

# Mathcamp Crash Course

Mathcamp 2025

Glenn Sun

*These notes may contain errors,  
and should not be considered an authoritative source.*

## Contents

<b>1</b>	<b>Syntax of mathematics</b>	<b>2</b>
1.1	Logic . . . . .	2
1.2	Sets and quantifiers . . . . .	6
<b>2</b>	<b>Introduction to proofs</b>	<b>12</b>
2.1	How to prove things . . . . .	12
2.2	How to use things . . . . .	16
<b>3</b>	<b>Advanced proof techniques</b>	<b>20</b>
3.1	Induction . . . . .	20
3.2	Contrapositive and contradiction . . . . .	26
<b>4</b>	<b>Functions</b>	<b>30</b>

# 1 Syntax of mathematics

Mathematicians share a common language to make precise what they are talking about. In this first section, we'll learn the basics of this language.

## 1.1 Logic

There are a couple of English words that we use casually in English, but have precise meanings in mathematics. First, the words “and”, “or”, and “not”. We can summarize what they mean using *truth tables*. (Because the symbols “T” and “F” look visually similar, we will use “0” for false and “1” for true instead.)

A	B	A and B	A	B	A or B	A	not A
0	0	0	0	0	0	0	1
0	1	0	0	1	1	1	0
1	0	0	1	0	1		
1	1	1	1	1	1		



In other words, “A and B” is true when *both* are true, and “A or B” is true when *at least one of them* is true, including when both are true! This resolves a contextual ambiguity in English: if someone says “You must have a Master’s degree or 3 years experience for this job,” it is certainly okay to have both a Master’s and 3 years experience, but if someone says “This lunch contains your choice of a piece of fruit or a bag of chips,” you are probably not allowed both fruit and chips.

Sometimes, there are multiple ways to express the same sentence. For example,

“I will not do TPS and I will not do relays.”

means the same thing as

“It is not true that I will do TPS or relays.”

Generalizing this example, we have:

**Theorem 1.1** (de Morgan’s laws). *For any two statements A and B,*

- “not [A and B]” means the same as “[not A] or [not B]”.
- “not [A or B]” means the same as “[not A] and [not B]”.

*Proof.* We can reason through all cases, depending on whether A and B are true or false. For example, if A and B are false, then “not [A and B]” is true, and “[not A] or [not B]” is also true (so they are the same). Here are all four cases of the first de Morgan’s law:

A	B	A and B	not [A and B]	A	B	not A	not B	[not A] or [not B]
0	0	0	1	0	0	1	1	1
0	1	0	1	0	1	1	0	1
1	0	0	1	1	0	0	1	1
1	1	1	0	1	1	0	0	0

The second law is left as practice for you. □

~~~

The next logical word we will learn is “implies”. The sentence “A implies B” is also often written as “if A, then B” or “B, if A.” The meaning of these sentences is summarized by the following truth table.

| A | B | A implies B |
|---|---|-------------|
| 0 | 0 | 1           |
| 0 | 1 | 1           |
| 1 | 0 | 0           |
| 1 | 1 | 1           |



This truth table can be confusing at first. For example, it suggests that the sentence “if 2 is odd, then 4 is odd” is true. You might think intuitively that such a sentence is neither true nor false: it is just meaningless because 2 is not odd. There is no situation where this sentence could help you reason about anything.

However, consider the sentence “for all  $n$ , if  $n$  is odd, then  $n + 2$  is odd.” We would certainly want this sentence to be considered true. Thus, when you plug in  $n = 2$ , you get “if 2 is odd, then 4 is odd,” so we should consider this to be true. We will talk more about sentences with variables like this in the next section.

**Proposition 1.2.** “A implies B” means the same thing as “[not A] or B.”

*Proof.* We just use a truth table again.

| A | B | A implies B | A | B | not A | [not A] or B |
|---|---|-------------|---|---|-------|--------------|
| 0 | 0 | 1           | 0 | 0 | 1     | 1            |
| 0 | 1 | 1           | 0 | 1 | 1     | 1            |
| 1 | 0 | 0           | 1 | 0 | 0     | 0            |
| 1 | 1 | 1           | 1 | 1 | 0     | 1            |

Again, because the final columns are the same, these are equivalent.

**Corollary 1.3.** “not [A implies B]” means the same thing as “A and [not B].”

*Proof.* Apply de Morgan’s law to the above proposition.

**Example 1.4.** Negate the following sentence. In other words, when is the following sentence a lie?

“If it is cold, I will put on a jacket and raise the thermostat.”

*Solution.* Negating the implication, we get

“It is cold, and it is not true that [I put on a jacket and raised the thermostat].”

We can apply de Morgan’s law to finally get

“It is cold, and [I did not put on a jacket or I did not raise the thermostat].”

There is also “A is implied by B,” which means the same as “B implies A,” and “A if and only if B,” which means the same as “A implies B, and A is implied by B.” In other words, we say “A if and only if B” when A and B are equivalent statements. In particular, “A if and only if B” has the following truth table.

| A | B | A if and only if B |
|---|---|--------------------|
| 0 | 0 | 1                  |
| 0 | 1 | 0                  |
| 1 | 0 | 0                  |
| 1 | 1 | 1                  |

This means that in all the theorems before where we said “means the same as,” we could have been more precise with our language and said “if and only if.”

~~~



Before closing off this section, be aware that when giving a definition, many people tend to write “if” when they really mean “if and only if”. For example, if someone says “A real number  $x$  is called positive if  $x > 0$ ,” this really means “A real number  $x$  is called positive if and only if  $x > 0$ .” There is no good reason for this, just a quirk of culture.

Also, you may occasionally see people use symbols for some of the logical words we’ve described above. These symbols are primarily used in personal notes, whiteboard shorthand, and when studying logic as a mathematical discipline. They should *not* be used in most formal mathematical writing.

and	or	not	implies	implied by	if and only if
$\wedge$	$\vee$	$\neg$ or $\overline{\phantom{x}}$	$\rightarrow$ or $\Rightarrow$	$\leftarrow$ or $\Leftarrow$	$\leftrightarrow$ or $\Leftrightarrow$ or iff

## Practice

- Use words from mathematical logic (“and”, “or”, “implies”, etc.) to rewrite the following English phrases:
  - Neither A nor B
  - For A, it suffices that B
  - A, but B
  - Exactly one of A and B is true
- For each of the following facts, write an example sentence to ensure that it makes intuitive sense. Then prove them using truth tables, until you feel bored. (But these are all important facts, so make sure you are comfortable using them even if you skip the proofs.)
  - (de Morgan’s laws, part 2)  
 “not (A or B)” means the same as “(not A) and (not B)”
  - (distributivity of or over and)  
 “A or (B and C)” means the same as “(A or B) and (A or C)”
  - (distributivity of and over or)  
 “A and (B or C)” means the same as “(A and B) or (A and C)”

- Does “not [A implies B]” mean the same thing as “A implies [not B]”? Explain.
- Negate the following sentence by applying rules. In other words, when is the following sentence false? In your final answer, ensure that the word “not” only appears before A, B, C, ... (not more complicated expressions).

If [A and B], then [[C or not D] and E].

## Extensions

These problems describe extra things to think about that might be interesting, but not fundamental for your future learning. They may be harder.

- (Universal gates, **22**) We introduced a bunch of logical words, like “and”, “or”, “not”, and “implies”. We saw that you don’t really need “implies” because “A implies B” is just shorthand for “[not A] or B.”

Here’s a fun fact: you can get away with even fewer words! Let “A nand B” mean “not [A and B]”. Here is the truth table of “nand”:

A	B	A nand B
0	0	1
0	1	1
1	0	1
1	1	0

It turns out that if you have “nand”, you don’t need “and”, “or”, or “not” at all! Just one logical word is enough to express any logical relationship that you want, such a word is called a *universal gate*. Show how to express “A and B”, “A or B”, and “not A” using just “nand” (and some parentheses). (Hint: figure out “not A” first.)

(As an aside: electrical engineers use “nand” a lot in their circuits for this reason! Instead of manufacturing lots of different logical pieces for different uses, sometimes, they find it useful to just make a lot of “nand gates” and string them together in the ways you discovered.)

- (DNF and CNF form, **22**) Let A, B, C, ... be some sentences without logical words (i.e. “it is raining”). A sentence is in *disjunctive normal form* (DNF form) if it looks something like:

“[A and [not B] and C] or [[not D] and E] or [F and G and [not H] and [not I]].”

In other words, call the sentences “A” and “not A” *atoms*, call an “and” of atoms a *term*, and a sentence in disjunctive normal form is an “or” of terms. Give a method to convert any logical sentence into DNF form. (In particular, this means that parentheses in a logical expression never need to be more than two levels deep.)

As an additional challenge, *conjunctive normal form* (CNF form) is the same thing, but with the roles of “and” and “or” swapped. In other words, a *clause* is a “or” of atoms, and a sentence is in CNF form if it is an “and” of clauses. Give a method to convert any logical sentence into CNF form.

(As an aside: DNF and CNF form are critically important in computer science! The P vs. NP problem, which has a \$1 million bounty for solving, is equivalent to asking: When given a formula in CNF form, is there an efficient way to determine whether or not the truth table has at least one 1 in the last column?)

## 1.2 Sets and quantifiers

Logic is about reasoning, but what are the things that mathematicians reason about? First, we typically think about some basic *objects*. These are the things that we aren't interested in further breaking into parts. Examples include 2,  $\pi$ , Alice, and the action of rotating the right face of a Rubik's cube by  $90^\circ$  clockwise. Then, we can put the objects together into collections called *sets*. Sets contain objects (or other sets!) and don't care about order or duplicates.

### Example 1.5.

- The set of Fruit at Mathcamp 2025: {Eric, Kevin, Marisa}.
- The set of Mathcamp RA groups: (redacted for privacy—it would look something like {{A, B, C, D}, {E, F, G}, {H, I, J, K, L}}) but with more students and groups.
- $\{1, 2, 2\} = \{1, 2\} = \{2, 1\}$ , because we don't care about order or duplicates.
- The natural numbers (or whole numbers):  $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ . It's typical to write an infinite list that follows a pattern using "...". Note that mathematicians do not agree on whether or not  $\mathbb{N}$  includes 0, but in this class we will include 0.
- The real numbers  $\mathbb{R}$  (all the numbers on the number line, including  $\pi$ ,  $\sqrt{2}$ , etc.). There is no way to write down all the elements of  $\mathbb{R}$  as a list that follows a pattern, but  $\mathbb{R}$  is still a set because it is a collection of objects.
- The integers  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ , the rationals  $\mathbb{Q}$  (fractions of integers), and the complex numbers  $\mathbb{C}$ .
- The empty set, having no objects:  $\emptyset$ . ┐

The most basic question that you can ask about a set is whether or not it contains a particular element. We use the following notation.

$$\begin{array}{ll} X \text{ contains the element } x & \longleftrightarrow x \in X \\ X \text{ does not contain the element } x & \longleftrightarrow x \notin X \end{array}$$

The symbol  $\in$  is pronounced “in”, and the symbol  $\notin$  is pronounced “not in”.

