Notes for Math 327: Discrete Mathematics

written by: Randall Paul

January 8, 2014

Contents

1 Fundamentals **5**

1.1 Introduction . . . 5
1.1.1 Notation . . . 6
1.1.2 Terms and Examples . . . 6
1.1.3 Problems . . . 8
1.2 Statements . . . 9
1.2.1 Simple Statements . . . 9
1.2.2 Compound Statements: And/Or . . . 11
1.2.3 Negation . . . 12
1.2.4 Compound Statements: Implications . . . 15
1.2.5 Problems . . . 20
1.3 Sets . . . 21
1.3.1 Basic Definitions . . . 21
1.3.2 Common Sets . . . 25
1.3.3 Operations on Sets . . . 27
1.3.4 Set Proofs . . . 30
1.3.5 Problems . . . 32
1.4 Binary Relations . . . 34
1.4.1 Example Relations . . . 34
1.4.2 Properties of Relations . . . 37
1.4.3 Problems . . . 44
1.5 Equivalence Relations . . . 46
1.5.1 Examples of Equivalence Relations . . . 47
1.5.2 Equivalence Classes . . . 49
1.5.3 Problems . . . 51
1.6 Partial Orders . . . 53
1.6.1 Examples of Partial Orders . . . 54
1.6.2 Hasse Diagrams . . . 56
1.6.3 Problems . . . 57
1.7 Functions . . . 58
1.7.1 Bijections . . . 62
1.7.2 Cardinality . . . 66
1.7.3 Problems . . . 70

2 Number Theory **71**
2.1 Divisibility . . . 71
2.1.1 Division Algorithm . . . 71
2.1.2 Factors and GCD . . . 73
2.1.3 Irrationality of $\sqrt{2}$ . . . 76
2.1.4 Problems . . . 78
2.2 Primes . . . 79
2.2.1 Some Theorems on Primes . . . 79
2.2.2 Sieve of Eratosthenes and the Prime Number Theorem . . . 80
2.2.3 Some Interesting Types of Primes . . . 82
2.2.4 Problems . . . 83
2.3 Euclid . . . 84
2.3.1 Calculating the GCD . . . 84
2.3.2 Euclid's Theorem . . . 84
2.3.3 Using Euclid's Theorem in proofs . . . 88
2.3.4 Problems . . . 89
2.4 Congruence . . . 90
2.4.1 Calculation mod N . . . 91
2.4.2 Theorems involving congruence . . . 92
2.4.3 Linear Congruence Equations . . . 93
2.4.4 Problems . . . 96

3 Sequences and Series **97**
3.1 Sequences . . . 97
3.1.1 Series . . . 99
3.1.2 Recursion . . . 102
3.1.3 Arithmetic and Geometric Examples . . . 104
3.1.4 Problems . . . 107
3.2 Induction . . . 108
3.2.1 Induction on Recursive Sequences . . . 108
3.2.2 Induction on Divisibility . . . 110
3.2.3 Induction for Series . . . 111
3.2.4 Problems . . . 116
3.3 Characteristics . . . 117

Chapter 1

Fundamentals

1.1 Introduction

I have three goals for this course.

1. To understand and apply mathematical definitions and statements.
2. To learn to make and prove mathematical statements.
3. To appreciate the beauty and power of mathematics.

I'm pretty sure most of you will be able to handle the first goal. The second is a lot harder. The third, well, some will and some won't and regardless it won't be on any exams.

The underlying idea of this course is that mathematics is a **language**. It's not the sort of language where you greet your friends or ask where the bathroom is, but it is a language nevertheless. Up to this point you've no doubt taken a number of mathematics courses, but probably your mathematics is at best a sort of 'pidgin' language. Our first goal is essentially to learn the grammar of mathematics. Our second goal is to learn to make an argument in mathematics; "math composition", if you will. Our third goal is to appreciate some of the ideas that can only be expressed in this language. It's the sort of thing you'd see in an English Lit class only it's math.

The key distinction between mathematics and other languages is that mathematics is extremely precise. Human languages like English are riven with ambiguity. Consider the statement: "I am going to the store."

It seems clear enough, but really it relies on a tremendous amount of unspoken context. For instance, are you in the process of going right this instant? Or are you about to go, but haven't started yet? Or are you saying you will go to the store sometime relatively soon? We can also wonder which store you're going to and whether that's all you're going to do or just one of several errands. That's fine in real life since if you need more precision you just ask for it. Mathematics strives not to do that. As much as is humanly possible a mathematical statement is true or false without reference to any sort of context or implied understanding. Even in mathematics we sometimes fall short of this ideal, but that is the ideal.

Now, mathematics can and will in this course be stated in English. You just have to be very careful. For instance we'll see that the statement "Professor Paul is the Queen of

England" is a perfectly acceptable mathematical statement. It has none of the vagueness of "I am going to the store." As long as "Professor Paul" and "the Queen of England" have been defined this statement is perfectly clear. It also happens to be false—which is also fine. It is much easier to determine if a statement is true or false if it is clearly and precisely stated.

1.1.1 Notation

Like many human languages, mathematics is a written language. Though all of our statements can be made in English we often use symbolic notation in place of the words to make the statements more compact and, in theory, clearer. In practice this is a great source of confusion and frustration. In response to the comments of former students, I'm going to list all of the symbols that I'll use in each section at the beginning of that section . You won't yet understand many of them, but if you get stuck later on you will have a resource for looking up the meaning of any obscure symbol you come across.

1.1.2 Terms and Examples

A *postulate* is a mathematical statement that we assume is true without proof. The ancient mathematician Euclid generated several books of geometry (called *The Elements*) based on just five postulates.

1. There is a line segment between any two points
2. Any line segment may be arbitrarily extended.
3. There is a circle for every center and radius.
4. All right angles are equal to one another.
5. If two lines are crossed by a third line in such a way that the interior angles are less than two right angles, then the two lines will cross if extended sufficiently.

This last was called the "parallel postulate" and was, in its day, controversial. Ancient mathematicians thought that you ought to be able to prove it true based on the other four (seemingly more basic) postulates. This turned out not to be the case. In fact if you omit the "parallel postulate" one can talk about so-called "non-Euclidian geometries".

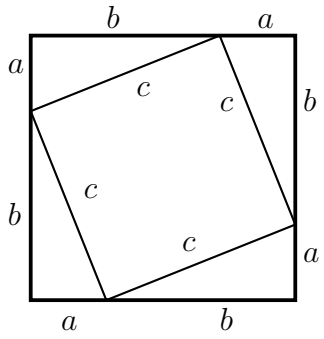
Mathematicians like to have as few postulates as possible. Students often become frustrated and annoyed when I make them prove "self-evidently true" statements like "an even integer plus an odd integer yields an odd integer". Yes, it's true... but really how do you **know** it's true? Could it be that there is some enormous odd integer that, when added to some other enormous even integer, yields another even integer? Why not?

In this class you may assume as postulates all the properties of real numbers and algebra rules you learned in high school. You may also assume basic results from high school geometry, as well as any result proven earlier in this text.

A *theorem* is a statement that is proven true based on your postulates and earlier theorems. We will prove many theorems in this class, so we might as well make the first one a good one.

> **Theorem 1.1.1:** (Pythagorean) If a right triangle has sides of length a and b and a hypotenuse of length c, then
>
> $$a^2 + b^2 = c^2$$

proof: Consider the square with sides of length $a + b$. Divide each side into segments of length a and b and connect the dividing lines with line segments as shown below.



The area of the square is $(a + b)^2$. The area of the square is also the sum of the areas of the inside square (c^2) and the four triangles ($\frac{1}{2}ab$ each).

Setting these two areas equal:

$$\begin{aligned} (a+b)^2 &= c^2 + 4\left(\tfrac{1}{2}ab\right) \\ a^2 + 2ab + b^2 &= c^2 + 2ab \qquad \text{algebra} \\ a^2 + b^2 &= c^2 \qquad \text{algebra} \end{aligned}$$

□ (This symbol marks the end of a proof.)

A *conjecture* is a statement which seems true, but has not been definitively proven or disproven. Conjectures are often questions at the edge of mathematical research and can be very technical to state. Some famous old conjectures, though, are easy to state and yet have remained unresolved (mathematicians say "open") for centuries. Here are two.

> **Conjecture 1.1.2:** (Goldbach's) Every even integer greater than two may be written as the sum of two prime numbers

It's easy to believe this conjecture. Think of any even integer greater than 2, say 28. Can 28 be written as the sum of two prime numbers? Sure, $28 = 17 + 11$. In fact you can usually do it many different ways. For instance $28 = 5 + 23$ as well. Yet no one has been able to prove you can do it for *every* even integer.

Conjecture 1.1.3: (Twin Primes) There are infinitely many pairs of primes whose difference is two.

We'll see later in this course that there are an infinite number of prime numbers. In fact this was proven by Euclid more than 2000 years ago. It is also easy to find lots of examples of primes whose difference is two. For instance 5 and 7... or 11 and 13. "Twin primes" of this type have been found that are very large, so there are certainly a very large number of them. On the other hand it is known that prime numbers become progressively less dense as you consider larger and larger numbers... so it is possible that, at some point, prime numbers are always separated by more than 2. The question remains open.

Famous old conjectures are sometimes resolved, though. Perhaps the most famous conjecture of all was "proven" (we believe falsely proven) by the French amateur mathematician (and circuit judge) Pierre de Fermat in 1637.

Conjecture 1.1.4: (Fermat's Last Theorem) There are no positive integer solutions x, y, z to the equation

$$x^n + y^n = z^n, \quad \text{for } n > 2$$

There are, of course, many solutions for $n = 1$, $(1^1 + 2^1 = 3^1)$ or $n = 2$, $(3^2 + 4^2 = 5^2$ or $7^2 + 24^2 = 25^2)$. It seems reasonable that you could find integers x, y, z so that, say, $x^3 + y^3 = z^3$. But Fermat said no. Famously he said he had a very clever proof of this, but "the proof does not fit into the margin of this text." (He wrote his proofs in a mathematics textbook that he carried with him as a traveling judge.) For over 350 years no one could produce a proof of this "theorem" that was really just a conjecture. It was finally proven by Andrew Wiles in 1995—357 years after Fermat.

1.1.3 Problems

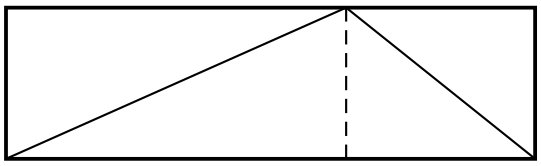
Problem 1.1.5: Show that Goldbach's conjecture is true for 42 in two different ways.

Problem 1.1.6: Do there exist positive integers x, y so that

$$x^5 + y^5 = 10,000,000,000$$

How do you know? (Remember you may cite a theorem from earlier...)

Problem 1.1.7: Prove that the area of a triangle is one half the base times the height using only the picture below and the fact that the area of a rectangle is the length times the width.



1.2 Statements

Notation

$\square$	end of proof
$\forall$	for all
$\exists$	there exists
$\ni$	such that
$\wedge$	and
$\vee$	or
$\neg$	negation
$\Leftrightarrow$	logically equivalent (if and only if)
$\Rightarrow$	(left hand side) logically implies (right hand side)

1.2.1 Simple Statements

A *mathematical statement* is simply a sentence (with a subject and a verb) which is either true or false.

Example 1.2.1: Which of the following are mathematical statements?

1. "The big dog eats."
2. "For every $x > 0$."
3. "Which integers are divisible by three?"
4. "There exists a set with no elements."
5. "Simplify."
6. "$(-3)^2 = -9$"

1. "The big dog eats." *Statement.*
2. "For every $x > 0$." *Not a statement.* In fact, not a sentence... just a phrase. It asserts nothing that may be true or false.
3. "Which integers are divisible by three?" *Not a statement,* a question. It asserts nothing that may be true or false.
4. "There exists a set with no elements." *Statement.*
5. "Simplify." *Not a statement,* a command. It asserts nothing that may be true or false.
6. "$(-3)^2 = -9$" *Statement.* It happens to be false, but it is still a sentence that asserts something.

Many statements in mathematics involve asserting that there is some number or some set or some... *thing* that satisfies some condition. This is so common, in fact, that we have a special symbol "$\exists$" that translates as "there is" or "there exists". For instance, the sentence

"For every even integer n there is an integer m such that $n = 2m$"

may be written

"For every even integer n $\exists$ an integer m such that $n = 2m$"

A similarly common sort of statement in mathematics is the assertion that something is true for every number or set or... *thing* that satisfies some condition. There is a special symbol $\forall$ that translates as "for all" or "for every" or even sometimes "every" or "all". The sentence

"All mammals are warm-blooded."

may be written

"$\forall$ mammals are warm-blooded."

These two modifiers very often occur together. Our example sentence for $\exists$ could be modified further to read:

"$\forall$ even integers n $\exists$ an integer m such that $n = 2m$"

It's worth noting here that the order of the modifiers is very important. The statement above is true. For every integer n (say $n = 14$ for example) there is an integer m ($m = 7$ in this example) so that $n = 2m$. What happens if we reverse the order? We have the statement:

"There exists an integer m such that for every integer n, $n = 2m$"

This is clearly false. There is no *single integer*, m, that is half of every possible integer n. For example, $m = 7$ works for $n = 14$, but not for $n = 16$ or $n = 18$.

While we're discussing it there is also a symbol "$\ni$" for the phrase "such that". Thus we can further modify our first example to read:

"$\forall$ even integers, n, $\exists$ an integer m, $\ni$ $n = 2m$"

I should also say that it's easy to get carried away with these symbols. Remember that you should always be able to translate the statement back into an English statement that makes sense.

Example 1.2.2: Translate the statements into English.

1. "$\exists$ two hump camels."
2. "$\forall$ insect has six legs."
3. "$\forall$ things $\exists$ a season and a purpose under heaven."
4. "$\exists$ a number x, $\ni$ $\forall$ numbers y, $xy = y$."
5. "$\forall$ number $x \neq 0$, $\exists$ a number y, $\ni$ $xy = 1$."

1. "There exist two hump camels."

2. "Every insect has six legs." or "All insects have six legs."

3. "To everything there is a season and a purpose under heaven."
   (For you fans of *The Birds* out there.)

4. "There is a number x, so that for every number y, $xy = y$."
   Of course that number is $x = 1$.

5. "For every number x not equal to zero, there is a number y so that $xy = 1$."
   Of course $y = 1/x$. Note that here the number that exists depends on the number x. This is because the order was $\forall \ldots \exists \ldots$. In the previous example a single x $(= 1)$ worked for every number y. This is because the order was $\exists \ldots \forall \ldots$.

1.2.2 Compound Statements: And/Or

There are various ways to build more complicated statements out simple statements. The logical *and* operator is one such way. It has the symbol "$\wedge$".

Definition 1.2.3: Given statements p and q, the compound statement $p \wedge q$ ("p and q") is true only when both p and q are true.

Example 1.2.4: Determine if the statements are true.

1. "Pandas are mammals and fish are vertebrates."

2. "$1 \neq 2$" $\wedge$ "$x^2 - 1 = (x-1)(x+1)$."

3. "$0 = 1$" $\wedge$ "whales are mammals."

4. "$1/0 = 0$" $\wedge$ "$x^2 + 4 = (x-2)(x+2)$."

1. "Pandas are mammals and fish are vertebrates." *True.* Pandas are mammals. Fish are vertebrates.

2. "$1 \neq 2$" $\wedge$ "$x^2 - 1 = (x-1)(x+1)$." *True.* 1 is not equal to 2. $x^2 - 1 = (x-1)(x+1)$.

3. "$0 = 1$" $\wedge$ "whales are mammals." *False.* Whales are mammals, but 0 is **not** equal to 1.

4. "$1/0 = 0$" $\wedge$ "$x^2 + 4 = (x-2)(x+2)$." *False.* Neither statement is true.

Logical *or* "$\vee$" is similar.

Definition 1.2.5: Given statements p and q, the compound statement $p \vee q$ ("p or q") is true when either p is true or q is true.

Example 1.2.6: Determine if the statements are true.

1. "Pandas are mammals or fish are vertebrates."
2. "$1 \neq 2$" $\vee$ "$x^2 - 1 = (x-1)(x+1)$."
3. "$0 = 1$" $\vee$ "whales are mammals."
4. "$1/0 = 0$" $\vee$ "$x^2 + 4 = (x-2)(x+2)$."

1. "Pandas are mammals or fish are vertebrates." *True.* Both statements are true.
2. "$1 \neq 2$" $\vee$ "$x^2 - 1 = (x-1)(x+1)$." *True.* Both statements are true.
3. "$0 = 1$" $\vee$ "whales are mammals." *True.* Whales are mammals. For logical *or* only one of the statements has to be true.
4. "$1/0 = 0$" $\vee$ "$x^2 + 4 = (x-2)(x+2)$." *False.* Both statements are false.

These properties can be compactly expressed in a "truth table" that lists all the possible true/false values for the statements p and q with the resulting true/false values for logical *and* and *or*.

p	q	$p \wedge q$	$p \vee q$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

1.2.3 Negation

Definition 1.2.7: The *negation* of a statement p "$\neg p$" is the statement that is true exactly when p is false, and false exactly when p is true.

Expressed as a truth table,

p	$\neg p$
T	F
F	T

Definition 1.2.8: We say two statements are *logically equivalent* "$\Leftrightarrow$" if they have the same truth table.

Example 1.2.9: Rewrite the following statements as logically equivalent statements without the negation.

1. ¬"$x = 0$"
2. ¬"n is an even integer"
3. ¬"$a < 1$"
4. ¬"Gina had no children"

1. ¬"$x = 0$" $\Leftrightarrow$ "$x \neq 0$"

   The statements may be true or false depending on what value x actually has. The point of logical equivalence is that they will both be true or they will both be false regardless of the actual value of x. If for example, $x = 5$, then both statements will be true.

2. ¬"n is an even integer" $\Leftrightarrow$ "n is an odd integer."

   Again if $n = 5$ then both statements are true. If $n = 8$ then both statements are false. There is no choice of n that will yield a *true* on one side and a *false* on the other.

3. ¬"$a < 1$" $\Leftrightarrow$ "$a \geq 1$"

4. ¬"Gina has no children" $\Leftrightarrow$ "Gina has children."

Negating a compound statement can be done relatively easily using the following theorem:

Theorem 1.2.10: De Morgan's Laws

1. $\neg(p \wedge q) \Leftrightarrow (\neg p) \vee (\neg q)$
2. $\neg(p \vee q) \Leftrightarrow (\neg p) \wedge (\neg q)$

proof: We will check (1) by writing down the truth table for both sides.

p	q	$p \wedge q$	$\neg p$	$\neg q$	$(\neg p) \vee (\neg q)$
T	T	T	F	F	F
T	F	F	F	T	T
F	T	F	T	F	T
F	F	F	T	T	T

Notice that the column for "$(\neg p) \vee (\neg q)$" is exactly the negation of the column for "$p \wedge q$." The proof of (2) is left as an exercise. □

Example 1.2.11: Rewrite the following statements as logically equivalent statements without the negation.

1. $\neg$"$(x = 4) \vee (x = 5)$"
2. $\neg$"n is an even integer and m is an odd integer"
3. $\neg$"Tom will order Chinese or I will not order Mexican."

1. $\neg$"$(x = 4) \vee (x = 5)$" $\Leftrightarrow$ "$(x \neq 4) \wedge (x \neq 5)$"

   Written in English the left side says, "It is not true that x equals four or five." Clearly this is the same as saying, "x is not equal to four and x is not equal to 5."

2. $\neg$"n is an even integer and m is an odd integer" $\Leftrightarrow$ "n is an odd integer **or** m is an even integer."

3. $\neg$"Tom will order Chinese or I will not order Mexican." $\Leftrightarrow$ "Tom will not order Chinese **and** I will order Mexican."

Just as negation turns statements involving a logical *and* into statements involving a logical *or* and vice versa, negation also turns statements involving a $\forall$ into statements involving a $\exists$ and vice versa. It can be a little more tricky to construct a sensible statement, but if you keep in mind to exchange $\forall$ and $\exists$ it's not that hard to construct the negation of such statements.

Consider the negation of the statement,

"Every mammal is warm-blooded."

What would it mean for this statement to be false? A common error is to say the negation is "Every mammal is cold-blooded." But not every mammal has to be cold-blooded for the statement above to be false. All it would take would be for some weird mammal in the Brazilian rain forest or the Australian outback to turn out to be cold-blooded for the statement to be false. That's because the statement asserts something about "every" mammal. There has to exist only *one* cold-blooded mammal for the statement to be false. Thus the negation is actually:

"There exists a cold-blooded mammal."

Likewise consider the negation of the statement,

"There is a teenager who does not like texting."

Well, if you believe there are no teenagers who do not like texting (the negation of the statement above) then you believe that:

"Every teenager likes texting."

Example 1.2.12: Rewrite the following statements as logically equivalent statements without the negation.

1. ¬"All children love presents."
2. ¬"Some kinds of candy aren't good."
3. ¬"For every number x there is a number y such that $xy = 1$."
4. ¬"There is a number x such that for every number y, $xy = y$."

1. ¬"All children love presents." $\Leftrightarrow$ "There is a child who does not love presents."
2. ¬"Some kinds of candy aren't good." $\Leftrightarrow$ "All kinds of candy are good."

   Here you can read "some" as "there is a" (kind of candy which isn't good.)
3. ¬"For every number x there is a number y such that $xy = 1$." $\Leftrightarrow$ "There is a number x such that, for every number y, $xy \neq 1$."

   This statement is actually true. For the number $x = 0$, $0 \cdot y = 0 \neq 1$ for every number y.
4. ¬"There is a number x such that for every number y, $xy = y$." $\Leftrightarrow$ "For every number x there is a number y so that $xy \neq y$."

   This statement happens to be false. For the number $x = 1$ there is no number y so that $1 \cdot y \neq y$.

1.2.4 Compound Statements: Implications

Definition 1.2.13: Given two statements p and q, an *implication* "$p \Rightarrow q$" is a statement which is true unless p is true and q is false. It is generally read "p implies q." Implications are also known as *if-then* statements. In that form they are written "If p then q." In an implication the first statement p is called the *hypothesis* while the second statement q is called the *conclusion*.

Using a truth table the definition seems simple enough.

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

The idea of an implication is that the truth of the hypothesis is supposed to guarantee the truth of conclusion. If it doesn't, then the implication is false. Consider the implication,

"If you clean your room then we will go to the movies."

Given that you manage to clean your room you expect to go to the movies. Now if you clean your room and you don't get to go to the movies then you'll probably be angry. That would mean the implication was false... Mom lied!

The part that is counter-intuitive about implications is what happens when the hypothesis is false. Say you don't clean your room. Then you may or may not still go to the movies depending on how strongly Mom felt about the whole clean room thing. Intuitively you expect that the statement above simply doesn't apply. But a mathematical statement cannot be "doesn't apply". By definition it must be true or false. A glance at the truth table reveals that the statement is true if the hypothesis is false, regardless of the conclusion. In this case we say the implication is *vacuously true*. The only way you could really say that Mom lied is if you follow through on your part to clean your room and she doesn't take you to the movies. She can hardly be accused of lying if you don't clean your room, regardless of whether you go to the movies in the end.

Consider the statement,

"If $1 = 2$ then Dr. Paul is the Queen of England."

This is a true statement. It does not matter that Dr. Paul is not, in fact, the Queen of England. Since $1 \neq 2$ the hypothesis is false, so the implication is vacuously true.

Example 1.2.14: Determine whether the statements below are true or false. Assume that x is a real number.

1. "If $x = 2$ then $x^2 = 4$"
2. "If $x^2 = 4$ then $x = 2$"
3. "If $x^2 = -4$ then $x = -2$"

1. "If $x = 2$ then $x^2 = 4$" *True.*
2. "If $x^2 = 4$ then $x = 2$" *False.*

   If $x = -2$ then the hypothesis is true and the conclusion false. In general, an implication has to be true for every allowed value of the variables to be *true*. Another way to think of it is, "Does x^2 being four force x to be two? No."
3. "If $x^2 = -4$ then $x = -2$" *True.*

   For x a real number it is not possible for $x^2 = -4$. Hence the statement is *vacuously true*. Note that if we allowed x to take on complex values then the statement would be false. Let $x = 2i$. Then the hypothesis is true, but the conclusion is false.

There are a number of statements that are associated to an implication. Consider first the negation of an implication.

Theorem 1.2.15:

$$\neg(p \Rightarrow q) \;\Leftrightarrow\; p \wedge (\neg q)$$

proof: Easily checked using a truth table.

p	q	$p \Rightarrow q$	p	$\neg q$	$p \wedge (\neg q)$
T	T	T	T	F	F
T	F	F	T	T	T
F	T	T	F	F	F
F	F	T	F	T	F

Notice that the negation of the third column is the same as the sixth column. □

This is just a more careful restatement of what we said earlier. The only way an implication can be false (and thus the only way its negation can be true) is if its hypothesis is true (p) **and** its conclusion is false ($\neg q$).

> **Definition 1.2.16:** The *converse* of an implication $p \Rightarrow q$ is the reversed implication $q \Rightarrow p$.

It is a common error to believe that the implication is logically equivalent to its converse. It is not. In general the converse of an implication is completely logically independent of the implication. That means that both may be true, both false, or either one true while the other is false.

Consider the implication

"If $x = 2$ then $x^2 = 4$."

This implication is true. Now consider its converse.

"If $x^2 = 4$ then $x = 2$."

As we saw earlier this implication is false. Another example,

"If an animal is human then the animal is a mammal."

True, but the converse...

"If an animal is a mammal then the animal is human."

...is clearly false.

> **Definition 1.2.17:** The *contrapositive* of an implication $p \Rightarrow q$ is the reversed implication with negations $(\neg q) \Rightarrow (\neg p)$.

Consider again the implication,

"If $x = 2$ then $x^2 = 4$."

Its contrapositive is

"If $x^2 \neq 4$ then $x \neq 2$."

Note that this implication is true. Consider again,

"If an animal is human then the animal is a mammal."

The contrapositive is

"If an animal is not a mammal then the animal is not human."

...which is again true. In fact, an implication is logically equivalent to its contrapositive.

Theorem 1.2.18:

"$p \Rightarrow q$" $\Leftrightarrow$ "$(\neg q) \Rightarrow (\neg p)$"

proof: Again we just need to check the truth tables.

p	q	$p \Rightarrow q$	$\neg q$	$\neg p$	$(\neg q) \Rightarrow (\neg p)$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

The third column and the sixth are the same, hence the two statements are logically equivalent. □

Example 1.2.19: Write the negation, the converse, and the contrapositive to the implications below.

1. "If you use natural ingredients then your soup will be good."
2. "If $b^2 - 4ac > 0$ then the equation $ax^2 + bx + c = 0$ has two solutions."
3. "If $f'(a) = 0$ and $f''(a) < 0$ then f has a local maximum at $x = a$."
4. "If there is a number a so that $\lim_{x \to a^+} f(x) \neq \lim_{x \to a^-} f(x)$ then f is not continuous."

