Math100: Introduction to Proof and Problem Solving

Sam Kim Miller

July 21, 2022

Contents

1 Sets

Before we get into proofs and logic, we first begin with one of the universal building blocks of mathematics, sets. Many mathematical structures are formed from sets, so having a good understanding and intuition of them is vital. Note that there is a highly abstract and formal subject called *set theory*, first introduced by Cantor, which formalizes many of the axioms we take for granted in studying mathematics, however what we will study is NOT exactly set theory. If one wants an introduction to formal set theory, the Stanford Encyclopedia of Philosophy has a good entry to read up on.

You've experienced sets before, whether you are aware or not. Many examples (and non-examples) will follow.

1.1 Basics of Sets

Definition 1.1. A **set** is a collection of objects. The objects which make up the set are called its **elements**, or **members**.

It is customary to use capital letters to denote (name) sets, and lower-case letters to represent elements if they are not explicit. If a is an element of the set A, we write: $a \in A$, and if a is **not** an element of A, then we write $a \notin A$.

Remark 1.2. In general, we will take our sets to *not* have repeated elements. There is a class of sets which may have repeated elements, called **multisets**. We may work with these later, but for now, sets will be assumed to not have repeated elements unless otherwise specified.
Two sets are equal if they contain all the same elements. The order in which we list the elements of the sets does not matter, for example, $\{1, 2, 3\} = \{2, 3, 1\}$.

Some standard notation for important sets are as follows:

- $\mathbb{Z}$ denotes the set of integers.
- $\mathbb{N}$ denotes the set of non-negative integers, sometimes called the **natural numbers**.
- $\mathbb{Q}$ denotes the set of rational numbers (numbers that can be expressed as a fraction).
- $\mathbb{R}$ denotes the set of real numbers.
- $\mathbb{C}$ denotes the set of complex numbers.

Sets can contain any sort of data - numbers, names, people, objects, even other sets!

Example 1.3. (a) The set

$$A = \{1, \text{blue}, \text{Ol Dirty Bastard}, \{a, b, c, d, e\}\}$$

contains *four* elements, the number 1, the color blue, the prolific rapper ODB, and another set. It may be tempting to think that this set has 9 elements, however this would be a mistake - the set contained within the set is counted as one element. We have that $c \notin A$, despite the fact that $c \in \{a, b, c, d, e\}$ and $\{a, b, c, d, e\} \in A$.

(b) A set need not contain any elements! For example the set of all real solutions to the polynomial equation $x^2 + 1 = 0$ is empty. There is *only one set* that contains zero elements, it is called **the empty set** or **null set**. We denote it by $\varnothing$.

Notational confusion may arise. Here, $\varnothing$ is the empty set, while $\{\varnothing\}$ is a set which contains one element, namely, the empty set. Some students erroneously write $\varnothing$ to denote the number 0, this causes even more confusion. **DO NOT DO THIS.**

(c) We sometimes use ellipses, or **the three dot notation**, to make expressing sets easier. For example,

$$B = \{1, 2, 3, \dots, 50\}$$

expresses the integers from 1 to 50, inclusive.

$$\mathbb{N}^+ = \{1, 2, 3, \dots\}$$

expresses all positive integers.

One must take care when using ellipses, and make it clear in the context exactly what the set in question is describing. An example: I wrote that above, $\{1, 2, 3, \dots\}$ denoted the set of all positive integers. However, this is not the only thing that this notation could express! It could possibly mean the set of Fibonacci numbers,

$$F = \{1, 2, 3, 5, 8, 13, \dots\}.$$

Of course, this is a bit of a contrived example - it should be fairly clear in context what set is being described. Be sure that when you are using ellipses, it is clear beyond any doubt what set you are describing!

Often, we wish to describe sets of things that satisfy some kind of property. There is a special notation that allows us to do so succinctly!

Definition 1.4. We may define a set as $S = \{x : p(x)\}$ (often written with a $|$ instead of a :), where by this, we mean that S consists of all the elements x which satisfy the condition "$p(x)$." This is called **set-builder notation**.

Generally, we assume all elements come from some **universal set** U, that is, the set for which all objects are defined to be living in. It is not always obvious what this universal set is, so it may be specified what U is. For example, the set $\{1\}$ could have universal set $\mathbb{Z}$, $\mathbb{R}$, or other possibilities. Here are some examples of set-builder notation where the universal set is specified.

Example 1.5. (a) We may express the set of all positive integers as:

$$\mathbb{N}^+ = \{x \in \mathbb{Z} : x > 0\}.$$

(b) The set $\{1, 2, 3\}$ may also be expressed as

$$\{1, 2, 3\} = \{x \in \mathbb{R} : (x - 1)(x - 2)(x - 3) = 0\}.$$

(c) We may express the set of all even integers as:

$$\{x \in \mathbb{R} : x \text{ is an even integer}\} \text{ or } \{2y : y \in \mathbb{R}, y \text{ is an integer}\}$$

(d) Let's describe the set:

$$\{7a+3b : a,b\in\mathbb{Z}\}.$$

The set contains all numbers of form $7a+3b$ where a and b are integers. By properties of integers, $7a+3b$ must be an integer as well. Which integers could $7a+3b$ be? Let n be some integer and identify $a=n, b=-2n$. Then we see:

$$7n+3(-2n)=n,$$

hence n is in the set. But since n was an arbitrary integer, we conclude that all integers belong to the set, and hence, the set is simply $\mathbb{Z}$.

Definition 1.6. For a set S, denote by $|S|$ the number of elements contained in S, called the **cardinality of** S. A set is **finite** if it has finite cardinality, and **infinite** otherwise.

Example 1.7. $\mathbb{N},\mathbb{Z},\mathbb{R},\mathbb{C}$ are all infinite. The set A from before has $|A|=4$, and the set B from before has cardinality $|B|=50$, hence A and B are finite.

Exercise 1.8. Which of the following sets contains -2 as an element?

- $S_1=\{-1,-2,\{-1\},\{-2\},\{-1,-2\}\}$
- $S_2=\{x\in\mathbb{N} : -x\in\mathbb{N}\}$
- $S_3=\{x\in\mathbb{Z} : x^2=2^x\}$
- $S_4=\{x\in\mathbb{Z} : |x|=-x\}$
- $S_5=\{\{-1,-2\},\{-2,-3\},\{-1,-3\}\}$

1.2 Subsets

Definition 1.9. A set A is a **subset** of a set B if every element of A also belongs to B. It is true that $A\subseteq A$. A set A is a **proper subset** of a set B if every element of A belongs to B, but $A\neq B$. We denote this $A\subset B$, or sometimes $A\subsetneq B$.

Remark 1.10. Observe that if $A\subseteq B$ and $B\subseteq C$, then $A\subseteq C$. Why? If $x\in A$, then $x\in B$. But if $x\in B$, then $x\in C$. Thus, if $x\in A$, then $x\in C$.
Every nonempty set has at least two subsets, namely itself and $\varnothing$. $\varnothing$ is the only set which has only one subset.

Example 1.11. (a) $\mathbb{N}\subset\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$.

(b) It is possibly for one set to be both a subset and an element of another set. For example, $A=\{1\}$ and $B=\{1,\{1\}\}$.

(c) For $a, b \in \mathbb{R}$ satisfying $a < b$, we have the following subsets of $\mathbb{R}$:

$$(a, b) = \{x \in \mathbb{R} : a < x < b\} \subset \mathbb{R}, \qquad [a, b] = \{x \in \mathbb{R} : a \leqslant x \leqslant b\} \subset \mathbb{R}.$$

(a, b) is an **open interval** of $\mathbb{R}$, while $[a, b]$ is a **closed interval** of $\mathbb{R}$. We may also replace $\mathbb{R}$ with $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$, or any ordered set. We can also form sets like $[a, b)$ or $(a, b]$ - these are called **half-open** or **half-closed** intervals. Finally, we have the **infinite intervals**:

$$(-\infty, a) = \{x \in \mathbb{R} : x < a\}, \qquad (a, \infty) = \{x \in \mathbb{R} : x > a\},$$

and similarly for closed brackets. Note that $(a, \infty]$ is not defined as a subset of $\mathbb{R}$, however there are other number systems where this *is* well defined!

Theorem 1.12. Two sets A and B are equal if and only if $A \subseteq B$ and $B \subseteq A$.

We have not discussed logically what “if and only if” means, so to be clear, this statement is saying two things:

- If A and B are equal, $A \subseteq B$ and $B \subseteq A$.
- If $A \subseteq B$ and $B \subseteq A$, then $A = B$.

We have not formally introduced proofs yet, but let's prove this statement rigorously.

Proof. First, we show the forward statement. Suppose $A = B$. Then for any $x \in A$, by equality, we have $x \in B$, hence $A \subseteq B$. Similarly, for any $y \in B$, by equality, we have $y \in A$, hence $B \subseteq A$. Thus, if A and B are equal, $A \subseteq B$ and $B \subseteq A$.
Next, we show the backwards statement. Suppose $x \in A$. Since $A \subseteq B$, $x \in B$ as well. Now suppose $y \in B$, since $B \subseteq A$, $y \in A$ as well. Thus, the elements in A and B must be equal, hence $A = B$, as desired. □

Remark 1.13. How many subsets are there of a set A? Well, it's fairly clear that if A is infinite, there are still infinitely many subsets. But if A is finite? To count this, we can consider the following procedure for building a subset of A: choose an ordering of the elements of A. Consider the first element of A and decide whether to add it or not. Then consider the second element, and decide whether to add it. Repeat through all the elements. This obtains a unique subset, and moreover, all subsets of A can be chosen in this way. Since in total we made $|A|$ choices, each of which had 2 options, we had $2 \cdot 2 \cdot \dots \cdot 2 = 2^{|A|}$ unique possible outcomes. We will formally prove this using combinatorics later - the proof uses this basic idea. Note that it is crucial that A contains no repeating elements.

Definition 1.14. Denote by $\mathcal{P}(A)$ the **power set** of A, which contains all subsets of A.

Theorem 1.15. If A is finite, $|\mathcal{P}(A)| = 2^{|A|}$.

1.3 Set Operations

Note: Be sure to draw Venn diagrams for this section!
Just like we have ways of combining two numbers to produce a new number (addition, multiplication), we have ways of combining sets to produce a new set. These are called **binary operations** - binary because they take in two things, and spit out one.

Definition 1.16.

- The **union** of two sets A, B is:
$$A \cup B = \{x : x \in A \text{ or } x \in B\}.$$
- The **intersection** of two sets A, B is:
$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$
- The **difference** of two sets A, B is:
$$A - B = \{x : x \in A \text{ and } x \notin B\}.$$
- The **compliment** of a set A is:
$$\overline{A} = \{x : x \notin A\}.$$
Note that for the compliment may be equivalently expressed as:
$$\overline{A} = U - A$$

Remark 1.17. Here, it is clear that $A \cap B = B \cap A$ and $A \cup B = B \cup A$ - the operations are **commutative**. In addition, $(A \cap B) \cap C = A \cap (B \cap C)$, in other words, the operations are **associative** so we can simply write $A \cap B \cap C$ and it is clear what this means.
However, it is not true in general that $A - B = B - A$, or that $(A - B) - C = A - (B - C)$!

Example 1.18. Let $A = \{x \in \mathbb{R} : |x| \leqslant 3\}, B = \{x \in \mathbb{R} : |x| > 2\}, C = \{x :\in \mathbb{R} : |x - 1| \leqslant 4\}$.

(a) In interval notation, $A = [-3, 3]$, $B = (-\infty, -2) \cup (2, \infty)$, and $C = [-3, 5]$.

(b) $A \cap B = [-3, -2) \cap (2, 3]$, $A - B = [-2, 2]$, $B \cap C = [-3, -2) \cap (2, 5]$, $B \cup C = \mathbb{R}$, $B - C = (-\infty, -3) \cup (5, \infty)$, and $C - B = [-2, 2]$. Note that as we would expect, $B - C \neq C - B$

Note that we may express the difference of two sets in another way!

Theorem 1.19. For any two sets A, B, we have $A - B = A \cap \overline{B}$.

Proof. Exercise. □

We have an distributive property of sets analogous to the distribution of addition and multiplication.

Theorem 1.20. For all sets A, B, C,
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

1.4 Indexed Collections of Sets

You may recall sum notation, such as $\sum_{i=1}^{1} 0i$, is used to denote large sums. Since unions and intersections are commutative and associative, we have similar notions.

Definition 1.21. Given an ordered list of sets, $A_1, \ldots, A_n$ (where n is a positive integer), we write:

$$\bigcup_{i=k}^{n} A_i = \{x : x \in A_i \text{ for some } i, k \leqslant i \leqslant n\}$$

$$\bigcap_{i=k}^{n} A_i = \{x : x \in A_i \text{ for all } i, k \leqslant i \leqslant n\}$$

The variable i is called a **dummy variable**.

Example 1.22. Let $B_1 = \{1, 2\}$, $B_2 = \{2, 3\}$, and so on (so in general, $B_k = \{k, k+1\}$, for any $k \in \mathbb{N}$). Given some non-negative integers $j \leqslant k$:

$$\bigcup_{i=j}^{k} B_i = \{j, j+1, \ldots, k+1\}.$$

Computing the intersection is a bit trickier, if $k - j \geqslant 2$,

$$\bigcap_{i=j}^{k} B_i = \varnothing.$$

However, if $k - j = 1$, then $\bigcap_{i=j}^{k} B_i = \{j+1\}$ and if $k = j$, then $\bigcap_{i=j}^{k} B_i = B_j = \{j, j+1\}$.

Remark 1.23. In the case of infinite ordered lists, we also allow notation such as

$$\bigcup_{i=-\infty}^{\infty} A_i = \{x : x \in A_i \text{ for some } i \in \mathbb{N}\}$$

$$\bigcap_{i=-\infty}^{\infty} A_i = \{x : x \in A_i \text{ for all } i \in \mathbb{N}\}$$

Example 1.24. For any $n \in \mathbb{N}^+$, let $S_n = (-1/n, 1/n)$. It is clear that $S_1 \supset S_2 \supset \ldots$, so we have

$$\bigcup_{i=1}^{\infty} S_i = S_1.$$

What is their intersection? Well, first note that $0 \in S_k$ for any k. Then, observe that for any nonzero $x \in \mathbb{R}$, there exists some positive integer k for which $|x| > 1/k$. Therefore, $x \notin S_k$, and thus,

$$\bigcap_{i=1}^{\infty} S_i = \{0\}$$

This is a classic example of the claim that "the intersection of closed intervals need not be closed!"

Definition 1.25. However, there are instances when the union or intersection of a collection of sets cannot be described conveniently, or perhaps at all, in the manners described above. In this case, we introduce a nonempty set I, which we call the **index set**, which is used as a mechanism for selecting the sets we wish to consider. Then, for every $\alpha \in I$, we assign a corresponding set, S_α, and write $\{S_\alpha\}_{\alpha \in I}$ to denote the collection of sets indexed this way, called an **indexed collection of sets**. Then, we can express their union and intersection as follows:

$$\bigcup_{\alpha \in I} S_\alpha = \{x : x \in S_\alpha \text{ for some } \alpha \in I\}$$

$$\bigcap_{\alpha \in I} S_\alpha = \{x : x \in S_\alpha \text{ for all } \alpha \in I\}$$

Example 1.26. (a) Going back to the previous example with $B_k = \{k, k+1\}$, we could define $I = \{j, j+1, \ldots, k-1, k\}$, and then rewrite the union and intersection notation as follows:

$$\bigcup_{i=j}^{k} B_i = \bigcup_{\alpha \in I} B_\alpha$$

$$\bigcap_{i=j}^{k} B_i = \bigcap_{\alpha \in I} B_\alpha$$

(b) A situation where we need to use the index notation is as follows: for all $x \in \mathbb{R}$, let $S_x = \{x\}$. Then, let $I = \mathbb{R}$, so we have

$$\bigcup_{\alpha \in I} S_\alpha = \mathbb{R}.$$

In this case, it would have been impossible to express this collection of sets in the more standard notation - this is due to **the uncountability of the reals**, proven by Cantor. However, had we used $\mathbb{Q}$ rather than $\mathbb{R}$, it is in fact possible to index the rationals with the natural numbers! We may prove both these statements later in class, if we do not, take Real Analysis to see this proof.

1.5 Cartesian Products and Partitions

We next cover a few more features of sets which will be of importance later in the course.

Definition 1.27. Two sets are **disjoint** if their intersection is the trivial set. A collection of sets is **pairwise disjoint** if every choice of two sets in the collection are disjoint.

Example 1.28. Let $A = \{1, 2\}, B = \{3, 4\}, C = \{5, 6\}$. Then A, B, C are pairwise disjoint. Let $A' = \{1, 2\}, B' = \{3, 4\}, C' = \{4, 5\}$. Then $A' \cap B' \cap C' = \varnothing$, and A' is disjoint with B' and C', but A', B', C' are not pairwise disjoint since $B' \cap C' \neq \varnothing$.

Definition 1.29. For a set A, a collection $\mathcal{S}$ of pairwise disjoint subsets of A is a **partition** of A if every element of A belongs to some set in $\mathcal{S}$.
Alternatively, a partition of A can be defined as a collection $\mathcal{S}$ of subsets of A satisfying:

(a) $X \neq \varnothing$ for every set $X \in \mathcal{S}$.

(b) For every two distinct sets $X, Y \in \mathcal{S}$, $X \cap Y = \varnothing$.

(c) $\bigcup_{X \in \mathcal{S}} S = A$.

Example 1.30. (a) $\mathbb{Z}$ may be partitioned into the set of even integers and the set of odd integers.

(b) For any finite set A, $\mathcal{P}(A)$ can be partitioned into $\{\mathcal{P}^0(A), \mathcal{P}^1(A), \ldots, \mathcal{P}^{|A|}(A)\}$, where $\mathcal{P}^i(A)$ is defined to be the set of all subsets of A containing exactly i elements. This partition will be used later in the course!

(c) For two sets A, B, their union $A \cup B$ has a partition (after removing empty sets as necessary) $\mathcal{S} = \{A - B, A \cap B, B - A\}$ (draw a venn diagram).

Next, we take a look at another method of forming sets, the Cartesian product.

Definition 1.31. An **ordered pair** is an object consisting of, pair of objects, written (a, b). The contents of an ordered pair are called its **coordinates**. Two ordered pairs (a, b) and (a', b') are equal if and only if $a = a'$ and $b = b'$, that is, their first and second coordinates match. For example, $(1, 2) \neq (2, 1)$.
The **Cartesian product** (sometimes just called the product) $A \times B$ of two sets A, B is the set of ordered pairs whose first coordinate belongs to A and second coordinate belongs to B. Explicitly,

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}.$$

Remark 1.32. As the name suggests, order matters in an ordered pair. If $a \neq b$, then $(a, b) \neq (b, a)$. Similarly, if $A \neq B$ as sets, then $A \times B \neq B \times A$.