### Example 1.6.

- $\pi \in \mathbb{R}$ .
- $\sqrt{2} \notin \mathbb{N}$ .
- $0 \notin \{\{0, 1\}, \{2, 3\}\}$ . This set contains two groups of numbers. For example,  $\{0, 1\} \in \{\{0, 1\}, \{2, 3\}\}$ . We would not say that it contains any numbers directly. ┐



~~~

With sets, there are two new logical words that we need to introduce: “for all” and “there exists”. These are called *quantifiers*. Note that every time you say “for all  $x$ ” or “there exists  $x$ ”, it is important that to mention what set you are talking about!

### Example 1.7. Here are some true statements.

- For all  $n \in \mathbb{N}$ , the number  $n(n + 1)$  is even.
- There exists  $x \in \mathbb{R}$  such that  $x^2 + x - 5 = 0$ . ┐

You can think of “for all” as a kind of infinite “and”, and “there exists” as a kind of “infinite or”. For example, if we allowed mathematics to involve infinitely long sentences, the sentence “for all  $n \in \mathbb{N}$ , the number  $n(n + 1)$  is even” could be rephrased as:

$0(0 + 1)$  is even and  $1(1 + 1)$  is even and  $2(2 + 1)$  is even and  $3(3 + 1)$  is even and ...

Recall de Morgan’s law, that “not [A and B]” means the same thing as “[not A] or [not B]”. By analogy, with the above way of thinking, if  $A(x)$  is a sentence about  $x$ , we should have the following:

- “not [for all  $x \in X$ ,  $A(x)$ ]” means “there exists  $x \in X$  such that not  $A(x)$ ”.
- “not [there exists  $x \in X$  such that  $A(x)$ ]” means “for all  $x \in X$ , not  $A(x)$ ”.



These rules are important. It is very easy to get lost when thinking about quantifiers and negation, and knowing these rules will help you prevent mistakes.

**Example 1.8.** Negate the following sentences without using the word “not” or anything similar.

“For all  $m \in \mathbb{N}$ , if there exists  $n \in \mathbb{N}$  such that  $m = 2n$ , then  $m$  is even.” ┘

*Solution.* Applying the above rule, we convert

“not [for all  $m \in \mathbb{N}$ , if there exists  $n \in \mathbb{N}$  such that  $m = 2n$ , then  $m$  is even]”

into

“there exists  $m \in \mathbb{N}$  s.t. not [if there exists  $n \in \mathbb{N}$  s.t.  $m = 2n$ , then  $m$  is even]”

which becomes

“there exists  $m \in \mathbb{N}$  s.t. [[there exists  $n \in \mathbb{N}$  s.t.  $m = 2n$ ] and not( $m$  is even)]”

which is the same as

“there exists  $m \in \mathbb{N}$  and  $n \in \mathbb{N}$  such that  $m = 2n$ , and  $m$  is odd.”

(We used “s.t.” to mean “such that” to make sure each sentence fit on one line: this is shorthand like  $\wedge$ ,  $\forall$ , etc. and should normally be avoided in formal writing.) □

~~~

Next, let us discuss one common way of writing down a set, called *set-builder notation*. It is used as follows:

$Y = \{\text{some expression using } x \mid x \in X, \text{ and possibly other conditions}\}.$

The symbol  $\mid$  is pronounced “such that” (but never replace the English words “such that” with  $\mid$ ). This set-builder expression means, go through everything in  $X$ , and for each  $x$  satisfying all the other conditions, include “some expression using  $x$ ” in the set  $Y$ .

**Example 1.9.**

- The set of square numbers:  $\{x^2 \mid x \in \mathbb{N}\}.$
- The set of squares of odd numbers:  $\{x^2 \mid x \in \mathbb{N} \text{ and } x \text{ is odd}\}.$  ┘

There are a couple variations on this notation. When the expression using  $x$  is just “ $x$ ”, many people prefer to write the shorthand notation:

$$Y = \{x \in X \mid \text{other conditions}\}.$$

It is also common to introduce multiple variables in the right hand side. When this happens, it means to go through all possible combinations of the variables.

$$Z = \{\text{some expression using } x \text{ and } y \mid x \in X, y \in Y, \text{ and possibly other conditions}\}.$$

**Example 1.10.**

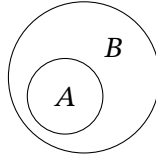
- The set of odd primes =  $\{x \in \mathbb{N} \mid x \text{ is odd and } x \text{ is prime}\}.$
- The set of complex numbers,  $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}.$

~~~

Now, let's get a bit familiar with common words used to talk about sets.

**Definition 1.11.** Let  $A$  and  $B$  be two sets.

- We say that  $A$  is a subset of  $B$ , written  $A \subseteq B$ , if for all  $x \in A$ , we also have  $x \in B$ .
- We say that  $A$  is a superset of  $B$ , written  $A \supseteq B$ , if for all  $x \in B$ , we also have  $x \in A$ .
- We say that  $A = B$  if  $A \subseteq B$  and  $A \supseteq B$ .



$A \subseteq B$ , equivalently  $B \supseteq A$



Note that in contrast to  $<$  and  $\leq$ , which makes sense, the symbol  $\subset$  does *not* typically mean “subset but not equal to”. Some authors use it as a synonym for  $\subseteq$ , others avoid this symbol entirely. To express “subset but not equal to”, use  $\subsetneq$ .

**Definition 1.12.** The power set of a set  $A$ , denoted  $\mathcal{P}(A)$  is the set of all subsets of  $A$ , including  $\emptyset$  (no elements) and  $A$  (all elements). In other words,  $B \in \mathcal{P}(A)$  means the same thing as  $B \subseteq A$ .

**Example 1.13.**

- $\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\}$
- There is not really a good way to write down the elements of  $\mathcal{P}(\mathbb{N})$  in a list, but for example, if  $A$  denotes the set of square numbers, then  $A \subseteq \mathbb{N}$  and  $A \in \mathcal{P}(\mathbb{N})$ .

The power set also allows us to write “for all  $A \subseteq B$ ”. This just means the same thing as “for all  $A \in \mathcal{P}(B)$ ”, and now you can use everything that you learned previously about quantifying over elements of sets to reason about quantifying over subsets. We often also use this in set-builder notation, i.e.

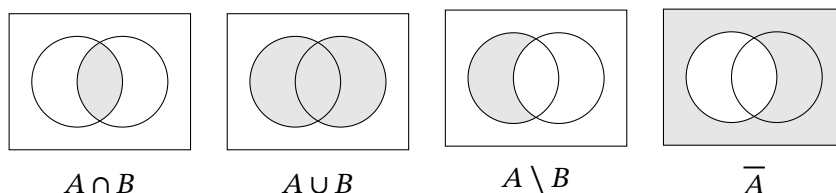
$$\{A \subseteq \mathbb{N} \mid 0 \in A\} = \{A \in \mathcal{P}(\mathbb{N}) \mid 0 \in A\}$$

is the set of all subsets of  $\mathbb{N}$  containing 0.

Basic sets can be put together using the following operations to make new sets.

**Definition 1.14.**

- (intersection)  $A \cap B$ : the set of elements in both  $A$  and  $B$
- (union)  $A \cup B$ : the set of elements in at least one of  $A$  or  $B$
- (difference)  $A \setminus B$ : the set of elements in  $A$  but not  $B$
- (complement)  $\overline{A}$ : a shorthand notation for  $U \setminus A$ , where  $U$  is a set representing the universe of all possibilities, usually inferred from context. (For example, if we are talking about subsets of  $\mathbb{N}$ , then the universe should probably be  $\mathbb{N}$ .) In formal situations, you should say explicitly what is  $U$ . ┘



A *tuple* is a collection of objects, but unlike a set, it cares about the order in which things are listed. For example,  $(1, 2) \neq (2, 1)$ . You're probably familiar with these tuples of length 2, known as ordered pairs, which are commonly used to represent points in the plane.

**Definition 1.15.** The Cartesian product of two sets  $X$  and  $Y$  is the set of ordered pairs

$$X \times Y = \{(x, y) \mid x \in X \text{ and } y \in Y\}.$$

We also write  $X^n$  for the set of ordered  $n$ -tuples of elements from  $X$ . ┘

Lastly, intervals of real numbers are so commonly used that we give them a special notation.

**Definition 1.16.**

- (closed interval)  $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ .
- (open interval)  $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$  (in Europe,  $]a, b[$ ).
- (half-open interval)  $(a, b]$  and  $[a, b)$  are as you expect (in Europe,  $]a, b]$  and  $[a, b[$ ).

Furthermore,  $a$  or  $b$  may be  $\infty$ , in which case we always write  $()$ , not  $[]$ . For example,  $(2, \infty) = \{x \in \mathbb{R} \mid x > 2\}$ . ┘

Europe prefers  $] [$  to disambiguate open intervals from ordered pairs. In the US, we unfortunately have to rely on context, since the notation is the same.

**Practice**

1. Write the following sets using set-builder notation:
  - (a) The first quadrant of the plane, where both coordinates are positive.
  - (b) The set of finite open intervals of  $\mathbb{R}$  (finite meaning no  $\infty$  endpoint(s)).

2. The following natural language sentences are false. Use words from mathematical logic (“for all”, “and”, “implies”, etc.) to rewrite them formally. Then, negate them, i.e. say what must be true in order to disprove the sentence.
- (a) There is a natural number bigger than every other natural number.
  - (b) There are two real numbers with no real numbers between them.
  - (c) There is a unique solution to the equation  $x^2 + 6x + 5 = 0$  in the real numbers.
3. Just like de Morgan’s laws for logic, with sets we have

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \quad \text{and} \quad \overline{A \cap B} = \overline{A} \cup \overline{B}.$$

Describe how you would draw a Venn diagram for each one (thus concluding that they are equal).

4. Express  $A \setminus B$  using only the symbols  $A$ ,  $B$ ,  $\cup$ ,  $\cap$ , and  $\overline{\phantom{x}}$ .
5. We are also allowed to take infinite unions and infinite intersections. Notations vary, but if you have an infinite list of sets  $A_1, A_2, A_3, \dots$ , one common way of writing them is

$$\bigcup_{i=1}^{\infty} A_i \quad \text{and} \quad \bigcap_{i=1}^{\infty} A_i.$$

Determine a simple expression for the following sets.

(a)  $\bigcup_{n=1}^{\infty} (-n, n)$

(c)  $\bigcap_{n=1}^{\infty} \left(0, \frac{1}{n}\right)$

(b)  $\bigcap_{n=1}^{\infty} \left[0, \frac{1}{n}\right]$


(d)  $\bigcup_{n=1}^{\infty} \left[0, 1 - \frac{1}{n}\right]$

## Extensions

These problems describe extra things to think about that might be interesting, but not fundamental for your future learning. They may be harder.

6. (Construction of  $\mathbb{N}$ ) As stated earlier, most mathematicians have a mental model consisting of indivisible objects, and sets of those objects (and other sets). However, some mathematicians called “set theorists” prefer to believe that there are no such things as “objects”—sets are the only thing we need to care about. Strangely enough, this is completely fine! Let’s take a peek at how it works.

Without any objects, find an infinite sequence of sets, giving a “definition” for each of the symbols  $0, 1, 2, 3, \dots$  (Hint:  $0$  should probably be “defined as” the empty set  $\emptyset$ . What other sets can you create without additional objects?)

7. (Russell’s paradox, ) When we defined set-builder notation, we always insisted that symbols appearing on the left (i.e.  $x$ ) always come from a bigger set that we specify (i.e.  $X$ ). However, historically, before the early 1900s, mathematicians were not so picky. They allowed themselves to write things like  $\{x \mid x \text{ is prime}\}$  without worrying about what larger set these primes belong to. (Today, we would write  $\{x \in \mathbb{N} \mid x \text{ is prime}\}$  or  $\{x \mid x \in \mathbb{N} \text{ and } x \text{ is prime}\}$ .)

In 1901, Bertrand Russell argued that the historical, less restrictive kind of set-builder notation was incorrect, because it leads to contradictions in mathematics. He considered “the set of sets that do not contain themselves”, i.e.

$$S = \{X \mid X \notin X\}.$$

What is wrong with this so-called “set”? (Hint: Is it true that  $S \in S$ ?)

## 2 Introduction to proofs

### 2.1 How to prove things

The language of mathematics is primarily used to communicate proofs. A proof is a way of convincing another person that your claim is true, using irrefutable arguments. In this first section, we'll give a basic template for you to begin proving things.

Suppose you were asked to prove:

“For all  $x \in \mathbb{R}$ , there exists  $y \in \mathbb{R}$  such that  $y > x$ .”

The quantifiers (“for all”, “there exists”) in the sentence provide a useful template for how you should prove it. From this sentence, the template goes:

- Let someone give me whatever  $x \in \mathbb{R}$  they like.
- I will say how to pick a  $y \in \mathbb{R}$  (maybe using  $x$ ).
- I will use my construction to explain why  $y > x$ .

Thus, we get the following proof.

**Example 2.1.** Prove that for all  $x \in \mathbb{R}$ , there exists  $y \in \mathbb{R}$  such that  $y > x$ . ┐

*Proof.* Let  $x \in \mathbb{R}$ . Pick  $y = x + 1$ . Then because  $x + 1 > x$ , we get  $y > x$ . □



In particular, it is standard practice to say how to create things, without explaining how you figured out what it was you had to create. In the above, we just said “set  $y = x + 1$ ” for no apparent reason, and that’s fine for the purpose of a proof, because the goal is just convince the reader that “there exists” is correct. An author who wants to communicate their motivations might write something like:

In order to get  $y > x$ , it suffices to take  $y = x + 1$ .

or even

In order to get  $y > x$ , it suffices to take  $y = x + a$  for any  $a > 0$ , for instance,  $y = x + 1$  suffices.

But this is not required for proofs, and many authors will choose to “pull things out of the hat” instead.

As a second example, suppose you were asked to prove, “there exists  $x \in \mathbb{R}$  such that  $x^2 - 2x - 5 = 0$ .” By default, a proof of this fact would *not* involve factoring, quadratic formula, completing the square, etc. as would be expected from the instruction “show your work.” Instead, the proof would look like the following.

**Example 2.2.** Prove that there exists  $x \in \mathbb{R}$  such that  $x^2 - 2x - 5 = 0$ . ┐

*Proof.* Pick  $x = 1 + \sqrt{6}$ . One verifies  $(1 + \sqrt{6})^2 - 2(1 + \sqrt{6}) - 5 = 0$ , as desired. □

Authors that are trying to teach their audience how to solve a problem (rather than just convincing their audience that the author is right) may choose to phrase their proof as follows, but this should be considered an advanced phrasing and not the default style of proof.

*Proof.* In what follows, each line is true if and only if the next line is true:

$$x^2 - 2x - 5 = 0$$

$$x^2 - 2x + 1 = 6$$

$$(x - 1)^2 = 6$$

Thus, it suffices to have  $x - 1 = \sqrt{6}$  or  $x - 1 = -\sqrt{6}$ . This is satisfied by taking  $x = 1 + \sqrt{6}$ .  $\square$