1. "If you use natural ingredients then your soup will be good."
   - *Negation:* "You use natural ingredients and your soup is not good."
   - *Converse:* "If your soup is good then you used natural ingredients."
   - *Contrapositive:* If your soup is not good then you did not use natural ingredients."
2. "If $b^2 - 4ac > 0$ then the equation $ax^2 + bx + c = 0$ has two solutions."
   - *Negation:* "$b^2 - 4ac > 0$ and the equation $ax^2 + bx + c = 0$ does not have two solutions."
   - *Converse:* "If the equation $ax^2 + bx + c = 0$ has two solutions then $b^2 - 4ac > 0$."
   - *Contrapositive:* "If the equation $ax^2 + bx + c = 0$ does not have two solutions then $b^2 - 4ac \leq 0$."
3. "If $f'(a) = 0$ and $f''(a) < 0$ then f has a local maximum at $x = a$."
   - *Negation:* "$f'(a) = 0$ and $f''(a) < 0$ and f does not have a local maximum at $x = a$."

- *Converse:* "If f has a local maximum at $x = a$ then $f'(a) = 0$ and $f''(a) < 0$."
- *Contrapositive:* "If f does not have a local maximum at $x = a$ then $f'(a) \neq 0$ or $f''(a) \geq 0$."

4. "If there is a number a so that $\lim_{x\to a^+} f(x) \neq \lim_{x\to a^-} f(x)$ then f is not continuous."

   - *Negation:* "There is a number a so that $\lim\limits_{x\to a^+} f(x) \neq \lim\limits_{x\to a^-} f(x)$ and f is continuous."
   - *Converse:* "If f is not continuous then there is a number a so that $\lim\limits_{x\to a^+} f(x) \neq \lim\limits_{x\to a^-} f(x)$"
   - *Contrapositive:* "If f is continuous then for every number a, $\lim\limits_{x\to a^+} f(x) = \lim\limits_{x\to a^-} f(x)$"

Finally I point out that the notation for implication and the notation for logical equivalence actually do agree. If p implies q and q implies p then p and q really are logically equivalent. This is often written as "p if and only if q." (The "If" part comes from $p \Rightarrow q$; the "Only if" part come from $q \Rightarrow p$.)

Said yet another way,

Theorem 1.2.20:

"$(p \Rightarrow q) \wedge (q \Rightarrow p)$" $\Leftrightarrow$ "$p \Leftrightarrow q$"

proof: Yet again we just need to check the truth tables.

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$	$p \Leftrightarrow q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

Recall that $p \Leftrightarrow q$ is the statement that is true when p and q have the same truth value (either both true or both false). Note that the fifth column and the sixth column are the same. Therefore the two statements are logically equivalent. $\square$

There will be very few true tables as we go on in the course. When we want to prove two statements are logically equivalent we will generally set about trying to prove first that one implies the other, then prove the converse. By the theorem above, that is the same as proving they are equivalent.

1.2.5 Problems

Problem 1.2.21: For the following statements write the negation.

1. $n > x$ or $n > y$ or $n > z$.
2. There exist x, y, z so that $(xy)z \neq x(yz)$.
3. For all integers a, b there are integers q, r so that $a = qb + r$.

Problem 1.2.22: For the following implications write the negation, the converse, and the contrapositive.

1. If $x^2 + y^2 = 0$ then $x = 0$ and $y = 0$.
2. If $\frac{a}{b}$ and $\frac{b}{c}$ are integers then $\frac{a}{c}$ is an integer.
3. Let $p(x)$ be a polynomial. If $p(x)$ has odd degree then there is a number a so that $p(a) = 0$.
4. If there exist numbers, $x, y \in \mathbb{R}$ so that $x \neq y$ and $x^2+xy+y^2+x+y = 0$ then f is not one-to-one.

Problem 1.2.23: (See Theorem 1.2.10) Use a true table to prove that

"$\neg(p \vee q)$" $\Leftrightarrow$ "$(\neg p) \wedge (\neg q)$"

Problem 1.2.24: A *syllogism* is a statement of the form

"If $p \Rightarrow q$ and $q \Rightarrow r$ then $p \Rightarrow r$."

This makes perfect sense if you think about it. The classic(al) example is:

"If Socrates is a man and men are mortal then Socrates is mortal."

Use the truth table below to prove that syllogisms are always true. Note that since a syllogism is constructed from three simple statements (p, q, r), the truth table has to have eight rows to accommodate the eight possible true/false combinations for p, q, and r. I've filled out the third row so you can see how it works.

p	q	r	$p \Rightarrow q$	$q \Rightarrow r$	$(p \Rightarrow q) \wedge (q \Rightarrow r)$	$p \Rightarrow r$	"$(p \Rightarrow q) \wedge (q \Rightarrow r)$" $\Rightarrow$ "$p \Rightarrow r$"
T	T	T					
T	T	F					
T	F	T	F	T	F	T	T (vacuously)
T	F	F					
F	T	T					
F	T	F					
F	F	T					
F	F	F					

1.3 Sets

Notation

$\in$	is an element of... some set
$\notin$	is not an element of... some set
$\subseteq$	subset, contained in
$\nsubseteq$	not a subset, not contained in
ϕ	empty set
2^A	power set of A
$\mathbb{N}$	Natural numbers
$\mathbb{Z}$	Integers (whole numbers)
$\mathbb{Q}$	Rational numbers
$\mathbb{R}$	Real numbers
$\mathbb{C}$	Complex numbers
$\cup$	set union
$\cap$	set intersection
$\setminus$	set subtraction
$\times$	Cartesian product
^{c}	set complement
$\mathbb{R}^2$	Cartesian plane

1.3.1 Basic Definitions

One of the most basic ideas in mathematics is the idea of a set. Because it is so basic it is kind of difficult to define carefully, and even if you do, the careful definition isn't very illuminating. Instead we will wave our hands just a little bit and define a set as follows:

> **Definition 1.3.1:** A *set* is a collection of objects such that any object either is or is not a member. Sets with only a few members are enclosed within "curly braces" { ...objects... }

You might reasonably now ask, "What's an object?" I would then shrug and reply that an object can be just about anything... including another set. It is possible to define a collection in a very clever way so that the "any object either is or is not a member" condition fails. The resulting collection is called a *class*. We're not going to worry about all that. Pretty much any reasonably defined collection is a set.

(If you have an interest in this, look up *Russell's Paradox*. It begins with the idea that you can have a set which has *itself as a member*! Freaky, huh?)

Example 1.3.2: The following are sets.

1. Let C be the set of all colors.
2. Let $S = \{\text{Peter, Paul, Mary}\}$.
3. Let $R = \{\text{red, green, blue}\}$.
4. Let $\mathbb{N} =$ positive, whole numbers.
5. Let H be the set of all humans.

Note that S and R are *finite* sets—they each have only three elements. On the other hand C and $\mathbb{N}$ are *infinite* sets. H is a finite set which still has a very large number of elements (several billion). We'll define the idea of finite and infinite sets more carefully in a later section.

Definition 1.3.3: An object that is in a set is called an *element* of that set.
If the set is named A and the object a, then we write "$a \in A$".

Since by definition any object either is or is not in any given set, "$a \in A$" is a mathematical statement—it is either true of false. The negation of this statement is written $a \notin A$.

Example 1.3.4: Using the set definitions from Example 1.3.2,

1. red $\in C$. $4 \notin C$.
2. Mary $\in S$. Dr.Paul $\notin S$.
3. green $\in R$.
4. Mary $\in H$. $17 \notin H$.

Definition 1.3.5: A set A is contained in another set B if and only if every element of A is also an element of B. The statement "A is contained in B" is written "$A \subseteq B$." We may also say "A is a subset of B."
More formally, we can write this as an implication,

"$A \subseteq B$" $\Leftrightarrow$ "$a \in A \ \Rightarrow \ a \in B$"

Example 1.3.6: Using the set definitions from Example 1.3.2,

1. $R \subseteq C$. This is a true statement since the three elements of R are also elements of C.

2. $S \subseteq H$. This is a true statement as long as we understand Peter, Paul, and Mary (the elements of S) are humans, rather than, say, cats or something.

3. $S \nsubseteq C$. This is how we write the negation for set containment, "$\neg(S \subseteq C)$." Since neither Peter, Paul, nor Mary are colors, S is not contained in C.

4. $\{\text{cyan}, \text{teal}, \text{Dr.Paul}\} \nsubseteq C$. The first two elements are colors, but Dr.Paul is not, so this set is **not** a subset of C. To be a subset *every* element in the small set must also be in the big set.

Note, by the way, that for any set A, the statement "$A \subseteq A$" is true. Every set is a subset of itself. We use this fact to define exactly what we mean by *set equality*. Intuitively if I say two sets are "equal" what do I mean? Surely that they have the same elements. Said another way, two sets are equal if every element in the first set is also in the second, and vice versa. Formally,

Definition 1.3.7: For sets A and B,

"$A = B$" $\Leftrightarrow$ "$A \subseteq B$" and "$B \subseteq A$"

Now we want to define a particularly important set.

Definition 1.3.8: The *empty set* "ϕ" is defined to be the set with no elements. Sometimes this is written "$\phi = \{\}$."

The empty set can be kind of slippery to get your head around. It is the set equivalent of the number "zero." Put yourself in the place of, say, and early Roman accountant. "Why do I need this number 'zero'," he might reasonably ask. "Why would I need a number that is nothing?" Of course zero is not "nothing." It is a very real, concrete number that represents the quantity "none." We're all very much more familiar with zero than our poor Roman accountant, and all understand how useful an idea it is. It may be less immediately obvious that ϕ is useful in a similar way. Like zero, the empty set is not "nothing." It represents the set that contains nothing. And like zero, that is very much something.

While we're talking about it, you should realize that zero and the empty set are very different things. Zero is a number, not a set. Further, the set that contains only zero is not empty—it contains zero! Similarly, ϕ is not a number, it is a set.

Theorem 1.3.9: For any set A, $\phi \subseteq A$

proof: $\phi \subseteq A$ is equivalent to the statement, "If $x \in \phi$ then $x \in A$." But this statement is vacuously true since the hypothesis is always *false*. There are no elements in ϕ. $\square$

All these definitions get a little confusing when we consider sets which have elements that are themselves sets.

Example 1.3.10: Consider the set,

$$A = \{x, y, \{x, y\}\}$$

A has three elements: x, y, and the set that contains x and y.
Which of the following statements are true?

1. $x \in A$.
2. $\{x\} \in A$.
3. $\{x\} \subseteq A$.
4. $\{x, y\} \in A$.
5. $\{x, y\} \subseteq A$.
6. $\phi \in A$.
7. $\phi \subseteq A$.

1. $x \in A$. *True.* x is the first listed element in A.
2. $\{x\} \in A$. *False.* The set that contains x is a completely different object than x itself. The set that contains x is not one of the three elements of A.
3. $\{x\} \subseteq A$. *True.* Every element in $\{x\}$—all one of them—is also an element of A.
4. $\{x, y\} \in A$. *True.* The set that contains x and y happens to also be an element of A. The third listed element, as it happens.
5. $\{x, y\} \subseteq A$. *True.* Both elements of $\{x, y\}$, that is x and y, are also elements of A.
6. $\phi \in A$. *False.* The empty set is not one of the three elements of A.
7. $\phi \subseteq A$. *True.* The empty set is a subset of *every* set including this one.

One last comment about the example above. I said "the first listed element" and "the third listed element." This was just to distinguish which elements of A I was talking about. In fact the order in which the elements of a set are listed have no bearing on the set. That is,

$$\{x, y, \{x, y\}\} = \{x, \{x, y\}, y\} = \{\{x, y\}, y, x\}$$

They all represent the same set. Now in a later section we will talk about "ordering" sets. This is actually a fairly tricky business. But when you are just defining a set by listing the elements, the order it which you list them is completely irrelevant. Generic sets have no order.

The most important type of set which contains sets is a *power set*.

Definition 1.3.11: Given a set A, the *power set* of A, 2^A, is the set of all subsets of A. That is,

$$2^A = \{B \mid B \subseteq A\}$$

Example 1.3.12: Write down the power set for the set $A = \{0, 1, a\}$.

$$2^A = \{\phi, \{0\}, \{1\}, \{a\}, \{0, 1\}, \{0, a\}, \{1, a\}, \{0, 1, a\}\}$$

Note that $a \notin 2^A$. 2^A is a set that contains only sets and a is a letter, not a set.
It is true that $\{a\} \in 2^A$.

Later we'll prove a theorem that if A is a finite set with n elements, then 2^A will have 2^n elements. This is why we use this sort of weird notation for the power set. We are not really "exponentiating" a set. (What would that even mean?)

1.3.2 Common Sets

In math classes the most common sets you come across are sets of numbers. Certain sets of numbers come up so often that they have their own names and symbols. We've already seen one, the *Natural numbers*, $\mathbb{N}$. This set was defined in Example 1.3.2. They are also known as the *Counting numbers*.

$$\mathbb{N} = \{1, 2, 3 \ldots\}$$

The natural numbers don't include zero or the negative whole numbers. The set that consists of all the whole numbers is called the *integers*, $\mathbb{Z}$.

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

(Why the 'Z'? you may ask. The German word for 'number' is 'zahlen'.)

Of course the type of number we usually mean when we say 'number' is a *real number*. The set of real numbers is denoted $\mathbb{R}$. While we're all very familiar with the real numbers,

they're actually kind of tricky to define. One way is to define them as all integers plus finite or infinite decimal parts. Even then there're some subtleties. For instance, two different decimals can represent the same real number.

$$0.99999\ldots = 1.00000\ldots$$

A class in mathematical *analysis* will get into the formal definition of the real numbers. In this class we'll just assume we more or less know what we're talking about when we say "x is a real number."

A way to define a set that we'll find useful at this point is the so-called "set builder" notation. Here is the basic form for defining a set S.

$$S = \{x \mid \text{some condition on } x\}$$

The "|" is read as "such that." (But wasn't "$\ni$" read "such that" in the last section, you ask? Yes it was. In set builder notation it's a |. Sorry, I didn't invent it. Don't shoot the messenger.)

> **Example 1.3.13:** Define the interval in the real numbers between 1 and 4, including 1 but not including 4, using set builder notation.
>
> $$[1, 4) = \{x \in \mathbb{R} \mid x \geq 1 \wedge x < 4\}$$
>
> In English, "the set of real numbers, x, such that x is greater than or equal to 1 **and** strictly less than 4."
> In practice we usually omit the explicit $\wedge$ and just list the conditions separated by commas. The logical *and* is implied.
>
> $$[1, 4) = \{x \in \mathbb{R} \mid x \geq 1, x < 4\}$$

We can now use set builder notation to define two other common sets. First the *rational numbers*, the set of all fractions.

$$\mathbb{Q} = \left\{ \frac{n}{m} \mid n, m \in \mathbb{Z}, m \neq 0 \right\}$$

So, for instance $\frac{1}{2} \in \mathbb{Q}$. $-\frac{527}{12} \in \mathbb{Q}$ as well. $8 \in \mathbb{Q}$ since $8 = \frac{8}{1}$. Thus $\mathbb{Z} \subseteq \mathbb{Q}$.

It is a subtle and interesting fact that $\mathbb{Q} \neq \mathbb{R}$. Later we will prove the fact that $\sqrt{2} \notin \mathbb{Q}$. That is, $\sqrt{2} \neq \frac{n}{m}$ for any integers n and m.

The final common set we'll define is the *complex numbers*, $\mathbb{C}$.

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}, i = \sqrt{-1}\}$$

So, for instance, $1 + i\sqrt{3} \in \mathbb{C}$. $\pi - ei \in \mathbb{C}$ as well.

For any real number, x, we have

$$x = x + 0i \in \mathbb{C}$$

hence $\mathbb{R} \subseteq \mathbb{C}$.

1.3.3 Operations on Sets

Just as we could combine simple statements in various ways to make more complex compound statements, there are several ways in which we can combine sets together to make new sets.

Definition 1.3.14: Given sets A and B, the *union* "$\cup$" of A and B is the set of elements that are in either A or B. In set builder notation,

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

Definition 1.3.15: Given sets A and B, the *intersection* "$\cap$" of A and B is the set of elements that are in both A and B. In set builder notation,

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

Example 1.3.16: List the elements of the union and intersection of the given sets.

1. $A = \{1, 2, 3, 4\} \quad B = \{a, b, c\}$
2. $A = \{1, 2, 3, 4\} \quad B = \{0, 2, 4, 6, 8\}$
3. $A = [1, 4) \quad B = (2, 7]$ (these are intervals of real numbers)
4. $A = \mathbb{N} \quad B = \mathbb{R}$

1. $A = \{1, 2, 3, 4\} \quad B = \{a, b, c\}$

   $A \cup B = \{1, 2, 3, 4, a, b, c\}$ Remember the order doesn't matter.
   It also true that $A \cup B = \{4, 1, a, 2, c, 3, b\}$

   $A \cap B = \phi$ There are no elements in both sets.

2. $A = \{1, 2, 3, 4\} \quad B = \{0, 2, 4, 6, 8\}$

   $A \cup B = \{0, 1, 2, 3, 4, 6, 8\}$

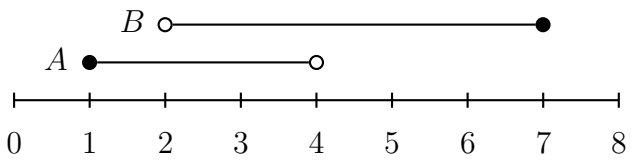
   $A \cap B = \{2, 4\}$

3. $A = [1, 4) \quad B = (2, 7]$

   $A \cup B = [1, 7]$

   $A \cap B = (2, 4)$

   This is perhaps most easily seen on a number line.



4. $A = \mathbb{N} \quad B = \mathbb{R}$

   $A \cup B = \mathbb{R}$

   $A \cap B = \mathbb{N}$

A similar operation is *subtraction* of sets.

Definition 1.3.17: Given sets A and B, *set subtraction* "\" of A minus B is the set of elements that are in A but not B. In set builder notation,

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

Example 1.3.18: List the elements of the set subtraction A minus B.

1. $A = \{1, 2, 3, 4\} \quad B = \{a, b, c\}$
2. $A = \{1, 2, 3, 4\} \quad B = \{0, 2, 4, 6, 8\}$
3. $A = [1, 4) \quad B = (2, 7]$ (these are intervals of real numbers)
4. $A = \mathbb{N} \quad B = \mathbb{R}$

1. $A = \{1, 2, 3, 4\} \quad B = \{a, b, c\}$

   $A \setminus B = \{1, 2, 3, 4\}$

   Since there are no elements of B in A, the set subtraction does nothing.

2. $A = \{1, 2, 3, 4\} \quad B = \{0, 2, 4, 6, 8\}$

   $A \setminus B = \{1, 3\}$

3. $A = [1, 4) \quad B = (2, 7]$

   $A \setminus B = [1, 2]$

4. $A = \mathbb{N} \quad B = \mathbb{R}$

   $A \setminus B = \phi$

We want to define one more set theoretic idea, that of the *complement*. Intuitively the complement of a set is everything that is **not** in the set. We have to restrict this a little bit, though. For instance you might argue that my cat, Gandalf, is in the complement of the interval $[0, 1]$. After all, Gandalf is not a real number between zero and one. To be useful the complement must be with respect to some "universal" set that is usually clear from the context.

Definition 1.3.19: Given a set A, the complement "A^c" is the universal set "U" (determined from the context) minus A. That is,

$$A^c = U \setminus A$$

Example 1.3.20: For each set A, write the universal set and the complement.

1. $A = \{\text{Saturday}, \text{Sunday}\}$
2. $A = [0, 1]$
3. $A = \{a + ib \in \mathbb{C} \mid b > 1\}$
4. $A = \mathbb{N}$

1. $A = \{\text{Saturday}, \text{Sunday}\}$
   $U = \{\text{Saturday}, \text{Sunday}, \text{Monday}, \text{Tuesday}, \text{Wednesday}, \text{Thursday}, \text{Friday}\}$
   $A^c = \{\text{Monday}, \text{Tuesday}, \text{Wednesday}, \text{Thursday}, \text{Friday}\}$
2. $A = [0, 1]$
   $U = \mathbb{R}$
   $A^c = (-\infty, 0) \cup (1, \infty)$
3. $A = \{a + ib \in \mathbb{C} \mid b > 1\}$
   $U = \mathbb{C}$
   $A^c = \{a + ib \in \mathbb{C} \mid b \leq 1\}$
4. $A = \mathbb{N}$
   $U = \mathbb{Z}$ (You could also argue for $U = \mathbb{R}$.)
   $A^c = \{\ldots - 3, -2, -1, 0\}$

We'll define one other operation, and this one will be very important in the next several sections.

Definition 1.3.21: The *Cartesian product* of two sets, "$A \times B$" is the set of ordered pairs (x, y) where $x \in A$ and $y \in B$. That is,

$$A \times B = \{(x, y) \mid x \in A,\ y \in B\}$$

Example 1.3.22: List the elements of the Cartesian product.

$$\{a, b, c\} \times \{1, 2, 3\}$$

$$\{a, b, c\} \times \{1, 2, 3\} = \{(a, 1),\ (a, 2),\ (a, 3),\ (b, 1),\ (b, 2),\ (b, 3),\ (c, 1),\ (c, 2),\ (c, 3)\}$$

Note that while the sets themselves are not ordered, the *pairs* are ordered. For example, $(b, 1) \in \{a, b, c\} \times \{1, 2, 3\}$ but $(1, b) \notin \{a, b, c\} \times \{1, 2, 3\}$. More generally, $A \times B \neq B \times A$.

The Cartesian product we are all most familiar with is the *Cartesian plane*, $\mathbb{R}^2$. This is just the set of ordered pairs of real numbers, where the first number denotes the horizontal position in the plane (x coordinate) and the second the vertical position (y coordinate). If we glance back at the definition of the Cartesian product we can see that $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.

1.3.4 Set Proofs

Our first foray into formal proofs beyond simple truth tables will be proving set containment. Recall that

$$A \subseteq B \ \Leftrightarrow\ x \in A \Rightarrow x \in B$$

That is, the way you prove that A is contained in B is to pick an arbitrary element of A and show that it has to also be in B. Thus proofs of containment always have the same basic "shape."

Consider $x \in$(the small set).

. . . do math . . . do math . . .

Therefore $x \in$(the big set).

The following example shows how important it is to use parentheses when writing sets with unions and intersections.

Example 1.3.23: Prove that for any sets A, B, and C,

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

Proof: Consider $x \in (A \cup B) \cap C$

$\Rightarrow x \in A \cup B$ and $x \in C$ definition of $\cap$
$\Rightarrow (x \in A$ or $x \in B)$ and $x \in C$ definition of $\cup$

When presented with logical *or*, the proof has to proceed in cases.

Case 1: $x \in A$ and $x \in C$

$\Rightarrow x \in A$ definition of and
$\Rightarrow x \in A$ or $x \in (B \cap C)$ definition of or
$\Rightarrow x \in A \cup (B \cap C)$ definition of $\cup$

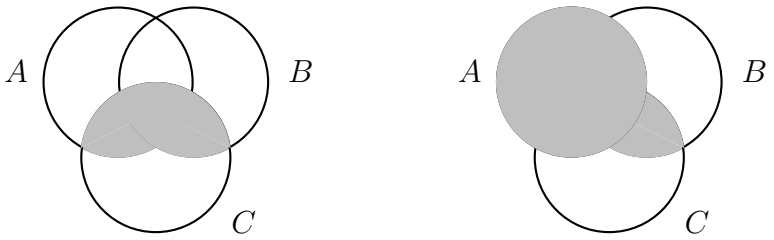
Case 2: $x \in B$ and $x \in C$

$\Rightarrow x \in B \cap C$ definition of $\cap$
$\Rightarrow x \in A$ or $x \in (B \cap C)$ definition of or
$\Rightarrow x \in A \cup (B \cap C)$ definition of $\cup$

Therefore, in either case, $x \in A \cup (B \cap C)$. $\square$

Now you might with some justice complain that I took two or three lines to show something that was blindingly obvious. I respond that this is the nature of a formal proof. It is true that as you progress in this course (and your career) your proofs will not be quite so gruesomely detailed. However at this point, it is a great exercise to break down the logical steps as much as is humanly possible.

Another criticism might be that the formal proof isn't very intuitive. True enough, and intuition is important. When presented with a statement that you are supposed to prove, it's a good practice to convince yourself it's true before beginning the formal proof. For instance when I first saw the last example, I drew a picture with three overlapping circles, and shaded in the set $(A \cup B) \cap C$. Then I did it again for $A \cup (B \cap C)$. It was immediately obvious that the theorem was true for this little special case.



Now the sets A, B, C are not generally subsets of the plane, much less the insides of circles. Still it's a useful way to train your intuition. It is not, however, a proof. Let me say that again.

These pictures are NOT a proof!

Let's move on to proving the *equality* of sets. Recall that

$$A = B \Leftrightarrow A \subseteq B \text{ and } B \subseteq A$$

Proofs of set equality, then, are just two proofs of set containment.

Example 1.3.24: Prove that for any sets A and B,

$$(A \cup B)^c = A^c \cap B^c$$

proof: We need to prove first that $(A \cup B)^c \subseteq A^c \cap B^c$, and then that $A^c \cap B^c \subseteq (A \cup B)^c$.

First, consider $x \in (A \cup B)^c$.

$\Rightarrow x \notin A \cup B$ definition of complement
$\Rightarrow \neg(x \in A \vee x \in B)$ definitions of negation and $\cup$
$\Rightarrow x \notin A \wedge x \notin B$ DeMorgan Law (Theorem 1.2.10)
therefore $x \in A^c \cap B^c$ definitions of complement and $\cap$

So $(A \cup B)^c \subseteq A^c \cap B^c$.
Second, consider $x \in A^c \cap B^c$.

$\Rightarrow x \notin A \wedge x \notin B$	definitions of complement and $\cap$
$\Rightarrow \neg(x \in A \vee x \in B)$	DeMorgan Law (Theorem 1.2.10)
$\Rightarrow \neg(x \in A \cup B)$	definition of $\cup$
$\Rightarrow x \notin (A \cup B)$	definition of negation
therefore $x \in (A \cup B)^c$	definition of complement

So $A^c \cap B^c \subseteq (A \cup B)^c$. Hence $(A \cup B)^c = A^c \cap B^c$. $\square$

1.3.5 Problems

Problem 1.3.25: Let $A = \{a\}$.

(a) Write down the set 2^A.

(b) Write down the set 2^{2^A}

Problem 1.3.26: Describe the sets using set-builder notation.

(a)

$$\{1,\ 4,\ 9,\ 16,\ 25\ldots\}$$

(b)

$$\{\ldots\frac{1}{27},\ \frac{1}{9},\ \frac{1}{3},\ 1,\ 3,\ 9,\ 27\ldots\}$$

Problem 1.3.27: List the elements of the set.

