An Introduction to Mathematical Reasoning

Matthew M. Conroy and Jennifer L. Taggart

University of Washington

Contents

Chapter 1

Preliminaries

1.1 Elementary properties of the integers

A ***statement*** is a sentence (written in words, mathematical symbols, or a combination of the two) that is either true or false.

Example 1.1. Determine whether each of the following is a statement. If it is a statement, determine whether it is TRUE or FALSE.

- 4+12 = 16

  This is a TRUE statement.

- $x + 4$

  This is not a statement. It is not a complete sentence.

- $-3 > 10$

  This is a FALSE statement.

- $x > 10$

  This is not a statement. Grammatically, it is a complete sentence, written in mathematical symbols, with a subject (x) and a predicate (*is greater than 10*). But the sentence is neither true nor false, since the value of x isn't specified.

- If $x = 11$, then $x > 10$.

  This is a TRUE statement.

- There exists a negative integer n such that $n > 2$.

  This is a FALSE statement.

- In the year 2015, there were at least four U.S. states with a name beginning with the letter "A."

  This is a TRUE statement.

- For every integer n, $(-n)^2 = n^2$.

  This is a TRUE statement.

- Is the number 20 an even number?

  This is not a statement. A question is neither true nor false.

A ***proof*** is a piece of writing that demonstrates that a particular statement is true. A statement that we prove to be true is often called a ***proposition*** or a ***theorem***. We construct proofs using logical arguments and statements that we already know to be true. But the proofs of those statements must depend on previously-proved statements and so on. If we keep tracing the statements back far enough, we must get to a point where we use a statement that we assume to be true without proof. A statement that we assume without proof is an ***axiom***.

At the beginning of this course, most of the statements you will prove will be about integers. We denote the set of ***integers*** by the letter $\mathbb{Z}$:

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

To indicate that x is an integer, we write $x \in \mathbb{Z}$, read as "x is an element of $\mathbb{Z}$."

In this set, the notion of *equality* has the following properties:

- $x = x$ for every integer x. (That is, equality is *reflexive*.)
- For every pair of integers x and y, if $x = y$, then $y = x$. (That is, equality is *symmetric*.)
- For any integers x, y, and z, if $x = y$ and $y = z$, then $x = z$. (That is, equality is *transitive*.)

(The integers form a subset of the set $\mathbb{R}$ of ***real numbers***. The set $\mathbb{R}$ should be familiar to you from your study of calculus. The set of ***rational numbers***, $\mathbb{Q}$, which consists of numbers that can be written in the form $\frac{m}{n}$, where m and n are integers and $n \neq 0$, is also a subset of $\mathbb{R}$.)

Table 1.1 contains statements about the integers, all of which should be familiar as the building blocks of basic algebra, that we will use without proof in this course. Some of these statements would be considered axioms, while others would be propositions proved from those axioms. In this course, we will not distinguish.

Note that we define ***subtraction*** by $a - b = a + (-b)$ and we treat the expression $a > b$ as equivalent to the expression $b < a$.

When you write proofs in this course, you **may**

- use any of the EPIs without proof
- make assertions about sums, products, and signs of *specific* integers without proving them (like $4 + 2 = 6$, $-5 \cdot 7 = -35$, and $62 > 0$); and
- cite any result proved in class or in your assigned homework.

You must prove any other statement you claim is true.

Elementary Properties of the Integers (EPIs)

Suppose a, b, c, and d are integers.

1. **Closure:** $a + b$ and ab are integers.
2. **Substitution of Equals:** If $a = b$, then $a + c = b + c$ and $ac = bc$.
3. **Commutativity:** $a + b = b + a$ and $ab = ba$.
4. **Associativity:** $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.
5. **The Distributive Law:** $a(b + c) = ab + ac$
6. **Identities:** $a + 0 = 0 + a = a$ and $a \cdot 1 = 1 \cdot a = a$.
   0 is called the ***additive identity***.
   1 is called the ***multiplicative identity***.
7. **Additive Inverses:** There exists an integer $-a$ such that $a + (-a) = (-a) + a = 0$.
8. **Trichotomy:** Exactly one of the following is true:
   $a > 0$, $-a > 0$, or $a = 0$.
9. **The Well-Ordering Principle:** Every non-empty set of positive integers contains a smallest element.
10. $a \cdot 0 = 0$
11. If $a + c = b + c$, then $a = b$.
12. $-a = (-1) \cdot a$
13. $(-a) \cdot b = -(ab)$
14. $(-a) \cdot (-b) = ab$
15. If $ab = 0$, then $a = 0$ or $b = 0$.
16. If $a \leq b$ and $b \leq a$, then $a = b$.
17. If $a < b$ and $b < c$, then $a < c$.
18. If $a < b$, then $a + c < b + c$.
19. If $a < b$ and $0 < c$, then $ac < bc$.
20. If $a < b$ and $c < 0$, then $bc < ac$.
21. If $a < b$ and $c < d$, then $a + c < b + d$.
22. If $0 \leq a < b$ and $0 \leq c < d$, then $ac < bd$.
23. If $a < b$, then $-b < -a$.
24. $0 \leq a^2$, where $a^2 = a \cdot a$.
25. If $ab = 1$, then either $a = b = 1$ or $a = b = -1$.

NOTE: Properties 17-23 hold if each $<$ is replaced with $\leq$.

Table 1.1: Elementary Properties of the Integers

Example 1.2. Below is a formal proof of the proposition: if a, b and c are integers, and $c = a + b$, then $a = c - b$. What justifies each step?

Proposition: If a, b and c are integers, and $c = a + b$, then $a = c - b$.

Proof.

Step	Justification
Suppose a, b and c are integers and $c = a + b$.	Hypothesis
b has an additive inverse, $-b$.	Additive Inverses
$c + (-b) = (a + b) + (-b)$	Substitution of Equals
$c + (-b) = a + (b + (-b))$	Associativity of Addition
$c + (-b) = a + 0$	Additive Inverses
$c + (-b) = a$	Additive Identity
$a = c + (-b)$	Symmetry of equality
$a = c - b$	Definition of subtraction

Your proofs in this course will generally be written in paragraph form, rather than a table. This example is simply an exercise to help you get familiar with the Elementary Properties.

1.2 Definitions

A ***definition*** is an agreement between the writer and the reader as to the meaning of a word or phrase. A definition requires no proof. The terms we define in this chapter are likely already familiar to you but you should pay attention to the precision with which they are written.

1.2.1 absolute value

Definition 1.1. Let n be an integer. We define the ***absolute value*** of n to be the integer $|n|$ given by the multi-part function

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

Example 1.3.

- Since $100 \geq 0$, $|100| = 100$.
- Since $0 \geq 0$, $|0| = 0$.
- Since $-79 < 0$, $|-79| = -(-79) = 79$.

1.2.2 divisibility

Definition 1.2. Suppose a and b are integers. We say that a ***divides*** b or that b is ***divisible*** by a and write $a \mid b$ if there exists an integer c such that $b = ac$. If there exists no such integer c, then we say that a ***does not divide*** b or that b is ***not divisible by*** a and we write $a \nmid b$.

Example 1.4.

- Since $56 = 7 \cdot 8$, we say that 7 divides 56 or that 56 is divisible by 7.
- $2 \mid 6$ since $6 = 2 \cdot 3$.
- 1 is not divisible by 13 since there is no integer c such that $1 = 13c$. (This follows from EPI #25: *If* $ab = 1$, *then either* $a = b = 1$ *or* $a = b = -1$. This means that the only integers that divide 1 are 1 and -1.)
- $4 \nmid 6$ since there is no integer c with the property that $6 = 4c$. (This is a statement that requires proof.)
- $-10 \mid 150$ since $150 = (-10)(-15)$.

Something to note about the definition of the word *divides*: it does not involve the arithmetic operation of division, only multiplication. In particular, it will be very tempting for some students to say that 2 divides 6 because $\frac{6}{2}$ is an integer or that 4 does not divide 6 because $\frac{6}{4}$ is not an integer. THIS SHOULD BE AVOIDED! This is hard to get used to at first, especially since it's right there in the word *divides*! But in the first few chapters of this text, we will deal only with integers, which means we only want to use operations between integers that always give integers. By the Closure property, if we add or multiply two integers, we get an integer. Further, the definition of subtraction and the Closure property guarantee that, when we subtract two integers, we get an integer. On the other hand, if we divide the integer 6 by the integer 4, we get the non-integer rational number $\frac{6}{4}$, which you should consider off-limits until later chapters (even though $\frac{6}{4}$ is a perfectly lovely number).

1.2.3 even and odd

Definition 1.3. An integer a is ***even*** if $a = 2k$ for some integer k. An integer a is ***odd*** if $a = 2k + 1$ for some integer k.

For example, -8 is even since $-8 = 2(-4)$. Similarly, $11 = 2(5) + 1$ and, thus, 11 is odd.

Note that the even integers are those that are divisible by 2.

We will prove later in the text that every integer is either even or odd, never both.

Definition 1.4. Two integers that are either both even or both odd are said to have the ***same parity***. If one integer is even and the other is odd, then the two have ***opposite parity.***

For example, 11 and -13 have the same parity, 26 and -100 have the same parity, and 1 and 2 have opposite parity.

1.3 Exercises

1.1. Prove each of the following. For this exercise only, write your proofs in table form (like in Example 1.2 in the text) with a column for each **Step** and its **Justification**. Your justifications may be any of the Elementary Properties of the Integers or a previous part of this exercise.

(a) If $a + b = a$, then $b = 0$.

(b) If a, b, c and d are integers, then $(a + b) + (c + d) = (a + c) + (b + d)$.

(c) If a, b, and c are integers such that $ac = bc$ and $c \neq 0$, then $a = b$.

(d) *Binomial Expansion:* If a and b are integers, then $(a+b)^2 = a^2 + 2ab + b^2$. (Note: for any integer x, $x^2 = x \cdot x$ and $x + x = 2x$. Also, by the Associative property, for any integers a, b and c, $a + b + c = (a + b) + c = a + (b + c)$.)

1.2. Determine whether each of the following statements is TRUE or FALSE. If the statement is TRUE, write a sentence or two explaining why. (This does not need to be a formal proof.) If the statement is FALSE, give a counterexample.

(a) If a is an integer and $a < -5$, then $|a| > 5$.

(b) Suppose a and b are integers. If $b > 0$, then $|a - b| < |a|$.

(c) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

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

(e) If a is an integer, then $2a$ and $3a$ have opposite parity.

(f) If a is an odd integer, then $2a$ and $3a$ have opposite parity.

Chapter 2

Logic and mathematical language

2.1 Negations

If P is a statement, then P has a ***truth value***: true or false. The ***negation*** of the statement P is the statement *it is not the case that P.* We may abbreviate the negation of P by writing *not* P.

A statement and its negation have opposite truth values. We often reword a statement's negation so that its meaning is clearer.

Example 2.1.

- Consider the statement

  P: 42 is even.

  The negation of P is the statement

  not P: It is not the case that 42 is even.

  The following statement has the same meaning but adds clarity

  not P: 42 is not even.

  Also, since every number that is not even is odd, we could also write

  not P: 42 is odd.

  Note that, in this example, P is true and *not* P is false.

- Consider the statement

  Q: There are fewer than three even integers between 0 and 10.

  The negation of Q is the statement

  not Q: There are at least three even integers between 0 and 10.

  Note that, in this example, Q is false and *not* Q is true.

  Also, consider the statement

  R: There are *more than* three even integers between 0 and 10.

  Even though R is true, it is not equivalent to the statement *not* Q.

2.2 And and Or

Consider two statements P and Q.

The statement P ***and*** Q is true provided P is true and Q is true. Otherwise, $P \; and \; Q$ is false.

The statement P ***or*** Q is true provided P is true, Q is true, or both are true. Otherwise, $P \; or \; Q$ is false.

(Colloquially, when we say *or*, we often mean an **exclusive** or. That is, when you say, *I'll have an apple or a banana*, you likely mean that you'll have one or the other but not both. In mathematics, an *or* is generally **inclusive**. That is, if you offer a mathematician an apple *or* a banana, don't be surprised if she takes both.)

Example 2.2.

P:	42 is even.	T
Q:	42 is divisible by 7.	T
R:	42 is odd.	F
S:	42 is divisible by 11.	F
$P \; and \; Q$:	42 is even and divisible by 7.	T
$P \; and \; R$:	42 is even and odd.	F
$Q \; and \; R$:	42 is divisible by 7 and is odd.	F
$R \; and \; S$:	42 is odd and divisible by 11.	F
$P \; or \; Q$:	42 is even or divisible by 7.	T
$P \; or \; R$:	42 is even or odd.	T
$Q \; or \; R$:	42 is divisible by 7 or is odd.	T
$R \; or \; S$:	42 is odd or divisible by 11.	F

2.2.1 Negation of *and* and *or* statements

To illustrate how we negate an *and* statement, let's consider the following scenario: at an amusement park, you must be at least 5 feet tall AND weigh at least 80 pounds to ride the roller coaster. A person must meet *both* the height and weight requirements in order to ride. Clearly, anyone who is less than 5 feet tall *and* who weighs less than 80 pounds will not be allowed to ride. Further, those who meet one requirement but not the other will also be denied entry. That is, a potential rider will be turned away if she is less than 5 feet tall OR weighs less than 80 pounds (or both).

In general, the statement $not \; (P \; and \; Q)$ has the same meaning as the statement $(not \; P) \; or \; (not \; Q)$.

To illustrate the negation of an *or* statement, let's consider a benefit concert for a food bank where admission is \$10 OR an item of non-perishable food. Anyone who donates either \$10 or an item of food (or both) is admitted; a person who doesn't give \$10 AND does not give food is not admitted.

In general, the statement $not \; (P \; or \; Q)$ has the same meaning as the statement $(not \; P) \; and \; (not \; Q)$.

Example 2.3. Give a meaningful negation of each of the following.

- Tina is at the dentist or at the movies.

  negation: Tina is not at the dentist and she is not at the movies.

- I did the laundry and took out the garbage.

negation: I didn't do the laundry or I didn't take out the garbage.

- n divides 100 and does not divide 40.
  negation: n divides 40 or does not divide 100.
- $n = -7$ or $|n| > 9$.
  negation: $n \neq -7$ and $|n| \leq 9$.

2.3 If, then

Many of the statements you'll prove in this course will be of the form *if P, then Q*. In practical terms, we can think of this statement as being the same as *if P is true, then Q is true*. Even more colloquially, we can interpret it as *we can't have P without Q.*

All of the following have the same meaning:

If P, then Q.
P implies Q.
$P \Rightarrow Q$ (read P *implies* Q)
Q, if P.
P only if Q.
Q when (or whenever) P.
Q is necessary for P.
P is sufficient for Q.

The truth value of the statement $P \Rightarrow Q$ depends on the truth values of P and Q. Formally, $P \Rightarrow Q$ is true **unless** P is true and Q is false.

To illustrate this, we'll think of $P \Rightarrow Q$ as an agreement: Joe makes a deal with his parents that every time he washes the dishes after dinner, he gets \$5. He's not required to do the dishes, but when he does, his parents promise to give him \$5. Let P be the statement *Joe did the dishes* and Q be the statement *Joe got \$5*. The agreement is

$P \Rightarrow Q$: If Joe did the dishes, then he got \$5.

In the case that Joe did the dishes (P is true) and got paid (Q is true), the agreement is met ($P \Rightarrow Q$ is true). In the case that Joe didn't do the dishes (P is false) and didn't get \$5 (Q is false), the agreement is met ($P \Rightarrow Q$ is true). But, since Joe isn't required to wash the dishes, his parents may choose to give him \$5 for some other reason. That is, in the case that Joe didn't wash the dishes (P is false) and got \$5 anyway (Q is true), the agreement is still met ($P \Rightarrow Q$ is true). The only instance in which the agreement is not met ($P \Rightarrow Q$ is false) is in the case that Joe did wash the dishes (P is true) but did not get the money from his parents (Q is false). This is summarized in the following table.

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

Let's stick with this story to discuss the negation of $P \Rightarrow Q$. Joe and his parents make this agreement about the dishes. Joe claims that his parents broke their verbal contract, while the parents deny Joe's

claim. That is, Joe's parents say that $P \Rightarrow Q$ is true, while Joe says that *not*$(P \Rightarrow Q)$ is true. If you were Joe's lawyer, what evidence would you have to provide to win the case? You would need to show that Joe washed the dishes and did not get paid. That is, you would need to show that P *and (not* Q*)* is true.

In general, the statement *not* $(P \Rightarrow Q)$ has the same meaning as the statement P *and (not* Q*)*.

Example 2.4. In each of the following, write the statement in *if, then* form and give its negation.

- The crust is brown only if the pie is done.
  if, then form: If the crust is brown, then the pie is done.
  negation: The crust is brown and the pie is not done.
- I take an umbrella whenever it is raining and I have to leave the house.
  if, then form: If it is raining and I have to leave the house, then I take an umbrella.
  negation: It is raining and I have to leave the house and I am not taking an umbrella.

2.3.1 Converse and Contrapositive

We associate two other *if, then* statements with the statement $P \Rightarrow Q$.

Definition 2.1. The ***converse*** of $P \Rightarrow Q$ is the statement $Q \Rightarrow P$. The ***contrapositive*** of $P \Rightarrow Q$ is the statement *(not* Q*)* $\Rightarrow$ *(not* P*).*

The statements $P \Rightarrow Q$ and its converse $Q \Rightarrow P$ need not have the same truth value. For example, it is true that, if Tom's cat is hungry, then she meows. But it is not true that, if Tom's cat meows, then she is hungry. (She also meows when she sees a bug she wants to chase, whether or not she is hungry.)

On the other hand, a statement and its contrapositive always have the same truth value. In the same example, assuming that it is true that if Tom's cat is hungry, then she meows, then Tom's cat meows whenever she is hungry. (Remember that "$P \Rightarrow Q$" has the same meaning as "Q whenever P.") This means that, if the cat does not meow, then she is not hungry.

Example 2.5. In each of the following, write the statement in *if, then* form and give its converse and contrapositive.

- The street gets wet whenever it is raining.
  if, then form: If it is raining, then the street gets wet.
  converse: If the street gets wet, then it is raining.
  contrapositive: If the street doesn't get wet, then it is not raining.
- $n > 0 \Rightarrow |n| > 0$
  if, then form: If $n > 0$, then $|n| > 0$.
  converse: If $|n| > 0$, then $n > 0$.
  contrapositive: If $|n| \leq 0$, then $n \leq 0$.
- n is a prime number larger than 2 only if n is odd.
  if, then form: If n is a prime number larger than 2, then n is odd.
  converse: If n is odd, then n is a prime number larger than 2.
  contrapositive: If n is not odd, then n is not a prime number larger than 2.

2.3.2 if and only if

Definition 2.2. The statement P *if and only if* Q, written $P \Leftrightarrow Q$, is equivalent to the statement
($P \Rightarrow Q$) and ($Q \Rightarrow P$).

$P \Leftrightarrow Q$ is true provided P and Q have the same truth value. If P and Q do not have the same truth value, then $P \Leftrightarrow Q$ is false.

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

As an example, *I am alive if and only if my heart is beating*. This is equivalent to saying, *If I am alive, then my heart is beating, and, if my heart is beating, then I am alive.*

Negating $P \Leftrightarrow Q$ requires almost everything we have discussed so far about negations:

not$(P \Leftrightarrow Q)$	is equivalent to	*not*$[(P \Rightarrow Q)$ *and* $(Q \Rightarrow P)]$
	which is equivalent to	$[$*not*$(P \Rightarrow Q)]$ *or* $[$*not*$(Q \Rightarrow P)]$
	which is equivalent to	*(P and not Q) or (Q and not P).*

A negation of *I am alive if and only if my heart is beating* is:
I am alive and my heart is not beating, or my heart is beating and I am not alive.

2.4 Quantifiers

Suppose n is an integer and let $P(n)$ be a statement about n. The truth value of $P(n)$ may change when the value of n changes. If $P(n)$ is true for at least one integer n, then we say
There exists n such that $P(n)$.

If $P(n)$ is true no matter what value n takes, then we say
For all n, $P(n)$.

The symbol $\exists$ may be substituted for the phrase *there exists* and the symbol $\forall$ may be substituted for the phrase *for all*.

Example 2.6. Determine whether each statement is true or false. (In each, assume n is an integer.)

- There exists n such that $|n| > 0$.

  In this example, $P(n)$ is the statement $|n| > 0$. The statement $P(14)$ is true since $|14| = 14 > 0$. There are many other values of n for which $P(n)$ is true. Since $P(n)$ is true for at least one integer n, the statement, *there exists n such that* $|n| > 0$, is true.

- For all n, $|n| > 0$.

  Again, $P(n)$ is the statement $|n| > 0$. The statement $P(0)$ is false since $|0| = 0$, which is not greater than 0. So the statement, *for all n,* $|n| > 0$, is false.

- $\forall n$, $|n| \geq 0$.

  This time, we have changed $P(n)$ slightly to $|n| \geq 0$. Since $P(n)$ is true regardless of the value of n, the statement, *for all* n, $|n| \geq 0$, is true.

- $\exists n$ such that $|n| < 0$.

  This statement is false. There is no value of n for which $|n| < 0$ is true.

2.4.1 Negations of quantified statements

The negation of *for all* n, $P(n)$ is:

there exists n *such that not*$(P(n))$.

The negation of *there exists* n *such that* $P(n)$ is:

for all n, *not*$(P(n))$.

If the nature of a variable is assumed, we often leave off the universal quantifier *for all*. For example, in the first few chapters of this book we are mainly discussing the set $\mathbb{Z}$ of integers. With that in mind, you can expect to see statements like:

If n *is divisible by 4, then* n *is even,*

when what we actually mean is:

For all integers n*, if* n *is divisible by 4, then* n *is even.*

There is an implied *for all integers* n at the beginning of the sentence. Its negation is therefore:

There is an integer n *such that* n *is divisible by 4 and* n *is not even.*

Example 2.7. Negate the statement. Reword when necessary to make the meaning clear.

- There exists n such that $|n| < 0$.

  negation: For all n, it is not the case that $|n| < 0$.

  negation reworded: For all n, $|n| \geq 0$.