~~~

The next three kinds of statements we'll learn to prove are of the form "not A", "A and B", and "A implies B". All of these are pretty obvious, but they are worth stating.

- To prove "not A", negate the sentence by applying de Morgan's laws, then prove the resulting sentence.
- To prove "A and B", prove A, then start a new paragraph and prove B.
- To prove "A implies B", just assume that A is true, and use that information to prove B. In particular, there is no need to think about what happens if A is false.

**Example 2.3.** Prove that there is no smallest positive real number.  $\lrcorner$

*Proof.* First, let's rewrite this natural language sentence logically to make sense of it.

"It is not true that there exists  $x \in (0, \infty)$  such that for all  $y \in (0, \infty)$ ,  $x < y$ ."

Applying rules to remove the negation, we get:

"For all  $x \in (0, \infty)$ , there exists  $y \in (0, \infty)$  such that  $x \geq y$ ."

So to prove it, we just write:

Let  $x \in (0, \infty)$ . This means  $x \in \mathbb{R}$  and  $x > 0$ . Pick  $y = x/2$ .

- To prove  $y \in (0, \infty)$ : Multiply both sides of  $x \geq 0$  by  $1/2$  to get  $x/2 \geq 0$ , thus  $y \geq 0$ . Thus  $y \in (0, \infty)$ .
- To prove  $x \geq y$ : Add  $x/2$  to both sides of  $x/2 \geq 0$  to get  $x \geq x/2 = y$  as desired.  $\square$

This proof also illustrated the fact that when picking  $y$  to prove "there exists  $y \in Y$ ", you should also make sure to prove that your choice of  $y$  really belongs to  $Y$ , if this fact is not obvious.

~~~

The last kind of statement that we'll discuss are statements of the form "A or B". To do this, divide the proof into two cases depending on a statement C that you come up with. In one case, you assume that C is true and prove A. In the other case, you assume that C is false and prove B.

**Definition 2.4.** The absolute value of  $x \in \mathbb{R}$  is defined

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

**Example 2.5.** Prove that for all  $x \in \mathbb{R}$ , if  $|x| \geq 1$ , then  $x \leq -1$  or  $x \geq 1$ . ┘

*Proof.* Let  $x \in \mathbb{R}$ . Assume  $|x| \geq 1$ . Break into cases depending on whether or not  $x \geq 0$ .

- Suppose  $x \geq 0$ . By definition,  $|x| = x$ . Thus,  $x = |x| \geq 1$ .
- Suppose  $x < 0$ . By definition,  $|x| = -x$ . Thus,  $-x = |x| \geq 1$ . Thus  $x \leq -1$ . □

Note that sometimes, even when the thing you are trying to prove doesn't look like "A or B", it could still be helpful to think about breaking a problem into cases. That's especially the case when using definitions involving cases in the first place, like the absolute value definition above.

~~~

To summarize, we have the following table:

Statement type	How to prove it
for all $x \in X$ , A	"Someone gives me $x \in X$ ." Then prove A.
there exists $x \in X$ such that A	"I pick $x \in X$ to be ...." Then prove A.
A implies B	Add A to my knowledge, then prove B.
A and B	Prove A. Prove B.
A or B	Pick cases based on C. In one case, assume C and prove A. In the other case, assume [not C] and prove B.

### Practice

1. Is the following proof correct? If correct, explain. If not correct, say what is wrong and provide a corrected proof.

**Example 2.6.** Prove that for all  $a, b, c \in \mathbb{R}$ , if  $b^2 - 4ac \geq 0$ , then there exists  $x \in \mathbb{R}$  such that  $ax^2 + bx + c = 0$ . ┘

*Proof.* Let  $a, b, c \in \mathbb{R}$ . We complete the square. Each of the following lines follows from the previous line.

$$\begin{aligned}
 ax^2 + bx + c &= 0 \\
 x^2 + \frac{b}{a}x + \frac{c}{a} &= 0 \\
 \left(x + \frac{b}{2a}\right)^2 &= \left(\frac{b}{2a}\right)^2 - \frac{c}{a} \\
 x + \frac{b}{2a} &= \pm \sqrt{\frac{b^2 - 4ac}{4a^2}} \\
 x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}
 \end{aligned}$$

For this to be a real number, we need  $b^2 - 4ac \geq 0$ , as was to be shown. □

2. Determine if the following sentences are true or false. If true, prove it. If false, prove the negation.

(a) There are numbers  $c \in \mathbb{N}$  and  $N \in \mathbb{N}$  such that for all  $n \in \mathbb{N}$ , if  $n \geq N$ , then  $cn \geq 3n + 10$ .

(b) There are numbers  $c \in \mathbb{N}$  and  $N \in \mathbb{N}$  such that for all  $n \in \mathbb{N}$ , if  $n \geq N$ , then  $cn \geq n^2$ .

(This is *asymptotic growth*, an important concept in analysis and computer science!)

3. Prove that for all  $x, y \in \mathbb{R}$ , the expression

$$\frac{x + y + |x - y|}{2}$$

is either equal to  $x$  or  $y$ . (What is the common name for this expression?)

4. (a) Prove that for all  $x \in \mathbb{R}$ , we have  $x \leq |x|$ .  
 (b) Prove the triangle inequality: for all  $x, y \in \mathbb{R}$ ,

$$|x + y| \leq |x| + |y|.$$

5. ( ))) Determine if the following sentences are true or false. If true, prove it. If false, prove the negation. (You will need to use the previous problem.)

(a) For all  $\epsilon \in \mathbb{R}$ , if  $\epsilon > 0$ , there exists  $\delta \in \mathbb{R}$  such that  $\delta > 0$  and for all  $x, y \in \mathbb{R}$ , if  $x > 0$ ,  $y > 0$ , and  $|x - y| < \delta$ , then  $|\sqrt{x} - \sqrt{y}| < \epsilon$ .