(a)

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

(b)

$$\{4n+1 \mid n \in \mathbb{Z}\}$$

Problem 1.3.28: List the elements of $A \cup B$, $A \cap B$, and $A \setminus B$.

(a) $A = \{a, b, c, d, e\}$ $B = \{a, c, f\}$.

(b) $A = (-\infty, -2] \cup [3, \infty)$ $B = (-5, 5)$.

(c) $A = \mathbb{Z}$ $B = \mathbb{N}$.

Problem 1.3.29: List the elements of the complement of the set A.

(a) $A = [0, 1] \cup [2, 4]$

(b) $A = \{2n + 1 \mid n \in \mathbb{Z}\}$

Problem 1.3.30: Prove that if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.

Problem 1.3.31: Prove that for any sets A and B,

$$(A \cap B)^c = A^c \cup B^c$$

1.4 Binary Relations

In the last section we talked a lot about sets. But if we think about it, the sets we care about are much more than loose collections of elements. In $\mathbb{R}$ or $\mathbb{Z}$, the numbers can be added and multiplied, and they have an order. Most sets that you see in a math class have much more structure than what you see in a generic set. One way to give a set "structure" is to define a *binary relation* on the set. This "relates" some points in the set to some other points. The "relations" are defined in a one-on-one way, hence the term "binary."

1.4.1 Example Relations

To illustrate this consider a set of five students: Ann, Bob, Carrie, David, and Edgar. If you wanted to say how they "relate" to each other, that would be a large and detailed undertaking. But if you wanted a simple overview, you might just ask "Among these students, who 'likes' whom?" The answer might be a list like the following:

Ann likes Bob, and Bob likes Carrie, but Ann and Carrie don't particularly like each other.

Carrie likes Edgar, David likes Edgar, and Edgar likes David (but not Carrie).

All the students like themselves except Carrie (who apparently has self-esteem issues).

To write this set of "relations" more compactly, you might just write them in pairs where the first person likes the second person.

(Ann, Bob)
(Bob, Carrie)
(Carrie, Edgar)
(David, Edgar)
(Edgar, David)
(Ann, Ann)
(Bob, Bob)
(David, David)
(Edgar, Edgar)

These nine pairs together define a binary relation on the set of students, S.

$S = \{\text{Ann, Bob, Carrie, David, Edgar}\}$.

Formally, the binary relation, B, is the set

$B = \{$(Ann, Bob), (Bob, Carrie), (Carrie, Edgar), (David, Edgar), (Edgar, David), (Ann, Ann), (Bob, Bob), (David, David), (Edgar, Edgar)$\}$

Since Ann likes Bob, (Ann,Bob)$\in B$. But since Bob doesn't like Ann, (Bob,Ann)$\notin B$. If you recall the definition of the Cartesian product (Definition 1.3.21) then clearly $B \subseteq S \times S$. In general this is all that a binary relation is.

> **Definition 1.4.1:** A *binary relation* R on a set A is simply a subset of $A \times A$. That is,
>
> $$R \subseteq A \times A$$

One way to think about the Cartesian product $S \times S$ is as a 5×5 table.

	Ann	Bob	Carrie	David	Edgar
Ann					
Bob					
Carrie					
David					
Edgar					

The binary relation B is then just a set of entrees in this table.

	Ann	Bob	Carrie	David	Edgar
Ann	x	x			
Bob		x	x		
Carrie					x
David				x	x
Edgar				x	x

The nine "x"s in the table correspond to the nine pairs in the binary relation.

For a less trivial example consider the relation D on the natural numbers $\mathbb{N}$ defined by

$$D = \left\{(n, m) \in \mathbb{N} \times \mathbb{N} \mid \frac{m}{n} \in \mathbb{N}\right\}$$

When presented with a weird set like this it's a good idea to try to figure out some of its elements... and then figure out some things that are **not** its elements.

$(2, 4) \in D$ since $\frac{4}{2} = 2 \in \mathbb{N}$.

$(2, 6) \in D$ since $\frac{6}{2} = 3 \in \mathbb{N}$.

$(3, 4) \notin D$ since $\frac{4}{3} \notin \mathbb{N}$.

$(5, 1) \notin D$ since $\frac{1}{5} \notin \mathbb{N}$.

That is, $(n, m) \in D$ if n divides evenly into m. $(3, 4) \notin D$ since four thirds is not a positive whole number (that's the definition of $\mathbb{N}$).

Since $\mathbb{N}$ is an infinite set we cannot list the complete relation in a table, but we can at least present part of it.

	1	2	3	4	5	6	7	8	...
1	x	x	x	x	x	x	x	x	
2		x		x		x		x	
3			x			x			
4				x				x	
5					x				
⋮									

Example 1.4.2: For each relation write two pairs that are in the relation and two that are not.

1. T on $\mathbb{Z}$ defined by

$$T = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n - m = 10\}$$

2. H on $\mathbb{R}$ defined by

$$H = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid xy = 1\}$$

3. M on $\mathbb{Z}$ defined by

$$M = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n - m = 3k \text{ for some } k \in \mathbb{Z}\}$$

4. P on $\mathbb{R}$ defined by

$$P = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid xy > 0\}$$

5. C on $\mathbb{R}^2$ defined by

$$C = \left\{((x, y), (z, t)) \in \mathbb{R}^2 \times \mathbb{R}^2 \mid x^2 + y^2 = z^2 + t^2\right\}$$

1. T on $\mathbb{Z}$ defined by

$$T = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n - m = 10\}$$

$(12, 2) \in T$ since $12 - 2 = 10$. $(6, -4) \in T$ since $6 - (-4) = 10$.
$(2, 12) \notin T$ since $2 - 12 = -10 \neq 10$. $(6, 4) \notin T$ since $6 - 4 = 2 \neq 10$.

2. H on $\mathbb{R}$ defined by

$$H = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid xy = 1\}$$

$\left(\frac{1}{2}, 2\right) \in H$ since $\frac{1}{2} \cdot 2 = 1$. $\left(-\frac{5}{12}, -\frac{12}{5}\right) \in H$ since $-\frac{5}{12} \cdot \left(-\frac{12}{5}\right) = 1$.

$(2, 2) \notin H$ since $2 \cdot 2 = 4 \neq 1$. $(-1, 1) \notin H$ since $(-1) \cdot 1 = -1 \neq 1$.

3. M on $\mathbb{Z}$ defined by

$$M = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n - m = 3k \text{ for some } k \in \mathbb{Z}\}$$

$(7, 1) \in M$ since $7 - 1 = 6 = 3(2)$. Here $k = 2$.
$(5, 17) \in M$ since $5 - 17 = -12 = 3(-4)$. Here $k = -4$.
$(6, 1) \notin M$ since $6 - 1 = 5 = 3\left(\frac{5}{3}\right)$ and $k = \frac{5}{3} \notin \mathbb{Z}$.
$(0, 7) \notin M$ since $0 - 7 = -7 = 3\left(-\frac{7}{3}\right)$ and $k = -\frac{7}{3} \notin \mathbb{Z}$.

4. P on $\mathbb{R}$ defined by

$$P = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid xy > 0\}$$

$(2, \sqrt{3}) \in P$ since $2 \cdot \sqrt{3} > 0$. $(-\pi, -15) \in P$ since $(-\pi) \cdot (-15) = 15\pi > 0$.

$(1, 0) \notin P$ since $1 \cdot (0) = 0 \leq 0$. $(-\sqrt{2}, \sqrt{3}) \notin P$ since $(-\sqrt{2}) \cdot \sqrt{3}) = -\sqrt{6} \leq 0$.

5. C on $\mathbb{R}^2$ defined by

$$C = \left\{((x, y), (z, t)) \in \mathbb{R}^2 \times \mathbb{R}^2 \mid x^2 + y^2 = z^2 + t^2\right\}$$

This one is a little tricky because it's a relation on $\mathbb{R}^2$ which is, itself, a Cartesian product. So C consists of *pairs of pairs* of numbers.

$((3, 4), (0, -5)) \in C$ since $3^2 + 4^2 = 25 = 0^2 + (-5)^2$.

$((-1, \sqrt{3}), (\sqrt{2}, \sqrt{2})) \in C$ since $(-1)^2 + (\sqrt{3})^2 = 4 = (\sqrt{2})^2 + (\sqrt{2})^2$.

$((3, 4), (7, 0)) \notin C$ since $3^2 + 4^2 = 25 \neq 49 = 7^2 + 0^2$.

$((1, -\sqrt{3}), (-2, -2)) \notin C$ since $1^2 + (-\sqrt{3})^2 = 4 \neq 8 = (-2)^2 + (-2)^2$.

1.4.2 Properties of Relations

A general binary relation is still a very general object. In order to get something useful we need to impose some further properties. In this class four properties will be important.

Definition 1.4.3: A binary relation R on a set A is *reflexive* if and only if for every $a \in A$, $(a, a) \in R$. That is,

$$R \text{ reflexive } \Leftrightarrow \forall a \in A, (a, a) \in R$$

Put another way, a binary relation is *reflexive* if every element is "related" to itself.

Looking back to the example binary relations from last subsection, we can see that B is **not** reflexive since Carrie does not like herself. (Carrie,Carrie)$\notin B$.

On the other hand, the binary relation D on $\mathbb{N}$ **is** reflexive. For any $n \in \mathbb{N}$, $(n, n) \in D$ since $\frac{n}{n} = 1 \in \mathbb{N}$. Notice it would not be reflexive if this were a relation on $\mathbb{Z}$ since $\frac{0}{0} \notin \mathbb{Z}$.

If your binary relation is laid out in a table, then the relation is reflexive if all the entrees on the diagonal are in the relation.

Example 1.4.4: Say whether or not the relations defined in Example 1.4.11 are reflexive and why (or why not).

1. T on $\mathbb{Z}$ defined by

   $$T = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n - m = 10\}$$

   Not reflexive.
   Here no element of the form (n, n) is in T since $n - n = 0 \neq 10$.

2. H on $\mathbb{R}$ defined by

   $$H = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid xy = 1\}$$

   Not reflexive. If we consider $(x, x) \in H$ that means that $x^2 = 1$. But that means $x = \pm 1$. The only elements of the form (x, x) in H are $(1, 1)$ and $(-1, -1)$. For all other x's, $(x, x) \notin H$.

3. M on $\mathbb{Z}$ defined by

   $$M = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n - m = 3k \text{ for some } k \in \mathbb{Z}\}$$

   Reflexive. For any $n \in \mathbb{Z}$, $n - n = 0 = 3(0)$. Here $k = 0$.
   So for all $n \in \mathbb{Z}$, $(n, n) \in M$.

4. P on $\mathbb{R}$ defined by

   $$P = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid xy > 0\}$$

   Not reflexive. $(x, x) \in P \Leftrightarrow x^2 > 0$. This is true for all real numbers **except** 0. Hence $(0, 0) \notin P$, so P is not reflexive. Even one exception makes the relation fail to be reflexive.

5. C on $\mathbb{R}^2$ defined by

   $$C = \left\{((x, y), (z, t)) \in \mathbb{R}^2 \times \mathbb{R}^2 \mid x^2 + y^2 = z^2 + t^2\right\}$$

   Reflexive. $((x, y), (x, y)) \in C \Leftrightarrow x^2 + y^2 = x^2 + y^2$. This is clearly true for any point $(x, y) \in \mathbb{R}^2$.

Definition 1.4.5: A relation R on a set A is *symmetric* if and only if $(a, b) \in R \Rightarrow (b, a) \in R$. That is,

$$R \text{ symmetric} \Leftrightarrow (a, b) \in R \Rightarrow (b, a) \in R$$

In other words a relation is symmetric if whenever a is related to b then b is related to a. Our first relation B from the beginning of the section is **not** symmetric since even though Ann

likes Bob, Bob does not like Ann. That is, (Ann,Bob)$\in B$, but (Bob,Ann)$\notin B$. Symmetry also fails for Bob/Carrie and Carrie/Edgar. Note that symmetry holds for David and Edgar, since both (David,Edgar)$\in B$ and (Edgar,David)$\in B$. Note as well that symmetry holds *vacuously* for pairs like Ann and Carrie. Ann doesn't like Carrie, and Carrie doesn't like Ann. The hypothesis "if (Ann,Carrie)$\in B$" is false, as well as "if (Carrie,Ann)$\in B$" so the implication is *true* in both cases.

The binary relation D is not symmetric either. $(1, 2) \in D$, but $(2, 1) \notin D$. In fact there are no two different integers for which the symmetry condition holds. We'll see shortly that this means that the binary relation D is *antisymmetric*.

Example 1.4.6: Say whether or not the relations defined in Example 1.4.11 are symmetric and why (or why not).

1. T on $\mathbb{Z}$ defined by

   $$T = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n - m = 10\}$$

   Not symmetric. $(10, 0) \in T$, but $(0, 10) \notin T$ since $0 - 10 = -10 \neq 10$.

2. H on $\mathbb{R}$ defined by

   $$H = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid xy = 1\}$$

   Symmetric. For this one let's go ahead and write a formal proof. Since symmetry is equivalent to the implication "$(x, y) \in H \Rightarrow (y, x) \in H$," the "shape" of any symmetry proof will be:

   Let $(x, y) \in H$

   ...do math...do math...

   Therefore $(y, x) \in H$

   So, H is symmetric.

   proof:

Let $(x, y) \in H$	
$\Rightarrow\ xy = 1$	by definition of H
$\Rightarrow\ yx = 1$	property of real numbers
Therefore $(y, x) \in H$	by definition of H $\square$

3. M on $\mathbb{Z}$ defined by

$$M = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n - m = 3k \text{ for some } k \in \mathbb{Z}\}$$

Symmetric.

proof:

Let $(n, m) \in M$	
$\Rightarrow$ $n - m = 3k$ for some $k \in \mathbb{Z}$	by definition of M
$\Rightarrow$ $m - n = -(n - m) = 3(-k)$ where $-k \in \mathbb{Z}$	algebra
Therefore $(m, n) \in M$	by definition of M $\square$

4. P on $\mathbb{R}$ defined by

$$P = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid xy > 0\}$$

Symmetric.

proof:

Let $(x, y) \in P$	
$\Rightarrow$ $xy > 0$	by definition of M
$\Rightarrow$ $yx > 0$	property of real numbers
Therefore $(y, x) \in M$	by definition of M $\square$

5. C on $\mathbb{R}^2$ defined by

$$C = \left\{((x, y), (z, t)) \in \mathbb{R}^2 \times \mathbb{R}^2 \mid x^2 + y^2 = z^2 + t^2\right\}$$

Symmetric.

proof:

Let $((x, y), (z, t)) \in C$	
$\Rightarrow$ $x^2 + y^2 = z^2 + t^2$	by definition of C
$\Rightarrow$ $z^2 + t^2 = x^2 + y^2$	algebra
Therefore $((z, t), (x, y)) \in C$	by definition of C $\square$

The third property we'll consider is *antisymmetry*. The formal definition of this property is a little bit strange, so let me first define it intuitively. A relation is *antisymmetric* if there are no symmetric pairs. Our very first example relation was not symmetric and it is not antisymmetric either. This is because there is one symmetric pair: David/Edgar. As with all of our properties, one exception means the property does **not** hold.

Definition 1.4.7: A relation R is *antisymmetric* if and only if $(x, y) \in R$ and $(y, x) \in R$ implies that $x = y$. That is,

$$R \text{ antisymmetric } \Leftrightarrow (x, y) \in R \wedge (y, x) \in R \Rightarrow x = y$$

Another way to think of this is, "The only pairs in which you can switch the order and remain in the relation are those where the first and second coordinates are the same." For instance, of course you can switch the order of (Ann,Ann) and remain in B. Switching (Ann,Ann) just gives you (Ann,Ann) again. B is not antisymmetric, though, because (David,Edgar)$\in B$ and (Edgar,David)$\in B$ but David$\neq$Edgar.

The relation D, however, *is* antisymmetric. Let's write down a proof. Again since antisymmetry is defined as an implication, the "shape" of the proof for antisymmetry is usually the same.

Let $(x, y) \in R$ and $(y, x) \in R$.

...do math...do math...

Therefore $x = y$

So, D is antisymmetric.

proof: Let $(n, m) \in D$ and $(m, n) \in D$

$\frac{m}{n} = k \in \mathrm{N}$ and $\frac{n}{m} = l \in \mathrm{N}$	by definition of D
$\Rightarrow kl = \frac{m}{n} \cdot \frac{n}{m} = 1$	substitution and simplification
$\Rightarrow k = \frac{1}{l}$	algebra
$l = 1$	property of $\mathbb{N}$
$\Rightarrow \frac{n}{m} = 1$	substitution into earlier line
Therefore $n = m$	algebra

□

Example 1.4.8: From Example 1.4.11(1) prove T is antisymmetric.

proof: Let $(n, m) \in T$ and $(m, n) \in T$

$\Rightarrow n - m = 10$ and $m - n = 10$ by definition of T
$\Rightarrow 10 = n - m = -(m - n) = -10$ algebra and substitution

Since $10 \neq -10$ we conclude that the hypothesis is *never true*. That is, there are no symmetric pairs in T (of the form (x, x) or otherwise).
Hence the statement, "If $(n, m) \in T$ and $(m, n) \in T$ then $n = m$" is *vacuously true*. Therefore T is antisymmetric. □
The logic here is a little contorted, but intuitively it is pretty clear. There are no symmetric pairs in T, so T is antisymmetric.

The other relations in Example 1.4.11 are all symmetric. While it is possible for a relation to be both symmetric and antisymmetric, such relations only have elements of the form (x, x). So none of the other relations in Example 1.4.11 are antisymmetric.

We'll do one more important example of an antisymmetric binary relation.

Example 1.4.9: Let O be a relation on $\mathbb{R}$ defined by

$$O = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$$

It is very easy to prove that O is antisymmetric.
proof: Let $(x, y) \in O$ and $(y, x) \in O$.

$\Rightarrow x \leq y$ and $y \leq x$ by definition of O
Therefore $x = y$ property of $\mathbb{R}$
□

The last property we'll discuss is *transitivity*. In words this is the property that "if a is related to b and b is related to c then a is related to c." Formally,

Definition 1.4.10: A relation R is *transitive* if and only if $(a, b) \in R$ and $(b, c) \in R$ implies that $(a, c) \in R$. That is,

$$R \text{ transitive } \Leftrightarrow (a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$$

Maintaining its perfect record of not having any of the properties we care about, our first relation B is also not transitive. This is because (Ann,Bob)$\in B$ and (Bob,Carrie)$\in B$, but (Ann,Carrie)$\notin B$. There are two other triples that violate transitivity: Bob-Carrie-Edgar, and Carrie-Edgar-David.

Again since it is defined as an implication the "shape" of a proof of transitivity will generally be:

Let $(a, b) \in R$ and $(b, c) \in R$

. . . do math. . . do math. . .

Therefore $(a, c) \in R$

So, D is transitive.

proof: Let $(n, m) \in D$ and $(m, p) \in D$.

$\frac{n}{m} = k \in \mathbb{Z}$ and $\frac{m}{p} = l \in \mathbb{Z}$	definition of D
$\Rightarrow n = mk$ and $m = lp$	algebra
$\Rightarrow n = (lp)k$	substitution
$\Rightarrow \frac{n}{p} = lk \in \mathbb{Z}$	algebra
Therefore $(n, p) \in D$	definition of D

□

Example 1.4.11: For each relation in Example 1.4.11, prove it is transitive or show it is not.

1. T on $\mathbb{Z}$ defined by

   $$T = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n - m = 10\}$$

   Not transitive. $(20, 10) \in T$ and $(10, 0) \in T$, but $(20, 0) \notin T$.

2. H on $\mathbb{R}$ defined by

   $$H = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid xy = 1\}$$

   Not transitive. $(2, \frac{1}{2}) \in H$ and $(\frac{1}{2}, 2) \in H$, but $(2, 2) \notin H$.

3. M on $\mathbb{Z}$ defined by

   $$M = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n - m = 3k \text{ for some } k \in \mathbb{Z}\}$$

   Transitive.

   proof: Let $(n, m) \in M$ and $(m, p) \in M$.

$\Rightarrow n - m = 3k$ and $m - p = 3l$ for $k, l \in \mathbb{Z}$	definition of M
$\Rightarrow n = m + 3k$ and $m = p + 3l$	algebra
$\Rightarrow n = (p + 3l) + 3k$	substitution
$\Rightarrow n - p = 3(l + k)$	algebra
Therefore $(n, p) \in M$	definition of M (noting that $l + k \in \mathbb{Z}$)

   □.

   Notice by the way that we wrote $n - m = 3k$, but $m - p = 3l$. Why not $m - p = 3k$? Well, to be in M, $n - m$ has to be 3 times some integer which we've named k. $m - p$ is also in M, so it is also 3 times some integer, but that integer is generally *different from* k. So we give this other integer a different name, l.

4. P on $\mathbb{R}$ defined by

$$P = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid xy > 0\}$$

Transitive.

proof: Let $(x, y) \in P$ and $(y, z) \in P$.

$\Rightarrow xy > 0$ and $yz > 0$	definition of P
$\Rightarrow (xy) \cdot (yz) > 0$	property of real numbers
$\Rightarrow xy^2z > 0$	algebra
$\Rightarrow xz > 0$	divide by y^2, (note $y^2 > 0$)
Therefore $(x, z) \in P$	definition of P

$\square$.

In the key step we divide by y^2. This leaves the inequality unchanged since $y^2 > 0$. (We know $y \neq 0$ since $xy > 0$.)

5. C on $\mathbb{R}^2$ defined by

$$C = \left\{((x, y), (z, t)) \in \mathbb{R}^2 \times \mathbb{R}^2 \mid x^2 + y^2 = z^2 + t^2\right\}$$

Transitive.

proof: Let $((x, y), (z, t)) \in C$ and $((z, t), (u, v)) \in C$

$x^2 + y^2 = z^2 + t^2$	definition of C
$z^2 + t^2 = u^2 + v^2$	definition of C
$\Rightarrow x^2 + y^2 = u^2 + v^2$	substitution
Therefore $((x, y), (u, v)) \in C$	definition of C

$\square$.

1.4.3 Problems

Problem 1.4.12:
Define a relation R on $S =$ {Ann, Bob, Carrie, David, Edgar} by the table:

	Ann	Bob	Carrie	David	Edgar
Ann	x		x		
Bob		x	x		
Carrie	x	x	x		
David				x	x
Edgar			x		x

Determine if R is reflexive, symmetric, antisymmetric, or transitive. You need not prove it if the property holds, but give a **specific** counterexample if the property does not hold.

Problem 1.4.13: Determine a relation on $S = \{\text{Ann, Bob, Carrie, David, Edgar}\}$ with at least ten pairs that has the properties given below. Present your relation in a table.

(a) Antisymmetric and reflexive, but not transitive.

(b) Transitive, but neither reflexive not symmetric.

(c) Reflexive, symmetric, and transitive.

(d) Reflexive, antisymmetric, and transitive.

Problem 1.4.14: Determine if the relation is reflexive, symmetric, antisymmetric, or transitive. If R has the property, prove it. If R does not have the property, give a **specific** counterexample.

(a) Let R be a relation on $\mathbb{R}^2$ defined by

$$R = \{((x, y), (z, t)) \in \mathbb{R}^2 \times \mathbb{R}^2 \mid x - z = y - t\}$$

(b) Let A by any set. Let R be a relation on 2^A defined by

$$R = \{(B, C) \in 2^A \times 2^A \mid B \cap C = \phi\}$$

1.5 Equivalence Relations

Notation

$\sim$	Equivalent (with respect to some equivalence relation)
$[x]$	the equivalence class containing x
$\widetilde{A}$	the set of equivalence classes on a set A

One of the most important things we do in mathematics is classifying two apparently different mathematical objects as being essentially "the same." By that we mean they differ only in characteristics that we don't care about.

For instance, in a geometry class we'll say that two triangles are "the same" when they are *congruent*. This means that they have the same side lengths and angles. Of course that does not mean they are truly identical. We can take a triangle and turn it upside down or move it across the page or color it red. The new triangle is still congruent to the first triangle because in a geometry class we don't care about things like the orientation of the triangle, its position, or its color. In other contexts we might care about these characteristics, and then we would need a different understanding of what "the same" means.

In a trigonometry class we will often think of two angles as being essentially "the same" if they differ by a multiple of 360°. For instance 90° and 450° are not the same angle. We'd never say they are equal. (Technically we say these angles are *coterminal*.) But they do correspond to the same direction in the plane, and all the trig functions have the same value for either one. So with respect to those applications at least, coterminal angles really are the same.

Formally the way we do this is to define some big set (the set of all triangles or the set of all angles, for example) and define as "related" the elements that we want to say are "the same". A binary relation of this type is called an *equivalence relation*, and to make sense it has to have three of the properties defined in the last section.

> **Definition 1.5.1:** A binary relation R on a set A is called an *equivalence relation* if and only if it is:
>
> 1. Reflexive
> 2. Symmetric
> 3. Transitive
>
> If $(a, b) \in R$ we say that "a is *equivalent* to b with respect to R."
> Usually R is understood from the context so we can just write this as "$a \sim b$."

For some elements $a, b, c \in A$, these properties can be interpreted as:

1. a is the same as a. That is, $a \sim a$.
2. If a is the same as b then b is the same as a. That is,

$$a \sim b \;\Rightarrow\; b \sim a$$

3. If a is the same as b and b is the same as c then a is the same as c. That is,

$$a \sim b \;\wedge\; b \sim c \Rightarrow a \sim c$$

I hope that all three of these properties seem to you necessary for any reasonable conception of "the same."

1.5.1 Examples of Equivalence Relations

Before getting into more technical examples let's consider the following binary relation defined on the set of humans. Let's say that human a is "related" to human b if they have the same parents. Is this an equivalence relation? Well...

1. Does a have the same parents as a? Sure.
2. If a has the same parents as b, does b have the same parents as a? Sure. a and b are siblings.
3. If a has the same parents as b and b has the same parents as c, does a have the same parents as c? Again, sure. a, b and c are all brothers and/or sisters.

So this *is* an equivalence relation. Now let's say we changed it to "a is related to b if they have a parent in common." Is this still an equivalence relation? The answer is no... why not? Which property fails?

It turns out this relation—it's still very much a relation—is no longer *transitive*. For instance, Andy might have the same mother as Brian, while Brian has the same father as Caleb. Andy and Brian are related, Brian and Caleb are also related, but Andy and Caleb might well have no parent in common. Brian is a half brother to both Andy and Caleb, but Andy and Caleb would not be related at all.

Example 1.5.2: Let's return to our set of five students from the previous section, $S = \{\text{Ann, Bob, Carrie, David, Edgar}\}$, and define another relation E between them using a table.

	Ann	Bob	Carrie	David	Edgar
Ann	x		x		
Bob		x		x	x
Carrie	x		x		
David		x		x	x
Edgar		x		x	x

Is E an equivalence relation?

