$$1 + 2 + 3 + \cdots + (k+1) = \frac{(k+1)((k+1)+1)}{2}.$$

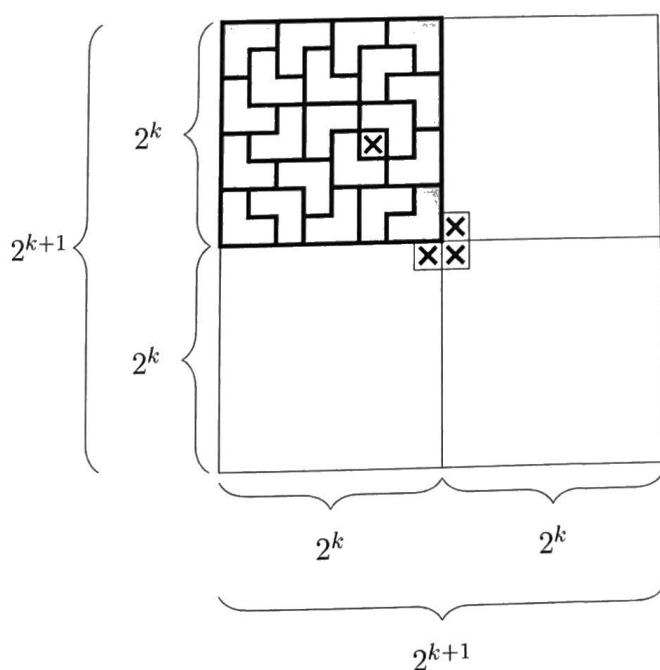
⁵This was obtained by looking at the proposition and plugging in $k+1$ for n .

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!

But what about the other three $2^k \times 2^k$ boards? 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:



Conclusion. By induction, this means that

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots < \infty,$$

completing the “proof.”



Once again, this must be 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.

$$1 = 2^1 - 1 \quad \checkmark$$

$$1 + 2 = 2^2 - 1 \quad \checkmark$$

$$1 + 2 + 4 = 2^3 - 1 \quad \checkmark$$

$$1 + 2 + 4 + 8 = 2^4 - 1 \quad \checkmark$$

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.

“Jessica wearing sunglasses is a necessary and sufficient condition for it to be sunny,” 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?

| | | | |
|--------|---------------------|-------------------|-------------------|
| | • $P \Rightarrow Q$ | | • P only if Q |
| Should | • If P , then Q | be the same as | or ? |
| | • Q if P | | • 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 $Q \Rightarrow P$.¹² 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.

¹²When 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.

$$A \cap B = \{x : x \in A \wedge x \in B\} \quad \text{and} \quad A \cup B = \{x : x \in A \vee x \in B\}.$$

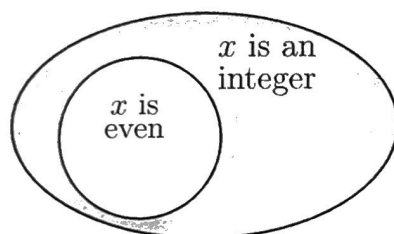
This is especially nifty because \cap and \wedge look a lot alike, and \cup and \vee look a lot alike.

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 $\sim P$.)¹³

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 ” (the set of residents of LA) is smaller than the “ Q ” (the set of residents of CA). Likewise, $A \subseteq B$ if the “ A ” is smaller than the “ B .” In the same way, $Q \Rightarrow P$ is analogous to $B \subseteq A$, and thus $P \Leftrightarrow Q$ is analogous to $A = B$. Here is an example of all this:

- Sets: Suppose $A = \{x : x \text{ is an even integer}\}$ and $B = \mathbb{Z}$. Then, $A \subseteq B$.

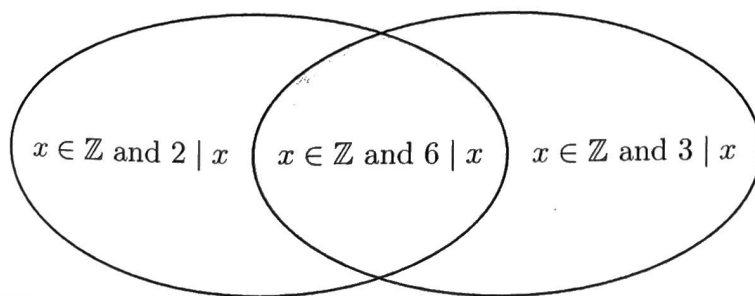
Logic: Suppose P is the open sentence “ x is even” and Q is the open sentence “ x is an integer.” Then, $P \Rightarrow Q$.