(b) For all  $\epsilon \in \mathbb{R}$ , if  $\epsilon > 0$ , there exists  $\delta \in \mathbb{R}$  such that  $\delta > 0$  and for all  $x, y \in \mathbb{R}$ , if  $|x - y| < \delta$ , then  $|x^2 - y^2| < \epsilon$ .

(This is *uniform continuity*, an important concept in real analysis!)

## Extensions

These problems describe extra things to think about that might be interesting, but not fundamental for your future learning. They may be harder.

6. (Nonconstructive existence, ))) While typically, when asked to prove “there exists  $x$ ”, you should pick an  $x$  and show that it works, that is not the only way to prove “there exists  $x$ ”. When you prove this without specifying exactly how you can get  $x$ , it is called a *nonconstructive* proof.

Recall that rational number is  $a/b$  for some  $a, b \in \mathbb{Z}$ , and irrational numbers are those in  $\mathbb{R}$  that cannot be expressed as such.  $\sqrt{2}$  is irrational. (We will prove this in a few lessons.) Prove that there exists two irrational numbers  $x, y \in \mathbb{R}$  such that  $a^b$  is rational. (Hint: Think about  $(\sqrt{2})^{\sqrt{2}}$  and consider a proof by cases.)

## 2.2 How to use things

So far, we've been proving theorems and identities from scratch. But most of mathematics is about building on top of theorems that other people have already proven. Let's talk about how to use more complicated assumptions, theorems, and definitions.

In summary, when you *use* a statement, everything is the opposite of what you would do if you were trying to prove it. We have the following summary table. Read this table carefully, and make sure each row makes sense to you.

	When proving	When using
for all $x \in X$ , A	"Someone gives me $x \in X$ ." Then prove A.	"I pick $x \in X$ to be ...." Then add A to my knowledge.
there exists $x \in X$ such that A	"I pick $x \in X$ to be ...." Then prove A.	"Someone gives me $x \in X$ ." Then add A to my knowledge.
A implies B	Add A to my knowledge, then prove B.	Prove A, then add B to my knowledge.
A and B	Prove A. Prove B.	Add A to my knowledge. Add B to my knowledge.
A or B	Pick cases based on C. In one case, assume C and prove A. In the other case, assume [not C] and prove B.	Get cases. In one case, add A to my knowledge. In the other case, add B to my knowledge.

Let us practice using statements. The following is a true statement that we will use.

**Theorem 2.7.** For all  $x \in \mathbb{R}$ , if  $x \geq 0$ , there exists  $y \in \mathbb{R}$  such that  $y \geq 0$  and  $y^2 = x$ .  $\lrcorner$

(This theorem just says "positive square roots exist", i.e.  $y = \sqrt{x}$ . Real square roots don't exist for negative  $x$ ! This is not as obvious as you think, since we would have to first understand what real numbers really are before proving it.) To *use* this theorem, the template is:

- I will pick  $x \in \mathbb{R}$ .
- I will prove that  $x \geq 0$ .
- Let someone give me  $y \in \mathbb{R}$ .
- They guarantee to me that  $y \geq 0$  and  $y^2 = x$ .

**Example 2.8.** Prove that for all  $a \in \mathbb{R}$ , if  $a \geq 0$ , there exists  $b \in \mathbb{R}$  such that  $b \geq 0$  and  $b^4 = a$ .  $\lrcorner$

*Proof.* Let  $a \in \mathbb{R}$ . Assume  $a \geq 0$ .

- In order to pick  $b$ , I want to use Theorem 2.7. I pick  $x$  in the theorem to be  $a$ , and I know  $x = a \geq 0$ . The theorem gives me  $y \in \mathbb{R}$  such that  $y^2 = a$  and  $y \geq 0$ . Call this number  $c$  (i.e.  $c^2 = a$  and  $c \geq 0$ ).

- I will use Theorem 2.7 again. I pick  $x$  in the theorem to be  $c$ , and I know  $x = c \geq 0$ . The theorem gives me  $y \in \mathbb{R}$  such that  $y^2 = c$  and  $y \geq 0$ . This time, I will call this number  $b$  (i.e.  $b^2 = c$  and  $b \geq 0$ ), which is the number I was hoping to pick.

Then  $b^4 = c^2 = a$ , and  $b = d \geq 0$ , as desired.  $\square$

You might have noticed that the proof is already getting a bit wordy. In fact, most mathematicians do not write to this level of detail. A proof is really a social object: a method of communication between author and reader. Most mathematicians assume that the reader can fill in some of the boilerplate and reorder the logic by themselves. In that case, they might just write the following. You should only write like this if you are first comfortable writing out all the full details, and that is getting boring and tedious.

*Proof.* By applying Theorem 2.7 on  $a$ , there exists  $c \in \mathbb{R}$  such that  $c^2 = a$  and  $c \geq 0$ . Applying it again on  $c$ , we get  $b \in \mathbb{R}$  such that  $b^2 = c$  and  $b \geq 0$ . Thus,  $b^4 = c^2 = a$  and  $b \geq 0$ .  $\square$