1. The diagonal entrees ((Ann,Ann), (Bob,Bob)...) are all in the relation, so it is *reflexive*.

2. All the off-diagonal entrees are in symmetric pairs (Ann,Carrie)/(Carrie,Ann), (Bob,David)/(David,Bob), etc. Therefore E is *symmetric*.

3. It's harder to see the transitive triples. There are none with Ann and Carrie. There are several with Bob, David, and Edgar, but they are all there. For instance (Bob,David) and (David,Edgar) are in E. Transitivity requires (Bob,Edgar) to be in E... and it is. After checking all the triples we conclude that E is *transitive*.

Therefore E *is* an equivalence relation.

Looking back to Example 1.4.11 in the previous section, we see there are two more relations that satisfy Definition 1.5.1.

Example 1.5.3: From Example 1.4.11(3), M on $\mathbb{Z}$ defined by

$$M = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n - m = 3k \text{ for some } k \in \mathbb{Z}\}$$

We proved that M is reflexive, symmetric, and transitive. Hence M is an equivalence relation. According to M, for instance, $7 \sim 1$ and $5 \sim 17$.
This might seem at first a strange and arbitrary conception of "the same." It turns out to be very important. Another way to look as this is two integers are "the same" if they have the same remainder when divided by 3. Later we'll talk about how two numbers are *congruent modulo* 3.

Example 1.5.4: From Example 1.4.11(5), C on $\mathbb{R}^2$ defined by

$$C = \left\{((x, y), (z, t)) \in \mathbb{R}^2 \times \mathbb{R}^2 \mid x^2 + y^2 = z^2 + t^2\right\}$$

We proved that C is reflexive, symmetric, and transitive. Hence C is an equivalence relation. According to C, for instance, $(3, 4) \sim (0, -5)$ and $(-1, \sqrt{3}) \sim (\sqrt{2}, \sqrt{2})$.
This conception of "the same" can be interpreted pretty easily as "two points in the plane are the same (with respect to C) if they are the same distance from the origin." This is clear once you remember that the distance from a point (x, y) to the origin is $\sqrt{x^2 + y^2}$.

1.5.2 Equivalence Classes

When we have an equivalence relation several elements of the set are somehow "the same" and should be treated as one thing. A collection of elements all equivalent to one another is called an *equivalence class*.

Definition 1.5.5: Given an equivalence relation on a set A, the *equivalence class* of $a \in A$, "[a]" is the set of elements which are equivalent to a. That is,

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

Example 1.5.6: For each element and equivalence relation write down the equivalence class.

1. Bob $\in S$ with respect to E.
2. $5 \in \mathbb{Z}$ with respect to M.
3. $(3, 4) \in \mathbb{R}^2$ with respect to C.

1. Bob $\in S$ with respect to E.

   $$[\text{Bob}] = \{\text{Bob}, \text{David}, \text{Edgar}\}$$

   It's easy to see this. Just look at what 'x's there are in Bob's row in the table.

2. $5 \in \mathbb{Z}$ with respect to M.

   What does it mean for $x \sim 5$? Well it means that $x - 5 = 3k$ for some integer k. Thus x is of the form $x = 5 + 3k$. For $k = 0, x = 5$. For $k = 1, x = 8$. For $k = -1, x = 2$, etc. You get a different x for each different value of k. Therefore [5] has an infinite number of elements in it.

   $$[5] = \{\ldots -4, -1, 2, 5, 8, 11 \ldots\}$$

3. $(3, 4) \in \mathbb{R}^2$ with respect to C.

   If $(x, y) \sim (3, 4)$ then $x^2 + y^2 = 3^2 + 4^2 = 25$. Thus,

   $$[(3, 4)] = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 25\}$$

   The points in the plane which satisfy this equation are those on the circle of radius 5, centered at the origin.

Now that we know what an individual equivalence class is, we need to define the set of **all** equivalence classes for some equivalence relation.

Definition 1.5.7: Given an equivalence relation R on some set A, the set of all equivalence class is called A *modulo* R, "$\widetilde{A}$"

$$\widetilde{A} = \{B \in 2^A \mid B \text{ is an equivalence class}\}$$

Since equivalence classes are *sets*, $\widetilde{A}$ is a *set of sets*.

Example 1.5.8: Write down the set of all equivalence classes for each equivalence relation.

1. E on S.

   $$\widetilde{S} = \{\ \{\text{Ann}, \text{Carrie}\}, \{\text{Bob}, \text{Dave}, \text{Edgar}\}\ \}$$

   According to E there are two equivalence classes in S. In this case it looks like they are "the girls" and "the boys."

2. M on $\mathbb{Z}$.

   We saw in Example 1.5.6 that the equivalence class of 5 is an infinite set consisting of all the integers of the form $5 + 3k$ where k is any integer. What are the other equivalence classes? If we take any other number in [5] we'll just get the same set back again. (You can check that, for instance $2 + 3k$ produces that same set of numbers. If we take another number, say 0, we find

   $$[0] = \{n \in \mathbb{Z} \mid n = 0 + 3k,\ k \in \mathbb{Z}\} = \{\ldots -6, -3, 0, 3, 6, 9 \ldots\}$$

   which is different set. This is another equivalence class. Now if we find a number that isn't already in [5] or [0], say 1, we find

   $$[1] = \{n \in \mathbb{Z} \mid n = 1 + 3k,\ k \in \mathbb{Z}\} = \{\ldots -5, -2, 1, 4, 7, 10 \ldots\}$$

   All the numbers in $\mathbb{Z}$ belong to one of these three sets. So, even though there are an infinite number of numbers in $\mathbb{Z}$ there are only *three* equivalence classes.

   $$\widetilde{\mathbb{Z}} = \{\ \{\ldots -4, -1, 2, 5, 8, 11 \ldots\}, \{\ldots -6, -3, 0, 3, 6, 9 \ldots\}, \{\ldots -5, -2, 1, 4, 7, 10 \ldots\}\ \}$$

3. C on $\mathbb{R}^2$.

   We saw in Example 1.5.6 that the equivalence class of $(3, 4)$ was just all the points on the circle that are the same distance from the origin as $(3, 4)$. The reasoning is the same for an arbitrary point $(a, b) \in \mathbb{R}^2$. If we let $r = \sqrt{a^2 + b^2}$ then

   $$[(a, b)] = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = r^2\}$$

   The set of all equivalence classes, then, is just the set of all circles with center at the origin, together with a one point equivalence class, $\{(0, 0)\}$.

Notice that each element appears in *exactly* one equivalence class. Each student is in S is either in the "boy" equivalence class or the "girl" equivalence class, and no student is in both. Each integer in $\mathbb{Z}$ is in [5], [0], or [1], and no number is in two of them. Each point in $\mathbb{R}^2$ is on one and only one circle centered at the origin, **except** the origin—which has its own one-point equivalence class.

When some large set is decomposed into a set of subsets, this set of subsets is called a *partition* of the set.

Definition 1.5.9: A *partition* of a set A, is a set of subsets of A, $\{B_1, B_2, \ldots\}$, so that

1. The union of all the subsets gives you the big set. That is,

$$\bigcup_i B_i = A$$

2. There are no points in more than one of the subsets. That is,

$$\forall i, j \quad B_i \cap B_j = \phi$$

We say the sets are *disjoint*.

It is a fact that any equivalence relation on a set A, the set of equivalence classes form a partition of A. We'll state this as a theorem, but omit the proof. (The proof actually isn't very hard. It just uses the three properties of equivalence relations.)

Theorem 1.5.10: For any equivalence relation R on A, $\widetilde{A}$ forms a partition of A.

1.5.3 Problems

Problem 1.5.11: Let M_5 be the relation on $\mathbb{Z}$ defined by

$$M_5 = \{(n, m) \in \mathbb{Z} \mid n - m = 5k \text{ for some } k \in \mathbb{Z}\}$$

(a) Prove M_5 is an equivalence relation.

(b) Write down the set of equivalence classes, $\widetilde{M_5}$.

Problem 1.5.12: Define an equivalence relation on S by

	Ann	Bob	Carrie	David	Edgar
Ann	x				x
Bob		x		x	
Carrie			x		
David		x		x	
Edgar	x				x

What are the equivalence classes?

Problem 1.5.13: Given the $Z = \{1, 2, 3, 4\}$, let R be an equivalence relation on 2^Z defined by

$$A \sim B \Leftrightarrow A \text{ and } B \text{ have the same number of elements}$$

(a) List all the elements of $[\{2, 3\}]$

(b) List one element from each equivalence class.

Problem 1.5.14: Define an equivalence relation V on $\mathbb{R}^2$ by

$$(x, y) \sim (z, t) \Leftrightarrow x = az, y = at \text{ for some } a \in \mathbb{R}, a > 0$$

So for instance, $(2, 3) \sim (10, 15)$ since $2 = \frac{1}{5} \cdot 10$ and $3 = \frac{1}{5} \cdot 15$. Here $a = \frac{1}{5}$.

(a) Prove V is an equivalence relation.

(b) Describe in words and sketch in $\mathbb{R}^2$ the equivalence class $[(2, 3)]$.

(c) Describe in words and sketches $\widetilde{\mathbb{R}}$ (the set of all equivalence classes of V). Don't forget the one equivalence class that doesn't look like any of the others.

1.6 Partial Orders

Notation

$\leq$	less than or equal to (as real numbers)
$\preceq$	less than or equal to (with respect to some partial ordering)
$\not\preceq$	not less than or equal to (with respect to some partial ordering)

Now we want to talk about "ordering" a set. That is we want to define in a consistent way the idea of one element in a set being "smaller" or "bigger" than another element. Again this is a type of binary relation. To be a *partial order* this relation must satisfy three properties.

> **Definition 1.6.1:** A relation R on a set A is a *partial order* if and only if R is
>
> 1. Reflexive
> 2. Antisymmetric
> 3. Transitive
>
> If $(a, b) \in R$, we write $a \preceq b$.

We should read "$a \preceq b$" as a is less than or equal to b *in some sense*. a and b may not be numbers. Even if they are numbers, a partial order might be completely different from the natural ordering you get from numbers. With this in mind let's look again at the properties that a partial order must satisfy.

1. a is less than **or equal** to a.

   $$a \preceq a$$

2. The only way a can be less than or equal to b **and** b less than or equal to a is if $a = b$.

   $$a \preceq b \ \wedge \ b \preceq a \Rightarrow a = b$$

3. If a is less than or equal to b and b is less than or equal to c then it should be that a is less than or equal to c.

   $$a \preceq b \ \wedge \ b \preceq c \Rightarrow a \preceq c$$

Again I hope you agree with me that these are all necessary for a reasonable conception of order.

1.6.1 Examples of Partial Orders

We have already seen two partial orders in Section 1.4, D and O.

Example 1.6.2: Recall that the relation D is defined as

$$D = \left\{(n, m) \in \mathbb{N} \times \mathbb{N} \mid \frac{m}{n} \in \mathbb{N}\right\}$$

We proved before that D is reflexive, antisymmetric, and transitive, so it is a partial order. According to this partial order, $2 \preceq 6$ (since $\frac{6}{2} = 3 \in \mathbb{N}$) and $3 \preceq 6$ (since $\frac{6}{3} = 2 \in \mathbb{N}$), so you might think this order is not different from the natural order on $\mathbb{N}$. This is false, though, because $2 \not\preceq 3$. Neither, more reassuringly, is $3 \not\preceq 2$. According to D, 2 and 3 are *incomparable*.

Definition 1.6.3: If R is a partial order on A, we say $a, b \in A$ are *incomparable* if a is not less than or equal to b **and** b is not less than or equal to a. That is,

$$a, b \in A \text{ incomparable } \Leftrightarrow\ a \not\preceq b\ \wedge\ b \not\preceq a$$

You may have been wondering what the "partial" in partial ordering was about. It refers to the idea that you may not be able to impose a meaningful conception of order on every single pair of elements. Thus you have only "partially" ordered the set. Now if there are no incomparable elements we say the set is **totally ordered**.

Definition 1.6.4: A partial order R on A is called a *total order* if and only if for every $a, b \in A$, $a \preceq b$ **or** $b \preceq a$. That is,

$$R \text{ total order } \Leftrightarrow\ \forall a, b \in A, a \preceq b\ \vee\ b \preceq a$$

Example 1.6.5: Recall that the relation O on $\mathbb{R}$ is defined as

$$O = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$$

We proved earlier that O is antisymmetric. It is easy to see that it is reflexive ($\forall x \in \mathbb{R}, x \leq x$) and transitive ($x \leq y$ and $y \leq z \Rightarrow x \leq z$). Thus O is a partial order. In fact for every pair of real numbers, x, y either $x \leq y$ or $y \leq x$. Hence O is a *total order*.

Let's return again to our set of students, S. This time we'll relate them to each other according to their math ability. (Uh-oh!)

Example 1.6.6: Define a binary relation, G as follows. Say Ann is better at math than Carrie, David, and Edgar, but not as good as Bob (who is better than everybody). Carrie is better than David, and we'll make the obvious statement that everyone is as good at math as themselves. Write this relation in a table, and determine if it is a partial order (or a total order).

	Ann	Bob	Carrie	David	Edgar
Ann	x	x			
Bob		x			
Carrie	x	x	x		
David	x	x	x	x	
Edgar	x	x			x

The diagonal is there so it's reflexive. There are no symmetric pairs (the only pair above the diagonal is (Ann,Bob), but (Bob,Ann) is not in the relation), so it is antisymmetric. There are several transitive triples, but they all work (e.g. David$\preceq$Carrie and Carrie$\preceq$Ann and, fortunately, David$\preceq$Ann), so it is transitive. Thus this *is* a partial order.

It is **not** a total order because Carrie and Edgar are incomparable... as are David and Edgar.

Example 1.6.7: Let $A = \{a, b, c\}$, and consider the power set, (see definition 1.3.11)

$$2^A = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Define a relation on 2^A by

$$I = \{(B, C) \in 2^A \times 2^A \mid B \subseteq C\}$$

1. Prove I is a partial order on 2^A.
2. Show I is not a total order on 2^A.

1. proof:
   (a) For any $B \in 2^A$, $B \subseteq B$, so $(B, B) \in I$. Therefore I is reflexive.
   (b) Let $B \subseteq C$ and $C \subseteq B$. Then, by the definition of set equality (definition 1.3.5) $B = C$. Hence I is antisymmetric.
   (c) Let $B \subseteq C$ and $C \subseteq D$. By problem 1.3.30, $B \subseteq D$. Thus I is transitive.

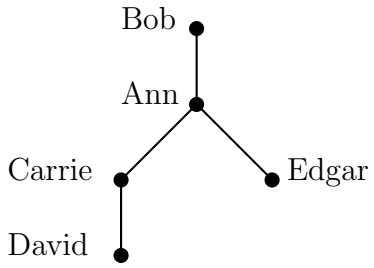
   As I is reflexive, antisymmetric, and transitive, I is a partial order. $\square$
2. $\{a, b\} \nsubseteq \{a, c\}$ and $\{a, c\} \nsubseteq \{a, b\}$. Thus $\{a, b\}$ and $\{a, c\}$ are incomparable with respect to I. Therefore I is not a total order.

1.6.2 Hasse Diagrams

One way to represent a partial order graphically is with a *Hasse diagram*.

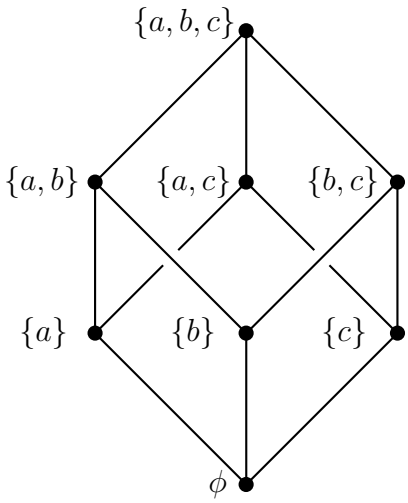
Definition 1.6.8: Given a partial order R on a set A, a *Hasse* diagram is a set of partially connected dots, where each dot represents an element in the set. One element b will appear higher than another a if $a \preceq b$. There will be a line connecting a and b if and only if there is **no element** c such that $a \preceq c$ and $c \preceq b$. That is, there is a line connecting a and b only if there is no c *between* them.

Example 1.6.9: Draw a Hasse diagram for the partial order G in Example 1.6.6.



Notice that we don't need to draw a line from Bob to Carrie or David because Ann is between them. Similarly for Ann and David, Carrie is between them. We could have drawn Edgar lower if we'd wanted to... we don't know what his math ability is compared to Carrie or David.

Example 1.6.10: Draw a Hasse diagram for the partial order I in Example 1.6.7.



Again there is no need to draw a line from $\{a, b, c\}$ to $\{a\}$ since $\{a, b\}$ is between them.

$$\{a\} \subseteq \{a, b\} \subseteq \{a, b, c\}$$

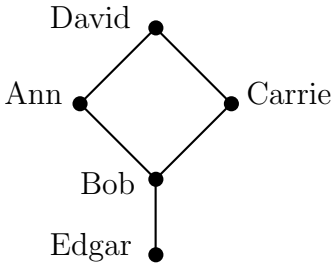
1.6.3 Problems

Problem 1.6.11: Define a partial order on S by

	Ann	Bob	Carrie	David	Edgar
Ann	x	x	x		
Bob		x	x		
Carrie			x		
David			x	x	
Edgar			x	x	x

Draw the Hasse diagram for this partial order.

Problem 1.6.12: Present in a table the partial order described by the Hasse diagram.



Problem 1.6.13: Let R be the partial order on $\mathbb{N}$ defined by

$$n \preceq m \;\Leftrightarrow\; m = 2^k n \text{ for some } k \in \mathbb{Z}, k \geq 0\}$$

(a) Prove R is a partial order.

(b) Draw the Hasse diagram for the elements $\{1,\ 2,\ \ldots 12\}$ using this partial order.

Problem 1.6.14: Let R be the partial order on $\mathbb{R}^2$ defined by

$$(x, y) \preceq (z, t) \;\Leftrightarrow\; x \leq z \text{ and } x + y \leq z + t$$

(a) Prove R is a partial order.

(b) Is R a total order? How do you know?

1.7 Functions

Notation

$\exists!$	There exists a unique
$F : X \to Y$	function F from set X to set Y
Domain(F)	domain of the function F
Range(F)	range of the function F

Most students who end up in a class like this one are already very familiar with the idea of a function. Not being content to leave well enough alone, though, we're going to define and work with functions in the context of what we've already learned about statements, sets, and relations.

First let's expand our definition of a binary relation. Before we defined it intuitively as something that establishes a "relationship" between some of the points of a single set A. Now we want to define it as something which establishes a relationship between points in *two different sets* X and Y. The new definition will be the same as the old definition if we let $X = Y$.

Definition 1.7.1: A *binary relation* F *from* a set X *to* a set Y is just a subset of the Cartesian product of X and Y. That is,

$$F \subseteq X \times Y$$

Example 1.7.2: Let's define a binary relation from a set of sports teams to a set of colors.

$$\text{Team} = \{\text{Lakers}, \text{Ducks}, \text{Trojans}, \text{Cardinal}, \text{Dodgers}, \text{Owls}\}$$

$$\text{Color} = \{\text{Purple}, \text{Gold}, \text{Green}, \text{Blue}, \text{Red}\}$$

Each team has one or two traditional colors so we can define a relation. Each element in the relation will be an ordered pair with the first coordinate a team and the second a color. For instance, the LA Lakers' traditional colors are purple and gold. Thus two elements of the relation (let's call it TC) are (Lakers, Purple) and (Lakers, Gold). All together a reasonable definition of TC might be:

TC = { (Lakers, Purple), (Lakers, Gold), (Ducks, Green), (Ducks, Gold), (Trojans, Gold), (Trojans, Red), (Cardinal, Red), (Dodgers, Blue), (Owls, Blue), (Owls, Gold) }

We can express this relation in a table as we did in previous sections.

	Purple	Gold	Green	Blue	Red
Lakers	x	x			
Ducks		x	x		
Trojans		x			x
Cardinal					x
Dodgers				x	
Owls		x		x	

Sometimes for these types of relations, though, we'll put the first coordinates (teams) across the bottom and the second coordinate (colors) on the left.

	Lakers	Ducks	Trojans	Cardinal	Dodgers	Owls
Purple	x					
Gold	x	x	x			x
Green		x				
Blue					x	x
Red			x	x		

As with the binary relations we defined earlier on a set, these binary relations need more structure to be really useful.

Definition 1.7.3: A binary relation F from X to Y is called a *function* if and only if for every $x \in X$ there is a unique $y \in Y$ so that $(x, y) \in F$. That is,

$$\text{F } \textit{function} \Leftrightarrow \forall x \in X, \exists!\ y \in Y, \ni (x, y) \in F$$

This is written:

$$F : X \to Y$$

The set X is called the *domain* of the function F, written Domain(F). The set Y is called the *Codomain* of F.
A pair $(x, y) \in F$ is more often written $F(x) = y$.

The key point in this definition is the word *unique*. That means there is **exactly one** y for any given x. (The '!' after $\exists$ means "unique.") The relation defined in Example 1.7.2 is **not** a function since there are **two** colors (Purple and Gold) for one team (Lakers). That is, two y's for one x.

Example 1.7.4: Let's define a new relation from the set "Team" above to the set "Number $= \{0, 1, 2, 3\}$."

$$\text{TN} = \{\ (\text{Lakers}, 2),\ (\text{Trojans}, 2),\ (\text{Ducks}, 2),\ (\text{Dodgers}, 1),\ (\text{Cardinal}, 1),\ (\text{Owls}, 2)\ \}$$

Is this relation a function?

Yes. You might have been fooled by the fact that there are four different teams for the number '2'. That means that there is not a unique x for each y... but that is not the condition required for a relation to be a function. What is required is that there be a single y for each x. That is, a single number for each team. If we present the relation in a table, then this requirement corresponds to the requirement that there be exactly one entry in each column.

	Lakers	Ducks	Trojans	Cardinal	Dodgers	Owls
3						
2	x	x	x			x
1				x	x	
0						

For this relation this is clearly the case, so it is a function. For the earlier relation it is clearly not, so it is not a function.

You might also have noticed that there are elements in "Numbers" which correspond to no element in "Teams." No team has 3 colors, for instance. That does not stand in the way of this relation being a function (as opposed if there were a team with no number—not even zero—then it would not be a function). The set of elements in the second set which *do* appear in at least one pair in the function is called the *range*.

Definition 1.7.5: Given a function $F : X \to Y$, the *range* of F is the set $\text{Range}(F) \subseteq Y$ which consists of elements y for which there is an element $x \in X$ satisfying $(x, y) \in F$. That is,

$$\text{Range}(F) = \{y \in Y \mid \exists x \in X \ \ni \ (x, y) \in F\}$$

In other words, the *range*, R, is the set of elements in Y which are "hit" by some element $x \in X$.

For the function above in Example 1.7.4, the range is $\{1, 2\}$.

Example 1.7.6: For the relations given below, determine if they are functions. If so, give the range. For these exercises let A be the set of letters in the alphabet.

1.

$$f = \{(\alpha, x) \in A \times \{0, 1\} \mid \alpha \text{ is a vowel and } x = 0, \textbf{ or } \alpha \text{ is a consonant and } x = 1\}$$

2.

$$F = \{(t^2, t^3) \in \mathbb{R} \times \mathbb{R} \mid t \in \mathbb{R}\}$$

3.

$$F = \{(t^2, t^4) \in \mathbb{R} \times \mathbb{R} \mid t \in \mathbb{R}\}$$

4.

$$F = \left\{ \left(x, \frac{1}{x} \right) \in \mathbb{R} \times \mathbb{R} \mid x \in \mathbb{R} \right\}$$

5.

$$G = \{(t^3, t^2) \in \mathbb{R} \times \mathbb{R} \mid t \in \mathbb{R}\}$$

6.

$$H = \{(B, n) \in 2^A \times \mathbb{Z} \mid n = \#\text{ of letters in } B\}$$

1.

$$f = \{(\alpha, x) \in A \times \{0, 1\} \mid \alpha \text{ is a vowel}, x = 0, \text{ or } \alpha \text{ is a consonant}, x = 1\}$$

It depends on what you do with the letter 'y'. If 'y' is both a consonant and a vowel, then $(y, 0) \in f$ and $(y, 1) \in f$. In that case f would not be a function. For the purposes of this class, however, let's define 'y' as a consonant. Then f *is* a function, and $\text{Range}(f) = \{0, 1\}$.

2.

$$F = \{(t^2, t^3) \in \mathbb{R} \times \mathbb{R} \mid t \in \mathbb{R}\}$$

Not a function. $t = 2 \Rightarrow (4, 8) \in F$, and $t = -2 \Rightarrow (4, -8) \in F$. Thus, F has two y values (8 and -8) for a single x value (4).

3.

$$F = \{(t^2, t^4) \in \mathbb{R} \times \mathbb{R} \mid t \in \mathbb{R}\}$$

Not a function. ...at least not a function $F : \mathbb{R} \to \mathbb{R}$. That's because there are no pairs for the negative x's. If we *restrict the domain* to $[0, \infty)$ then F will be a function. That is,

$$F = \{(t^2, t^4) \in [0, \infty) \times \mathbb{R} \mid t \in \mathbb{R}\}$$

is a function.

4.

$$F = \left\{ \left(x, \frac{1}{x} \right) \in \mathbb{R} \times \mathbb{R} \mid x \in \mathbb{R} \right\}$$

Not a function. Again, F is not defined for every $x \in \mathbb{R}$. In particular, there is no pair of the form (0,?). If we *restrict the domain* to $\mathbb{R} \setminus \{0\}$, then F is a function.

5.

$$G = \{(t^3, t^2) \in \mathbb{R} \times \mathbb{R} \mid t \in \mathbb{R}\}$$

Function. Here if $x = t^3$ then for a given x there is only one t, $t = \sqrt[3]{x}$. Thus there's only one possible y, $y = \sqrt[3]{x^2}$. For any possible x, $y \geq 0 \Rightarrow \text{Range}(G) = [0, \infty)$.

6.

$$H = \{(B, n) \in 2^A \times \mathbb{Z} \mid n = \#\text{ of letters in } B\}$$

Function. The domain of this function is a little strange, but any $B \in 2^A$ is a subset of A. Therefore it has some single, finite number of letters in it, e.g. $H(\{j, m, n, w\}) = 4$. Since there are only 26 letters, $\text{Range}(H) = \{0,\ 1,\ 2,\ 3,\ \ldots\ 25,\ 26\}$.

1.7.1 Bijections

Obviously functions are incredibly important and useful binary relations. Nevertheless sometimes we want to impose yet more structure on them. There are two more properties that we'll find useful.

Definition 1.7.7: A function $F : X \to Y$ is *onto* if and only if $\text{Range}(F) = Y$. That is,

$$F \text{ onto } \Leftrightarrow \forall y \in Y,\ \exists\, x \in X \ni F(x) = y$$

In other words F is onto if every $y \in Y$ is hit by some $x \in X$.