If A and B are finite, then $|A \times B| = |A| \cdot |B|$ - we may see why this is by considering the number of possible ways to form an ordered pair. There are $|A|$ possible choices from A and $|B|$ possible choices from B - each way we can choose will be unique, and every ordered pair can be chosen in this fashion.

Example 1.33. (a) A classic example of a Cartesian product is the xy-plane, or two-dimensional Euclidean space, which can simply be expressed as $\mathbb{R} \times \mathbb{R}$, or $\mathbb{R}^2$. Similarly, any graph of a function $y = f(x)$ can be expressed as the set of points $\{(x, y) \in \mathbb{R}^2 : y = f(x)\}$.

(b) If $A = \{1, 2\}$ and $B = \{1, 3\}$, then $A \times B = \{(1, 1), (1, 3), (2, 1), (2, 3)\}$ and $B \times A = \{(1, 1), (1, 2), (3, 1), (3, 2)\}$. These are not equal.

We can extend this notion further beyond just pairs, and form Cartesian products of more than just two sets.

Definition 1.34. An **ordered tuple** is an ordered list, $(x_1, x_2, \dots)$ which may be finite or infinite. Two ordered tuples are equal if and only if they have equal size and each coordinate is equal.

The Cartesian product of sets $A_1, \dots, A_k$ is:

$$A_1 \times \cdots \times A_k = \{(x_1, \dots, x_k) : x_1 \in A_1, \dots, x_k \in A_k\}.$$

Take caution - the set $A \times (B \times C)$ and the set $A \times B \times C$ are not quite identical - the former consists of ordered pairs, and the latter consists of ordered triples. However, the sets "look the same" (are bijective) and we can identify $(a, (b, c))$ with (a, b, c) without much issue - we will expand on this further in the course.

Example 1.35. (a) 3-dimensional Euclidean space, or xyz-plane, is $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3$. As before, we can express the graph of a function $z = f(x, y)$ as the set $\{(x, y, z) \in \mathbb{R}^3 : z = f(x, y)\}$.

(b) If we flip a coin once, there are two possible outcomes, either a heads or tails. We can express this as a set $S = \{H, T\}$. Suppose we want to count the number of outcomes of flipping a coin some number of times, where the order of flips matters. For example, with 2 flips, there are four possible outcomes: $\{(H, H), (H, T), (T, H), (T, T)\}$. This is exactly the set S^2! In general, S^n details the set of all possible outcomes when we flip a coin n times. We see that $|S^n| = 2^n$. Constructions like these are very useful in the study of probability.

1.6 Are All Collections Sets? Russell's Paradox

One may notice that I have occasionally refrained from calling some things "sets," and instead used terminology like "collections" or "lists." This is intentional - we may ask the question, "is every collection of objects a set?" This should be tautologically true by the definition given at the beginning of this chapter, however, we shall see that some issues may arise.

The philosopher and mathematician Bertrand Russell (1872 - 1970) researched groundbreaking work on the theory of sets and foundations of mathematics. He spent much of his life attempting to reduce mathematics to classical logic (what we will study in the next chapter), and his book *Principia Mathematica*, published with Alfred Whitehead, is considered one of the great classical logic publications. He is additionally famous for discovering **Russell's Paradox** (1902). At the time, significant work was being put into building an axiomatic and purely logical approach to mathematics, and this paradox proved troublesome, as it

demonstrated an inconsistency in some of the axiomatic approaches mathematicians (including Russell himself) had taken. Russell's paradox may be one of the largest logical breakthroughs, along with Godel's Incompleteness Theorems (which are often abused in pop culture and taken to be more powerful statements than they actually are - please do not make statements about the incompleteness theorems until you have the understanding to be able to do so).
For more historical reading, the graphic novel *Logicomix* is quite informative, while still remaining light reading! See also Stanford's Encyclopedia of Philosophy.

Consider the following set of sets:

$$A = \{X : X \text{ is a set and } X \notin X\}.$$

In other words, A is the set of all sets which do not include themselves. Most sets we can think of are in A - for example, any set which contains only numbers cannot contain itself, and therefore belongs to A.

A set not in A is as follows: let $B = \{\{\{\cdots\}\}\}$ - we may think of this as a set of infinite, identical Russian dolls nested inside each other endlessly. However, there is a simpler way of expressing this set: $B = \{B\}$. Clearly, $B \in B$, hence $B \notin A$.

Russell's Paradox asks the question:

Is A an element of A?

If $A \in A$, then by definition of A, $A \notin A$, which is a logical contradiction. Therefore, $A \notin A$, but then by definition of A, this implies that $A \in A$, again, a logical contradiction! More formally, if $A \in A$ is true, then it is false, and if $A \in A$ is false, then it is true.

The ultimate conclusion here is that our approach to the definition of a set, which is known as **naive set theory**, is logically inconsistent - not every collection of objects can be a set. Eventually, mathematicians settled upon a collection of axioms for set theory, which are the **Zermelo-Fraenkel axioms**, which define properties sets may have, as well as rules for what may constitute a set. One such axiom, the **axiom of foundation**, states that no non-empty set X is allowed to have the property $X \cap x \neq \varnothing$ for all its elements x. This rules out our "set" $B = \{B\}$.

In practice, one need not worry about modern set theory and the ZF axioms - almost any set which we care about is a logically consistent set, and paradoxes like Russell's do not tend to come up in everyday mathematics, even in modern research mathematics. However, Russell's paradox is an important lesson - precision of thought and language is an important part of doing mathematics. We will shift to logic next, a codification of this.

2 Logic

The goal of mathematics is not multiplying large numbers together, it is to determine absolute truth. Are there connections between two mathematical objects? What are they? Finding answers to questions like these is important, but more important is demonstrating that we are right and that our explanation is logically convincing to others. The reasoning we use as we proceed from what we already know as truth to what we wish to show is truth must follow the laws of logic, and in this way, it will make sense to others, not only to ourselves.

There is a joint responsibility:

- It is the writer's responsibility to use laws of logic to give a valid and clear argument, with enough details provided for the reader to understand what we have written and to be convinced.
- It is the reader's responsibility to know the laws of logic and to study the concepts involved sufficiently well, so they will not only be able to understand a well-presented argument but can decide as well if it is valid or not.

Logic itself is a very deep academic field, however we will only go through what is necessary to know in order to do mathematics.

2.1 Statements

In mathematics, we constantly deal with statements, specifically, statements that deal with mathematics,

Definition 2.1. A **statement** is a declarative sentence or assertion that is either true or false, but not both. The truth-ness or false-ness of a statement is its **truth value** - a statement can be **true** (denoted **T**) or **false** (denoted **F**).
We often use P, Q, R, or $P_1, P_2, \ldots$ to denote statements.

Example 2.2. The sentences "The integer 3 is odd" and "The integer 57 is prime" are both statements, the first is true and the second is false. The statement "The sky is currently dark" is a statement, but the truth value may change depending on the time of day. The statement "The 100th digit in the decimal expansion of π is 7" is a statement, but it may take some work to verify the truth value of this statement. A statement need not have a truth value which is immediately known.
The imperative sentence "Find the derivative of e^x," the interrogative sentence "Are these sets disjoint?" and the exclamation "How difficult this problem is!" are all *not* statements.

Definition 2.3. "The real number r is rational" is a statement, but unless we know what r is, we cannot assign a truth value to it. This statement is **an open sentence**, or a statement with one or more variables representing a value in a prescribed set, the **domain** of the variable. Note that if no data is given on the variable, an open sentence is not necessarily a statement. We denote open sentences with their variables listed, like $P(x)$ for example.

If $P(x)$ is an open sentence and the domain of x is S, we say $P(x)$ **is an open sentence over the domain** S.

Example 2.4. (a) The open sentence $P(x) : 3x = 12$ has truth value T when $x = 4$, and has truth value F when $x \neq 4$. $P(x)$ is not a statement, however, if nothing is substituted for x.

(b) For the open sentence

$$Q(x, y) : |x + 1| + |y| = 1$$

in two variables, suppose the domain of the variable x is $S = \{-2, -1, 0, 1\}$ and the domain of the variable $T = \{-1, 0, 1\}$. Then we check:

$$P(-1, 1) : |(-1) + 1| + |1| = 1$$

is a true statement, while

$$P(1, -1) : |1 + 1| + | - 1| = 1$$

is a false statement. In fact, $P(x, y)$ is a true statement when

$$(x, y) \in \{(-2, 0), (-1, -1), (-1, 1), (0, 0)\},$$

and $P(x, y)$ is a false statement for all other $(x, y) \in S \times T$.

Definition 2.5. The possible truth values of a statement, or possible combinations of truth values for a list of statements, can be listed together in a table, called a **truth table**.

Example 2.6. Here are the truth tables for two independent statements, P, Q:

P
T
F

Q
T
F

P	Q
T	T
F	T
T	F
F	F

Truth tables will become more useful when we begin to look at statements which have dependent relationships.

2.2 The Negation, Disjunction, and Conjunction

Like with numbers and sets, we look to construct new statements from old ones in a variety of ways. The first example concerns producing a new statement from a single given statement.

Definition 2.7. The **negation** of a statement P is the statement "not P," denoted by $\sim P$. In English, it is always possible to express the negation as "It is not the case that P," but this is usually not succinct.

Example 2.8. The negation of the statement

$$P_1 : \text{"The integer 3 is odd"}$$

is the statement

$$\sim P_1 : \text{"The integer 3 is not odd"}.$$

We could also write "The integer 3 is even."
The negation of the statement

$$P_2 : \text{"The integer 57 is prime"}$$

is the statement

$$\sim P_2 : \text{"The integer 57 is not prime"}$$

Remark 2.9. The negation of a true statement is always false, and the negation of a false statement is always true. Therefore, for a statement P, P and $\sim P$ have the truth table as follows:

P	$\sim P$
T	F
F	T

Next we introduce two binary operators on statements, stemming from "or" and "and".

Definition 2.10. The **disjunction** of the statements P, Q is the statement

$$P \textbf{ or } Q$$

and is denoted $P \vee Q$. The disjunction is true if at least one of P and Q is true, and false otherwise.

The **conjunction** of P, Q is the statement

$$P \textbf{ and } Q$$

and is denoted $P \wedge Q$. The conjunction is true only when both P and Q are true.

For shorthand, we may also call the disjunction the "or" and the conjunction the "and."

Example 2.11. For the statements P_1 : "The integer 3 is odd" and P_2 : "The integer 57 is prime" from earlier, the disjunction $P_1 \vee P_2$ is:

$$P_1 \vee P_2 : \text{Either 3 is odd or 57 is prime,}$$

and the conjunction $P_1 \wedge P_2$ is:

$$P_1 \wedge P_2 : \text{Both 3 is odd and 57 is prime.}$$

Here, $P_1 \vee P_2$ is true and $P_1 \wedge P_2$ is false.

Remark 2.12. The truth tables for disjunction and conjunction are as follows:

P_1	P_2	$P_1 \vee P_2$	$P_1 \wedge P_2$
T	T	T	T
F	T	T	F
T	F	T	F
F	F	F	F

The wording for disjunction can be a bit confusing - the "or" may sound like it suggests that both P_1 and P_2 shouldn't both be true. This is not the meaning we assign, but there is a separate statement, **exclusive or**, written "**XOR**," which fills this role instead. That is, P_1 XOR P_2 is true if only one of P_1, P_2 is true.

2.3 Logical Connectives & Logical Equivalences

Definition 2.13. The symbols which input and output statements, like $\sim, \vee, \wedge$, and more which we have yet to introduce, are referred to as **logical connectives**. As we've seen, we can use these logical connectives to form more intricate statements, like $(P \vee Q) \wedge (P \vee R)$ (note the use of parentheses). These are **compound statements**, statements composed of one or more given statements and logical connectives. The shortest compound statement is $\sim P$.

Example 2.14. Some compound statements are: $P \vee Q, (\sim P) \wedge Q, P \wedge (Q \vee R), P \wedge (\sim P), P \vee (\sim P), \sim (P \vee Q), \sim (\sim P)$. Note that some of these compound statements have fixed truth value regardless of the values of P, Q, R. For example, $P \wedge (\sim P)$ is always false, and $P \vee (\sim P)$ is always true.

Definition 2.15. A compound statement P which is true regardless of the truth values which comprise P is called a **tautology**. Similarly, a compound statement S which is false regardless of the truth values which comprise S is called a **contradiction**.

Example 2.16. Here are the truth tables of the tautology $P \vee (\sim P)$ and the contradiction $P \wedge (\sim P)$:

P	$\sim P$	$P \vee (\sim P)$	$P \wedge (\sim P)$
T	F	T	F
F	T	T	F

Each row is the same value for the tautology and contradiction.

Remark 2.17. It is possible to have two compound statements whose truth table columns are identical, in other words, the two compound statements have exactly the same truth value for ever combination of statement truth values. Some simple examples are: P and $\sim (\sim P)$, or $P \vee Q$ and $Q \vee P$:

P	$\sim P$	$\sim (\sim P)$
T	F	T
F	T	F

P	Q	$P \vee Q$	$Q \vee P$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

Definition 2.18. Let R and S be two compound statements involving the same component statements. Then R and S are called **logically equivalent** if R and S have the same truth values for all combinations of truth values of their component statements. We denote this by $R \equiv S$.

Logical equivalence can be quite practical. For instance, if $R \equiv S$, and we wish to show that S is true, we may do so by showing R is true instead, which will imply that S is true! There are many times in mathematics when we want to show some statement is true, and can do so by proving another statement which is logically equivalent. We will revisit this idea after introducing a few more logical connectives, and use it often when proving things.

Some useful logical equivalences are as follows (note the similarity to the set equivalences):

Theorem 2.19. For any statements P, Q, R:

(a) Commutative laws:

  (a) $P \vee Q \equiv Q \vee P$

  (b) $P \wedge Q \equiv Q \vee P$

(b) Associative laws:

  (a) $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$

  (b) $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$

(c) Distributive laws:

(a) $P \vee (Q \wedge R) \equiv (P \vee Q)(\wedge(P \vee R)$

(b) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

(d) **De Morgan's Laws:**

(a) $\sim (P \vee Q) \equiv (\sim P) \wedge (\sim Q)$

(b) $\sim (P \wedge Q) \equiv (\sim P) \vee (\sim Q)$

Proof. All of these may be proven by means of a truth table. Some of these are left as exercises for you! □

2.4 The Implication $\Rightarrow$

Perhaps the most used statement and connective in mathematics is the implication.

Definition 2.20. For statements P and Q, the **implication** (sometimes called the **conditional**) is the statement

"If P, then Q," or P **implies** Q.

We denote it by $P \Rightarrow Q$. Its truth table is:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Note that $P \Rightarrow Q$ is false only when P is true but Q is false.

Example 2.21. As before, let P_1 : 3 is odd, and P_2 : 57 is prime. Then $P_1 \Rightarrow P_2$ reads as, "If 3 is odd, then 57 is prime." As P_1 is true, but P_2 is false, then $P_1 \Rightarrow P_2$ is false.
$P_2 \Rightarrow P_1$ reads as, "IF 57 is prime, then 3 is odd." In this case, $P_2 \Rightarrow P_1$ is true, despite P_1 being false.

Remark 2.22. While the other logical connectives may seem intuitive, the implication affords an explanation. The basic idea is that when P is false, we cannot make any statements about Q, so the implication is vacuously true. Let's see why its truth table is as we've defined it with the following example:

Say you're taking a course and are currently receiving a B+. You go to your prof and ask if there's any way you can get an A in the course, and they respond: "If you earn an A on the final, you'll receive an A in the course." We check the truth or falseness of this implication based on the various combinations of truth or falseness. We have: P : "You earn an A on the final exam," and Q : "You receive an A for your final grade," let's check $P \Rightarrow Q$ based on whether your professor told the truth or not.

- If P and Q are both true, then your professor told the truth. You got an A on the final so you got an A in the class, hence $P \Rightarrow Q$ is true as well.
- If P is true but Q is false, then your professor lied - you got an A on the final, but still did not get an A in the class as promised. So $P \Rightarrow Q$ is false.
- If P is false and Q is false, then your professor told the truth, as you were only promised an A if you got an A on the final. Hence $P \Rightarrow Q$ is true.
- Suppose P is false but Q is true, that is, you did not get an A on the exam but still got an A in the class. How could this happen? It's possible the exam was curved, it's possible there was a clerical error, or it's possible the professor just likes you. Regardless, the professor didn't lie, as they didn't guarantee *anything* if you didn't get an A. Hence $P \Rightarrow Q$ is true.

So to sum up, the only situation for when $P \Rightarrow Q$ is a false statement is when P is true, but Q is false.

Remark 2.23. There are a number of ways to write $P \Rightarrow Q$, such as:

- If P then Q
- Q if P
- P implies Q
- P only when Q
- P is sufficient for Q
- Q is necessary for P

Generally, we are more interested in open sentences which contain variables than simply statements, and whose truthfulness is only known once we've assigned values to the variables. Just as we've formed new statements with logical connectives, we can form new open sentences in the same way.

Example 2.24. (a) Let $x \in \mathbb{R}$, $P(x)$ be the sentence "x is positive," and $Q(x)$ be the sentence "x is not positive." Now, consider the open sentence which we should certainly hope is valid for any x:

$$\text{If } x \text{ is positive, then } -x \text{ is not positive.}$$

This can be expressed by:

$$P(x) \Rightarrow Q(-x).$$

- If x is positive, then $P(x)$ is true and $Q(x)$ is true, so the implication is true.
- If x is negative, then $P(x)$ is false and $Q(x)$ is false, so the implication is true.
- If x is zero, then $P(x)$ is false but $Q(x)$ is true, so the implication is true.

Thus for all possible values of $x \in \mathbb{R}$, $P(x) \Rightarrow Q(x)$ is true.

(b) For a triangle T, let $P(T) : T$ is equilateral, and $Q(T) : T$ is isosceles. Consider the implication $P(T) \Rightarrow Q(T)$, where the domain of T is all triangles.

- For an equilateral triangle T_1, both $P(T_1)$ and $Q(T_1)$ are true, so $P(T_1) \Rightarrow Q(T_1)$ is true.
- For an isosceles triangle T_2, $P(T_2)$ is false but $Q(T_2)$ is true, so $P(T_1) \Rightarrow Q(T_1)$ is true.
- For a scalene triangle T_3, $P(T_3)$ and $Q(T_3)$ are false, so $P(T_3) \Rightarrow Q(T_3)$ is true.

Thus for all triangles T, $P(T) \Rightarrow Q(T)$ is true.

(c) Let $S = \{2, 3, 5\}$, and define

$$P(n) : n^2 - n + 1 \text{ is prime.}, \qquad , Q(n) : n^3 - n + 1 \text{ is prime},$$

be open sentences over domain S. Plugging in values of n, we have:

$$P(2) : 3 \text{ is prime}, \; Q(2) : 7 \text{ is prime}.$$

$$P(3) : 7 \text{ is prime}, \; Q(3) : 25 \text{ is prime}.$$

$$P(5) : 21 \text{ is prime}, \; Q(5) : 121 \text{ is prime}.$$

Here, $P(2) \Rightarrow Q(2)$ and $P(5) \Rightarrow Q(5)$ are true, but $P(3) \Rightarrow Q(3)$ is false.

