Discrete Math Notes - Steven Senger

1 Logic

1.1 Propositional logic

HOMEWORK: 1.1 # 1–4

- statement, proposition, compound, truth table,
- not, or, xor, and, implication, double implication, iff,
- hypothesis, conclusion, inverse, converse, contrapositive

1.1.1 Propositions

A **statement** or **proposition** is a declarative sentence that can be either true or false, but not both. A **compound proposition** is a proposition made of a combination of propositions.

Example 1.1.1. *These are two declarative sentences.*
"The sky is red." This has a single truth value.
"This sentence is false." This does NOT have a truth value.

The six basic operations on propositions are:

negation (not)	assert the opposite	$\neg$
conjunction (and)	true when both are true, false otherwise	$\wedge$
disjunction (or)	false when both are false, true otherwise	$\vee$
exclusive or (xor)	false when they match, true otherwise	$\oplus$
implication (if, then)	false when first true and second false, and true otherwise	$\rightarrow$
double implication (if and only if, "iff")	true when same, false when different	$\leftrightarrow$

Note that 'or' above is assumed to be the "inclusive or," which is true if either input is true. An example of an inclusive or would be, "You should bring a pen or pencil." In that case, it's understood that you could bring both. However, in colloquial speech, we sometimes use the word 'or' as an "exclusive or," which is only true if the two inputs have different truth values. An example of an exclusive or would be, "Either we could go to the pool or we could watch a movie, but we don't have time for both." Sometimes the context is less clear in spoken language, so be careful!

In an implication, $p \to q$, we often call p the **hypothesis**, and q the **conclusion**. You also might hear that p is **sufficient** for q, and that q is **necessary** for p. Given an implication, $p \to q$, its **converse** is $q \to p$. Its **contrapositive** is $\neg q \to \neg p$, which is logically equivalent to the original implication. Finally, its **inverse** is $\neg p \to \neg q$.

Some equivalent English statements for $p \to q$ are: "if p, then q," "if p, q," "p, implies q," "if p, therefore q," "p only if q," "q if p," "p is sufficient for q," "q is necessary for p."

We often use T and F to represent 'true' and 'false' respectively. Then when we know the truth values of some propositions, we can plug T or F in to a compound proposition to get its truth value, according to the rules given above.

Example 1.1.2. *Suppose p is true and q is false. Evaluate $p \vee q$.*
Solution: *We start with $p \vee q$, and plug in the truth values of p and q to get $T \vee F$. By the definition of disjunction (inclusive or), we get a final answer of T, for true.*

Example 1.1.3. *Let p and q both be true, and r be false. Evaluate $(p \wedge q) \to r$.*
Solution: *We start with $p \wedge q$, and plug in the truth values of p and q to get $T \wedge T$, which by the definition of conjunction (and), evaluates to T. Next we put this back in with the rest of the implication to get $T \to r$. Plug in F for r, and we see that we have, $T \to F$, the only case when an implication is false, giving us a final answer of F.*

A **truth table** is a list of all possible truth values of a collection of propositions, paired with the resulting truth values of a compound proposition. Two propositions are said to be **logically equivalent** if they have the same truth table.

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \to q$	$p \leftrightarrow q$
T	T	F	T	T	F	T	T
T	F	F	F	T	T	F	F
F	T	T	F	T	T	T	F
F	F	T	F	F	F	T	T

1.1.2 English sentences

We might have to modify a few words here and there, but it is important to be able to translate between symbolic logic and English sentences. Otherwise, you might end up falling prey to any number of logical fallacies, or have trouble communicating your ideas precisely.

Example 1.1.4. *Let p = "the sky is blue," q = "my shoes are wet," and r = "it is raining." Now write the following sentence using symbols. "If the sky is blue or it is raining, but not both, then my shoes are wet."*
Solution $(p \oplus r) \to q$.

Example 1.1.5. *With the same propositions as above, translate the following into English, $q \leftrightarrow (p \wedge r)$.* **Solution:** *"My shoes are wet if, and only if, both the sky is blue and it is raining."*

1.1.3 Homework

Problem 1.1.1. You are ordering dinner, and your server says that your meal comes with a side of soup or salad. Is this more likely to be an "inclusive or," or an "exclusive or?"

Problem 1.1.2. Suppose p is true, while q and r are both false. Evaluate the following: (a) $(p \to q) \vee r$, (b) $\neg(p \vee q) \wedge r$, and (c) $\neg(p \wedge q)$.

Problem 1.1.3. Write out the truth table for $p \to (q \vee r)$. You have three variables, so you will need a total of eight possible combinations of true and false.

Problem 1.1.4. Let p stand for, "the sky is blue," and let q stand for, "my shoes are wet." Translate this sentence to symbols: "The sky is blue if and only if my shoes are wet."

Problem 1.1.5. Given that p and q are true and r is false, evaluate $(p \wedge q) \to (r \vee p)$.

Problem 1.1.6. Given that p and q are false and r is true, evaluate $(p \vee q) \to (q \wedge r)$.

1.2 Logical equivalence

HOMEWORK: 1.2 # 1–4

- tautology, contradiction, logical equivalence, De Morgan's Laws

A proposition that is always true is called a **tautology**. We will give an example of a tautology as well as a gentle example of a proof below.

Example 1.2.1. *The compound proposition $p \vee \neg p$ is a tautology.*

Proof. We will view the inclusive or ($\vee$) as a function that takes two inputs, p and $\neg p$, and returns some output. Notice that because p is a proposition, it is either true or false. If p is true, then the whole thing evaluates to true, because $\vee$ only needs one of its inputs to be true to return a true value. If p is false, then even though p inputs a false to the $\vee$, the $\neg p$ will input a true, making the $\vee$ output a true. So regardless of the truth value of p, the compound proposition $p \vee \neg p$ is true. □

On the other hand, a proposition that is always false is called a **contradiction**, such as $p \wedge \neg p$. We say that p and q are **logically equivalent** iff (remember, 'iff' means "if and only if") $p \leftrightarrow q$ is a tautology. We sometimes write $p \equiv q$.

Example 1.2.2. *Prove that $(p \to q) \vee (p \to \neg q)$ is a tautology.*
Solution 1: *We construct a truth table. Recall that the inputs are to the left of the double vertical line, and the outputs are to the right. If you chose to record some different output columns on the right side, or organized things a little differently, don't worry! Just make sure that you have covered every possible case, and that you can find every possible output in your table. In the table below, notice that the outcome (the central 'or' column) is always true.*

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

Solution 2: *Alternately, we could have just argued the same facts presented in the truth table using English. Here is one such argument. The first implication is always true unless the truth values of p and q are true and false, respectively. But in that case, the second implication is true. Since the two implications are connected by an inclusive or, we only need one of them to be true for the whole expression to evaluate as true. Hence, it is true in any case, and therefore a tautology.*

1.2.1 De Morgan's Laws

In this class, we will encounter more than one result called "De Morgan's Laws." They all have a similar feel, even though their statements may look quite different superficially.

Theorem 1.2.1 (De Morgan's Laws)**.**

$$(i) \quad \neg(p \wedge q) \equiv \neg p \vee \neg q$$

$$(ii) \quad \neg(p \vee q) \equiv \neg p \wedge \neg q$$

Proof. To prove (i), we will appeal to a truth table. The first column to the right of the double line is $p \wedge q$, which is then negated in the second column. The third column is $\neg p \vee \neg q$, which has equivalent values to the second column, thus proving their equivalence. Note that you might organize your truth table differently, and that is okay, as long as you explain what is going on.

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

To prove (ii), we translate each compound proposition to English, and verify their equivalence. The proposition $\neg(p \vee q)$ says, "It is not the case that either p or q or both are true." This is the same as saying that neither of them can be true, which is the same as saying, "Both of p and q are false." That is the same as saying, "p is false and q is false," which is exactly what $\neg p \wedge \neg q$ means. □

1.2.2 Homework

Problem 1.2.1. Prove that $p \wedge \neg p$ is a contradiction. You can use Example 1.2.1 as a guide.

Problem 1.2.2. Show that $p \equiv \neg(\neg p)$ in English, and using a truth table.

Problem 1.2.3. Show that $\neg(p \wedge \neg q) \equiv (p \to q)$ using a truth table.

Problem 1.2.4. Show that $p \to q$ is logically equivalent to its contrapositive.

Problem 1.2.5. Rewrite the statement and proofs of De Morgan's Laws a few times until you can do so by heart. There won't be much memorizing in this class, but this will be good practice for what comes later.

Problem 1.2.6. Show that $\neg(p \wedge q)$ is not logically equivalent to $(\neg p) \wedge (\neg q)$.

Problem 1.2.7. Show that $\neg(p \vee q)$ is not logically equivalent to $(\neg p) \vee (\neg q)$.

1.3 Predicates and quantifiers

HOMEWORK: 1.3 # 1–4

- universal quantifier, existential quantifier, counterexample,

- uniqueness quantifier, DeMorgan negation, $P(x)$

Recall from basic sentence construction that the **subject** of a sentence is the actor, and the **predicate** of the sentence is the action. This area of mathematics is sometimes called predicate logic for that very reason. Let $P(x)$ be a statement depending on x. So instead of just p from before, which is just defined as some sentence, this new type of statement will be a sentence that has a variable or input.

Example 1.3.1. *Let $P(x) =$ "x is an even number." Then the statement $P(2)$ is true, while the statement $P(7)$ is false. The statement $P($raisin bran$)$ is false. Even though it's a 10/10 cereal, it's not actually a number, so it can't be an even number.*

1.3.1 Single quantifiers

So, it can be a little disheartening to stare down a page full of new symbols and try to derive meaning from them. I don't introduce these new symbols lightly though. What we will see in this class is that while natural language is comparatively easier to speak and understand, it relies a LOT on context, and sometimes that context is not entirely clear. Recall the distinction between 'inclusive or' and 'exclusive or' from before. Things can get even pricklier if we have a sentence like, "I was busy suplexing a shark wearing a bolo tie," from Mr. Torgue in Borderlands 2. The question there is, who was wearing the bolo tie, Mr. Torgue or the shark? In mathematics, we try to tamp down this potential vagueness by relying on some very common phrases like, "such that," and "for which." Because mathematical sentences can get really wordy and repetitive, we have a whole bunch of shortcut symbols.

The **universal quantifier**, $\forall$, is used to make statements about all, each, or every element in the subject.