Definition 1.7.8: A function $F : X \to Y$ is *one-to-one* if and only if for any $y \in \text{Range}(F)$ there is **only one** $x \in X$ so that $y = F(x)$. That is,

$$F \text{ one to one } \Leftrightarrow \forall y \in \text{Range}(F),\ \exists!\, x \in X \ni F(x) = y$$

In other words F is one-to-one if every $y \in \text{Range}(F)$ is hit by **no more than one** $x \in X$.

Another way to say F is one-to-one is with the implication: $F(x_1) = F(x_2) \Rightarrow x_1 = x_2$. You can read this as "If F is taking two points x_1 and x_2 to the same y, then x_1 and x_2 must be the same point." We will use this implication whenever we are trying to prove a function is one-to-one.

Example 1.7.9: Let $F : \mathbb{Z} \to \mathbb{Z}$, defined by

$$F = \{(n, 2n + 1) \in \mathbb{Z} \times \mathbb{Z} \mid n \in \mathbb{Z}\}$$

More commonly this definition will be written: $F(n) = 2n + 1,\ n \in \mathbb{Z}$.
Is F onto? Is F one-to-one?

F is not onto. To show this, set F equal to some element in $\mathbb{Z}$ and show that there is no $n \in \mathbb{Z}$ which gives you that element. That is,

$$\begin{aligned} F(n) &= 2 \\ 2n+1 &= 2 \\ \Rightarrow n &= \tfrac{1}{2} \notin \mathbb{Z} \end{aligned}$$

Thus the only n which produces $F(n) = 2$ is not in the domain of F. Hence $2 \notin \text{Range}(F)$ and so F is not onto. In fact, if you think about it for a second, Range(F) is just the set of **odd** integers.

F is one-to-one. This requires a proof. As with all the other proofs we've done in this class, the "shape" of a one-to-one proof is always the same.

Let $F(x_1) = F(x_2)$
...do math...do math...
Therefore $x_1 = x_2$

So, proof that F is one-to-one:

Let $F(n_1) = F(n_2)$
$\Rightarrow$ $2n_1 + 1 = 2n_2 + 1$ Definition of F
$\Rightarrow$ $2n_1 = 2n_2$ Algebra
Therefore $n_1 = n_2$ Algebra
Hence F is one-to-one. $\square$

Example 1.7.10: Let $F : \mathbb{R} \to \mathbb{R}$ defined by $F(x) = 2x + 1$. So this looks like the same function as Example 1.7.9 above, except for the fact that the domain of F is now defined to be $\mathbb{R}$ rather than $\mathbb{Z}$.
Is F now onto? Is F still one-to-one?

F is now onto. The "shape" of an onto proof is spiritually just "Pick a y. Find the x that hits the y. Done."
Somewhat more formally,

Let $F(x) = y \in$Codomain of F
...do math...do math...
Therefore $x \in$ Domain of F

Proof that F is onto:

Let $F(x) = y \in \mathbb{R}$
$\Rightarrow$ $2x + 1 = y$ Definition of F

$\Rightarrow$ $x = \frac{y-1}{2}$ Algebra

Therefore $x \in \mathbb{R}$ Properties of $\mathbb{R}$
Hence F is onto. $\square$

F is still one-to-one. The proof is exactly the same as the proof given in Example 1.7.9 above. That proof only used definitions and algebra properties that hold for both $\mathbb{Z}$ and $\mathbb{R}$.

Why doesn't the proof we just gave for the onto-ness of F work for the onto-ness of Example 1.7.9? It is a property of a real number that you may divide it by two and get another real number. That is not true for integers!

So we've just shown that, as a function on the real numbers, $F(x) = 2x + 1$ is both onto and one-to-one. Such functions are called *bijections.*

Definition 1.7.11: A function F which is onto is also said to be a *surjection.* A function F which is one-to-one is also said to be an *injection.* If F is both a *surjection* and an *injection* then we say F is a *bijection.*

Example 1.7.12: Let $g : A \to \{1,\ 2, \ldots 25,\ 26\}$ where A is the set of letters in the alphabet. Define g by $g(\alpha) =$ place of the letter α in the alphabet. For example $g(a) = 1$ and $g(j) = 10$.
Is g a bijection?

Clearly g is onto since there are 26 letters so each integer from 1 to 26 corresponds to a letter.

Similarly g is one-to-one since if $g(\alpha) = g(\beta) = n$, then both $\alpha = \beta =$ the n-th letter in the alphabet. For instance, if $g(\alpha) = g(\beta) = 3$ then we know $\alpha = \beta =$ the letter 'c'.

Since g is both onto (surjective) and one-to-one (injective) it is a bijection.

Example 1.7.13: Let $M : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $M(m, n) = mn$. So the domain of M is *pairs* of integers. The action of M is just multiplication. For example, $M(4, 3) = 12$.
Is M onto? Is M one-to-one?

M is onto.
proof: Let $p \in \mathbb{Z}$. Then $(p, 1) \in \mathbb{Z} \times \mathbb{Z}$ and $M(p, 1) = p$. Hence M is onto. $\square$.

M is not one-to-one. $M(4, 3) = 12$ and $M(6, 2) = 12$. So, $M(4, 3) = M(6, 2)$ yet $(4, 3) \neq (6, 2)$. Thus M is not one-to-one. (This is the negation of the implication: "If $M(m_1, n_1) = M(m_2, n_2)$ then $(m_1, n_1) = (m_2, n_2)$.")

Since M is not one-to-one it is **not** a bijection.

Example 1.7.14: Let $L : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $L(m, n) = 9m + 12n$.
So for example, $L(2, 3) = 18 + 36 = 54$.
Is L onto? Is L one-to-one?

L is not onto. Let $p \in \mathbb{Z}$ and $L(n, m) = p$. Then,

$$\begin{aligned} 9m + 12n &= p \\ 3(3m + 4n) &= p \\ 3m + 4n &= \tfrac{p}{3} \end{aligned}$$

$3m + 4n \in \mathbb{Z}$ for any integers m and n, but $\frac{p}{3} \notin \mathbb{Z}$ unless p is a multiple of 3. So we know L only produces integers which are multiples of three. For instance there are no integers m, n so that $L(m, n) = 7$. Thus L is not onto.

L is not one-to-one. Again just notice that:
$L(-1, 2) = 3 = L(3, -2)$, yet $(-1, 2) \neq (3, -2)$. Hence L is not one-to-one.

Example 1.7.15: Define $f : \mathbb{Z} \to \mathbb{Z}$ by

$$f(x) = x^2 + 14x - 51$$

Is f onto? Is f one-to-one?

Hopefully you recall that if the graph of f would be a parabola—if its domain were $\mathbb{R}$. It's actually $\mathbb{Z}$, but we would still not expect f to be either onto or one-to-one. But that observation is not a proof.

f is not onto. Let $f(x) = y \in \mathbb{Z}$.

$x^2 + 14x - 51 = y$ definition of f

$\Rightarrow x^2 + 14x - 51 - y = 0$ algebra

$\Rightarrow x = \frac{-14 \pm \sqrt{14^2 - 4(-51-y)}}{2}$ quadratic formula

$\Rightarrow x = \frac{-14 \pm \sqrt{400+4y}}{2}$ simplification

If $y < -100$ then $x \notin \mathbb{Z}$ since $y < -100 \Rightarrow \sqrt{400 + 4y}$ is **complex**

Thus f is not onto. In fact Range$(f) = [-100, \infty)$.

f is not one-to-one. Let $f(x_1) = f(x_2)$.

$x_1^2 + 14x_1 - 51 = x_2^2 + 14x_2 - 51$ definition of f

$\Rightarrow x_1^2 - x_2^2 + 14x_1 - 14x_2 = 0$ algebra

$\Rightarrow (x_1 - x_2)(x_1 + x_2) + 14(x_1 - x_2) = 0$ algebra

$\Rightarrow (x_1 - x_2)(x_1 + x_2 + 14) = 0$ factor out $(x_1 - x_2)$

So if $(x_1 - x_2) = 0$ then $x_1 = x_2$ and f would be one-to-one. Unfortunately it's also possible for $x_1 + x_2 + 14 = 0$. So if $x_1 = -8$ and $x_2 = -6$ we see that $f(-8) = -99 = f(-6)$. Since $-8 \neq -6$ f is **not** one-to-one.

Note, by the way, that if we restrict the domain to $(-7, \infty)$ then $x_1, x_2 > -7$ and $x_1 + x_2 + 14 > 0$. Then $x_1 - x_2 = 0$ and f *is* one-to-one.

Both of these statements were examples of how *trying to prove something is true* can show you how it is *actually false*.

1.7.2 Cardinality

What do we mean when we say that two sets are the "same size"? Well, if they are finite sets that's easy—they are the same size if they have the same number of elements. If the sets are infinite, however, it's a much harder question to answer. You might think that all infinite sets are the same size, "infinitely big." We'll see, though, that there really are different sizes of infinity. The idea that captures the "size" of a set is its *cardinality*.

> **Definition 1.7.16:** Two sets A and B have the same *cardinality*, written $|A| = |B|$, if there is a bijection f from A to B. That is,
>
> $$|A| = |B| \;\Leftrightarrow\; \exists f : A \to B,\ f \text{ bijection}$$

First let's think of this definition in terms of *finite* sets.

> **Example 1.7.17:** Show that the set $A = \{a, b, c, d, e\}$ has the same cardinality as the set $B = \{0, 2, 4, 6, 8\}$. That is
>
> $$|\{a, b, c, d, e\}| = |\{0, 2, 4, 6, 8\}|$$

We need a bijection, $f : \{a, b, c, d, e\} \to \{0, 2, 4, 6, 8\}$. There are many choices, but one possibility is:

$$f = \{(a, 4),\ (b, 8),\ (c, 0),\ (d, 6),\ (e, 2)\}$$

Intuitively this makes all kinds of sense. The two sets clearly have five elements, so they have the same size. It's worth considering why

$$|\{a, b, c, d, e\}| \neq |\{0, 2, 4, 6, 8, 10\}|$$

Intuitively, there are five elements in the first set and six in the second, so they have different cardinality. But how does that jive with our definition of cardinality? Consider a function $g : \{a, b, c, d, e\} \to \{0, 2, 4, 6, 8, 10\}$. Could g be a bijection? No. Since g is a function there is only one element from the codomain for each element in the domain. Therefore only five things are "hit" by g. There are six things in the codomain, so g will inevitably miss one of them. Hence g cannot be *onto*.

Similarly, there cannot be a bijection the other way $h : \{0, 2, 4, 6, 8, 10\} \to \{a, b, c, d, e\}$. The first five elements in $\{0, 2, 4, 6, 8, 10\}$ could go to different letters, but the sixth would have to hit one of the letters already hit by a previous number. Therefore h could not be *one-to-one*.

It's pretty easy to see that *finite* sets have the same cardinality if and only if they have the same number of elements. The beauty of this definition of cardinality is that you can get a handle on the size of *infinite* sets. Then some strange things happen.

Theorem 1.7.18: The cardinality of the integers is the same as the cardinality of the *even integers*. That is,

$$|\mathbb{Z}| = |\{2n \mid n \in \mathbb{Z}\}|$$

proof: We need a bijection $f : \mathbb{Z} \to \{2n \mid n \in \mathbb{Z}\}$. It's easy enough to find one. Let $f(m) = 2m$.

To show f is onto let $y \in \{2n \mid n \in \mathbb{Z}\}$. By definition $y = 2n$ for some integer n. Then $f(n) = 2n = y$. Hence f is onto.

To show f is one-to-one let $f(n_1) = f(n_2)$. Then $2n_1 = 2n_2 \Rightarrow n_1 = n_2$. Hence f is one-to-one.

Thus f is a bijection, and the two sets have the same cardinality. $\square$.

So this result is a little weird because the even integers are a strict subset of the integers. You would think that would mean there were "fewer" even integers. Yet, paradoxically, the two sets are the same "size"—at least in the sense of their cardinality. The following example is similar. Despite the fact that the natural numbers $\mathbb{N}$ are a strict subset of the integers $\mathbb{Z}$, we'll see they have the same cardinality.

Example 1.7.19: Show $|\mathbb{N}| = |\mathbb{Z}|$

We need a bijection $f : \mathbb{N} \to \mathbb{Z}$. Again there are many choices. Constructing one just requires a little ingenuity.

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \\ -\frac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

Plugging in some numbers we see that $f(2) = 1,\ f(4) = 2,\ f(6) = 3 \ldots$. Thus the even naturals are sent to the positive integers. Simlarly, $f(1) = 0,\ f(3) = -1,\ f(5) = -2 \ldots$. Thus the odd naturals are sent to the negative integers (and zero).

So much for the intuition, but now we need a formal proof. First that f is onto.

proof: Let $f(n) = m \in \mathbb{Z}$.

The proof now has to proceed *in cases* (we saw an example of this way back in section 1.3).

Case 1: $m > 0$

$\Rightarrow \frac{n}{2} = m$ definition of f

Therefore $n = 2m \in \mathbb{N}$. algebra and recalling that $m > 0$ (and an integer).

Case 2: $m \leq 0$

$\Rightarrow -\frac{n-1}{2} = m$ definition of f

Therefore $n = 1 - 2m \in \mathbb{N}$. algebra and recalling that $m \leq 0$ (and an integer).

In either case $n \in \mathbb{N}$, so f is onto.

We also need to prove that f is one-to-one.
proof: Let $f(n_1) = f(n_2) = m$.

Again the proof proceeds in cases.

Case 1: $m > 0$

$\Rightarrow \frac{n_1}{2} = \frac{n_2}{2}$ definition of f

Therefore $n_1 = n_2$. algebra

Case 2: $m \leq 0$

$\Rightarrow -\frac{n_1-1}{2} = -\frac{n_2-1}{2}$ definition of f

$\Rightarrow n_1 - 1 = n_2 - 1$ algebra

Therefore $n_1 = n_2$. algebra

In either case $n_1 = n_2$, so f is one-to-one.

Thus f is a bijection. $\square$

Ok so far all our examples of infinite sets have proven to have the same cardinality. Such sets are said to be *countable*.

> **Definition 1.7.20:** A set A is *countable* or *countably infinite* if and only if $|\mathbb{N}| = |A|$.

This definition is a little silly since we can't actually *count* a set like the integers. It is, after all, infinite. The idea, though, is that you could count them if you had an infinite time to do so. Well, you might ask, isn't that true of *any* set? The answer to that is, surprisingly, **'no'**. You cannot, for instance, *count* the real numbers.

> **Theorem 1.7.21:** The real numbers are not countable. That is, $|\mathbb{N}| \neq |\mathbb{R}|$.

The proof is just a little beyond the scope of this course, but you can show that there is no **onto** function $g : \mathbb{N} \to \mathbb{R}$. In some really freaky-cool way there are just "more" real numbers than there are natural numbers (or integers or any of the other countable sets).

Now you might not find this fact all that strange once you think about it. In some sense the real numbers give you "solid" intervals while countable sets like the integers are represented by a bunch of isolated points. But then along comes the following fact:

> **Theorem 1.7.22:** The rational numbers are countable. That is, $|\mathbb{N}| = |\mathbb{Q}|$.

Recall that the rational numbers $\mathbb{Q}$ is the set of all fractions. It is a fact that there are infinitely many rational numbers in any interval you might choose, no matter how small. There are infinitely many rational numbers in the interval $(1, 1.00000001)$ for instance. A former student of mine described them as "infinitely dense" just like the real numbers. Yet they are still countable. Freaky.

The formal proof is once again a little beyond the scope of this course, but the idea is fairly straight-forward. First list 0. Then list all the rational numbers with a 1 or less in the numerator and denominator. There are only two: 1, -1. Then list all the rational numbers with a 2 or less in the numerator and denominator. If we omit $\frac{2}{2}$ (which we've already listed) there are four: $\pm 2, \pm\frac{1}{2}$. Proceeding this way you'll construct an infinite list which would have all possible rational numbers in it.

$$\mathbb{Q} = \left\{0,\ \pm 1,\ \pm 2,\ \pm\frac{1}{2},\ \pm 3,\ \pm\frac{3}{2},\ \pm\frac{1}{3},\ \pm\frac{2}{3},\ \pm 4,\ \pm\frac{4}{3}\ldots\right\}$$

Our bijection $f : \mathbb{N} \to \mathbb{Q}$ would have $f(1) = 0,\ f(2) = 1,\ f(3) = -1,\ f(4) = 2 \ldots f(11) = -\frac{3}{2}\ldots$

While this argument is not a proof, I hope you can see how it is possible to construct a bijection from $\mathbb{N}$ to $\mathbb{Q}$ in this way.

Back to stuff I might actually test you on!

> **Example 1.7.23:** Show that the open interval $(0, 1)$ has the same cardinality as the set of positive real numbers. That is, $|(0, 1)| = |(0, \infty)|$.

We need a bijection $f : (0, 1) \to (0, \infty)$. One possibility might be

$$f(x) = \frac{1}{x} - 1$$

f is onto.
proof: Let $f(x) = y \in (0, \infty)$.

$\frac{1}{x} - 1 = y$	definition of f
$\Rightarrow x = \frac{1}{y+1}$	algebra
$\frac{1}{y+1} > 0$	since $y > 0$ (and using properties of real numbers)
$\frac{1}{y+1} < 1$	since $y + 1 > 1$ (and using properties of real numbers)
Hence $x \in (0, 1)$	applying the previous three statements

So f is onto.

f is one-to-one.
proof: Let $f(x_1) = f(x_2)$.

$\frac{1}{x_1} - 1 = \frac{1}{x_2} - 1$	definition of f
$\Rightarrow \frac{1}{x_1} = \frac{1}{x_2}$	algebra
Hence $x_1 = x_2$	algebra

So f is one-to-one. Hence f is a bijection. $\square$

1.7.3 Problems

Problem 1.7.24: Is the set $\{(t^3 - t, t^2) \in \mathbb{R}^2 \mid t \in \mathbb{R}\}$ a function? Explain why or why not.

Problem 1.7.25: Often we will define a function *in pieces*.
Let $S = \{1, 2, 3, 4, 5\}$ and consider the function $f : S \to \mathbb{Z}$ defined below.

$$f(x) = \begin{cases} x^2 + 1 & \text{if } x \text{ even} \\ 2x - 5 & \text{if } x \text{ odd} \end{cases}$$

(a) Express f in a table.

(b) What is the range of f?

(c) Is f one-to-one?

Problem 1.7.26: Let $X = \{a, b\}$ and $Y = \{1, 2, 3\}$.

(a) List all the possible **onto** functions $f : X \to Y$ and $g : Y \to X$.

(b) List all the possible **one-to-one** functions $f : X \to Y$ and $g : Y \to X$.

Problem 1.7.27: Prove that the function $f : \mathbb{Z} \to \mathbb{R}$ defined by

$$f(x) = x^2 + \sqrt{5}x - 13$$

is one-to-one.

Problem 1.7.28: Prove that the set of integers divisible by 3 has the same cardinality as the even integers. That is,

$$|\{\ldots -6,\ -3,\ 0,\ 3,\ 6,\ 9\ldots\}| = |\{\ldots -4,\ -2,\ 0,\ 2,\ 4,\ 6\ldots\}|$$

Problem 1.7.29: Show that the cardinality of the interval $(0, 1)$ is the same as the cardinality of the interval $(-1, 2)$. That is prove: $|(0, 1)| = |(-1, 2)|$.

Chapter 2

Number Theory

2.1 Divisibility

Notation

$m \mid n$	m divides evenly into n
$m \nmid n$	m does not divide evenly into n

2.1.1 Division Algorithm

One of the big differences between the integers and sets like the rational or real numbers is that, while you may add, subtract, or multiply integers and get integers you cannot in general *divide* integers and get other integers. The best you can do when you divide is get a *quotient* and a *remainder*. The fact that you can do that, and precisely what you mean by that, is included in a theorem called the *Division Algorithm*. It's a bit of a misnomer because it's not really an algorithm. It doesn't tell you *how* to calculate the quotient and the remainder—just that they exist. (In this it's like a lot of cool-but-frustrating mathematics.)

Theorem 2.1.1: (Division Algorithm) Let $a, b \in \mathbb{Z}, b \neq 0$. Then there exist unique integers q and r such that $a = qb + r$, where $0 \leq r < |b|$.
q is called the *quotient*, and r the remainder.

Example 2.1.2: Find the q and r and write $a = qb + r$, given the values a and b below:

1. $a = 23$, $b = 5$.
2. $a = 37$, $b = 11$.
3. $a = 373723$, $b = 111$.

1. $23 = (4)5 + 3$. Here $q = 4$ is the quotient and $r = 3$ the remainder. Note that $r \geq 0$ and $r < 5$.

2. $37 = (3)11 + 4$. $q = 3,\ r = 4$.

3. $373723 = (3366)111 + 97$. $q = 3366,\ r = 97$. Again note that $r < 111$.

Keep in mind the requirement that r be a nonnegative number. It does not matter if we divide by a positive or a negative integer, we want the remainder to always be nonnegative!

> **Example 2.1.3:** Find the quotient q and remainder r as defined in the Division Algorithm (in particular, note that the remainder r is always defined as a positive number).
>
> 1. $a = 23$, $b = -5$.
>
> 2. $a = -37$, $b = 11$.
>
> 3. $a = -112$, $b = -13$.
>
> 4. $a = -2097$, $b = 41$.

1. $23 = (-4) \cdot (-5) + 3$. Note $r = 3 < |-5|$ as required by the theorem.

2. $-37 = (-4) \cdot 11 + 7$.

3. $-112 = 9 \cdot (-13) + 5$

4. $-2097 = (-52) \cdot 41 + 35$

So with the help of a hand calculator it is simple to implement the Division Algorithm. It's worth pointing out, though, that the Division Algorithm is a theorem rather than an axiom that you assume is true. That is, it's something that you would have to prove. We won't write down a formal proof, but the idea is this: For natural numbers a and $b \neq 0$ let S be the set:

$$S = \{a - bk \in \mathbb{N} \mid k \in \mathbb{Z}\}$$

While S is an infinite set, S has a smallest element which is the remainder, r. The value of k that produces that r is the quotient q. By the way, the assumption that any set of natural numbers has a smallest element *is* an axiom—called the *Well-Ordering Principle*.

Once you've proven the Division Algorithm for natural numbers it's not difficult to generalize it to the integers.

While not particularly deep, the Division Algorithm is quite useful in proving facts that are not quite so "obvious."

Example 2.1.4: Let a be any integer. Prove that there exists an integer k such that $a^2 = 5k$, $a^2 = 5k + 1$, or $a^2 = 5k + 4$.

Before getting into the proof, let's convince ourselves that the statement is correct. Let $a = 4$. Then $a^2 = 16 = 5(3) + 1$, so that works with $k = 3$. Let $a = 20$. Then $a^2 = 400 = 5(80)$, so that works too.

What's ruled out? Well, apparently it's not possible for $a^2 = 5k + 2$ or $5k + 3$. That is, if we list the numbers of the form $5k + 2$ *none of them* will be perfect squares. Looking at the first couple we see that's so: $2,\ 7,\ 12,\ 17,\ 22 \ldots$. Similarly there are no perfect squares of the form $5k + 3 :\ 3,\ 8,\ 13,\ 18,\ 23 \ldots$. Once you think about it for a while it's kind of a surprising result. On to the proof.

proof:

$a = 5q + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < 5$.	Division Algorithm
$a^2 = 25q^2 + 10qr + r^2$	algebra
$a^2 = 5(5q^2 + 2qr) + r^2$	algebra

Now we have five cases for the five possible values for r. Remember $r = 0, 1, 2, 3,$ or 4.

Case 1: $r = 0$. Then $a^2 = 5(5q^2)$. So $a^2 = 5k$ where $k = 5q^2$.

Case 2: $r = 1$. Then $a^2 = 5(5q^2 + 2q) + 1$. So $a^2 = 5k + 1$ where $k = 5q^2 + 2q$.

Case 3: $r = 2$. Then $a^2 = 5(5q^2 + 4q) + 4$. So $a^2 = 5k + 4$ where $k = 5q^2 + 4q$.

Case 4: $r = 3$. Then $a^2 = 5(5q^2 + 6q) + 9 = 5(5q^2 + 6q + 1) + 4$.
So $a^2 = 5k + 4$ where $k = 5q^2 + 6q + 1$.

Case 5: $r = 4$. Then $a^2 = 5(5q^2 + 8q) + 16 = 5(5q^2 + 8q + 3) + 1$.
So $a^2 = 5k + 1$ where $k = 5q^2 + 8q + 3$.

So in all cases $a^2 = 5k,\ 5k + 1,$ or $5k + 4$. □

2.1.2 Factors and GCD

Sometimes when we apply the Division Algorithm to integers a and b we obtain a remainder of zero. This means b "divides evenly" into a, or simply b *divides* a.

Definition 2.1.5: Let a, b be integers. We say that b *divides* a, written $b|a$, if and only if $a = qb$ for some integer q. That is,

$$b|a \ \Leftrightarrow\ \exists q \in \mathbb{Z} \ \ni \ a = qb$$

b is then called a *divisor* or a *factor* of a.

We give a few examples just so you see this is just what you think it is.

Example 2.1.6:

1. $3|18$ since $18 = (6) \cdot 3$. Here $q = 6$.
2. $-15|60$ since $60 = (4) \cdot (-15)$.
3. $4|(-100)$ since $-100 = (-25) \cdot 4$.

There are a few other things to notice about this definition. The first thing is that 1 divides any integer n, since $n = n \cdot 1$ (here $q = n$). So $1|n$ for any $n \in \mathbb{Z}$.

Next any integer n divides 0, since $0 = 0 \cdot n$ (here $n = b$ and $q = 0$). So we can write $n|0$. On the other hand, $a = q \cdot 0$ only if $a = 0$. So 0 is not a divisor for any integer *except* 0.

Example 2.1.7: State whether the following statements are *true* or *false*. If true, write a quick proof. If false, give a concrete counterexample.

1. If $a|b$ and $b|c$ then $a|c$.
2. If $a|b$ and $a|c$ then $a|bc$.
3. If $a|c$ and $b|c$ then $ab|c$.

1. If $a|b$ and $b|c$ then $a|c$.

   True. proof:

$b = ka$ for some $k \in \mathbb{Z}$.	Definition of $a\|b$
$c = lb$ for some $l \in \mathbb{Z}$.	Definition of $b\|c$
$\Rightarrow c = l(ka) = (lk)a$,	substitution
Therefore $a\|c$	definition of $\|$ where $q = lk \in \mathbb{Z}$ $\square$

2. If $a|b$ and $a|c$ then $a|bc$.

   True. proof:

$b = ka$ for some $k \in \mathbb{Z}$.	Definition of $a\|b$
$c = la$ for some $l \in \mathbb{Z}$.	Definition of $a\|c$
$\Rightarrow bc = (ka)(la) = (kla)a$,	substitution
Therefore $a\|bc$	definition of $\|$ where $q = kla \in \mathbb{Z}$ $\square$

3. If $a|c$ and $b|c$ then $ab|c$.

   False. $6|12$ and $4|12$, but $24 \nmid 12$.