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 $\sim P$ is the statement “ x is an odd integer.” Another example:

- Sets: Suppose that $A = \{x \in \mathbb{Z} : 2 \mid x\}$ and $B = \{x \in \mathbb{Z} : 3 \mid x\}$. Then, $A \cap B = \{x \in \mathbb{Z} : 6 \mid x\}$.

Logic: Suppose 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 $6 \mid x$.”



¹³In 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 $!P$.

tables for $P \Rightarrow Q$ and $Q \Rightarrow P$:

| P | Q | $P \Rightarrow Q$ |
|-------|-------|-------------------|
| True | True | True |
| True | False | False |
| False | True | True |
| False | False | True |

| P | Q | $Q \Rightarrow P$ |
|-------|-------|-------------------|
| True | True | True |
| True | False | True |
| False | True | False |
| 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 (open) sentence

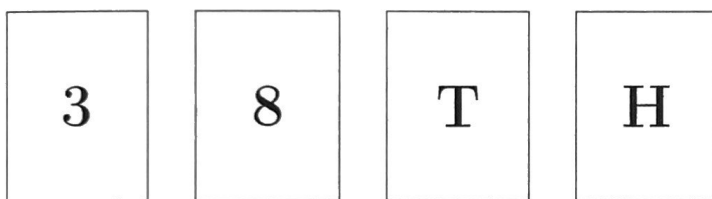
“ n is even”

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,

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 drunk, 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.

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.⁴

⁴ Meme that I can't print without paying *The Office* an annoyingly large amount of money:
 Pam to Michael: Corporate needs you to find the differences between this picture ($P \Rightarrow Q$) and this picture ($\sim Q \Rightarrow \sim P$).
 Pam to the camera: They're the same picture.

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.

For the next result, recall that in Lemma 2.17 part (iii) we proved that if $p \mid bc$, then $p \mid b$ or $p \mid c$. Let's now prove the indivisibility⁹ 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 $p \nmid b$.

You might hope that this proposition is precisely the contrapositive of Lemma 2.17 part (iii); 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 of each other. 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 $\sim Q \Rightarrow \sim P$.¹⁰

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,

$$ab = (pk)b = p(kb).$$

⁹Fun fact: "indivisibility" has more copies of 'i' in it than any other English word. Other winners: "abracadabra" has the most copies of a, knickknack has the most ks, whippersnapper the most ps, bowwow the most ws, and pizzazz has the most zs.

¹⁰In fact, $\sim P \Rightarrow \sim Q$ is the converse of the contrapositive. (Or, the contrapositive of the converse.)

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 Counterexamples

The contrapositive is naturally a shorter topic than our other proof methods, so I am going to steal a few pages here to discuss counterexamples. We first mentioned counterexamples way back on Page 11 as a way to disprove a conjecture. The idea is this: In order to disprove a “universal” statement (like one using the words “for all” or “for every”), it suffices to find one example against it. If I said “every NBA player can dunk,” to disprove it you would have to find a single NBA player that cannot dunk. If you did, then that single NBA player is a *counterexample* to the claim “every NBA player can dunk.” Indeed, to disprove a statement, you must prove its negation. And the negation of a “for all” statement is always a “there exists” statement. We can do this with a single counterexample.

Likewise, if I said “every prime number is odd,” you could disprove that by presenting the counterexample of 2. Of course, sometimes it is more difficult to find a counterexample. Suppose, for instance, you saw this conjecture:

Conjecture 1. If p is prime, then $2^p - 1$ is prime.

Disproof Idea. Notice that even though we did not use language like “for all,” this is still a universal statement, as it is asserting something about every prime p . As it turns out, this conjecture is false. Since it is a false universal statement, there must be a counterexample. You could try the first few cases:

$$2^2 - 1 = 3, \text{ which is prime}$$

$$2^3 - 1 = 7, \text{ which is prime}$$

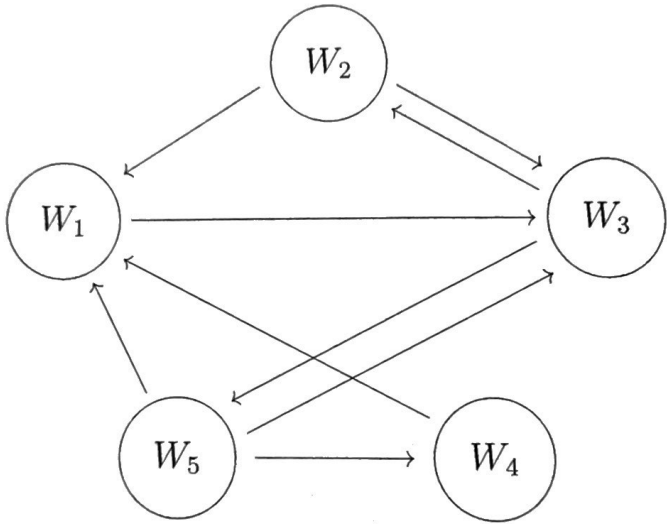
$$2^5 - 1 = 31, \text{ which is prime}$$

$$2^7 - 1 = 127, \text{ which is prime}$$

I remember the days before Google. I remember being in first grade and having to write a short report on dogs. My family didn't have a book to help me, nor did we have a set of the Encyclopedia Britannica — which would be the standard resource for such a project — and so I turned to my Plan B: the Internet. After a long and noisy dial-up process, I was on! But...how do I find websites about dogs? I remember trying `dog.com` and `dogs.com`, and when they weren't helpful, I was out of ideas.

Why? Because this was before Google! There were a few search engines out there, but they were bad and I probably didn't even know about them. These primitive search engines had succeeded in indexing lots and lots of websites, so if you searched for "facts about dogs" it could return websites that used all three words, but they struggled mightily to rank them by importance. The magic behind Google is that the "good stuff" always winds up near the top. For example, "Long Form Math" returns nearly 500 million results — but this book's companion website, `longformmath.com`, is at the top of the list.²⁵

So how does Google do it? The one piece of information that they can easily collect about a website is the number of links it has to other websites, and which websites it links to. As a *much* smaller example, consider an internet with five websites, and the following links ($A \rightarrow B$ means website A linked to website B).



Our goal is to assign to each website a numerical *value*. Let v_1 be the value of website W_1 , let v_2 be the value of website W_2 , and so on. You can think about a link as an endorsement — if $A \rightarrow B$, then in some ways website A has endorsed website B as being important. Now, there are two tensions here:

- It should be more valuable to be endorsed by an important website than a bad website.
- It should be less valuable to be endorsed by a website if that website endorses lots of other websites.

You can think about this like a political endorsement in a presidential primary. It should be considered more valuable to be endorsed by the governor than by a

²⁵Please check it out!

city council member. But if someone endorses both you and someone else, then it shouldn't be worth quite as much as if you were the only candidate they supported; it is basically a half endorsement.

With this intuition, look at the internet graph above, and for now let's consider website W_1 .

| | | | |
|-----------------------------------|-------|-------|-------|
| W_1 endorsed by: | W_2 | W_4 | W_5 |
| Which has value: | v_2 | v_4 | v_5 |
| Number of websites they endorsed: | 2 | 1 | 3 |

Website W_1 , in a sense, received half of an endorsement from W_2 , because W_2 also endorsed one other website. Website W_1 also received a full endorsement from W_4 and a third of an endorsement from W_5 . Therefore, if we wish to assign a numerical value v_1 to the website W_1 , and if this value is to be determined by these endorsements, it would make sense to want

$$v_1 = \frac{v_2}{2} + v_4 + \frac{v_5}{3}.$$

Doing this for all other websites, this would produce the following.

$$v_1 = \frac{v_2}{2} + v_4 + \frac{v_5}{3}$$

$$v_2 = \frac{v_3}{2}$$

$$v_3 = v_1 + \frac{v_2}{2} + \frac{v_5}{3}$$

$$v_4 = \frac{v_5}{3}$$

$$v_5 = \frac{v_3}{2}$$

Big question. Is it possible to assign numerical values to v_1, v_2, v_3, v_4 and v_5 so that the above are all satisfied?

Although it might seem silly to put these into vectors, having these all satisfied is indeed the same thing as saying

$$\begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{bmatrix} = \begin{bmatrix} \frac{1}{2}v_2 + v_4 + \frac{1}{3}v_5 \\ \frac{1}{2}v_3 \\ v_1 + \frac{1}{2}v_2 + \frac{1}{3}v_5 \\ \frac{1}{3}v_5 \\ \frac{1}{2}v_3 \end{bmatrix}.$$

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 sides 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 begun 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 a land 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, so 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.⁵

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

⁵We 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.