Example 1.3.2. *"$\forall$ coffee shop, there is at least one customer that insists on pronouncing the word, 'croissant,' in the most annoying and incorrect way imaginable."*
You could read this aloud as, "For every coffee shop..." or "At each coffee shop..." or many other ways. Also, of course this customer doesn't even want a croissant. They just want everyone in the establishment to know that they have totally been to Paris.

A **counterexample** is an element in the subject that does not obey the predicate, therefore showing the invalidity of a statement with a universal quantifier.

Example 1.3.3. *Let $P(x)$ be the statement x is odd. Then the claim, "$\forall$ prime numbers x, $P(x)$," claims that all prime numbers are odd. However, we know this two be false, because of the counterexample, $x = 2$.*

The **existential quantifier**, $\exists$, is used in positing the existence of an object with the stated features. When it is followed by an exclamation point, it asserts that not only does such an object exist, but that it is moreover unique. Also, a colon in an existential statement is often used to mean, "such that," or "for which."

Example 1.3.4. *Consider the statement, "$\exists! x : x$ is prime and x is even." This is a true statement because there is exactly one even prime, 2. This claim would be false if there were no even primes or if there were more than one even prime.*

Here is De Morgan's name popping up again. After going through this, try to compare it to the other De Morgan Laws we saw earlier and try to see the similarities.

Theorem 1.3.1 (De Morgan negation)**.**

$$(i) \quad \neg(\exists x : P(x)) \equiv \forall x, \neg P(x)$$

$$(ii) \quad \neg(\forall x, P(x)) \equiv \exists x : \neg P(x)$$

Proof. To see (i), translate it to English. The left side says, "It is not the case that there exists an x for which $P(x)$ is true." That is the same as saying that for every x, $P(x)$ is false, which is precisely what the right side says. To prove (ii), consider the left hand side. It says that it is not the case that every x satisfies $P(x)$. That is the same as saying that there is an x for which $P(x)$ does not hold, which is exactly what the right side says. □

1.3.2 Nested quantifiers

Expression	Meaning
$\forall x, \forall y, P(x, y)$ or $\forall y, \forall x, P(x, y)$	$P(x, y)$ holds for every pair of x and y.
$\forall x, \exists y : P(x, y)$	For every x, there is a specific y for which $P(x, y)$ holds
$\exists x : \forall y, P(x, y)$	There is an x such that $P(x, y)$ holds for every y.
$\exists x : \exists y : P(x, y)$ or $\exists y : \exists x : P(x, y)$	There is a specific pair, x and y, for which $P(x, y)$ holds.

Recall that $\exists! x$ (there is a *unique* x), is very different from $\exists x$ (there is an x, possibly not unique).

Example 1.3.5. *We can translate, "Everyone has exactly one favorite animal," as "* $\forall$ *people,* $\exists!$ *favorite animal."*

Keep in mind that many of the statements we consider in this section are false. Also, the order of the variables may be important.

Example 1.3.6. *Let* x *and* y *be elements of the set of people. Let* $P(x, y)$ *mean "*x *has respect for* y*."*

Expression	*Meaning*
$\forall x, \exists y : P(x, y)$	*"Everyone respects someone."*
$\forall y, \exists x : P(x, y)$	*"Everyone is respected by someone."*
$\exists x : \forall y, P(x, y)$	*"There is someone that respects everyone."*
$\exists y : \forall x, P(x, y)$	*"There is someone that everyone respects."*

Example 1.3.7. *Let* x *and* y *be elements of the set of real numbers. Let* $P(x, y)$ *mean "*$x \geq y$*."*

Expression	*Meaning*
$\forall x, \exists y : P(x, y)$	*"Every real number is bigger than or equal to some real number."*
$\forall y, \exists x : P(x, y)$	*"For every real number, there is real number bigger than or equal to it."*
$\exists x : \forall y, P(x, y)$	*"There is a real number that is greater than or equal to all real numbers."*
$\exists y : \forall x, P(x, y)$	*"There is a real number that is less than or equal to all real numbers."*

Now let's look at some more complicated situations.

Example 1.3.8. *Let* $P(x, y)$ *mean "*x *eats* y*," and suppose that* x *and* y *are types of animals. Symbolically express, "Every animal eats some other type of animal."*

Solution: *There is subtle issue here with the word "other." We could try, "* $\forall x, \exists y : P(x, y)$*," but this doesn't quite cut it. What's the problem? This doesn't preclude the possibility that there's some type of animal that only eats its own species, and the statement in quotes explicitly says, "other type of animal." How can we handle this? We just need to put in the caveat that* x *isn't the same type of animal as* y*, or simply* $x \neq y$*. Since we need this AND* $P(x, y)$ *to hold, we will use the logical conjunction (and) from before. This gives us a final answer of,*

$$\text{“ } \forall x, \exists y : (P(x, y) \wedge (x \neq y)).$$

Example 1.3.9. *Let $P(x, y)$ mean "x likes y," and suppose that x, y, and z are people. Convert this to English,*

$$\text{“ } \forall z, \exists x : \exists y : ((x \neq y) \wedge (P(z, x) \wedge P(z, y))).\text{”}$$

Solution: *We start by noticing that this statement is universal in z, and existential for x and y. So it's saying that for every z, there exist an x and a y that have certain properties. These properties are tied up with some 'and' conditions. The first one is $x \neq y$, which just tells us that x and y are different people. Finally, we encounter our P statements, that z likes x and z likes y. So, putting this all together, we get that for every z, there are two people x and y that z likes. Notice that if we didn't specify that $x \neq y$, we could potentially have z just liking one person, who happens to be referred to by x as well as y. So our final translation for this is, "Everyone likes at least two people."*

1.3.3 Homework

Problem 1.3.1. Let x, y, and z be real numbers. Translate this into English. “ $\forall x, \forall y, \exists z : x + y = z$.”

Problem 1.3.2. Let x and y be choices in the game Rock, Paper, Scissors. Translate this into English. “ $\forall x, \exists! y : x$ beats y.”

Problem 1.3.3. Write this using the fancy new symbols from this section to express the following: “Everyone likes at least one person.”

Problem 1.3.4. Write this using the fancy new symbols from this section to express the following: “Everyone likes at least one other person.” Note that in contrast to the previous problem, we have to take care of the word, “other.”

Problem 1.3.5. Translate to symbols, “One person likes everyone.”

Problem 1.3.6. Translate to symbols, “There are two people that like each other.”

Problem 1.3.7. Translate to symbols, “No two people like each other.”

1.4 Introduction to proofs

- theorem, axiom, proof, even, odd, rational,

- types of proofs: direct, contraposition, contradiction, cases,

An **axiom** is a statement that is generally accepted to be true. A **theorem** is a statement that can be logically deduced from axioms. A **proof** is this series of logical deductions. We say that an integer, n, is **even** if there exists some integer, k, such that $n = 2k$. An integer is **odd** if it is not even, and therefore, there must be an integer, k, such that $n = 2k + 1$. A number is **rational** if it can be written as a ratio of two integers, in lowest terms, with the denominator nonzero.

A **direct proof** follows a line of logical implications.

Example 1.4.1. *Show that if n is even, then n^2 is also even.*

Proof. Since n is even, there exists an integer, k, such that $n = 2k$. Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Since $2k^2$ is an integer, we have that n^2 is equal to 2 times an integer, and is therefore even. □

A **proof by contraposition** is where we have a statement $p \to q$, and prove the contrapositive of the statement, $\neg q \to \neg p$, which is logically equivalent to the original statement.

Example 1.4.2. *Suppose n is an integer. Show that if n^2 is even, then n is even.*

Proof. We will proceed by contraposition. Consider the original statement as $p \to q$, where $p =$ "n^2 is even," and $q =$ "n is even." The contrapositive is $\neg q \to \neg p$. So we will assume that n is odd ($\neg q$), and show that it implies that n^2 is odd ($\neg p$). Since n is odd, there is an integer, k, such that $n = 2k + 1$. So $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is one more than twice an integer, and therefore odd. □

A **proof by way of contradiction** (often abbreviated **BWOC**), is where we assume the opposite of what we want to prove, and derive a contradiction in the very fabric of logic, thereby proving that the false statement was our assumption. Think of it like proving someone's innocence by showing that there is no way that the person is guilty.

Example 1.4.3. *$\sqrt{2}$ is not rational.*

Proof. We will proceed by way of contradiction (BWOC). Suppose that $\sqrt{2}$ is rational. Then there exist integers, p and q such that $\sqrt{2} = \frac{p}{q}$, in lowest terms, with q nonzero. Squaring both sides of our equality yields $2 = \frac{p^2}{q^2}$, which means that $2q^2 = p^2$. Since p^2 is two times an integer, it must be

even. By Example 1.4.2, above, we see that p must also be even. So there is some integer, k, such that $p = 2k$. Then $2q^2 = (2k)^2 = 4k^2$. Dividing both sides by two gives us that $q^2 = 2k^2$, which means that q^2 is twice an integer, and therefore also even. Reasoning as before, by using Example 1.4.2, we see that q must also be even. But this means that the fraction, $\frac{p}{q}$, was not in lowest terms (the top and bottom are both divisible by two) to begin with– contradiction! □

A **proof by cases** is where we exhaust all possibilities by breaking things up into a (relatively) small number of cases, and handling each case separately.

Example 1.4.4. *Show that for any natural numbers, a, b, and n, such that $ab = n$, we have that either $a \geq \sqrt{n}$ or $b \geq \sqrt{n}$.*

Proof. We prove this by cases. In one case, $a \geq \sqrt{n}$, and in the other case, $a < \sqrt{n}$. Well, in the first case, we are already done, so now we examine the second case. If $a < \sqrt{n}$, then we can multiply both sides of that inequality by b to get

$$ba < b\sqrt{n},$$

but recall that $ba = ab = n$. So this implies that

$$n = ba < b\sqrt{n}.$$

Now, we divide both sides by $\sqrt{n}$ and get

$$\sqrt{n} < b,$$

which implies that $b \geq \sqrt{n}$, and we see that we are done in the second case as well. □

Occasionally, we will use the acronym **WLOG** to mean "Without Loss Of Generality." This is employed when an almost identical proof would deal with each of many cases, but with only slight alterations. When the alterations are obvious, we proceed without loss of generality.