Theorem 2.25. There is a logical equivalence $P \Rightarrow Q \equiv (\sim P) \vee Q$, as demonstrated by the following truth table:

P	Q	$P \Rightarrow Q$	$\sim P$	$(\sim P) \vee Q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Therefore, there is also a logical equivalence $\sim (P \Rightarrow Q) \equiv P \wedge (\sim Q)$.

Theorem 2.26. There is a logical equivalence $P \Rightarrow Q \equiv (\sim Q) \Rightarrow (\sim P)$ - the latter statement is called the **contrapositive**.

2.5 The Biconditional

Definition 2.27. For statements or open sentences P, Q, the implication $Q \Rightarrow P$ is called the **converse** of $P \Rightarrow Q$. Note that if $P \Rightarrow Q$, it is not necessarily true that $Q \Rightarrow P$. For example, the true statement "If 57 is prime, then 3 is odd" has false converse "If 3 is odd, then 57 is prime."

For statements or open sentences P and Q, the conjunction

$$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$$

is called the **biconditional**, denoted $P \Leftrightarrow Q$. We say this as **"P is equivalent to Q"** or **"P if and only if Q"**. It has truth table:

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

It follows that $P \Leftrightarrow Q$ is true only when P and Q have the same truth values.

Example 2.28. (a) The biconditional "3 is an odd integer if and only if 57 is prime" is false, but the biconditional "100 is even if and only if 101 is prime" is true. Furthermore, "5 is even if and only if 4 is odd" is also true.

(b) Consider the open sentences $P_1(x) : x = 3$ and $P_2(x) : |x| = 3$ over the domain $\mathbb{R}$. The implication

$$P_1(x) \Rightarrow P_2(x) : \text{If } x = -3, \text{ then } |x| = 3,$$

is true for all $x \in \mathbb{R}$. However, the converse:

$$P_2(x) \Rightarrow P_1(x) : \text{If } |x| = 3, \text{ then } x = -3$$

is false when $x = 3$, since $P_2(3)$ is true and $P_1(3)$ is false. Hence, the biconditional

$$P_1(x) \Leftrightarrow P_2(x) : x = -3 \text{ if and only if } |x| = 3$$

is false when $x = 3$ and true for all other numbers x.

Negating the biconditional is rather lengthy but follows by definitions and DeMorgan's laws.

Theorem 2.29. $\sim (P \Leftrightarrow Q) \equiv (P \wedge (\sim Q)) \vee (Q \wedge (\sim P))$

Returning to logical equivalences, one may note that if R and S are two compound statements which are logically equivalent, then $R \Leftrightarrow S$ is a tautology, that is, it's always true.

2.6 Quantified Statements

We can convert open sentences into statements in ways other than substituting values for variables via quantification.

Definition 2.30. Let $P(x)$ be an open sentence over a domain S. Adding the phrase "**For all** $x \in S$" to $P(x)$ produces a statement called a **quantified statement**. The phrase "for all" is referred to as the **universal quantifier** and is denoted by the symbol $\forall$, and is writ in shorthand by

$$\forall x \in S, P(x)$$

and is written in words with

$$\text{For all } x \in S, P(x).$$

The quantified statement is false if $P(x)$ is false for at least one element $x \in S$.

Example 2.31. If $P(x)$ is the sentence "x is positive" and $S = \mathbb{N}$, adding "for all" gives "For all $x \in \mathbb{N}$, x is positive," which is false, since 0 is not positive. If we change $S = \mathbb{N}^+$, the quantified statement is true.

Definition 2.32. Another quantified statement can be created by adding the phrase "**there exists**", called the **existential quantifier**, to a open sentence $P(x)$, denoted $\exists$. In shorthand, this is written

$$\exists x \in S, P(x)$$

and is written in words with

$$\text{There exists } x \in S \text{ such that } P(x).$$

This is true if $P(x)$ is true for one or more $x \in S$.

Example 2.33. If $P(x)$ is the sentence "x is a solution to $x^2 + 1 = 0$" and $S = \mathbb{R}$, then adding "there exists" produces "There exists an $x \in \mathbb{R}$ such that $x^2 + 1 = 0$" which is false. If we change $S = \mathbb{C}$, then the produced quantified statement is true.

Theorem 2.34. Negation of the quantified statements produces the following equivalences:

- $\sim (\forall x \in S, P(x)) \equiv \exists x \in S, (\sim P(x))$
- $\sim (\exists x \in S, P(x)) \equiv \forall x \in S, (\sim P(x))$

We think of this as follows, if $\forall x \in S, P(x)$ is false, then there must exist some x such that $P(x)$ is false, a counterexample to the claim. Similarly, if $\exists x \in S, P(x)$ is false, then we can't find any x making $P(s)$ true, hence, it must be true that for all $x \in S, P(x)$ is false.

Example 2.35. (a) Let $A = \{1, 2, 3\}$ and $\mathcal{P}(A) = S$. Then the quantified statement

$$\text{For all sets } B \in \mathcal{P}(A), A - B \neq \varnothing$$

is false since the subset $B = A$ satisfies $A - B = \varnothing$. We negate this as follows:

$$\text{There exists } B \in \mathcal{P}(A) \text{ such that } A - B = 0,$$

and this is true, again since $B = A$ demonstrates this. We can think of negating a "for all" negation as "finding a counterexample."

(b) Consider the statement

$$\text{There exists a real number } x \text{ such that } x^2 = -1$$

which is false. The negation is

$$\text{For every real number } x,\ x^2 \neq -1$$

which is true, as every real number has non-negative square. We can think of an "exists" negation as "proving the opposite."

Remark 2.36. More generally, open sentences can be turned into quantified statements by adding quantifiers to each variable - be careful that order matters. Moreover, equivalence of negations can be found by negating the sentence and "switching the quantifier" for each quantifier present and keeping the order of variables and quantifiers. We illustrate with an example:

Example 2.37. (a) Consider the open sentence

$$Q(x, y) : x + y \text{ is prime}$$

where x has domain $S = \{3, 5, 7\}$ and y has domain $T = \{2, 6, 8, 12\}$. The quantified statement

$$\exists x \in S, \forall y \in T, Q(x, y)$$

expressed in words is

$$\text{There exists some } x \in S \text{ such that for every } y \in T,\ x + y \text{ is prime.}$$

For $x = 5$ this is true - 5+12, 5+6, 5+8, 5+12 are prime. We negation is as follows: notice that $\forall y \in T, Q(x, y)$ is itself a sentence, and $\exists p \in S$ is a quantifier. Therefore, we compute the negation in parts:

$$\sim (\exists x \in S, \forall y \in T, Q(x, y)) \equiv \forall x \in S, \sim (\forall y \in T, Q(x, y)) \equiv \forall x \in S, \exists y \in T, (\sim Q(x, y))$$

In words, this is

$$\text{For all } x \in S, \text{ there exists a } y \in T \text{ such that } x + y \text{ is not prime.}$$

(b) Consider the open sentence

$$P(x, y) : xy \text{ is odd,}$$

where $x, y \in \mathbb{N}$. Then the quantified statement

$$\forall x \in \mathbb{N}, \exists y \in N, Q(x, y)$$

expressed in words is

For all positive integers x, there exists a positive integer y such that xy is odd.

This statement turns out to be false, if $x = 0$ then no integer y satisfies $0y$ is odd. The negation of this statement is

$$\exists x \in N, \forall y \in N, (\sim Q(x, y))$$

which is words is

There exists a positive integer x such that for all positive integers y, xy is not odd.

Definition 2.38. A modification we can make to the existential quantifier is as follows, we add **"There exists a unique"** and denote this $\exists!$. This is the **uniqueness quantifier**, and for a statement $\exists! x \in S : P(x)$, it is true only when there is exactly one $x \in S$ such that $P(x)$ is true.

Example 2.39. The statement "there exists a unique $x \in \mathbb{Z}$ such that $x^2 = 9$" is false, as there exist two values x such that $x^2 = 9$, 3 and -3. The statement "there exists a unique $x \in \mathbb{Z}$ such that $x^2 = 8$ is also false, since there do not exist any $x \in Z$ such that $x^2 = 8$. However, the statement "there exists a unique $x \in \mathbb{Z}$ such that $x^2 = 0$" is true, since only $x = 0$ satisfies $x^2 = 0$.

2.7 Characterization of Statements

Recall the biconditional "if and only if", sometimes written by mathematicians as "**iff**." Recall that if we see $P$iff$Q$, we mean "$P \Rightarrow Q$ and $Q \Rightarrow P$."

Definition 2.40. Suppose some concept or object if expressed in an open sentence $P(x)$ over a domain S, and $Q(x)$ is another open sentence over S. We say $P(x)$ is **characterized** by $Q(x)$ if

$$\forall x \in S, P(x) \Leftrightarrow Q(x)$$

is a true statement.

In some sense, we can think of a characterization of some concept as an "alternative definition" of that concept, in that the alternate definition gives a concept which has exactly the same properties as before.

Example 2.41. (a) The irrational numbers are defined to be the real numbers which are not rational, that is, $\mathbb{I} := \mathbb{R} - \mathbb{Q}$. One characterization of any irrational number is that it has a nonrepeating decimal expansion, so we have a characterization,

A real number r is irrational if and only if r has a nonrepeating decimal expansion.

(b) Recall that equilateral triangles are defined as triangles whose sides are all equal. However, recall that equilateral triangles have equal angles, and conversely, any triangle which has equal angles is equilateral. Therefore we have a characterization:

"A triangle T is equilateral if and only if T has three equal angles."

3 First Proof Methods: Direct, Contrapositive, Casework

We've finally reached the main topic of this course - mathematical proofs. Initially, we are concerned with one question - given some mathematical statement, how can we show that it is true? Generally, these statements will be in the form of implications or biconditionals, e.g. "x is even if and only if $2|x$," or "if $f(x)$ is a continuous function on a compact domain, then $f(x)$ has a global maximum." Note that these are open sentences, but can be considered statements by adding the universal modifier in front implicitly. This will be elaborated on later.

Definition 3.1. A mathematical statement whose truth is accepted without proof is referred to as an **axiom.** For example, an axiom of Euclidean geometry is that for every line l and point P not on l, there is a unique line containing P which is parallel to l. Axioms are the logical foundations of mathematics.

A true mathematical statement whose truth can be verified is often referred to as a **theorem**, though usually the word theorem is reserved for particularly interesting, important, or nontrivial statements. For example "2+3=5" is not a theorem. We sometimes use the words "proposition" or "result" to characterize more basic results. A logically sound argument that a statement is true is a **proof.**

A **corollary** is a true statement whose truth can be deduced directly from some earlier theorem or result. A **lemma** is a result which is proven in order to prove some greater result, sort of like a "helping result." However, some lemmas historically have gained great significance on their own, such as Schur's Lemma in my field of Representation Theory, Burntside's Lemma in Group Theory, Yoneda's Lemma in Category Theory, or Zorn's Lemma, which can be shown is logically equivalent to the Axiom Of Choice.

3.1 Trivial and Vacuous Proofs

Nearly all implications we will encounter are quantified statements (or implicitly implied to be quantified statements), i.e. "for all x, if $P(x)$ then $Q(x)$." It is rare that $P(x)$ or $Q(x)$ are true for all $x \in S$, so whether $P(x)$ or $Q(x)$ is true ordinarily depends on which element $x \in S$ is considered. Let's recall the truth table of $\Rightarrow$:

$P(x)$	$Q(x)$	$P(x) \Rightarrow Q(x)$
T	T	T
T	F	F
F	T	T
F	F	T

Note that (or recall the logical equivalence) if $Q(x)$ is true for all $x \in S$ or $P(x)$ is false for all $x \in S$, then no matter what the other statement's truth value is, $P(x) \Rightarrow Q(x)$ is true! A situation where we can show $Q(x)$ is true for all $x \in S$ is called a **trivial proof** and a situation where we can show $P(x)$ is false for all $x \in S$ is called a **vacuous proof**. We say "this statement is trivially/vacuously true" in this instance. This is not to be confused with saying "this proof is trivial" which some mathematicians say to just say that a proof is "easily" completed by the reader. Try not to say that unless it is absolutely clear that the proof is easily completed by anyone.

Example 3.2. (a) Consider the statement "Let $n \in \mathbb{Z}$. If $n^3 > 0$, then 3 is odd." Written in symbolic form, this is $\forall n \in \mathbb{Z}, P(n) \Rightarrow Q$, where $P(n) : n^3 > 0$, and Q : "three is odd." A trivial proof here consists of only observing that 3 is an odd integer.

(b) Let's prove the following: "Let $x \in \mathbb{R}$. If $x < 0$, then $x^2 + 1 > 0$."

Proof. Since $x^2 \geqslant 0$ for all $x \in \mathbb{R}$, it follows that

$$x^2 + 1 > x^2 \geqslant 0.$$

Hence $x^2 + 1 > 0$, so the implication is true. □

Note that we end the proof with a box - this is standard notation for denoting a proof is complete. If we write out the statement as "$\forall x, P(x) \Rightarrow Q(x)$", we've demonstrated $Q(x)$ is always true, hence the implication is true.

(c) Let's prove: "Let $x \in \mathbb{R}$. If $x^2 - 2x + 2 \leqslant 0$, then $x^3 \geqslant 8$.

Proof. First observe that

$$x^2 - 2x + 1 = (x^2 - 1)^2 \geqslant 0.$$

Hence $x^2 - 2x + 2 = (x - 1)^2 + 1 \geqslant 1 > 0$. Thus $x^2 - 2x + 2 \leqslant 0$ is false for all $x \in \mathbb{R}$, so the implication is true. □

If we write out the statement as $\forall x, P(x) \Rightarrow Q(x)$, we've demonstrated $P(x)$ is false, hence the implication is true.

Trivial or vacuous proofs occur very rarely in mathematics, but it is important to understand their significance logically.

3.2 Direct Proofs

Typically if we have a statement $P(x) \Rightarrow Q(x)$ (implicitly implying the quantifier) we wish to prove, there is some connection between $P(x)$ and $Q(x)$, that is the truth value of $Q(x)$ depends on the truth value of $P(x)$. These are the mathematically and logically interesting statements we will be working with.
If it is our goal to show $P(x) \Rightarrow Q(x)$, then if $P(x)$ is false for some $x \in S$, we know the implication is vacuously true. Therefore, we only need to concern ourselves with the values of x where $P(x)$ is true - namely, the only concern is that $Q(x)$ may be false. To prove the implication then, we *assume* $P(x)$ is true for some *arbitrary* $x \in S$, and show that $Q(x)$ must be true as well for this element x. This method of proof is the most common in mathematics, it is a **direct proof**.

Gaining skill at these proofs simply takes practice, but seeing examples of proof strategies, that is, plans of attack, can help. Additionally, performing proof analysis in post can help us improve our proofwriting abilities. Let's go through examples:

Example 3.3. (a) Let's prove the statement "If n is an odd integer, then $3n + 7$ is an even integer."

Proof. Recall an even integer is an integer a which can be expressed as $a = 2b$ for some integer b. Assume that n is odd, since n is odd, we may write it as $n = 2k + 1$ for some integer k. Now,

$$3n + 7 = 3(2k + 1) + 7 = 6k + 3 + 7 = 6k + 10 = 2(3k + 5).$$

Since $3k + 5$ is an integer, identifying b from above with $3k + 5$ demonstrates $3n + 7$ is even. □

(b) For two integers $m, n \in \mathbb{Z}$, we say m **divides** n, written $m \mid n$, if $n = mk$ for some integer k. For example, $4 \mid 48$, $-3 \mid 27$, and $-101 \mid 0$. Let us prove the statement "For 3 integers a, b, c, if $a \mid b$ and $b \mid c$, then $a \mid c$."

Proof. Since $a \mid b$, we may write $b = ax$ for some integer x, and since $b \mid c$, we may write $c = yb$ for some integer y. Therefore, $c = y(ax) = (xy)a$, and since xy is an integer, we conclude $a \mid c$. □

(c) Let's prove the statement "Let $a, b, c, x, y \in Z$. If $a|b$ and $a|c$, then $a|(bx + cy)$."

Proof. Assume $a|b$ and $a|c$, then we may write $b = ar$ and $c = as$ for some $r, s \in \mathbb{Z}$. Then,

$$bx + cy = (ar)x + (as)y = a(rx + sy).$$

Since $rx + sy$ is an integer, $a|(bx + cy)$ as desired. □

(d) Let's prove the statement "For all sets A, B, $A - B = A \cap \overline{B}$." Note that there is no implication here other than assuming A, B are sets. We simply need to show that the sentence is true with that assumption. Recall we show sets are equal by showing they contain each other.

Proof. We prove this by showing $A - B \subseteq A \cap \overline{B}$, then by showing $A - B \supseteq A \cap \overline{B}$. Let $x \in A - B$. Then $x \in A$ and $x \notin B$. Since $x \notin B$, it follows $x \in \overline{B}$, and since $x \in A$, $x \in A \cap \overline{B}$. Thus, $A - B \subseteq A \cap \overline{B}$.

Now suppose $y \in A \cap \overline{B}$. Let $y \in A \cap \overline{B}$, it follows that $y \in A$ and $y \in \overline{B}$, and this implies $y \notin B$. Now because $y \in A$ and $y \notin B$, we conclude that $y \in A - B$, and thus, $A \cap \overline{B} \subseteq A - B$. Since both sets are subsets of each other, they must be equal. □

(e) Let's prove the statement "If $x, y \in \mathbb{R}$, then $x^2 + y^2 \geqslant 2xy$."

Proof. Recall for any $r \in \mathbb{R}$ that $r^2 \geqslant 0$. Identify r with $(x-y)$, so we have $(x-y)^2 \geqslant 0$. This expands to $x^2 - 2xy + y^2 \geqslant 0$, and adding $2xy$ to each side of the inequality completes the proof. □

For this proof it may have not been obvious to begin with the statement $(x - y)^2 \geqslant 0$. Sometimes, it helps to begin with what we want to show, and work backwards. Working backwards doesn't necessarily constitute a proof, but it can give us a good idea of what we need to do.

3.3 Proof by Contrapositive

Recall that the implication $P \Rightarrow Q$ is logically equivalent to its **contrapositive** $(\sim Q) \Rightarrow (\sim P)$. This gives us an alternative way of proving statements of the form $\forall x \in S : P(x) \Rightarrow Q(x)$, by proving $\forall x \in S : (\sim Q(x)) \Rightarrow (\sim P(x))$ instead - this is a **proof by contrapositive**.

Example 3.4. Let's prove, "Let $x \in \mathbb{Z}$. If $5x - 7$ is even, then x is odd."