An important fact about divisibility is that if you take two numbers that are divisible by a third, then any linear combination of the two will also be divisible by the third. For instance, $3|15$ and $3|21$. It's a fact that we will prove in a moment that 3 will divide $15k+21l$ for any $k, l \in \mathbb{Z}$. So if $k = 3$ and $l = 2$ then $15k + 21l = 45 + 42 = 87$. And $3|87$ (since $87 = (29) \cdot 3$) just as it's supposed to.

Theorem 2.1.8: If $n|a$ and $n|b$ then for any $k, l \in \mathbb{Z}$, $n|(ka + lb)$.

Proof:

$a = rn$ for $r \in \mathbb{Z}$	Definition of $n\|a$
$b = sn$ for $s \in \mathbb{Z}$	Definition of $n\|b$
$ka + lb = k(rn) + l(sn) = (kr + ls)n$	substitution and factoring
Therefore $n\|(ka + lb)$	Definition of $\| \ \square$

Definition 2.1.9: Given any two integers a, b (not both zero), we say that g is the *greatest common divisor* of a and b, written $\gcd(a, b)$, if and only if g is the largest integer such that $g|a$ and $g|b$.

Later in this chapter we will describe and use a fast, efficient way of calculating the gcd called the *Euclidean Algorithm*. For the moment, though, let's find a gcd using only the definition.

Example 2.1.10: Find $\gcd(18, 27)$.

Make a list of all the *divisors* of 18. Make another list for 27.

divisors of 18: 1, 2, 3, 6, 9, 18
divisors of 27: 1, 3, 9, 27

The largest number that appears in both lists is 9. Therefore $\gcd(18, 27) = 9$.

Here are a few others, just to make sure you've got the idea.

Example 2.1.11: Find the greatest common divisor for the following pairs of a and b.

1. $a = 26, b = 14$
2. $a = 52, b = 80$
3. $a = -196, b = -32$
4. $a = 1573, b = -169$
5. $a = -89, b = -97$

1. $\gcd(26, 14) = 2$
2. $\gcd(52, 80) = 4$
3. $\gcd(-196, -32) = 4$
4. $\gcd(1573, -169) = 13$
5. $\gcd(-89, -97) = 1$

Note that since 1 is a divisor of any number, the gcd of any two numbers is always *at least* 1. If they have no other common divisors then we say they are *relatively prime*.

> **Definition 2.1.12:** a and b are called *relatively prime* if and only if $\gcd(a, b) = 1$.

Thus from Example 2.1.11, we see that -87 and -97 are relatively prime.

We have one more theorem that will be critical to our use of the *Euclidean Algorithm* later in the chapter.

> **Theorem 2.1.13:** Let a, b, q, r be integers such that $a = qb + r$.
> Then $\gcd(a, b) = \gcd(b, r)$.

Consider the following example: $a = 52, b = 10$. This theorem says that since $52 = 5(10) + 2$, then $\gcd(52, 10) = \gcd(10, 2) = 2$. Which is, of course, true.

The proof is a little tricky. It's straight forward to prove something is a common divisor of two numbers, but not so easy to prove that it is the *greatest* common divisor. The logic of the proof is this: We'll prove first that $\gcd(b, r) \leq \gcd(a, b)$. Then we'll prove the opposite inequality, $\gcd(a, b) \leq \gcd(b, r)$. Thus the two must be equal.

proof: Let $g = \gcd(a, b)$ and $h = \gcd(b, r)$.

$h\|b$ and $h\|r$	Definition of gcd
$h\|(qb + r)$	Theorem 2.1.8 with $k = q$ and $l = 1$
$h\|a$	Since $a = qb + r$
$\Rightarrow h$ is a common divisor of a and b	since h divides both a and b
Therefore $h \leq g$	since g is the *greatest* common divisor of a and b

Conversely,

$g\|a$ and $g\|b$	Definition of gcd
$g\|(a - qb)$	Theorem 2.1.8 with $k = 1$ and $l = -q$
$g\|r$	Since $r = a - qb$
$\Rightarrow g$ is a common divisor of b and r	since g divides both b and r
Therefore $g \leq h$	since h is the *greatest* common divisor of b and r

Since we have both $h \leq g$ and $g \leq h$, it must be that $h = g$. □

2.1.3 Irrationality of $\sqrt{2}$

I want to finish this section with one of the greatest mathematical discoveries of the ancient world. The Greeks took it as an article of faith that all numbers could be written as a ratio of integers. The idea that there could be some other type of number was, to them, just *irrational*. Imagine their shock, then, when it was proven that the length of the diagonal of a square with sides of length one *could not be written as a fraction*. Stated another way,

> **Theorem 2.1.14:**
>
> $$\sqrt{2} \neq \frac{p}{q} \quad \text{for any } p, q \in \mathbb{Z}$$

There is a (probably apocryphal) story that the young mathematician who proved this fact so upset his colleagues that they tied a rock to his leg and dropped him into the Mediterranean Sea!

We're going to write down the proof of this theorem, but first we need another theorem that we'll use in the proof. (Such "small theorems" used in the proof of a "more important" theorem are often called *lemmas*.)

Theorem 2.1.15: For any $a \in \mathbb{Z}$, if $2|a^2$ then $2|a$.

It's pretty easy to convince yourself that this is true. $2|36 = 6^2$ and $2|6$. $2|64 = 8^2$ and $2|8$. But like so many things in number theory, it's not so easy to see how to write a formal proof. Well, you'll get the chance to try in Problem 2.1.20. Let's assume you'll succeed and move on to the big proof.

Proof of Theorem 2.1.14: This will be a *proof by contradiction*. That is, we'll assume the theorem is false, and derive from that assumption a statement which is false. We then conclude that the original theorem must be true.

So, if the theorem is false then there exist $p, q \in \mathbb{Z}$ so that $\sqrt{2} = \frac{p}{q}$.

We may assume that either p or q is odd since if they were both even we could cancel factors of two until we arrived at smaller integers, at least one of which is odd. (Really this statement deserves its own lemma, but I'm going to let it pass.)

$\frac{p^2}{q^2} = 2$	Algebra
$\Rightarrow p^2 = 2q^2$	Algebra
$\Rightarrow 2\|p^2$	Definition of |
$\Rightarrow 2\|p$	Theorem 2.1.15

So p is even

But if p is even then $p = 2n$ for some $n \in \mathbb{Z}$. So

$\frac{(2n)^2}{q^2} = 2$	substitution
$\Rightarrow 4n^2 = 2q^2$	Algebra
$\Rightarrow q^2 = 2n^2$	Algebra
$\Rightarrow 2\|q^2$	Definition of |
$\Rightarrow 2\|q$	Theorem 2.1.15

So q is even as well

But this is a contradiction of the fact that either p or q had to be odd. Hence it must not be possible to write $\sqrt{2} = \frac{p}{q}$. $\square$

2.1.4 Problems

Problem 2.1.16: Let a be any integer. Prove that there exists an integer k such that $a^2 = 7k$, $a^2 = 7k + 1$, $a^2 = 7k + 2$, or $a^2 = 7k + 4$.
(Your proof should have *seven* cases.)

Problem 2.1.17: Let a, b be two integers such that $a = qn+r$ and $b = pn+r$, where n, q, p, r are integers (in other words, a and b have the same remainder upon division by n).
Prove that $a - b$ is divisible by n.

Problem 2.1.18: Prove that given any two consecutive integers a and $a+1$, one of them is divisible by 2.

Warning You can't just wave your hands with an argument like:
"Odd numbers and even numbers alternate so if you take two in a row one of them is even. There I proved it."
Intuitively that's correct, but it's not a proof. Apply the Division Algorithm to a and 2, and write a short proof with two cases.

Problem 2.1.19: Use Theorem 2.1.13 to prove that $2^{100} + 1$ and $2^{100} + 3$ are relatively prime.

Problem 2.1.20: We're going to prove Theorem 2.1.15:

For any $a \in \mathbb{Z}$, if $2|a^2$ then $2|a$.

(a) It turns out it's easier to prove the *contrapositive* of this theorem. Recall from Theorem 1.2.18 that the contrapositive is logically equivalent to the original implication. So, first write down the contrapositive to Theorem 2.1.15.

(b) Now prove the theorem by proving its contrapositive. Start by applying the Division Algorithm to a and 2.

2.2 Primes

Prime numbers have long fascinated people. You can unearth a large number of various entries regarding primes by simply just searching the web. Here we will focus on few basics about primes, with the understanding that this is a rich and still researched field of Number Theory. Following the divisibility definitions developed so far, one can easily recognise the primes as the building blocks behind the factorization of integers.

> **Definition 2.2.1:** A natural number $p \geq 2$ is called *prime* if and only if the only natural numbers that divide p are 1 and p.
> A natural number $n \geq 2$ that is not prime will be referred to as a *composite* number.

Some prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47. 10 and 322 are examples of composite numbers.

See if you can find (on Wikipedia or a similar site) the largest known (computed) prime number (and when it was discovered). Here are two large primes discovered so far:

$$2^{2,976,221} - 1$$

$$2^{24,036,583} - 1.$$

Of course, how would you check that these are in fact prime? Both of the exponents that appear are also prime - can you check at least that?... As you can tell, this business of finding primes is not cheap (both literally and figuratively speaking). There are quite a few people out there who are simply obsessed with primes, and luckily there are also a lot of people who are very interested in primes, so the whole thing is quite lucrative overall... Primes are key to encryption codes, hence there are a lot for parties (banks, credit card companies, etc) interested in working with large primes.

2.2.1 Some Theorems on Primes

So how big do primes get? How many primes are there? This question was answered by the Greeks over 2300 years ago.

> **Theorem 2.2.2:** There are infinitely many primes.

Proof: This is a classic proof by contradiction. Say there were only a *finite* number of primes, $\{2,\ 3,\ 5 \ldots p_N\}$. Here p_N is the N-th and "last" prime number. Let M be the product of all N primes, $M = 2 \cdot 3 \cdot 5 \cdots p_{N-1} \cdot p_N + 1$. Now apply the Division Algorithm to M and $M + 1$.

$$(M+1) = (1)M + 1$$

$\Rightarrow \gcd(M+1, M) = \gcd(M, 1)$	By Theorem 2.1.13 ($q = 1$)
$\gcd(M, 1) = 1$	$\gcd(n, 1) = 1$ for any $n \in \mathbb{N}$
$\Rightarrow \gcd(M+1, M) = 1$	substitution

Hence $M + 1$ is not divisible by any of the N primes. Thus $M + 1$ is either a prime or divisible by a prime not on the list. This is a contradiction to the assumption that there were only the N primes. Therefore there are not N primes for any $N \in \mathbb{N}$, which is means there are an infinite number of primes. $\square$

> **Theorem 2.2.3:** If a natural number $n > 1$ is not prime, then n is divisible by some prime number $p \leq \sqrt{n}$.

So for example $n = 21$ is not prime, and by this theorem should be divisible by a prime p that is less than or equal to $\sqrt{21} \approx 4.58$. Clearly, 21 is divisible by 3, and $3 < 4.58$.

This works in our favor in other way. When we try to check that a number n is prime, we only need to check that n is not divisible by any of the primes that are less than $\sqrt{n}$. So for example, if we wanted to check that $2,976,221$ is prime, we need only check if any primes less than $\sqrt{2,976,221} \approx 1725.2$ are divisors of $2,976,221$. This is a considerably easier task than to check than all the primes smaller than $2,976,221$.

You probably learned at some point that any natural number $n \geq 2$ can be written as a product of prime numbers. If we allow grouping of primes, then any n can be written as

$$n = p_1^{q_1} p_2^{q_2} \cdots p_k^{q_k}$$

where $p_1, p_2, \ldots, p_k$ are all distinct prime numbers. So for example, $1960 = 2^3 \cdot 5 \cdot 7^2$.

> **Theorem 2.2.4:** Let a, b be two integers such that $p \mid ab$, where p is prime. Then $p \mid a$ or $p \mid b$.

We'll prove theorem 2.2.4 in the next section. This result is key in proving that the prime factorization of any natural number n (as given above) is *unique*. The uniqueness of a number's prime factorization is so important that you probably already know it from some earlier course, but perhaps didn't know it by its proper name, "the Fundamental Theorem of Arithmetic."

The prime factors (or the prime divisors) of an integer $n \geq 2$ are the prime numbers that divide n. The *multiplicity* of each prime is the largest number q such that $p^q \mid n$. The factorization of a natural number n into its factors, with their corresponding multiplicities, is unique.

2.2.2 Sieve of Eratosthenes and the Prime Number Theorem

An algorithm for finding primes is the Sieve of Eratosthenes. This algorithm can generate (in time) all the primes less than or equal to a given natural number n. So let's consider the steps:

- list all integers from 2 to n
- circle 2 and then cross out all the multiples of 2 from the list
- circle 3 and cross out all the multiples of 3 from the list

- continue this process, such that at the general stage, you circle the first number that is neither crossed out nor circled, and cross out all its multiples
- continue until all numbers less than or equal to $\sqrt{n}$ have been circled or crossed out

At the end of this process, all the integers left behind are primes smaller than or equal to n. This is the Sieve of Eratosthenes.

> **Example 2.2.5:** Use the Sieve of Eratosthenes to find all primes less than or equal to 35.

List the integers from 2 to 35.

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35$$

2 is prime, so remove all subsequent multiples of 2.

$$2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35$$

3 is prime, remove all subsequent multiples of 3.

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35$$

5 is prime, remove all subsequent multiples of 5. In this list the only remaining numbers are 25 and 35.

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$$

$\sqrt{35} \approx 5.92$ so the only possible prime factors of composite integers less than or equal to 35 are 2, 3, or 5. Since we've checked all those, the remaining numbers are prime.

Perhaps the most interesting result about primes is the Prime Number Theorem. This theorem explains how many primes there are less than a certain number. For instance, how many primes are there less than or equal to 5? This is simple enough because we can count them, there are 3. But what happens as we look at a very large number n, like, say 10^{100}?

To understand this, mathematicians introduced a function $\pi(x)$ which takes as input a natural number x, and assigns as output the number of primes less than or equal to x. So $\pi(5) = 3,\ \pi(7) = 4,\ \pi(8) = 4,\ \pi(9) = 4$, etc.

> **Theorem 2.2.6:** (Prime Number) Let $\pi(x)$ denote the number of primes $p \leq x$. Then as x becomes very large ($x \to \infty$), the function $\pi(x)$ approaches the ratio $\frac{x}{\ln x}$. In other words
>
> $$\lim_{x\to\infty} \frac{\pi(x)}{\left(\frac{x}{\ln x}\right)} = 1 \quad \Rightarrow \quad \pi(x) \approx \frac{x}{\ln x} \text{ (for large } x)$$

In example 2.2.5 we found all the primes less than 35. There were eleven, so $\pi(35) = 11$. Now the estimate given by the Prime Number theorem is

$$\pi(35) \approx \frac{35}{\ln(35)} \approx 9.8$$

which is pretty close.

2.2.3 Some Interesting Types of Primes

In the world of primes, there are some types of primes that are "famous." Mersenne primes are primes of the form $2^p - 1$. Now it turns out that the exponent p must itself be prime or $2^p - 1$ is necessarily composite (we'll see why in a moment). However p prime does *not* guarantee that $2^p - 1$ is prime. For instance, $2^{61} - 1$ is prime, but $2^{257} - 1$ is not prime (even though 257 is prime). So when we call a prime a Mersenne prime, it must be both prime and of the form $2^p - 1$. There are algorithms for checking whether a number is prime, and it turns out that these work particularly well for numbers of the form $2^p - 1$. Because of that, most of the largest know primes are Mersenne primes. It is still an open problem whether there are infinitely many Mersenne primes.

Example 2.2.7: Is $2^{15} - 1$ prime?

$2^{15} - 1$ is not prime, since $15 = 3 \cdot 5$ is not prime. In particular,

$$2^{15} - 1 = (2^3 - 1) \cdot (2^{12} + 2^9 + 2^6 + 2^3 + 1) = 7 \cdot 4681$$

If you multiply out the right hand side you can see the "telescoping effect" where all the intermediate terms cancel out. (e.g. $2^3 \cdot 2^9$ cancels with $(-1) \cdot 2^{12}$.) Similarly,

$$2^{15} - 1 = (2^5 - 1) \cdot (2^{10} + 2^5 + 1) = 31 \cdot 1057$$

So both factors of 15 can be used to generate factors of $2^{15} - 1$.

The Fermat primes are prime numbers of the form $2^{2^n} + 1$. For $n = 0, 1, 2, 3, 4$ these are in fact prime, but $2^{2^5} + 1$ is not prime. To this day, there have been no other Fermat primes discovered... but there are still lots of people with super-computers looking for one!

2.2.4 Problems

Problem 2.2.8: Find the prime decomposition of each of the following:

(a) 856

(b) 9970

(c) 9833

(d) 2323

Problem 2.2.9:

(a) Use the Sieve of Eratosthenes to find all primes less than 200. (This is a nice little programming exercise, if you are so inclined.)

(b) Use theorem 2.2.6 to estimate $\pi(200)$ and see how your results compare.

Problem 2.2.10: Estimate the number of primes less than 6000, less than 60000, less than 600000 and less than 6000000.

Problem 2.2.11:

(a) Is $2^4 + 1$ a Fermat prime?

(b) Is $2^4 - 1$ a Mersenne prime?

(c) Is $2^5 - 1$ a Mersenne prime?

Problem 2.2.12: $2^{91} - 1$ not prime. Explain how you know and produce some factors.

2.3 Euclid

Notation

$\gcd(a, b)$	greatest common divisor of $a, b \in \mathbb{Z}$
$\text{lcm}[a, b]$	least common multiple of $a, b \in \mathbb{Z}$

2.3.1 Calculating the GCD

Our method for calculating the gcd is called *Euclid's Algorithm*. We begin by applying the Division Algorithm, dividing the larger number by the smaller. Next we apply the Division Algorithm again, dividing the smaller number by the remainder. Similarly we continue by dividing the first remainder by the second, the second by the third and so on. Since each remainder is nonnegative and strictly less than the last, eventually the remainder will be zero. The last non-zero remainder turns out to be the gcd.

Finding the $\gcd(98, 42)$ requires only two divisions.

$$\begin{aligned} 98 &= 2 \cdot 42 + 14 \\ 42 &= 3 \cdot 14 + 0 \end{aligned}$$

The last (and only) nonzero remainder is 14, hence $\gcd(98, 42) = 14$.

Euclid's Algorithm may, however, require many divisions. For instance to find $\gcd(111, 69)$

$$\begin{aligned} 111 &= 1 \cdot 69 + 42 \\ 69 &= 1 \cdot 42 + 27 \\ 42 &= 1 \cdot 27 + 15 \\ 27 &= 1 \cdot 15 + 12 \\ 15 &= 1 \cdot 12 + 3 \\ 12 &= 4 \cdot 3 + 0 \end{aligned}$$

Hence $\gcd(111, 69) = 3$.

Why does Euclid's Algorithm work? It is a consequence of Theorem 2.1.13. Applying the theorem to each line of Euclid's Algorithm gives the following string of equalities.

$$\gcd(111, 69) = \gcd(69, 42) = \gcd(42, 27) = \gcd(27, 15) = \gcd(15, 12) = \gcd(12, 3) = \gcd(3, 0)$$

For any integer $n | n$ and $n | 0$, so $\gcd(n, 0) = n$. In particular $\gcd(3, 0) = 3$.

2.3.2 Euclid's Theorem

If Euclid's Algorithm were only a fast way of calculating a gcd, it would not be particularly important. In fact, though, it is key to finding *integer* solutions to equations of the form $ax + by = c$ where $a, b, c \in \mathbb{Z}$.

For instance $17k + 25l = 1$ has infinitely many integer solutions, including $k = 3, l = -2$. On the other hand $21x + 56y = 2$ has no integer solutions at all. How do we know if there are solutions, and if there are how do we find them? The first step is the following theorem.

Theorem 2.3.1: (Euclid)
If $a, b \in \mathbb{N}$
Then There are integers k and l so that:

$$ka + lb = \gcd(a, b)$$

In particular, if a and b are relatively prime then there are integers k and l so that: $ak + bl = 1$

To find k and l we just have to use the equations generated from calculating the gcd via Euclid's Algorithm. For 98 and 42 it is very simple—we need only solve for 14 (the gcd) from our application of the Division Algorithm. Thus:

$$98 = 2 \cdot 42 + 14 \;\Rightarrow\; 98k + 42l = 14 \text{ where } k = 1,\; l = -2$$

But what if the gcd didn't appear until after many applications of the Division Algorithm? For instance let's find a solution to $k111 + l69 = 3$.

Begin by recalling Euclid's algorithm for finding the gcd of 111 and 69 from section 2.3.1. Starting at the fifth application of the quotient algorithm, we solve for the gcd.

$$15 - 1 \cdot 12 = 3$$

But our final k and l have 111 and 69 in the equation, not 15 and 12. We get 111 and 69 into the expression for the gcd by using the higher equations to solve and substitute; first for 12, then 15, 27, and 42. Starting with 12, we have from the fourth equation that:

$$12 = 27 - 1 \cdot 15$$

Substituting into the fifth equation gives:

$$\begin{aligned} 15 - 1 \cdot (27 - 1 \cdot 15) = 3 \quad &\Rightarrow\; 15 - 27 + 15 = 3 \\ &\Rightarrow (-1) \cdot 27 + 2 \cdot 15 = 3 \end{aligned}$$

Notice how we do *not* multiply out $2 \cdot 15$. That's so we can substitute for 15 in the next step, like so:

$$\begin{aligned} 15 = 42 - 1 \cdot 27 \quad &\text{so} \quad (-1) \cdot 27 + 2 \cdot (42 - 1 \cdot 27) = 3 \\ &\Rightarrow \quad (-1) \cdot 27 + 2 \cdot 42 + (-2) \cdot 27 = 3 \\ &\Rightarrow \quad 2 \cdot 42 + (-3) \cdot 27 = 3 \\ 27 = 69 - 1 \cdot 42 \quad &\text{so} \quad 2 \cdot 42 + (-3) \cdot (69 - 1 \cdot 42) = 3 \\ &\Rightarrow \quad 2 \cdot 42 + (-3) \cdot 69 + 3 \cdot 42 = 3 \\ &\Rightarrow \quad (-3) \cdot 69 + 5 \cdot 42 = 3 \\ 42 = 111 - 1 \cdot 69 \quad &\text{so} \quad (-3) \cdot 69 + 5 \cdot (111 - 1 \cdot 69) = 3 \\ &\Rightarrow \quad (-3) \cdot 69 + 5 \cdot 111 + (-5) \cdot 69 = 3 \\ &\Rightarrow \quad 5 \cdot 111 + (-8) \cdot 69 = 3 \end{aligned}$$

So one solution is: $k = 5$ and $l = -8$. How do we find other solutions? To do that we'll need to define the *least common multiple*.

Definition 2.3.2: Given two integers a and b, the *least common multiple* of a and b, written $\text{lcm}[a, b]$, is the smallest positive integer, L, such that $L = an$ and $L = bm$ for integers $n, m \in \mathbb{Z}$.

Example 2.3.3: Find the $\text{lcm}[16, 12]$.

The multiples of 16 are $16,\ 32,\ 48,\ 64\ldots$ while the multiples of 12 are $12,\ 24,\ 36,\ 48,\ 60\ldots$. The smallest number on both lists is 48, so $\text{lcm}[16, 12] = 48$.

For larger numbers the lcm can be a little difficult to calculate. The following theorem can be very useful.

Theorem 2.3.4: For any integers $a, b \in \mathbb{N}$,

$$\text{lcm}[a, b] = \frac{ab}{\gcd(a, b)}$$

We won't actually prove this theorem, though when you think about it, it's a very believable result. It's worth thinking about how you might prove it, but it's a little tricky.

Example 2.3.5: Use Theorem 2.3.4 to find the $\text{lcm}[111, 69]$.

$$\text{lcm}[111, 69] = \frac{111 \cdot 69}{\gcd(111, 69)} = \frac{7659}{3} = 2553$$

Returning to our equation, $111k + 69l = 3$, let's consider how we can use $\text{lcm}[111, 69] = 2553 = (23)111 = (37)69$. In fact we can generate as many other solutions as we want by adding and subtracting multiples of this lcm.

$$\begin{aligned} 111(5) + 2553n + 69(-8) - 2553n = 3 &\Rightarrow 111(5) + n \cdot 23 \cdot 111 + 69(-8) - n \cdot 37 \cdot 69 = 3 \\ &\Rightarrow 111(5 + 23n) + 69(-8 - 37n) = 3 \end{aligned}$$

We already found that one solution is $k = 5$ and $l = -8$. Now we can generate another solution for each n, where $k = 5 + 23n$ and $l = -8 - 37n$. So for example, $k = 28,\ l = -45$ $(n = 1)$ and $k = -41,\ l = 66$ $(n = -2)$ are other solutions to the equation.

So what about the general equation $ak + bl = c$?

Theorem 2.3.6: If $\gcd(a, b) | c$ then the equation $ak + bl = c$ has infinitely many solutions $k, l \in \mathbb{Z}$.
If $\gcd(a, b) \nmid c$ then the equation $ak + bl = c$ has no solutions $k, l \in \mathbb{Z}$.

Rather than write a proof let's just see how Theorem 2.3.1 can give us solutions to the general case.

Example 2.3.7: Find all solutions $k, l \in \mathbb{Z}$ to

$$21k + 15l = 6$$

First we find the gcd of 21 and 15. We know it's 3, but we'll use Euclid's Algorithm so we have the equations.

$$\begin{aligned} 21 &= (1)15 + 6 \\ 15 &= (2)6 + 3 \\ 6 &= (2)3 + 0 \end{aligned}$$

Now we solve $21x + 15y = \gcd(21, 15) = 3$.

$$3 = 15 - (2)6 = 15 - 2(21 - 15) = (-2)21 + (3)15$$

So one solution is $x = -2$ and $y = 3$.
To get a solution to our original equation we need only multiply through by 2.

$$6 = (-4)21 + (6)15$$

To find all solutions we note that $\text{lcm}[21, 15] = 105 = 21 \cdot 5 = 15 \cdot 7$. Then,

$$\begin{aligned} (-4) \cdot 21 + 105n + (6)15 - 105n &= 6 \\ (-4) \cdot 21 + 21 \cdot 5n + (6)15 - 15 \cdot 7n &= 6 \\ 21(-4 + 5n) + 15(6 - 7n) &= 6 \end{aligned}$$

So for any $n \in \mathbb{Z}$, $k = -4 + 5n$ and $l = 6 - 7n$. For instance $k = 1,\ l = -1$ $(n = 1)$ is a solution.