1.4.1 Homework

This section is different. Please practice these proofs until you can rewrite them from memory. I know that sounds annoying. There won't be a whole lot of memorization in this class, but learning how to learn proofs is an important skill. My advice is to get a blank sheet of paper and hide these notes. Start writing the proofs from memory until you get stuck. Look at the notes briefly to jog your memory, then hide them and keep writing. Once you finish a proof, cover up what you've written and start again. Do this until you can reproduce each of these from memory.

2 Set theory

2.1 Sets

HOMEWORK: 2.1 # 1–6

- sets, elements, empty set, subsets, cardinality, power set, Cartesian product

2.1.1 Primitive notions

A **set** is an unordered collection of objects called **elements**. You may notice that this is not a good definition. For the purposes of this class, we will assume that a set is just an unordered list of things. Also, for the moment, we will have no notion of "how many times" something is on a list. Either a thing is on the list or it isn't. In fact, what we have above isn't really a definition so much as it expresses a relationship and desperately hopes that you don't look to closely. This is because things can get really nasty if we start looking at sets that can contain themselves.

Example 2.1.1. *The Barber of Seville shaves only those that don't shave themselves. Obviously everyone is shaved, because it's a silly story. Now, who shaves the Barber? If he shaves himself, then he can't be shaved by the Barber of Seville. So clearly he can't shave himself, which means he doesn't shave himself, and is therefore shaved by the Barber of Seville. But we just decided that he can't shave himself! Therein lies the paradox.*

The previous example is based on Russel's paradox, which defines a set S as the set of all sets that don't contain themselves. So, similar to the conundrum of the Barber of Seville, S simultaneously must contain itself and cannot contain itself. We won't delve too far into this here, but it is worth being aware that there are problems with the version of set theory that we will work with in this class. As far as this class is concerned, we will typically just assume that sets cannot contain themselves, for simplicity's sake. For more information on how to avoid such problems, look up Zermelo-Fraenkel set theory and get ready for a deep dive.

2.1.2 Basic notation

If an element, a is in a set, A, then we write $a \in A$. If not, we write $a \notin A$. We list the elements in a set either explicitly, or by rules, between $\{$ and $\}$. The colon that appears inside of the curly braces can be interpreted as "such that."

Example 2.1.2. *We can write $A = \{1, 2, 3\}$, as an explicit definition of a set. We can write $E = \{x : x \text{ is an even natural number}\}$ to mean that E is the set of even natural numbers. The definition is read "E is the set consisting of all x such that x is an even natural number."*

Some important sets are: $\mathbb{N}$ = the set of natural numbers, $\mathbb{Z}$ = the set of integers, $\mathbb{Q}$ = the set of rational numbers, $\mathbb{R}$ = the set of real numbers, and $\varnothing$ which is the **empty set**, or set containing no elements. We also have the following interval notation.

(a, b)	$a < x < b$	**open interval**
$[a, b]$	$a \leq x \leq b$	**closed interval**
$[a, b)$	$a \leq x < b$	**half-open interval**
$(a, b]$	$a < x \leq b$	**half-open interval**

Two sets are said to be **equal** if they consist of exactly the same elements. If everything under consideration is understood, we call the set containing all possible elements the **Universe**, and is often denoted by the set U.
If every element in a set A is also an element in a set B, then we say A is a **subset** of B. We write $A \subseteq B$. To write this succinctly with symbols,

$$A \subseteq B \leftrightarrow \forall a \in A, a \in B.$$

Note, $\varnothing$ is a subset of every set. Now, $A \subseteq B$ and there are elements in B which are NOT in A, we say that A is a **proper subset** of B. That is to say, A is a subset of B, but $A \neq B$. Some books will write $A \subset B$ or $A \subsetneq B$ to indicate this. We can say that $\mathbb{Z}$ is a proper subset of $\mathbb{R}$, because every integer is a real number, but not every real number is an integer.

2.1.3 Trickier bits

However, things can get tricky if we let sets be elements of sets. Note that we are still not concerned with sets that are elements of themselves, as in Russel's paradox above, but things are nonetheless easy to mess up. Read the next two examples very carefully. This is a minor point, but it's worth taking a minute to understand.

Example 2.1.3. *Let T denote the set of football teams in the NFL. Let P denote the set of players of the team, the Chiefs. Suppose that x stands for Patrick Mahomes. Now, notice that x is an element of P, because x is a player on the Chiefs. However, if I asked you to list out all of the teams in the NFL, you wouldn't write down x as the name of a team, so x is NOT an element of the set T, even though x clearly plays for the NFL.*

Example 2.1.4. *Let* $A := \{1\}, B := \{1,2\}, C := \{\{1\},2\}$, *and* $D := \{1,2,\{1\}\}$.
Now, A *is a subset of* B *because every element in* A *is an element of* B. *However,* A *is NOT a subset of* C, *because* 1 *is not itself an element in* C *(that is,* 1 *is not listed on its own within the braces defining* C*; it's inside of another set inside of* C*.). There is an element in* C *which is a set containing the element 1. This happens to be the same as the set* A, *so* A *is an element of* C, *but not a subset. For similar reasons,* B *is not a subset of* C *(If that doesn't make sense yet, read the next paragraph and come back to this later). Now, consider* D. A *is both an element of AND a subset of* D, *because every element in* A *is and element in* D. *Look at all of the elements of* B, *and notice that each element from* B *is listed on its own in* D, *so* B *is a subset of* D. *Finally,* B *is not an element of* D *because the set,* $\{1,2\}$ *isn't listed inside of the braces defining* D.

If S is a set with exactly n elements, we write $|S| = n$. This is called the **cardinality** of S. If $n < \infty$, then S is **finite**. If S is not finite, then it is **infinite**. The set of all subsets of a set S is called the **power set** of S, and is denoted $\mathcal{P}(S)$ or 2^S.

Example 2.1.5. *Let* $A := \{1,2,3\}$. *We can see that* $|A| = 3$, *and its power set is*

$$\mathcal{P}(S) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}.$$

Notice that $|\mathcal{P}(S)| = 8$, *which is* 2^3.

The **Cartesian product** of two sets, A and B is

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

Example 2.1.6. *The Cartesian product* $\{2,3\} \times \{w,-1\}$ *is the set*

$$\{(2,w),(2,-1),(3,w),(3,-1)\}.$$

Here is a bigger example.

Example 2.1.7. *The Cartesian product* $\{1,2,3,4\} \times \{a,b,c\}$ *is the set*

$$\{(1,a),(2,a),(3,a),(4,a),(1,b),(2,b),(3,b),(4,b),(1,c),(2,c),(3,c),(4,c)\}.$$

Notice that there is no arithmetic multiplication occurring. The familiar xy-plane (also known as that Cartesian coordinate plane) is $\mathbb{R} \times \mathbb{R}$, and is often denoted $\mathbb{R}^2$.

2.1.4 Homework

Problem 2.1.1. Consider the sets $\mathbb{N}$ and $[0, 13)$. What elements are in both sets?

Problem 2.1.2. What elements are in the set $\varnothing$?

Problem 2.1.3. If $\exists a \in A : a \in B$, is it necessary that $A \subseteq B$? Is it possible?

Problem 2.1.4. Explain in English why $1 \notin \{\{1\}\}$.

Problem 2.1.5. Compute $|\mathcal{P}(\{a, b, c, d, e\})|$.

Problem 2.1.6. Let $A := \{1, 2, 3, 4, 5, 6, 7, 8\}$, and let $B := \{a, b, c, d, e, f, g, h\}$. Without writing out the whole set, describe $A \times B$.

Problem 2.1.7. Write out the elements of the Cartesian product of $\{1, 2, 3\}$ with itself.

Problem 2.1.8. How many elements are in the Cartesian product of $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ with itself?

2.2 Set operations

HOMEWORK: 2.2 # 1–6

- union, intersection, complement, difference, disjoint, Venn diagrams

Given two sets, A and B, the **union** of the two sets is the set of all elements that are in either A OR B or both, and is written $A \cup B$. The **intersection** of the two sets is the set of all elements that are in both A AND B, and is written $A \cap B$. Notice that in natural language, there could be ambiguity in how we speak of sets, as the following example shows.

Example 2.2.1. *Let E be the set of players on the soccer team for England and F be the set of players for the soccer team from France. Suppose these teams are playing a match. You could answer the question, "Who is playing soccer right now?" by saying, "England and France," but set theoretically, you would mean $E \cup F$, not $E \cap F$.*

Two sets are called **disjoint** if their intersection is nothing. The **complement** of a set A is the set of all elements in the universe NOT in A, and is written $\overline{A}, A', A^c$, and many other ways. The **difference** or, "set-minus," of two sets is the set of elements in the first but NOT in the second, and is written $A \setminus B$.

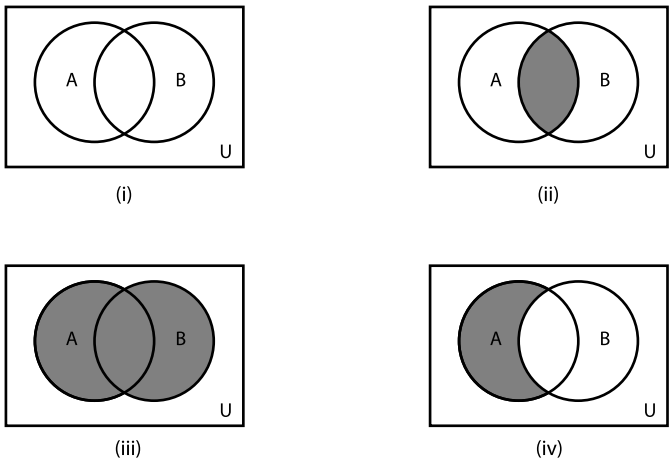


Figure 1: Some Venn diagrams with sets A, B, and universe, U. (i) shows $\varnothing$, (ii) shows $A \cap B$, (iii) shows $A \cup B$, and (iv) shows $A \setminus B$.