Proof. We prove the contrapositive, "if x is even, then $5x - 7$ is odd." If x is even, then $x = 2k$ for some $k \in \mathbb{Z}$. Then $5(2k) - 7 = 10k - 7 = 2(5k - 4) + 1$, hence $5x - 7$ is odd. □

So far, we have been only proving implications, rather than biconditionals. However, proving a biconditional statement isn't much different, if we have a biconditional $\forall x \in S, P(x) \Leftrightarrow Q(x)$, this is equivalent to proving $\forall x \in SP(x) \Rightarrow Q(x)$ and $\forall x \in S, Q(x) \Rightarrow P(x)$. Sometimes, it is easier to prove the contrapositive of one of these statements, so we instead show, $\forall x \in S, P(x) \Rightarrow Q(x)$ and $\forall x \in S, (\sim P(x)) \Rightarrow (\sim Q(x))$.

Example 3.5. Let's prove, "Let $x \in \mathbb{Z}$. Then x^2 is even if and only if x is even."

Proof. ($\Leftarrow$) First, we show x is even implies x^2 is even. Let $x = 2k$, then $x^2 = 4k^2 = 2(2k^2)$, hence x^2 is even. ($\Rightarrow$) We show the contrapositive, that is, if x is odd, then x^2 is odd. Let $x = 2k + 1$, then $x^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, hence x^2 is odd. □

Note that I am being terse here by not specifying that k is an integer, however it is clear by the usage at this point that it is, so it is an acceptable omission of clarity.

3.4 Proof by Cases

Sometimes when we're giving a proof of a mathematical statement concerning some $x \in S$, it helps to note that x can have some sort of property which defines a subset of S, for example, "x even" and "x odd" make up two subsets of $\mathbb{Z}$, and "x positive," "x negative," and "$x = 0$" make up three. If we can verify the truth of the statement for each possible property that x can have, we have a proof of the statement. Such a proof is divided into **cases**, each case corresponding to a property x can have. This is a **proof by cases**. This is a vague description, but some examples should help.

Example 3.6. (a) If $n \in \mathbb{Z}$, then $n^2 + 3n + 5$ is odd.

Proof. We proceed by cases, corresponding to if n is even or odd. If n is even, then suppose $n = 2x$. We have:

$$n^2 + 3n + 5 = (2x)^2 + 3(2x) + 5 = 4x^2 + 6x + 5 = (2(2x^2 + 3x + 2) + 1.$$

Hence, $n^2 + 3n + 5$ is odd.

If n is odd, then let $n = 2y + 1$. Then,

$$\begin{aligned} n^2 + 3n + 5 &= (2y + 1)^2 + 3(2n + 1) + 5 \\ &= 4y^2 + 10y + 9 \\ &= 2(2y^2 + 5y + 4) + 1 \end{aligned}$$

Hence, $n^2 + 3n + 5$ is odd. Since we have satisfied all cases for n, we are done. □

(b) Let $x, y \in \mathbb{R}$. $xy = 0$ if and only if $x = 0$ or $y = 0$.

Proof. ($\Leftarrow$) The reverse direction is obvious.

($\Rightarrow$) Suppose $xy = 0$. We consider two cases, if $x = 0$ or if $x \neq 0$. If $x = 0$ then we are done. Otherwise, if $x \neq 0$, then $1/x$ is a real number. Therefore multiplying the equality $xy = 0$ by $1/x$ on each side yields the equality $y = 0$, as desired. □

Sometimes, we may omit casework that involves assigning cases to different variables which play out identically (it will become clear what this means with an example) - when we do this, we write **without loss of generality**, or WLOG for short.

Example 3.7. Let $x, y \in \mathbb{Z}$. If $3 \nmid xy$, then $3 \nmid x$ and $3 \nmid y$.

Proof. We prove the contrapositive, which is, "If $3 \mid x$ or $3 \mid y$, then $3 \mid xy$. Suppose **without loss of generality** that $3 \mid x$. Then $x = 3z$ for some z, so $xy = (3z)y = 3(zy)$, hence $3 \mid xy$. □

Here, we omitted the case where $3 \mid y$ because it would follow in the exact same manner as before, only with reversed variables. Be careful to not abuse the power of WLOG and cut out cases which may actually play out differently! Usually the only time WLOG is usable is when we are given a scenario like "a or b has some property."

Proofs involving sets very frequently involve casework. Sometimes the casework is unavoidable but sometimes, we can exploit symmetry to use WLOG.

Example 3.8. (a) For every two sets A and B,

$$(A \cup B) - (A \cap B) = (A - B) \cup (B - A)$$

Proof. ($\subseteq$) Suppose $x \in (A \cup B) - (A \cap B)$. Then $x \in A \cup B$ and $x \notin A \cap B$. Therefore, either $x \in A$ or $x \in B$. Without loss of generality, we can assume $x \in A$. Since $x \notin A \cap B$, we have $x \notin B$. Therefore, $x \in A - B$, and hence, $x \in (A - B) \cup (B - A)$. Hence,

$$(A \cup B) - (A \cap B) \subseteq (A - B) \cup (B - A)$$

($\supseteq$) Now, suppose $x \in (A - B) \cup (B - A)$. Then, either $x \in (A - B)$ or $x \in (B - A)$, without loss of generality, say $x \in (A - B)$. Therefore, $x \in A$ and $x \notin B$. So $x \in A \cup B$, but $x \notin A \cap B$. Therefore, $x \in (A \cup B) - (A \cap B)$, and hence

$$(A \cup B) - (A \cap B) \supseteq (A - B) \cup (B - A)$$

as desired. □

Note that we can end the proof with an "as desired" rather than restating the conclusion if it is obvious enough what the conclusion is.

We finish with an important theorem concerning real numbers. (draw a picture)

Theorem 3.9. (The Triangle Inequality). For every two numbers x, y,

$$|x + y| \geqslant |x| + |y|$$

Proof. Since $|x + y| = |x| + |y|$ if either x, y are 0, then we can assume x and y are nonzero. We proceed by cases.

(a) $x > 0$ and $y > 0$. Then $x + y > 0$, so $|x + y| = x + y = |x| + |y|$.

(b) $x < 0$ and $y < 0$. Then $x + y < 0$, so $|x + y| = -(x + y) = (-x) + (-y) = |x| + |y|$.

(c) x, y have opposite sign, suppose without loss of generality that $x > 0$ and $y > 0$. We consider two subcases.

  (a) $x + y \geqslant 0$. Then,

$$|x| + |y| = x + (-y) = x - y > x + y = |x + y|$$

  (b) $x + y \leqslant 0$. Then

$$|x| + |y| = x + (-y) = x - y > -x - y = -(x + y) = |x + y|$$

Thus, $|x + y| \leqslant |x| + |y|$ for all $x, y \in \mathbb{R}$. □

3.5 Introduction to Modular Arithmetic

We now briefly diverge our study of proof techniques to introduce a method of characterizing numbers that is preserved under various operations such as addition, multiplication, and raising to powers. These will give rise to plenty of opportunities for straightforward proofs to practice on.

As a motivating example, consider two integers x, y which are the same **parity**, that is, they are both odd or both even. It follows that $2 \mid (x - y)$, that is, their difference is even. Consequently, $2 \mid (x - y)$ if and only if x and y have the same remainder divided by two.

Or considering 3 instead of 2, any integer can be expressed as $3q, 3q + 1, 3q + 2$ for some integer q, based on what its remainder is when divided by 3. If two integers x, y have the same remainder when divided by 3, it follows that $3 \mid (x - y)$. This may be generalized for numbers $n \geqslant 2$.

Definition 3.10. Given two integers a, b and an integer $n \geqslant 2$, we say a **is congruent to** b **modulo** n if $n \mid (a - b)$. We express this as $a \equiv b \mod n$. For example, $4 \equiv 7 \mod 3$, as $3 \mid (7 - 4)$. Doing arithmetic under modular number systems is known as **modular arithmetic**.

Note that every integer x is equivalent to some number $0 \leqslant k \leqslant n$ modulo n, so when working modulo n, it suffices to only consider naturals less than n, and we generally only express numbers in this way. For example, with $n = 4$, every integer satisfies $x \equiv 0, 1, 2, 3 \mod 4$. So we would write $2 \cdot 3 \equiv 2 \mod 4$, since $6 \equiv 2 \mod 4$.

Let's go over some fundamental properties of modular arithmetic, with proofs attached. We will often use these properties in the future, which will eliminate the need to consult the definition of modulo, but for these first few proofs, everything will be proven via definition.

Proposition 3.11. Let $a, b, k, n \in \mathbb{Z}$ with $n \geqslant 2$. If $a \equiv b \mod n$, then $ka \equiv kb \mod n$.

Proof. Let $a \equiv b \mod n$. Then $n \mid (a-b)$, so $a-b = nx$ for some integer x. Therefore,

$$ka - kb = k(a-b) = k(nx) = n(kx).$$

Therefore, $n \mid (ka - kb)$ and hence, $ka \equiv kb \mod n$. □

We may prove using essentially the same proof that if $a \equiv b \mod n$, then $a + k \equiv b + k \mod n$. However, these two facts don't necessarily allow us to add numbers of different integral value but same modular value. For example, if we have $1 \equiv 4 \mod 3$, then $1+2 \equiv 4+2 \mod 3$, but it is not necessarily true yet that $1 + 2 \equiv 4 + 5 \mod 3$, despite $2 \equiv 5 \mod 3$.

Fortunately, the next two theorems will assert that essentially, we can perform addition and multiplication in modular arithmetic without any concern.

Theorem 3.12. Let $a, b, c, d, n \in \mathbb{Z}$, and $n \geqslant 2$. If $a \equiv b \mod n$ and $c \equiv d \mod n$, then $a + c \equiv b + d \mod n$.

Proof. Assuming the statement, we have $n \mid a - b$ and $n \mid c - d$, so we may write $a - b = nx$ and $c - d = ny$ for some integers x, y. Adding these equalities obtains:

$$(a-b) + (c-d) = nx + ny$$

and so

$$(a+c) - (b+d) = n(x+y).$$

Therefore, $n \mid (a+c) - (b+d)$, as desired. □

Theorem 3.13. Let $a, b, c, d, n \in \mathbb{Z}$, and $n \geqslant 2$. If $a \equiv b \mod n$ and $c \equiv d \mod n$, then $ac \equiv bd \mod n$.

Before we proceed, let's note that we may need a different strategy. If we multiply $(a-b)(c-d)$, we obtain $ac + bd - bc - ad$, which are more terms than we want to have to show that $ac \equiv bd \mod n$.

Proof. Assuming the hypothesis, we have $a - b = nx$ and $c - d = ny$ for some $x, y \in \mathbb{Z}$. Thus $a = b + nx$ and $c = d + ny$. Multiplying these two equations yields:

$$ac = (b + nx)(d + ny) = bd + dnx + bny + n^2xy = bd + n(dx + by + nxy)$$

Thus, $n \mid ac - bd$, so $ac \equiv bd \mod n$, as desired. □

These last two theorems essentially tell us that in doing arithmetic, it is always okay to simplify computations down to integers less than n. We will come back to modular arithmetic after introducing a few more proof techniques.

4 More Proof Techniques: Existence, Proof by Contradiction

We next introduce some more proof techniques and a different type of statement which requires a different approach to proving, statements which require proof of existence rather than statements using the universal qualifier.

4.1 Counterexamples

Definition 4.1. Obviously, not all quantified statements of the type $\forall x \in S, R(x)$ are false. Recall that the negation of that statement is $\exists x \in S, \sim R(x)$ - such an element x is called a **counterexample** of the false statement $\forall x \in S, R(x)$, and the discovery of such a counterexample verifies the falseness of the claim. Note that if $R(x)$ is an implication, so the statement is of the form $\forall x \in S, P(x) \Rightarrow Q(x)$, then a counterexample x would be such an x for which $P(x)$ is true but $Q(x)$ is false.

From now on, some problems will now be presented in "prove or disprove" fashion. While many of these problems will be disprovable with a counterexample, some of them will be true! This is to help build and test your mathematical intuition.

Example 4.2. Prove or disprove: "If $x \in \mathbb{R}$, then $(x^2 - 1)^2 > 0$"

Proof. The above statement is false. Choosing $x = 1$ gives $(1^2 - 1)^2 = 0$. □

Example 4.3. Prove or disprove: "If x is a real number, then $\tan^2 x + 1 = \sec^2 x$."

One may recall this equality from a precalculus course. Does this mean it is true?

Proof. The above statement is false. If $x = \pi/2$, then both $\tan \pi/2$ and $\sec \pi/2$ have no numerical value, and hence, the given equality cannot hold. □

However, the statement is true if one rewrites the statement as follows: "If $x \in R$, then if both $\tan x$ and $\sec x$ have numerical value, then $\tan^2 x + 1 = \sec^2 x$." The proof is left as an exercise (hint: $\sin^2 x + \cos^2 x = 1$)

Example 4.4. Prove or disprove: Let a, b be nonzero real numbers. If $x, y \in \mathbb{R}^+$, then:

$$\frac{a^2}{2b^2}x^2 + \frac{b^2}{2a^2}y^2 > xy.$$

Sometimes, it helps to play around with a problem statement if we don't know if a statement is obviously true or false.

Proof. First, we multiply the inequality by $2a^2b^2$ to eliminate all fractions, obtaining

$$a^4x^2 + b^4y^2 > 2a^2b^2xy \Leftrightarrow a^4x^2 - 2a^2b^2xy + b^4y^2 > 0$$

Note we may factor this to

$$(a^2x - b^2y)^2 > 0.$$

Choosing $x = b^2$ and $y = a^2$ demonstrates that the statement is false. □

As demonstrated in the proof, the statement is true if we replace the $>$ with a $\geqslant$. A well-written proof can do more than just demonstrate something is true or false, but rather, some of the inner workings of the problem.

Note that in the previous problems that most arithmetic manipulation of an expression gives rise to logically equivalent statements. However, note that some operations are non-reversible, such as squaring.

4.2 Proof by Contradiction

If we have an statement R we wish to show is true, we already have two methods, direct proof and contrapositive proof (I am now considering proof by cases a type of direct proof). We now introduce a new method which can sometimes be the path of least resistance for some problems.

Suppose we assume R is false, and from this assumption, we reach a statement that contradicts some assumption we made in the proof or some other known fact. If we call this fact P, then we have deduced $C = P \wedge (\sim P)$, establishing the truth of the implication $(\sim R) \Rightarrow C$. The only way this can be true is if $(\sim R)$ is false, that is, R is true. This technique is called a **proof by contradiction**. We often begin by writing

Suppose for contradiction that R is false.

If R is a quantified statement $\forall x \in S, P(x) \Rightarrow Q(x)$, a proof by contradiction consists of verifying the implication

$$\sim (f\forall x \in S, P(x) \Rightarrow Q(x)) \Rightarrow C$$

for some contradiction C. However, recall the logical equivalence

$$\sim (f\forall x \in S, P(x) \Rightarrow Q(x)) \equiv \exists x \in S, (P(x) \wedge (\sim Q(x)),$$

so a proof by contradiction begins by assuming there exists some element $x \in S$ for which $P(x)$ is true but $Q(x)$ is false. We would begin by writing

Suppose for contradiction that there exists some x for which $P(x)$ is true and $Q(x)$ is false.

Let's see some examples!

Example 4.5. Prove that there is no smallest positive real number.

Proof. Suppose for contradiction that there is a smallest real number r. Then $0 < r/2 < r$, which contradicts r being the smallest real number. □

Example 4.6. If a is an even integer and b is an odd integer, then $4 \nmid (a^2 + 2b^2)$.

Proof. Suppose for contradiction that a is even, b is odd, and $4 \mid (a^2 + 2b^2)$. Let $a = 2x, b = 2y + 1$, and $a^2 + 2b^2 = 4z$ for some integers x, y, z. Then,

$$a^2 + 2b^2 = (2x)^2 + 2(2y + 1)^2 = 4z$$

Simplifying obtains $4x^2 + 8y^2 + 8y + 2 = 4z$, or equivalently,

$$2 = 4z - 4x^2 - 8y^2 - 8y = 4(z - x^2 - 2y^2 - 2y)$$

This implies $4 \mid 2$, which is impossible. □

A divisibility statement can often be reworded into a statement about modular arithmetic. We could also prove this via modular arithmetic, as the statement is equivalently saying that $a^2 + 2b^2 \not\equiv 0 \mod 4$.

Proof. We wish to show that $a^2 + 2b^2 \not\equiv 0 \mod 4$. Observe that if a is even, then $a^2 \equiv 0 \mod 4$, and if b is odd, then $b^2 \equiv 1 \mod 4$. Then $a^2 + 2b^2 \equiv 2 \mod 4$, as desired. □

Let's now prove an important theorem, establishing the irrationality of $\sqrt{2}$.

Theorem 4.7. $\sqrt{2}$ is irrational.

Proof. Suppose for contradiction that $\sqrt{2}$ is rational. Express $\sqrt{2} = a/b$, where a and b are relatively prime integers. Then $2 = a^2/b^2$, so $a^2 = 2b^2$. Since b^2 is an integer, a^2 is even. Then from an earlier result, a is even as well. Therefore, we may write $a = 2k$ for some $k \in \mathbb{Z}$. Then, $(2k)^2 = 4k^2 = 2b^2$, which reduces to $2k^2 = b^2$, and thus, b^2, and therefore b, is even as well. However, this implies that 2 divides both a and b, which contradicts the fact that a and b are relatively prime. □

One may use a similar proof to show that $\sqrt{p}$ is irrational for any prime p. One may generalize to show that $\sqrt{n}$ is irrational for any nonsquare n, but it takes a bit more work. This result is a classic example where proof by contradiction is by far the easiest method of proof.

To wrap up, let's next prove a classical result, that there are infinitely many primes. The argument will be made a bit simpler by utilizing modular arithmetic.

Theorem 4.8. There are infinitely many primes.

Proof. Suppose for contradiction that there are finitely many primes, call them $p_1, \ldots, p_k$. Recall that every number may be expressed uniquely as a product of primes, so every positive integer greater than 1 must be divisible by at least one of these primes. Consider the number $n = p_1 p_2 \ldots p_k + 1$. We may observe that $n \equiv 1 \mod p_i$ for any $i \in \{1, \ldots, k\}$. Therefore, no prime divides n, a contradiction. □

4.3 Recap - Three Implication Proof Methods

To sum up the past few sections, we've covered three methods of proof when presented with a statement of the form $\forall x \in S, P(x) \Rightarrow Q(x)$. For each of these, you should know how a proof should start and what the end goal is.

- **Direct**: "Assume that there exists $x \in S$ such that $P(x)$ is true" We aim to show $Q(x)$ is true for this element x.
- **Contrapositive**: "Assume there exists $x \in S$ such that $Q(x)$ is false." We aim to show $P(x)$ is false for this element x.
- **Contradiction**: "Assume there exists $x \in S$ such that $P(x)$ is true and $Q(x)$ is false." We aim to produce a contradiction.

Some statements can be completed using any of the three techniques, while others are most easily proven using one specific technique. Generally, for statements that can be proven in any of these ways, it is considered good form to prove something directly, but there are counterexamples. Let's see an example of using proof by contradiction unnecessarily:

Example 4.9. Show that if 4 divides an integer n, then n is even.