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 $(p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_k) + 1$. Either this number is prime, in which case it is a *new* prime, since it is bigger than each p_i , or⁶ 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 being 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 $N = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_k$, which is the product of every prime. Next, consider the number $N + 1$, which is $(p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_k) + 1$. 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.

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

⁶By 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 \dots 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.

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 contradiction. Then, you would assume for a contradiction that 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*.³¹ 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, 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.

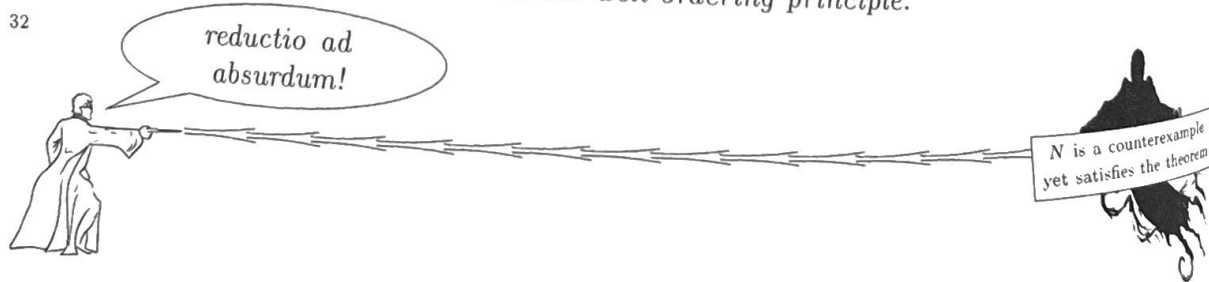
Proof. Assume for a contradiction that this is not true. Then there must be a minimal counterexample; let's say N is the smallest natural number greater than or equal to 2 which is neither prime nor the product of primes. Since it is not prime, by definition this means that it is composite: $N = ab$ 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.

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,³² completing the proof. \square

³¹ Again, this is because of the fact that every nonempty set of natural numbers must contain a smallest element, which is sometimes called the *well-ordering principle*.

³²



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:

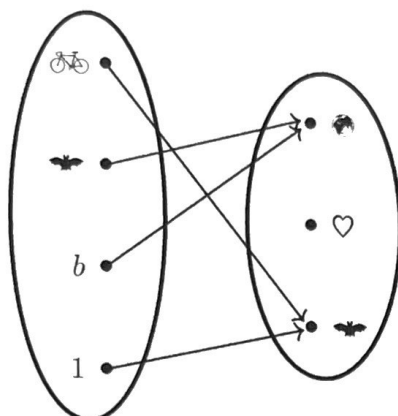
- If you two both say you worked together, you will fail that assignment, but that's it.
- If you both accuse the other of cheating off them, then the university will decide neither to be credible and so neither will be expelled. But the professor says she would act harshly, and you would both fail her 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: McDonald's Hiring? Tom: No Punishment |
| | Blame Tom | You: No Punishment Tom: McDonald's Hiring? | You: Fail Class Tom: Fail Class |

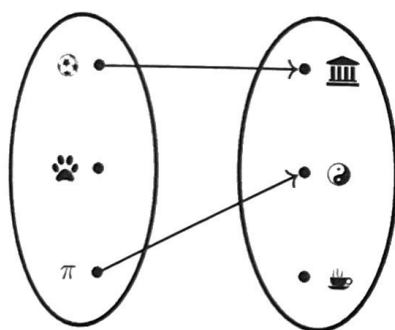
You don't know Tom too well, so you don't know what he will do. And for the sake of this problem, the truth about who cheated is not important. We simply ask: If you and Tom are "rational actors" (i.e., selfish logicians), and will therefore choose the option which minimizes your own penalty, what will you and Tom do?

A function's domain and codomain can each be *any* set. For example, here's a graphical way to write some function f :

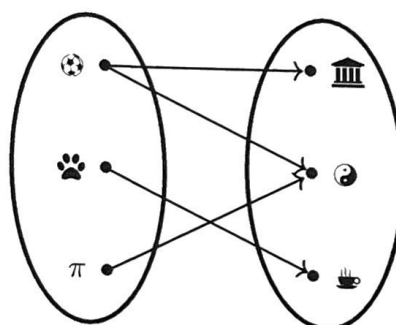


This is a function with domain $\{1, b, \text{flower}, \text{bicycle}\}$, codomain $\{\text{flower}, \text{heart}, \text{flower}, \text{flower}\}$, and range $\{\text{flower}, \text{heart}\}$. For example, $f(1) = \text{flower}$, so flower is in the range. However, there does not exist any $x \in \{1, b, \text{flower}, \text{bicycle}\}$ such that $f(x) = \text{heart}$, which is why heart is not in the range.³

For a diagram like this to *not* represent a function, it would have to fail either the existence or the uniqueness part of being a function, as discussed in the Recurring Theme Alert. Below are two examples.