Example 2.2.2. *Let* $A := \{1, 2, 3\}, B := \{2, 3, 4\}, C := \{4, 5\}$ *and the universe,* $U := \{1, 2, 3, 4, 5\}$. *Then we can compute some simple set operations.*
$A \cup B = \{1, 2, 3, 4\}$,
$A \cap B = \{2, 3\}, \overline{A} = C$, *and* $B \setminus A = \{4\}$. *Also, notice that* A *and* C *are disjoint.*

We can write each of these operations in symbols and set builder notation as follows:

$$\begin{aligned} A \cup B &= \{x : (x \in A) \vee (x \in B)\} \\ A \cap B &= \{x : (x \in A) \wedge (x \in B)\} \\ \overline{A} &= \{x : (x \in U) \wedge (x \notin A)\} \\ A \setminus B &= \{x : (x \in A) \wedge (x \notin B)\} \end{aligned}$$

A **Venn diagram** is a picture showing all possible intersections and unions of a collection of sets. See Figure 1 for some examples of Venn diagrams made with two sets and a universe.

2.2.1 Homework

Problem 2.2.1. Suppose $E := \{1, 2, 3\}$, and $F := \{3, 4, 5\}$. Compute $E \cap F$, $E \cup F$, $E \setminus F$, and $F \setminus E$.

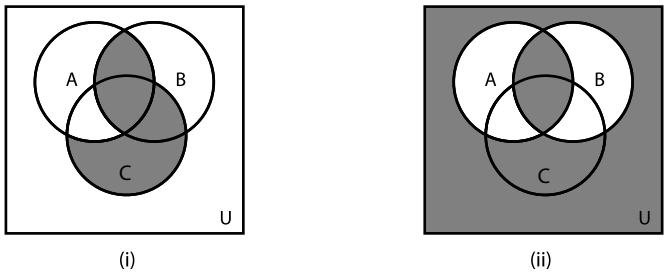


Figure 2: See Problem 2.2.5

Problem 2.2.2. Suppose that two finite sets, X and Y, are disjoint. How many elements are in $(X \cup Y)$?

Problem 2.2.3. Prove or disprove: $\forall$ sets A and B, $(A \cap B) \subseteq (A \cup B)$.

Problem 2.2.4. Given sets A and B, suppose $(A \setminus B) = (B \setminus A)$. Prove that $A = B$.

Problem 2.2.5. Figure 2 shows two Venn diagrams with three sets each. Write out how you would describe the shaded regions with set theoretical notation.

Problem 2.2.6. Draw Venn diagrams for the following: $A \cap B \cap C$, $A \setminus (B \cup C)$, and $\overline{A} \cup (B \cap C)$.

Problem 2.2.7. Draw Venn diagrams for the following: $A \cap (B \cup C)$, $A \setminus (B \cap C)$, and $\overline{A} \cap (B \cup C)$.

Problem 2.2.8. Suppose that two finite sets, X and Y, are NOT disjoint. What is the maximum number of elements in $(X \cup Y)$?

3 Functions

3.1 Function basics

HOMEWORK: 3.1 # 1–4

- function, domain, codomain, range, inverse, one-to-one, onto, bijection, factorial, floor, ceiling

3.1.1 Basic definitions

A **function**, f, from a set, A, to a set, B, is an assignment of every element in A to exactly one element in B. Note that there is a potential ambiguity in the natural language here. We do NOT mean that every element in A is necessarily mapped to the same element in B. Continuing, we write $f : A \to B$, and $f(a) = b$ or $f : a \mapsto b$, for $a \in A$ and $b \in B$. The set A is called the **domain**. The set B is called the **codomain** or **target**. Be careful not to confuse this with the **image** or **range**, which is the subset of elements in B which are mapped to by elements in A by f.

Example 3.1.1. *Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. Notice that the domain is $\mathbb{R}$, the set of all real numbers. Every real number has a square. The codomain is also $\mathbb{R}$. But notice that the range is not all of $\mathbb{R}$, as there are elements in $\mathbb{R}$ that are not mapped to, namely the negative numbers.*

The **graph** of f is $\{(a, b) : f(a) = b\}$, which is a subset of the Cartesian product $A \times B$. Notice that a graph in the plane can belong to a function only if it passes the Vertical Line Test, which is that it cannot touch any vertical line more than once.

3.1.2 Operations and attributes

Consider two functions, f and g. We write $(f + g)(x)$ to mean $f(x) + g(x)$. We write $(fg)(x)$ to mean $f(x)g(x)$. We write $(f \circ g)(x)$ to mean $f(g(x))$. Finally, f and g are **inverses** if $(g \circ f)(x) = (f \circ g)(x) = x$, for every x in the domains of f and g, respectively.

Example 3.1.2. *Let $f(x) = 2x + 1, g(x) = \frac{x-1}{2}$, and $h(x) = x^2$.*
Compute $f + g, fh, f \circ g, g \circ f, f \circ h$, and $h \circ f$.
$(f + g)(x) = f(x) + g(x) = 2x + 1 + \frac{x-1}{2} = \frac{5x+1}{2}$.
$(fh)(x) = f(x)h(x) = (2x + 1)x^2 = 2x^3 + x^2$.
$(f \circ g)(x) = f(\frac{x-1}{2}) = 2\frac{x-1}{2} + 1 = x$.
$(g \circ f)(x) = \frac{f(x)-1}{2} = \frac{2x+1-1}{2} = x$.
$(f \circ h)(x) = f(x^2) = 2x^2 + 1$.
$(h \circ f)(x) = h(2x + 1) = (2x + 1)^2 = 4x^2 + 4x + 1$.
In this case $f \circ g = g \circ f$, so f and g are inverses of one another. However, h and f are not inverses of one another.

A function, $f : A \to B$, is called **injective** or **one-to-one** (often abbreviated **1-1**) if every element in the range is associated to a unique element in the domain; if no two input values take the same output value. A function from $\mathbb{R}$ to $\mathbb{R}$ is one-to-one if it passes the Horizontal Line Test, that is,

the graph of f touches no horizontal line more than once. Notice that f is injective iff $f(a) = f(b) \to a = b$.

A function, $f : A \to B$, is called **surjective** or **onto** if every element in the codomain is associated to an element in the domain; if the range is the whole codomain. Notice that f is surjective iff $\forall b \in B, \exists a \in A : f(a) = b$. Also, a function is called **bijective** or a **one-to-one correspondence** iff it is both one-to-one and onto.

Example 3.1.3. *Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. This function is not one-to-one because there are multiple inputs that lead to the same output. For example, $f(-3) = 9 = f(3)$, but $-3 \neq 3$. It is also not onto, because it never has any negative numbers as output, but its codomain is all real numbers.*

Example 3.1.4. *Let $r : \mathbb{R} \to [0, \infty)$ be defined by $r : x \mapsto x^2$. This function is not one-to-one for the same reason that f in the previous example wasn't. However, it is onto, because for any output y, we can find a corresponding input $x = \sqrt{y}$ so that $r(x) = y$.*

Example 3.1.5. *Let $g : [0, \infty) \to \mathbb{R}$ be defined by $g(x) = x^2$. This function is one-to-one because it only uses positive numbers as inputs, so we never have two distinct inputs leading to the same output, as we did with the previous example. However, it is still not onto, because again, it never has any negative numbers as output, but its codomain is all real numbers.*

Example 3.1.6. *Let $h : \mathbb{R} \to \mathbb{R}$ be defined by $h(x) = x^3$. This function is one-to-one because it passes the Horizontal Line Test (sketch it and check).It is also onto, because any possible output, $y \in \mathbb{R}$, has a corresponding input, $x = y^{\frac{1}{3}}$. Therefore, $h(x)$ is a bijection.*

3.1.3 Special functions

The **factorial** (the exclamation point after a number) takes natural numbers and zero as input, and outputs natural numbers. For $n \in \mathbb{N}$, $n! = n \cdot (n - 1) \cdot \cdots \cdot 2 \cdot 1$. Also, $0! = 1$, by definition.

Example 3.1.7. $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$.

The **floor** function, $\lfloor x \rfloor$ takes a real number x and returns the greatest integer which is less than or equal to it.

Example 3.1.8. $\lfloor 2.1 \rfloor = 2, \lfloor 2.9 \rfloor = 2,$ *and* $\lfloor -1.1 \rfloor = -2$.

Similarly, the **ceiling** function, $\lceil x \rceil$ takes a real number x and returns the least integer which is greater than or equal to it. So if floor rounds down, ceiling rounds up.

3.1.4 Homework

Problem 3.1.1. Let $f(x) = 2x - 1, g(x) = \frac{x+1}{2}$, and $h(x) = x^2$.
Compute $f + g, fh, f \circ g, g \circ f, f \circ h$, and $h \circ f$.

Problem 3.1.2. Let $f : \mathbb{R} \to \mathbb{R}$. Sketch a graph of $f(x) = x^3 - x$, and verify that it is onto, but not one-to-one.

Problem 3.1.3. Give an example of a function $g : \mathbb{N} \to \mathbb{N}$ that is one-to-one, but not onto.

Problem 3.1.4. Compute the following explicitly: $5!, \lfloor -2.3 \rfloor, \lceil 4.1 \rceil, \lceil -4 \rceil$.

Problem 3.1.5. Give an example of a function $h : \mathbb{R} \to \mathbb{R}$ that is onto, but not one-to-one.

Problem 3.1.6. Compute the following explicitly: $0!, \lfloor 2.3 \rfloor, \lceil -4.1 \rceil, \lceil 0 \rceil$.

Problem 3.1.7. Consider the function $p : \mathbb{N} \to \mathbb{R}$ given by $p : x \mapsto x^4$. Show that p is one-to-one but not onto.

3.2 Sequences and series

HOMEWORK: 3.2 # 1–6

- sequence, closed form, recursive sequence, series, summation notation

3.2.1 Sequences

A **sequence** is an ordered list of numbers, $a_0, a_1, \ldots, a_n$. We can think of it as a function from $\{0, 1, 2, \ldots\}$ to $\mathbb{R}$. Sometimes we refer to a sequence as $\{a_n\}_{n=0}^{\infty}$, but sometimes we are lazy and just write a_n to denote the whole sequence, similarly to how we often write $f(x)$ to refer to a function. Note that this is ambiguous, because a_n is also the the element of the sequence associated to a specific number n, so context matters. There are two main ways to communicate a sequence. One is called **closed form**, which is where each element is defined explicitly, such as in the following example.

Example 3.2.1. *Define* $a_n := \frac{1}{n+2}$. *Then* $a_0 = \frac{1}{2}, a_1 = \frac{1}{3}, a_2 = \frac{1}{4}, \ldots$

A **recurrence relation** or **recursively defined** sequence is a sequence where each term is defined in terms of previous terms, and a small number of terms is defined explicitly.