Proof. Suppose for contradiction that n is not even. Since 4 divides n, we have $n = 4k$ for some integer k. Then $n = 2(2n)$, which is even. This is a contradiction. □

What went wrong here? The contradictory hypothesis in the first sentence was totally unnecessary - we could delete the first and last sentences and we would have an airtight proof!

4.4 Existence Proofs

For a **existence theorem**, the existence of an object is asserted. The statements are generally of the form,

$$\exists x \in S : R(x) : \quad \text{There exists } x \in S \text{ such that } R(x).$$

An existence proof may consist of simply finding some $x \in S$ for which $R(x)$ is true and demonstrating its truthness, or it may not give a specific $x \in S$ but assert its existence somehow. Many existence theorems demonstrate the existence of some object, but not which object it specifically is. For example, David Hilbert says "There is at least one student in the class for whom the following statement is true: No other student in the class has more hairs on their head than this person. Which student is it? That we shall never know, but their existence is absolutely certain."

The following example is a classic!

Example 4.10. There exist irrational numbers a and b such that a^b is rational.

Proof. Consider the number $\sqrt{2}^{\sqrt{2}}$. This number is either rational or irrational, so we consider these cases separately:

(a) If $\sqrt{2}^{\sqrt{2}}$ is rational, we are done.

(b) If $\sqrt{2}^{\sqrt{2}}$ is irrational, we consider

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^{2} = 2,$$

and we are done.

□

We don't know which choice of a, b are the proper ones for which a^b is rational, but we know beyond a shadow of a doubt that one of those two choices must work!

We state an important theorem without proof - for the proof, take real analysis.

Theorem 4.11. (Intermediate Value Theorem) If f is a function that is continuous on the closed interval $[a, b]$ and k is a number between $f(a)$ and $f(b)$, then there exists a number $c \in (a, b)$ such that $f(c) = k$.

We can use this as follows:

Example 4.12. The function $f(x) = x^5 + 2x - 5$ defined on $\mathbb{R}$ has a root between $x = 1$ and $x = 2$.

Proof. Observe that $f(1) = -2$ and $f(2) = 31$, so $f(1) < 0 < f(2)$, and therefore by the IVT, there exists some $c \in (1, 2)$ for which $f(c) = 0$, as desired. □

We haven't had much experience citing other theorems when proving things, generally at this stage of your mathematical career it doesn't hurt to restate the theorem, or at least hint at what its implication is, before using it. Generally "by [theorem]," or "[theorem] implies.." is good form.

Recall earlier when I brought up **uniquenness** statements, something of the form

$$\exists! x \in S, R(x), \quad \text{There exists a unique } x \in S \text{ such that } R(x).$$

To prove statements of this form, we must also demonstrate that x is the only element in S satisfying $R(x)$. There are a few ways of doing this.

- Assume that a, b are elements of S satisfying $R(x)$, show they are equivalent.

- Assume that a, b are *distinct* elements of S satisfying $R(x)$, produce a contradiction.
- If a is known, show that all $b \neq a \in S$ do not satisfy $R(x)$.

Example 4.13. The function $f(x) = x^5 + 2x - 5$ defined on $\mathbb{R}$ has a *unique* root between $x = 1$ and $x = 2$.

Proof. We have established existence of a root. Suppose for contradiction that $f(x)$ has two distinct roots in $(1, 2)$, a and b. Suppose without loss of generality that $1 < a < b < 2$. Recall ir $r > 1$, then $r^k > r$ for any integer $k \geqslant 2$. Therefore $a^5 + 2a - 5 < b^5 + 2b - 5$. On the other hand, $a^5 + 2a - 5 = b^5 + 2b - 5 = 0$, a contradiction. Thus $f(x)$ has a unique root in $(1, 2)$. □

Of course, not all existence statements are true. To disprove existence statements, remember the negation:

$$(\exists x \in S : R(x)) \equiv \forall x \in S : (\sim R(x))$$

Example 4.14. Prove or disprove: There is a real number x such that $x^6 + 2x^4 + x^2 + 2 = 0$.

Proof. Let $x \in \mathbb{R}$. Observe $x^6, x^4, x^2 \geqslant 0$, so

$$x^6 + 2x^4 + x^2 + 2 \geqslant 2 > 0.$$

Thus the statement is false. □

5 Induction

We now come to a new proof method, induction. Induction works when we have some infinite collection of statements that we can order, i.e. $P(1), P(2), P(3), \ldots$. To motivate the concept, let's consider the following scenario: (this would work better if we were in person, but we aren't, so here we go)

I have you all stand in a line. I every single person other than the first one to raise their hand after they see the person directly in front of them do so. Then, I tell the person first in line. What happens? Everyone raises their hand!

Mathematical induction works similarly - if we can show that $P(1)$ is true, and that $P(1)$ implies $P(2)$, $P(2)$ implies $P(3)$, and so on, then we will have that $P(n)$ is true for any n. This is just an overview, there are some technicalities which must be discussed first.

5.1 The Well-Ordered Principle & Induction

Definition 5.1. Let A be a nonempty set of real numbers. A number $m \in A$ is called a **least element** or **minimum** of A if $x \geqslant m$ for all $x \in A$. Note that if A has a least element, then this element is unique.

Example 5.2. $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ do not have a least element, but $\mathbb{N}$ does. $\mathbb{R}^+$ and $\mathbb{Q}^+$ do not have a least element, but the set $[0, \infty)$ does. In general, all closed intervals and finite unions of closed intervals have a least element, and all open intervals do not have a least element. Recall from HW1 though that it is possible for an infinite intersection of open intervals to have a least element!

Definition 5.3. A set A under a total ordering $(A, \geqslant)$ is **well-ordered** if every subset of A has a least element.

Note that being indexed by $\mathbb{N}$ or having a least element is not sufficient to be a well-ordered set.

Example 5.4.

- A set that is *not* well-ordered despite being indexed by $\mathbb{N}$ is:

$$\left\{ \frac{1}{n} : n \in \mathbb{N}^+ \right\}$$

- A set that has a least element but is not well-ordered is $\{r \in \mathbb{R} : r \geqslant 0\}$.

Theorem 5.5. (Well-Ordering Principle) $\mathbb{N}$ and any subset of $\mathbb{N}$ is well-ordered.

We can use this now to prove the validity of induction.

Theorem 5.6. (Principle of Mathematical Induction) For each positive integer n, let $P(n)$ be a statement. If

(a) $P(1)$ is true, and

(b) The implication $P(k) \Rightarrow P(k+1)$ is true for every positive k,

then $P(n)$ is true for every positive integer n.

Proof. Suppose for contradiction that the theorem is false. Then the two conditions are satisfied but there exist some positive integers n for which $P(n)$ is false. Let $S = \{n \in N : P(n) \text{ is false.}\} \subset \mathbb{N}$. It follows by the Well-Ordering Principle that S has a least element s. Since $P(1)$ is true, $s \geqslant 2$, and $s - 1 \in \mathbb{N}^+$. Therefore, $s - 1 \notin S$, so $P(s-1)$ is true. But $P(s-1) \Rightarrow P(s)$ is true, so $P(s)$ must be true as well, a contradiction! □

Remark 5.7. Therefore, the quantified statement $\forall n \in N^+$, $P(n)$ can be proven in two steps:

(a) The **Base Case**: Prove $P(1)$ is true.

(b) The **Inductive Step**: Assume $P(n)$ for some $n \geqslant 1$ (this is the **Inductive Hypothesis**) and prove $P(n+1)$ is true.

This is a **proof by induction.**

A classic example of easy proofs by induction are sum formulas (which can usually be proven in more interesting combinatorial ways). Let's see an example:

Example 5.8. Prove the following equality:

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

Proof. We proceed by induction. For $n = 1$, we see $1^2 = \frac{1 \cdot 2 \cdot 3}{6}$, so the base case $n = 1$ is satisfied. Now, assume that

$$1^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

We wish to prove that:

$$1^2 + \cdots + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}.$$

□

Remark 5.9. Note that we can retool induction if we instead have a quantified statement $\forall n \in S, P(n)$ where S is a subset of $\mathbb{Z}$ which has a least element e. In this case, the base case requires we prove $P(e)$ is true, and in the inductive step, we assume $P(n)$ is true for some $n \geqslant e$. This is the slightly more general form of induction.

Example 5.10. For every integer $n \geqslant 5$, $2^n > n^2$.

Proof. We proceed by induction. Since $2^5 > 5^2$, the base case is satisfied for $n = 5$. Now assume that $2^n > n^5$ for some $n \geqslant 5$. We show that $2^{n+1} > (n+1)^2$. Observe that

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n > 2n^2 = n^2 + n^2 \geqslant n^2 + 5n \\ &= n^2 + 2n + 3n \geqslant n^2 + 2n + 15 \\ &> n^2 + 2n + 1 = (n+1)^2 \end{aligned}$$

Thus, $2^{n+1} > (n+1)^2$, so by induction, $2^n > n^2$ for every integer $n \geqslant 5$. □

Observe that in the algebra, we used both the base case and the inductive hypothesis when simplifying, as well as the assumption that $n \geqslant 5$. Let's now see an induction proof using sets. Recall De Morgan's law which states for two sets A, B that $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Example 5.11. For any finite collection of sets $A_1, \ldots A_n$,

$$\overline{A_1 \cup \cdots \cup A_n} = \overline{A_1} \cap \cdots \cap \overline{A_n}$$

The corresponding statements P_n correspond to when there are n sets.

Proof. We proceed by induction. The base case $n = 1$ is trivial, and for $n = 2$, the result is given by De Morgan's law, and is therefore true. We now assume the result is true for $n \geqslant 2$ sets, that is,

$$\overline{A_1 \cup \cdots \cup A_n} = \overline{A_1} \cap \cdots \cap \overline{A_n}.$$

We wish to show the following:

$$\overline{A_1 \cup \cdots \cup A_n \cup A_{n+1}} = \overline{A_1} \cap \cdots \cap \overline{A_n} \cap \overline{A_{n+1}}.$$

Let $B = A_1 \cup \cdots \cup A_n$. We may write

$$\overline{A_1 \cup \cdots \cup A_n \cup A_{n+1}} = \overline{B \cup A_{n+1}}$$

Then, by De Morgan's law,

$$\overline{B \cup A_{n+1}} = \overline{B} \cap \overline{A_{n+1}}$$

By the inductive hypothesis, we also have

$$\overline{B} = \overline{A_1 \cup \cdots \cup A_n}$$

Therefore,

$$\begin{aligned} \overline{A_1 \cup \cdots \cup A_n \cup A_{n+1}} &= \overline{B \cup A_{n+1}} = \overline{B} \cup \overline{A_{n+1}} \\ &= \overline{A_1} \cap \cdots \cap \overline{A_n} \cap \overline{A_{n+1}} \end{aligned}$$

as desired. □

We wrap up this section by looking at where an inductive proof can fail. Let's consider the following statement and "prove" it:

Example 5.12. In any finite group of horses, all horses are the same color.

Proof. We proceed by induction. For $n = 1$ horse, the statement is trivial. Now let's assume that any n horses all are the same color and consider a set of $n + 1$ horses, $H_1, \ldots, H_{n+1}$. By induction, the horses $H_1, \ldots, H_n$ all are the same color, and again by induction, the horses $H_2, \ldots, H_{n+1}$ are all the same color. Therefore, horse H_{n+1} is the same color as the first n horses. Thus, all horses are the same color. □

But obviously, this cannot be true. Where is the hole in the proof? We used the inductive hypothesis correctly... (give the class a moment to think). The issue arises in our base case, and that our inductive step proof only works when we have $n \geqslant 2$ horses or more! In the case when $n + 1 = 2$, the two sets do not overlap, so the inductive step does not work! Therefore we also need to provide a base case for $n = 2$ horses - but this is clearly impossible. The lesson here is as follows: *make sure your inductive step works in generality for any n - and for any cases that do not, include them in your base cases.*

5.2 Proof by Minimum Counterexample

Some statements of the form we've been proving, that is, $\forall n \in N, P(n)$, are not well-suited to be proven by induction. However, there is another technique we can utilize which utilizes the well-orderedness of the naturals and contradiction. We begin by supposing that $\forall n \in N, P(n)$ is false - then there must exist some positive integers k for which $P(k)$ is false. By the well-ordered principle, there must exist a *smallest* positive integer k for which $P(k)$ is false, and for any $1 \leqslant i < k$, $P(i)$ is true. This integer k is called a **minimum counterexample** of the statement. We now have a wealth of possibilities to find a contradiction, some include

- Deducing that there exists some $i < m$ for which $P(i)$ is false, contradicting minimality of m.
- Showing that $P(m)$ is also true, using the fact that $P(i)$ is true for $i < m$.

Let's illustrate with an example:

Example 5.13. For every positive integer n,

$$6 \mid (n^3 - n)$$

Proof. Suppose for contradiction there are positive integers n for which $6 \nmid n^3 - n$. Then there is a smallest positive integer n for which the statement is false, label it m. We now check some small cases:

- For $n = 1$, $6 \mid 1^3 - 1$.

- For $n = 2$, $6 \mid 2^3 - 2$.

Therefore $m \geqslant 3$, so we may write $m = k + 2$ for some other $k \in \mathbb{N}^+$. Observe now that:

$$\begin{aligned} m^3 - m &= (k+2)^3 - (k+2) = (k^3 + 6k^2 + 12k + 8) - (k+2) \\ &= (k^3 - k) + 6(k^2 + 2k + 1) \end{aligned}$$

Recall the general fact that if $n \mid x$ and $n \mid y$, then $n \mid (x + y)$. The contrapositive of this statement is that if $n \nmid (x + y)$, then $n \nmid x$ or $n \nmid y$. Applying this here, we have that since $6 \nmid (m^3 - m)$, but $6 \mid 6(k^2 + 2k + 1)$, it must follow that $6 \nmid (k^3 - k)$. However, this contradicts the fact that m was the *minimum counterexample*, thus proving that $6 \mid (n^3 - n)$ for all positive n. □

Let's also note that this could also be proven via modular arithmetic:

(sketch). The statement $6 \mid (n^3 - n)$ is equivalently stating that $n^3 \equiv n \mod 6$ for all positive integers n. Therefore, it suffices to check the statement $n \equiv 0, 1, \ldots, 5$, which is easily performed. □

This statement could also be proven using strong induction, which will be introduced next section. One final question would be asking how we knew to substitute $m = k + 2$ rather than $m = k + 1$ - the answer I would give to this isn't the most enlightening - if we try $k + 1$ instead, this could also work, but one additional step would be verifying that $k(k + 1)$ is even. It is, but it's extra work and the $k + 2$ substitution is simply more fluid.

Example 5.14. For every nonnegative integer n,

$$3 \mid \left(2^{2n} - 1\right)$$

Proof. Suppose for contradiction there are nonnegative integers for which the above does not hold. Then there exists a smallest nonnegative integer m for which $3 \nmid 2^{2m} - 1$. Therefore, $3 \mid 2^{2n} - 1$ for all $0 \leqslant n < m$. Since $3 \mid 2^{2 \cdot 0} - 1$, it follows that $m \geqslant 1$, so we may write $m = k + 1$. By minimality of m, we have $3 \mid 2^{2k} - 1$, so $2^{2k} - 1 = 3x$ for some integer x. Consequently, $2^2k = 3x + 1$. Now, observe that

$$\begin{aligned} 2^{2m-1} &= 2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 2^2 \cdot 2^{2k} - 1 \\ &= 4(3x + 1) - 1 = 12x + 3 = 3(4x + 1) \end{aligned}$$

This implies $3 \mid 2^{2m} - 1$, which is absurd. □

In the first proof, we contradicted minimality of m, while in the second, we contradicted the fact that m was a counterexample. Sometimes one strategy is easier than the other, while other times, either can be used! Remember though - if possible, a proof is best performed direct. This shouldn't discourage you from attempting this strategy, but rather, after completing a proof by minimum counterexample, it may be wise to check if in your proof, you can eliminate the need for it and turn your proof into a direct induction proof.

5.3 Strong Induction

We finish with a stronger form of induction, aptly named the Strong Form of Induction

Theorem 5.15. (**The Strong Principle of Mathematical Induction**) For each positive integer n, let $P(n)$ be a statement. If

(a) $P(1)$ is true and

(b) the implication

$$\text{If } P(i) \text{ for every integer } i \text{ with } 1 \leqslant i \leqslant n, \text{ then } P(n+1)$$

is true for every positive integer n,

then $P(n)$ is true for every positive integer n.

The only significant difference between the previous form of induction and strong induction lies in the inductive hypothesis - previously we only assumed $P(n)$ to show $P(n+1)$ is true, but here we assume all of $P(1), \cdots P(n)$ are true. As before, we can also generalize - we do not have to iterate over $\mathbb{N}$, we can work over any subset of $\mathbb{Z}$ which has a least element.

A classic example of mathematical statements which are provable by strong induction are **recursive sequences** such as the Fibonacci sequence, that is, sequences where after the first few terms, the rest of the series is defined recursively via a **recurrence relation** such as $a_{n+1} = a_n + a_{n-1}$. Let's look at some examples.

Example 5.16. Consider the sequence $\{a_n\}$ with $a_1 = 1$, $a_2 = 4$, and $a_n = 2a_{n-1} - a_{n-2} + 2$ for $n \geqslant 3$. Conjecture a formula for a_n and prove your conjecture is correct.

Playing around with this sequence, we see $a_3 = 2 \cdot 4 - 1 + 2 = 9$, and $a_4 = 2 \cdot 9 - 4 + 2 = 16$. It seems like the pattern is that $a_n = n^2$ - let's prove it.

Proof. We wish to show $a_n = n^2$ for all $n \geqslant 1$. The base cases $n = 1$ and $n = 2$ are given to be true. Suppose the formula holds true for $1, 2, \cdots n$. Then we have

$$\begin{aligned} a_{n+1} &= 2a_n - a_{n-1} + 2 = 2n^2 - (n-1)^2 + 2 \\ &= 2n^2 - (n^2 - 2n + 1) + 2 = n^2 + 2n + 1 = (n+1)^2 \end{aligned}$$

Thus by strong induction, $a_n = n^2$ for all $n \in \mathbb{N}$. □

5.4 The Fibonacci Numbers

Definition 5.17. The **Fibonacci Numbers** F_n are defined by $F_1 = 1, F_2 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for $n \geqslant 1$.

The Fibonacci numbers have some incredible patterns (no, not the ones that "occur in nature," that's nothing more than drawing spirals over things). We will encounter some of the incredible properties of the Fibonacci numbers soon, but first, let's prove its general formula with strong induction.

Theorem 5.18.