- For all n, $|n| = 0$.

  negation: There exists n such that it is not the case that $|n| = 0$.

  negation reworded: There exists n such that $|n| \neq 0$.

- There exists n that is even and greater than 100.

  negation: For all n, it is not the case that n is even and greater than 100.

  negation reworded: For all n, n is odd or $n \leq 100$.

- If $n < 0$, then $n - 1 < 0$.

  Note that there is an understood *for all* n at the beginning of this statement:

  For all n, if $n < 0$, then $n - 1 < 0$.

  negation: There exists n such that it is not the case that, if $n < 0$, then $n - 1 < 0$.

  negation reworded: There exists n such that $n < 0$ and $n - 1 \geq 0$.

2.5 Summary of Negations

The negations of common logical expressions are summarized in the following table.

statement	**negation**
P *and* Q	(*not* P) *or* (*not* Q)
P *or* Q	(*not* P) *and* (*not* Q)
$P \Rightarrow Q$	P *and* (*not* Q)
$P \Leftrightarrow Q$	(P *and not* Q) *or* (Q *and not* P)
$\forall n$, $P(n)$	$\exists n$ such that *not*$(P(n))$
$\exists n$ such that $P(n)$	$\forall n$, *not*$(P(n))$

2.6 Exercises

2.1. Write each of the following in *if-then* form and give its converse and contrapositive.

(a) $n = 4k$ implies n is even.

(b) Angela sleeps in only if it is Saturday.

(c) $|a| > 0$ whenever $a \neq 0$.

2.2. Give, if possible, an example of a TRUE *if-then* statement for which:

(a) the converse is true.

(b) the converse is false.

(c) the contrapositive is true.

(d) the contrapositive is false.

2.3. Write useful negations of the following statements in english. (In most cases, you should write the statement symbolically with quantifiers, negate the resulting expression, and then rewrite in english.)

(a) $5 \mid 17$ or $3 < 10$.

(b) It is raining and Charlie is cold.

(c) If it is raining, then Charlie is cold.

(d) For every real number x, there exists a real number y such that $x + y = 0$.

(e) There exists a real number z such that for all real numbers y, $zy = 0$.

(f) For all pairs (x, y) of real numbers, there is a real number k such that $x^k + y^k = 2$.

(g) For every integer a, $|a| \geq 0$.

(h) There exists an integer a such that $a^2 - 1 < 2$.

(i) For every integer a, there exists an integer b such that $a < b$.

(j) For all real x, if $x \neq 0$, then $x^2 > 0$.

(k) For every $M > 0$, there is an $N > 0$ such that, for every $n > N$, $n^2 + 1 > M$.

(l) For all integers a and b, if a and b are odd, then $4|(a - b)$ or $4|(a + b)$.

(m) $|a| > 0$ if and only if $a \neq 0$.

2.4. Write useful contrapositives of the following sentences. Express the contrapositives as sentences, not as symbolic expressions. Reword, if necessary, to clarify the meaning of the contrapositive.

(a) If you earned at least 90% in my class, then you got an A.

(b) If x and y are integers, then $x + y$ is an integer.

(c) If x and y are integers, and at least one of them is even, then xy is even.

(d) If it rains or snows, then I will go for a walk but I will not ride my bike.

Chapter 3

Writing Proofs

Again, a proof is a piece of writing that demonstrates that a particular statement is true. A proof is generally written in paragraph form using complete sentences in a mix of words and mathematical symbols.

Things you may do in a proof:

- **state an assumption**

  Assumptions usually start with one of the following words: *suppose*, *let*, *assume*.

  For example,

  - Suppose m and n are positive integers.
  - Assume that $m \leq n$.
  - Let $\ell = n - m$.

- **make a statement that you and your audience know to be true**

  In this course, these include the elementary properties given in section 1.1 and results proved in class or in assigned homework.

- **apply principles of mathematical logic to make deductions and draw conclusions**

  Consider, for example, the following excerpts from proofs:

  - *We have just shown that the integer n cannot be both divisible by 2 and divisible by 3. That is, n is not divisible by 2 or n is not divisible by 3.*
    The underlined phrase is an application of the principle that $not(P \ and \ Q)$ is equivalent to $(not \ P) \ or \ (not \ Q)$. We're simply rewording a negation to add clarity.
  - *Suppose the integer n is divisible by 4. We have shown that, if n is divisible by 4, then n is also divisible by 2. Thus, n is divisible by 2.*
    We suppose a statement P is true and showed that the statement $P \Rightarrow Q$ is true. We may therefore conclude that the statement Q is true.

- **remind the reader what you need to show**

  While you never want to state your conclusion until you have actually proven that it is true, in longer proofs with many steps, it may be helpful to remind the reader (and yourself) where you

are headed. Start a sentence with a phrase like *We need to show...* or *It remains to show that...* when you want to remind the reader the conclusion you are working toward.

As an example, consider the beginning of this proof that the sum of two odd integers is even.

Proof. Suppose a and b are odd. Then $a = 2k_1 + 1$ and $b = 2k_2 + 1$ for some integers k_1 and k_2. We want to show that $a + b = 2k$ for some k. ... (The proof would continue from there.)

3.1 Direct Proofs

To prove an *if, then* statement directly, start the proof by assuming your ***hypotheses*** (the statements after the *if*) and use definitions, logic, EPIs, and previously proved results to reach the desired ***conclusion*** (the statement after the *then*).

As an example, we'll prove the following theorem.

Theorem 3.1. If a and b are even integers, then $a + b$ is even.

Proof. Suppose a and b are even integers.

This means $a = 2k_1$ and $b = 2k_2$ for some integers k_1 and k_2.

Then $a + b = 2k_1 + 2k_2 = 2(k_1 + k_2)$.

Let $k = k_1 + k_2$.

Then k is an integer and $a + b = 2k$.

Thus, $a + b$ is even. ■

In the previous proof, with the exception of the assumptions and the use of the definition of *even*, every step is due to one of the Elementary Properties of the integers. When a step is justified by an EPI or definition, it is usually not necessary to cite it explicitly. When you construct a proof, think through the justification for each step. If you find that a step cannot be justified by an EPI or definition, then you may need to break it down further or cite another result already proven.

As an exercise, let's break down the above proof and examine the justification for each step to make sure that each statement is sufficiently supported.

statement in proof	**justification**
Suppose a and b are even integers.	assumption (we assume our hypothesis)
This means $a = 2k_1$ and $b = 2k_2$ for some integers k_1 and k_2.	definition of *even*
Then $a + b = 2k_1 + 2k_2$.	Substitution of Equals
$= 2(k_1 + k_2)$	Distributive Law
Let $k = k_1 + k_2$.	assumption (we introduce a new variable and assume its properties)
Then k is an integer	Closure property
and $a + b = 2k$.	Substitution of Equals
Thus, $a + b$ is even.	definition of *even*

Here is another example of a direct proof of an *if, then* statement.

Theorem 3.2. Suppose a, b, and c are integers. If $a|b$ and $b|c$, then $a|c$.

Proof. Suppose a, b, and c are integers and that $a|b$ and $b|c$.

Then $b = ak$ for some integer k and $c = b\ell$ for some integer ℓ.

This means that $c = b\ell = (ak)\ell = a(k\ell)$.

Since $k\ell$ is an integer, this means that $a|c$. ■

Note that each step of this proof after the initial assumption of the hypotheses follows by one of the EPIs or by the definition of divisibility.

3.2 Proof by Cases

Consider the following theorem:

Theorem 3.3. The product of two consecutive integers is even.

This can be reworded: If n is an integer, then $n(n+1)$ is even. If you had to prove this statement, you might think something like, "Well, if n is even then it's obvious why $n(n+1)$ is even." This is an indication that a divide-and-conquer approach may be useful: prove the statement in the case that n is even and prove it in the case that n is odd and you've proved it for every possible integer n.

Proof. Suppose n is an integer.

Then n is either even or odd.

Case 1: Suppose n is even.

Then $n = 2k$ for some integer k.

This means that $n(n+1) = (2k)(n+1) = 2[k(n+1)]$.

We know that $k(n+1)$ is an integer.

Thus, $n(n+1)$ is even in the case that n is even.

Case 2: Suppose instead that n is odd.

Then $n = 2k+1$ for some integer k.

This means that $n(n+1) = n(2k+1+1) = n(2k+2) = 2[n(k+1)]$.

We know that $n(k+1)$ is an integer.

Thus, $n(n+1)$ is even in the case that n is odd.

■

The above proof has two cases but you may use any number of cases in a proof. A proof by cases is sometimes called a ***proof by exhaustion***.

Since the absolute value of a number is given by a piece-wise defined function (page 10), a proof about absolute values may be handled by a proof by cases.

Theorem 3.4 (Elementary Properties of Absolute Value)**.** Suppose a and b are integers. Then:

(a) $|a| \geq 0$.

(b) $|-a| = |a|$.

(c) $-|a| \leq a \leq |a|$.

(d) $|a|^2 = a^2$.

(e) $|ab| = |a||b|$.

(f) $|a| \leq |b|$ if and only if $-|b| \leq a \leq |b|$.

Proof. (a) Let a be an integer.

Then either $a \geq 0$ or $a < 0$.

Case 1: Suppose $a \geq 0$.
By definition of absolute value, this means that $|a| = a \geq 0$.

Case 2: Suppose $a < 0$.
By definition of absolute value, this means that $|a| = -a$.
Since $a < 0$, $-a > 0$.
Thus, $|a| = -a > 0$.

Therefore, $|a| \geq 0$ for every integer a.

(b) Let a be an integer.

Then either $a > 0$, $a = 0$, or $a < 0$.

Case 1: Suppose $a > 0$.
Then $-a < 0$.
Then $|a| = a$ (since $a > 0$) and $|-a| = -(-a)$ (since $-a < 0$), both by definition of absolute value.
We then have $|-a| = -(-a) = a = |a|$.
Thus, $|-a| = |a|$.

Case 2: Suppose $a = 0$.
Then $|a| = |0| = 0$ by definition of absolute value.
Also $-a = -0 = 0$ and, again by definition of absolute value, $|-a| = |0| = 0$.
Thus, $|a| = |-a|$.

Case 3: Suppose $a < 0$.
Then $-a > 0$.
By definition of absolute value, $|a| = -a$ (since $a < 0$) and $|-a| = -a$ (since $-a > 0$).
Thus, $|-a| = |a|$.

Therefore, $|-a| = |a|$ for every integer a.

We leave the proofs of parts (c)-(f) as exercises.

■

The following theorem is quite useful. It may be proved by cases but we give a shorter proof that utilizes the Elementary Properties of Absolute Value.

Theorem 3.5 (The Triangle Inequality)**.** If a and b are integers, then $|a+b| \leq |a| + |b|$.

Proof. Suppose a and b are integers.

By part (c) of the Elementary Properties of Absolute Value, we have

$$-|a| \leq a \leq |a| \text{ and } -|b| \leq b \leq |b|.$$

By the elementary properties of the integers, we add the inequalities and we then have

$$-|a| + (-|b|) \leq a + b \leq |a| + |b|.$$

That is,

$$-(|a| + |b|) \leq a + b \leq |a| + |b|.$$

By part (f) of the Elementary Properties of Absolute Value, this gives

$$|a+b| \leq |a| + |b|.$$

■

3.3 Contrapositive

Recall that the statement $P \Rightarrow Q$ has the same truth value as its contrapositive $(not\ Q) \Rightarrow (not\ P)$. Therefore, if you wish to prove that $P \Rightarrow Q$ is true, you may prove instead that its contrapositive is true. This is called ***proof by contrapositive***: you suppose $not\ Q$ as your hypothesis and show that, under that assumption, $not\ P$ is true.

Theorem 3.6. Suppose n is an integer. If n^2 is even, then n is even.

Proof. Suppose n is an integer that is not even.

That is, suppose n is odd.

Then $n = 2k + 1$ for some integer k, and by Exercise 1.1(d) we have

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

Since $2k^2 + 2k$ is an integer, this means that n^2 is odd.

Thus, if n^2 is even, it must be the case that n is even. ■

Theorem 3.7. Let n be an integer. If $n^2 + 2n < 0$, then $n < 0$.

Proof. Let n be an integer and suppose $n \geq 0$.

We know that $n^2 \geq 0$.

By elementary properties of the integers, we then have

$$n^2 + 2n \geq 0 + 2n = 2n \geq 0.$$

Thus, if $n^2 + 2n < 0$, it must be the case that $n < 0$. ■

As a reminder, the statement $P \Rightarrow Q$ **always has the same truth value as its contrapositive** $(not\ Q) \Rightarrow (not\ P)$. However, the statement $P \Rightarrow Q$ **may not have the same truth value as its converse** $Q \Rightarrow P$. For example, the converse of Theorem 3.6 (*if n is even, then n^2 is even*) is TRUE but the converse of Theorem 3.7 (*if $n < 0$, then $n^2 + 2n < 0$*) is FALSE. (Why?)

3.4 Contradiction

In a ***proof by contradiction***, we use the fact that a statement and its negation have opposite truth values. To prove that P is true, suppose instead that $not(P)$ is true and apply logic, definitions, and previous results to arrive at a conclusion you know to be false. Then you may conclude that $not(P)$ must be FALSE and thus P must be TRUE.

Theorem 3.8. No integer is both even and odd.

Proof. Suppose there is an integer n that is both even and odd.

Since n is even, $n = 2k$ for some integer k.

Since n is also odd, $n = 2\ell + 1$ for some integer ℓ.

Then by the elementary properties of integers, we have

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

But this implies that 2 divides 1, which we know is not true since it contradicts EPI 25.

Thus, no integer n is both even and odd. ■

In the previous proof, notice that we made only one assumption (that n was an integer that was both even and odd) and every subsequent step necessarily followed from there. Because the logic of the rest of the proof is valid, when we arrived at a statement that we knew was false, it had to be because our original assumption was false.

As another example of a proof by contradiction, we prove that $\sqrt{2}$ is not a rational number. Recall that the set of rational numbers $\mathbb{Q}$ consists of those real numbers that can be written in the form $\frac{m}{n}$, where m and n are integers and $n \neq 0$.

Theorem 3.9. $\sqrt{2}$ is irrational.

Proof. Suppose for the sake of contradiction that $\sqrt{2}$ is in $\mathbb{Q}$.

Then there exist integers m and n ($n \neq 0$) such that $\sqrt{2} = \frac{m}{n}$.

We may assume that the fraction $\frac{m}{n}$ is in reduced form.

In particular, we may assume that m and n are not both even. (Otherwise, we could reduce the fraction by dividing the numerator and denominator by 2, giving a different fraction that is still equivalent to $\sqrt{2}$.)

Multiplying by n and squaring both sides, we have $2n^2 = m^2$.

This means that m^2 is even, which implies that m is even. (Theorem 3.6.)

So there exists an integer k such that $m = 2k$.

We now have $2n^2 = m^2 = (2k)^2 = 4k^2$, so $2n^2 - 4k^2 = 0$.

Hence, $2(n^2 - 2k^2) = 0$ and since $2 \neq 0$, $n^2 - 2k^2 = 0$, i.e., $n^2 = 2k^2$.

This means that n^2 is even, which again by Theorem 3.6, means n is even.

This contradicts our assumption that n and m are not both even.

Thus, $\sqrt{2}$ is not a rational number. ■

Caution: It is not unusual even for experienced proof-writers to confuse contrapositive and contradiction when proving an *if-then* statement.

To prove the statement $P \Rightarrow Q$

- **by contrapositive:** suppose $not(Q)$ is true and prove that $not(P)$ must follow;
- **by contradiction:** suppose $P \Rightarrow Q$ is FALSE (that is, suppose P and $not(Q)$ are both TRUE) and arrive at a statement that you know is FALSE.

In particular, if you suppose P and $not(Q)$ are TRUE, but never *use* the assumption that P is TRUE, and finally *arrive* at the conclusion that P is FALSE, then you have done a proof by contrapositive, not by contradiction.

Example 3.1. Give two proofs of Theorem 3.10.

Theorem 3.10. Let a be an integer. If a^2 is odd, then a is odd.

Proof by contrapositive. Suppose a is not odd.

That is, suppose a is even.

Then $a = 2k$ for some integer k and $a^2 = (2k)^2 = 2(2k^2)$, which is even.

Since no integer is both even and odd, this means a^2 is not odd.

Thus, if a^2 is odd, then it must be the case that a is odd. ■

Proof by contradiction. Suppose a is an integer with the property that a^2 is odd and a is even.

Then, by Exercise 3.1(a), $a^2 + a$ is odd.

But $a^2 + a = a(a + 1)$.

So $a(a + 1)$ is odd and this contradicts Theorem 3.3, which says that the product of two consecutive integers must be even.

Thus, if a^2 is odd, it must be the case that a is odd. ■

3.5 Proof of an *if-and-only-if* Statement

Recall that $P \Leftrightarrow Q$ has the same meaning as

$$P \Rightarrow Q \; and \; Q \Rightarrow P.$$

In this course, when you prove an *if-and-only-if* statement, you will prove $P \Rightarrow Q$ and then prove $Q \Rightarrow P$. Each of these sub-proofs may be a direct proof, a proof by contrapositive, or a proof by contradiction.

Theorem 3.11. Let a be an integer. Then a is odd if and only if $a^2 - 1$ is even.

Proof.

We will prove one direction (if a is odd, then $a^2 - 1$ is even) directly. We will prove the other direction (if $a^2 - 1$ is even, then a is odd) by contrapositive.

$\Rightarrow$ Suppose a is odd.

Then $a = 2k + 1$ for some integer k.

Then $a^2 - 1 = (2k + 1)^2 - 1 = (4k^2 + 4k + 1) - 1 = 2(2k^2 + 2k)$, which is even.

Thus, if a is odd, then $a^2 - 1$ is even.

$\Leftarrow$ Suppose a is not odd.

That is, suppose a is even.

Then $a = 2k$ for some integer k.

So, $a^2 - 1 = (2k)^2 - 1 = (2k)^2 - 2 + 1 = 2(2k^2 - 1) + 1$, which is odd.

Thus, if $a^2 - 1$ is even, it must be the case that a is odd.

■

3.6 Exercises

3.1. Suppose a and b are integers. Prove each of the following.

(a) If a and b are both odd, then $a + b$ is even.

(b) If a is even and b is odd, then $a + b$ is odd.

(c) If $a + b$ is odd, then a and b must have opposite parity.

3.2. Prove the remaining parts of the Elementary Properties of Absolute Value. (Parts (a) and (b) are proved in the text.)

Suppose a and b are integers.

(c) $-|a| \leq a \leq |a|$.

(d) $|a|^2 = a^2$.

(e) $|ab| = |a||b|$.

(f) $|a| \leq |b|$ if and only if $-|b| \leq a \leq |b|$.

3.3. Let a and b be **negative** integers. Prove that if $a < b$ then $a^2 > b^2$.

3.4. Suppose a and b are **positive** integers. Prove that, if $a|b$, then $a \leq b$.

3.5. Let a, b and c be positive integers. Prove that if $a|b$ and $b|c$, then $a|c$.

3.6. Suppose $a > 0$ and $b \geq 0$ are integers such that $a \mid b$. Prove that, if $b < a$, then $b = 0$.

3.7. We've introduced the concept of the *rational* numbers: a number q is rational if it can be written in the form $\frac{m}{n}$, where m and n are integers and $n \neq 0$. Any real number that is not rational is *irrational*.

In the following problem, you may use these facts about rational numbers:

- Given two rational numbers $\frac{a}{b}$ and $\frac{c}{d}$, we define their sum and product as follows:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

- For any integer $a \neq 0$, $\frac{a}{a} = 1$.
- Every rational number q has a rational additive inverse $-q$ such that $q + (-q) = (-q) + q = 0$.
- Every irrational number r has an irrational additive inverse $-r$ such that $r + (-r) = (-r) + r = 0$.

Prove the following:

(a) If q and r are rational, then $q + r$ and qr are rational.

(b) If q is rational and r is irrational, then $q + r$ is irrational.

(c) If q is rational, $q \neq 0$, and r is irrational, then qr is irrational.

(d) The sum of two irrational numbers may be a rational number.

3.8. Let a and b be integers. Prove that $a^2b + a + b$ is even if and only if a and b are both even.

3.9. Prove that, if n is the product of any four consecutive integers, then $n+1$ is the square of an integer.

Chapter 4

Proofs Involving Quantifiers

4.1 Proofs of *for all* statements

The statement

for all integers x, $P(x)$

is equivalent to the statement

if x *is an integer, then* $P(x)$.

For example, the statement in Theorem 3.4, part (a),

for all integers a, $|a| \geq 0$

and the statement

if a *is an integer, then* $|a| \geq 0$

have precisely the same meaning. Our proof of this theorem began with *let* a *be an integer.* Rather than dealing with all of the integers at once, we selected a single *arbitrary* integer and proved that the conclusion was true for that integer. This is a valuable technique.

As another example we will prove the following theorem.

Theorem 4.1. Let a, b, and c be integers and suppose that $c|a$ and $c|b$. For all integers n and m, $c|(an + bm)$.

Once you assume the hypotheses about a, b, and c, you must prove a statement about every possible pair of integers n and m. There are infinitely many such pairs. Instead of trying to deal with all of these pairs at once, we'll simply assume that we have two *arbitrary* integers n and m and prove that the conclusion is true for those two.

Proof. Let a, b, and c be integers and suppose that $c|a$ and $c|b$.

Then there exist integers k_1 and k_2 such that $a = ck_1$ and $b = ck_2$.

Suppose n and m are integers.

Then $an + bm = (ck_1)n + (ck_2)m = c(k_1n + k_2m)$.

By the Closure property, $k_1n + k_2m$ is an integer.

Thus, c divides $an + bm$. ■

4.2 Proofs of *there exist* statements

In this course, when we prove a statement of the form *there exists an n such that $P(n)$*, we will often do so ***by construction.*** That is, we will find such an n and then demonstrate that $P(n)$ is true.

Example 4.1. Prove the following statements.

- There exist integers m and n such that $10m + 13n = 3$.

  Proof. Let $m = -1$ and $n = 1$.

  Then m and n are integers and $10m + 13n = 10(-1) + 13(1) = 3$.