Note that if you are trying to prove “A implies B” and the sentence A involves quantifiers, the proof template should be similar to considering it a “theorem”. We’ll see an example next.

~~~

The vast majority of proofs in mathematics rely on *definitions*. So far, we’ve relied on properties that you’ve already learned about  $\mathbb{R}$  and  $\mathbb{N}$  to write proofs. Now, and throughout the rest of your mathematical career, you’ll see new definitions to talk about new objects. Unlike definitions in English, which can be argued about and may change over time, mathematical definitions are hard laws that we agree upon.

**Definition 2.9.**

- A number  $n \in \mathbb{N}$  is even if there exists  $k \in \mathbb{N}$  such that  $n = 2k$ .
- A number  $n \in \mathbb{N}$  is odd if there exists  $k \in \mathbb{N}$  such that  $n = 2k + 1$ .  $\lrcorner$

**Example 2.10.** Prove that the sum of two odd numbers is even.  $\lrcorner$

*Proof.* Again, let’s rewrite this natural language sentence logically to make sense of it.

“For all  $n \in \mathbb{N}$  and  $m \in \mathbb{N}$ , if  $n$  is odd and  $m$  is odd, then  $n + m$  is even.”

So to prove it, we write:

Let  $n \in \mathbb{N}$  and  $m \in \mathbb{N}$ . Assume  $n$  and  $m$  are odd. We are trying to prove that  $n + m$  is even. By definition of even, this means we have to prove “there exists  $a \in \mathbb{N}$  such that  $n + m = 2a$ .”

By definition of odd, let someone give me  $k \in \mathbb{N}$  and  $\ell \in \mathbb{N}$  such that  $n = 2k + 1$  and  $m = 2\ell + 1$ . Pick  $a = k + \ell + 1$ . Then

$$\begin{aligned} n + m &= (2k + 1) + (2\ell + 1) \\ &= 2(k + \ell + 1) \\ &= 2a, \end{aligned}$$

as desired.  $\square$

Written more concisely, this proof would look like:

*Proof.* Let  $n = 2k + 1$  and  $m = 2\ell + 1$  for some  $k, \ell \in \mathbb{N}$ . Then,

$$\begin{aligned} n + m &= (2k + 1) + (2\ell + 1) \\ &= 2(k + \ell + 1), \end{aligned}$$

thus picking  $a = k + \ell + 1$  proves that  $n + m = 2a$ , and  $n + m$  is even.  $\square$

Here are a few more definitions that will be used in the exercises.

**Definition 2.11.** Recall that  $\mathbb{Z}$  denotes the integers  $\{\dots, -2, -1, 0, 1, 2, \dots\}$ .

- Given numbers  $a, b \in \mathbb{Z}$ , we write  $a \mid b$  (and say, “ $a$  divides  $b$ ”) if there exists  $k \in \mathbb{Z}$  such that  $b = ka$ .
- Given numbers  $a, b, n \in \mathbb{Z}$ , we say that  $a \equiv b \pmod{n}$  if  $n \mid a - b$ .  $\lrcorner$

For example,  $2 \equiv 37 \pmod{5}$  because  $5 \mid 37 - 2$ , because  $37 - 2 = 35$  and  $35 = 5k$  when  $k = 7$ .

### Practice

1. Prove that for all  $n \in \mathbb{N}$ , if  $n$  is odd, then  $n^2$  is odd.
2. Recall the theorem known as the zero product property:

**Theorem 2.12.** For all  $a, b \in \mathbb{R}$ , if  $ab = 0$ , then  $a = 0$  or  $b = 0$ .  $\lrcorner$

Use the zero product property to formally prove that for all  $x \in \mathbb{R}$ , if  $x^2 + x - 6 = 0$ , then  $x = -3$  or  $x = 2$ .

3. Remember that in this class,  $\mathbb{N}$  includes 0. Is the following an equivalent definition of odd?


“A number  $n \in \mathbb{N}$  is odd if there exists  $m \in \mathbb{N}$  such that  $n = 2m - 1$ .”

If not, give an example of a number that odd in one definition but not the other. If so, prove that a number  $n \in \mathbb{N}$  satisfies this definition of odd if and only if it satisfies the definition given in the lesson.

4. Verify (i.e. prove) the following basic properties of  $\equiv \pmod{k}$ . These properties allow us to do *modular arithmetic*.
  - (a) For all  $a, b, c, d, n \in \mathbb{Z}$ , if  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$ , then  $a + c \equiv b + d \pmod{n}$ . (Therefore we can add as if  $\equiv$  was a normal  $=$  sign.) Say quickly why this also means we can subtract as if  $\equiv$  was a normal  $=$  sign.
  - (b) For all  $a, b, c, d, n \in \mathbb{Z}$ , if  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$ , then  $ac \equiv bd \pmod{n}$ . (Therefore we can multiply as if  $\equiv$  was a normal  $=$  sign. We also automatically get that  $a \equiv b \pmod{n}$  implies  $a^k \equiv b^k \pmod{n}$ , by applying this fact with  $c = a$  and  $d = b$  many times.)
  - (c) Prove that the following is false: For all  $a, b, c, d, n \in \mathbb{Z}$ , if  $ac \equiv bd \pmod{n}$  and  $c \equiv d \pmod{n}$ , then  $a \equiv b \pmod{n}$ . (Therefore, we generally cannot do division in modular arithmetic.)
5. Prove that if  $n$  is even, then  $3 \mid 2^n - 1$ .

## Extensions

These problems describe extra things to think about that might be interesting, but not fundamental for your future learning. They may be harder.

6. (Reasoning from axioms, ) For most of this section, we focused on reasoning from theorems, assumptions, and definitions. There is a special kind of definition, which lists several *axioms* (basic properties) for the object.

Here is one example. A *group* is a set  $G$  with an operation, usually denoted  $\cdot$  (though it might be different from the multiplication that you're familiar with), satisfying a set of axioms. Like normal multiplication, we often write  $ab$  instead of  $a \cdot b$  as notation. The axioms of a *group* are:

- (closure) For all  $a, b \in G$ ,  $ab \in G$ .
- (associativity) For all  $a, b, c \in G$ ,  $a(bc) = (ab)c$ .
- (identity) There exists  $e \in G$  such that for all  $a \in G$ ,  $ea = ae = a$ . (The element  $e$  is called the identity.)
- (inverse) For all  $a \in G$ , there exists an element  $b$  such that  $ab = ba = e$ . (We typically write  $a^{-1}$  as notation for this  $b$ .)

- (a) Are the following sets with operations groups?

- The set of integers  $\mathbb{Z}$  with the standard  $+$  operation.
- The set of strings of English letters (like “yes”, “ilny”, “”) with the concatenation operation  $++$  (in which “yes”  $++$  “ilny” = “yesilny”).
- The set of rationals  $\mathbb{Q}$  with the standard  $\cdot$  operation.
- The following set of 8 actions on the plane (rotations counterclockwise):
  - do nothing
  - rotate  $90^\circ$
  - rotate  $180^\circ$
  - rotate  $270^\circ$
  - flip across  $x$ -axis
  - flip across  $x$ -axis then rotate  $90^\circ$
  - flip across  $x$ -axis then rotate  $180^\circ$
  - flip across  $x$ -axis then rotate  $270^\circ$

The operation is the word “then”.

- (b) Prove the following facts about all groups  $(G, \cdot)$  using the axioms.

- The identity is unique (so we are justified in calling it *the* identity). In other words, for all  $e_1, e_2 \in G$ , if for all  $a \in G$ ,  $e_1a = ae_1 = a$  and  $e_2a = ae_2 = a$ , then  $e_1 = e_2$ .
- Inverses are unique (so the notation  $a^{-1}$  is not ambiguous). In other words, for all  $a, b_1, b_2 \in G$ , if  $ab_1 = b_1a = e$  and  $ab_2 = b_2a = e$ , then  $b_1 = b_2$ .
- The shoes and socks theorem: you can put on your socks and then your shoes, but to remove them, your shoes come off first, then your socks. In other words, for all  $a, b \in G$ ,  $(ab)^{-1} = b^{-1}a^{-1}$ .
- Give an example of a group  $G$  and two elements  $a, b \in G$  such that  $(ab)^{-1} \neq a^{-1}b^{-1}$ . (Hint: one of the above examples works.)

### 3 Advanced proof techniques

While the basic proof techniques from the previous section work for a very large number of statements, some statements require more advanced techniques.

#### 3.1 Induction

Suppose you were asked to prove the following theorem.

**Theorem 3.1.** *All natural numbers are even or odd.* ┘

First, why is this not obvious? We defined “even” to mean  $2k$ , and “odd” to mean  $2k + 1$ . Nothing about the definition directly implies that these two cases are exhaustive. That means we need proof.

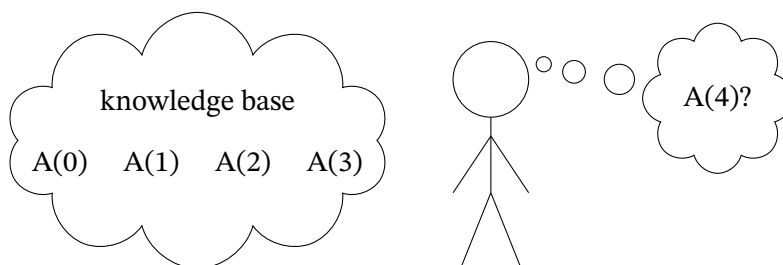
Previously, we learned that the standard way to prove “A or B” is to take cases based on something, then in one case prove A, and in the other case prove B. But unlike the examples with absolute value, there is nothing particularly obvious to take cases on.

What’s missing is that the truth of this sentence depends crucially on what the set of natural numbers  $\mathbb{N}$  actually is. For example, it’s certainly false that all real numbers are either even or odd. Thus, to prove the theorem, we *must* use some property of  $\mathbb{N}$  that is false for  $\mathbb{R}$ . We cannot just use logic and arithmetic—those things work for  $\mathbb{R}$  too!

The key property of  $\mathbb{N}$  is known as the *principle of induction*, as follows:

**Theorem 3.2** (Principle of induction). *Suppose  $A(n)$  is a sentence that depends on  $n$ , and you want to prove the sentence “for all  $n \in \mathbb{N}$ ,  $A(n)$  is true.” Then it is enough to prove:*

- *A base case, that  $A(0)$  is true, and*
- *An inductive step, that assuming you already know that  $A(0), A(1), A(2), \dots, A(n-1)$  are true,  $A(n)$  is also true.* ┘



In other words,  $\mathbb{N}$  has the property that you can prove sentences about  $\mathbb{N}$  one number at a time, relying on previous numbers to help you reason about future numbers. Let’s see an example of how this works.

**Example 3.3.** Prove that all natural numbers are either even or odd. ┘

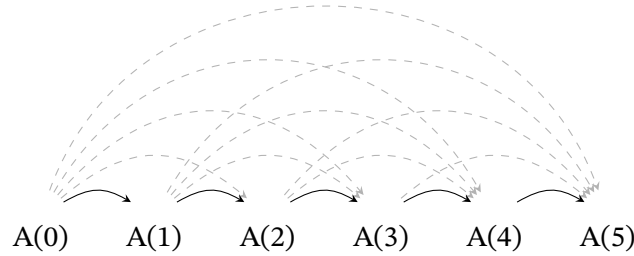
*Proof.* We will prove the theorem using induction. Let  $n \in \mathbb{N}$ .

- **Base case** ( $n = 0$ ): The number 0 is even, as  $0 = 2k$  where  $k = 0$ . Thus, 0 is even or odd.
- **Inductive step:** We want to show that  $n$  is either even or odd, assuming that everything less than  $n$  is already known to be even or odd. In particular, we know that  $n - 1$  is even or odd. Take cases.

- Suppose  $n - 1$  is even. That means  $n - 1 = 2k$  for some  $k \in \mathbb{N}$ . Then,  $n = 2k + 1$ , so  $n$  is odd. Thus  $n$  is even or odd.
- Suppose  $n - 1$  is odd. That means  $n - 1 = 2k + 1$  for some  $k \in \mathbb{N}$ . Let  $\ell = k + 1$ . Then  $n = 2k + 2 = 2\ell$ , so  $n$  is even. Thus  $n$  is even or odd.  $\square$

~~~

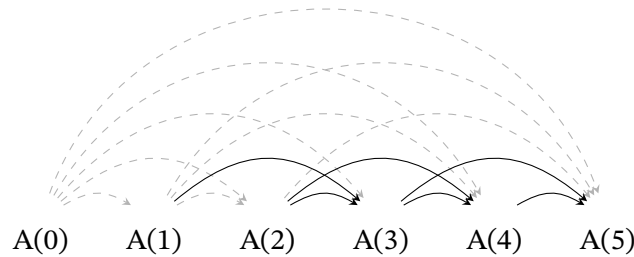
Note that we actually didn't use the full power of induction in the above example, we only used  $A(n - 1)$ . This is rather typical—it's rare to have an induction argument where you actually need to use all of  $A(0), A(1), \dots, A(n - 1)$  to prove  $A(n)$ . In other words, if we drew a picture that shows which statements were used to prove which other statements, our proof above only used the black edges below, but we are actually also allowed to use all of the gray dashed edges.



For another example, take the following problem.

**Example 3.4.** Define the Fibonacci numbers to be  $F_1 = 1, F_2 = 1$ , and  $F_n = F_{n-1} + F_{n-2}$  for all  $n \in \mathbb{N}$  with  $n \geq 3$ . Prove that for all  $n \in \mathbb{N}$ , if  $n \geq 1$ , then  $F_n < 2^n$ .  $\lrcorner$

Based on the problem statement, we'll choose to use the edges depicted in the following picture. In other words we will prove two base cases:  $A(1)$  and  $A(2)$ , then primarily rely on  $A(n - 2)$  and  $A(n - 1)$  to prove  $A(n)$ , just like the definition of Fibonacci numbers.



*Proof.* By induction.

- **Base cases** ( $n = 1$  and  $n = 2$ ): Certainly  $F_1 = 1 < 2^1 = 2$ , and  $F_2 = 1 < 2^2 = 4$ .
- **Inductive step:** Since we are working step by step, we already know that  $F_1 < 2^1$ ,  $F_2 < 2^2$ ,  $\dots$ , and  $F_{n-1} < 2^{n-1}$ , and we want to prove  $F_n < 2^n$ . But as we hinted earlier, we're not going to use all of these. We will just use

$$F_{n-1} < 2^{n-1} \quad \text{and} \quad F_{n-2} < 2^{n-2}.$$

Thus, we get that

$$\begin{aligned}
 F_n &= F_{n-1} + F_{n-2} \\
 &< 2^{n-1} + 2^{n-2} \\
 &= \frac{3}{2} \cdot 2^{n-1} \\
 &< 2^n,
 \end{aligned}$$

as was to be shown.  $\square$

Here is one more induction using a different structure. In this example, we really use more of our knowledge base  $A(0), A(1), \dots, A(n-1)$ , not just the last few cases.

**Definition 3.5.** A number  $n \in \mathbb{N}$  is called prime if it cannot be written as  $ab$  for some  $a, b \in \mathbb{N}$ , where  $a < n$  and  $b < n$ .  $\lrcorner$

**Theorem 3.6** (Fundamental Theorem of Arithmetic). *Every  $n \in \mathbb{N}$  with  $n \geq 2$  can be written as the product of prime numbers. In other words, prime factorizations exist.*  $\lrcorner$

*Proof.* We will prove the theorem using induction.