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$$

Proof. We prove so by strong induction. For $n = 1, 2$, we verify:

$$F_1 = \frac{\left(\frac{1+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)}{\sqrt{5}} = 1$$

$$F_2 = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2}{\sqrt{5}} = \frac{\left(\frac{3+\sqrt{5}}{2}\right) - \left(\frac{3-\sqrt{5}}{2}\right)}{\sqrt{5}} = 1$$

Now, let us assume the formula holds for $1, 2, \ldots, n$, and show it holds for $n+1$. We compute directly:

$$\begin{aligned}
F_{n+1} = F_n + F_{n-1} &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}} + \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}}{\sqrt{5}} \\
&= \frac{\frac{1+\sqrt{5}}{2}\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \frac{1-\sqrt{5}}{2}\left(\frac{1-\sqrt{5}}{2}\right)^{n-1}}{\sqrt{5}} + \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}}{\sqrt{5}} \\
&= \frac{\left(1 + \frac{1+\sqrt{5}}{2}\right)\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(1 + \frac{1-\sqrt{5}}{2}\right)\left(\frac{1-\sqrt{5}}{2}\right)^{n-1}}{\sqrt{5}}
\end{aligned}$$

A quick verification demonstrates that:

$$\left(\frac{1+\sqrt{5}}{2}\right)^2 = 1 + \frac{1+\sqrt{5}}{2} \quad \text{and} \quad \left(\frac{1-\sqrt{5}}{2}\right)^2 = 1 + \frac{1-\sqrt{5}}{2}$$

Therefore, the previous line is:

$$\begin{aligned}
&= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^2\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^2\left(\frac{1-\sqrt{5}}{2}\right)^{n-1}}{\sqrt{5}} \\
&= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}}{\sqrt{5}}
\end{aligned}$$

Thus, the formula holds for the $n+1$ case, and we are done. □

This proof is rather un-enlightening, as it doesn't tell us *where* the formula comes from. This is a tale for another day, however. The Fibonacci numbers often have interesting recurrence relations, many of which can be proven combinatorially as well as via induction. Let's see one:

Example 5.19. For all $n \geqslant 1$, $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$.

Proof. We prove with induction. For $n = 1$, we have $1^2 - 1 \cdot 1 - 1^2 = (-1)^1$, so the formula holds. Let us proceed to the inductive step - assume the equality holds for $1, 2, \cdots n$, and we wish to show it true for $n + 1$. We proceed using the inductive hypothesis and the definition of Fibonacci numbers.

$$\begin{aligned}
F_{n+2}^2 - F_{n+2}F_{n+1} - F_{n+1}^2 &= (F_{n+1} + F_n)^2 - (F_{n+1} + F_n)F_{n+1} - F_{n+1}^2 \\
&= F_{n+1}^2 + 2F_{n+1}F_n + F_n^2 - F_{n+1}^2 - F_nF_{n+1} - F_{n+1}^2 \\
&= -F_{n+1}^2 + F_{n+1}F_n + F_n^2 \\
&= -(F_{n+1}^2 - F_{n+1}F_n - F_n^2) \\
&= -(-1)^n \\
&= (-1)^{n+1}
\end{aligned}$$

Therefore, it follows by induction that the equality holds for every $n \in \mathbb{N}$. □

6 Evaluating Proofs & Conjectures

Around the midterm, it is a good idea to discuss a few auxiliary topics about proofs. This is the last chapter, for now, in which we talk about proofs specifically, as we will be moving onto discussing other interesting topics and applying our proof skills there as a "proof playground."

6.1 Evaluating Proofs

At this point, we've stated plenty of results and have given a proof of each result. Let's reverse this process by giving an example of a proof of a result but not stating the result being proved.

Example 6.1. Given below is the proof of a result.

Proof. Assume that n is an odd integer. Then $n = 2k + 1$ for some integer k. Then

$$3n - 5 = 3(2k + 1) - 5 = 6k + 3 - 5 = 2(3k - 1).$$

Since $3k - 1$ is an integer, $3n - 5$ is even. □

What is proved above?

(a) $3n - 5$ is an even integer.

(b) If n is an odd integer, then $3n - 5$ is an even integer.

(c) Let n be an integer. If $3n - 5$ is an even integer, then n is an odd integer.

(d) Let n be an integer. If $3n - 5$ is an odd integer, then n is an even integer.

The correct answers are (b) and (d). The proof given is a direct proof of (b) and a proof by contrapositive of (d). The sentence (a) is an open sentence, not a statement, and is only the conclusion of (b). Statement (c) is the converse of (b), and the converse of a true implication is not necessarily true (it is true exactly when an implication is a biconditional). Here, (c) can be in fact proven true, but simply because a statement is true does NOT imply that a supposed proof of the statement is valid.

When learning any new mathematical subject, it is quite normal to make mistakes. Part of learning mathematics is learning from these mistakes, and mistakes of others. For this reason, we will look at a few examples of (possibly) faulty proofs, and determine where the proof is invalid, if anywhere at all, and attempt to fix it. Being able to find errors in valid proofs indicates strong understanding of proof-writing.

Example 6.2. Evaluate the proposed proof of the following result: "If x and y are integers of the same parity, then $x - y$ is even."

Proof. Let x and y be two integers of the same parity. We consider two cases, according to whether x and y are both even or both odd.

- Case 1: x and y are both even. Let $x = 6$ and $y = 2$ which are both even. Then $x - y = 4$, which is even.

- Case 2: x and y are both odd. Let $x = 7$ and $y = 1$, which are both odd. Then $x - y = 6$, which is even.

□

Although the proof starts fine, assuming x and y are integers of the same parity, and then proceeding by cases, the proof of each case is incorrect. When we assume that x and y are even, they must represent *arbitrary* integers, of which we know nothing more about, not *specific* integers.

Example 6.3. Evaluate the proposed proof of the following result: "If m is an even integer and n is an odd integer, then $3m + 5n$ is odd."

Proof. Let m be an even integer and n an odd integer. Then $m = 2k$ and $n = 2k + 1$, where $k \in \mathbb{Z}$. Therefore,

$$\begin{aligned} 3m + 5n &= 3(2k_{+}5(2k + 1) = 6k + 10k + 5 \\ &= 16k + 5 = 2(8k + 2) + 1 \end{aligned}$$

Since $8k + 2$ is an integer, $3m + 5n$ is odd. □

The mistake occurs in the 2nd line of the proof, where we assign $m = 2k$ and $n = 2k+1$. We have inadvertently added the assumption that $n = m + 1$, which was never given as a valid assumption. To be more general here, we must assign $m = 2k$ and $n = 2l + 1$ for integers $k, l \in \mathbb{Z}$ which may or may not be related.

Example 6.4. Evaluate the proposed proof of the following result. "Let $x, y \in \mathbb{Z}$ such that $3 \mid x$. If $3 \mid (x + y)$, then $3 \mid y$."

Proof. Since $3 \mid x$, it follows that $x = 3a$, where $a \in \mathbb{Z}$. Assume that $3 \mid (x + y)$. Then $x + y = 3b$ for some integer b. Hence $y = 3b - x = 3b - 3a = 3(b - a)$. Thus $3 \mid y$.
For the converse, assume that $3 \mid y$. Therefore, $y = 3c$, where $c \in \mathbb{Z}$. Thus $x + y = 3a + 3c = 3(a + c)$. Since $a + c$ is an integer, $3 \mid (x + y)$. □

As a matter of fact, this proof is actually airtight, we're simply proving a stronger statement, the 'iff' version of this statement.

Example 6.5. Evaluate the proposed proof of the following result. "Given $a, b \in \mathbb{R}^+$, $(1/a + 1/b)(a + b) \geqslant 4$."

Proof. We have:

$$\begin{aligned}
\left(\frac{1}{a}+\frac{1}{b}\right)(a+b) &\geqslant 4\\
1+\frac{a}{b}+\frac{b}{a}+1 &\geqslant 4\\
\frac{a^2+b^2}{ab} &\geqslant 2\\
a^2+b^2 &\geqslant 2ab\\
a^2+b^2-2ab &\geqslant 0\\
(a-b)^2 &\geqslant 0
\end{aligned}$$

Since $(a-b)^2 \geqslant 0$, we are done. □

Though this proof has the right strategy and all the right algebra, what it has actually proven is that $(1/a+1/b)(a+b) \geqslant 4$ implies that $(a-b)^2 \geqslant 0$. This is a trivially true statement, since $(a-b)^2 \geqslant 0$ regardless of any condition set on a or b. To correct this proof, we may simply reverse all the algebraic steps, starting with $(a-b)^2 \geqslant 0$, and ending with the desired inequality. Or we can make it clear that each of these algebraic statements are equivalently true by indicating with an $\Leftrightarrow$ between each line (but this generally looks bad).

One final example which I cooked up from the midterm:

Example 6.6. Prove that the product of two irrational numbers is irrational.

Proof. Suppose a, b are irrational, and suppose for contradiction that their product is rational. We may write $ab = \frac{p}{q}$ for $p, q \in \mathbb{Z}$. Since 0 is rational, a and b are nonzero. Therefore we may divide by b to obtain the equality $a = \frac{p}{bq}$. However, we have now expressed a as a fraction, implying it is rational. This is a contradiction, thus the product of two irrationals is irrational. □

The error here comes from applying the definition of rationality. A rational number is a number that can be expressed as a fraction of two *integers*. Though we have expressed a as a fraction, b is irrational, so we do not know that the fraction $p/(bq)$ is a fraction consisting of integers. Make sure when you use a characterization of some concept, you are applying it entirely!

6.2 Conjectures

In mathematics, if we don't know if a statement is true, we call the statement a **conjecture** (in some cases, an open conjecture). When the conjecture is proved, it becomes a theorem. However, if the conjecture is shown to be false, not all hope is lost - often new questions arise from the false conjecture. This is how mathematics develops - by guessing then repeating the process, and learning along the way. Most of modern mathematics consists of formulating and proving conjectures - conjectures are one of the cornerstones of the culture of mathematics. We will now look at some famous conjectures, some open, some closed.

Example 6.7. One of the most famous "easy to state" conjectures is the Collatz conjecture. It is as follows: pick some positive integer n. If it is even, divide it by two. If it is odd, multiply it by 3, then add one. Then with your new number, apply the same process, and do this until you arrive at 1.
For example, let's start with 20. It's even, so we divide and reach 10. That's even so we reach 5. 5 is odd, so we multiply by 3 and add 1 to get 16. 16,8,4,2,1.
The Collatz Conjecture claims that no matter what number is chosen to start, the sequence always terminates. Surprisingly, the conjecture is still open! It is known that the sequence stops for up to very large numbers, but no proof exists that the sequence terminates for *all* natural numbers. Though this conjecture is relatively "unimportant" mathematically, as in it has practically no applications or ties into other programs, it is incredible that such an easily stated problem is not understood fully enough to be proven.

Some conjectures, like the Collatz conjecture, are famous simply because of how long they have been open. Simply stated open conjectures are especially rare, here is another.

Example 6.8. A word or number is a palindrome if it reads the same forwards and backwards. Let's consider the following process: take a number such as 27. It is not a palindrome, so reverse its digits (72) and sum the two numbers. 27+72 =99, which is a palindrome, so we are done.
Let's repeat with 59. 59 is not a palindrome, so we take 59+95=154. This is not a palindrome, so we reverse it and sum the two: 154+451=605. Again, not a palindrome, so we try again. 506+605=1111, which is a palindrome.
It is conjectured that if we begin with any positive integer and apply the technique described, we eventually reach at a palindrome. This conjecture is still open as well, but is known for smaller values.

Simply stated conjectures are by no means guaranteed to have elementary proofs. A famous conjecture turned theorem is as follows:

Example 6.9. Suppose a country is divided up into states on a map. The question then remains: is it possible to color the states on a map with 4 colors such that no two touching states have the same color? The question was originally asked in 1852, and multiple elementary faulty proofs were proposed at the time. An analogous proof was presented for 5 colors, called the five color theorem (one typically sees this proof in a graph theory course).

In 1976, the **Four Color Proof** was finally presented - though it was a mathematical proof, it utilized computers to check over 1000 cases. The proof consisted of reducing checking every possible graph to checking these 1000. A simply stated problem need not have a simple solution!

Example 6.10. Speaking of problems which do not have a simple solution, perhaps the most famous conjecture in mathematics is Fermat's Last "Theorem." Conjectured by Pierre Fermat around 1637, it states that there do not exist any nontrivial integer solutions to the equation $x^n + y^n = z^n$ for $n > 2$. Fermat famously claimed "I have discovered a truly marvelous proof of this, which this margin is too narrow to contain." It is highly apocryphal that such a proof was valid.

The proof was not found until 1993 by Andrew Wiles, who proved so by completing the Taniyama–Shimura–Weil (a different Weil, Andre Weil) conjectures, which connect various modern fields of mathematics, and includes the use of Elliptic Curves, Modular Forms, Algebraic Number Theory, and Algebraic Geometry. That conjecture was originally posed by Goro Shimura in the 50s. A summarization of the complete proof of Andrew Wiles can be found on Wikipedia. The lesson here is that sometimes, relying on elementary statements, like the ones we've been using in this course, or even computer verification, like in the four color theorem, may not be enough to prove some statements. Some statements require centuries of mathematical discoveries and connections, and the joint work of many brilliant minds, to be show to be true.

Example 6.11. The final conjectures we will cover here are as follows. The Goldbach conjecture conjectures that every even integer $\geqslant 4$ is the sum of 2 primes. This conjecture is more likely to be closed in the coming years than any of the other open ones we have listed. A weaker conjecture, that every integer above 5 is the sum of 3 primes, was proven in 2013. The other is the Twin Prime conjecture, which claims that there are infinitely many pairs of "twin primes" or primes that differ by 2.

7 Relations, Functions

We now shift gears a bit and introduce relations and functions.

7.1 Relations

In mathematics, there are practically endless ways of relating objects to each other. Here are some examples: $5 < 10, 5 \leqslant 5, 6 = 30/5, 5 \mid 80, 7 > 4, x \neq y, 8 \nmid 3, a \equiv b \mod n, 6 \in \mathbb{Z}, X \subseteq Y, 2 \notin \mathbb{Z}, \mathbb{Z} \nsubseteq \mathbb{N}$. In each case, two entities appear on each side of a symbol, and the symbol expresses some relationship between the two entities. Such symbols are called **relations**, since they relate the two objects in question. Rather than focusing on each relation in individually, we will develop a general theory that covers all relations.

Example 7.1. Consider the set $A = \{1, 2, 3, 4\}$. Elements of A can be compared to each other by the symbol $<$. Imagine trying to explain this to an alien, who has no concept of integers. One way you could do this is by explicitly writing the following set:

$$R = \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$$

The set R encodes the meaning of the $<$ relation for A - an ordered pair (a,b) appears if and only if $a < b$.

Definition 7.2. A **relation** on a set A is a subset $R \subseteq A \times A$. We often abbreviate the statement $(x,y) \in \mathbb{R}$ as xRy, and $(x,y) \notin R$ as $x\not{R}y$.

Often I will denote a relation by $\sim$.

Example 7.3. For $A = \{1,2,3,4\}$

(a) $\leqslant$

(b) Parity

(c) Intersection of relations can be seen as combining relations using the conjunction.

(d) Let $B = \{0,1,2,3,4,5\}$ and let $U = \{(1,3),(3,3),(5,2),(2,5),(4,2)\} \subseteq B \times B$. U is a relation on B but doesn't necessarily have any meaning. We may express this in a directed graph (draw a graph).

(e) Consider the set $R = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : x - y \in \mathbb{N}\}$. This is another way of expressing $\geqslant$.

(f) The set $R = \{(x,x) \in \mathbb{R} \times \mathbb{R}\}$ is the relation $=$ on $\mathbb{R}$.

Relations can have certain natural properties which arise.

Definition 7.4. Suppose R is a relation on set A.

(a) R is **reflexive** if xRx for all $x \in A$.

(b) R is **symmetric** if xRy implies yRx for all $x, y \in A$.

(c) R is **transitive** if xRy and yRz implies xRz for all $x, y, z \in A$.

Example 7.5. Let $A = \mathbb{Z}$.

(a) $<$ is not reflexive, not symmetric, but transitive.

(b) $\leqslant$ is reflexive, not symmetric, and is transitive.

(c) $=$ is reflexive, symmetric, and transitive.

(d) $\mid$ is reflexive, not symmetric, and is transitive.

(e) $\nmid$ is not reflexive, symmetric, or transitive.

(f) $\neq$ is not reflexive, is symmetric, and not transitive.

Example 7.6. Let $A = \{a, b, c, d, e\}$ and $\sim= \{(b, b), (b, c), (c, b), (c, c), (d, d), (b, d), (d, b), (c, d), (d, c)\}$. This relation is not reflexive, $b \sim b$ but not $a \sim a$. One can verify that $\sim$ is symmetric. One can verify with a lot more work that $\sim$ is also transitive (it's not fun). What is the relation? It is the the relation "x and y are both consonants." Once we look at it this way, it is immediately clear that it is transitive, which illustrates a point: once the meaning of a relation is known, checking these properties becomes much easier.
(Draw a picture of R) With a picture, some properties of R become a lot clearer than from the set description.

Visually, the properties look like so:

(a) A relation is reflexive if for each point x, there is a loop at x.

(b) A relation is symmetric if for every directed edge from x to y, there is one from y to x.

(c) A relation is transitive if whenever there are arrows from x to y and y to z, there is one from x to z. In the case when $x = z$, there is a loop at x.

Theorem 7.7. The relation $\equiv \mod n$ on the set $\mathbb{Z}$ is reflexive, symmetric, and transitive.

Proof. First we show $\equiv$ is reflexive. Since $n \mid 0$, $n \mid x - x$, and thus $x \equiv x \mod n$.

Next let's show $\equiv$ is symmetric. Suppose $x \equiv y \mod n$, then $n \mid (x - y)$. But $n \mid -(x - y)$ as well, so $n \mid (y - x)$, and hence, $y \equiv x \mod n$.

Finally, we must show $x \equiv y \mod n$ and $y \equiv z \mod n$ implies $x \equiv z \mod n$ (this was an exercise. We have $n \mid (x - y)$ and $n \mid (y - z)$, so $x - y = nk$ and $y - z = nl$ for $k, l \in \mathbb{Z}$. So $x - z = nk + nl = n(k + l)$, and thus $n \mid (x - z)$ as desired. □

Remark 7.8. One final note - we have specified that a relation R must be defined on a set A. We can also define a relation between sets. A relation from a set A to a set B is a subset $R \subseteq A \times B$. All the same properties may follow.

7.2 Equivalence Relations

Modulo n is an example of an equivalence relation, a relation which satisfies the three previously introduced properties.

Definition 7.9. A relation R on a set A is a **equivalence relation** if it is reflexive, symmetric, and transitive. For any $a \in A$, the **equivalence class containing a** is the subset $[a] = \{x \in A : xRa\} \subseteq A$.

Example 7.10. Given set $A = \{-1, 1, 2, 3, 4\}$, we introduce 4 equivalence relations.

(a) $=$ is an equivalence relation. It has 5 equivalence classes.

(b) "has same parity as" is an equivalence relation, with 2 equivalence classes, the set of odd numbers and even numbers.