  Thus, there exist integers m and n such that $10m + 13n = 13$. ■

- For every integer a, there exists an integer b such that $a + b = 1$.

  (**Note:** Remember that to prove a statement that applies to all integers, we start by letting a be an arbitrary integer. Once we've done that, we can find the b that does the trick for that value of a. In this particular example, if we know a and we want the b such that $a + b = 1$, then we simply solve for b: $b = 1 - a$. In the proof, we must demonstrate that, given a, this value of b does what we want.)

  Proof. Suppose a is an integer and let $b = 1 - a$.

  Then b is an integer and $a + b = a + (1 - a) = 1$.

  Thus, for each integer a, there is an integer $b = 1 - a$ such that $a + b = 1$. ■

4.3 Existence and uniqueness

In Example 4.1, we proved two statements:

- There exist integers m and n such that $10m + 13n = 3$.
- For every integer a, there exists an integer b such that $a + b = 1$.

We proved the first by giving specific values m and n such that $10m + 13n = 3$. But these values of m and n are not *unique*: there are many pairs of integers m and n such that $10m + 13n = 3$ (for example, $m = 12$ and $n = -9$, $m = -14$ and $n = 11$, $m = 25$ and $n = -19$, among others).

With the second statement, however, given an integer a, the value of b such that $a + b = 1$ is indeed unique: the value of b that we constructed in the proof is the *only* integer with this property. One technique to show that a mathematical object is the only one to have a certain property is to suppose that there are two objects with that property and then demonstrate that they must actually be the same.

We'll update the statement and its proof to reflect the uniqueness of this integer b.

Theorem 4.2. For every integer a, there exists a unique integer b such that $a + b = 1$.

Proof. (Note the proof of the existence of such a b is exactly the same as in Example 4.1.)

Suppose a is an arbitrary integer and let $b = 1 - a$.

Then b is an integer and $a + b = a + (1 - a) = 1$.

Thus, for each integer a, there is an integer $b = 1 - a$ such that $a + b = 1$.

(Now here's the new part.)

To prove that this is the only integer with this property, suppose that c is also an integer such that $a + c = 1$.

Then $c = 1 - a = b$.

Thus, there is a unique integer $b = 1 - a$ such that $a + b = 1$.

■

Here is another example of a proof of existence and uniqueness. In the following, we prove that for every integer a, there exists a unique integer b such that $10a + 2b = 4$. In order to find the b that "works," we do a little algebra before we start the proof. Given an integer a, we solve the equation $10a + 2b = 4$ for b:

$$\begin{aligned} 10a + 2b &= 4 \\ 2b &= 4 - 10a \\ b &= 2 - 5a. \end{aligned}$$

This calculation is not part of the proof, but it tells us what value of b to introduce in the proof.

Theorem 4.3. For every integer a, there is a unique integer b such that $10a + 2b = 4$.

Proof. Suppose a is an integer and let $b = 2 - 5a$.

Then b is an integer and $10a + 2b = 10a + 2(2 - 5a) = 10a + (4 - 10a) = 4$.

Thus, there exists an integer b such that $10a + 2b = 4$.

To prove b is unique, suppose that c is also an integer such that $10a + 2c = 4$.

We will show that c must equal b.

Since $10a + 2b = 4$ and $10a + 2c = 4$, we have $10a + 2b = 10a + 2c$, which implies that $2b = 2c$.

We then have $0 = 2c - 2b = 2(c - b)$.

This means that either $2 = 0$ or $c - b = 0$ and, since $2 \neq 0$, $c - b = 0$, which implies that $c = b$.

Thus, $b = 2 - 5a$ is the unique integer that satisfies the equation $10a + 2b = 4$. ■

4.4 Exercises

4.1. Prove that, for all integers m and n, $4 \mid (m^2 + n^2)$ if and only if m and n are even.

4.2. Prove that, for all integers a, b, and c, with $c \neq 0$, $a \mid b$ if and only if $ca \mid cb$.

4.3. Prove that there exist integers m and n such that $2m + 3n = 12$. Are these integers unique? (Justify your answer.)

4.4. Prove that there is no negative integer n such that $n^2 + n < 0$.

(HINT: Notice that you are proving the negation of: there exists a negative integer n such that $n^2 + n < 0$.)

4.5. Prove that, for every integer m, there is a unique integer n such that $5m - n = 8$.

Chapter 5

Sets

Perhaps the most fundamental and commonly-encountered mathematical concept is that of a ***set***. A set can be thought of as a collection of things, where the things are mathematical objects themselves, e.g., numbers, functions, other sets. The things in a set are called ***elements*** of the set. A set is defined by what is *in* it, and two sets are *the same* if they have the same elements. We can specify a set by listing or describing the things in the set.

When there are only a few things in the set, we can specify a set by explicitly listing the set's elements, inside curly braces.

For instance, $\{1, 2, 3\}$ is the set containing the numbers 1, 2, and 3 (and nothing else).

The order in which a set's elements are listed does not matter. So the set $\{1, 2, 3\}$ is exactly the same as the set $\{2, 3, 1\}$, and so on.

We can give names to sets for easier discussion and manipulation. We might let $A = \{1, 2, 3, 4, 5\}$, $B = \{2, 10, 11\}$, and $C = \{-4.5, -3.6, 2.23, 17.1\}$, for example.

A set can have *no* elements. There is just one such set, and it is called the ***empty set***. It is denoted by $\varnothing$. This is very similar to the Danish letter Ø, but was specially invented for this purpose in 1939. Occasionally, you will see people write $\{\}$ for the empty set.

To say that some element is in a set, we use the symbol $\in$. For instance, $1 \in \{1, 2, 3\}$ and $2 \in \{1, 2, 3\}$. However, 4 is not in $\{1, 2, 3\}$ and we can say this symbolically like this: $4 \notin \{1, 2, 3\}$.

If a set has many elements, it may not be practical to list all of them. Suppose, for instance, that we wanted D to be the set of all integers between 5 and 103. We could write

$$D = \{5, 6, \ldots, 103\}.$$

This is pretty good, but what if we feel uncomfortable about what happens in the "$\ldots$" part? We can be more precise by defining D using a *rule* that tells us whether or not a given thing is in D. We can write it like this:

$$D = \{x \in \mathbb{Z} : 5 \leq x \leq 103\}.$$

This should be read as, "D is the set of all integers, x, that are between 5 and 103, inclusive."

Similarly, we can say $E = \{6, 8, \ldots, 24\}$, but it would be better to say

$$E = \{x \in \mathbb{Z} : 6 \leq x \leq 24, x \text{ even }\}$$

or

$$E = \{x \in \mathbb{Z} : x = 2j \text{ where } j \in \mathbb{Z} \text{ and } 3 \leq j \leq 12\}.$$

Can you see why these two ways of defining E are equivalent (that is, they define the same set)?

5.1 Union

Given two sets, we can combine them into a new set. We say that the ***union*** of two sets A and B is the set that contains all elements that are in A or B. We write this as $A \cup B$. Here are some examples.

Example 5.1. (a) $\{1, 2, 3\} \cup \{4, 5, 6\} = \{1, 2, 3, 4, 5, 6\}$

(b) $\{1, 2, 3\} \cup \{1, 3, 7\} = \{1, 2, 3, 7\}$

(c) $\{1, 2, 3\} \cup \{3, 1, 2\} = \{1, 2, 3\}$

(d) $\{1, 2, 3\} \cup \{2, 3\} = \{1, 2, 3\}$

(e) $\{1, 2, 3\} \cup \varnothing = \{1, 2, 3\}$

(f) $\{1, 2, 3\} \cup \mathbb{Z} = \mathbb{Z}$

(g) $\mathbb{Z} \cup \mathbb{R} = \mathbb{R}$

Note that we always have $A \cup B = B \cup A$.

Notice in example (b) that 1 and 3 are in both starting sets, but we don't include them twice in the union. Once we say 1 is in the union, that's it. A good way to think of a union is this: an element is in the union of sets A and B if it is in A or it is in B. If an element is in both A and B, it still occurs only once in the union.

In example (c), the two sets are the same, so anything in the first set is in the second, and vice versa. As a result, the union is the set itself. For any set A,

$$A \cup A = A.$$

In example (d), every element of the second set is an element of the first set. We may think of the union as the result of a process wherein we start with the first set and add to it any elements from the second set that are not in the first set; the resulting set is the union. So in this example, the union ends up being the first set.

In example (e), since the empty set has no elements, the union of $\{1, 2, 3\}$ with it yields simply $\{1, 2, 3\}$.

In example (f), since 1, 2, and 3 are all integers, and so are already elements of $\mathbb{Z}$, the union is $\mathbb{Z}$.

In example (g), since all integers are real numbers, the union is $\mathbb{R}$.

5.2 Intersection

The ***intersection*** of two sets A and B is the set that contains all elements that are in *both* A and B. If A and B have no elements in common (i.e., if there is no element that is in both A and B), then the intersection is the empty set.

Note that for any sets A and B, $A \cap B = B \cap A$.

Here are some examples.

Example 5.2. (a) $\{1, 2, 3\} \cap \{2, 3, 4\} = \{2, 3\}$

(b) $\{1, 2, 3\} \cap \{1, 2, 3\} = \{1, 2, 3\}$

(c) $\{1, 2, 3\} \cap \{1, 2\} = \{1, 2\}$

(d) $\{1, 2, 3\} \cap \{4, 5, 7\} = \varnothing$

In example (a), the elements 2 and 3 are the only elements that are in both of the sets, so the intersection is $\{2, 3\}$.

In example (b), the two sets are the same, so all elements are in both sets, and the intersection is the set itself. For any set A, we can say that

$$A \cap A = A.$$

In example (c), all of the elements in the second set are in the first set, so the intersection is the second set.

If the intersection of two sets is the empty set, then we say that the sets are ***disjoint***. That is, two sets A and B are disjoint whenever

$$A \cap B = \varnothing.$$

In example (d), no elements are in both sets, so the intersection has nothing in it; it is the empty set. The sets $\{1, 2, 3\}$ and $\{4, 5, 7\}$ are disjoint.

5.3 Subsets

A very useful concept when working with sets is that of ***subsets***. If A and B are sets, and all of the elements of A are also elements of B, then we say that A is a *subset* of B. This is written $A \subseteq B$. It can be useful to think of this as saying that B "contains" A.

That is, $A \subseteq B$ if and only if, for every x in A, x is also in B.

Here are some examples.

Example 5.3. (a) $\{1, 2, 3\} \subseteq \{1, 2, 3, 4, 5\}$ (since the elements 1, 2 and 3 are all elements of $\{1, 2, 3, 4, 5\}$)

(b) $\{1, 3, 5, 7\} \subseteq \{1, 3, 5, 7\}$ (since the two sets are the same, if an element is in the first set, it is necessarily in the second set)

(c) $\varnothing \subseteq \{5, 8, 10\}$

(d) $\varnothing \subseteq \varnothing$

Note that we always have $A \cap B = B \cap A$.

Example (b) illustrates the following fact. For any set A,

$$A \subseteq A.$$

Example (c) is an odd one. Why do we say that $\varnothing$ is a subset of $\{5, 8, 10\}$? To say that a set A is a subset of a set B is to say the following: For any element a, if $a \in A$, then $a \in B$.

However, when $A = \varnothing$, the condition $a \in A$ is always false, and so the statement "if $a \in A$, then $a \in B$" is always true. As a result, $\varnothing$ is a subset of all sets, including itself (example (d)).

Another way to view this is to imagine starting with a set A. If we remove elements from it, we create new sets, and these new sets are always subsets of A. This is true even if we remove *all* the elements, leaving us with the empty set, and so the empty set is a subset of A.

Many times we encounter proofs that involve showing that a set, A, is a subset of another set, B. A general method of attack in such proofs is to begin with an element x in A, and argue that x is in B. This allows us to conclude that *every* element of A is in B, and that is equivalent to saying that A is a subset of B. Here is an example.

Theorem 5.1. Let A, B, C and D be sets. Suppose $A \subseteq B$ and $C \subseteq D$. Then $A \cup C \subseteq B \cup D$.

Proof. Let A, B, C and D be sets. Suppose $A \subseteq B$ and $C \subseteq D$.

Suppose $x \in A \cup C$.

Then $x \in A$ or $x \in C$.

Case 1: Suppose $x \in A$. Then, since $A \subseteq B$, $x \in B$. Hence, $x \in B \cup D$.

Case 2: Suppose $x \in C$. Then, since $C \subseteq D$, $x \in D$. Hence, $x \in B \cup D$.

Thus, $x \in B \cup D$.

Thus, $x \in A \cup C$ implies $x \in B \cup D$, and hence $A \cup C \subseteq B \cup D$.

■

5.4 Set equality

When we define new mathematical objects, one of the first things we need to know is what it means for two of those objects to be equal. What does it mean for two sets to be equal? Since sets are defined exactly by their elements, two sets are equal if and only if they have the same elements. That is, sets A and B are equal if for all $x \in A$, $x \in B$ and for all $x \in B$, $x \in A$.

In practice, to show two sets are equal, we may show that each is a subset of the other. That is, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

5.5 Set Difference

Given two sets A and B, we can define the ***set difference***, written $A \setminus B$, to be the set of everything in A that is not in B:

$$A \setminus B = \{x : x \in A \text{ and } x \notin B\}.$$

Here are some examples.

Example 5.4. (a) $\{1, 3, 5\} \setminus \{3\} = \{1, 5\}$ (since 3 is in both sets, we remove it from the first set to get the set difference)

(b) $\{1, 3, 5, 7\} \setminus \{3, 5, 8, 12\} = \{1, 7\}$ (3 and 5 are in both sets, so we remove them from the first set to get the set difference; since 8 and 12 are not in the first set, they have no effect on the resulting set difference)

(c) $\{1, 3, 5, 7\} \setminus \{4, 6, 10, 16\} = \{1, 3, 5, 7\}$ (since the sets have no elements in common, there is nothing to remove from the first set)

(d) $\{1, 3, 5, 7\} \setminus \{1, 3, 5, 7\} = \varnothing$ (since the sets are the same, we remove *all* elements from the first set to the get the set difference, the empty set)

Theorem 5.2. Let A be a set. Then $A \setminus A = \varnothing$.

Proof. Let A be a set.

Suppose $x \in A \setminus A$.

Then $x \in A$ and $x \notin A$. This is a contradiction.

Hence, our supposition that $x \in A \setminus A$ is false.

That is, there is nothing in $A \setminus A$.

Hence, $A \setminus A = \varnothing$. ■

Theorem 5.3. Let A, B, and C be sets. Then $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Proof. Let A, B, and C be sets. We will show that

$$A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C) \text{ and } (A \setminus B) \cap (A \setminus C) \subseteq A \setminus (B \cup C),$$

and so conclude $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Suppose $x \in A \setminus (B \cup C)$.

Then $x \in A$ and $x \notin (B \cup C)$.

Hence, $x \in A$ and $x \notin B$ and $x \notin C$.

Saying this in a verbose way, we have $x \in A$ and $x \notin B$, and $x \in A$ and $x \notin C$.

Hence, $x \in (A \setminus B)$ and $x \in (A \setminus C)$, and so $x \in (A \setminus B) \cap (A \setminus C)$.

Thus, we have shown that $A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$.

Now, suppose $x \in (A \setminus B) \cap (A \setminus C)$.

Then $x \in A \setminus B$ and $x \in A \setminus C$.

That is, $x \in A$ and $x \notin B$ and $x \in A$ and $x \notin C$.

Simply, $x \in A$ and $x \notin B$ and $x \notin C$. Hence, $x \in A \setminus (B \cup C)$.

So, $(A \setminus B) \cap (A \setminus C) \subseteq A \setminus (B \cup C)$.

Thus, $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

■

5.6 Sets of sets

So far, the set examples have contained only numbers. The elements of sets can be anything you can define. We can talk about a set of polygons, or functions, for example.

In fact, the elements of sets can be *sets themselves*.

Here's an example. Let $A = \{1, 2, 3\}$, $B = \{1, 3, 6, 10\}$, $C = \{2, 4, 11, 17, 22\}$. Then we can define the set D by writing

$$D = \{A, B, C\}.$$

Thus, $D = \{\{1, 2, 3\}, \{1, 3, 6, 10\}, \{2, 4, 11, 17, 22\}\}$.

Whereas A, B and C are sets of integers, D is a *set of sets*. Notice that $A \in D$, and though $1 \in A$, we do *not* say that $1 \in D$. The elements of D are sets, not integers.

Sets of sets are also called ***families***, to help indicate that they are sets whose elements are sets.

We can extend this process to have *sets of sets of sets*, and so forth. For instance, using the sets above, we could let $E = \{A, C\}$ and $F = \{B, C\}$, and the define the set of sets of sets

$$G = \{D, E, F\}.$$

One particular kind of family is the power set of a set.

Definition 5.1. The ***power set*** of a set A is the set of all subsets of A.

The power set of A is written $\mathcal{P}(A)$.

For example, let $A = \{2, 3\}$. The subsets of A are $\varnothing, \{2\}, \{3\}$, and $\{2, 3\}$, so the power set of A is

$$\mathcal{P}(A) = \{\varnothing, \{2\}, \{3\}, \{2, 3\}\}.$$

If A has many elements, $\mathcal{P}(A)$ has *lots* of elements. For example, if $A = \{2, 3, 5, 7\}$, then

$$\begin{aligned}\mathcal{P}(A) =&\{\varnothing, \{2\}, \{3\}, \{2, 3\}, \{5\}, \{2, 5\}, \{3, 5\}, \{2, 3, 5\},\\ &\{7\}, \{2, 7\}, \{3, 7\}, \{2, 3, 7\}, \{5, 7\}, \{2, 5, 7\}, \{3, 5, 7\}, \{2, 3, 5, 7\}\}.\end{aligned}$$

One thing to note is that the empty set is an element of every power set, since the empty set is a subset of every set. In other words, for any set A,

$$\varnothing \in \mathcal{P}(A).$$

Example 5.5. We note that $\mathcal{P}(\varnothing) = \{\varnothing\}$. This is not the empty set! The set $\{\varnothing\}$ has something in it: $\varnothing \in \{\varnothing\}$.

Here are some theorems illustrating how to work with power sets.

Theorem 5.4. Let A and B be sets. Then $\mathcal{P}(A) \subseteq \mathcal{P}(A \cup B)$.

Proof. Let A and B be sets.

Suppose $S \in \mathcal{P}(A)$.

Since $\mathcal{P}(A)$ is the set of all subsets of A, $S \subseteq A$.

Suppose $y \in S$.

Then $y \in A$, so $y \in A \cup B$.

Hence, $y \in S$ implies $y \in A \cup B$, so $S \subseteq A \cup B$.

Thus, $S \in \mathcal{P}(A \cup B)$.

Hence, $S \in \mathcal{P}(A)$ implies $S \in \mathcal{P}(A \cup B)$.

Therefore, $\mathcal{P}(A) \subseteq \mathcal{P}(A \cup B)$. ■

Theorem 5.5. Let A and B be sets. Then $A \cap B = \varnothing$ if and only if $\mathcal{P}(A) \cap \mathcal{P}(B) = \{\varnothing\}$.

Proof. Let A and B be sets.

We prove both directions using contrapositive.

($\Leftarrow$) We first prove that $A \cap B \neq \varnothing$ implies $\mathcal{P}(A) \cap \mathcal{P}(B) \neq \{\varnothing\}$.

Suppose $A \cap B \neq \varnothing$.

Then there exists $x \in A \cap B$.

Then $x \in A$ and $x \in B$.

Let $S = \{x\}$. (This is the critical idea: given an element, we can create the set containing that element.)

Then $S \subseteq A$ and $S \subseteq B$, and $S \neq \varnothing$.

That is, $S \in \mathcal{P}(A)$ and $S \in \mathcal{P}(B)$.

So, $S \in \mathcal{P}(A) \cap \mathcal{P}(B)$, and so $\mathcal{P}(A) \cap \mathcal{P}(B) \neq \{\varnothing\}$.

Thus, $A \cap B \neq \varnothing$ implies $\mathcal{P}(A) \cap \mathcal{P}(B) \neq \{\varnothing\}$.

($\Rightarrow$) We now prove that $\mathcal{P}(A) \cap \mathcal{P}(B) \neq \{\varnothing\}$ implies $A \cap B \neq \varnothing$

Suppose $\mathcal{P}(A) \cap \mathcal{P}(B) \neq \{\varnothing\}$.

Hence, $\mathcal{P}(A) \cap \mathcal{P}(B) = \varnothing$ or $\mathcal{P}(A) \cap \mathcal{P}(B)$ contains a set other than the empty set.

Since $\varnothing \in \mathcal{P}(A)$ and $\varnothing \in \mathcal{P}(B)$, $\varnothing \in \mathcal{P}(A) \cap \mathcal{P}(B)$, and so $\mathcal{P}(A) \cap \mathcal{P}(B) \neq \varnothing$.

Hence there exists a set $S \in \mathcal{P}(A) \cap \mathcal{P}(B)$ such that $S \neq \varnothing$.

Then $S \in \mathcal{P}(A)$ and $S \in \mathcal{P}(B)$, i.e., $S \subseteq A$ and $S \subseteq B$.

Since $S \neq \varnothing$, there exists $x \in S$.

Then $x \in A$ since $S \subseteq A$ and $x \in B$ since $S \subseteq B$.

Thus, $x \in A \cap B$, so $A \cap B \neq \varnothing$.

Thus, $\mathcal{P}(A) \cap \mathcal{P}(B) \neq \{\varnothing\}$ implies $A \cap B \neq \varnothing$.

Therefore, $A \cap B = \varnothing$ if and only if $\mathcal{P}(A) \cap \mathcal{P}(B) = \{\varnothing\}$. ■

5.6.1 Unions and Intersections of Families

If F is a family, we define $\bigcup F$ and $\bigcap F$ as follows:

$$\bigcup F = \{a : \text{there exists } A \in F \text{ with } a \in A\}$$

and

$$\bigcap F = \{a : \text{ for all } A \in F, a \in A\}$$

Thus, $\bigcup F$ is the set of all elements that appear in at least one set in F and $\bigcap F$ is the set of all elements that appear in *every* set in F.