- **Base case** ( $n = 2$ ): 2 itself is prime, so it is certainly a product of primes (a single prime).
- **Inductive step:** We know that the numbers  $2, 3, 4, \dots, n-1$  can be written as a product of primes, and our goal is to show how  $n$  can be written as a product of primes. Take two cases.
  - If  $n$  is prime, then just like the base case, it is a product of primes.
  - If  $n$  is not prime, then by definition of prime,  $n = ab$  for some  $a, b \in \mathbb{N}$  where  $a < n$  and  $b < n$ . So  $a$  and  $b$  can be written as a product of primes, and thus so can  $n = ab$ .  $\square$

~~~

In some more difficult instances of induction, you will need to prove something different than what you are actually asked to prove. That sounds strange, but consider the following.

**Example 3.7.** Prove that for all  $n \in \mathbb{N}$ , if  $n \geq 1$ , then

$$1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2} < 2. \quad \lrcorner$$

*Proof.* Suppose we tried to prove this statement directly by induction. We would write something like the following.

- **Base case** ( $n = 1$ ): Certainly  $1 < 2$ .
- **Inductive step:** We want to show that

$$1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2} < 2,$$

and our knowledge base consists of

$$1 < 2, \quad 1 + \frac{1}{4} < 2, \quad \dots, \quad 1 + \frac{1}{4} + \dots + \frac{1}{(n-1)^2} < 2.$$

But none of these are helpful! I want to add  $1/n^2$  to the left hand side of the last inequality, but adding  $1/n^2$  to the right hand side makes the right hand side certainly too big.

Instead, the solution is very creative: instead of proving the original inequality, we will prove a *stronger* inequality. It might be surprising that it is easier to prove something stronger than something weaker. But really, this shouldn't be surprising at all—the stronger, more powerful inequalities are also going into your knowledge base for you to use! We will show that for all  $n \in \mathbb{N}$ , if  $n \geq 1$ , then

$$1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2} \leq 2 - \frac{1}{n}.$$

- **Base case** ( $n = 1$ ): Certainly  $1 \leq 2 - 1/1 = 1$ .
- **Inductive step**: From our knowledge base, we have the claim for  $n - 1$ , that is,

$$1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{(n-1)^2} \leq 2 - \frac{1}{n-1}.$$

Now if we add  $1/n^2$  to both sides, we get

$$\begin{aligned} 1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2} &\leq 2 - \frac{1}{n-1} + \frac{1}{n^2} \\ &< 2 - \frac{1}{n-1} + \frac{1}{n(n-1)} \\ &= 2 - \frac{n}{n(n-1)} + \frac{1}{n(n-1)} \\ &= 2 - \frac{n-1}{n(n-1)} \\ &= 2 - \frac{1}{n}, \end{aligned}$$

as desired.

Now, we can get the original intended conclusion of

$$1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2} \leq 2 - \frac{1}{n} < 2. \quad \square$$

Figuring out the right way to strengthen the claim is often a very difficult part of an induction proof: there is no clear-cut method. But if you try lots of examples, and can hypothesize that a stronger version of the claim is actually true, it is almost always helpful in induction to try to prove a stronger claim than a weaker claim. Remember—a stronger claim gives you a stronger knowledge base to work with!

## Practice

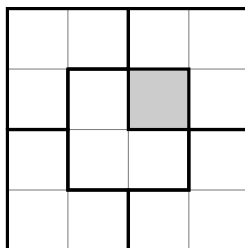
1. Read the following attempted solution using induction.

**Example 3.8.** On a certain island, there are  $n$  cities,  $n \geq 2$ , some of which are connected by (two-way) roads. If each city is connected by a road to at least one other city, is it true that you can travel from any city to any other city along the roads? J

*Solution.* Yes, it is true. We proceed by induction on  $n$ .

- **Base case** ( $n = 2$ ): If there are two cities, and each city is connected by a road to at least one other city, then the two cities are connected to each other, and you can travel from any city to any other city.
- **Inductive step:** From our knowledge base, we know that the claim is true when there are  $n - 1$  cities. To prove that it's also true for  $n$  cities, we add another city to this island. This new city is connected by a road to at least one of the old cities. From the claim on  $n - 1$  cities, we know that once we get there, we can go to any other city. Thus you can travel from the new city to any other city, as well as between any two of the old cities, as claimed.  $\square$

- (a) Show that the answer is actually false by providing a counterexample to the claim.
  - (b) State exactly which part of the argument went wrong.
2. In Problem 3.1.4(b), we said that for all  $a, b, n \in \mathbb{N}$ , if  $a \equiv b \pmod{n}$ , then for all  $k \in \mathbb{N}$ ,  $a^k \equiv b^k \pmod{n}$ , by “applying a fact many times.” Formalize that argument using induction.
  3. We proved that all natural numbers are even or odd. Can we conclude from this fact that “not even” means the same thing as “odd”, and “not odd” means the same thing as “even”? If so, explain. If not, prove this fact.
  4. Prove by induction that for all  $n \in \mathbb{N}$ , if  $n^2$  is even, then  $n$  is even. (You may use as a fact that sums and differences of even numbers is even—these proofs look nearly identical to “odd + odd = even” that we did last section.)  
Note that induction is not the best way to prove this fact. It is overly complicated. We will discuss an easier way to prove this fact in the next section.
  5. A  $2^n \times 2^n$  grid has one of the center 4 squares removed. Prove that for all  $n \in \mathbb{N}$ , you can always cover the rest of the grid using L-shaped trominoes. An example for is shown below.



## Extensions

These problems describe extra things to think about that might be interesting, but not fundamental for your future learning. They may be harder.

6. (Programming is induction,  $\P\P$ ) When programming, it is important that your code is correct. That means on every possible input, your output matches the desired output. Programmers in real life find verifying correctness to be too tedious and not worth the effort, so they'll just try 10 inputs and call it a day (that's why published code has bugs) but as mathematicians we can formally prove that the code works on all inputs, and the key is almost always induction!

Let  $A = [a_0, a_1, a_2, \dots, a_{n-1}]$  be an array of length  $n$ . (An array is just a finite list of elements, and in the spirit of programming we start at 0.) Consider the following code, which I've written in a way so that hopefully, you can translate to your favorite programming language easily, or even if you don't know programming, you can understand what it means.

- Set  $m = -\infty$  and  $i = 0$ .
- Run the following block  $n$  times.
  - If  $a_i > m$ , set  $m = a_i$ .
  - Set  $i = i + 1$  (i.e. increment  $i$ ).
- Output  $m$ .

Prove that the program outputs the largest number in  $A$ , or  $-\infty$  if  $A$  is empty. (Hint: find a statement that is true every iteration, and prove that with induction.)

7. (Division theorem,  $\P\P$ ) In elementary school, you learned how to divide natural numbers, leaving a quotient and remainder. In most math now, division usually means that we are okay with ending up with fractions, but for this question, we'll consider the old quotient-and-remainder meaning of division instead.

Prove that for all  $a, b \in \mathbb{N}$ , if  $b > 0$ , there exist unique  $q, r \in \mathbb{N}$  such that  $a = bq + r$  and  $0 \leq r < b$ . The number  $q$  is called the quotient and  $r$  is called the remainder. "Exists unique" means that you should prove two things:

- (a) For all  $a, b \in \mathbb{N}$ , if  $b > 0$ , there exist  $q, r \in \mathbb{N}$  such that  $a = bq + r$  and  $0 \leq r < b$ .
- (b) For all  $a, b, q_1, q_2, r_1, r_2 \in \mathbb{N}$ , if  $a = bq_1 + r_1$ ,  $a = bq_2 + r_2$ ,  $0 \leq r_1 < b$ , and  $0 \leq r_2 < b$ , then  $q_1 = q_2$  and  $r_1 = r_2$ .

The fact that you can do division in  $\mathbb{N}$  sounds trivial until you consider what other systems allow or don't allow division.

- (c)  $\mathbb{Q}[x]$  is the set of polynomials with coefficients in  $\mathbb{Q}$ , such as  $x^3 + 2x + 1/2 = 0$ . Formally,

$$\mathbb{Q}[x] = \{a_n x^n + \dots + a_2 x^2 + a_1 x + a_0 \mid a_n, \dots, a_0 \in \mathbb{Q} \text{ and } n \in \mathbb{N}\}.$$

Sketch how to modify the above argument to show the division theorem for  $\mathbb{Q}[x]$ . That is, for all  $a(x), b(x) \in \mathbb{Q}[x]$ , there exist unique  $q(x), r(x) \in \mathbb{Q}[x]$  such that  $a(x) = b(x)q(x) + r(x)$  and  $0 \leq \deg(r) < \deg(b)$ , where  $\deg$  denotes the degree of the polynomial (the exponent of the largest term).

- (d) Show that the same statement for  $\mathbb{Z}[x]$  is false.

### 3.2 Contrapositive and contradiction

Earlier, we proved that for all  $n \in \mathbb{N}$ , if  $n$  is odd, then  $n^2$  is odd. It's very similar to show that if  $n$  is even, then  $n^2$  is even. What about the opposite, that if  $n^2$  is even, then  $n$  is even? In Problem 3.1.4, you proved (or will prove) using induction that this is true, but the induction proof is rather convoluted and long. A much easier way is to use the *contrapositive*.

The contrapositive of “A implies B” is the sentence “[not B] implies [not A]”. We can verify that these are equivalent using a truth table.

| A | B | A implies B | A | B | not B | not A | [not B] implies [not A] |
|---|---|-------------|---|---|-------|-------|-------------------------|
| 0 | 0 | 1           | 0 | 0 | 1     | 1     | 1                       |
| 0 | 1 | 1           | 0 | 1 | 0     | 1     | 1                       |
| 1 | 0 | 0           | 1 | 0 | 1     | 0     | 0                       |
| 1 | 1 | 1           | 1 | 1 | 0     | 0     | 1                       |

At the same time, think about a few examples to make sure this makes intuitive sense to you. For instance, “if I go swimming, I will get wet” means the same thing as “if I do not get wet, I did not go swimming.”



The contrapositive is not the same as the *converse*. The converse of “A implies B” is “B implies A”. For example, the converse of “if I go swimming, I will get wet” is “if I got wet, then I went swimming.” That’s not true—maybe it was just raining heavily.

Applied the contrapositive to this problem about even squares, we get the following proof.

**Example 3.9.** Prove that for all  $n \in \mathbb{N}$ , if  $n^2$  is even, then  $n$  is even. ┘

*Proof.* We prove by contrapositive. The statement is equivalent to

For all  $n \in \mathbb{N}$ , if  $n$  is not even, then  $n^2$  is not even.

In Problem 3.1.3, you proved (or will prove that) a number is not even if and only if it is odd, and not odd if and only if it is even. Thus, this is equivalent to

For all  $n \in \mathbb{N}$ , if  $n$  is odd, then  $n^2$  is odd.

We proved this in Problem 2.2.1. □

~~~

Another spiritually similar technique is called *proof by contradiction*. To do a proof by contradiction, if your goal is to prove A, instead prove “[not A] implies false”. “False” means any statement that is clearly not true, for example  $0 = 1$  or “C and [not C]” for some sentence C.

**Example 3.10.** Prove that for all  $n, m \in \mathbb{N}$ , if  $n \geq 2$  and  $n \mid m$ , then  $n \nmid m + 1$ . (The symbol  $\nmid$  means “not divisible by”). ┘

*Proof.* We prove by contradiction. The negation of the sentence is, “There exists  $n, m \in \mathbb{N}$  such that  $n \geq 2$ ,  $n \mid m$ , and  $n \mid m + 1$ ”. By definition, this means there exists  $k, \ell \in \mathbb{N}$  such that  $m = nk$  and  $m + 1 = n\ell$ . Subtracting, we find that  $1 = n(k - \ell)$ . Take two cases.