(c) "has same sign as" is an equivalence relation, with 2 equivalence classes, the positive and negative numbers.

(d) "has same parity and sign as" is an equivalence relation, with 3 equivalence classes.

Example 7.11. Some equivalence relations on infinite sets are as follows:

(a) Let P be the set of all polynomial with real coefficients. Define a relation $\sim$ on P as follows: given $f(x), g(x) \in P$, write $f(x) \sim g(x)$ when $f(x)$ and $g(x)$ have the same degree, that is, same highest power of x with nonzero coefficient. So for example, $x^2 + 3x - 4 \sim 3x^2 - 2$. The equivalence classes of R are easy to describe, they're the sets of polynomials with fixed degree. So for example, $[3x^2 + 2]$ is the set of all polynomials of degree 2. In other words, $[3x^2 + 2] = \{ax^2 + bx + c, a, b, c \in \mathbb{R}, a \neq 0\}$.

(b) We proved $\equiv \mod n$ is an equivalence relation. The equivalence classes can be represented by $[0], [1], \ldots, [n-1]$. So in this sense, when we do modular arithmetic, we are actually doing arithmetic on the equivalence classes $\mod n$, not just on numbers!

To be precise: recall we proved that if $a \equiv b \mod n$ and $c \equiv d \mod n$, then $a+c \equiv b+d \mod n$, and similarly for multiplication. This implies that we perform addition and multiplication as $[a] + [b]$ or $[a] \cdot [b]$ modulo n - to do so, take any convenient $a' \in [a]$ and $b' \in [b]$ - then $[a] + [b] \equiv [a' + b'] \mod n$ no matter what choice is used.

We denote **the integers modulo n by $\mathbb{Z}/n\mathbb{Z}$.**

(c) The relation $=$ on the set $\{(a, b) : a, b \in \mathbb{Z}, b \neq 0\}$ given by $(a, b) \sim (c, d)$ when $ad = bc$ can be more clearly realized as the equivalence $=$ on the set $\mathbb{Q}$, or loosely, as the equivalence relation which reduces fractions. In this sense, we can think of $\mathbb{Q}$ as the set of equivalence classes of $\mathbb{Z} \times (\mathbb{Z}\backslash 0)$ under this relation $\sim$, i.e. $1/2 = 2/4$ are the same value, and live in the same equivalence class. This is an equivalence relation you've worked with all your life without realizing it!

(d) The antiderivative $\int f(x)\,dx$ is the set of functions $F(x) + c$ whose derivatives are $f(x)$. This is an equivalence class in the set of integrable functions, where functions are related if their difference is a constant.

The point here is that equivalence classes and equivalence relations occur everywhere in mathematics. This is especially true in advanced mathematics, where equivalence relations become necessary for constructions or for considering a class of objects in one fell swoop.

7.3 Partitions

Theorem 7.12. Given an equivalence relation $\sim$ on a set A, for $a, b \in A$, $[a] = [b]$ if and only if $a \sim b$.

Proof. First suppose $[a] = [b]$. Since $a \sim a$ by the reflexive property,

$$a \in \{x \in A : x \sim a\} = [a] = [b] = \{x \in A : x \sim b\}$$

But a belonging to that last set implies $a \sim b$.
Now suppose $a \sim b$. First we show $[a] \subseteq [b]$. Suppose $c \in [a]$. By definition of $[a]$, $a \sim c$. Since $a \sim c$ and $a \sim b$, it follows that $b \sim c$. This implies $c \in [b]$, so $[a] \subseteq [b]$. The opposite inclusion follows identically, so $[a] = [b]$. □

Theorem 7.13. If $\sim$ is an equivalence relation on a set A, then the set of equivalence classes of $\sim$ forms a partition of A.

Proof. We must show two things, that the union of all equivalency classes $[a]$ is equal to A, and must show that $[a] \cap [b] = \varnothing$ for $[a] \neq [b]$. To show the former, we must show every $x \in A$ belongs to some equivalency class $[a]$. However, $x \in [x]$, and thus the union of all equivalency classes is equal to A.

To show the latter, that if $[a] \neq [b]$, then $[a] \cap [b] = \varnothing$, we prove via contrapositive. Suppose $[a] \cap [b] \neq \varnothing$. Then there exists some x with $x \in [a]$ and $x \in [b]$. Then from the previous theorem, $x \sim a$ and $x \sim b$, so by transitivity, $a \sim b$ and hence $[a] = [b]$, as desired. □

7.4 Functions

Of course you recall what a function is - take for example, $f(x) = x^2$ - you put in a number and get another. However, functions can be more than just numerical relationships. Let's redefine functions in a more abstract way involving sets and relations.

Definition 7.14. Suppose A and B are sets. A **function** from A to B (denoted $f : A \to B$) is a relation $f \subseteq A \times B$ from A to B, satisfying the property that for each $a \in A$ the relation f contains exactly one ordered pair of form (a, b). The statement $(a, b) \in f$ is abbreviated $f(a) = b$.
The **domain** of f is A and the **codomain** of f is B. The **range** or **image** of f is the set $\{f(a) : a \in A\}$, denoted $f(A)$.
Two functions $f(x), g(x) : A \to B$ are **equal** if for all $a \in A$, $f(a) = g(a)$. Equivalently, $f = g$ as sets.

Example 7.15. (a) The function $f(x) = x^2$ on $\mathbb{R}$ can be expressed as the relation $\{(x, x^2) : x \in \mathbb{R}\}$ on $\mathbb{R} \times \mathbb{R}$. It's range is $[0, \infty)$. Note that the way we wrote it, its codomain is unclear - it could be $\mathbb{R}$ or $[0, \infty)$.

(b) The function $f : A \to B$, for sets $A = \{0, 1, 2\}$ and $B = \{a, b, c\}$ defined by $\{(0, a), (1, a), (2, c)\}$ is relatively uninteresting. It has domain A, codomain B, and range $\{a, c\}$. (draw a picture)

(c) The function $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $\{(x, [x]) : x \in \mathbb{Z}\}$ is the "projection onto $\mathbb{Z}/n\mathbb{Z}$."

We emphasis that according to the definition, the function is really just a special kind of set, that is a function $f : A \to B$ is a subset of $A \times B$. Another equivalent way to think about it is a choice to think about it is a choice of element $f(a) \in B$ for every $a \in A$. We write this $a \mapsto f(a)$.

Example 7.16. First, note that if we have a function whose domain is a cartesian product such as $\mathbb{Z}^2$, we may simplify the notation. Given $f : \mathbb{Z}^2 \to \mathbb{Z}$, we may write $f(m, n)$ instead of $f((m, n))$, although the latter is more accurate. One may also think of this as a function with two inputs, however, the domain is still $\mathbb{Z}^2$ in this context.
Say a function $f : \mathbb{Z}^2 \to \mathbb{Z}$ is defined by $f(m, n) = 6m - 9m$. As a set, this function is $f = \{((m, n), 6m - 9n) : (m, n) \in \mathbb{Z}^2\} \subseteq \mathbb{Z}^2 \times \mathbb{Z}$. What is the image of f?

Proof. First observe that any element in $f(A)$ is divisible by three. Indeed, $6m - 9n = 3(2m - 3n)$. We show that if $3 \mid x$, then there exist m, n such that $f(m, n) = x$. Observe that $f(2, 1) = 3$, and that the function is multiplicative. Therefore if $x = 3k$ is a multiple of 3, then the choice $f(2k, k) = 12k - 9k = 3k = x$ satisfies the condition. Hence the image $f(A)$ is all multiples of 3. □

Definition 7.17. We denote the set of all functions from A to B by B^A. That is, $B^A = \{f : f : A \to B\}$. In general, $|B^A| = |B|^{|A|}$.

7.5 Injective & Surjective Functinos

Recall the terms "one-to-one" and "onto" from calculus - these are other names for injective and surjective functions respectively.

Definition 7.18. A function f is:

(a) **injective** if for all $a, a' \in A$, $a \neq a'$ implies $f(a) \neq f(a')$.

(b) **surjective** if for every $b \in B$, there is an $a \in A$ with $f(a) = b$.

(c) **bijective** if f is both injective and surjective.

(provide pictures)

Notice that whether f is surjective or not depends on how its codomain is defined. For example, $f(x) = x^2$ is surjective if $f : \mathbb{R} \to [0, \infty)$, but not if $f : \mathbb{R} \to \mathbb{R}$. In short, a function is surjective if and only if its codomain equals its image. That is, $f(A) = B$.

Remark 7.19. In general, if we wish to show a function $f : A \to B$ is injective, there are two ways to go about this. The direct approach is to suppose $a, a' \in A$ and $a \neq a'$, then prove $f(a) \neq f(a')$. The contrapositive way (which generally is more practical) is to suppose $a, a' \in A$ and $f(a) = f(a')$, and prove $a = a'$.
To show a function f is surjective, suppose $b \in B$, and show there exists $a \in A$ such that $f(a) = b$.

Example 7.20. (a) Show that the function $f : \mathbb{R} - \{0\} \to \mathbb{R}$ given by $x \mapsto 1/x + 1$ is injective but not surjective.

Proof. To show f is injective, suppose $a, a' \in \mathbb{R} - \{0\}$ with $f(a) = f(a')$. Then $1/a + 1 = 1/a' + 1$, which implies $1/a = 1/a'$, and since $a, a' \neq 0$, we may conclude $a = a'$.

To show f is not surjective, it suffices to find some $b \in \mathbb{R}$ such that no $f(a) \neq b$ for all $a \in \mathbb{R} - \{0\}$. The element $b = 1$ works, since $1/x \neq 0$ for all $x \in \mathbb{R} - \{0\}$. □

(b) On the other hand, if we set the codomain of the above function to be $\mathbb{R} - \{1\}$, we may prove that f is surjective as well. To do so, let's take an arbitrary $b \in \mathbb{R} - \{1\}$, and find an $a \in \mathbb{R} - \{0\}$ such that $f(a) = b$. One may verify that $a = 1/(b-1)$ satisfies this: indeed, $1/(1/(b-1)) - 1 = b$, so $f(1/(b-1)) = b$, as desired. Hence f is injective, surjective, and thus bijective.

When we have functions between finite sets of same cardinality, it can be easier to show a function is bijective.

Theorem 7.21. If $f : A \to B$ is a function and $|A| = |B|$, then f is surjective if and only if f is injective.
Equivalently, if $|A| = |B|$, then f is bijective if and only if f is either injective or surjective.

Proof. First let's assume f is injective. Since there are n elements of A, each with distinct images, there are n distinct images. Therefore, $f(A) = B$, so f is surjective.
Next, let's assume f is surjective. Then each of the n elements in B are the image for some element of A. Consequently, the n elements of A have n distinct images in B, implying no two distinct elements of A can have the same image. Hence f is one-to-one. □

We now state a classic counting result, and apply it to our study of functions.

Theorem 7.22. (Pigeonhole Principle) If there are n pigeons nesting in k holes, then at least one hole has $\lceil \frac{n}{k} \rceil$ pigeons.

Now consider this in terms of functions. If we have a elements in set A and need to assign them to b elements in B, if it is the case that $a > b$, then the pigeonhole principle states that there must be two elements of A assigned to the same element in B. On the other hand, if it is the case that $b > a$, then at least one hole will go unfilled. Rigorously:

Theorem 7.23. (Pigeonhole Principle of Functions) Suppose A and B are finite sets and $f : A \to B$ is a function.

(a) If $|A| > |B|$ then f is not injective.

(b) If $|B| > |A|$ then f is not surjective.

Let's see some applications of this.

Example 7.24. If A is a set of 10 integers between 1 and 100, then there exist two different subsets $X \subseteq A$ and $Y \subseteq A$ for which the sum of elements in X equals the sum of elements in Y.

Proof. Suppose $A \subseteq \{1, 2, \ldots, 100\}$ with $|A| = 10$. Note if $X \subseteq A$, then X has no more than 10 elements, each of which are at most 100, so the sum of elements in X is less than $100 \cdot 10 = 1000$. Consider the function

$$f : \mathcal{P}(A) \to \{0, 1, \ldots, 1000\}$$

for which $f(X)$ sums the values of X. Since $|\mathcal{P}(A)| = 2^{10} = 1024 > 1001 = |\{0, 1, \ldots, 1000\}|$, the pigeonhole principle implies f is not injective. Therefore, there are two unequal sets $X, Y \subseteq A$ such that $f(X) = f(Y)$, as desired. □

Pigeonhole principal problems usually involve showing that given some set of something, there must be some subset that has some certain property, and the proofs usually involve constructing the "holes" in the right way.

7.6 Composition

You may be familiar with the notion of composition already, but it is worthwhile to revisit.

Definition 7.25. Suppose $f : A \to B$ and $g : B \to C$ are functions where the codomain of f is a subset of the domain of g. The **composition** of f and g, denoted $g \circ f : A \to C$, is the function with domain A and codomain C defined by $(g \circ f)(x) = g(f(x))$.

Example 7.26. Suppose $A = \{a, b, c\}$ and $B = \{1, 2, 3\}$. Set $f : A \to B$ to be the function $f = \{(a, 1), (b, 2), (c, 3)\}$ and $g : B \to A$ to be the function $g = \{(1, c), (2, b), (3, c)\}$. Then we may compute:

(a) $g \circ f = \{(a, c), (b, b), (c, c)\}$

(b) $f \circ g = \{(1, 3), (2, 2), (3, 3)\}$

(c) $f \circ f$ and $g \circ g$ are not defined.

Here we note that composition is not commutative, that is $g \circ f \neq f \circ g$. In fact, they don't even share domains or codomains!

Theorem 7.27. Composition of functions is associative, that is, for three functions f, g, h whose composition is defined,

$$(h \circ g) \circ f = h \circ (g \circ f)$$

In particular, we may unambiguously take the composition of any finite number of functions.

Proof. To prove this, we must show that the two functions are equal for all x in the domain of A. We compute:

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))).$$

Similarly,

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))).$$

Since both sides equal $h(g(f(x)))$ for all x in the domain of A, we may conclude the functions are equal. □

Theorem 7.28. Suppose $f : A \to B$ and $g : B \to C$.

(a) If both f and g are injective, then $g \circ f$ is injective.

(b) If both f and g are surjective, then $g \circ f$ is surjective.

Proof. First suppose f and g are injective. We must show that $g \circ f(x) = g \circ f(y)$ implies $x = y$ for arbitrary $x, y \in A$. We have $g(f(x)) = g(f(y))$, by injectivity of g we have that $f(x) = f(y)$, and injectivity of f implies $x = y$ as desired.
Now, suppose f and g are surjective. We must show that for any $y \in C$, there is $x \in A$ such that $g \circ f(x) = y$, or equivalently $g(f(x)) = y$. Surjectivity of g implies there is some $z \in B$ such that $g(z) = y$, and surjectivity of f implies there is some $x \in A$ such that $f(x) = z$. Choosing x implies $g(f(x)) = g(z) = y$, as desired. □

Corollary 7.29. Suppose $f : A \to B$ and $g : B \to C$. If both f, g are bijective, $g \circ f$ is bijective.

7.7 Inverse Functions

You may recall that a bijective function has an inverse function f^{-1} that "undoes" the effect of f, that is, $f(f^{-1}(x)) = f^{-1}(f(x)) = x$. We make this notion more precise.

Definition 7.30. For a set A, the **identity function** on A is the function $i_A : A \to A$ defined as $i_A(x) = x$ for all $x \in A$. Equivalently $i_A = \{(x, x) : x \in A\}$. It is bijective.

Definition 7.31. Given a relation $R : A \to B$, the **inverse relation of R**, denoted R^{-1} is the relation from $B \to A$ defined as $R^{-1} = \{(y, x) : (x, y) \in R\}$. In other words, the inverse of R is the relation R^{-1} obtained by interchanging the elements for every ordered pair in R.

Example 7.32. Let $f : A \to B$, where $A = \{a, b, c\}, B = \{1, 2, 3\}$. Suppose f is the relation $f = \{(a, 2), (b, 3), (c, 1)\}$. Then $f^{-1} = \{(2, a), (3, b), (1, c)\}$. Note that f^{-1} is indeed a function, as each element of B appears exactly once as the first term of a tuple. Note f is bijective.
Let $g : A \to B$ be $g = \{(a, 2), (b, 3), (c, 3)\}$. Then $g^{-1} = \{(2, a), (3, b), (3, c)\}$. This is not a function - 3 is mapped twice, and 1 has no mapping. Note g is not injective or surjective.

Theorem 7.33. Let $f : A \to B$ be a function. Then f is bijective if and only if f^{-1} is a function from $B \to A$.

Proof. Suppose $f : A \to B$ is bijective. Then every element in B appears exactly once in the 2nd coordinate of a tuple of f^{-1}. Therefore, every element of B appears exactly once in a 1st coordinate of f^{-1}, implying f^{-1} is a function.

Now suppose f^{-1} is a function from $B \to A$. Since every element of B appears in a tuple in f^{-1}, this implies every element of B appears in a tuple in f as well, and thus f is surjective. Additionally, since every element of B appears in a tuple in f^{-1} no more than once, this implies every element of B appears in a tuple of f no more than once. Suppose $f(x) = f(y)$ - since there is only one tuple containing $f(x)$, it must be the case that $x = y$, and thus, f is injective, as desired. □

Definition 7.34. If $f : A \to B$ is bijective, then its **inverse** is the function $f^{-1}B \to A$. The functions f and f^{-1} obey the functions $f^{-1} \circ f = i_A$ and $f^{-1} \circ f = i_B$.

Remark 7.35. We now have two equivalent ways of proving a function is bijective - the first is showing it is surjective and injective, and the other is constructing an inverse and checking it is both a left inverse and right inverse.

Take caution - for a function $f : A \to B$, just because a function $g : B \to A$ is a left inverse, i.e. $g \circ f = i_A$, does not necessarily imply it is a right inverse, that is, $f \circ g = i_B$. For example, let $A = \{1\}$ and $B = \{1, 2\}$. The function $f : A \to B$ give by $f(1) = 1$ and $g : B \to A$ given by $g(1) = g(2) = 1$ satisfy $g \circ f = i_A$ but $f \circ g \neq i_B$.

Example 7.36. You've had experience with finding inverses of functions before. For example,

(a) The function $f(x) = x^3 + 1$ has an inverse. Suppose $f(x) = y$, we want to find the function f^{-1} satisfying $f^{-1}(y) = x$. Write $y = x^3+1$, simple algebra shows $x = \sqrt[3]{y - 1}$. One may verify that indeed the function $f^{-1}(x) = \sqrt[3]{x - 1}$ is an inverse function to $f(x) = x^3 + 1$.

(b) The function $g : \mathbb{Z}^2 \to \mathbb{Z}^2, (m, n) \mapsto (m + n, m + 2n)$ is bijective, one may verify this using linear algebra (row reduction). We find its inverse as follows: begin by writing $(m, n) = g(x, y) = (x + y, x + 2y)$. We wish to find the function g^{-1} such that $g^{-1}(m, n) = (x, y)$ So we wish to solve the system of equations:

$$x + y = m, \quad x + 2y = n$$

A little linear algebra gives us that $x = 2m - n$ and $y = n - m$. Indeed, $g^{-1}(x, y) = (2x - y, y - x)$ is the inverse function to g.