Example 5.6. Let $F = \{\{1, 2, 3\}, \{2, 3, 5\}, \{3, 4, 5\}\}$. Then $\bigcup F = \{1, 2, 3, 4, 5\}$ and $\bigcap F = \{3\}$.

Example 5.7. Let $G = \{\{1, 2, \{2, 3\}\}, \{1, 2, 3, 4\}, \{1, 2\}\}$. Then $\bigcup G = \{1, 2, 3, 4, \{2, 3\}\}$ and $\bigcap G = \{1, 2\}$.

The following proof illustrates how to work with families.

Theorem 5.6. Let A and B be families. Then $\bigcup(A \cap B) \subseteq (\bigcup A) \cap (\bigcup B)$.

Proof. Let A and B be families.

Suppose $x \in \bigcup(A \cap B)$.

Then there exists $S \in A \cap B$ such that $x \in S$.

So $S \in A$ and $S \in B$.

Hence, $x \in S$ and $S \in A$, so $x \in \bigcup A$.

Also, $x \in S$ and $S \in B$, so $x \in \bigcup B$.

Thus, $x \in (\bigcup A) \cap (\bigcup B)$.

Therefore, $x \in \bigcup(A \cap B)$ implies $x \in (\bigcup A) \cap (\bigcup B)$, and so $\bigcup(A \cap B) \subseteq (\bigcup A) \cap (\bigcup B)$. ■

5.7 Exercises

5.1. Prove that, for any sets A and B:

(a) $A \cap B \subseteq A$.

(b) $A \subseteq A \cup B$.

5.2. Let $A = \{n \in \mathbb{Z} : 18 \mid n\}$, $B = \{n \in \mathbb{Z} : 3 \mid n\}$, and $C = \{n \in \mathbb{Z} : 2 \mid n\}$. Prove that $A \subseteq B \cap C$.

5.3. Let $A = \{n \in \mathbb{Z} : n = 4k + 1 \text{ for some } k \in \mathbb{Z}\}$ and $B = \{n \in \mathbb{Z} : n = 4k - 3 \text{ for some } k \in \mathbb{Z}\}$. Prove that $A = B$.

5.4. Let $A = \{n \in \mathbb{Z} : 6 \mid n\}$ and $B = \{n \in \mathbb{Z} : 3 \mid n\}$. Is $A \subseteq B$? Is $B \subseteq A$? Is $A = B$? Prove that you are correct.

5.5. Let A and B be sets. Prove the following facts.

(a) $A \cup B = (A \setminus B) \cup (A \cap B) \cup (B \setminus A)$

(b) The sets $A \setminus B$, $A \cap B$ and $B \setminus A$ are ***pairwise disjoint*** (i.e., the intersection of any pair of them is empty (so you have three things to prove here)).

5.6. Give an example of a set S which contains an element x such that $x \in S$ and $x \subseteq S$.

5.7. Prove the following theorem: Let A and B be sets. Then $A \setminus (A \cap B) = A \setminus B$.

5.8. Prove the following theorem: Let A, B and C be sets. Then $(A \setminus C) \cap (B \setminus C) = (A \cap B) \setminus C$.

5.9. Let A, B, and C be sets. Prove that $(A \cup C) \cap B \subseteq A \cup (B \cap C)$.

5.10. Let A, B, and C be sets. Suppose $A \cup C \subseteq B \cup C$. Prove that $A \setminus C \subseteq B$.

5.11. Show that for every non-empty set A, there is a set S with exactly one element such that $S \in \mathcal{P}(A)$.

5.12. Let A and B be sets. Prove that $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

5.13. Let A and B be sets. Prove that $A \subseteq B$ iff $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

5.14. Let A and B be sets. Prove each of the following.

(a) $A \subseteq B$ if and only if $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

(b) $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$

(c) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$

(d) There exist sets A and B such that $\mathcal{P}(A \cup B) \nsubseteq \mathcal{P}(A) \cup \mathcal{P}(B)$.

(e) $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$ if and only if $A \subseteq B$ or $B \subseteq A$.

5.15. Let $\mathcal{F}$ and $\mathcal{G}$ be families. Prove that $\bigcup(\mathcal{F} \cup \mathcal{G}) = (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G})$.

5.16. Prove that there exist non-empty families $\mathcal{F}$ and $\mathcal{G}$ such that $\bigcup(\mathcal{F} \cap \mathcal{G}) = (\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G})$.

5.17. Prove that there exist non-empty families $\mathcal{F}$ and $\mathcal{G}$ such that $\bigcup(\mathcal{F} \cap \mathcal{G}) \neq (\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G})$.

5.18. Suppose $\mathcal{F}$ and $\mathcal{G}$ are families. Prove that $(\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G}) \subseteq \bigcup(\mathcal{F} \setminus \mathcal{G})$.

5.19. Suppose $\mathcal{F}$ and $\mathcal{G}$ are families. Prove that if $\mathcal{F} \subseteq \mathcal{G}$, then $\bigcup \mathcal{F} \subseteq \bigcup \mathcal{G}$.

5.20. Suppose $\mathcal{F}$ and $\mathcal{G}$ are families, and $\mathcal{F} \neq \varnothing$ and $\mathcal{G} \neq \varnothing$. Prove that if $\mathcal{F} \subseteq \mathcal{G}$, then $\bigcap \mathcal{G} \subseteq \bigcap \mathcal{F}$.

Chapter 6

Proofs by Induction

6.1 The Principle of Mathematical Induction

The set of ***natural numbers*** is the set $\mathbb{N} = \{1, 2, 3, ...\}$. (Note that though some authors choose to include the number 0 in the set of natural numbers, we do not include it.) If you are tasked with proving that a statement $P(n)$ is true for every natural number n, the following theorem (presented without proof) may be of use.

Theorem 6.1. (The Principle of Mathematical Induction) The statement $P(n)$ is true for all $n \in \mathbb{N}$ if both of the following are satisfied:

- $P(1)$ is true; and
- whenever $P(k)$ is true, $P(k+1)$ is also true.

A proof that uses the Principle of Mathematical Induction is called a ***proof by induction***. Proofs by induction have a standard structure:

Base Case: Prove that the statement $P(1)$ is true.

Induction Step: Assume that $P(k)$ is true for some k. (This is the ***inductive hypothesis***.) Use the inductive hypothesis to prove that under this assumption $P(k+1)$ is also true.

Conclude that $P(n)$ is true for all $n \in \mathbb{N}$.

Note the distinction between the conclusion and the inductive hypothesis. The conclusion is that $P(n)$ is true for *every* natural number n. The inductive hypothesis is that $P(k)$ is true only for *some* natural number k.

Induction is often compared to falling dominoes. You set up the dominoes so that, if the k^{th} one falls, then the $k + 1^{st}$ will also fall (this is the inductive step) and you make the first one fall (this is the base case). If you do both of those steps, then *every* domino will fall (this is the conclusion).

6.2 Examples involving divisibility

The following examples involve positive integer powers.

For any integer m and any natural number n, we define m^n to be

$$m^n = \begin{cases} m & \text{if } n = 1 \\ m \cdot m^{n-1} & \text{if } n \geq 2. \end{cases}$$

Note that this leads to the notion of m^n with which you are already familiar:

$$\begin{aligned} m^1 &= m \\ m^2 &= m \cdot m^1 = m \cdot m \\ m^3 &= m \cdot m^2 = m \cdot m \cdot m \\ &\text{etc.} \end{aligned}$$

Theorem 6.2. For every $n \in \mathbb{N}$, $3|(7^n - 1)$.

Proof. We proceed by induction on n.

Base Case: If $n = 1$, then $7^n - 1 = 7 - 1 = 6 = 3(2)$ and thus 3 divides $7^n - 1$ when $n = 1$.

Induction Step: Suppose 3 divides $7^k - 1$ for some natural number k.

Then there exists an integer m such that $7^k - 1 = 3m$ or $7^k = 3m + 1$.

We then have:

$$\begin{aligned} 7^{k+1} - 1 &= 7 \cdot 7^k - 1 \\ &= 7(3m + 1) - 1 \text{ (by the inductive hypothesis)} \\ &= 3(7m) + 7 - 1 \\ &= 3(7m) + 6 \\ &= 3(7m + 2). \end{aligned}$$

Since $7m + 2$ is an integer, this means that 3 divides $7^{k+1} - 1$.

Thus, whenever 3 divides $7^k - 1$, 3 also divides $7^{k+1} - 1$.

Therefore, 3 divides $7^n - 1$ for every natural number n. ■

The next example is similar and involves the trick of adding zero in a clever way in order to apply the inductive hypothesis.

Theorem 6.3. For every $n \in \mathbb{N}$, $5|(8^n - 3^n)$.

Proof. We proceed by induction on n.

Base Case: If $n = 1$, then $8^n - 3^n = 8 - 3 = 5 = 5(1)$ and thus 5 divides $8^n - 3^n$ when $n = 1$.

Induction Step: Suppose 5 divides $8^k - 3^k$ for some natural number k.

Then there is an integer m such that $8^k - 3^k = 5m$.

We must now show that 5 divides $8^{k+1} - 3^{k+1}$.

(Since we've assumed that $5 \mid (8^k - 3^k)$, we do some algebraic wrangling to the expression $8^{k+1} - 3^{k+1}$ to make $8^k - 3^k$ appear.)

We have:

$$\begin{aligned} 8^{k+1} - 3^{k+1} &= 8^{k+1} - 3 \cdot 8^k + 3 \cdot 8^k - 3^{k+1} \\ &= 8 \cdot 8^k - 3 \cdot 8^k + 3 \cdot 8^k - 3 \cdot 3^k \\ &= (8-3) \cdot 8^k + 3(8^k - 3^k) \\ &= 5 \cdot 8^k + 3(8^k - 3^k) \\ &= 5 \cdot 8^k + 3(5m) \text{ (by the inductive hypothesis)} \\ &= 5(8^k + 3m) \end{aligned}$$

Since $8^k + 3m$ is an integer, this proves that 5 divides $8^{k+1} - 3^{k+1}$.

Thus, whenever 5 divides $8^k - 3^k$, 5 also divides $8^{k+1} - 3^{k+1}$.

Therefore, 5 divides $8^n - 3^n$ for every natural number n. ■

The previous proof uses the trick of adding and subtracting $3 \cdot 8^k$ to the expression $8^{k+1} - 3^{k+1}$. This, of course, does not change the value of the expression since $-3 \cdot 8^k + 3 \cdot 8^k = 0$ but it is a clever way to bring the expression $8^k - 3^k$ into view so that we can apply the inductive hypothesis. While it may take some getting used to and it may take a lot of experimentation to come up with the right thing to add and subtract, this is a technique that is quite common and is often worth trying.

6.3 Examples involving inequalities

Theorem 6.4. For all $n \in \mathbb{N}$, $2^n \geq 2n$.

Proof. We proceed by induction on n.

Base case: If $n = 1$, then $2^n = 2 = 2n$.

Thus, $2^n \geq 2n$ if $n = 1$.

Induction step: Suppose $2^k \geq 2k$ for some natural number k.

We will show that $2^{k+1} \geq 2(k+1)$.

We have:

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &\geq 2 \cdot 2k \text{ (by the inductive hypothesis)} \\ &= 4k \\ &= 2k + 2k \\ &\geq 2k + 2 \text{ (since } k \geq 1) \\ &= 2(k+1). \end{aligned}$$

Thus, whenever $2^k \geq 2k$, it is also true that $2^{k+1} \geq 2(k+1)$.

Therefore, $2^n \geq 2n$ for all $n \in \mathbb{N}$. ■

The next example involves a ***factorial***. For a natural number n, we define $n!$ (read "n-factorial") to be:

$$n! = \begin{cases} 1 & \text{if } n = 1 \\ n \cdot (n-1)! & \text{if } n \geq 2. \end{cases}$$

This leads to the same notion of $n!$ with which you are likely familiar:

$$\begin{aligned} 1! &= 1 \\ 2! &= 2 \cdot 1! = 2 \cdot 1 \\ 3! &= 3 \cdot 2! = 3 \cdot 2 \cdot 1 \\ &\text{etc.} \end{aligned}$$

Theorem 6.5. For every $n \in \mathbb{N}$, $n! \leq n^n$.

Proof. We proceed by induction on n.

Base case: If $n = 1$, then $n! = 1 = 1^1 = n^n$.

Thus $n! \leq n^n$ if $n = 1$.

Induction step: Suppose $k! \leq k^k$ for some natural number k.

We will prove that $(k+1)! \leq (k+1)^{k+1}$.

We have:

$$\begin{aligned} (k+1)! &= (k+1) \cdot k! \\ &\leq (k+1) \cdot k^k \text{ (by the inductive hypothesis)} \\ &< (k+1) \cdot (k+1)^k \text{ (by Exercise 6.2)} \\ &= (k+1)^{k+1}. \end{aligned}$$

Thus, whenever $k! \leq k^k$, it is also true that $(k+1)! \leq (k+1)^{k+1}$.

Therefore, $n! \leq n^n$ for every $n \in \mathbb{N}$. ■

6.4 Examples involving summations and products

We use the greek letters *sigma* ($\sum$) and *pi* ($\prod$) in denoting the sum and product, respectively, of a list of numbers. You may remember sigma notation from your study of calculus.

In particular, let n be a natural number and a_1, a_2, ... , a_n be a list of numbers.

- We define $\displaystyle\sum_{i=1}^{n} a_i$ by $\displaystyle\sum_{i=1}^{1} a_i = a_1$ and $\displaystyle\sum_{i=1}^{n} a_i = \left(\sum_{i=1}^{n-1} a_i\right) + a_n$ if $n \geq 2$.

This leads to the familiar:

$$\sum_{i=1}^{1} a_i = a_1$$
$$\sum_{i=1}^{2} a_i = \left(\sum_{i=1}^{1} a_i\right) + a_2 = a_1 + a_2$$
$$\sum_{i=1}^{3} a_i = \left(\sum_{i=1}^{2} a_i\right) + a_3 = a_1 + a_2 + a_3$$
$$\text{etc.}$$

For example,

- $\sum_{i=1}^{5} i = 1 + 2 + 3 + 4 + 5$
- $\sum_{i=1}^{4} (i^2 - 1) = (1^2 - 1) + (2^2 - 1) + (3^2 - 1) + (4^2 - 1) = 0 + 3 + 8 + 15$

- We define $\prod_{i=1}^{n} a_i$ by $\prod_{i=1}^{1} a_i = a_1$ and $\prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) \cdot a_n$ if $n \geq 2$.

This leads to:

$$\prod_{i=1}^{1} a_i = a_1$$
$$\prod_{i=1}^{2} a_i = \left(\prod_{i=1}^{1} a_i\right) \cdot a_2 = a_1 \cdot a_2$$
$$\prod_{i=1}^{3} a_i = \left(\prod_{i=1}^{2} a_i\right) \cdot a_3 = a_1 \cdot a_2 \cdot a_3$$
$$\text{etc.}$$

For example,

- $\prod_{i=1}^{5} i = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 5!$
- $\prod_{i=1}^{4} (3i^2) = (3 \cdot 1^2)(3 \cdot 2^2)(3 \cdot 3^2)(3 \cdot 4^2)$

Theorem 6.6. For every $n \in \mathbb{N}$, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Proof. We proceed by induction on n.

Base case: If $n = 1$, then $\sum_{i=1}^{n} i = \sum_{i=1}^{1} i = 1 = \frac{1(2)}{2} = \frac{n(n+1)}{2}$.

Induction step: Suppose $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$ for some $k \in \mathbb{N}$.

We will prove that $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

We have:

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \text{ (by the inductive hypothesis)} \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}.\end{aligned}$$

Thus, whenever $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, it is also true that $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

Therefore, for every $n \in \mathbb{N}$, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. ■

Theorem 6.7. For all $n \in \mathbb{N}$, $\prod_{i=1}^{n}(4i-2) = \frac{(2n)!}{n!}$.

Proof. We proceed by induction on n.

Base case: If $n = 1$, then $\prod_{i=1}^{n}(4i-2) = \prod_{i=1}^{1}(4i-2) = 4(1) - 2 = 2 = \frac{2!}{1!} = \frac{(2n)!}{n!}$.

Induction step: Suppose $\prod_{i=1}^{k}(4i-2) = \frac{(2k)!}{k!}$ for some natural number k.

We then have:

$$\begin{aligned}\prod_{i=1}^{k+1}(4i-2) &= \left(\prod_{i=1}^{k}(4i-2)\right) \cdot [4(k+1)-2] \\ &= \frac{(2k)!}{k!} \cdot (4k+2) \text{ (by the inductive hypothesis)} \\ &= \frac{(2k)!}{k!} \cdot 2(2k+1) \\ &= \frac{(2k)!}{k!} \cdot 2(2k+1) \cdot \frac{k+1}{k+1} \\ &= \frac{(2k+2)(2k+1)(2k)!}{(k+1)k!} \\ &= \frac{[2(k+1)]!}{(k+1)!}\end{aligned}$$

Thus, whenever $\prod_{i=1}^{k}(4i-2) = \frac{(2k)!}{k!}$, it is also true that $\prod_{i=1}^{k+1}(4i-2) = \frac{[2(k+1)]!}{(k+1)!}$.

Therefore, for every $n \in \mathbb{N}$, $\prod_{i=1}^{n}(4i-2) = \frac{(2n)!}{n!}$. ■

Note that, in the preceding proof, we multiplied an expression by the multiplicative identity 1 in the form $\frac{k+1}{k+1}$. This is similar to the "adding zero" trick we used in the proof of Theorem 6.3. Why did we choose to multiply numerator and denominator by $k+1$? One reason is that, before we apply this trick, we have an expression whose denominator is $k!$ and we know we want the denominator ultimately to be $(k+1)!$ and multiplying the denominator by $k+1$ will get us what we want in the denominator. Luckily, multiplying the numerator by $k+1$ also gives the desired result. Again, it may take time and practice to decide what kind of algebraic manipulations are useful, but you will find this technique helpful.

6.5 Some advice and Euclid's Division Theorem

A word of advice: When you do a proof by induction, state clearly where you use the inductive hypothesis. It is not uncommon for students to put a direct proof of a statement in the framework of a proof by induction —with a base case and an induction step—but never apply the inductive hypothesis during the induction step. In this case, the proof is likely a direct proof and should be presented as such.

Consider the following theorem. Since it is of the form *for all* $n \in \mathbb{N}$, $P(n)$, it may seem at first blush that a proof by induction would be in order. However, a direct proof is quick and easy. Moreover, you should, as an exercise, think about how you might prove this by induction. How would you use the inductive hypothesis to complete the inductive step?

Theorem 6.8. For every $n \in \mathbb{N}$, $n^2 - n \geq 0$.

Proof. Suppose n is a natural number.

Then $n^2 - n = n(n-1)$.

Since n is a natural number, $n \geq 1$.

This means that $n > 0$ and $n - 1 \geq 0$.

Thus, $n^2 - n = n(n-1) \geq 0$. ■

As one more example of a proof by induction, we present a theorem that dates back (at least) to Euclid. This theorem will be useful in a later chapter.

Theorem 6.9. (The Euclidean Division Theorem) For every pair of natural numbers m and n, there exist unique non-negative integers q and r with $0 \leq r < m$ such that

$$n = qm + r.$$

Proof. If $m = 1$, then, for any $n \in \mathbb{N}$, $n = n \cdot m + 0$, and $0 < m$, and we are done.

So suppose m is a natural number such that $m > 1$.

We need to show that, for every $n \in \mathbb{N}$, there exist non-negative integers q and r such that $n = qm + r$ and $0 \leq r < m$.

(Once we've established the existence of such q and r, we will show that they are unique.)

We proceed by induction on n.

Base case: Suppose $n = 1$. Then $n = 0 \cdot m + 1$.

Thus, for $q = 0$ and $r = 1$, $n = qm + r$ and $0 \leq r < m$.

Induction step: Suppose $k \in \mathbb{N}$ and there exist non-negative integers q and r such that $k = qm + r$ and $0 \leq r < m$.

Then $k + 1 = qm + (r + 1)$.

Since $r < m$ and r and m are both integers, we have $r + 1 \leq m$.

If $r + 1 < m$, we let $q' = q$ and $r' = r + 1$ and then we have $k + 1 = q'm + r'$ and $0 \leq r' < m$.

Suppose instead that $r + 1 = m$. Then $k + 1 = qm + m = (q + 1)m + 0$.

Letting $q' = q + 1$ and $r' = 0$, we now have a pair of non-negative integers q' and r' such that $k + 1 = q'm + r'$ and $0 \leq r' < m$.

Thus, if there exist non-negative integers q and r such that $k = qm + r$ and $0 \leq r < m$, then there exist non-negative integers q' and r' such that $k + 1 = q'm + r'$ and $0 \leq r' < m$.

Therefore, for every $m \in \mathbb{N}$ and for every $n \in \mathbb{N}$, there exist non-negative integers q and r such that $n = qm + r$ and $0 \leq r < m$.

To show that such q and r are unique, suppose m and n are natural numbers and that

$$n = q_1 m + r_1 = q_2 m + r_2,$$

with $0 \leq r_1 < m$ and $0 \leq r_2 < m$.

Note that we may assume that $r_2 \geq r_1$ (otherwise, we could simply re-name the variables).

Then $(q_1 - q_2)m = r_2 - r_1$, which by definition of *divides* means that $m|(r_2 - r_1)$.

Since $r_1 \leq r_2$, $0 \leq r_2 - r_1$.

Since $r_1 \geq 0$, $r_2 - r_1 \leq r_2$.

Since $r_2 < m$, we have $0 \leq r_2 - r_1 < m$.

Since $m|(r_2 - r_1)$ and $0 \leq r_2 - r_1 < m$, it must be the case that $r_2 - r_1 = 0$ by Exercise 3.6.

Thus, $r_2 = r_1$.

This means that $(q_1 - q_2)m = 0$ and, since $m \neq 0$, $q_1 = q_2$.

We have therefore shown that, for every pair of natural numbers m and n, there exist unique non-negative integers q and r with $0 \leq r < m$ such that

$$n = qm + r.$$

■

This theorem can be extended to negative m and negative n, but we will not need those results in this course.