For the other case, consider this example

Example 2.3.8: Show there are no integer solutions to

$$21k + 15l = 8$$

We may factor 3 out of the left side giving us

$$3(7k + 5l) = 8$$

But that means the left hand side is divisible by 3 (regardless of the values of k and l) while the right side clearly is not. Hence the equation has no integer solutions. This agrees with Theorem 2.3.6 since $\gcd(21, 15) = 3$ and $3 \nmid 8$.

2.3.3 Using Euclid's Theorem in proofs

Theorem 2.3.1 is also a very important tool for proving facts about the integers, divisibility, and primes. Consider Theorem 2.2.4 from last section.

> **Theorem 2.3.9:** **If** a and b are any two integers, p is prime, and $p|ab$
> **Then** $p|a$ or $p|b$

Note that this isn't true if p is not prime. For instance if $a = 2$, $b = 6$, and $p = 4$ we have that $p|ab$ (since $4|12$), but 4 does not divide 2 or 6.

proof:
We'll assume that p does not divide a and then show that p must then divide b.

$\gcd(p, a) = 1$	since $p \nmid a$ and the only divisors of p are p and 1
$kp + la = 1$ for some $k, l \in \mathbb{Z}$	Theorem 2.3.1
$\Rightarrow\ kpb + lab = b$	multiplying through by b
$ab = np$ for some $n \in \mathbb{Z}$	since $p|ab$
$\Rightarrow\ kpb + l(pn) = b$	substitution
$\Rightarrow\ (kb + ln)p = b$	factoring out p
$\Rightarrow\ p|b$	definition of $\|$

Thus if $p \nmid a$ then $p|b$. $\square$

2.3.4 Problems

Problem 2.3.10:

(a) Use Euclid's algorithm to find the gcd of 18 and 26.

(b) Use Euclid's algorithm to find integers k and l so that

$$18k + 26l = \gcd(18, 26)$$

(c) Find all integer solutions of the equation above.

Problem 2.3.11:

(a) Use Euclid's algorithm to find the gcd of 103 and 49.

(b) Use Euclid's algorithm to find integers k and l so that

$$103k + 49l = \gcd(103, 49)$$

(c) Find all integer solutions of the equation above.

Problem 2.3.12: If it is possible, find all integer solutions to the following equations.

1. $20k + 14l = 8$
2. $20k + 14l = 9$

Problem 2.3.13: A candy company has a special rate with a delivery company to deliver 1 kilogram boxes of candy. The boxes should contain a roughly equal mixture of mint chocolates (weighing 17 grams each) and toffees (weighing 31 grams each).
What should the number of mint chocolates and toffees in each box be so as to take full advantage of the 1 kilogram (1000 gram) weight limit?
Hint: If k = number of mint chocolates and l = number of toffees, you're really just looking for a "reasonable" solution to

$$17k + 31l = 1000$$

Problem 2.3.14: Prove the following statement:
If a is relatively prime to n and b is relatively prime to n
then ab is relatively prime to n.
Hint: Use Euclid's Theorem (2.3.1) twice.

2.4 Congruence

Notation

$\equiv$ Congruent modulo some natural number

Back in Section 1.5 one example of an equivalence relation was Example 1.5.3. We wrote the binary relation as

$$M = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n - m = 3k \text{ for some } k \in \mathbb{Z}\}$$

Once we see it is an equivalence relation we may use our more recent notation and write it as

$$n \sim m \Leftrightarrow 3|(n - m)$$

A glance back at the proof that this is an equivalence relation shows there's nothing particularly special about the 3. Any other natural number gives us another equivalence relation. In fact this class of equivalence relations is so important that when integers are equivalent with respect to them, we say the integers are *congruent*.

> **Definition 2.4.1:** Two integers, $n, m \in \mathbb{Z}$ are *congruent modulo* N, written $n \equiv m \mod N$, if and only if N divides $n - m$. That is,
>
> $$n \equiv m \mod N \Leftrightarrow N|(n - m)$$
>
> here $N \in \mathbb{N}$.

So for instance, $8 \equiv 2 \mod 3$ since $8 - 2 = 6 = 2(3)$. That is, $3|(8 - 2)$.

> **Theorem 2.4.2:** *Congruence modulo* N is an equivalence relation on $\mathbb{Z}$ for any $N \in \mathbb{N}$.

The proof is the same as our proof that the relation in Example 1.5.3 is an equivalence relation—simply replace the 3 with an N.

Intuitively, congruence modulo N says that—in the right context—an integer isn't really changed by adding or subtracting N.

This idea that adding or subtracting a particular number doesn't change something is more common than you might initially think. For instance if you fall asleep with your clock reading 12:00 and wake up with it reading 1:00, then you may have slept one hour... or thirteen hours—you can't tell the difference just by looking at your clock (let's leave am/pm out of this). Your clock gives the same time if you add or subtract 12 hours. Thus your clock gives the time *modulo* 12.

We have already seen a similar idea with respect to angles. If we only care about direction (and not the amount of rotation) then adding or subtracting 360° is not an important change. 420° is *congruent* to 60° *modulo* 360°.

2.4.1 Calculation mod N

You sometimes see the mathematical term "mod" used to describe a binary operation (like addition or multiplication) that means "divide and take the remainder". For instance you may see

$$25 \bmod 12 = 1$$

This implies $25 \equiv 1 \mod 12$. (True since $25 - 1 = 2 \cdot 12$.) Of course it's also true that $25 \equiv 13 \mod 12$ and $25 \equiv -11 \mod 12$, but you would never write $25 \bmod 12 = 13$ or -11.

In general the binary operation "mod" returns the remainder, r, produced when you apply the Division Algorithm. If $a = qN + r$ then $a \equiv r \mod N$ since $a - r = qN \Rightarrow N|(a - r)$.

Considering "mod" as a binary operation we have $a \bmod N = r$. So it's easy to see that binary *mod* and *congruence modulo* N are related, but not exactly the same.

The following theorem makes calculation modulo N a lot easier.

Theorem 2.4.3:
If $a \equiv b \mod N$ then for any $c \in \mathbb{Z}$,

(i) $a + c \equiv b + c \mod N$

(ii) $a \cdot c \equiv b \cdot c \mod N$

We'll prove (i) and leave (ii) as an exercise.
proof:

$a - b = kN$ for some $k \in \mathbb{Z}$	definition of $\equiv \mod N$	
$\Rightarrow\ a + c - b - c = kN$	algebra	
$\Rightarrow\ (a + c) - (b + c) = kN$	algebra	
$\Rightarrow\ (a + c) \equiv (b + c) \mod N$	definition of $\equiv \mod N$	$\square$

For instance, calculating $8 \cdot 5 \mod 3$ (and including all the excruciating details)

$8 \equiv 2 \mod 3$	$\Rightarrow 8 \cdot 5 \equiv 2 \cdot 5 \mod 3$	Theorem 2.4.3(ii)
$5 \equiv 2 \mod 3$	$\Rightarrow 2 \cdot 5 \equiv 5 \cdot 2 \equiv 2 \cdot 2 \mod 3$	symmetry and Theorem 2.4.3(ii)
	$\Rightarrow 8 \cdot 5 \equiv 2 \cdot 2 \mod 3$	transitivity
	$\Rightarrow 8 \cdot 5 \equiv 4 \equiv 1 \mod 3$	Definition of $\equiv \mod 3$

In practice this theorem means that you should never calculate with numbers bigger than N. Every time you find yourself with a large number you can replace it with a number congruent to it and less than N.

Example 2.4.4: Calculate: $241 \cdot 28 + 23 \mod 24$.

Well calculating the hard way,

$$241 \cdot 28 + 23 \equiv 6771 \equiv 3 \mod 24$$

But $241 \equiv 1 \mod 24$, $28 \equiv 4 \mod 24$, and $23 \equiv -1 \mod 24$, so

$$241 \cdot 28 + 23 \equiv 1 \cdot 4 - 1 \equiv 3 \mod 24$$

Example 2.4.5: Calculate $7^5 \mod 11$.

7^5 is a large number, but we need not calculate it directly.

$$\begin{aligned} 7^2 &\equiv 49 \equiv 5 \mod 11 \\ 7^4 \equiv 7^2 \cdot 7^2 &\equiv 5^2 \equiv 25 \equiv 3 \mod 11 \\ 7^5 \equiv 7^4 \cdot 7 &\equiv 3 \cdot 7 \equiv 21 \equiv 10 \mod 11 \end{aligned}$$

In general it is quick and efficient to use this method of squaring and reducing to find the 2nd, 4th, 8th, 16th, etc powers of a number (mod N). You then multiply these results appropriately to find all powers not powers of 2.

2.4.2 Theorems involving congruence

Modular arithmetic can be used to prove some well-known facts about the integers written base 10. First recall what it means to write an integer "base b".

Definition 2.4.6: For any $n \in \mathbb{N}$, we write n *base* b as a sequence of *digits*, d_k where $0 \leq d_k < b$ and $k = 0, 1, 2 \ldots K$ so that

$$n = d_K \cdot b^K + d_{K-1} \cdot b^{K-1} + \ldots + d_1 \cdot b + d_0$$

This representation is written $n = (d_K d_{K-1} \cdots d_1 d_0)_b$.

The most common base is 10. So for instance,

$$2322 = (2322)_{10} = 2 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10 + 2$$

but the same integer could just as well be written base 7,

$$2322 = 6 \cdot 7^3 + 5 \cdot 7^2 + 2 \cdot 7 + 5 = (6625)_7$$

Theorem 2.4.7: Let $x = (d_k d_{k-1} \ldots d_1 d_0)_{10}$.
Then x is divisible by 2 if and only if d_0 is divisible by 2.

This is not necessarily true if the base isn't 10. For instance, 143_5 is an even number ($1 \cdot 5^2 + 4 \cdot 5 + 3 = 48$) despite the fact that the last digit is 3. Likewise 2322 is even, but in base 7 $d_0 = 5$ which is odd.

proof:
First note that

$$\begin{array}{rll} m \text{ even} & \Leftrightarrow & m = 2k \text{ for some } k \in \mathbb{Z} \quad \text{Definition of even} \\ & \Leftrightarrow & m \equiv (0)k \equiv 0 \mod 2 \quad \text{Since } 2 \equiv 0 \mod 2. \end{array}$$

So any integer m is even if and only if $m \equiv 0 \mod 2$. This lets us use the machinery of congruence to get at the question of divisibility.

$$\begin{array}{rll} x & \equiv 10^k d_k + 10^{k-1} d_{k-1} + \ldots + 10 d_1 + d_0 \mod 2 & \text{since they are equal} \\ \Leftrightarrow x & \equiv 0^k d_k + 0^{k-1} d_{k-1} + \ldots + 0 d_1 + d_0 \mod 2 & \text{since } 10 \equiv 0 \mod 2 \\ \Leftrightarrow x & \equiv d_0 \mod 2 & \text{simplification} \end{array}$$

So, $x \equiv 0 \mod 2$ if and only if $d_0 \equiv 0 \mod 2$. Thus $2|x$ if and only if $2|d_0$. $\square$

Clearly the same argument can be made for 5 since $10 \equiv 0 \mod 5$ as well. In fact you can generalize to say that the divisibility by y of some integer x written to some base b will be determined by its last digit if and only if the $y|b$.

Another well-known fact that you probably couldn't prove (until now) is the following:

Theorem 2.4.8: Let $x = (d_k d_{k-1} \ldots d_1 d_0)_{10}$.
Then x is divisible by 3 if and only if $d_0 + d_1 + \ldots + d_k$ is divisible by 3.

For instance $3|261$ since $261 = 3(87)$. And $2 + 6 + 1 = 9$ which is also divisible by 3.

proof:

Again it's easy to see that a number is divisible by 3 if and only if it is congruent to 0 modulo 3. Thus,

$$\begin{array}{rll} x & \equiv 10^k d_k + 10^{k-1} d_{k-1} + \ldots + 10 d_1 + d_0 \mod 3 & \text{since they are equal} \\ \Leftrightarrow x & \equiv (1)^k d_k + (1)^{k-1} d_{k-1} + \ldots + (1) d_1 + d_0 \mod 3 & \text{since } 10 \equiv 1 \mod 3 \\ \Leftrightarrow x & \equiv d_k + d_{k-1} + \ldots + d_0 \mod 3 & \text{simplification} \end{array}$$

Thus $x \equiv 0 \mod 3$ if and only if $d_k + d_{k-1} + \ldots + d_0 \equiv 0 \mod 3$. $\square$

2.4.3 Linear Congruence Equations

We now address the question of solving linear congruences. How would you solve the following? Are there solutions at all?

$$3x \equiv 5 \mod 7$$

By the definition of congruence, this equation is equivalent to:

$$7|(3x - 5)$$

which is in turn equivalent to:

$$3x - 5 = 7y$$

for some integer y. We can rearrange to get

$$3x - 7y = 5$$

This is something that we've seen before. Theorem 2.3.6 says that since $\gcd(3,7) = 1$ and so divides 5, there are infinitely many solutions, x and y. Euclid's Algorithm gives us $x = -10, y = 5$. In this context we only care about the x, and since $-10 \equiv 4 \mod 7$ we can just take $x = 4$ as our solution. In fact this is the **only** solution modulo 7. Checking,

$$3 \cdot 4 \equiv 12 \equiv 5 \mod 7$$

It's easy to see we can solve any linear congruence $ax \equiv c \mod b$ if $\gcd(a,b) = 1$. On the other hand, if $\gcd(a,b) \neq 1$ then there may be no solutions... or multiple solutions. For instance,

$$2x \equiv 3 \mod 4 \Leftrightarrow 2x - 4y = 3$$

which, by theorem 2.3.6, has no solutions since $\gcd(2,4) = 2 \not| 3$. However,

$$2x \equiv 2 \mod 4 \Leftrightarrow 2x - 4y = 2$$

has solutions since $2|2$. Obviously letting $x = 1$ and $y = 0$ works. Using the adding and subtracting trick we can get all the solutions since

$$2(1 + 2n) - 4(0 + n) = 2$$

Thus for every $n \in \mathbb{N}$ we have a solution,

$$x = 1 + 2n = \ldots -1, 1, 3, 5 \ldots$$

Modulo 4 there are just two different solutions here: $x \equiv 1 \mod 4$ and $x \equiv 3 \mod 4$.

In general the situation is described by the following theorem.

Theorem 2.4.9: The linear congruence equation $ax \equiv b \mod N$ has:

i) no solutions if $\gcd(a,N) \not| b$

ii) $\gcd(a,N)$ solutions (modulo N) if $\gcd(a,N)|b$

Example 2.4.10: Find all solutions to

$$69x \equiv 6 \mod 111$$

Since $\gcd(69,111) = 3$ and $3|6$ we expect by Theorem 2.4.9 that there are three different solutions modulo 111.

The congruence equation implies $69x - 111y = 6$ (for some integer y). Back in Section 2.3.1 we found all solutions to $111k + 69l = 3$. We only care about the coefficient of 69, which turned out to be $l = -8 - 37n$. To find solutions to $69x - 111y = 6$, we need only multiply through by two. Hence, $x = -16 - 74n$. What are the three solutions modulo 111?

$$n = 0 \Rightarrow x = -16 \equiv 95 \mod 111$$

Checking we see that $69 * 95 - 6 = 6549 = 111(59)$. Since $111|(69 * 95 - 6)$,

$$69 \cdot 95 \equiv 6 \mod 111$$

Similarly,

$$n = -1 \;\Rightarrow\; x = -16 + 74 = 58$$

and

$$n = -2 \;\Rightarrow\; x = -16 + 148 = 132 \equiv 21 \mod 111$$

Checking we have

$$69 \cdot 58 - 6 = 3996 = 111(36) \;\Rightarrow\; 69 \cdot 58 \equiv 6 \mod 111$$

and

$$69 \cdot 21 - 6 = 1443 = 111(13) \;\Rightarrow\; 69 \cdot 21 \equiv 6 \mod 111$$

Therefore the three different solutions modulo 111 are

$$x = 21,\ 58,\ 95$$

Are we sure there aren't any more? Well letting $n = -3$ gives

$$x = -16 + 222 = 206 \equiv 95 \mod 111$$

But we already had that solution. In fact decreasing (or increasing) n further will just cause us to cycle through the three different solutions that we'd already discovered. Thus these three solutions are the only solutions between 0 and 111.

2.4.4 Problems

Problem 2.4.11: Prove that if $a \equiv b \mod N$ then for any $c \in \mathbb{Z}$,

$$a \cdot c \equiv b \cdot c \mod N$$

Problem 2.4.12:

(a) Use the method in Example 2.4.5 to find $0 < a < 19$ such that

$$a \equiv 6^{16} \mod 19$$

(b) Use the previous part to find $0 < b < 19$ such that

$$b \equiv 6^{21} \mod 19$$

Problem 2.4.13: Let $x = (d_k d_{k-1} \ldots d_1 d_0)_{10}$. Prove that x is divisible by 11 if and only if the following alternating sum is divisible by 11.

$$d_0 - d_1 + d_2 - d_3 + \ldots + (-1)^k d_k$$

So for example consider 1925. $11 \mid 1925$ since $1925 = 11 \cdot 175$. It also happens that $5 - 2 + 9 - 1 = 11$ and, of course, $11 \mid 11$ just as this statement predicts.

Problem 2.4.14: Use the methods described in this section to find all solutions (modulo 391) to

$$29x \equiv 1 \mod 391$$

Problem 2.4.15: Use the methods described in this section to find all solutions (modulo 4322) to

(a)

$$846x \equiv 2 \mod 4322$$

(b)

$$846x \equiv 5 \mod 4322$$

(c)

$$846x \equiv 6 \mod 4322$$

Chapter 3

Sequences and Series

3.1 Sequences

Notation

a_n sequence

$\sum_{i=0}^{n} a_i$ sum of the first n terms of the sequence a_i.

A **sequence** is an infinite list of numbers *in a particular order*. The individual numbers in the list are called the *terms* of the sequence. Some examples of sequences are

Example 3.1.1:

(a) $2, -4, 6, -8, 10, ...$

(b) $1, 2, 4, 8, 16, ...$

(c) $1, 0, 1, 0, 1, 0, ...$

(d) $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, ...$

(e) $1, 1, 2, 3, 5, 8, 13, ...$

(f) $\pi, \sqrt{\pi}, \sqrt[3]{\pi}, \sqrt[4]{\pi}, ...$

(g) $7, -53, 2, 17, 421, 0, -5, 0, -5, 28, ...$

We are primarily concerned with sequences of integers, but we may occasionally see sequences of rational or real numbers. Our sequences will generally have some sort of governing pattern, but the last example above illustrates that the terms of a sequence need not exhibit an obvious pattern or any pattern at all. Finally, make note of the fact that *sequences are not sets*. In a set the order of the elements is of no importance, but the terms of a sequence have a definite order. Also, terms in a sequence may be repeated, whereas elements in a set may not.

Consider the first sequence above. Its first term is 2, its second term -4, its third 6, and so on. When we talk about a "first", "second", "third", etc., we are essentially assigning to each natural number 1, 2, 3, ... the corresponding term of the sequence. Thus a sequence can be thought of as a function a defined on the natural numbers.

Definition 3.1.2: A *sequence* is a function $a : \mathbb{N} \to \mathbb{R}$ or $a : \{0\} \cup \mathbb{N} \to \mathbb{R}$.
A *bi-infinite sequence* is a function $a : \mathbb{Z} \to \mathbb{R}$.
The n-th term, $a(n)$, of either type of sequence is usually written a_n.

Example 3.1.3: Give an explicit function defining the following sequences.

(a) $2, -4, 6, -8, 10, ...$

(b) $1, 2, 4, 8, 16, ...$

(c) $1, 0, 1, 0, 1, 0, ...$

(d) $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, ...$

There's not much of a method for doing this. For the most part it's just a matter of intuition, trial and error.

(a) $2, -4, 6, -8, 10, ...$

$$a_n = (-1)^{(n+1)}2n, \quad n \in \mathbb{N}$$

Checking the first two terms we see $a_1 = (-1)^{1+1}2(1) = 2$ and $a_2 = (-1)^{2+1}2(2) = -4$, just as we expect. Had we decided to begin our sequence with $n = 0$ rather than $n = 1$ as above, then the function would be slightly different.

$$a_n = (-1)^n 2(n+1), \quad n = \{0,\ 1,\ 2, \ldots\}$$

Again checking the first two terms, $a_0 = (-1)^0 2(0+1) = 2$ and $a_1 = (-1)^1 2(1+1) = -4$

(b) $1, 2, 4, 8, 16, ...$

$$a_n = 2^{n-1}, \quad n = 1, 2, 3 \ldots \qquad \text{or} \quad a_n = 2^n, \quad n = 0, 1, 2 \ldots$$

(c) $1, 0, 1, 0, 1, 0, ...$

$$a_n = \frac{1 + (-1)^n}{2}, \quad n = 0, 1, 2 \ldots$$

(d) $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, ...$

$$a_n = \frac{1}{n}, \quad n = 1, 2, 3 \ldots$$

Example 3.1.4: Write out the first five terms of each sequence.

(a) $-3(2)^n, \quad n = 0, 1, 2, ...$

(b) $5n + 1, \quad n = 1, 2, 3, ...$

This is just a "plug and chug" exercise.

(a) $a_n = -3(2)^n, \quad n = 0, 1, 2, ...$

$$-3,\ -6,\ -12,\ -24,\ -48$$

(b) $a_n = 5n + 1, \quad n = 1, 2, 3, ...$

$$6,\ 11,\ 16,\ 21,\ 26$$

3.1.1 Series

From any sequence we may make a new sequence called the *sequence of partial sums*. The n-th term in this new sequence is just the sum of the first n terms of the old sequence.

Definition 3.1.5: Given a sequence a_n, the *sequence of partial sums*, s_n, is the sequence formed by adding the first n terms of the sequence a_n. That is, assuming a_n starts at $n = 1$,

$$s_n = a_1 + a_2 + \ldots + a_n$$

We will often denote this sum with *summation notation*,

$$s_n = \sum_{i=1}^{n} a_i$$

Here the variable i is called the *index*, and runs through the integers from 1 to n.

Example 3.1.6: For each sequence find the first five terms of the sequence of partial sums, and then write s_5 using summation notation. (Assume the each sequence begins with $n = 1$.)

(a) $2, -4, 6, -8, 10, ...$

(b) $1, 2, 4, 8, 16, ...$

(a) $2, -4, 6, -8, 10, ...$

$$\begin{array}{lll} s_1 = a_1 & = 2 & = 2 \\ s_2 = a_1 + a_2 & = 2 - 4 & = -2 \\ s_3 = a_1 + a_2 + a_3 & = 2 - 4 + 6 & = 4 \\ s_4 = a_1 + a_2 + a_3 + a_4 & = 2 - 4 + 6 - 8 & = -4 \\ s_5 = a_1 + a_2 + a_3 + a_4 + a_5 & = 2 - 4 + 6 - 8 + 10 & = 6 \end{array}$$

So the sequence of partial sums is: $2, -2, 4, -4, 6 \ldots$

$$s_5 = \sum_{i=1}^{5} (-1)^{i+1} 2i = (-1)^2 2(1) + (-1)^3 2(2) + (-1)^4 2(3) + (-1)^5 2(4) + (-1)^6 2(5)$$

(b) $1, 2, 4, 8, 16, ...$

$$\begin{array}{lll} s_1 = 1 & = 1 \\ s_2 = 1 + 2 & = 3 \\ s_3 = 1 + 2 + 4 & = 7 \\ s_4 = 1 + 2 + 4 + 8 & = 15 \\ s_5 = 1 + 2 + 4 + 8 + 16 & = 31 \end{array}$$

So the sequence of partial sums is: $1, 3, 7, 15, 31 \ldots$

$$s_5 = \sum_{i=1}^{5} 2^{i-1} = 2^0 + 2^1 + 2^2 + 2^3 + 2^4$$

In general, the sequence of partial sums can only be calculated by actually adding together the terms of its parent sequence, just as we did above. In practice, however, we can find s_n as a simple function of n just as we did for our first several sequences.

The most famous example of this is attributed to the great mathematician Friedrich Gauss who was supposedly assigned the mind-numbingly boring task of adding together the numbers from 1 to 1000 (it was apparently some sort of class punishment). In the language of this section Gauss had been asked to find

$$\sum_{i=1}^{1000} i = 1 + 2 + 3 + \ldots + 999 + 1000$$

or s_{1000} for the sequence $a_i = i$. Gauss's solution is simple and brilliant. The idea is to write out the terms of the sum both forward *and backward*, and then add them.

$$\begin{array}{rccccccccccc} s_{1000} = & 1 & + & 2 & + & 3 & + & \ldots & + & 999 & + & 1000 \\ +s_{1000} = & 1000 & + & 999 & + & 998 & + & \ldots & + & 2 & + & 1 \\ \hline 2s_{1000} = & 1001 & + & 1001 & + & 1001 & + & \ldots & + & 1001 & + & 1001 \end{array}$$

$$2s_{1000} = 1000(1001) \quad \Rightarrow \quad s_{1000} = \frac{1000(1001)}{2} = 500500$$

Of course there's nothing special about 1000 in this proof; the proof works just as well if 1000 is replaced by n. That gives us a formula for the n-th partial sum of the sequence $a_i = i$. We might as well call it a theorem.

Theorem 3.1.7: For the sequence: $1, 2, 3 \ldots$ the sequence of partial sums may be written:

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

We can try it for some small values of n just to see it in action.

Example 3.1.8: Find the value of the partial sums.

(a) $1 + 2 + 3$

(b) $1 + 2 + 3 + 4 + 5$

(a)

$$1 + 2 + 3 = \sum_{i=1}^{3} i = \frac{3(3+1)}{2} = 6$$

which we can clearly see is correct. Similarly,

(b)

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

also clearly correct.

There are several other examples of explicit formulas for the partial sums of certain sequences. Here are two you may have seen in a calculus course.

Theorem 3.1.9:

(a) For the sequence of squares: $1, 4, 9 \ldots$ the sequence of partial sums may be written:

$$1 + 4 + 9 \ldots + n^2 = \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

(b) For the sequence of cubes: $1, 8, 27 \ldots$ the sequence of partial sums may be written:

$$1 + 8 + 27 \ldots + n^3 = \sum_{i=1}^{n} i^3 = \left[\frac{n(n+1)}{2}\right]^2$$

In general the proofs of theorems of this sort use the *Principle of Mathematical Induction* which we will study in the next section. I will give the proof of Theorem 3.1.9(a) while you'll be asked to prove Theorem 3.1.9(b). But that's next section.

3.1.2 Recursion

When we represent a sequence *explicitly* we are telling how to find a term of a sequence based on the index of the term. If we want to know the 100-th term in the sequence $a_n = 2n + 1$ we need only plug 100 in for n and get $a_{100} = 2(100) + 1 = 201$. There is another way to represent a sequence, which we call a *recursive* representation of the sequence. A recursive representation consists of giving the first term (or first several terms) of the sequence and then telling how to obtain each term from the one term (or several terms) preceding it.