Fails existence

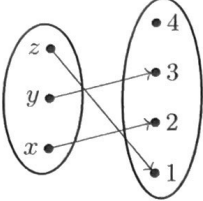
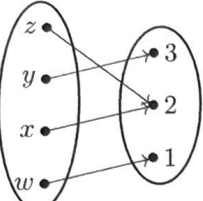
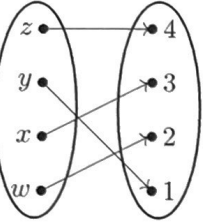


Fails uniqueness

It is perfectly ok to have two arrows pointing at the same dot in the codomain (or zero arrows, or more than two arrows), 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;⁴ the first because paw is being sent to nowhere, and the second because π is being sent to two places.

³Another metaphor: Suppose Cupid is shooting arrows at a target; he hits different spots on the target, but never misses the target completely. Then, Cupid is like a function. The codomain is the target, since those are the possible points that can get hit. The range is the set of points on the target that actually do get hit by an arrow. So, for the function above, since heart was not in the range, Cupid missed love. :-)

⁴We 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 responds to an action with a single, anticipated reaction.

| | 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,⁶ 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.⁷

⁶Simply being a function means that everyone in A has found love. The surjectivity guarantees that everyone in B has also found love.

⁷Foreshadowing Alert: For f to be a function, we demanded existence and uniqueness criteria on A . If $f : A \rightarrow B$ is a bijection, then we demand those same criteria [footnote continues on next page]

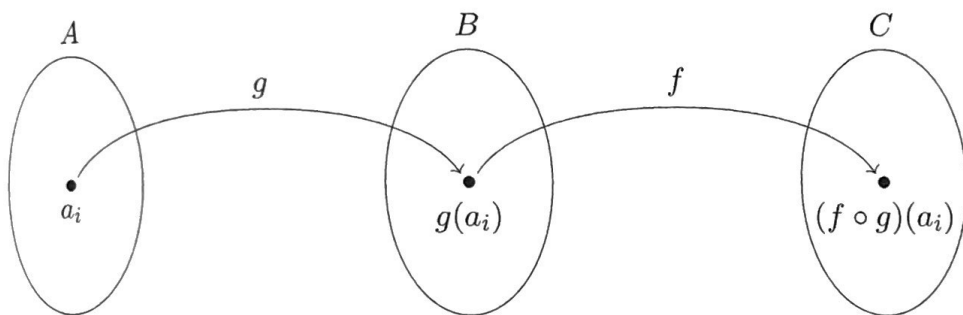
Theorem.

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 $a_1 = a_2$. Basically, the proof consists of two copies of the standard injective proof, with the definition of a composition thrown in (which is what makes it challenging). Here is the proof overview:

$$f(g(a_1)) = f(g(a_2)) \xRightarrow{f \text{ is injective}} g(a_1) = g(a_2) \xRightarrow{g \text{ is injective}} a_1 = a_2.$$

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 that works for *any* two elements in B . In particular, note that $g(a_1)$ 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 $f(b_1) = f(b_2)$ for any $b_1, b_2 \in B$, then $b_1 = b_2$. 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

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 generated by 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 generated by a* to be the set

$$\{b \in A : a \sim b\}.$$

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 .”

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 unique²¹ element $b \in B$ for which $(a, b) \in F$.

And with that — as far as functions are concerned — your undergraduate brain expansion is now complete.

What you were
taught in grade school



A function is
like x^2

What you were
taught in middle school



If it passes
the vertical
line test

What you were
taught in high school



If every input
has only one output

What I told you
in Chapter 8



Each x in the domain
is sent to one
 y in the codomain

What I told you
earlier this chapter



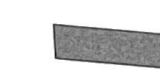
A special subset F
of the Cartesian
product $A \times B$.