6.6 Exercises

6.1. Prove: If a is a non-negative integer, then $a^n \geq 0$ for all $n \in \mathbb{N}$.

6.2. Prove: If a and b are non-negative integers such that $a < b$, then $a^n < b^n$ for all $n \in \mathbb{N}$.

6.3. Let n be a positive integer. Use induction to prove that $9 \mid 10^n - 1$.

6.4. Let n be a positive integer. Use induction to prove that $8 \mid 3^{2n} - 1$.

6.5. Let n be a positive integer. Use induction to prove that $6 \mid n^3 - n$.

6.6. Let n be a positive integer. Use induction to prove that

$$\sum_{k=1}^{n} k \cdot k! = (n+1)! - 1.$$

6.7. Let n be a positive integer. Use induction to prove that $\displaystyle\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

6.8. Note that the base case in a proof by induction need not be $n = 1$.

(a) Prove that for all natural numbers $n \geq 2$, $\displaystyle\prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right) = \frac{n+1}{2n}$.

(b) Prove that for all integers $n \geq 0$, $7 \mid 2^{n+2} + 3^{2n+1}$.

6.9. Use induction to prove that $2^n > n$ for all integers $n \geq 0$.

6.10. Find the smallest $k \in \mathbb{Z}$ such that $n! > n^4$ for all $n \geq k$. Prove the result using induction.

Chapter 7

Relations

7.1 Cartesian products

Let A and B be sets. We define the ***Cartesian product*** of A and B to be the set of all ***ordered pairs*** (a, b) where $a \in A$ and $b \in B$. The term *ordered pair* means that the order of the pair is significant. So, for example, $(2, 3)$ and $(3, 2)$ are different ordered pairs. (Compare this to the way we write sets, where the set $\{2, 3\}$ is the same as the set $\{3, 2\}$.)

The Cartesian product of A and B is denoted $A \times B$:

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

For example, if $A = \{1, 2, 3\}$ and $B = \{4, 5\}$, then the Cartesian product of A and B is

$$A \times B = \{(a, b) : a \in \{1, 2, 3\}, b \in \{4, 5\}\} = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)\}.$$

Notice that $A \times B$ is not generally the same set as $B \times A$, though equality is possible.

Example 7.1. $\mathbb{R} \times \mathbb{R} = \{(x, y) : x \in \mathbb{R}, y \in \mathbb{R}\}$ is often thought of as the set of points in the xy-plane. (Notice that here the ordered requirement of the elements of the Cartesian product is important: the point $(1, 5)$ is not the same as the point $(5, 1)$).

Example 7.2. Let $A = B = \mathbb{Z}$. Then $A \times B$ is the set of all points (x, y) in the xy-plane such that x and y are integers. Note that $\mathbb{Z} \times \mathbb{Z} \subseteq \mathbb{R} \times \mathbb{R}$.

Example 7.3. Suppose you have three types of nut butter: peanut, almond and pistachio. Suppose, too, that you have three types of bread: wheat, sourdough and potato. If we let

$$A = \{\text{peanut}, \text{almond}, \text{pistachio}\} \text{ and } B = \{\text{wheat}, \text{sourdough}, \text{potato}\},$$

then $A \times B$ corresponds to the set of all sandwiches you can make with one type of nut butter and one type of bread.

7.2 Relations

Let A and B be sets. A ***relation*** from A to B is a subset of $A \times B$. A relation from A to A is a relation *on* A.

A relation can be used to describe a certain connection, or relationship, between elements of A and B.

Example 7.4. Let $A = B = \{1, 2, 3, 4, 5, 6\}$. We can define a relation R from A to B like this:

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

So, R consists of all pairs of positive integers (a, b), both less than or equal to 6, where a divides b.

Thus,

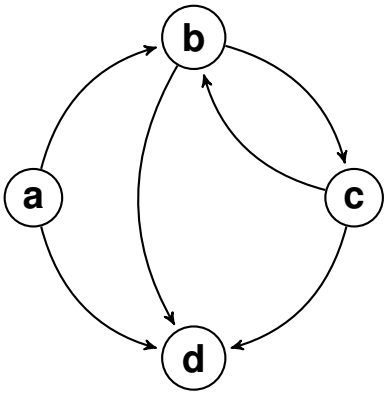
$$R = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,2), (2,4), (2,6), (3,3), (3,6), (4,4), (5,5), (6,6)\}.$$

Notice that the order of elements here is important, since $a \mid b$ does not imply $b \mid a$. For example, $(1, 4) \in R$, but $(4, 1) \notin R$.

Thus R captures a certain *relationship* between the integers in A. It defines a way that two integers in A can be related.

Example 7.5. A *directed graph* is a set of vertices, together with a set of one-way connections (called *edges*) between pairs of vertices.

The figure below shows the directed graph with vertices a, b, c, and d with edges from a to b, b to c, c to b, c to d, b to d, and a to d.



Let $V = \{a, b, c, d\}$, and $E = \{(a, b), (b, c), (c, b), (c, d), (b, d), (a, d)\}$. Then $E \subseteq V \times V$, so E is a relation on V.

Example 7.6. Let A be the set of all English words. Define a relation R on A by

$$R = \{(x, y) : x \in A, y \in A \text{ where } x \text{ and } y \text{ have the same number of letters}\}.$$

For example, (cat, rug) $\in R$ and (unsanded, aardvark) $\in R$, while (furniture, dog) $\notin R$. Notice that if $(x, y) \in R$, then $(y, x) \in R$. Also, if x is any English word, then $(x, x) \in R$.

Example 7.7. We can certainly have less "natural" relations. Let $A = \{-1, 0, 1\}$ and $B = \{2, 5, 6, 12\}$, and then define R from A to B by

$$R = \{(-1, 2), (-1, 5), (0, 2), (0, 6), (1, 5), (1, 6), (1, 12)\}.$$

This is a relation, since $R \subseteq A \times B$, but it does not have any simple, natural interpretation.

Example 7.8. Define a relation R on $\mathbb{R}$ by

$$R = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} : \left(x - \frac{1}{2}\right)^2 + \left(y - \frac{1}{2}\right)^2 > \frac{1}{25}\right\}.$$

R is the set of points outside the circle of radius $\frac{1}{5}$ centered at $\left(\frac{1}{2}, \frac{1}{2}\right)$.

Example 7.9. Let A be the set of all movie performers. Define a relation M on A by

$$(a, b) \in M \text{ if and only if } a \text{ and } b \text{ performed in the same movie.}$$

For example, Judy Garland and Billie Burke were both in 1939's *The Wizard of Oz*, so

$$(\text{ Judy Garland , Billie Burke }) \in M.$$

Whether or not we want to include pairs (a, a) in R is a contentious point: was Judy Garland in a movie with herself? This shows that our definition of M above is not complete. We can eliminate this contention by changing our definition to clear up this point. For instance, we could say

$$(a, b) \in M \text{ if and only if } a \neq b \text{ and } a \text{ and } b \text{ performed in a movie together}$$

and then M would not include pairs (a, a).

7.3 Equivalence Relations

Let A be a set and R be a relation on A. R may have various properties. There are three in particular that we are interested in.

- We say the relation R is ***reflexive*** if $(a, a) \in R$ for all $a \in A$.
- We say the relation R is ***symmetric*** if $(a, b) \in R$ implies that $(b, a) \in R$.
- We say the relation R is ***transitive*** if $(a, b) \in R$ and $(b, c) \in R$ implies that $(a, c) \in R$.

Some relations have none of these properties. Some have one or two or them. Some have all three, and those we call ***equivalence relations***.

Definition 7.1. An ***equivalence relation*** is a relation that is reflexive, symmetric and transitive.

In example 7.4,

- R is reflexive, since $(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)$ and $(6, 6)$ are all in R.
- R is not symmetric. To see this, we need only show that there is some pair (a, b) in R while (b, a) is not in R. The pair $(1, 3)$ does the job.
- R is transitive. This can be shown explicitly, by checking all possible pairs of pairs $(a, b), (b, c)$. Alternatively, we can use the fact that if $a \mid b$ and $b \mid c$, then by Theorem 3.2, $a \mid c$. Hence, if (a, b) and (b, c) are in R, then (a, c) is in R.

Thus R is not an equivalence relation.

In example, 7.5,

- V is not reflexive (since $(a, a) \notin V$).
- V is not symmetric (since $(a, b) \in V$ but $(b, a) \notin V$).

- V is not transitive (since $(a, b) \in V$ and $(b, c) \in V$, but $(a, c) \notin V$).

Thus V is not an equivalence relation.

In example 7.6, as noted R is reflexive and symmetric. Now, suppose $(a, b) \in R$ and $(b, c) \in R$. Then a and b are words with the same number of letters; say they have n letters. Then b and c have the same number of letters, so c has n letters. Hence, a and c have n letters, and so $(a, c) \in R$. Hence, R is transitive. Therefore, R is an equivalence relation.

In example 7.7, $A \neq B$, so R is not an equivalence relation.

In example 7.8,

- R is not reflexive, since $0 \in \mathbb{R}$, but $(0, 0) \notin R$.
- R is symmetric. To see this, we can note that the condition

$$\left(x - \frac{1}{2}\right)^2 + \left(y - \frac{1}{2}\right)^2 > \frac{1}{25}$$

  is identical to the condition

$$\left(y - \frac{1}{2}\right)^2 + \left(x - \frac{1}{2}\right)^2 > \frac{1}{25}.$$

  Hence, if $(x, y) \in R$, then $(y, x) \in R$.
- R is not transitive, and to show this we can note that $(\frac{1}{2}, 0) \in R$ and $(0, \frac{1}{2}) \in R$, but $(\frac{1}{2}, \frac{1}{2}) \notin R$.

So R is not an equivalence relation.

In example 7.9, using the second, more complete definition, M is not reflexive. It is symmetric, since the statement "X and Y have been in a movie together" is equivalent to the statement "Y and X have been in a movie together." M is not transitive, however. You may be able to think of lots of counterexamples yourself. For example, Kate Winslet and Gloria Stuart were both in 1997's *Titanic*, and Gloria Stuart and Claude Rains were both in 1933's *The Invisible Man*, but Claude Rains, who died in 1967, was never in a movie with Kate Winslet, who was born in 1975. In other words,

$$\text{(Kate Winslet, Gloria Stuart)} \in M, \text{ and (Gloria Stuart, Claude Rains)} \in M, \text{but}$$

$$\text{(Kate Winslet, Claude Rains)} \notin M$$

so M is not transitive, and so M is not an equivalence relation.

7.3.1 Proving things are, or are not, equivalence relations

Suppose we have a relation R and we are wondering whether or not it is an equivalence relation. To decide, we need to determine whether or not R is reflexive, symmetric and transitive.

If R fails to be reflexive, fails to be symmetric, or fails to be transitive, then we can conclude that R is *not* an equivalence relation. So to show that R is *not* an equivalence relation, we need only show one thing.

To show that R *is* an equivalence relation, we must show three things: that R is reflexive, symmetric and transitive.

For students it is good practice, though, to determine, for any given relation, all three: is it reflexive, is it symmetric, is it transitive? That is what we will do in the next example.

Example 7.10. Let $A = \mathbb{R}$. Define $R \subseteq A \times A$ by

$$(a, b) \in R \text{ if and only if } |a - b| < 0.2.$$

So (a, b) is in R if a and b are "close" to each other.

Is R reflexive? Let $a \in \mathbb{R}$.

Then $|a - a| = 0 < 0.2$, so $(a, a) \in R$

Thus, for all $a \in \mathbb{R}$, $(a, a) \in R$, and so R is reflexive.

Is R symmetric? Suppose $(a, b) \in R$.

Then $|b - a| = |a - b| < 0.2$, so $(b, a) \in R$.

Thus, for all $(a, b) \in R$, $(b, a) \in R$, and so R is symmetric.

Is R transitive? It may help to think about what this would mean in terms of "closeness." If a and b are close to each other, and b and c are close to each other, does that necessarily mean that a and c are close to each other? In fact, we can find many examples where this is not the case. For instance, $(0, 0.15) \in R$ and $(0.15, 0.3) \in R$, but $(0, 0.3) \notin R$. This example, by itself, shows that R is not transitive. We never need more than one example to show that a relation is not transitive.

Thus, R is reflexive and symmetric, but not transitive. So R is not an equivalence relation.

Example 7.11. Define a relation R on $\mathbb{Z} \times \mathbb{Z}$ by

$$((a, b), (c, d)) \in R \text{ if and only if } a + d = b + c.$$

Is R reflexive? Suppose $(a, b) \in \mathbb{Z} \times \mathbb{Z}$.

Then $a + b = b + a$, so $((a, b), (a, b)) \in R$.

Thus, R is reflexive.

Is R symmetric? Suppose $((a, b), (c, d)) \in R$.

Then $a + d = b + c$, so $c + b = d + a$, and hence $((c, d), (a, b)) \in R$.

Thus, R is symmetric.

Is R transitive? Suppose $((a, b), (c, d)) \in R$ and $((c, d), (e, f)) \in R$.

Then $a + d = b + c$ and $c + f = d + e$.

Adding, we then have $a + d + c + f = b + c + d + e$. Subtracting $d + c$ from both sides of the equation yields, $a + f = b + e$, and so $((a, b), (e, f)) \in R$.

Thus, R is transitive.

Hence, R is reflexive, symmetric and transitive, and so R is an equivalence relation.

7.4 Exercises

7.1. Prove that, for all sets A, B, and C:

$$A \times (B \cap C) = (A \times B) \cap (A \times C).$$

7.2. For each of the following relations, determine whether it is reflexive, symmetric, and transitive.

(a) Let $A = \{1, 2, 3, 4, 5\}$. Define a relation R on A by

$$R = \{(1, 1), (2, 2), (2, 3), (3, 2), (4, 4), (5, 5)\}.$$

(b) Define a relation R on $\mathbb{Z}$ by

$$(n, m) \in R \Leftrightarrow nm > 0.$$

(c) Define a relation R on $\mathbb{Z}$ by

$$(n, m) \in R \Leftrightarrow n \mid m.$$

(d) Define a relation R on $\mathbb{Z}$ by

$$(n, m) \in R \Leftrightarrow |n - m| = 1.$$

7.3. Define a relation R on $\mathbb{R}$ by

$$(x, y) \in R \Leftrightarrow x - y \in \mathbb{Q}.$$

Prove that R is an equivalence relation.

7.4. Define a relation R on $\mathbb{Z}$ by

$$R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x^2 + y^2 \text{ is even}\}.$$

Is R an equivalence relation? (Justify your answer, of course.)

7.5. There are five equivalence relations on the set $A = \{a, b, c\}$. List all of them.

7.6. Suppose that A is a set and R and S are both equivalence relations on A. Prove that $R \cap S$ is an equivalence relation on A.

7.7. Show that the union of two equivalence relations on a set A need not be an equivalence relation. (You might be able to use some of the relations you created in exercise 7.5).

7.8. Let A be a non-empty set and T be a relation on A with the property that, for every $a \in A$, there exists $b \in A$ such that $(a, b) \in T$. Prove or give a counterexample of the following statement: If T is symmetric and transitive, then T is an equivalence relation.

Chapter 8

Congruences

Definition 8.1. Let m be a positive integer. For integers a and b, we say

$$a \text{ is } \textbf{\textit{congruent}} \text{ to } b \textit{ modulo } m$$

whenever $m \mid (a - b)$ (that is, m divides the difference of the two integers a and b). When this is the case, we write

$$a \equiv b \pmod{m}.$$

A statement of this form is called a ***congruence***

Example 8.1. Since $14 - 2 = 12$, and $6 \mid 12$, we have

$$14 \equiv 2 \pmod{6}.$$

Similarly, we have $14 \equiv 2 \pmod{1}$, $14 \equiv 2 \pmod{2}$, $14 \equiv 2 \pmod{3}$, $14 \equiv 2 \pmod{4}$ and $14 \equiv 2 \pmod{12}$.

Since $5 \nmid 12$, 14 is not congruent to 2 modulo 5: $14 \not\equiv 2 \pmod{5}$. Similarly,

$$14 \not\equiv 2 \pmod{7}, 14 \not\equiv 2 \pmod{10}, \text{ etc.}$$

Note that, for any integer n and positive integer m, $n \equiv 0 \pmod{m}$ if and only if $m \mid n$.

Also, for any positive integer m and any integers a and b, if $a = b$, then $a \equiv b \pmod{m}$ (why?).

Several important features of congruences are encapsulated in the following theorem.

Theorem 8.1. Congruence modulo m is an equivalence relation.

Proof. Let m be a positive integer. We may define a relation R on $\mathbb{Z}$ by

$$(a, b) \in R \text{ if and only if } a \equiv b \pmod{m}.$$

To show that R is reflexive, let $a \in \mathbb{Z}$. Then $a - a = 0$, and so $m \mid (a - a)$. Hence, $a \equiv a \pmod{m}$, and so $(a, a) \in R$.

Thus $(a, a) \in R$ for all $a \in \mathbb{Z}$, and so R is reflexive.

To show that R is symmetric, suppose $(a, b) \in R$. Then $m \mid (a - b)$.

Hence, there exists a $k \in \mathbb{Z}$ such that $a - b = mk$, and so $b - a = m(-k)$.

Since $-k \in \mathbb{Z}$, we have $m \mid (b - a)$, and hence $b \equiv a \pmod{m}$.

Thus, $(b, a) \in R$, and so R is symmetric.

To show that R is transitive, suppose $(a, b) \in R$ and $(b, c) \in R$.

Then $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, and hence there exist integers k_1 and k_2 such that

$$a - b = mk_1 \text{ and } b - c = mk_2.$$

Adding these expressions, we find

$$a - c = m(k_1 + k_2)$$

and since $k_1 + k_2 \in \mathbb{Z}$, $a \equiv c \pmod{m}$.

Hence, $(a, c) \in R$, and thus R is transitive.

Since R is reflexive, symmetric and transitive, R is an equivalence relation.

■

Theorem 8.2. For any positive integer m, every integer is congruent to exactly one element of the set $\{0, 1, 2, \ldots, m - 1\}$ modulo m.

Proof. Let m be a positive integer. Let n be an integer.

By Theorem 6.9 (Euclid's theorem), there exist integers k and r, with $0 \leq r < m$ such that

$$n = mk + r.$$

Thus, $n - r = mk$, and $m \mid (n - r)$, i.e., $n \equiv r \pmod{m}$ and $r \in \{0, 1, 2, \ldots, m - 1\}$.

Now, suppose that there exist r_1 and r_2 such that $n \equiv r_1 \pmod{m}$, $n \equiv r_2 \pmod{m}$ and $0 \leq r_1, r_2 < m$.

Then there exist integers k_1 and k_2 such that $n - r_1 = mk_1$ and $n - r_2 = mk_2$.

So, $n = mk_1 + r_1 = mk_2 + r_2$. By Theorem 6.9, n is uniquely represented in the form $n = mk + r$, and so $r_1 = r_2$.

Thus, there is a unique integer r between 0 and $m - 1$ such that $n \equiv r \pmod{m}$.

■

Note that the r in the above proof is the remainder when n is divided by m. In many instances, we will make use of the fact that a number is congruent to this remainder modulo m.

For example, suppose $n = 107$ and $m = 11$. Dividing 11 into 107, we find a remainder of 8 since

$$107 = 9 \cdot 11 + 8.$$

Thus, $107 \equiv 8 \pmod{11}$. Since 8 is so much smaller than 107, we say that 107 *reduced* modulo 11 is 8. Likewise, 1234 reduces to 4 modulo 5 (since $1234 \equiv 4 \pmod{5}$), and 4321 reduces to 3 modulo 17 (since $4321 \equiv 3 \pmod{17}$).

As a result of Theorem 8.2, we say that the integers are *partitioned* into m ***congruence classes*** modulo m. This means that there are m pairwise-disjoint, nonempty subsets of the integers whose union is all of the integers, and two integers are in a given subset if and only if they are congruent modulo m.

Example 8.2. Let $m = 4$. Define four non-empty subsets of the integers:

$$A_0 = \{n \in \mathbb{Z} : n \equiv 0 \pmod 4\} = \{\dots, -8, -4, 0, 4, 8, 12, \dots\},$$
$$A_1 = \{n \in \mathbb{Z} : n \equiv 1 \pmod 4\} = \{\dots, -7, -3, 1, 5, 9, 13, \dots\},$$
$$A_2 = \{n \in \mathbb{Z} : n \equiv 2 \pmod 4\} = \{\dots, -6, -2, 2, 6, 10, 14, \dots\},$$
$$A_3 = \{n \in \mathbb{Z} : n \equiv 3 \pmod 4\} = \{\dots, -5, -1, 3, 7, 11, 15, \dots\}.$$

Then $\mathbb{Z} = A_0 \cup A_1 \cup A_2 \cup A_3$. Since $A_i \cap A_j = \varnothing$ whenever $i \neq j$, we say the sets A_0, A_1, A_2, and A_3 are pairwise disjoint.

The sets A_0, A_1, A_2, and A_3 are called the ***congruence classes*** modulo 4. Note that every integer is in exactly one congruence class modulo 4.

8.1 Modular Arithmetic

The concept of congruences really gets going when we realize that we can do *arithmetic* on the congruence classes.

In Exercise 8.1, you will prove that, if $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then

$$a + c \equiv b + d \pmod m \text{ and } ac \equiv bd \pmod m$$

So, in this sense, we can add and multiply congruences together.

A simple case of these facts is that, if $a \equiv b \pmod m$ and k is any integer, then

$$a + k \equiv b + k \pmod m \text{ and } ak \equiv bk \pmod m.$$

All of these facts suggest that the congruence symbol $\equiv$ can be treated, to a certain extent, the way we treat $=$.

We must be careful, however.

Let m be a positive integer. Suppose x and y are integers, and $xy \equiv 0 \pmod m$. Can we necessarily conclude that $x = 0$ or $y = 0$ (as we could if we knew $xy = 0$)?

We can do some experiments to investigate. Suppose we make a *multiplication table modulo* 6. Since every integer is congruent to one of $0, 1, 2, 3, 4$ or 5 modulo 6, we consider products of pairs of the integers $0, 1, 2, 3, 4$, and 5. When we find a product, we ***reduce*** it modulo 6; that is, we replace it, if necessary, by the value between 0 and 5 that it is congruent to modulo 6.