We also can compute this by seeing that g can be represented by matrix multiplication, multiplying the matrix:

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x + y \\ x + 2y \end{bmatrix}.$$

To find the inverse, we simply need to invert the matrix - its inverse is

$$\begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix},$$

and indeed, we see that representing these functions as matrices,

$$\begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$$

and similarly for the other composition.

(c) For non-numerical functions, sometimes inverses can require a bit more tact to find. A quick example: define the function $f : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ given by $X \mapsto \overline{X}$. This function is its own inverse!

Finally, one quick definition which will certainly be seen in future classes.

Definition 7.37. Let $f : A \to B$.

(a) The **image** of $X \subseteq A$ is the set $f(X) = \{f(x) : x \in X\} \subseteq B$.

(b) The **preimage** of $Y \subseteq B$ is the set $f^{-1}(X) = \{x \in A : f(x) \in Y\} \subseteq A$.

Note that a function $f : A \to B$ is surjective if and only if $f(A) = B$. A function defined on a finite set is injective if and only if for every $X \subseteq f(A)$, $|f^{-1}(X)| = |B|$. Note that if set $f(A) = C$, the same function with redefined codomain, $f : A \to C$ is automatically surjective.

7.8 Well-Definedness

A note of caution - often when we define functions, we define them using rules rather than explicitly writing out where each function is mapped. This is fairly normal, but one has to take caution to make sure that the construction which is being used implies that each element in the domain sends an element to only one element in the codomain, in an unambiguous way. We say that a function is **well-defined** if this occurs, and **ill-defined** or **ambiguous** if not.

This is not the same as a function being **undefined** for certain values - for example, the function $f(x) = 1/x$ is undefined at $x = 0$, but still well-defined. We just must restrict the function so 0 is not included in the domain. Let's see some examples of not well-defined functions.

Example 7.38. (a) Let A_0 and A_1 be sets, define $A = A_0 \cup A_1$, and define $f : A \to \{0, 1\}$ as $f(a) = 0$ if $a \in A_0$ and $f(a) = 1$ if $a \in A_1$. If $A_0 \cap A_1 = \varnothing$ then f is well-defined, but if $A_0 \cap A_1 \neq \varnothing$, then f is ambiguous for elements belonging to both A_0 and A_1.

(b) Defining functions between differing moduli spaces in modular arithmetic can be iffy. Consider the function $f : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ sending $[a]_8 \mapsto [a]_4$. One can verify that this is a well-defined function by checking that any integer belonging to $[a]_8$ is sent to the same value $[a]_4$. This follows because if $a \equiv b \mod 8$, or $8 \mid a - b$, then $4 \mid a - b$ as well, so $a \equiv b \mod 4$.

However, switching things up, $f : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$, sending $[a]_4 \mapsto [a]_8$ is not well-defined. To see an example, note that $0, 4 \in [0]_4$, but $0 \in [0]_8$ and $4 \in [4]_8$. Hence, $[0]_4 \mapsto [0]_8$ and $[4]_4 \mapsto [4]_8$, but since $[0]_4 = [4]_4$, this means that the way this function is constructed, it is not well-defined.

(c) Consider the function $f(x) = x/2$. This function is well-defined, but if f is defined as $f : \mathbb{Z} \to \mathbb{Z}$, the function's codomain is too small.

In general, one does not need to check for well-definedness of functions if the function is being defined explicitly. However, when a function is either defined on a set of equivalence classes, or is defined based on some logical rules, one must check that indeed, the function is well-defined.

8 Cardinality, Revisited

Before, we defined the cardinality of a finite set to be the number of elements it contains, and the cardinality of an infinite set to be "infinity" otherwise. We expand on this notion.

8.1 Numerically Equivalent Sets

Definition 8.1. Two sets A and B, either finite or infinite, are said to have **same cardinality**, written $|A| = |B|$, when either A and B are both empty or there is a bijective function $f : A \to B$. We say A and B are **numerically equivalence**.

Theorem 8.2. Let S be a nonempty collection of nonempty sets. A relation $\sim$ is defined on S by $A \sim B$ if there exists a bijective function from A to B. Then R is an equivalence relation.

Proof. Let A in S. The identity function $i_A : A \to A$ is bijective, so $A \sim A$, thus $\sim$ is reflexive.
Now suppose $A \sim B$, so there is a bijective function $f : A \to B$. Then $f^{-1} : B \to A$ is a bijective function, so $B \sim A$. Hence $\sim$ is symmetric.
Now suppose $A \sim B$ and $B \sim C$, so there are bijective functions $f : A \to B$ and $G : B \to C$. Then $g \circ f : A \to C$ is bijective, so $A \sim C$, and $\sim$ is transitive. □

By the equivalence relation $\sim$, the equivalence class $[A]$ is all sets in S having the same cardinality as A, hence the term "numerically equivalent sets."
We are particularly interested in sets which are numerically equivalent to $\mathbb{N}$.

8.2 Denumerable Sets

Notationally for this chapter, $\mathbb{N}$ will not contain 0.

Definition 8.3. A set A is called **denumerable** or **countably infinite** if $|A| = |\mathbb{N}|$. In other words, A is denumerable when there is a bijective function $f : \mathbb{N} \to A$ such that $A = \{f(1), f(2), f(3), \dots\}$. Equivalently, A is denumerable if and only if we can list the elements of A as distinct $a_1, a_2, a_3, \dots$ (where $a_i = f(i)$).

Say a set A is **countable** if it is finite or countably infinite. Otherwise, it is **uncountable**.

Let's see some examples of countably infinite sets.

Theorem 8.4. $\mathbb{Z}$ is countably infinite.

Proof. Observe that $\mathbb{Z}$ can be listed as $0, 1, -1, 2, -2, \dots$. Then we have a list: $a_1 = 0, a_2 = 1, a_3 = -1, \dots$, and the function describing this mapping is clearly injective and surjective. Explicitly, it can be written

$$f(n) = \frac{1 + (-1)^n(2n-1)}{4}$$

□

As a result, this example demonstrates that it is possible for two sets to have the same cardinality when one is a proper subset of the other.

Theorem 8.5. Suppose A, B are infinite with $B \subseteq A$. If A is countable, then B is countable.

Proof. Suppose $B \subseteq A$ with B infinite and A countably infinite. Since A is countably infinite, we can express it as $A = \{a_1, a_2, a_3, \dots\}$. Our goal is to write $B = \{b_1, b_2, \dots\}$.

Let $S = \{i \in \mathbb{N} : a_i \in B\}$, that is S consists of all those positive integers that are subscripts of the elements in A which also belong to B. Since B is infinite, so is S. First we use induction to show B contains a countably infinite subset. Since S is a nonempty subset of $\mathbb{N}$, the well-ordering principle implies S has a least element. Let $b_1 = a_{i_1}$. Let $S_1 = S - \{i_1\}$. Since $S_1 \neq \emptyset$, S_1 has a least element i_2. Let $b_2 = a_{i_2}$, which is distinct from b_1. We repeat this process, in general suppose the distinct elements $b_1, b_2, \dots, b_k$ have been defined by $b_j = a_{i_j}$ for each integer j with $1 \leqslant j \leqslant k$, where i_1 is the smallest element in S and i_j is the minimum element in $S_{j-1} = S - \{i_1, \dots, i_{j-1}\}$ for $2 \leqslant j \leqslant k$. Then let i_{k+1} be the minimum element of $S_k = S - \{i_1, i_2, \dots, i_k\}$ and let $b_{k+1} = a_{i_{k+1}}$. It follows for each integer $n \geqslant 2$, an element b_n belongs to B that is distinct from $b_1, \dots, b_{n-1}$. Thus, the elements $b_1, b_2, b_3, \dots \in B$.

Let $B' = \{b_1, b_2, \dots\}$, which is countably infinite. It is clear $B' \subseteq B$. It remains to show $B \subseteq B'$. Let $b \in B$ - since $B \subseteq A$ it follows that $b = a_n$ for some $n \in \mathbb{N}$ and so $n \in S$. If $n = i_1$ then $b = b_1$, so $b \in B'$. Otherwise, assume $n > i_1$. Let S' consist of the positive integers less than n that belong to S. Since $n > i_1$ and $i_1 \in S$, it follows that $S' \neq \emptyset$. It is clear that $1 \leqslant |S'| \leqslant n-1$ so S' is finite, so say $|S'| = m$. Then S' consists of the m smallest integers of S, i.e. $S' = \{i_1, \dots, i_m\}$. The smallest integer belonging to S greater than i_m is i_{m+1} and $i_{m+1} \geqslant n$, so $n = i_{m+1}$ and thus $b = a_n = a_{i_{m+1}}$. Thus $b \in B'$ and we conclude $B = B'$. □

Corollary 8.6. $k\mathbb{N}$ and $k\mathbb{Z}$ are countably infinite for any $k \in \mathbb{N}$.

Theorem 8.7. If A and B are countably infinite, then $A \times B$ is countably infinite.

Proof. Write $A = \{a_1, a_2, \dots\}$ and $B = \{b_1, b_2, \dots\}$.(draw a table) Compare the table of $A \times B$ shown which have a countably infinite number of rows and columns, where a_i increase by row and b_i increase by columns - (a_i, b_j) appears in the ith row and jth column. Obviously every element of $A \times B$ appears once. We now order the elements as follows: (draw a picture)

$$(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_3, b_1), (a_2, b_2), (a_1, b_3), \dots$$

This is a bijective function since every element of $A \times B$ occurs once. Thus $A \times B$ is denumerable. □

Corollary 8.8. $\mathbb{Q}^+$ is countably infinite.

Proof. This follows by considering $\mathbb{Q}^+$ as $\mathbb{N} \times \mathbb{N}$ with all ordered pairs (a, b) with $\gcd(a, b) > 1$ removed, and application of the previous two theorems. Equivalently, one may use the same function as used in the previous proof, but with skipping over any unreduced fraction. □

One must take care in the way that the bijection is created - for example, traversing by each row will not work. However, there are many ways of traversing $\mathbb{Q}^+$ which all result in bijections.

Corollary 8.9. $\mathbb{Q}$ is countably infinite.

Proof. Write $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$. We can write $\mathbb{Q}^+ = \{q_1, q_2, \dots\}$ and it is clear the function $\mathbb{Q}^+ \to \mathbb{Q}^-$ given by taking the negative of each rational is a bijection, so we may also write $\mathbb{Q}^- = \{-q_1, -q_2, \dots\}$. Then the sequence $\mathbb{Q} = \{0, q_1, -q_1, q_2, -q_2, \dots\}$ is a bijection, and so $\mathbb{Q}$ is countably infinite. □

We conclude with one final statement which will not be proven.

Theorem 8.10. The cartesian product of a countably infinite collection of countable sets is countable.

8.3 Uncountable Sets

Let's review a few facts of real numbers and decimal expansions. Every irrational number has a unique *nonrepeating* decimal expansion which is nonrepeating. However some rational numbers have two repeating decimal expansions, for example, $1/2 = .50000\cdots = .499999\dots$. In particular, a rational number a/b has two decimal expansions if and only if the only primes dividing b are 2 and 5, and in particular, then one of the expansions repeats the number 0.

Recall that $(a, b) = \{x \in \mathbb{R}, a < x < b\}$. We can prove any open interval of this form is indeed uncountable by Cantor's Diagonalization Argument, but the standard way to do so is to prove $(0, 1)$ is uncountable.

Theorem 8.11. $(0, 1)$ is uncountable.

Proof. Suppose for contradiction $(0, 1)$ is countable, hence countably infinite. Therefore there must exist a way to write $(0, 1) = \{a_1, a_2, \dots\}$ with each a_i distinct. Each number a_n has a decimal expansion, say $a_n = 0.a_{n1}a_{n2}\dots$. To avoid confusion, when a number has a nonunique decimal expansion, we choose the expansion which repeates the digit 0 from some point on, so there is no real number a_n that has a decimal expansion which repeats 9 from some point on. (draw a sequence of decimal expansions)

We show that f is not onto. Define $b = 0.b_1b_2b_3\dots$ by

$$b_i = \begin{cases} 4 & a_{ii=5} \\ 5 & a_{ii} \neq 5 \end{cases}$$

Note that $b \neq a_i$ for any $i \in \mathbb{N}$, because the ith decimal place is not equal. Thus b is not the image of any element of $\mathbb{N}$, so f is not onto, a contradiction. □

Theorem 8.12. Let A, B be sets such that $A \subseteq B$. If A is uncountable, then B is uncountable.

Proof. This is directly the contrapositive of (8.5). □

Note that this theorem does not imply that A and B are numerically equivalent in this case - just that they are uncountable.

Corollary 8.13. $\mathbb{R}$ is uncountable.

So we have proven that $|\mathbb{Q}| \neq |\mathbb{R}|$! In general it should be clear that countable and uncountable sets cannot be numerically equivalent.

Theorem 8.14. $(-\pi/2, \pi/2)$ and $\mathbb{R}$ are numerically equivalent.

Proof. One may observe that $f(x) = \tan(x)$ is an explicit bijection between the sets. □

Corollary 8.15. $\mathbb{R}$ is numerically equivalent to any open interval.

Proof. One may construct a linear function $f(x)$ mapping $(-\pi/2, \pi/2)$ to (a, b) for any $a < b \in \mathbb{R}$ (that is, $f(-\pi/2) = a$ and $f(\pi/2) = b$). We leave the details as an exercise. □

8.4 Comparing Cardinalities

Definition 8.16. A set A is said to have **smaller cardinality** than B, denoted $|A| < |B|$, if there is an injective function $f : A \to B$, but no bijection from A to B. If we write $|A| \leqslant |B|$, then either $|A| < |B|$ or $|A| = |B|$.

Example 8.17. The inclusion $\mathbb{N} \to \mathbb{R}$ and the Diagonalization argument demonstrates $|\mathbb{N}| < |\mathbb{R}|$.

Definition 8.18. The cardinality of the set $\mathbb{N}$ of natural numbers is denoted $\aleph_0$, "**aleph null**". The cardinality of $\mathbb{R}$ is denoted c and is called **the continuum**.

The **continuum hypothesis** is a conjecture by Georg Cantor, one of the founders of Set Theory. It claims that there exists no set S such that

$$\aleph_0 < |S| < c.$$

If true, it would imply that every subset of $\mathbb{R}$ is either countable or numerically equivalent to $\mathbb{R}$.

In 1931, Kurt Godel proved it was impossible to disprove the Continuum Hypothesis from the axioms of set theory. However in 1963, Paul Cohen demonstrated it is also impossible to prove the Continuum Hypothesis from these same axioms. Hence the Continuum Hypothesis is independent of the axioms of set theory!

In general, comparing the cardinalities of sets which are known to not be countable can be difficult. However, we do have the following result:

Theorem 8.19. If A is a set, then $|A| < |\mathcal{P}(A)|$.

Proof. This is trivial if A is finite. Let's consider when A is infinite. We have created an injection $A \to \mathcal{P}(A)$ Suppose for contradiction that there exists a bijective function $f : A \to \mathcal{P}(A)$. For each $x \in A$, let $g(x) = A_x$, where $A_x \subseteq A$. We show there is a subset of A that is distinct from A_x for each $x \in A$. Define $B \subseteq A$ by:

$$B = \{x \in A : x \notin A_x\}$$

By assumption there exists an element $y \in A$ such that $B = A_y$. If $y \in A_y$, then $y \notin B$ by the definition of B. However, if $y \notin A_y$, then according to the definition, $y \in B$. Hence y belongs to exactly one of B and A_y, so $A_y \neq B$, a contradiction! □

In particular, there is no largest set. Moreover, there is no reason to assume there is no cardinality falling between $|A|$ and $|\mathcal{P}(A)|$ for any set A.

8.5 The Schroder-Bernstein Theorem

Definition 8.20. Let $f : A \to B$ be a function and $D \subseteq A$. The **restriction** of f to D is the function $f|_D : D \to B$ for which $f|_D(x) = f(x)$ for all $x \in D$. Note that if f is injective, $f|_D$ is as well. On the other hand, if f is not injective, $f|_D$ can be - for example the function $f(x) = x^2$ on $\mathbb{R}$ is not injective, but restricted to $[0, \infty)$ it is.

If $f : A \to B$ and $g : C \to D$ are functions with A, C disjoint, we can define a function $h : A \cup C \to B \cup D$ by:

$$h(x) : \begin{cases} f(x) & x \in A \\ g(x) & x \in B \end{cases}$$

If f and g are surjective, then so is h, but if f and g are injective, h is not necessarily injective. A sufficient (but not necessary) condition for injectivity is for $B \cap D = \varnothing$.

Finally, note let $B \subseteq A$ be nonempty sets and let $f : A \to B$. Since $B \subseteq A$, $f(x) \in A$ and $f(f(x)) \in B$. We can recursively apply this logic to define in this case, the function $f^1(x) = f(x)$ and for $k > 1$, $f^k(x) = f(f(\ldots(x))\ldots) = f^{k-1}(f(x))$. For example, if $f : \mathbb{Z} \to 2\mathbb{Z}$ is defined by $f(n) = 4n$, then $f^1(3) = 12, f^2(3) = f(f(3)) = 48$.

Theorem 8.21. Let A and B be nonempty sets such that $B \subseteq A$. If there exists an injective function from A to B, there exists a bijective function from A to B.

Proof. See book □

From what we know of inqualities of real numbers, one would expect that if $|A| \leqslant |B|$ and $|B| \leqslant |A|$, then $|A| = |B|$. This is correct, and is the result of the Schroder-Bernstein Theorem

Theorem 8.22. If A and B are sets satisfying $|A| \leqslant |B|$ and $|B| \leqslant |A|$, then $|A| = |B|$.

Proof. Since $|A| \leqslant |B|$ and $|B| \leqslant |A|$ there are injective functions $f : A \to B$ and $g : B \to A$. Then $g_1 : B \to g(B)$ (the same function with restricted codomain) is a bijection. So $g_1^{-1} : g(B) \to B$ exists and is bijective too.
Since $f : A \to B$ and $g_1 : B\ tog(B)$ are injective functions, it follows that $g_1 \circ f : A \to g(B)$ is an injective function. Because $g(B) \subseteq A$, by the previous theorem, there exists a bijective function $h : A \to g(B)$. Thus $h : A \to g(B)$ and $g_1^{-1} : g(B) \to B$ are bijective functions, and therefore $g_1^{-1} \circ h : A \to B$ is a bijective function as desired. □

We end this discussion of infinities by stating perhaps a surprising fact.

Theorem 8.23. $\mathbb{P}(\mathbb{N})$ and $\mathbb{R}$ are numerically equivalent.

9 Number Theory

We will conclude the course with some more work in Modular Arithmetic and Number Theory. [At this point, I began using a separate set of notes which are not included]