- Case 1:  $k - \ell = 0$ . Then  $1 = 0$ , contradiction.
- Case 2:  $k - \ell \geq 1$ . Then  $1 \geq 2(k - \ell) \geq 2$ , contradiction.  $\square$

Proof by contradiction is often difficult, because you will need some creativity to figure out how to reach an absurd conclusion. The basic proof templates that we learned before no longer really apply.

~~~

Proof by contradiction is useful because it gives you more knowledge to work with. In other words, it can be hard to prove a sentence  $A$ , when you don't know very much about the elements in the sentence. But when you use proof by contradiction, you gain knowledge by adding  $[\text{not } A]$  to your knowledge base.

Also note that proof by contradiction is extremely common when you asked to prove that something is false. For instance, in the previous problem, you were asked to prove  $n \nmid m + 1$ . If you actually tried to negate the definition of “divides”, you would get, “for all  $k \in \mathbb{N}$ ,  $m + 1 \neq nk$ .” This feels very hard to prove! By using proof by contradiction, we not only gain knowledge to use in our proof, but we can also avoid negating the complicated definition.

Here is one more classic example. In this case, we know what it means for a number to be rational:  $a/b$  for some integers  $a$  and  $b$ . The definition of “irrational” is simply “not rational”, but again, the negated definition is hard to work with. Instead, use proof by contradiction!

**Example 3.11.** Prove that  $\sqrt{2}$  is irrational. (Assume for free that fractions of integers can be expressed in “lowest terms”, so that the numerator and denominator share no common factors apart from 1.)  $\square$

*Proof.* We prove by contradiction. Assume that  $\sqrt{2}$  is rational. That means that there exists  $a, b \in \mathbb{Z}$  such that  $\sqrt{2} = a/b$  and  $a$  and  $b$  share no common factors apart from 1. From this equation, we get

$$\begin{aligned}\sqrt{2} &= \frac{a}{b} \\ 2 &= \frac{a^2}{b^2} \\ 2b^2 &= a^2\end{aligned}$$

Because  $a^2 = 2k$  where  $k = b^2$ ,  $a^2$  is even. By Example 3.9, this means  $a$  is even. Thus, there exists  $\ell \in \mathbb{N}$  such that  $a = 2\ell$ . Thus,

$$\begin{aligned}2b^2 &= (2\ell)^2 \\ 2b^2 &= 4\ell^2 \\ b^2 &= 2\ell^2\end{aligned}$$

For the same reasons, now  $b$  is even. This is a contradiction, because  $a$  and  $b$  share no common factors apart from 1.  $\square$

~~~

Lastly, to comment on the difference between contrapositive and contradiction, one can view each as a special case of the other, so it is really just a matter of perspective. In one way, every proof by contrapositive is a proof by contradiction: “Suppose A implies B is false, so A and [not B]. Then, here is my proof by contrapositive that [not B] implies [not A]. Thus, I know A and [not A], contradiction.” Likewise, every proof by contradiction is also a proof by contrapositive: “To prove A, it is the same as proving true implies A. Then my proof by contradiction that [not A] implies false is exactly the contrapositive of true implies A.” However, they are still morally different things, so make sure to use the right word for the argument that you are making.

## Practice

1. Prove that for all  $x, y \in \mathbb{N}$ , if  $xy$  is odd, then  $x$  is odd and  $y$  is odd.
2. Prove that  $\log_{10}(2)$  is irrational. (You may use for free that prime factorizations are unique, i.e. two products of prime numbers are equal if and only if they are literally multiplying the same list of numbers, possibly in a different order.)
3. Prove that there are infinitely many prime numbers. (Hint: use the result of Example 3.10.)
4. A set is called *countably infinite* if you can write an infinite list of its elements in such a way that starting from the beginning, you will reach every element in finite time. For example,  $\{0, 1, 2, 3, \dots\}$  is countably infinite, but if you tried to show that  $\mathbb{Z}$  is countably infinite by listing elements  $\{0, 1, 2, 3, \dots, -1, -2, -3, -4, \dots\}$ , this does not work, because you will not reach  $-1$  in finite time according to this list.
  - (a) (not a contradiction proof) Show that even still,  $\mathbb{Z}$  is countable.
  - (b) Show that the closed interval  $[0, 1]$  is not countable (and hence neither is  $\mathbb{R}$ ). (Hint: consider the table below.)


		1	2	3	4	5	6	7	
1	0.	1	7	8	3	0	2	6	...
2	0.	2	4	1	5	1	5	5	...
3	0.	6	8	9	9	3	0	5	...
4	0.	7	9	9	6	6	4	5	...
5	0.	8	8	1	3	1	8	8	...
6	0.	9	0	9	5	4	7	7	...
7	0.	3	6	2	9	2	6	8	...
	:	:	:	:	:	:	:	:	...

## Extensions

These problems describe extra things to think about that might be interesting, but not fundamental for your future learning. They may be harder.

5. (Uncomputable functions, 🐉🐉🐉) A computer program is a text file of instructions for the computer. When you *run* the program, it takes an input and then either produces an output or gets stuck in an infinite loop. For simplicity, imagine that

the input and output are always be encoded as binary strings (like 00101110101). Let  $B$  denote the set of binary strings. Thus, the program can be described as computing a function  $f : B \rightarrow B \cup \{\perp\}$ , where  $\perp$  is a special value indicating that the program got stuck in an infinite loop.

- (a) Prove that there are a countable number of computer programs.
  - (b) Prove that there are an uncountable number of functions  $f : B \rightarrow B \cup \{\perp\}$ , using an argument similar to Problem 3.2.4. (Thus, most functions are not computable!)
6. (Completeness of  $\mathbb{R}$ , ) The most important feature of  $\mathbb{R}$  that distinguishes  $\mathbb{R}$  from  $\mathbb{Q}$  is called the *completeness axiom* or *least upper bound property*.

**Definition 3.12.** We say that  $m \in \mathbb{R}$  is an *upper bound* on a subset  $S \subseteq \mathbb{R}$  if for all  $x \in S$ , we have  $x \leq m$ . We say that  $m$  is a *least upper bound* on  $S$  if it is an upper bound, and for all  $M \in \mathbb{R}$ , if  $M$  is also an upper bound on  $S$ , then  $m \leq M$ . ┘

- (a) Prove that 1 is the least upper bound of  $(0, 1]$ .
- (b) Prove that 1 is the least upper bound of  $(0, 1)$ .
- (c) Prove the Archimedean property: that for all  $x, y \in \mathbb{R}$ , if  $x > 0$ , then there exists  $n \in \mathbb{N}$  such that  $nx > y$ . (Note: you cannot use things like floor/ceiling functions for this problem, if you are familiar with them, because the definition of these depends on the Archimedean property being true.)

The least upper bound property is the following fact (or axiom, depending on exactly how you formalize the real numbers).

**Theorem 3.13.** For all  $S \subseteq \mathbb{R}$ , if  $S$  has an upper bound, then  $S$  has a least upper bound. ┘

- (d) Prove that  $\sqrt{2}$  exists: there exists  $x \in [0, \infty)$  such that  $x^2 = 2$ . (Hint: Consider  $S = \{y \in \mathbb{R} \mid y^2 \leq 2\}$ .)

## 4 Functions

You might have seen functions informally before, in courses such as Algebra 1 in school. There, you likely learned that a function is like a machine that takes in input and produces output. Usually, you concerned yourself with functions that take in a real number  $x \in \mathbb{R}$  as input and produced an output  $f(x) \in \mathbb{R}$  as output. The *domain* was the set of all possible inputs that make sense for the function, and the *range* was the set of all possible outputs. For example, you considered

$$f(x) = \sqrt{x + 5}$$

to be a function with domain  $\{x \in \mathbb{R} \mid x \geq -5\}$  and range  $\{y \in \mathbb{R} \mid y \geq 0\}$ .

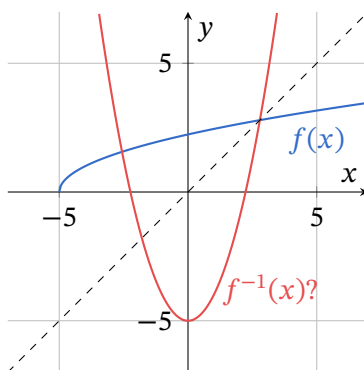
This view is slightly outdated by modern standards. Here is the problem: what is the *inverse* of this function? In Algebra 1, the definition says that the inverse of  $f$  is the function that undoes  $f$ , i.e. if  $f(1) = 2$ , then  $f^{-1}(2) = 1$ . To find do this in general, we swap the roles of  $x$  and  $f(x)$ . In other words,

$$x = \sqrt{f^{-1}(x) + 5},$$

which can be rearranged into

$$f^{-1}(x) = x^2 - 5.$$

What is the domain and range of this function? By swapping the roles of  $x$  and  $f(x)$ , the domain and range should also swap. But if you blindly apply the Algebra 1 definitions,  $f^{-1}$  certainly has range  $\{y \in \mathbb{R} \mid y \geq -5\}$ , matching the domain of  $f$ , but it has domain all of  $\mathbb{R}$ , which is not the same as the range of  $f$ .



The problem is illustrated in the graphs of  $y = f(x)$  and  $y = f^{-1}(x)$  above. By “swapping the roles of  $x$  and  $f(x)$ ”, we should get a function that is reflected over the line  $y = x$ , showed dashed above. Thus, we should really be cutting off  $f^{-1}(x)$  to only be defined for  $x \geq 0$ , even though the formula  $x^2 - 5$  makes sense for all  $x \in \mathbb{R}$ .

The modern definition of a function resolves this problem by requiring you to specify the domain when defining what the function is. In other words, today, we would say that

$$f(x) = \sqrt{x + 5}$$

is *not* a complete definition of a function. Instead, to define  $f$ , we would need to say something like:

$$f : [-5, \infty) \rightarrow \mathbb{R}, \quad f(x) = \sqrt{x + 5}.$$

The set  $\{x \in \mathbb{R} \mid x \geq -5\}$  is the domain by definition, and  $\mathbb{R}$  is the *codomain*, the ambient space where  $f$  maps into, which may be bigger than the range.

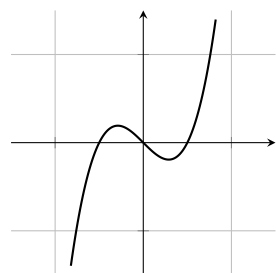
**Definition 4.1.** A function contains 3 pieces of information: a domain  $X$ , a codomain  $Y$ , and a rule mapping every element of  $X$  to some element of  $Y$ .