For example, 2 times 4 is 8, which is congruent to 2 modulo 6.

Doing all the multiplications and reductions, we have the resulting table:

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

We see that $3 \cdot 2 \equiv 3 \cdot 4 \equiv 2 \cdot 3 \equiv 4 \cdot 3 \equiv 0 \pmod 6$.

Hence, *the product of two non-zero values can be zero* when working modularly.

Another thing to note is that $5 \cdot 5 = 5^2 \equiv 1 \pmod 6$.

However, we can note as well that $5 \equiv -1 \pmod 6$, and so $5^2 \equiv (-1)^2 \equiv 1 \pmod 6$. Hence, $x^2 \equiv 1 \pmod 6$ implies that $x \equiv \pm 1 \pmod 6$, just as, when working with regular integer arithmetic, $x^2 = 1$ implies $x = \pm 1$.

This is not true for all moduli. For example, $4^2 \equiv 1 \pmod{15}$, $41^2 \equiv 1 \pmod{112}$ and $593^2 \equiv 1 \pmod{999}$.

Similarly, we might expect that

$$2a \equiv 2b \pmod m$$

would imply that $a \equiv b \pmod m$ (by "cancelling" the 2s). However, our table above shows us that $2 \cdot 1 \equiv 2 \cdot 4 \pmod 6$, while $1 \not\equiv 4 \pmod 6$, so cancelling the 2s is not valid here.

8.2 Divisibility questions involving large exponents

Modular arithmetic allows us to deal with many very large numbers in ways that would otherwise be unthinkable.

Example 8.3. Suppose we are interested in determining whether or not 11 divides $6^{123} - 7$. One could expand $6^{123} - 7$ and try dividing it by 11. This could take some time, and would involve so many steps that an error would be difficult to avoid.

Instead, we may use the fact that 11 divides $6^{123} - 7$ if and only if $6^{123} - 7 \equiv 0 \pmod{11}$, i.e.,

$$6^{123} \equiv 7 \pmod{11}.$$

So the question comes down to reducing 6^{123} modolo 11.

Starting with $6 \equiv 6 \pmod{11}$, we then have $6^2 \equiv 36 \equiv 3 \pmod{11}$.

Then

$$\begin{aligned} 6^3 &= (6^2)(6) \equiv (3)(6) \equiv 18 \equiv 7 \pmod{11} \\ 6^4 &= (6^3)(6) \equiv (7)(6) \equiv 42 \equiv 9 \pmod{11} \\ 6^5 &= (6^4)(6) \equiv (9)(6) \equiv 54 \equiv 10 \pmod{11} \end{aligned}$$

Noting that $10 \equiv -1 \pmod{11}$, we have $6^5 \equiv -1 \pmod{11}$. This is very useful, since powers of -1 are easily handled: $(-1)^a \equiv -1 \pmod{11}$ if a is odd and $(-1)^a \equiv 1 \pmod{11}$ if a is even.

Next, we write 123 as $120 + 3 = (5)(24) + 3$, so that

$$6^{123} = 6^{5 \cdot 24 + 3} = \left(6^5\right)^{24} 6^3$$

and so

$$6^{123} \equiv \left(6^5\right)^{24} 6^3 \equiv (-1)^{24} 6^3 \equiv (1) 6^3 \equiv 7 \pmod{11}.$$

Thus, 11 divides $6^{123} - 7$.

In this example, we reached a power that was congruent to -1 modulo 11. Finding a power that is congruent to 1 or -1 modulo your modulus is very helpful, as powers of 1 and -1 are easily computed.

8.3 Sums of powers of integers

Many very old problems in mathematics center around the question of which integers can be expressed as certain sums of powers of integers. One such questions is "What integers can be written as the sum of two squares (i.e., squared integers)?" Just using the modular arithmetic ideas we've seen so far, we can make some headway toward answering this question.

Theorem 8.3. Every integer that is the sum of two squares is congruent to 0, 1 or 2 modulo 4.

Proof. Let a be an integer. Then, by Theorem 8.2, $a \equiv 0, 1, 2,$ or $3 \pmod 4$. Since

$$0^2 \equiv 0 \pmod 4, 1^2 \equiv 1 \pmod 4, 2^2 \equiv 0 \pmod 4, \text{ and } 3^2 \equiv 1 \pmod 4,$$

we conclude that

$$a^2 \equiv 0 \text{ or } 1 \pmod 4.$$

Suppose b is an integer. Then $b^2 \equiv 0$ or $1 \pmod 4$, and so the sum $a^2 + b^2 \equiv 0, 1,$ or $2 \pmod 4$ as the following table shows:

+	0	1
0	0	1
1	1	2

Thus, the sum of two squares is congruent to 0, 1 or 2 modulo 4.

■

A big takeaway from this theorem is that, if an integer is congruent to 3 modulo 4, then it is *not* the sum of two squares.

For example, we can tell that 123456780000003 is not the sum of two squares.

The theorem does not completely answer our original question, unfortunately. You can check, for instance, that 22 is not the sum of two squares, even though $22 \equiv 2 \pmod 4$.

8.4 Digits

When we write out an integer, like $n = 1546$, we are expressing n as a sum involving powers of 10:

$$1546 = 1 \cdot 10^3 + 5 \cdot 10^2 + 4 \cdot 10 + 6.$$

In general, a positive integer n can be expressed as

$$n = d_k 10^k + \cdots + d_1 10 + d_0$$

for some integers $k \geq 0$ and $d_0, \ldots, d_k$ where $0 \leq d_i < 10$ for all $0 \leq i \leq k$. We say that the d_i are the *digits* of n.

We can do some analysis of an integer's digits using congruences.

For example, $1034 \equiv 4 \pmod{10}$. Similarly, $15342 \equiv 42 \pmod{100}$ and $54347257 \equiv 7257 \pmod{10000}$.

Perhaps the most famous theorem involving digits is the following.

Theorem 8.4. Let n be a postive integer and let s be the sum of the digits of n. Then $n \equiv s \pmod 9$.

Proof. Let k be a non-negative integer, and $\{a_0, \ldots, a_k\}$ be a set of integers (these will be our digits later). Then we need to prove that

$$\sum_{i=0}^{k} a_i 10^i \equiv \sum_{i=0}^{k} a_i \pmod 9.$$

We proceed by induction on k. For k a non-negative integer, let $P(k)$ be the statement

$$\text{“For any integers } a_0, \ldots, a_k, \sum_{i=0}^{k} a_i 10^i \equiv \sum_{i=0}^{k} a_i \pmod 9\text{.”}$$

Base case: Suppose $k = 0$. Suppose a_0 is an integer. Then $\sum_{i=0}^{k} a_i 10^i = a_0$, so

$$\sum_{i=0}^{k} a_i 10^i \equiv a_0 \equiv \sum_{i=0}^{k} a_i \pmod 9.$$

Hence, $P(0)$ is true.

Induction step: Suppose $P(b)$ is true for some integer $b \geq 0$.

Let $a_0, \ldots a_{b+1}$ be integers.

Then

$$\sum_{i=0}^{b+1} a_i 10^i = a_{b+1} 10^{b+1} + \sum_{i=0}^{b} a_i 10^i.$$

By Exercise 8.2, we know that $10^{b+1} \equiv 1 \pmod 9$. By our induction hypothesis, we know that

$$\sum_{i=0}^{b} a_i 10^i \equiv \sum_{i=0}^{b} a_i \pmod 9.$$

Hence,

$$a_{b+1} 10^{b+1} + \sum_{i=0}^{b} a_i 10^i \equiv a_{b+1} + \sum_{i=0}^{b} a_i \equiv \sum_{i=0}^{b+1} a_i \pmod 9$$

and so $P(b+1)$ is true.

Thus, $P(b)$ implies $P(b+1)$, and since $P(0)$, by induction $P(k)$ is true for all $k \geq 0$.

Now, let n be a positive integer with digits $d_k, \ldots, d_0$ so that

$$n = d_k 10^k + \cdots + d_1 10 + d_0 = \sum_{i=0}^{k} d_i 10^i.$$

Let $s = \sum_{i=0}^{k} d_i$, the sum of the digits of n.

Then, $n \equiv \sum_{i=0}^{k} d_i \equiv s \pmod 9$. ■

So, for example, we can tell that 764732 is not divisible by 9, since $7+6+4+7+3+2 = 29 \equiv 2 \pmod 9$, while 9999999949999995 is divisible by 9, since the sum of its digits is congruent to

$$0+4+5 = 9 \equiv 0 \pmod 9.$$

8.5 Exercises

8.1. Let $a, b \in \mathbb{Z}$. Let m be a positive integer.

Prove that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

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

and

$$ac \equiv bd \pmod{m}.$$

8.2. Use induction to prove that, for any non-negative integer n, $10^n \equiv 1 \pmod{9}$.

8.3. Prove that $20 \mid 3^{5427} - 7$.

8.4. Prove that $35 \mid 14^{7800} - 21$.

8.5. Let $n \in \mathbb{Z}$. If $4 \mid n$, then $76n \equiv n \pmod{100}$.

8.6. Which digits can appear as the right-most digit of a squared integer? What about a cubed integer? State and prove a theorem.

8.7. Find the smallest positive integer k such that 26 divides $23^{78910} - k$. Prove that you are correct.

8.8. Prove that there are infinitely many positive integers that are not the sum of two cubes (hint: look at the situation modulo 7).

Chapter 9

Functions

Definition 9.1. Let A and B be sets. A ***function*** f from A to B is a relation from A to B such that, for all $a \in A$, there is exactly one $b \in B$ such that $(a, b) \in f$.

We use the notation $f : A \to B$ to denote that f is a function from A to B.

When f is a function from A to B, we call A the ***domain*** of f and B the ***codomain*** of f.

For a function f from A to B, we define the ***range*** of f to be the set of values $b \in B$ such that there exists an $a \in A$ with $(a, b) \in f$. That is, the range of f is the set

$$\{b \in B : (a, b) \in f \text{ for some } a \in A\}.$$

Since a function is a relation, and a relation is a set of ordered pairs, a function is a set of ordered pairs.

Example 9.1. Let $A = \{1, 2, 3, 4\}$ and $B = \{\alpha, \beta\}$. Then

$$f = \{(1, \alpha), (2, \alpha), (3, \beta), (4, \alpha)\}$$

is a function from A to B.

The relation

$$g = \{(1, \alpha), (1, \beta), (2, \beta), (4, \alpha)\}$$

is not a function from A to B. There are two reasons for this. First, $3 \in A$, but there is no pair $(3, b)$ in g for any $b \in B$ (that is, $(3, \alpha) \notin g$ and $(3, \beta) \notin g$). Second, $(1, \alpha) \in g$ and $(1, \beta) \in g$, and this violates the requirement that there be exactly one $b \in B$ such that $(1, b) \in g$.

We use the notation $f(x) = y$ to denote that $(x, y) \in f$. So if $(x, y) \in f$, we have $(x, f(x)) \in f$.

Note that $f(x)$ is an *element* of B.

We may define a function by listing all the ordered pairs in it as in the example above. However, if the set A is large, or infinite, this is impossible, or at least impractical. Often, we define functions using a *rule* that tells us how the entries of each ordered pair in the function are related.

Example 9.2. Define a function $f : \mathbb{Z} \to \mathbb{Z}$ by

$$(a, b) \in f \text{ if and only if } b = 2a - 3.$$

That is, $f = \{(a, b) : a, b \in \mathbb{Z}, \text{ and } b = 2a - 3\}$.

Equivalently, we may define $f : \mathbb{Z} \to \mathbb{Z}$ by $f(a) = 2a - 3$ for all $a \in \mathbb{Z}$.

To verify that f is indeed a function, we must show that, for each $a \in \mathbb{Z}$, there is a unique pair $(a, b) \in f$. Let $a \in \mathbb{Z}$. Then $2a - 3 \in \mathbb{Z}$, so $(a, 2a - 3) \in f$. Now suppose that $(a, b_1) \in f$ and $(a, b_2) \in f$. Then $b_1 = 2a - 3$ and $b_2 = 2a - 3$, so $b_1 = b_2$. Hence, there is a unique pair $(a, b) \in f$ for every $a \in \mathbb{Z}$.

We often need to use multiple rules to define a function. This is referred to as defining a function ***piecewise*** .

Example 9.3. Define $f : \mathbb{Z} \to \mathbb{Z}$ by

$$f(x) = \begin{cases} x^2 & \text{if } x \text{ is odd,} \\ 5x - 9 & \text{if } x \text{ is even.} \end{cases}$$

So, for example, $f(0) = -9$, $f(1) = 1$, $f(2) = 1$, $f(3) = 9$ and $f(4) = 11$.

For any set A, we define the ***identity function*** *on* A to be $f = \{(a, a) : a \in A\}$, the function from A to A, with $f(a) = a$ for all $a \in A$.

Let A and B be sets, where B is non-empty. Let $b \in B$. Then define $f : A \to B$ by

$$f(a) = b \text{ for all } a \in A.$$

Thus $f = \{(a, b) : a \in A\}$. That is, the second entry in all ordered pairs in f is always b.

Such a function is called a ***constant function***. For sets A and B, there will be as many constant functions from A to B are there are elements of B.

9.1 Composition

Functions can be combined to create new functions.

Let A, B and C be sets, $f : A \to B$ and $g : B \to C$.

Then define the ***composition*** of g with f, denoted $g \circ f$, by

$$g \circ f = \{(a, c) : a \in A, c \in C, c = g(f(a))\}.$$

Since f takes elements of A and "sends" them to B, and g takes elements of B and "sends" them to C, we can put these two actions together into one function: $g \circ f$ takes elements of A and "sends" them to C via f and g.

We can see that $g \circ f \subseteq A \times C$ and hence $g \circ f$ is a relation. We now prove that $g \circ f$ is a *function* from A to C.

Theorem 9.1. Let A, B and C be sets, $f : A \to B$ and $g : B \to C$. Then $g \circ f$ is a function from A to C.

Proof. Let A, B and C be sets, $f : A \to B$ and $g : B \to C$.

Then $g \circ f = \{(a, c) : a \in A, c \in C, c = g(f(a))\}$.

Let $a \in A$.

Then $f(a) \in B$, so $g(f(a)) \in C$.

Let $c = g(f(a))$. Then $(a, c) \in g \circ f$.

Hence, for all $a \in A$ there exists a $c \in C$ such that $(a, c) \in g \circ f$.

To prove that there is *exactly one* $c \in C$ such that $(a, c) \in g \circ f$ for all $a \in A$, suppose $a \in A$ and that $(a, c_1) \in g \circ f$ and $(a, c_2) \in g \circ f$.

Then $g(f(a)) = c_1$ and $g(f(a)) = c_2$, and so $c_1 = c_2$.

Hence, for all $a \in A$ there is a unique c in C such that $(a, c) \in g \circ f$.

Therefore, $g \circ f : A \to C$.

■

Example 9.4. Let $A = \{a, b, c, d\}, B = \{r, s, t, u\}$, and $C = \{v, w, x\}$.

Define $f = \{(a, s), (b, t), (c, s), (d, u)\}$ and $g = \{(r, v), (s, w), (t, v), (u, x)\}$.

Then $f : A \to B$, $g : B \to C$ and $g \circ f = \{(a, w), (b, v), (c, w), (d, x)\}$.

Figure 9.1 shows how we can diagram these functions.

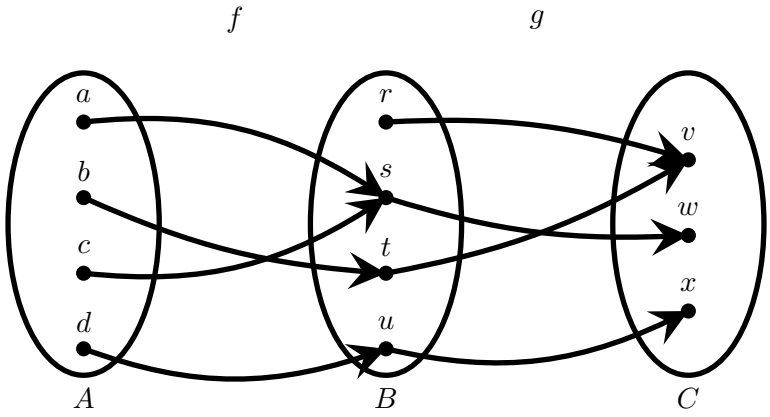


Figure 9.1: Two functions

9.2 Injections

Let A and B be sets, and suppose $f : A \to B$.

Then we say that f is ***injective*** or ***one-to-one*** if, whenever $f(a_1) = f(a_2)$, $a_1 = a_2$. That is, f is injective if $f(a_1) = f(a_2)$ implies $a_1 = a_2$.

Equivalently, f is injective if $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$.

If f is injective, then we say that f is an ***injection***.

Example 9.5. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = 5x - 7$ for all $x \in \mathbb{Z}$.

Suppose $f(a_1) = f(a_2)$ for some $a_1, a_2 \in \mathbb{Z}$.

Then $5a_1 - 7 = 5a_2 - 7$, and so $5(a_1 - a_2) = 0$. Hence, $a_1 - a_2 = 0$, so $a_1 = a_2$.

Thus, $f(a_1) = f(a_2)$ implies $a_1 = a_2$, so f is injective.

Example 9.6. Let $g : \mathbb{Z} \to \mathbb{Z}$ by defined by

$$g(x) = \begin{cases} x + 1 & \text{if } x \text{ is even,} \\ 3x - 4 & \text{if } x \text{ is odd.} \end{cases}$$

Is g an injection? To start investigating the question, we might calculate a few values of g:

$$g(0) = 1, g(1) = -1, g(2) = 3, g(3) = 5, g(4) = 5$$

So we see that $g(3) = g(4)$, and since $3 \neq 4$, g is not injective.

This is often the best way to show that a function f is not injective: find a_1 and a_2 with $a_1 \neq a_2$ but $f(a_1) = f(a_2)$.

Figure 9.2 is a diagram of an injective function. Notice how each element in the right-hand set has at most one arrow into it. Figure 9.3 is a diagram of a non-injective function. Notice how there is at least one element in the right-hand set with more than one arrow into it.

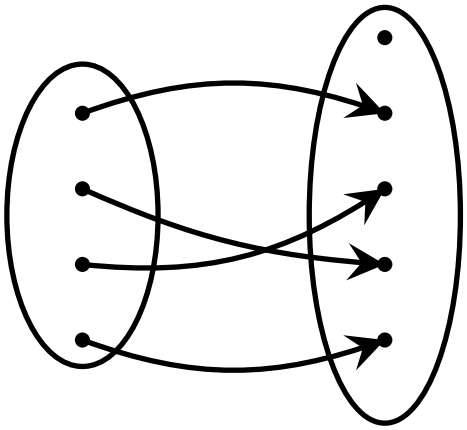


Figure 9.2: An injective function

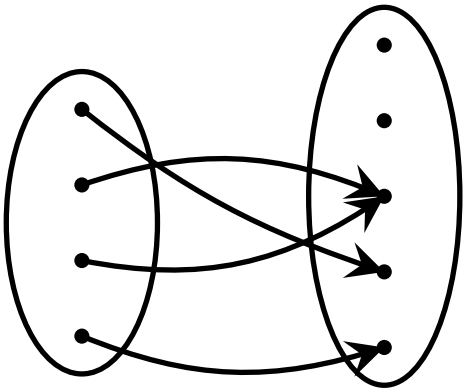


Figure 9.3: A non-injective function

Injectivity is a property that functions may "inherit" via composition. The next theorem illustrates an example of this.

Theorem 9.2. Let A, B and C be sets. Suppose $f : A \to B$ and $g : B \to C$ are injective functions. Then $g \circ f$ is an injective function from A to C.

Proof. Let A, B and C be sets. Suppose $f : A \to B$ and $g : B \to C$ are injective functions.

Let $h = g \circ f$.

Suppose there exist $a_1, a_2 \in A$ such that $h(a_1) = h(a_2)$.

Then $g(f(a_1)) = g(f(a_2))$.

Since g is injective, we conclude that $f(a_1) = f(a_2)$.

Since f is injective, we conclude that $a_1 = a_2$.

Hence, $h(a_1) = h(a_2)$ implies $a_1 = a_2$, and so h is injective. ■

9.3 Surjections

Let A and B be sets, and suppose $f : A \to B$.

Then we say that f is ***surjective*** or ***onto*** if, for all $b \in B$, there exists an $a \in A$ such that $f(a) = b$.

A surjective function is called a ***surjection***.

Example 9.7. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by

$$f(x) = \begin{cases} x + 2 & \text{if } x \text{ is even} \\ x - 6 & \text{if } x \text{ is odd.} \end{cases}$$

Let $b \in \mathbb{Z}$.

Suppose b is even. Let $a = b - 2$. Then a is even, and $f(a) = a + 2 = b - 2 + 2 = b$.

Suppose b is odd. Let $a = b + 6$. Then a is odd, and $f(b + 6) = b + 6 - 6 = b$.

Thus, for all $b \in \mathbb{Z}$, there exists an $a \in \mathbb{Z}$ such that $f(a) = b$. Hence, f is surjective.

Example 9.8. Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^2 - 4x + 7$ for all $x \in \mathbb{R}$.

Then $g(x) = (x - 2)^2 + 3$ and since $(x - 2)^2 \geq 0$ for all $x \in \mathbb{R}$, we conclude that $g(x) \geq 3$ for all $x \in \mathbb{R}$.

Thus, there is no x such that $g(x) = 1$, for example. Hence, g is not surjective.

Figure 9.4 is a diagram of a surjective function. Notice how each element in the right-hand set has at least one arrow into it. Figure 9.5 is a diagram of a non-surjective function. Notice how there is at least one element in the right-hand set with no arrow into it.