Example 3.2.2. *Define* $a_n := 2a_{n-1} + 1; a_0 = 4$. *Then* $a_0 = 4, a_1 = 9$, $a_2 = 19, a_3 = 39 \ldots$

The **Fibonacci Sequence** is $a_n = a_{n-1} + a_{n-2}; a_0 = 0; a_1 = 1$. So it looks like 0, 1, 1, 2, 3, 5, 8, 13, ...

A **geometric progression** is a sequence of the form $a_n = ar^n$.

Example 3.2.3. *Define* $a_n := 3 \cdot 2^n$. *Then* $a_0 = 3, a_1 = 6, a_2 = 12, \ldots$

A **arithmetic progression** is a sequence of the form $a_n = a + dn$.

Example 3.2.4. *Define* $a_n := 6 + 2n$. *Then* $a_0 = 6, a_1 = 8, a_2 = 10, \ldots$

3.2.2 Series

To express large sums, we often rely on **summation notation**, denoted with a capital letter sigma, Σ. We call a sum of a sequence a **series**.

$$\sum_{j=m}^{n} a_j = a_m + a_{m+1} + \ldots a_{n-1} + a_n.$$

Often times, we don't bother to define a separate sequence, but instead, we put the sequence definition into the sum.

Example 3.2.5.

$$\sum_{j=2}^{4} 2^j = 2^2 + 2^3 + 2^4 = 4 + 8 + 16 = 28.$$

A **double sum** is just a sum whose terms are also themselves sums.

Example 3.2.6.

$$\begin{aligned}
\sum_{i=1}^{3}\sum_{j=2}^{4} j^i &= \sum_{j=2}^{4} j^1 + \sum_{j=2}^{4} j^2 + \sum_{j=2}^{4} j^3 \\
&= (2^1 + 3^1 + 4^1) + (2^2 + 3^2 + 4^2) + (2^3 + 3^3 + 4^3) \\
&= 9 + 29 + 99 \\
&= 137
\end{aligned}$$

3.2.3 Homework

Problem 3.2.1. Compute the first five terms of the recursively defined sequence given by $a_0 = 5, a_n = 2a_{n-1} - 3$.

Problem 3.2.2. Come up with a closed form definition of the sequence that follows this pattern: 15, 18, 21, 24, 27, ...

Problem 3.2.3. Come up with a recursive definition of the sequence that follows this pattern: 3, 6, 12, 24, 48, ...

Problem 3.2.4. Suppose that $\{a_n\}_{n=0}^{\infty}$ is an arithmetic progression. Let $\{g_n\}_{n=0}^{\infty}$ be a new sequence, defined by $g_n = 2^{a_n}$. What kind of sequence is $\{g_n\}_{n=0}^{\infty}$?

Problem 3.2.5. Compute the following sum: $\sum_{i=1}^{7}\sum_{j=1}^{9} 5$.

Problem 3.2.6. Compute the following sum: $\sum_{i=1}^{3}\sum_{j=4}^{7}(j-i)^2$.

Problem 3.2.7. Come up with a definition of the sequence that follows this pattern: -3, -1, 2, 6, ...

Problem 3.2.8. Compute the following sum: $\sum_{i=1}^{3}\sum_{j=1}^{3}(j+i)^2$.

Problem 3.2.9. Compute the following sum: $\sum_{i=3}^{6}\sum_{j=2}^{7} 1$.

3.3 Asymptotics

HOMEWORK: 3.3 # 1–6

- Big-O, witness, big-Ω, big-Θ

3.3.1 Comparing functions with big-O

Which function is bigger, $n!$ or 2^n? Well, $3! < 2^3$, but for $n \geq 4$, we have $n! > 2^n$. So we can't say that one function is bigger than the other for all inputs. So, we have the following helpful notion of size comparison. Let f and g be functions from the natural numbers to the real numbers. We say f is **big-O** of g, and write, "f is $O(g)$," or even, "$f = O(g)$," if there exist positive constants, C and k, such that for all $n > k$, we have $|f(n)| \leq C|g(n)|$. We call the numbers C and k **witnesses**. The basic idea is that if $f = O(g)$, then f grows no more quickly than g as n approaches infinity. You may also see $f \lesssim g$.

Example 3.3.1. *Show* $10n^2$ *is* $O(n^3)$.

Proof. Now, we know that as n grows large, eventually n^3 will overtake $10n^2$, but we cannot say that $10n^2 \leq n^3$ in general, because it is not true for small values of n. Where is this crossover point? Let's try to "solve for n" to see. Specifically, for which n does the following hold? We can see by dividing by n^2 on both sides.

$$\begin{aligned} 10n^2 &\leq n^3 \\ 10 &\leq n \end{aligned}$$

So our desired inequality holds for $n \geq 10$. Recall that we want to find C and k such that

$$|10n^2| \leq C|n^3|$$

for all $n > k$, so we let $C = 1$ and $k = 10$, and we are done. □

Notice that while we have computed explicit values of the constants C and k, we do not need to optimize their choices in any way. We just need to show that such witnesses exist. What happens if we cannot find constants to satisfy the definition of big-O? We'll explore this in the next example.

Example 3.3.2. *Show n^2 is NOT $O(10n)$.*

Proof. Now, we know that as n grows large, eventually n^2 will always be larger than n, but we cannot say that $n^2 \geq 10n$ in general, because it is not true for small values of n. Let's proceed by way of contradiction (BWOC) and suppose that there are constants, C and k such that for all $n > k$, we have $|n^2| \leq C|10n|$. Watch what happens when we divide both sides by n.

$$\begin{aligned} n^2 &\leq C \times 10n \\ n &\leq 10C \end{aligned}$$

So our desired inequality holds for $n \leq 10C$. Recall that we want to find C and k such that

$$|n^2| \leq C|n|$$

for ALL $n > k$, but notice that regardless of how large we choose C to be, n can't get bigger than $10C$, so our desired inequality doesn't hold for ALL $n > k$. □

3.3.2 Other comparisons

First we introduce the companion notion of big-O, namely **big-Omega**. We say f is $\Omega(g)$ if there exist natural numbers, C and k, such that for all $n > k$, we have $|f(n)| \geq C|g(n)|$. That is, f grows no more slowly than g

as n approaches infinity. If f is $\Omega(g)$, then we know that g is $O(f)$. This relationship is also expressed as $f \gtrsim g$.

If f is $O(g)$ and f is $\Omega(g)$, we say that f is $\Theta(g)$. That is, they have the same order of growth. We also write $f \approx g$, though this notation can also be used to express other relationships, so be careful about the context.

Example 3.3.3. *Let $f(x) = 2x^2$, and $g(x) = 3x^2$. We can show that $f = O(g)$ by setting $C = k = 1$. We can also show that $g = O(f)$ by setting $C = \frac{2}{3}$ and $k = 1$. Since $g = O(f)$, that means that $f = \Omega(g)$. Therefore we also have that $f = \Theta(g)$.*

3.3.3 Homework

Problem 3.3.1. Show $5n + 2 = O(n^2)$.

Problem 3.3.2. Show $5n^2 + 2 = O(n^2)$.

Problem 3.3.3. Show $5n^3 + 2$ is NOT $O(n^2)$.

Problem 3.3.4. Show $5n^3 + 2 = \Omega(n^2)$.

Problem 3.3.5. Show $5n^2 + 2 = \Theta(n^2)$.

Problem 3.3.6. Suppose $f = O(g), g = O(h)$, and $h = O(f)$. Prove that $f = \Theta(g)$.

Problem 3.3.7. Show $5n^3 + 2n^2 = O(n^4)$.

Problem 3.3.8. Show $5n^3 + 2n^2$ is not $O(n^2)$.

4 Number Theory

4.1 Division Algorithm

HOMEWORK: 4.1 # 1–4

- divides, multiple, factor, Theorem 4.1.1 (know the proofs of all parts), Theorem 4.1.2 (Division Algorithm),

4.1.1 Divisibility

Given two integers, a and b, we say that a **divides** b if there exists an integer, c, such that $b = ac$. We write $a|b$ and say that b is a **multiple** of a. We also say that a is a **factor** of b.

Example 4.1.1.
Does $3|17$ *? No, because if we divide 17 by three, we get a remainder.*
Does $4|12$ *? Yes, because there exists an integer, 3, such that* $12 = 3 \cdot 4$.

Theorem 4.1.1. *For all* $a, b, c \in \mathbb{Z}$, *with* $a \neq 0$, *the following hold:*
(i) $a|b$ *and* $a|c \Rightarrow a|(b + c)$,
(ii) $a|b \Rightarrow a|bc$,
(iii) $a|b$ *and* $b|c \Rightarrow a|c$.

Proof. (i) We start each of these with the following restatement of the hypothesis $a|b$. This will happen often. Since a divides b, we know that there exists an integer, k, such that $b = ak$. Also, since $a|c$, we know that there is an integer, ℓ, such that $c = a\ell$. Notice that $b + c = ak + a\ell = a(k + \ell)$. Since $(k + \ell)$ is an integer, we have that $(b + c)$ is a times an integer. This is the definition of $a|(b + c)$.
(ii) Since a divides b, we know that there exists an integer, k, such that $b = ak$. Notice that $bc = akc$. Since kc is an integer, we have that bc is a multiple of a. Therefore, $a|bc$.
(iii) Since a divides b, we know that there exists an integer, k, such that $b = ak$. (Is a pattern emerging?) Since b divides c, we know that there exists an integer ℓ such that $c = b\ell$. So, $c = b\ell = ak\ell$. Since $k\ell$ is an integer, we have that c is a times an integer. This is the definition of $a|c$. □

4.1.2 Division Algorithm

Theorem 4.1.2. *[Division Algorithm] Let* $a, d \in \mathbb{Z}$, *with* $d \neq 0$. *Then there exist unique integers,* q *and* r, *such that* $0 \leq r < |d|$, *and* $a = qd + r$.

Example 4.1.2. *Apply the Division Algorithm with* $a = 15$ *and* $d = 6$. *We know that the largest multiple of 6 that goes into 15 is 12, which is* 2×6. *Also, 15-12=3. So we have* $q = 2$ *and* $r = 3$, *or* $15 = 2 \times 6 + 3$.

4.1.3 Homework

Problem 4.1.1. Prove that $3|348$.

Problem 4.1.2. (i) Can any even number ever divide any odd number? (ii) Can any odd number ever divide any even number?