For example, we can define the sequence above, $a_n = 2n + 1$, can also be generated by specifying that $a_0 = 1$ and $a_{n+1} = a_n + 2$. To see how just start generating terms.

$$\begin{aligned} a_1 = a_0 + 2 &= (1) + 2 = 3 \\ a_2 = a_1 + 2 &= (3) + 2 = 5 \\ a_3 = a_2 + 2 &= (5) + 2 = 7 \end{aligned}$$

If you add 2 to an odd number you get the next largest odd number, so clearly this sequence just gives you all the odd numbers starting from 1. This is of course the same as the sequence $a_n = 2n+1, \quad n = 0, 1, 2 \ldots$. In general, though, it is quite difficult to find an *explicit* formula for a sequence defined *recursively*. Even after listing several terms of a sequence and guessing a pattern we will need the *Principle of Mathematical Induction* to prove our guess is correct. (More work for next section.)

One of the most interesting recursively defined sequences is the very famous *Fibonacci Sequence*. (Fibonacci originally came up with it to describe the number of rabbits he had in his n-th year of raising rabbits.)

Example 3.1.10: Write out the first several terms of the sequence defined recursively by:

$$a_1 = 1, \; a_2 = 1, \; a_{n+2} = a_{n+1} + a_n$$

$$\begin{aligned} a_3 = \;& a_2 + a_1 = \; 1 + 1 = 2 \\ a_4 = \;& a_3 + a_2 = \; 2 + 1 = 3 \\ a_5 = \;& a_4 + a_3 = \; 3 + 2 = 5 \\ a_6 = \;& a_5 + a_6 = \; 5 + 3 = 8 \\ a_7 = \;& a_6 + a_5 = \; 8 + 5 = 13 \\ & \ldots \end{aligned}$$

While there is an explicit formula for the Fibonacci Sequence, it is quite difficult and would be practically impossible to guess just from looking at the terms.

Example 3.1.11: For each recursively defined sequence write out the first seven terms of the sequence. Then try to guess an explicit definition.

(a) $a_1 = 20, \quad a_{n+1} = a_n - 3$

(b) $a_0 = 2, \quad a_{n+1} = 3a_n$

(a) $a_1 = 20, \quad a_{n+1} = a_n - 3$

$$\begin{aligned} a_2 &= a_1 - 3 &&= (20) - 3 = 17 \\ a_3 &= a_2 - 3 &&= (17) - 3 = 14 \\ a_4 &= a_3 - 3 &&= (14) - 3 = 11 \end{aligned}$$

So the sequence is:

$$20,\ 17,\ 14,\ 11,\ 8,\ 5,\ 2\ldots$$

Since the sequence starts at 20 and decreases by 3 each term,

$$a_n = 23 - 3n$$

fits the bill. You should always check the first few terms of your guess.
$a_1 = 23 - 3(1) = 20$. $a_2 = 23 - 3(2) = 17$. $a_3 = 23 - 3(3) = 14$.

(b) $a_0 = 2, \quad a_{n+1} = 3a_n$

$$\begin{aligned} a_1 &= 3a_0 &&= 3(2) = 6 \\ a_2 &= 3a_1 &&= 3(6) = 18 \\ a_3 &= 3a_2 &&= 3(18) = 54 \end{aligned}$$

So the sequence is:

$$2,\ 6,\ 18,\ 54,\ 162,\ 486,\ 1458\ldots$$

It's hard to see the pattern until you divide all the terms by 2. Then you see

$$1,\ 3,\ 9,\ 27,\ 81,\ 243,\ 729\ldots$$

These are clearly powers of 3. Thus we guess,

$$a_n = 2 \cdot 3^n$$

This formula certainly gives the terms listed above.

Example 3.1.12: Define each of the following sequences both explicitly and recursively.

(a) $4, 7, 10, 13, ...$

(b) $1, 2, 4, 8, 16, ...$

(c) $5, -5, 5, -5, 5, ...$

(a) $4, 7, 10, 13, ...$

The sequence starts at 4 and increases by 3 each term, so a recursive definition would be

$$a_1 = 4, \quad a_{n+1} = a_n + 3$$

And an explicit formula

$$a_n = 1 + 3n, \quad n = 1, 2, 3 \ldots$$

(b) $1, 2, 4, 8, 16, ...$

The sequence starts at 1 and doubles each term, so a recursive definition would be

$$a_0 = 1, \quad a_{n+1} = 2a_n$$

And an explicit formula

$$a_n = 2^n, \quad n = 0, 1, 2 \ldots$$

(c) $5, -5, 5, -5, 5, ...$

The sequence starts at 5 and switches sign each term, so a recursive definition would be

$$a_0 = 5, \quad a_{n+1} = -a_n$$

And an explicit formula

$$a_n = (-1)^n \cdot 5, \quad n = 0, 1, 2 \ldots$$

3.1.3 Arithmetic and Geometric Examples

You have already seen two of the most important types of sequence in the Example 3.1.12: (a) is an example of a *arithmetic sequence*, and (b) is an example of a *geometric sequence*.

> **Definition 3.1.13:** A sequence is called an *arithmetic sequence* if the difference between any two consecutive terms is constant. That is,
>
> $$a_{n+1} - a_n = d$$
>
> for any n for which the sequence is defined.

Another way to write this is to say that $a_{n+1} = a_n + d$ for any n for which the sequence is defined. Here d can be any number, as long as it is *constant* (that is, it does not depend on n).

Hence the sequence $4, 7, 10, 13, ...$ is arithmetic with $d = 3$. $(7 - 4 = 3,\ 10 - 7 = 3 \ldots)$

Definition 3.1.14: A sequence is called a **geometric sequence** if the ratio between any two consecutive terms is constant. That is,

$$\frac{a_{n+1}}{a_n} = r$$

for any n for which the sequence is defined.

Again, another way to write this is $a_{n+1} = ra_n$. The sequence $1, 2, 4, 8, 16, ...$ is geometric with $r = 2$. $(2/1 = 2,\ 4/2 = 2,\ 8/4 = 2 \ldots)$

Not only do these sequences have explicit formulas, but their sequences of partial sums do as well. We'll prove these results in the next section.

Theorem 3.1.15: For the arithmetic sequence defined recursively by $a_1 = A$ and $a_{n+1} = a_n + d$,

(a)

$$a_n = A + (n-1)d, \quad n = 1, 2, 3 \ldots$$

(b)

$$\sum_{i=1}^{n} a_i = An + \frac{n(n-1)}{2}d$$

Example 3.1.16: For the sequence $4, 7, 10, 13, ...$ find an explicit formula and an explicit formula for the sequence of partial sums.

Here $A = 4$ and $d = 3$, so

(a) $a_n = 4 + (n-1)3 = 3n + 1, \quad n = 1, 2, 3 \ldots$

(b)

$$\sum_{i=1}^{n} a_i = 4n + \frac{n(n-1)}{2}3 = \frac{3n^2 + 5n}{2}$$

Checking the first couple of terms,

$$\sum_{i=1}^{1} a_i = 4 = \frac{3(1)^2 + 5(1)}{2}$$

$$\sum_{i=1}^{2} a_i = 4 + 7 = \frac{3(2)^2 + 5(2)}{2}$$

So we're reasonably confident of our result.

Theorem 3.1.17: For the geometric sequence defined recursively by $a_0 = A$ and $a_{n+1} = ra_n$, where $r \neq 1$,

(a)

$$a_n = Ar^n, \quad n = 0, 1, 2 \ldots$$

(b)

$$\sum_{i=1}^{n} a_i = A\left(\frac{r^{n+1} - 1}{r - 1}\right)$$

Example 3.1.18: For the sequence $1, 2, 4, 8, 16, ...$ find an explicit formula and an explicit formula for the sequence of partial sums.

Here $A = 1$ and $r = 2$, so

(a) $a_n = (1)2^n = 2^n, \quad n = 0, 1, 2 \ldots$

(b)

$$\sum_{i=1}^{n} a_i = (1)\frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1$$

Checking the first couple of terms,

$$\sum_{i=1}^{1} a_i = 1 = 2^{0+1} - 1$$

$$\sum_{i=1}^{2} a_i = 1 + 2 = 2^{1+1} - 1$$

So again we're reasonably confident of our result.

3.1.4 Problems

Problem 3.1.19: Guess a formula for the partial sum,

$$\frac{1}{2}+\frac{1}{6}+\frac{1}{12}+\ldots+\frac{1}{n(n+1)}=\sum_{i=1}^{n}\frac{1}{i(i+1)}$$

Problem 3.1.20: Use Theorems 3.1.1 and 3.1.9 to find the value of the sums.

(a) $100+101+102+\ldots+200$
Hint: Write as a difference of two sums starting at 1.

(b) $64+81+100+\ldots+361+400$

(c) $2+16+54+\ldots+1458+2000$.
Hint: Factor out a 2.

Problem 3.1.21: Consider the recursively defined sequence where $a_0=2,\ a_1=3$, and $a_{n+2}=3a_{n+1}-2a_n$.

(a) Find a_2 through a_6.

(b) Guess an explicit formula for a_n.

(c) Write a new recursive definition for this sequence so that a_{n+1} depends only on a_n.

Problem 3.1.22: Recall the Fibonacci sequence, which is defined by $a_1=1$, $a_2=1$, $a_{n+2}=a_{n+1}+a_n$.

(a) Find a_1+a_3, $a_1+a_3+a_5$ and $a_1+a_3+a_5+a_7$.

(b) Make a conjecture about

$$a_1+a_3+a_5+\cdots+a_{2n-1}=\sum_{i=1}^{n}a_{2i-1}=\ ?$$

(c) Repeat part (b) for the even terms of the Fibonacci sequence.

3.2 Induction

In the previous section, we spent some time making (educated) guesses about the explicit or recursive definition for a given sequence. A typical problem was the definition of a sequence via recursion, then a question asking for its corresponding explicit definition. Even when we were able to provide such an explicit definition, we could only confirm its validity for a few terms. This was mostly an exhaustive process in which we (manually) computed these terms using both definitions and compared the results.

In this section we will learn a better way to do this. We will be able to *prove* that some explicit formula we've guessed actually correctly generates *all* the terms in a recursively defined sequence.

Most of us have done the following: Stand a set of dominoes up on end in such a way that when we push the first one over, it knocks over the second, which in turn knocks over the third, and so on. In this section we will see a method for proving theorems that is analogous to that game. The process works as follows.

- Show that the theorem is true for $n = 0$, $n = 1$, or perhaps some other starting value. This is called the *base step*.
- Show that if the theorem is true for any whole or natural number k, then it holds for the next $k + 1$ as well. this is called the *inductive step*. The assumption that the theorem is true for k is called the *inductive hypothesis*.
- Conclude that the fact must be true for any non-negative number n greater than the starting value.

This process is formally known as the Principle of Mathematical Induction (which is an over-arching theorem that is used as the basis of every proof by induction).

The above process is sort of backward from the dominoes. The second item above is like setting up the dominoes in such a way that each will knock the next over if it goes over. It says that if the fact is true for 0, then it must be true for 1 as well. And if it is true for 1, then it is true for 2, and so on. Then we need only start the process, which is the first item above. That is, we show the fact is true for $n = 0$ or some other starting value. The process is called **proof by induction**.

3.2.1 Induction on Recursive Sequences

Example 3.2.1: Consider the sequence defined recursively by

$$a_0 = 3,\ a_{n+1} = a_n + 5$$

Use mathematical induction to prove that $a_n = 5n + 3$ for every non-negative integer n.

First, show the *base step* is true. That is, show $a_n = 5n + 3$ when $n = 0$.

$5(0) + 3 = 3 = a_0$

so $a_n = 5n + 3$ holds for $n = 0$.

Second, for the *inductive step*, assume that $a_n = 5n + 3$ is true for $n = k$ and show that it must then be true for $n = k + 1$. In other words, assume that $a_k = 5k + 3$ (this is the *inductive hypothesis*). Then,

$$\begin{array}{rll} a_{k+1} = & a_k + 5 & \text{Recursive definition of the sequence} \\ \Rightarrow a_{k+1} = & (5k + 3) + 5 & \text{Inductive hypothesis} \\ \Rightarrow a_{k+1} = & 5(k + 1) + 3 & \text{algebra} \end{array}$$

Thus $a_n = 5n+3$ being true for $n = k$ leads to it being true for $n = k+1$. Since we have already shown that the formula holds for $n = 0$, it must now hold for $n = 1$. Since it holds for $n = 1$ it must hold for $n = 2$ and so on for every non-negative integer n. □

Most proofs that use induction begin with one statement which lets the reader know that the proof that follows is a proof by induction. This is similar to what we did when we were proving things by contradiction or by the contrapositive. If we don't let the reader know what method of proof we intend to use, the default is a direct proof.

Example 3.2.2: Prove that each of the following recursively defined sequences has the given explicit formula.

(a) Let $a_0 = 1$ and $a_{n+1} = 4a_n$. Prove that $a_n = 4^n$.

(b) Let $a_0 = 2$ and $a_{n+1} = 3a_n - 2$. Prove that $a_n = 3^n + 1$.

(c) Let $a_0 = 2$ and $a_{n+1} = (a_n)^2$. Prove that $a_n = 2^{2^n}$.

(a) Proof is by induction.

Base: $a_0 = 1 = 4^0$ so $a_n = 4^n$ for $n = 0$

Inductive: Assume $a_k = 4^k$.

$$\begin{array}{rll} a_{k+1} = & 4a_k & \text{Recursive definition of the sequence} \\ \Rightarrow a_{k+1} = & 4(4^k) & \text{Inductive hypothesis} \\ \Rightarrow a_{k+1} = & 4^{k+1} & \text{algebra} \end{array}$$

Hence by the Principle of Mathematical Induction, $a_n = 4^n$ for all $n \geq 0$. □

(b) Proof is by induction.

Base: $a_0 = 2 = 3^0 + 1$ so $a_n = 3^n + 1$ for $n = 0$

Inductive: Assume $a_k = 3^k + 1$.

$$\begin{array}{rll} a_{k+1} = & 3a_k - 2 & \text{Recursive definition of the sequence} \\ \Rightarrow a_{k+1} = & 3(3^k + 1) - 2 & \text{Inductive hypothesis} \\ \Rightarrow a_{k+1} = & 3^{k+1} + 3 - 2 & \text{algebra} \\ \Rightarrow a_{k+1} = & 3^{k+1} + 1 & \text{algebra} \end{array}$$

Hence by the Principle of Mathematical Induction, $a_n = 3^n + 1$ for all $n \geq 0$. □

(c) Proof is by induction.

Base: $a_0 = 2 = 2^{2^0} = 2^1$ so $a_n = 2^{2^n}$ for $n = 0$

Inductive: Assume $a_k = 2^{2^k}$.

$$\begin{array}{rll} a_{k+1} = & (a_k)^2 & \text{Recursive definition of the sequence} \\ \Rightarrow a_{k+1} = & (2^{2^k})^2 & \text{Inductive hypothesis} \\ \Rightarrow a_{k+1} = & 2^{2^k \cdot 2} & \text{algebra} \\ \Rightarrow a_{k+1} = & 2^{2^{k+1}} & \text{algebra} \end{array}$$

Hence by the Principle of Mathematical Induction, $a_n = 2^{2^n}$ for all $n \geq 0$. □

Induction can also be used to prove explicit formulas for sequences recursively defined in terms of the previous *two* terms.

Example 3.2.3: Prove that the sequence defined by

$$a_0 = 2,\ a_1 = 3,\ a_{n+2} = 3a_{n+1} + 4a_n$$

has the explicit formula $a_n = 4^n + (-1)^n$.

Base: You must check both $n = 0$ and $n = 1$ since the inductive step assumes that the formula holds for the previous *two* terms.

$$a_0 = 4^0 + (-1)^0 = 1 + 1 = 2, \quad a_1 = 4^1 + (-1)^1 = 4 - 1 = 3$$

Inductive: Assume both $a_k = 4^k + (-1)^k$ and $a_{k+1} = 4^{k+1} + (-1)^{k+1}$ and then use these to prove that $a_{k+2} = 4^{k+2} + (-1)^{k+2}$.

$$\begin{array}{rll} a_{k+2} & = 3a_{k+1} + 4a_k & \text{Recursive definition of the sequence} \\ & = 3(4^{k+1} + (-1)^{k+1}) + 4(4^k + (-1)^k) & \text{Inductive hypotheses} \\ & = 3(4^{k+1}) - 3(-1)^k + 4^{k+1} + 4(-1)^k & \text{algebra} \\ & = 4(4^{k+1}) + (-1)^k & \text{combine like terms} \\ & = 4^{k+2} + (-1)^{k+2} & \text{algebra} \end{array}$$

Hence by the Principle of Mathematical Induction, $a_n = 4^n + (-1)^n$ for all $n \geq 0$. □

3.2.2 Induction on Divisibility

Induction can be used to prove all kinds of statements, some having nothing to do with recursion. Here we'll prove some facts about the divisibility of expressions involving a natural number n.

Example 3.2.4: Prove that $5^n - 1$ is divisible by 4 for every $n \geq 1$.

Before proceeding to the proof it's a good idea to convince yourself that it's true. For instance if $n = 2$ then

$$5^2 - 1 = 24 = 4(6)$$

So $4 \,|\, 5^2 - 1$. If $n = 3$ then

$$5^3 - 1 = 124 = 4(31)$$

So $4 \,|\, 5^3 - 1$. On to the proof.

Proof is by induction.

Base: Here we start with $n = 1$. Then $5^1 - 1 = 4$ and certainly $4|4$ as required.

Inductive: Assume $4 \,|\, (5^k - 1)$. Thus $5^k - 1 = 4l$ for some integer l. We need to show that $5^{k+1} - 1 = 4m$ for some integer m.

$$\begin{aligned} 5^{k+1} - 1 &= 5(5^k) - 1 && \text{algebra} \\ &= 5(4l + 1) - 1 && \text{Inductive hypothesis } 5^k = 4l + 1 \\ &= 20l + 5 - 1 && \text{algebra} \\ &= 4(5l + 1) && \text{factor out a 4} \end{aligned}$$

Thus $5^{k+1} - 1 = 4m$ for $m = 5l + 1$. Hence $4 \,|\, (5^{k+1} - 1)$, and by the Principle of Mathematical Induction $5^n - 1$ is divisible by 4 for every $n \geq 1$. □

Example 3.2.5: Prove that $8^n - 3^n$ is divisible by 5 for every $n \geq 1$.

Proof is by induction.

Base: Here we start with $n = 1$. Then $8^1 - 3^1 = 5$ and $5|5$ as required.

Inductive: Assume $5 \,|\, (8^k - 3^k)$. Thus $8^k - 3^k = 5l$ for some integer l. We need to show that $8^{k+1} - 3^{k+1} = 4m$ for some integer m.

$$\begin{aligned} 8^{k+1} - 3^{k+1} &= 8(8^k) - 3(3^k) && \text{algebra} \\ &= 8(3^k + 5l) - 3(3^k) && \text{Inductive hypothesis } 8^k = 3^k + 5l \\ &= (8 - 3)3^k + 40l && \text{algebra} \\ &= 5(3^k + 8l) && \text{factor out a 5} \end{aligned}$$

Thus $8^{k+1} - 3^{k+1} = 5m$ for $m = 3^k + 8l$. Hence $5 \,|\, (8^{k+1} - 3^{k+1})$, and by the Principle of Mathematical Induction $8^n - 3^n$ is divisible by 5 for every $n \geq 1$. □

3.2.3 Induction for Series

In section 3.1 we presented Theorems 3.1.7 and 3.1.9 which gave formulas for various sums depending on the number of terms n. It is our objective in this section to prove such statements are true for all n using induction. The process is exactly as before. We first need to show that this formula holds for $n = 1$. Second we show that if it holds for $n = k$ then it holds for $n = k + 1$.

We'll start with an easier one, then go on to prove one of the theorem sums.

Example 3.2.6: Prove that

$$1 + 3 + 5 + \ldots + (2n - 1) = n^2, \qquad n = 1, 2, 3 \ldots$$

Proof is by induction.
Base: For $n = 1$ we just have $1 = 1^2$.

Inductive: Here we assume that $1 + 3 + 5 + \ldots + (2k - 1) = k^2$, and use it to show that $1 + 3 + 5 + \ldots + (2k + 1) = (k + 1)^2$.
Using the summation notation our induction hypothesis is

$$\sum_{j=1}^{k}(2j - 1) = k^2$$

while we're trying to show

$$\sum_{j=1}^{k+1}(2j - 1) = (k + 1)^2$$

We start with the left side and hope to get to the right.

$$\sum_{j=1}^{k+1}(2j - 1) = 1 + 3 + \ldots + (2k - 1) + (2(k + 1) - 1) \quad \text{definition of sum}$$

$$= \sum_{j=1}^{k}(2j - 1) + (2k + 1) \quad \text{separating, simplifying the last term}$$

$$= k^2 + 2k + 1 \quad \text{Inductive hypothesis}$$

$$= (k + 1)^2 \quad \text{factoring}$$

We've shown that if the formula is true for $n = k$ then it is true for $n = k + 1$, so by the Principle of Mathematical Induction it is true for all $n \geq 1$. □

Example 3.2.7: Prove Theorem 3.1.9(a)

$$\sum_{j=1}^{n} j^2 = \frac{n(n + 1)(2n + 1)}{6}, \qquad n = 1, 2, 3...$$

Proof is by induction.
Base:

$$\sum_{j=1}^{1} j^2 = 1^2 = 1 \quad \text{and} \quad \frac{(1)(1 + 1)(2(1) + 1)}{6} = \frac{(1)(2)(3)}{6} = 1$$

Thus the formula holds when $n = 1$.

Inductive: Next we assume that

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

and show that this leads to

$$\sum_{j=1}^{k+1} j^2 = \frac{(k+1)[(k+1)+1][2(k+1)+1]}{6}$$

This one is a little long, so stay with me.

$$\begin{aligned}
\sum_{j=1}^{k+1} j^2 &= 1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 && \text{definition of sum} \\
&= \left(\sum_{j=1}^{k} j^2\right) + (k+1)^2 && \text{separate the last term} \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 && \text{Inductive hypothesis} \\
&= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} && \text{Common denominator} \\
&= \frac{(k+1)\,(\,k(2k+1) + 6(k+1)\,)}{6} && \text{factor out } k+1 \\
&= \frac{(k+1)(2k^2+7k+6)}{6} && \text{expand what's left} \\
&= \frac{(k+1)(k+2)(2k+3)}{6} && \text{factor again} \\
&= \frac{(k+1)[(k+1)+1][2(k+1)+1]}{6} && \text{write in terms of } k+1
\end{aligned}$$

We've shown that if the formula is true for $n = k$ then it is true for $n = k + 1$, so by the Principle of Mathematical Induction it is true for all $n \geq 1$. $\square$

Note that to get from the the fourth line to the sixth line, *we factored first, then expanded what was left.* If we would have expanded the quantity $k(k+1)(2k+1)+6(k+1)^2$, we would have gotten $2k^3 + 9k^2 + 13k + 6$. That's not so easy to factor!

We'll finish by proving Theorem 3.1.15 from Section 3.1:

Theorem 3.1.15 For the arithmetic sequence defined recursively by

$$a_1 = A, \quad a_{n+1} = a_n + d$$

We have that

(a) $a_n = A + (n-1)d, \quad n = 1, 2, 3 \ldots$

(b) $\displaystyle\sum_{i=1}^{n} a_i = An + \frac{n(n-1)}{2}d$

(a) Proof is by induction.

Base: $a_1 = A + (1-1)d = A$ as required.

Inductive: Assume $a_k = A + (k-1)d$ and try to prove $a_{k+1} = A + kd$.

a_{k+1}	$= a_k + d$	definition of arithmetic sequence
	$= A + (k-1)d + d$	Inductive hypothesis
	$= A + kd$	algebra

So by the Principle of Mathematical Induction, $a_n = A + (n-1)d$ for all $n \geq 1$. □

(b) Proof is by induction.

Base:

$$\sum_{i=1}^{1} a_i = a_1 = A = A(1) + \frac{1(1-1)}{2}d$$

Inductive: Assume

$$\sum_{i=1}^{k} a_i = Ak + \frac{k(k-1)}{2}d$$

and try to prove that

$$\sum_{i=1}^{k+1} a_i = A(k+1) + \frac{(k+1)k}{2}d$$

$$\begin{aligned}
\sum_{i=1}^{k+1} a_i &= a_1 + a_2 + \ldots + a_k + a_{k+1} && \text{Definition of sum} \\
&= \left(\sum_{i=1}^{k} a_i\right) + a_{k+1} && \text{separate last term} \\
&= \left(Ak + \frac{k(k-1)}{2}d\right) + (A + kd) && \text{Inductive hypothesis and part (a)} \\
&= A(k+1) + \left(\frac{k^2 - k}{2} + k\right) d && \text{algebra} \\
&= A(k+1) + \left(\frac{k^2 - k + 2k}{2}\right) d && \text{common denominator} \\
&= A(k+1) + \left(\frac{(k+1)k}{2}\right) d && \text{factor}
\end{aligned}$$

So by the Principle of Mathematical Induction the formula is correct for all $n \geq 1$. □

We'll omit the proof of Theorem 3.1.17. I did not include it as an official "Problem", but it's a good exercise to consider how you would prove it.

Theorem 3.1.17 For the geometric sequence defined recursively by

$$a_0 = A, \quad a_{n+1} = ra_n$$

We have that

(a) $a_n = Ar^n, \quad n = 0, 1, 2 \ldots$

(b) $\displaystyle\sum_{i=1}^{n} a_i = A\left(\frac{r^{n+1} - 1}{r - 1}\right)$

3.2.4 Problems

Problem 3.2.8: Prove that each of the following recursively defined sequences has the given explicit formula.

(a) Let $a_0 = 3$ and $a_{n+1} = 2a_n$. Prove that $a_n = 3(2)^n$.

(b) Let $a_1 = 3$ and $a_{n+1} = 2a_n + 1$. Prove that $a_n = 2^{n+1} - 1$.

Problem 3.2.9: Use mathematical induction to prove that n^3+2n is divisible by 3 for all $n \geq 1$.

Problem 3.2.10: Use induction to prove the formula you guessed in Problem 3.1.19 for the sum

$$\frac{1}{2} + \frac{1}{6} + \frac{1}{12} + \ldots + \frac{1}{n(n+1)} = \sum_{i=1}^{n} \frac{1}{i(i+1)}$$

Problem 3.2.11: Use induction to prove the formulas.

(a) Theorem 3.1.7

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

(b) Theorem 3.1.9(b)

$$\sum_{j=1}^{n} j^3 = \left[\frac{n(n+1)}{2}\right]^2$$

Problem 3.2.12:

(a) Use induction to prove your conjecture from Problem 3.1.22(a). *You will need to use the recursion formula for the Fibonacci sequence for the proof*, along with the standard inductive step.

(b) Use induction to prove your conjecture from Problem 3.1.22(b).

3.3 Characteristics