(More formally, a function is a tuple  $(X, Y, F)$  where  $X$  and  $Y$  are sets, and  $F \subseteq X \times Y$  is a set of pairs in which for all  $x \in X$ , there is exactly one  $(a, b) \in F$  with  $a = x$ . We write  $f(x) = y$  as shorthand for  $(x, y) \in F$ .)

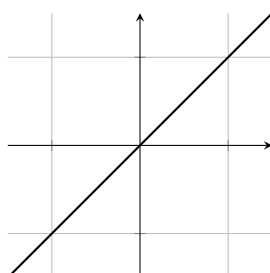
**Definition 4.2.** A function  $f : X \rightarrow Y$  is called

$\left. \begin{array}{l} \text{surjective} \\ \text{bijective} \\ \text{injective} \end{array} \right\}$	$\text{if for all } y \in Y, \text{ there exists}$	$\left\{ \begin{array}{l} \text{at least one} \\ \text{exactly one} \\ \text{at most one} \end{array} \right\}$	$x \in X \text{ such that } y = f(x).$
--	--	---	--

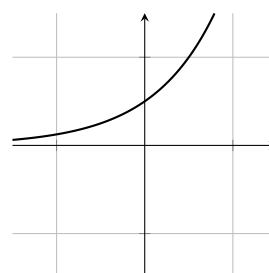
**Example 4.3.** Consider the following examples, all with signature  $f : \mathbb{R} \rightarrow \mathbb{R}$ .



$f(x) = x^3 - x$   
surjective, not injective



$f(x) = x$   
bijective



$f(x) = 2^x$   
injective, not surjective

The function  $f(x) = x^3 - x$  is surjective, because every point along the  $y$ -axis is reached by some input  $x$ . It is not injective because in the middle, there are some  $y$ -values that are reached by three different values of  $x$ .

The function  $f(x) = x$  is both surjective and injective, and thus bijective, because clearly there is exactly one  $x$  that produces each  $y$ .

The function  $f(x) = 2^x$  is injective, because every  $y$ -value is certainly achieved by no more than one  $x$ . However, it is not surjective, at least when defined with signature  $f : \mathbb{R} \rightarrow \mathbb{R}$ , because not every point in the codomain is reached. In particular,  $(-\infty, 0]$  is not reached.

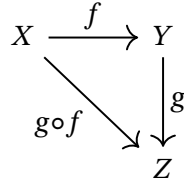
**Definition 4.4.** The inverse of a bijective function  $f : X \rightarrow Y$  is denoted  $f^{-1} : Y \rightarrow X$ , and we define  $f^{-1}(y)$  to be the unique  $x$  such that  $f(x) = y$ .

**Example 4.5.** The inverse of  $f : \mathbb{R} \rightarrow \mathbb{R}$ ,  $f(x) = x + 1$  is the function  $f^{-1} : \mathbb{R} \rightarrow \mathbb{R}$ ,  $f^{-1}(x) = x - 1$ . In other words,  $+1$  and  $-1$  are inverses because they undo each other.

~~~

**Definition 4.6.** Given  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$ , their composition is the function  $g \circ f : X \rightarrow Z$ , given by  $(g \circ f)(x) = g(f(x))$ . People often also write  $f^n$  for the function  $f \circ f \circ \dots \circ f$  ( $n$  times).<sup>1</sup>

<sup>1</sup>Except for trigonometric functions and log, for which the standard meaning of  $\sin^2(x)$  is  $(\sin(x))^2$ , not  $\sin(\sin(x))$ , etc. This is just a mathematical notation quirk to remember.



Note that  $g \circ f$  means “do  $f$  first, then  $g$ ,” i.e. operate in a right-to-left order. This is just a standard mathematical convention. People in other fields who prefer to think left-to-right may write things like  $f; g$ , but this is uncommon for mathematicians.

**Example 4.7.** Suppose  $f, g : \mathbb{R} \rightarrow \mathbb{R}$  and  $f(x) = 2x$  with  $g(x) = x + 1$ . Then,

- $(g \circ f)(x) = g(f(x)) = g(2x) = 2x + 1$ .
- $(f \circ g)(x) = f(g(x)) = f(x + 1) = 2(x + 1) = 2x + 2$ .

Thus, note that it is very important: usually  $g \circ f \neq f \circ g$ !

~~~

Functions can be defined recursively. For example, we encountered the Fibonacci sequence earlier. We said to define  $F_1 = 1$ ,  $F_2 = 1$ , and  $F_n = F_{n-1} + F_{n-2}$  for  $n \geq 3$ . This is secretly a function! All infinite sequences are formally functions with domain  $\mathbb{N}$ . In this case, we have:

$$F : (\mathbb{N} \setminus \{0\}) \rightarrow \mathbb{N} \quad \begin{cases} F(1) = 1 \\ F(2) = 1 \\ F(n) = F(n-1) + F(n-2) \end{cases} .$$

Functions can also take multiple inputs. Formally, a function that is taking multiple inputs is not actually taking multiple inputs, it is just taking one input that is a tuple. For example, you might want to write a function that adds two real numbers, and you have seen people write things like  $f(x, y) = x + y$ . Formally, this is the function

$$f : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \quad f((x, y)) = x + y.$$

In other words,  $f$  takes an ordered pair  $(x, y)$  as input, then adds the two things in the pair to produce one number. However, in standard notation, we do drop the double parentheses and just write

$$f : \mathbb{R}^2 \rightarrow \mathbb{R} \quad f(x, y) = x + y.$$

Not all functions look the same. For most functions that we define in math, we use *prefix* notation. That’s what we’ve been doing this whole section, writing  $f(x, y)$  for applying  $f$  to the inputs  $x$  and  $y$ . For some special functions on two inputs, we like to use *infix* notation. In other words, common operations like  $+$  and  $\cdot$  are actually functions! For example, the standard definition of  $\cdot$  for  $\mathbb{N}$  looks like the following recursive definition

$$\cdot : \mathbb{N}^2 \rightarrow \mathbb{N} \quad \begin{cases} 0 \cdot b = 0 \\ a \cdot b = (a-1) \cdot b + b \quad \text{if } a \geq 1 \end{cases} .$$

For some functions, we also like to use *postfix* notation. The most common example is factorial, which is defined recursively by

$$! : \mathbb{N} \rightarrow \mathbb{N} \quad \begin{cases} 0! = 1 \\ n! = n((n-1)!) \quad \text{if } n \geq 1 \end{cases}$$

Some older calculators may also use postfix notation for operations like square root. On those calculators, to compute  $\sqrt{7}$ , you would press first “7”, then the “ $\sqrt{\phantom{x}}$ ” button.

## Practice

- For all of the following situations, pick an appropriate domain and codomain to describe the situation as a function. Is your function surjective, bijective, injective, or none? If bijective, describe the inverse function.
  - A database for a chat program that maps usernames to display names.
  - A computer program that converts natural numbers from base 10 to base 2.
  - Multiplying two numbers, then dividing by their sum.
  - Finding all multiples of 3 between two given integers, inclusive.
- The *range* or *image* of a function  $f : X \rightarrow Y$  is the set

$$\text{im}(f) = \{y \in Y \mid \text{there exists } x \in X \text{ s.t. } f(x) = y\}.$$

In other words, it is the set of all values actually attained by the codomain, which is the concept of range that you are familiar with, which could potentially be smaller than the codomain.

Prove that every function is surjective onto its range. In other words, given a function  $f : X \rightarrow Y$ , prove that the function

$$\hat{f} : X \rightarrow \text{im}(f) \quad \hat{f}(x) = f(x)$$

is well-defined (the output as defined by the formula belongs to the codomain) and surjective. Conclude that every injective function is bijective onto its range.

- You will sometimes encounter an alternative definition of injective: Prove that a function  $f : X \rightarrow Y$  is injective (by our definition) if and only if for all  $x_1, x_2 \in X$ , if  $f(x_1) = f(x_2)$ , then  $x_1 = x_2$ .
- Let  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$  be functions.
  - Suppose  $f$  and  $g$  are both bijective. Explain why  $g \circ f$  is bijective.
  - Following the previous part,  $f$ ,  $g$ , and  $g \circ f$  are all bijective and thus have inverses. Express  $(g \circ f)^{-1}$  in terms of  $f^{-1}$  and  $g^{-1}$ . Prove your expression.
- Let  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$  be functions. Prove or disprove the following.
  - If  $g \circ f$  is injective, then  $f$  is injective.
  - If  $g \circ f$  is injective, then  $g$  is injective.
  - If  $g \circ f$  is surjective, then  $f$  is surjective.
  - If  $g \circ f$  is surjective, then  $g$  is surjective.
- Find 3 distinct functions  $f : \mathbb{R} \rightarrow \mathbb{R}$  such that  $f^2 = \text{id}_{\mathbb{R}}$ . (id is the common name of the identity function,  $\text{id}_{\mathbb{R}} : \mathbb{R} \rightarrow \mathbb{R}$ ,  $\text{id}_{\mathbb{R}}(x) = x$ .)

## Extensions

These problems describe extra things to think about that might be interesting, but not fundamental for your future learning. They may be harder.

7. (Axiom of choice, 🐉🐉) If you've heard of the axiom of choice before, you might have heard that it's a crazy tool that allows you to make subsets of  $\mathbb{R}$  for which there is no valid notion of length, or break one sphere into 5 pieces and reassemble them into two spheres identical to the original. Mathcamp is teaching several courses about it this summer!

But the axiom says something very simple and believable. Let  $\mathcal{A}$  be a set of sets. The axiom just says that there is a way to pick one element from each of these sets. More formally, there exists a function  $f : \mathcal{A} \rightarrow \bigcup_{A \in \mathcal{A}} A$  such that  $f(A) \in A$  for all  $A \in \mathcal{A}$ . This axiom is also important for some very basic, seemingly obvious theorems, described below.

- (a) Prove (without anything fancy) that if a function  $f : X \rightarrow Y$  is injective, it has a *left inverse*. A left inverse is a function  $f^{-1} : Y \rightarrow X$  such that  $f^{-1}(f(x)) = x$  for all  $x \in X$ . (In other words, it undoes  $f$  after you've already done  $f$ .)
- (b) Prove using the axiom of choice that if a function  $f : X \rightarrow Y$  is surjective, it has a *right inverse*. A right inverse is a function  $f^{-1} : Y \rightarrow X$  such that  $f(f^{-1}(y)) = y$  for all  $y \in Y$ . (In other words, it preemptively undoes  $f$ , setting up a state where if you then do  $f$ ,
- (c) Prove that if every surjective function has a right inverse, then the axiom of choice is true. (Thus, these two claims are completely equivalent.)