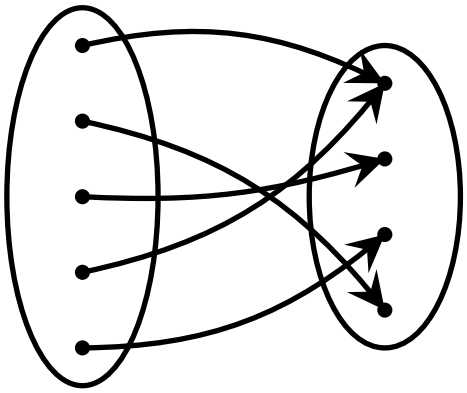


Figure 9.4: A surjective function

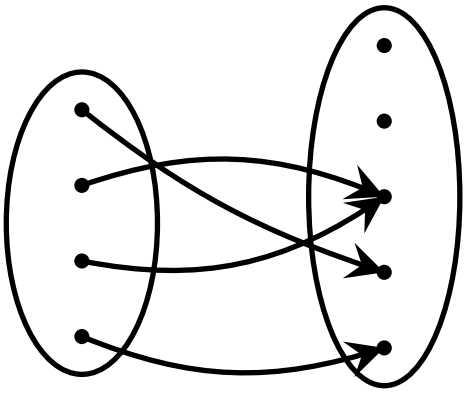


Figure 9.5: A non-surjective function

Surjectivity is another property of functions that may be inherited through composition.

Theorem 9.3. Let A, B and C be sets. Suppose $f : A \to B$ is surjective and $g : B \to C$ is surjective. Then $g \circ f$ is a surjective function from A to C.

Proof. Let A, B and C be sets. Suppose $f : A \to B$ is surjective and $g : B \to C$ is surjective.

Let $h = g \circ f$.

Suppose $c \in C$.

Then, since g is surjective, there exists a $b \in B$ such that $g(b) = c$.

Then, since f is surjective, there exists an $a \in A$ such that $f(a) = b$.

Thus, $h(a) = g(f(a)) = g(b) = c$.

Hence, for all $c \in C$ there exists an $a \in A$ such that $h(a) = c$, and so h is surjective. ■

9.4 Bijections

A ***bijection*** is a function that is injective and surjective.

Example 9.9. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by

$$f(x) = \begin{cases} x + 2 & \text{if } x \text{ is even} \\ x - 6 & \text{if } x \text{ is odd.} \end{cases}$$

In Example 9.7, we saw that f is surjective. Let's show that it is one-to-one.

First, we note that if x is even, then $f(x) = x + 2$ is even, and if x is odd, then $f(x) = x - 6$ is odd. Hence, if $f(x)$ is even, then x is even, and if $f(x)$ is odd, then x is odd.

Now, suppose $f(x_1) = f(x_2)$ for some $x_1, x_2 \in \mathbb{Z}$.

Case 1: Suppose $f(x_1)$ is even.

Then x_1 is even, and so $f(x_1) = x_1 + 2$.

Since $f(x_1) = f(x_2)$, x_2 is even, and $f(x_2) = x_2 + 2$.

Thus, $x_1 + 2 = x_2 + 2$ and so $x_1 = x_2$.

Case 2: Suppose $f(x_1)$ is odd.

Then x_1 is odd, and so $f(x_1) = x_1 - 6$.

Since $f(x_1) = f(x_2)$, x_2 is odd, and $f(x_2) = x_2 - 6$.

Thus, $x_1 - 6 = x_2 - 6$ and so $x_1 = x_2$.

Thus, the statement $f(x_1) = f(x_2)$ implies $x_1 = x_2$, and so f is injective.

So, f is injective and surjective, and hence f is a bijection.

We can diagram f as in Figure 9.6.

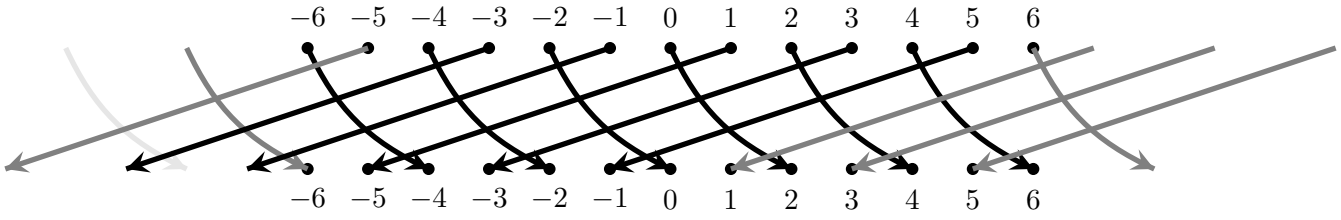


Figure 9.6: A bijection from $\mathbb{Z}$ to $\mathbb{Z}$

9.5 Inverses

Let A and B be sets and let $R \subseteq A \times B$ be a relation.

Then we define the ***inverse*** of R to be

$$R^{-1} = \{(b, a) : (a, b) \in R\}.$$

Example 9.10. Let $A = B = \{1, 2, 3, 4\}$ and $R = \{(1, 3), (1, 2), (2, 2), (3, 3), (4, 1), (4, 3)\}$.

Then $R^{-1} = \{(3, 1), (2, 1), (2, 2), (3, 3), (1, 4), (3, 4)\}$.

We can see that, if $R \subseteq A \times B$, then $R^{-1} \subseteq B \times A$.

Hence, the inverse of a relation is a relation.

Now, functions are relations. Are inverses of functions functions? The answer is: sometimes.

Theorem 9.4. Let A and B be sets. Suppose $f : A \to B$. Then f^{-1} is a function from B to A if and only if f is a bijection.

Proof. Let A and B be sets. Suppose $f : A \to B$.

($\Leftarrow$) Suppose f is a bijection.

Suppose $b \in B$. Then, since f is onto, there exists an $a \in A$ such that $f(a) = b$.

Hence, $(a, b) \in f$ and so $(b, a) \in f^{-1}$.

Now, suppose (b, a_1) and $(b, a_2) \in f^{-1}$.

Then $(a_1, b) \in f$ and $(a_2, b) \in f$, i.e. $f(a_1) = b$ and $f(a_2) = b$.

Since f is one-to-one, $a_1 = a_2$.

Thus, for all $b \in B$, there is a unique $a \in A$ such that $(b, a) \in f^{-1}$.

Hence, f^{-1} is a function from B to A.

($\Rightarrow$) Now, suppose $f^{-1} : B \to A$.

Suppose $a_1, a_2 \in A$ and $f(a_1) = f(a_2)$.

Since $(a_1, f(a_1)) \in f$, $(f(a_1), a_1) \in f^{-1}$.

Likewise, $(a_2, f(a_2)) \in f$ so $(f(a_2), a_2) \in f^{-1}$.

That is, $f^{-1}(f(a_1)) = a_1$ and $f^{-1}(f(a_2)) = a_2$.

Since $f^{-1}(f(a_1)) = f^{-1}(f(a_2))$, $a_1 = a_2$.

Thus, f is one-to-one.

Let $b \in B$. Let $a = f^{-1}(b)$. Then $(b, a) \in f^{-1}$, so $(a, b) \in f$, i.e., $f(a) = b$.

Hence, for all $b \in B$, there is an $a \in A$ such that $f(a) = b$ and thus f is onto.

Therefore, f is one-to-one and onto, and so it is a bijection.

■

So a function has an inverse function if and only if the function is a bijection.

The following theorem gives us a useful tool for working with inverses.

Theorem 9.5. Let A and B be sets. Let i_A and i_B be the identity functions on A and B, respectively. Suppose $f : A \to B$, $g : B \to A$, and $g \circ f = i_A$ and $f \circ g = i_B$. Then $g = f^{-1}$.

Proof. This proof is a nice reminder that *functions are sets of ordered pairs*.

Let A and B be sets, $f : A \to B$, $g : B \to A$, and $g \circ f = i_A$ and $f \circ g = i_B$.

Suppose $(b, a) \in g$ (i.e., $g(b) = a$).

Then $f(g(b)) = i_B(b) = b$, i.e., $f(a) = b$. So $(a, b) \in f$ and thus $(b, a) \in f^{-1}$.

Hence, $(b, a) \in g$ implies $(b, a) \in f^{-1}$.

Thus, $g \subseteq f^{-1}$.

Now, suppose $(b, a) \in f^{-1}$.

Then $(a, b) \in f$, so $f(a) = b$.

Then $g(b) = g(f(a)) = i_A(a) = a$. Hence, $(b, a) \in g$.

Hence, $(b, a) \in f^{-1}$ implies $(b, a) \in g$.

Thus, $f^{-1} \subseteq g$.

Since $g \subseteq f^{-1}$ and $f^{-1} \subseteq g$, we conclude that $g = f^{-1}$.

■

Example 9.11. Let $a, b \in \mathbb{R}$, with $a \neq 0$. Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = ax + b$ for all $x \in \mathbb{R}$.

Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = \frac{1}{a}(x - b)$ for all $x \in \mathbb{R}$.

Composing these two functions, we find, for any $x \in \mathbb{R}$,

$$(g \circ f)(x) = g(f(x)) = g(ax + b) = \frac{1}{a}(ax + b - b) = \frac{1}{a}(ax) = x$$

and

$$(f \circ g)(x) = f(g(x)) = a(g(x)) + b = a\left(\frac{1}{a}(x - b)\right) + b = x - b + b = x$$

Hence, $g \circ f = i_{\mathbb{R}}$ and $f \circ g = i_{\mathbb{R}}$. Hence, by Theorem 9.5, $g = f^{-1}$.

By Theorem 9.4, we conclude also that f is a bijection.

9.6 Exercises

9.1. Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{a, b, c, d\}$. For each of the following relations from A to B, answer these questions: Is it a function from A to B? If it is a function, is it one-to-one? If it is a function, is it onto?

(a) $\{(1, c), (2, c), (3, c), (4, c), (5, d)\}$

(b) $\{(1, a), (2, d), (3, a), (4, c)\}$

(c) $\{(1, d), (2, a), (2, d), (3, a), (4, b), (4, d), (4, c)\}$

(d) $\{(1, c), (2, b), (3, a), (4, d), (5, a)\}$

9.2. Suppose $f : A \to C$ and $g : B \to C$. Prove that if $A \cap B = \varnothing$, then $f \cup g : (A \cup B) \to C$.

9.3. Suppose R is a relation on a set A. Is it possible that R is both a function and an equivalence relation? Complete and prove the statement "R is a function and an equivalence relation iff ...".

9.4. Let S and T be sets and $f : S \to T$. Define a relation R on S by

$$(a, b) \in R \Leftrightarrow f(a) = f(b).$$

Prove that R is an equivalence relation.

9.5. Prove that the identity function is a bijection. That is, let A be a set and define $F : A \to A$ by $f(x) = x$. Prove that f is a bijection.

9.6. Let $\mathbb{Q}_{pos} = \{q \in \mathbb{Q} : q > 0\}$ and $\mathbb{Q}_{neg} = \{q \in \mathbb{Q} : q < 0\}$. Prove that the function $h : \mathbb{Q}_{pos} \to \mathbb{Q}_{neg}$ defined by $h(x) = -x$ is a bijection.

9.7. Let A and B be sets, and suppose $f : A \to B$ is a bijection. Prove that f^{-1} is a bijection from B to A.

9.8. Let A, B and C be sets. Let $f : A \to B$ and $g : B \to C$.

(a) Prove that if f and g are onto, then $g \circ f$ is onto.

(b) Prove that if $g \circ f$ is onto, then g is onto.

(c) If $g \circ f$ is onto, is f necessarily onto? Prove your answer.

(d) If $g \circ f$ is one-to-one, is f necessarily one-to-one? Prove your answer.

9.9. Let A and B be sets, and $f : A \to B$. Suppose f is one-to-one. Then f^{-1} is a *relation* from B to A Prove that there exists a subset $C \subseteq B$ such that f^{-1} is a *function* from C to A.

NOTE: The next few problems involve the set $\mathbb{R}$ of real numbers. The elementary properties of the integers that we have been working with since the beginning of the quarter all hold if every instance of the word *integer* is replaced with the words *real number*. In addition, every non-zero real number has a **multiplicative identity**: for all real $r \neq 0$, there exists a real number r^{-1} such that $r \cdot r^{-1} = r^{-1} \cdot r = 1$. You may apply these elementary properties of the real numbers whenever you need them for the remainder of this course.

9.10. Define a function $f : \mathbb{R} \to \mathbb{R}$ by

$$f(x) = \begin{cases} 2x & \text{if } x \in \mathbb{Q} \\ -3x & \text{if } x \notin \mathbb{Q} \end{cases}$$

Is f one-to-one? Is f onto? Is f^{-1} a function? State and prove a theorem.

9.11. Define a function $f : \mathbb{R} \setminus \left\{-\frac{4}{3}\right\} \to \mathbb{R} \setminus \{0\}$ by $f(x) = \dfrac{1}{3x+4}$ and a function $g : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \left\{-\frac{4}{3}\right\}$ by $g(x) = \dfrac{1-4x}{3x}$. Prove that $g = f^{-1}$.

(HINT: Show that $g \circ f$ and $f \circ g$ are the appropriate identity functions.

9.12. Let a, b, c and d be real numbers. Suppose $cd \neq 0$ and $ad - bc \neq 0$.

Define $f : \mathbb{R} \setminus \{-\frac{d}{c}\} \to \mathbb{R} \setminus \{\frac{a}{c}\}$ by

$$f(x) = \frac{ax+b}{cx+d}.$$

(a) Show that f is one-to-one and onto.

(b) Give a formula for $f^{-1}(x)$. Prove that you are correct.

9.13. Let c be a real number. Define a function $f : \mathbb{R} \to \mathbb{R}$ by

$$f(x) = \begin{cases} x^2 - 4x + c & \text{if } x \geq 2 \\ -\frac{1}{2}x^2 + 2x - 1 & \text{if } x < 2 \end{cases}$$

Find a value of c for which f a bijection. Prove that you are correct.

9.14. Define a function $f : \mathbb{R} \to \mathcal{P}(\mathbb{R})$ by

$$f(x) = \{z \in \mathbb{R} : |z| > x\}.$$

Is f one-to-one? Is f onto? Prove that you are correct.

Chapter 10

Cardinality

10.1 Equinumerosity

You may have noticed that throughout our work with sets, we have never made use the number of elements of a set. We begin discussing this concept in this chapter.

First, we must address the question of what it means for two sets to have "the same number of elements."

Definition 10.1. We will say that two sets are ***equinumerous*** whenever there exists a bijection between the two sets.

If sets A and B are equinumerous, we will write $A \sim B$.

Example 10.1. Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{a, b, c, d, e\}$.

We can define a function $f : A \to B$ by

$$f = \{(1, a), (2, b), (3, c), (4, d), (5, e)\}.$$

By direct checking, we can tell that f is one-to-one and onto, so it is a bijection. Hence, A and B are equinumerous. (This probably does not surprise you, since you can see that the sets each have five elements).

Now, consider $C = \{a, b, c, d\}$.

If we try to create a bijection from A to C, we will run out of unused elements in C to pair up with elements in A: any function from A to C must fail to be one-to-one. On the other hand, if we try to create a bijection from C to A, we will run out of elements in C before we have paired up all the elements of A: any function from C to A must fail to be surjective. Thus, A and C are not equinumerous.

Example 10.2. Let E be the set of even integers. Let $f : \mathbb{Z} \to E$ be defined by $f(x) = 2x$ for all $x \in \mathbb{Z}$.

Let's show that f is a bijection and hence that $\mathbb{Z}$ and E are equinumerous.

Suppose $f(x_1) = f(x_2)$ for some $x_1, x_2 \in \mathbb{Z}$. Then $2x_1 = 2x_2$, so $2(x_1 - x_2) = 0$. Since $x_1 - x_2 \in \mathbb{Z}$, we conclude that $x_1 - x_2 = 0$, and hence $x_1 = x_2$. Thus, f is one-to-one.

Let $y \in E$. Then $y = 2k$ for some integer k. Then $f(k) = y$. Hence, f is onto.

Thus, f is a bijection, and so $\mathbb{Z}$ and E are equinumerous.

This should seem at least mildly disturbing, since $E \subseteq \mathbb{Z}$ and there are infinitely many integers in $\mathbb{Z}$ that are not in E.

If we think of E and $\mathbb{Z}$ not as sets of integers, but as sets of objects with certain labels, the existence of the bijection between them shows that we can go through the objects in the set $\mathbb{Z}$ and relabel each one (with twice the old label) and we will have transformed $\mathbb{Z}$ into E without adding or removing any elements. This is why we say that the two sets are equinumerous.

You can see from these examples that finite sets and infinite sets present different characteristics. Before going further, we need to define these terms.

Definition 10.2. Let S be a set. Then S is ***finite*** if $S = \varnothing$ or there exists a bijection f from S to the set $\{1, 2, 3, \ldots, n\} = \{x \in \mathbb{Z} : 1 \leq x \leq n\}$ for some positive integer n.

So, a non-empty set S is finite if it is equinumerous with $\{1, 2, 3, \ldots, n\}$ for some positive integer n. In this case, we say that S has ***cardinality*** n, and we write $|S| = n$.

If a set S is not finite, then we say that S is ***infinite*** .

Theorem 10.1. Let n be a positive integer. Then all subsets of $\{1, \ldots, n\}$ are finite.

Proof. We use induction on n.

For any positive integer c, let I_c denote the set $\{1, \ldots, c\}$.

Let $P(n)$ be the statement "all subsets of $\{1, \ldots, n\}$" are finite.

Let $n = 1$. The subsets of $\{1\}$ are $\{1\}$ and $\varnothing$ which are finite by our definition of finite set. So $P(1)$ is true.

Now, suppose $P(n)$ is true for some integer $k \geq 1$. So $P(k)$ is true.

Consider the set $I_{k+1} = \{1, \ldots, k, k+1\}$. Let S be a subset of I_{k+1}. We wish to show that S is finite.

There are two cases to consider.

Suppose $k + 1 \notin S$. Then every element of S is an element of I_k, and so S is subset of I_k. Since $P(k)$ is true, we conclude that S is finite.

Suppose that $k+1 \in S$. Then we may write $S = T \cup \{k+1\}$, where $T \subseteq I_k$. Since $P(k)$ is true, T is finite, and so $T \sim \{1, \ldots, m\}$ for some positive integer m. Hence, there is a bijection f from T to $\{1, \ldots, m\}$. We can then create a function g from S to I_{m+1} by

$$g(x) = \begin{cases} f(x) & \text{if } x \in T, \\ m+1 & \text{if } x = k+1. \end{cases}$$

We wish to show that g is a bijection.

Let $y \in I_{m+1}$. If $y = m + 1$, then we have $k + 1 \in S$ and $g(k + 1) = m + 1 = y$. If $y \neq m + 1$, then $y \in I_m$ and so there is an $x \in T$ (and hence $x \in S$) such that $g(x) = y$. Hence, g is onto.

Suppose $g(x_1) = g(x_2)$ for some $x_1, x_2 \in S$. Suppose $g(x_1) = g(x_2) = m + 1$. Then $x_1 = x_2 = k + 1$.

Suppose $g(x_1) \neq m + 1$. Then $g(x_1) = f(x_1) = g(x_2) = f(x_2)$, and since f is a bijecion, $x_1 = x_2$.

Thus g is one-to-one, and so g is a bijection from S to I_{m+1}. Hence, S is finite.

Therefore, every subset of I_{k+1} is finite, so $P(k+1)$ is true.

Thus, by induction and the fact that $P(1)$ is true, $P(n)$ is true for all integers $n \geq 1$; that is, for all integers $n \geq 1$, all subsets of $\{1, \ldots, n\}$ are finite.

■

In discussing and thinking about equinumerosity, the following theorem is very helpful.

Theorem 10.2. Equinumerosity is an equivalence relation. That is, if $\mathcal{F}$ is a family, then the relation $R \subseteq \mathcal{F} \times \mathcal{F}$ defined by

$$(a, b) \in R \text{ if and only if } A \sim B$$

is an equivalence relation.

Proof. Let $\mathcal{F}$ be a family.

Let $A \in \mathcal{F}$. Define $f : A \to A$ by $f(x) = x$ for all $x \in A$. Then f is a bijection by Exercise 9.5, and so $A \sim A$. Hence, equinumerosity is reflexive.

Suppose $A, B \in \mathcal{F}$ and $A \sim B$. Then there exists a bijection $f : A \to B$. Hence, $f^{-1} : B \to A$, and f^{-1} is a bijection (by Exercise 9.7), and so $B \sim A$. Hence, equinumerosity is symmetric.

Suppose $A, B,$ and $C \in \mathcal{F}$, and $A \sim B$ and $B \sim C$. Then there exist bijections $f : A \to B$ and $g : B \to C$. By Theorem 9.2 and Theorem 9.3, $g \circ f$ is a bijection from A to C and so $A \sim C$. Thus, equinumerosity is transitive.

Since equinumerosity is reflexive, symmetric and transitive, equinumerosity is an equivalance relation.

■

One way this theorem is helpful is that it tells us that if $A \sim B$ and $A \sim C$, then $B \sim C$. Thus we need not always find a bijection between two sets to show that they are equinumerous: instead, we can find bijections between each of the sets and a common third set. This is often easier.

10.2 Countable sets

Definition 10.3. A set is ***countable*** if it is finite or equinumerous to the set of natural numbers, $\mathbb{N}$. A set that is infinite and countable is said to be ***countably infinite***.

Not all infinite sets are countable, as we shall see.

Example 10.3. We will show that $\mathbb{Z}$ is countable. To do this, we need to show that $\mathbb{Z}$ and $\mathbb{N}$ are equinumerous. To do that, we need to show that there is a bijection from one set to the other. Note that, thanks to Theorem 10.2, finding a bijecion in either direction will do the trick (equinumerosity is symmetric). Let us see how we can create a bijection from $\mathbb{Z}_{>0}$ to $\mathbb{Z}$.

We have to figure out what to pair each of $1, 2, 3, \ldots$ with. We cannot just pair them to themselves: this would give a one-to-one function, but it would not be onto (we would miss zero and all negative integers). What will work is to send 1 to 0, and then send the next integers to, alternately, positive and negative integers, making sure not to skip any along the way. So our bijection would pair 1 with 0, 2 with 1, 3 with -1, 4 with 2, 5 with -2, and so forth. To define the bijection with a rule, let $f : \mathbb{N} \to \mathbb{Z}$ be

given by

$$f(x) = \begin{cases} -\frac{x-1}{2} & \text{if } x \text{ is odd,} \\ \frac{x}{2} & \text{if } x \text{ is even.} \end{cases}$$

Next, define $g : \mathbb{Z} \to \mathbb{N}$ by

$$g(x) = \begin{cases} 2x & \text{if } x > 0, \\ 1 - 2x & \text{if } x \leq 0. \end{cases}$$

Suppose $x \in \mathbb{Z}$, $x > 0$. Then $f(g(x)) = f(2x) = \frac{2x}{2} = x$. Suppose $x \in \mathbb{Z}$, $x \leq 0$. Then

$$f(g(x)) = f(1 - 2x) = -\frac{(1 - 2x) - 1}{2} = x.$$

Hence, $f \circ g$ is the identity map on $\mathbb{Z}$.