Problem 4.1.3. Suppose $a, b, c \in \mathbb{N}$, and $a|bc$. Is it necessary that either $a|b$ or $a|c$?

Problem 4.1.4. Suppose $a, b, c \in \mathbb{N}$. If $a|c$ and $b|c$, is it necessary that $(a+b)|c$?

Problem 4.1.5. Write down the Division Algorithm a few times.

Problem 4.1.6. Suppose $a, b \in \mathbb{N}$. If $a|b$, is it necessary that $(a+a)|b$?

Problem 4.1.7. Suppose $a, b \in \mathbb{N}$. If $a|b$, is it possible that $b|(a+a)$?

4.2 Modular Arithmetic

HOMEWORK: 4.2 # 1–4

- congruence modulo m, Proposition 4.2.1, Theorem 4.2.2 (know the proof of (i)), $\mathbb{Z}_m$

When $a, b \in \mathbb{Z}$, and $m \in \mathbb{N}$, we say a is **congruent** to b **modulo** m, if $m|(b-a)$ (or, equivalently, $m|(a-b)$). The number m is called the **modulus**. We write $a \equiv b \pmod{m}$. One use of this is when we want to talk about numbers that have the same remainder after we divide by a particular number m.

Proposition 4.2.1. *If $a, b \in \mathbb{Z}$, and $m \in \mathbb{N}$, and $a \equiv b \pmod{m}$, then a and b must have the same remainder upon division by m.*

Proof. If $a \equiv b \pmod{m}$, then $m|(b-a)$, so there is an integer, k, such that $(b-a) = km$. Now, the Division Algorithm tells us that there exist unique integers, q and r, such that $0 \leq r < m$, and $a = qm + r$, and there exist unique integers, q' and r', such that $0 \leq r' < m$, and $b = q'm + r'$.
Now, we compare two ways to write $(b-a)$.

$$km = (b-a) = (q'm + r' - qm + r) = (q'-q)m + (r'-r).$$

Since $0 \leq r', r < m$, and $km = (q'-q)m + (r'-r)$, we must have $r' = r$. □

Those of you who are familiar with computer languages may think of this as similar to the % operator. If $a \equiv b \pmod{m}$, then we would have:
`(a % m) == (b % m)`

Example 4.2.1.
$14 \equiv 2 \ (mod\ 6)$.
$9475 \equiv 5 \ (mod\ 10)$.

We want to list off some properties about the modulo relations. The following theorem shows two types of equivalences that we can expect from congruence modulo m.

Theorem 4.2.2. *Let m be a natural number, and a, b, c, and d be integers, with $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then the following hold:*
(i) $a + c \equiv b + d \ (mod\ m)$,
(ii) $ac \equiv bd \ (mod\ m)$.

Proof. First, we write down some simple consequences of the hypotheses. Namely, $a \equiv b \pmod{m}$ gives us that there must be an integer, k, such that $(a - b) = km$, and $c \equiv d \pmod{m}$ gives us that there must be an integer, ℓ, such that $(c - d) = \ell m$. With this in tow, we continue to the proofs of the individual parts.
(i) If we show that $(a + c) - (b + d)$ is a multiple of m, we will be done with part (i), as that is the definition of $a + c \equiv b + d \pmod{m}$. So, consider $(a + c) - (b + d)$:

$$(a + c) - (b + d) = (a - b) + (c - d) = km + \ell m = (k + \ell)m,$$

so $m|((a + c) - (b + d))$, which is the definition of $a + c \equiv b + d \pmod{m}$.
(ii) We will follow a similar strategy to the proof of the last part, but with the expression $ac - bd$. However, at some point, we will add and subtract bc. The reason we do this is so we can factor out helpful quantities that we have a handle on. Consider $(ac - bd)$:

$$\begin{aligned} ac - bd &= ac + 0 - bd \\ &= ac + (bc - bc) - bd \\ &= ac - bc + bc - bd \\ &= (a - b)c + b(c - d) \\ &= kmc + b\ell m \\ &= (kc + b\ell)m, \end{aligned}$$

so $m|(ac - bd)$, which means that $ac \equiv bd \pmod{m}$. □

Given a natural number, m, define the set $\mathbb{Z}_m$ to be

$$\mathbb{Z}_m := \{0, 1, 2, \ldots, (m - 1)\}.$$

For example, $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

4.2.1 Homework

Problem 4.2.1. Find three numbers that are congruent to 17 modulo 12.

Problem 4.2.2. Suppose $a, d \in \mathbb{Z}$. If $a > d$, I apply the Division Algorithm to them to get $a = qd + r$, then what is a number that a is congruent to modulo d?

Problem 4.2.3. Let m be a natural number, and a, b, c, and d be integers, with $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, show that $a - c \equiv b - d \pmod{m}$.

Problem 4.2.4. Suppose m and n are natural numbers with $m < n$. How would you describe the set $\mathbb{Z}_m \cap \mathbb{Z}_n$? What about $\mathbb{Z}_m \cup \mathbb{Z}_n$?

Problem 4.2.5. Find the smallest natural number congruent to 31 mod 6.

Problem 4.2.6. Find the smallest natural number congruent to 42 mod 8.

4.3 Representations of numbers

HOMEWORK: 4.3 # 1–5

- Theorem 4.3.1, base b representation, binary, octal, decimal, hexadecimal

Theorem 4.3.1. *Given natural numbers n and b, there exists a unique sequence, $\{a_j\}_{j=1}^{k}$, with $a_j \in \mathbb{Z}_b$, such that*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_2 b^2 + a_1 b + a_0.$$

This sequence is called the *base b representation of n*. The representation of a natural number in: base 2 is called *binary*, base 8 is called *octal*, base 10 is called *decimal*, and base 16 is called *hexadecimal*. We often write a subscript indicating the base if it is not clear from context, as we will see below. We typically write in decimal. Also, when we run out of Arabic numerals, we start using letters. Here are some examples of translating between various bases and representations.

Example 4.3.1. *Write out 743 in decimal, just by expanding its base 10 representation.*

$$743 = 743_{10} = 7 \times 10^2 + 4 \times 10 + 3.$$

Example 4.3.2. *Convert 44 in base 10 to octal.*

$$44 = 44_{10} = 5 \times 8 + 4 = 54_8.$$

Example 4.3.3. *Convert the hexadecimal* $CB4_{16}$ *to decimal.*

$$CB4_{16} = 12 \times 16^2 + 11 \times 16 + 4 = 3,072 + 176 + 4 = 3,252.$$

Example 4.3.4. *Convert* 233 *to base* 7.
Solution: *To do this, we find the biggest power of* 7 *that fits into* 233. *We can compute that* $7^3 = 343$, *which is too big, so* $7^2 = 49$ *is the biggest power that fits into* 233. *We see* $4 \times 49 = 196$, *and we cannot fit any more multiples of* 49 *into* 233. *So what's left? Well,* $233 - 196 = 37$. *So, how many times does* 7 *fit into* 37*? Well, since* $7 \times 5 = 35$, *we can fit* 5 *factors of* 7 *in. Finally,* $37 - 35 = 2$, *so the ones place has a* 2 *in it, for a final answer of*

$$233_{10} = 4 \times 7^2 + 5 \times 7 + 2 = 452_7.$$

The following table can be helpful for translating between various bases.

decimal	binary	octal	hexadecimal
0	0000	00	0
1	0001	01	1
2	0010	02	2
3	0011	03	3
4	0100	04	4
5	0101	05	5
6	0110	06	6
7	0111	07	7
8	1000	10	8
9	1001	11	9
10	1010	12	A
11	1011	13	B
12	1100	14	C
13	1101	15	D
14	1110	16	E
15	1111	17	F

Because powers of two work so well together, we can quickly convert between bases that are powers of two using the table above.

Example 4.3.5. *Convert* $EF1C_{16}$ *to binary, one hexadecimal digit at a time.*

$$EF1C_{16} = 1110\ 1111\ 0001\ 1100 = 1110111100011100_2.$$

4.3.1 Homework

Problem 4.3.1. Convert 345_{10} into binary.

Problem 4.3.2. Convert 345_8 into binary.

Problem 4.3.3. Convert 345_8 into decimal.

Problem 4.3.4. Convert 345_9 into decimal.

Problem 4.3.5. Convert $3A5_{16}$ into binary.

Problem 4.3.6. Convert $3A5_{16}$ into decimal.

Problem 4.3.7. Convert $3FA5_{16}$ into binary.

Problem 4.3.8. Convert 3465_{10} into hexadecimal.

Problem 4.3.9. Convert 365_7 into base 9.

4.4 Primes

HOMEWORK: 4.4 # 1–3

- prime, composite, Theorem 4.4.1 (Fundamental Theorem of Arithmetic), Theorem 4.4.2 (know proof), Theorem 4.4.3 (Infinitude of primes, know proof), Theorem 4.4.4 (Prime Number Theorem)

A natural number greater than one is called **prime** if its only factors are itself and 1. A natural number greater than one that is not prime is called **composite**. The following shows one reason why primes are so important.

Theorem 4.4.1. *[Fundamental Theorem of Arithmetic] Every natural number greater than one can be written uniquely as a product of primes.*

Theorem 4.4.1 tells us that any natural number greater than one has a unique "multiplicative genetic code" made up of primes. This is similar to the unique representation we have in any fixed base b.

Example 4.4.1.
$120 = 2^3 \cdot 3 \cdot 5$. *Any other product of primes will not work out to* 120. *However,* $120 = 119 + 1 = 118 + 2 = \ldots$ *We can see that there are many ways to write* 120 *as a sum of numbers. Notice that once we pick a base (here we are in base ten), we do have such a unique representation.*

While Theorem 4.4.1 guarantees the existence of a unique prime factorization, it does not give us any clue as to what those primes are. The next result gives us a simple way to narrow our search for prime factors of a given composite number. At the heart of this proof is an idea that we've seen before.

Theorem 4.4.2. *If n is composite, then it has a prime divisor, p, with $p \leq \sqrt{n}$.*

Proof. Since n is composite, we know that it must have at least one integer factor aside from itself or one. Call this factor a. Now, as a and n are integers, and a is a factor of n, we have that there must be an integer, b, such that $n = ab$.

We will now show that either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. By way of contradiction, suppose that both $a > \sqrt{n}$ and $b > \sqrt{n}$. If this were the case, then we would have that

$$ab > a\sqrt{n} > \sqrt{n}\sqrt{n} = n,$$

which contradicts the fact that $ab = n$.