What I told you
just now

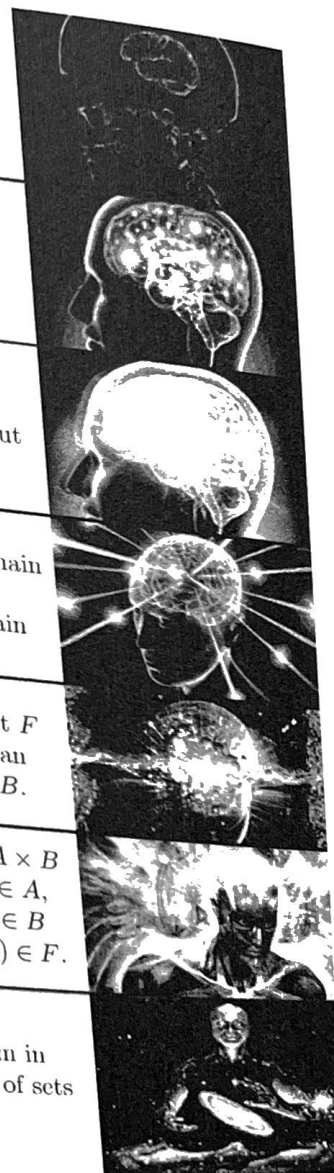


A relation on $A \times B$
such that $\forall a \in A$,
 \exists a unique $b \in B$
such that $(a, b) \in F$.

Go to
grad school



A morphism in
the category of sets



²¹ 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 there is a b for which $(a, b) \notin F$ for all $a \in A$. But if this doesn’t happen, then we again have a special name for such a function: a surjection!

Appendix A: Other Proof Methods

Throughout this text we have discussed many approaches to prove a theorem. These include:

- Pigeonhole Principle
- Direct Proof
- Proof by Cases
- Principle of Mathematical Induction
- Proof by Contraposition
- Proof by Contradiction (and, relatedly, proof by minimal counterexample)

These methods were mostly justified through our discussion on logic, and they are sufficient to prepare you for later math courses. There is another class of proof methods, which are justified using the theorems/techniques from some area of math, like probability, linear algebra or combinatorics. If these approaches prove useful enough, they might be given the lofty title of a “method.” Indeed, the first three sections of this appendix will be on the probabilistic method, the linear algebra method, and the combinatorial method. The probabilistic and combinatorial methods are really important and used a lot. Connections to linear algebra appear all over mathematics, but the linear algebra method that we will be discussing does not play a central role in math. Nevertheless, it is worth including because most of you have seen linear algebra and it is another good example of applying one area of math to another.

We have studied proofs by cases, and an extreme version of this is a proof with so many cases it will feel like a brute-force argument. In recent decades, computers have proven useful at tackling such problems. As such, we will discuss computer-assisted proofs.

Finally, we will discuss proofs that rely almost entirely on a picture. Calling this a proof *method* is stretching the term to its breaking point, but they are useful and fun and it’s my book so I’m doing it.

To keep the focus on the methods rather than on theory-building, we will focus our attention on applications from areas of math that have already been discussed in this book and/or have lower points of entry: Ramsey theory, number theory, set theory, coding theory and combinatorics.

Appendix B: Proofs From The Book

Paul Erdős (who passed away in 1996) imagined a book in which God wrote down every theorem, and following each theorem He wrote down the best, most beautiful, most elegant proof of that theorem. Ironically, Erdős was an agnostic atheist, yet his idea of “The Book” caught on, and soon it entered the standard vocabulary of research mathematicians. It also highlights a common belief among mathematicians that proofs should be beautiful. As G.H. Hardy said, “there is no permanent place in this world for ugly mathematics.”

Indeed, I once attended a math conference and was chatting with the photographer who was hired to document the event. She said that academic conferences are her specialty and had taken pictures at conferences in dozens of different areas, from the sciences to the humanities. I asked her what stood out about the math conferences, expecting us to spend the next couple minutes joking around about mathematicians’ lack of fashion, or something. But she remarked that the thing which most surprised her was how often mathematicians talked about beauty in their field. She said that only art conferences talked about beauty more than us.

If Erdős read a proof and found it correct yet ugly, he might comment that it is good that we know the theorem is true, but we should still search for “the proof from The Book!” This refrain has echoed through the decades.

The title of this appendix was stolen¹ from Martin Aigner and Günter M. Ziegler, who had the wonderful idea to write a book with the same name and idea. It’s the type of idea which, if I had had it first, I probably would have dropped all other projects to focus exclusively on it. A couple proofs in this appendix are also included in their delightful book, although the collection in this appendix is much more geared to mathematicians at your stage of learning (and I again take a long-form approach to the task). But I encourage you to check out their book; it is broken up by subject, so after you finish each of your upper division math courses you can read through the Book Proofs they amassed from that field. Enjoy!

¹Well, let’s call it a tribute.