Suppose $x \in \mathbb{N}$.

If x is odd, then $g(f(x)) = g(-\frac{x-1}{2}) = 1 - 2\left(-\frac{x-1}{2}\right) = x$.

If x is even, then $g(f(x)) = g\left(\frac{x}{2}\right) = 2\left(\frac{x}{2}\right) = x$.

Hence, $g \circ f$ is the identity function on $\mathbb{N}$.

Thus, by Theorem 9.5, $g = f^{-1}$, and hence by Theorem 9.4, f is a bijection. Therefore, $\mathbb{Z}$ and $\mathbb{N}$ are equinumerous.

Thus, if we want to show an infinite set is countable, we can find a bijection between the set and $\mathbb{Z}$ or $\mathbb{N}$, since equinumerosity is transitive.

There is nothing special about the positive integers: we will prove that *any* infinite subset of $\mathbb{Z}$ is equinumerous to $\mathbb{Z}$.

We begin with a lemma.

Lemma 10.3. Let $A \subseteq \mathbb{N}$. Then A is countable.

Proof. Let $A \subseteq \mathbb{N}$.

If A is finite, then A is countable.

Suppose A is not finite.

Since A is a subset of the positive integers, by the well-ordering principle it has a smallest element, a_1. Then $A \setminus \{a_1\}$ is a subset of the positive integers, so *it* has a smallest element, a_2. Continuing in this way, we have

$$A = \{a_1, a_2, \dots\}.$$

Define $f : A \to \mathbb{N}$ by $f(a) = i$ where $a = a_i$.

Since the a_i are distinct, f is one-to-one.

Since A is infinite, for all $k \in \mathbb{N}$ there exists an $a_k \in A$ and $f(a_k) = k$. Hence, f is onto.

So f is a bijection, and so $A \sim \mathbb{N}$. Hence, A is countable. ■

We now use this lemma to prove a more general theorem.

Theorem 10.4. Subsets of countable sets are countable.

Proof. Let A be a countable set and B be a subset of A.

If B is finite, then B is countable.

Suppose B is infinite.

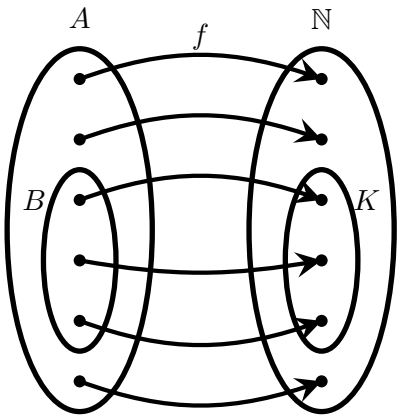
Since A is countable, there exists a bijection $f : A \to \mathbb{N}$.

Let $K = \{n \in \mathbb{N} : \text{ there exists } b \in B \text{ such that } f(b) = n\}$.

(We say that K is the *range of f restricted to B*.)

Let $g : B \to K$ be defined by $g(b) = f(b)$ for $b \in B$.

Then g is one-to-one (since f is one-to-one) and g is onto (because of the way we defined K).



Since $K \subseteq \mathbb{N}$, K is countable, by Lemma 10.3.

Since $B \sim K$, B is countable. ■

Thus, in particular, all subsets of $\mathbb{Z}$ are countable.

10.3 Cardinality of unions of sets

When we have two sets, and we know their cardinalities, there is often much we can say about the cardinality of their union.

The following believable theorem is proved in Exercise 10.2.

Theorem 10.5. The union of two finite sets is finite.

The union of two countable infinite sets is countable. We prove this in a few steps.

Theorem 10.6. Let A be a finite set and B be a countable infinite set. Suppose $A \cap B = \varnothing$. Then $A \cup B$ is a countable infinite set.

Proof. Let A be a finite set and B be a countable infinite set.

If $A = \varnothing$, then $A \cup B = B$ and so $A \cup B$ is a countable infinite set.

Suppose $A \neq \varnothing$.

Let $n = |A|$. Then $n \geq 1$ and there exists a bijection $f : A \to \{1, 2, 3, \ldots, n\}$.

Since B is a countable set, there exists a bijection $g : B \to \mathbb{N}$.

Define $h : A \cup B \to \mathbb{N}$ by

$$h(x) = \begin{cases} f(x) & \text{if } x \in A, \\ g(x) + n & \text{if } x \in B. \end{cases}$$

We will show that h is a bijection. Note that if $x \in A$, then $h(x) \leq n$, and if $x \in B$, then $h(x) > n$.

Let $m \in \mathbb{N}$.

Suppose $m \leq n$. Then $m \in \{1, 2, 3, \ldots, n\}$ and so there is an element $a \in A$ such that $f(a) = m$. Hence, $h(a) = m$.

Suppose $m > n$. Then $m - n \geq 1$, so $m - n \in \mathbb{N}$, and so there is an element $b \in B$ such that $g(b) = m - n$. Then $h(b) = m - n + n = m$.

Thus, h is surjective.

Suppose $h(x_1) = h(x_2)$ for some $x_1, x_2 \in A \cup B$.

Suppose $h(x_1) \leq n$. Then $h(x_2) \leq n$ and so $x_1 \in A$ and $x_2 \in A$. Hence,

$$f(x_1) = h(x_1) = h(x_2) = f(x_2).$$

Since f is a bijection, $x_1 = x_2$.

Suppose $h(x_1) > n$. Then $h(x_2) > n$ and so $x_1 \in B$ and $x_2 \in B$.

Hence, $g(x_1) + n = h(x_1) = h(x_2) = g(x_2) + n$ and hence $g(x_1) = g(x_2)$.

Since g is a bijection, $x_1 = x_2$.

Thus h is a bijection from $A \cup B$ to $\mathbb{N}$ and so $A \cup B$ is a countable infinite set. ■

Theorem 10.7. The union of two disjoint infinite countable sets is countable.

Proof. Let A and B be infinite countable sets, with $A \cap B = \varnothing$.

Then $A \sim \mathbb{N}$ and $B \sim \mathbb{N}$ so there exist bijections $f : A \to \mathbb{N}$ and $g : B \to \mathbb{N}$.

Define $h : A \cup B \to \mathbb{N}$ by

$$h(x) = \begin{cases} 2f(x) - 1 & \text{if } x \in A, \\ 2g(x) & \text{if } x \in B. \end{cases}$$

Note that h pairs up elements of A with odd positive integers, and elements of B with even positive integers.

Let $m \in \mathbb{N}$.

Suppose m is even. Then $m = 2k$ for some $k \in \mathbb{N}$. Since g is onto, there exists a $z \in B$ with $g(z) = k$ and $h(z) = 2g(z) = 2k = m$.

Suppose m is odd. Then $m = 2k - 1$ for some $k \in \mathbb{N}$. Since f is onto, there exists a $z \in A$ with $f(z) = k$ and $h(z) = 2f(z) - 1 = 2k - 1 = m$.

Hence, for all $m \in \mathbb{N}$, there exists $z \in A \cup B$ with $h(z) = m$ and so h is onto.

Suppose $x_1, x_2 \in A \cup B$ and $h(x_1) = h(x_2)$.

Suppose $h(x_1)$ is odd. Then $h(x_2)$ is odd, and hence

$$h(x_1) = 2f(x_1) - 1 = 2f(x_2) - 1 = h(x_2)$$

so that $2(f(x_1) - f(x_2)) = 0$, and hence $f(x_1) = f(x_2)$. Since f is a bijection, we conclude that $x_1 = x_2$.

Suppose $h(x_1)$ is even. Then $h(x_2)$ is even, and so

$$h(x_1) = 2g(x_1) = 2g(x_2) = h(x_2)$$

so $2(g(x_1) - g(x_2)) = 0$ and hence $g(x_1) = g(x_2)$. Since g is a bijection, we conclude that $x_1 = x_2$.

Thus, h is one-to-one, and so h is a bijection, and so $A \cup B$ is countable. ■

Theorem 10.8. The union of two countably infinite sets is a countably infinite set.

Proof. Let A and B be two countably infinite sets.

Then, by Exercise 5.5, $A \cup B = (A \setminus B) \cup (A \cap B) \cup (B \setminus A)$ and

$$(A \setminus B) \cap (A \cap B) = (A \cap B) \cap (B \setminus A) = (A \setminus B) \cap (B \setminus A) = \varnothing.$$

Since $A \setminus B \subseteq A$, $A \setminus B$ is finite or countably infinite.

Since $A \cap B \subseteq A$, $A \cap B$ is finite or countably infinite.

Since $B \setminus A \subseteq B$, $B \setminus A$ is finite or countably infinite.

Not all of $A \setminus B, A \cap B$ and $B \setminus A$ are finite, since, if they were, then $A \cup B$ would be finite. Hence, at least one of $A \setminus B, A \cap B$ and $B \setminus A$ is countably infinite.

Hence, by our previous theorems, $(A \setminus B) \cup (A \cap B)$ is finite or countably infinite.

If it is finite, then $B \setminus A$ is countably infinite, and hence $A \cup B = (A \setminus B) \cup (A \cap B) \cup (B \setminus A)$ is countably infinite.

If $(A \setminus B) \cup (A \cap B)$ is countably infinite, then $A \cup B = ((A \setminus B) \cup (A \cap B)) \cup (B \setminus A)$ is countably infinite.

Thus, $A \cup B$ is countably infinite. ■

10.4 Countability of $\mathbb{Q}$

In some senses, the set of rational numbers seems "bigger" than the set of integers: the integers form a proper subset of $\mathbb{Q}$. Also, thinking in terms of real numbers, we know that there are infinitely many rational numbers between 0 and 1, and between 1 and 2, etc.

However, we will in fact prove that $\mathbb{Q}$ is equinumerous to $\mathbb{Z}$. That is, we will prove that $\mathbb{Q}$ is countable. We will take a few steps to prove this.

Theorem 10.9. $\mathbb{N} \times \mathbb{N}$ is equinumerous to $\mathbb{N}$.

Proof. The set $\mathbb{N} \times \mathbb{N}$ can be depicted as an infinite table, or grid, like this:

	1	2	3	4	$\cdots$
1					
2					
3					
4					
$\vdots$					

Each box represents an element of $\mathbb{N} \times \mathbb{N}$. If we can fill these boxes in uniquely with all of the elements of $\mathbb{N}$, then we will have a bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$. It can be done by moving along *diagonals*, like this:

	1	2	3	4	⋯
1	1	3	6	10	
2	2	5	9		
3	4	8			
4	7				
⋮					

Continuing in this way, you can see that we will eventually fill in the entire table, and each box will have a unique element of the positive integers, and every element of the positive integers will appear somewhere in the table. This, then, shows that a bijection exists between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$.

For instance, the table shows that we can pair $(1, 1)$ with 1, $(1, 2)$ with 3, $(2, 1)$ with 2, etc.

Explicitly, define $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $f(i, j) = j + \frac{1}{2}(i + j - 2)(i + j - 1)$. You can check that $f(1, 1) = 1$, $f(1, 2) = 3$ and $f(2, 1) = 2$. As an exercise, you can show that f is a bijection.

Since there exists a bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$, we conclude that $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$ are equinumerous. ■

Theorem 10.10. The set of positive rational numbers, $\mathbb{Q}_{>0}$, is countable.

Proof. For each $x \in \mathbb{Q}_{>0}$, there exist unique $a, b \in \mathbb{N}$ with no common divisor besides ± 1 such that $x = \frac{a}{b}$.

Define $g : \mathbb{Q}_{>0} \to \mathbb{N} \times \mathbb{N}$ by $g(x) = (a, b)$ where $x = \frac{a}{b}$, $a, b \in \mathbb{Z}_{>0}$ and a and b have no common divisor other than ± 1.

Note that g is not onto: $g(x) \neq (3, 6)$ for any $x \in \mathbb{Q}_{>0}$, since $\frac{3}{6} = \frac{1}{2}$, and $g(\frac{1}{2}) = (1, 2)$.

Let C be the range of g.

Suppose $g(x_1) = g(x_2)$ for some $x_1, x_2 \in \mathbb{Q}_{>0}$. Say $g(x_1) = (a_1, b_1)$ and $g(x_2) = (a_2, b_2)$. Then $a_1 = a_2$ and $b_1 = b_2$, and so

$$x_1 = \frac{a_1}{b_1} = \frac{a_2}{b_2} = x_2.$$

Hence, g is one-to-one. Since C is the range of g, $g : \mathbb{Q}_{>0} \to C$ is surjective. Thus, $g : \mathbb{Q}_{>0} \to C$ is a bijection.

Since $C \subseteq \mathbb{N} \times \mathbb{N}$, and $\mathbb{N} \times \mathbb{N}$ is countable, C is countable.

Since g is a bijection, $\mathbb{Q}_{>0} \sim C$, and so $\mathbb{Q}_{>0}$ is countable. ■

Theorem 10.11. $\mathbb{Q}$ is countable.

Proof. By Theorem 10.10, $\mathbb{Q}_{>0}$ is countable.

The function $h : \mathbb{Q}_{>0} \to \mathbb{Q}_{<0}$ given by $h(x) = -x$ is a bijection (by Exercise 9.6). Hence, $\mathbb{Q}_{<0}$ is countable.

Then, by Theorem 10.8, $\mathbb{Q}_{<0} \cup \mathbb{Q}_{>0}$ is countable, and hence $\mathbb{Q} = \mathbb{Q}_{<0} \cup \{0\} \cup \mathbb{Q}_{>0}$ is countable. ■

10.5 Uncountability of $\mathbb{R}$

It is a very significant fact that the set of real numbers is *not* countable. That is, there is no bijection between $\mathbb{Z}$ and $\mathbb{R}$. This was first proved by Georg Cantor, who published his proof in 1891.

We will use the following theorem to prove that the set of real numbers is uncountable.

Theorem 10.12. The real interval $(0,1)$ and the set $\mathbb{R}$ are equinumerous.

Proof. We need a bijection from $(0,1)$ to $\mathbb{R}$. Any function on $(0,1)$ that is strictly increasing, and approaches $-\infty$ and ∞ as x approaches 0 and 1, could be shown to work.

Define $f : (0,1) \to \mathbb{R}$ by

$$f(x) = \begin{cases} \frac{1}{x} - 2 & \text{if } 0 < x \leq \frac{1}{2}, \\ 2 - \frac{1}{1-x} & \text{if } \frac{1}{2} < x < 1. \end{cases}$$

This function is strictly decreasing on $(0,1)$, and approaches ∞ as x approaches 0 and $-\infty$ as x approaches 1.

Define a function g on $\mathbb{R}$ by

$$g(x) = \begin{cases} \frac{1}{x+2} & \text{if } x \geq 0, \\ 1 + \frac{1}{x-2} & \text{if } x < 0. \end{cases}$$

Suppose $x \geq 0$. Then $g(x) = \frac{1}{x+2}$, and

$$0 < \frac{1}{x+2} \leq \frac{1}{2}.$$

Suppose $x < 0$. Then $g(x) = 1 + \frac{1}{x-2}$, and

$$\frac{1}{2} < 1 + \frac{1}{x-2} < 1.$$

Thus, $g : \mathbb{R} \to (0,1)$.

Let $z \in (0,1)$. Suppose $z \leq \frac{1}{2}$. Then $f(z) = \frac{1}{z} - 2 > 0$, so

$$g(f(z)) = g\left(\frac{1}{z} - 2\right) = \frac{1}{\frac{1}{z} - 2 + 2} = z.$$

Suppose $z > \frac{1}{2}$. Then $f(z) = 2 - \frac{1}{1-z} < 0$, so

$$g(f(z)) = g\left(2 - \frac{1}{1-z}\right) = 1 + \frac{1}{2 - \frac{1}{1-z} - 2} = z.$$

Thus $g \circ f = i_{(0,1)}$.

Now, let $z \in \mathbb{R}$. Suppose $z \geq 0$. Then

$$0 < g(z) = \frac{1}{z+2} \leq \frac{1}{2}$$

and

$$f(g(z)) = f\left(\frac{1}{z+2}\right) = \frac{1}{\frac{1}{z+2}} - 2 = z.$$

Suppose $z < 0$. Then

$$\frac{1}{2} < g(z) = 1 + \frac{1}{z-2} < 1$$

and

$$f(g(z)) = 2 - \frac{1}{1 - (1 + \frac{1}{z-2})} = z.$$

Thus, $f \circ g = i_{\mathbb{R}}$.

Hence, by Theorem 9.5 and Theorem 9.4, f is a bijection.

Therefore, the interval $(0, 1)$ and the set of real numbers are equinumerous.

■

There is nothing special about the interval $(0, 1)$ here. You can prove that *every* non-empty interval of real numbers is equinumerous to $\mathbb{R}$ by finding the appropriate bijection.

We now prove that $\mathbb{R}$ is uncountable. This proof is essentially Cantor's, and uses his **diagonal argument**.

Theorem 10.13. The set of real numbers is uncountable.

Proof. We will show that the real interval $(0, 1)$ is uncountable.

Let $f : \mathbb{N} \to (0, 1)$. We will show that f cannot be a bijection.

Each $x \in (0, 1)$ has a decimal expansion that starts with a zero followed by a decimal point and then an infinite sequence of digits.

For example, $\frac{1}{2} = 0.5000000\ldots$.

For each $n \in \mathbb{N}$, let $a_{n,j}$ be the jth digit to the right of the decimal point in the decimal expansion of $f(n)$. We can make a table of the values of this function like this:

n	$f(n)$
1	$0.\, a_{1,1}\, a_{1,2}\, a_{1,3}\, a_{1,4}\, \ldots$
2	$0.\, a_{2,1}\, a_{2,2}\, a_{2,3}\, a_{2,4}\, \ldots$
3	$0.\, a_{3,1}\, a_{3,2}\, a_{3,3}\, a_{3,4}\, \ldots$
4	$0.\, a_{4,1}\, a_{4,2}\, a_{4,3}\, a_{4,4}\, \ldots$
5	$0.\, a_{5,1}\, a_{5,2}\, a_{5,3}\, a_{5,4}\, \ldots$
$\vdots$	$\vdots$

Now, consider the diagonal of this right-hand column, made up of the digits $a_{1,1}, a_{2,2}, a_{3,3}$, etc.

We will create a real number $\widehat{x}$ between 0 and 1. For all $i \in \mathbb{N}$, define d_i by

$$\widehat{d_i} = \begin{cases} 1 & \text{if } a_{i,i} \neq 1, \\ 2 & \text{if } a_{i,i} = 1. \end{cases}$$

Now, let $\widehat{x} = 0.d_1 d_2 d_3 \ldots$, so that the i-th digit of $\widehat{x}$ is d_i.

Thus, $\widehat{x}$ is a real number between 0 and 1, with digits 1 and 2, with the property that, for every $i \in \mathbb{N}$, **the i-th digit of $\widehat{x}$ is different from the i-th digit of $f(i)$**. Hence, $\widehat{x} \neq f(i)$ for all $i \in \mathbb{N}$. That is, there is no $i \in \mathbb{N}$ such that $f(i) = \widehat{x}$, and thus f is not surjective. [1]

So, f is not a bijection, and thus there exists no bijection between $\mathbb{N}$ and the interval $(0, 1)$.

Therefore, the interval $(0, 1)$ and $\mathbb{N}$ are not equinumerous.

Hence, $\mathbb{R}$ and $\mathbb{N}$ are not equinumerous.

In other words, $\mathbb{R}$ is uncountable.

[1] It is possible for a real number to have two distinct decimal expansions (e.g., $0.5 = 0.4999\ldots$). However, for two decimal expansions to represent the same real number, one must end in repeating nines, and the other in repeating zeros. Since $\widehat{x}$ does not end in repeating nines or zeros, we know that $\widehat{x}$ is not equal to any number in the table.

■

This proof might leave you with the impression that the set of reals is *just barely* not countable: that there is just this one $\widehat{x}$, and if it were not for that number, $\mathbb{R}$ would be countable. However, we can create infinitely many other "bad" real numbers by modifying the construction. For instance, we could make numbers with digits 3 and 4, or 3, 4 and 7, etc. Or, we could use a different diagonal, or not use a diagonal at all, but some other scheme to select a digit from $f(i)$.

Here's a theorem that makes the situation clearer.

Corollary 10.14. $\mathbb{R} \setminus \mathbb{N}$ is uncountable.

Proof. Since $\mathbb{R} = (\mathbb{R} \setminus \mathbb{N}) \cup \mathbb{N}$, if $\mathbb{R} \setminus \mathbb{N}$ were countable, then $\mathbb{R}$ would be the union of two countable sets, and hence countable by Theorem 10.6. Since we just proved that $\mathbb{R}$ is not countable, we may conclude that $\mathbb{R} \setminus \mathbb{N}$ is uncountable. ■

10.6 Exercises

10.1. Prove that if A is a finite set, and B is a subset of A, then B is finite.

10.2. Prove the following theorems.

(a) Let A and B be finite sets. If $A \cap B = \varnothing$, then $|A \cup B| = |A| + |B|$.

(b) For any finite sets A and B, $|A \setminus B| + |A \cap B| = |A|$.

(c) For any finite sets A and B, $|A \cup B| = |A| + |B| - |A \cap B|$. Thus, the union of two finite sets is finite.

10.3. Let A be a finite set. Prove that if $f : A \to A$ is injective, then f is bijective.

10.4. Suppose A is an infinite set and B is a finite subset of A. Prove that $A \setminus B$ is infinite.

10.5. Prove that, if $A \sim B$, then $\mathcal{P}(A) \sim \mathcal{P}(B)$.

10.6. Let n be a positive integer. Using the fact that the union of two countable sets is countable, use induction to prove that the union of n countable sets is countable.

Index