Without loss of generality, suppose that $a \leq b$ (if not, from here through the rest of the proof, work with b in place of a). If a is prime, then our prime factor, p, is just a, and we are done. If a is not prime, then by the Fundamental Theorem of Arithmetic, it has at least one (possibly repeated) prime factor, p, which must also be less than or equal to a, and therefore also less than or equal to $\sqrt{n}$. □

Theorem 4.4.2 essentially says that if we have a natural number n, then we only have to check divisibility for numbers up to $\sqrt{n}$, and if we don't find any factors, then n must be prime. This is just one example of the many ways in which prime factorization algorithms can be simplified. Next, we show that there are infinitely many primes.

Theorem 4.4.3. *There are infinitely many primes.*

Proof. By way of contradiction, suppose that there are only finitely many primes. Then we could construct an exhaustive list, $\{p_1, p_2, \ldots, p_k\}$. Consider the number

$$x := p_1 \cdot p_2 \cdots p_k + 1.$$

Now, by the Fundamental Theorem of Arithmetic, it has at least one prime factor. Notice that x is one more than a multiple of any of the p_j, so it cannot be evenly divided by any of them. Also notice that x is greater than all of the elements on the list, so it is not on our list of primes. Therefore, there must be a prime missing, causing a contradiction! □

Finally, we include the following because it is a famous and important result. It never ceases to amaze me how often it comes up in casual conversation among engineers and computer scientists.

Theorem 4.4.4. *[Prime Number Theorem] Given $x > 0$, the number of primes $\leq x$ is $\Theta\left(\frac{x}{\ln x}\right)$.*

4.4.1 Homework

Problem 4.4.1. Write 360 as a product of prime factors.

Problem 4.4.2. Suppose I have natural numbers a and b, and $n = ab$. If n is prime, what do I know about a and b?

Problem 4.4.3. Seriously, learn the proof of Theorem 4.4.3, that there are infinitely many primes!

Problem 4.4.4. Why does the proof of Theorem 4.4.3 NOT give us a formula to find the precise values of new prime numbers?

Problem 4.4.5. Restate the Prime Number Theorem in your own words. You don't have to be terribly precise, but practice writing things carefully in your own words.

4.5 Greatest common divisor

HOMEWORK: 4.5 # 1–5

- gcd, relatively prime, coprime, lcm, Theorem 4.5.1, Euclidean Algorithm, Theorem 4.5.2 (Bézout Identity), Lemma 4.5.3 (know proof), Lemma 4.5.4, Theorem 4.5.5

Given any two integers, a and b, the largest integer than divides both of them is called their **greatest common divisor,** or **gcd**, written $\gcd(a, b)$. If the gcd of two numbers is 1, we call them **relatively prime** or **coprime**. The smallest natural number divisible by a and b is called their **least common multiple**, or **lcm**, written $\text{lcm}(a, b)$. We begin by stating a result that demonstrates a relationship between the gcd and lcm.

Theorem 4.5.1. *Given $a, b \in \mathbb{N}$, $gcd(a, b)lcm(a, b) = ab$.*

Proof. Suppose that the infinite sequence of primes is $\{p_i\}_{i=1}^{\infty}$, where $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$. By the Fundamental Theorem of Arithmetic, both a and b have unique prime factorizations:

$$a = p_1^{a_1} \cdot p_2^{a_2} \ldots p_n^{a_n}, \text{ and}$$

$$b = p_1^{b_1} \cdot p_2^{b_2} \ldots p_n^{b_n},$$

where the powers of the primes (a_i and b_i) are either zero or natural numbers, and p_n is the biggest prime that divides either of a and b. By definition, we

can see that the gcd of a and b is the product of the largest powers of prime factors that fit into both, so

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \dots p_n^{\min(a_n,b_n)}.$$

Similarly, the lcm is the product of the largest powers of prime factors that fit into either, so

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \dots p_n^{\max(a_n,b_n)}.$$

Notice that for any i, we have

$$a_i + b_i = \min(a_i, b_i) + \max(a_i, b_i). \tag{1}$$

Now it's just a matter of checking the exponent each prime factor p_i on the left- and right-hand sides of the equation in the statement of the proof.

$$ab = p_1^{a_1+b_1} \cdot p_2^{a_2+b_2} \dots p_n^{a_n+b_n},$$

but by (1), this is just

$$\begin{aligned} p_1^{\min(a_1,b_1)+\max(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)+\max(a_2,b_2)} \dots p_n^{\min(a_n,b_n)+\max(a_n,b_n)} \\ = \gcd(a,b) \cdot \operatorname{lcm}(a,b). \end{aligned}$$

□

Example 4.5.1. $24 \cdot 36 = 12 \cdot 72 = \mathit{gcd}(24,36) \cdot \mathit{lcm}(24,36)$.

The **Euclidean Algorithm** is a process for finding the gcd of two suitable integers. The general procedure is to repeatedly write the integers as a and d in the Division Algorithm, and make your old d the new a, and your old r the new d. We show it here generally and show an explicit example.

4.5.1 Euclidean Algorithm

Given two integers, a and b, with $b \neq 0$, we can calculate $\gcd(a,b) = r_k$, from the following series of applications of the Division Algorithm, that is, with q_j and r_j integers, with $0 \leq r_j < q_j$:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k + 0. \end{aligned}$$

Example 4.5.2. *Find gcd*$(91, 287)$.
Solution:

$$\begin{aligned} 287 &= 3 \cdot 91 + 14 \\ 91 &= 6 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0, \end{aligned}$$

so gcd$(91, 287) = 7$.

Theorem 4.5.2 (Bézout Identity)**.** *Given two integers, a and b, there exist two integers, s and t, such that gcd$(a, b) = sa + tb$.*

The proof of this lies in rolling the Euclidean Algorithm calculations backwards, solving for their gcd, r_k, and substituting in for previous values of r_j until we reach the desired equation. We state this in general, but the example following is probably more instructive. In general, we have

$$\begin{aligned} r_k &= r_{k-2} - q_k r_{k-1} \\ &= r_{k-2} - q_k(r_{k-3} - q_{k-1} r_{k-2}) \\ &\quad \vdots \\ &= sa + tb. \end{aligned}$$

Example 4.5.3. *Find two integers, s and t, such that $7 = s \cdot 91 + t \cdot 287$.*
Solution:
We will start with the final line of Example 4.5.2, and put the gcd on one side of the equal sign, and the rest on the other side. We continue by simplifying and substituting in for the remainder on the previous line in the Euclidean Algorithm calculation until we reach the top, in which case we are done.

$$\begin{aligned} 7 &= 91 - 6 \cdot 14 \\ &= 91 - 6 \cdot (287 - 3 \cdot 91) \\ &= 19 \cdot 91 - 6 \cdot 287. \end{aligned}$$

So $s = 19$, and $t = -6$.

Example 4.5.4. *Find gcd*$(3114, 1350)$*, then find two integers, s and t, such that* $\gcd(3114, 1350) = 3114s + 1350t$.
Solution:

$$
\begin{aligned}
3114 &= 2 \cdot 1350 + 414 \\
1350 &= 3 \cdot 414 + 108 \\
414 &= 3 \cdot 108 + 90 \\
108 &= 1 \cdot 90 + 18 \\
90 &= 5 \cdot 18 + 0,
\end{aligned}
$$

so $gcd(3114, 1350) = 18$. *We will start with the final line of the previous calculation, and put the gcd on one side of the equal sign, and the rest on the other side. We continue by simplifying and substituting in for the remainder on the previous line in the Euclidean Algorithm calculation until we reach the top, in which case we are done.*

$$
\begin{aligned}
18 &= 108 - 1 \cdot 90 \\
&= 108 - 1 \cdot (414 - 3 \cdot 108) \\
&= 4 \cdot 108 - 1 \cdot 414 \\
&= 4 \cdot (1350 - 3 \cdot 414) - 1 \cdot 414 \\
&= 4 \cdot 1350 - 13 \cdot 414 \\
&= 4 \cdot 1350 - 13 \cdot (3114 - 2 \cdot 1350) \\
&= 30 \cdot 1350 - 13 \cdot 3114
\end{aligned}
$$

So $s = -13$, *and* $t = 30$.

Lemma 4.5.3. *For any natural numbers,* a, b, *and* c, *with* $gcd(a, b) = 1$ *and* $a|bc$, *we have that* $a|c$.

Proof. Since $a|bc$, we know that there exists an integer, k, such that $ak = bc$. By Bézout (Theorem 4.5.2), $\gcd(a, b) = 1$ implies that there exist integers, s and t, such that $sa + tb = 1$. Multiplying both sides of that equation by c yields

$$sac + tbc = c. \tag{2}$$

So, we can substitute ak in place of bc in (2), to get

$$sac + tak = c.$$

Thus we can factor out an a on the left-hand side to get

$$a(sc + tk) = c.$$

Therefore, c is a multiple of a. That is, $a|c$. □

Lemma 4.5.4. *Given a prime number, p, and integers, a_j, if $p|a_1 \cdot a_2 \cdots a_n$, then p divides at least one of the a_j.*

This lemma is proved by repeated application of Lemma 4.5.3.

Theorem 4.5.5. *Given a natural number, m, and integers, a, b, and c, with $gcd(m, c) = 1$, if $ac \equiv bc \ (mod\ m)$, then $a \equiv b \ (mod\ m)$.*

Proof. Given that $ac \equiv bc \pmod{m}$, we know that $m|(ac - bc)$. By factoring out a c, we see that $m|(a - b)c$. We will now apply Lemma 4.5.3. Try not to get confused by the fact that there is a variable called a in this proof, and a (possibly) different variable called a in the statement of Lemma 4.5.3. The same is true of b and c. Here is a table to guide you through the application:

this proof	Lemma 4.5.3
m	a
c	b
(a-b)	c

So, the variable m here will take the place of the variable a in Lemma 4.5.3, etc... Now, the conclusion of Lemma 4.5.3 will give us that $m|(a - b)$, which is precisely what we need to see that $a \equiv b \pmod{m}$. □

We can also prove this theorem directly, by including the relevant parts of the proof of Lemma 4.5.3.

Proof. Given that $ac \equiv bc \pmod{m}$, we know that $m|(ac - bc)$. By factoring out a c, we see that $m|(a - b)c$. So there exists an integer k such that

$$mk = (a - b)c. \tag{3}$$

Now, by By Bézout (Theorem 4.5.2), $\gcd(m, c) = 1$ implies that there exist integers, s and t, such that

$$sm + tc = 1. \tag{4}$$

Multiply both sides of (4) by $(a - b)$ to get

$$sm(a - b) + tc(a - b) = (a - b).$$

Now, we use (3) to substitute mk in for $c(a - b)$ to get

$$(a - b) = sm(a - b) + tmk.$$

Factoring out an m on the right hand side yields

$$(a - b) = m(s(a - b) + tk),$$

which has m times an integer on the right-hand side, so $m|(a - b)$, which means that $a \equiv b \pmod{m}$. □

Example 4.5.5. $3 \cdot 5 \equiv 3 \cdot 7(\ mod\ 6)$, *but* $5 \not\equiv 7(\ mod\ 6)$, *as* $gcd(3,6) > 1$.

4.5.2 Homework

Problem 4.5.1. Verify that $42 \cdot 27 = \gcd(42,27) \cdot \text{lcm}(42,27)$.

Problem 4.5.2. Use the Euclidean Algorithm to find the gcd of 210 and 78, then use this derivation to find integers s and t so that

$$210s + 78t = \gcd(210, 78).$$

Problem 4.5.3. Use the Euclidean Algorithm to find the gcd of 1290 and 315, then use this derivation to find integers s and t so that

$$1290s + 315t = \gcd(1290, 315).$$

Problem 4.5.4. Suppose $a_1, a_2, \ldots, a_{n-1}, a_n, b \in \mathbb{N}$. If $b | a_1 \cdot a_2 \cdots a_{n-1} \cdot a_n$, but b does NOT divide any of the a_j, what can we conclude about b?
Hint: Consider Lemma 4.5.4.

Problem 4.5.5. Suppose that for $a, b, c, m \in \mathbb{N}$, we have that $ac \equiv bc \pmod{m}$. In light of Theorem 4.5.5, what more do we need to know to be sure that $a \equiv b \pmod{m}$? Note, do not just repeat the definition of congruence modulo m.

Problem 4.5.6. Use the Euclidean Algorithm to find the gcd of 211 and 78, then use this derivation to find integers s and t so that

$$211s + 78t = \gcd(211, 78).$$

Problem 4.5.7. Use the Euclidean Algorithm to find the gcd of 378 and 75, then use this derivation to find integers s and t so that

$$378s + 75t = \gcd(378, 75).$$

5 Mathematical Induction

5.1 Induction

HOMEWORK: 5.1 # 1–5

- $P(n)$, Mathematical Induction, Base Case, Induction Hypothesis, Inductive Step

Recall that we reference a statement with the variable n like this: $P(n)$.

Example 5.1.1. *Let $P(n) =$ "n is a prime number." Then $P(4)$ is false, but $P(5)$ is true.*

Mathematical Induction is a way of proving an infinite number of statements of the form $P(n)$ in a finite number of steps. First, we prove that $P(n_0)$ is true for some initial integer, n_0 (usually 0, 1, or 2). This is called the **Base Case**. Next, we assume that $P(n)$ is true for some n. This is called the **Induction Hypothesis**. Finally, we show that $P(n)$ implies $P(n+1)$. This is called the **Inductive Step**. There are other methods of induction, but they are logically equivalent to this method. One note before moving forward, remember that

$$\sum_{j=1}^{n} j = 1 + 2 + 3 + \cdots + n \text{ and } \sum_{j=1}^{n+1} j = 1 + 2 + 3 + \cdots + n + (n+1).$$

Example 5.1.2. *Use induction to show that for all natural numbers, n:*

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}.$$

Solution:
Define $P(n)$ to be:

$$P(n) := \text{ the statement } \text{“ } \sum_{j=1}^{n} j = \frac{n(n+1)}{2}. \text{ ”}$$

Our Base Case will be $n_0 = 1$, because 1 is the smallest natural number, and we want to prove $P(n)$ for all natural numbers. Check the validity of $P(1)$. That is, verify that the following is true:

$$\sum_{j=1}^{1} j = 1 = \frac{1(1+1)}{2}.$$

With this in tow, we now assume that $P(n)$ is true (the Induction Hypothesis), and try to show that it implies that $P(n+1)$ is also true (the Inductive Step). So we start by writing down $P(n)$, and using mathematical manipulations to make it look like $P(n+1)$. Note, we are NOT just changing variables and replacing n by $n+1$, as that would not be valid. Read through to the end

of this example, even if some steps don't make sense at first.

$$
\begin{aligned}
& P(n) \\
& \sum_{j=1}^{n} j = \frac{n(n+1)}{2} \\
\sum_{j=1}^{n} j + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\
\sum_{j=1}^{n+1} j &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\
\sum_{j=1}^{n+1} j &= \frac{n^2+n}{2} + \frac{2n+2}{2} \\
\sum_{j=1}^{n+1} j &= \frac{n^2+3n+2}{2} \\
\sum_{j=1}^{n+1} j &= \frac{(n+1)(n+2)}{2} \\
P(n+1) &
\end{aligned}
$$

Now, for your first read through, just verify that each line follows from the previous line. After you understand that each step is correct, start trying to figure out why we chose the manipulations that we did.

The "big picture" idea here is to manipulate the side with the most "stuff hanging off of it" until it looks like you want it to, then clean up the other side and hope for the best. In this case, we started by writing down $P(n)$. Now, the left-hand side is the sum of the first n terms. We want the sum of the first $n+1$ natural numbers, so we added $(n+1)$ to both sides. This gives us the sum of the first $(n+1)$ natural numbers, which is what the left-hand side of $P(n+1)$ should look like. To clean up, we verify that the right-hand side is indeed what we want for the right-hand side of $P(n+1)$ by using basic algebra.

Example 5.1.3. *Use induction to show that for any non-negative integer, n, and for any real number, $x > -1$, we have $1 + nx \leq (1+x)^n$.*
Solution:
The base case will be $P(0)$, namely, $1+0 \cdot x \leq (1+x)^0$, which is true, as both sides of the inequality are 1. For the induction hypothesis, we will assume that $P(n)$ is true, for some non-negative integer, n, and try to show that this

implies that $P(n+1)$ is also true. This is the inductive step. We start by multiplying both sides by $(1+x)$, which is positive for $x > -1$, so we need not worry about the $\leq$ sign changing direction. We continue by multiplying out the left-hand side, and simplifying.

$$\begin{aligned} & P(n) \\ 1 + nx &\leq (1+x)^n \\ (1+nx)(1+x) &\leq (1+x)(1+x)^n \\ 1 + nx + x + nx^2 &\leq (1+x)^{n+1} \\ 1 + (n+1)x + nx^2 &\leq (1+x)^{n+1} \end{aligned}$$

Notice that $nx^2 \geq 0$, so

$$1 + (n+1)x + nx^2 \geq 1 + (n+1)x.$$

So the last line of our first calculation actually gives us that

$$1 + (n+1)x \leq 1 + (n+1)x + nx^2 \leq (1+x)^{n+1}.$$

If we ignore the middle, we have $1+(n+1)x \leq (1+x)^{n+1}$, which is $P(n+1)$. We have just shown that $P(n)$ implies $P(n+1)$, so we are therefore done by induction.

Example 5.1.4. *Use mathematical induction to show that for all $n \in \mathbb{N}$:*

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

Solution:
Define $P(n)$ to be:

$$P(n) := \text{ the statement } \text{“ } \sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}. \text{ ”}$$

Our Base Case will be $n_0 = 1$, because 1 is the smallest natural number, and we want to prove $P(n)$ for all natural numbers. Check the validity of $P(1)$. That is, verify that the following is true:

$$\sum_{j=1}^{1} j^2 = 1 = \frac{1(1+1)(2(1)+1)}{6}.$$

With this in tow, we now assume that $P(n)$ is true (the Induction Hypothesis), and try to show that it implies that $P(n+1)$ is also true (the Inductive Step). So we start by writing down $P(n)$, and using mathematical manipulations to make it look like $P(n+1)$. Note, we are NOT just changing variables and replacing n by $n+1$.

$$
\begin{aligned}
&P(n)\\
&\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}\\
\sum_{j=1}^{n} j + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2\\
\sum_{j=1}^{n+1} j^2 &= \frac{n(n+1)(2n+1)}{6} + \frac{6(n+1)^2}{6}\\
\sum_{j=1}^{n+1} j &= \frac{n^2+n}{2} + \frac{2n+2}{2}\\
\sum_{j=1}^{n+1} j &= \frac{n^2+3n+2}{2}\\
\sum_{j=1}^{n+1} j &= \frac{(n+1)(n+2)}{2}\\
P(n+1)&
\end{aligned}
$$

Example 5.1.5. *Use induction to show that $8|n^2-1$ for all odd natural numbers, n.*

Solution:

First, the base case. $P(1)$ is just the statement that $8|1^2-1$, or that $8|0$. This is true, as 0 is an integer, and $8 \cdot 0 = 0$. (Don't worry– we are not dividing by zero here.) Now for the induction hypothesis. $P(n)$ is precisely the statement $8|n^2-1$. If we assume that $P(n)$ is true, then the inductive step is showing that it logically implies $P(n+2)$. This time, we are adding 2 to n because we want to look at the next odd natural number, and not just the next natural number. So, we consider $(n+2)^2-1$, and we will show that it is divisible by 8.

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

Now, we know that n^2-1 is a multiple of 8, by the induction hypothesis. Also, notice that since n is odd, $(n+1)$ must be even. So $4(n+1)$ is 4 times

an even number, which must be a multiple of 8. So $(n+2)^2 - 1$ *is the sum of two multiples of 8, and therefore, itself a multiple of 8. So we are done by induction.*

Finally, we end with an example of when induction seems like a good idea, but is not, strictly speaking, necessary. We will start by writing an inductive proof, and that will lead to a nice organization of the information at hand, which will lead us to a non-inductive proof!

Example 5.1.6. *Prove that the difference of the squares of two consecutive odd natural numbers is four times their average.*
Solution:
We start with the smallest pair of consecutive odd numbers, 1 and 3, for the base case.

$$3^2 - 1^2 = 9 - 1 = 8 = 4(2) = 4\left(\frac{1+3}{2}\right).$$

Now, how do we write this as a statement $P(n)$*? There are many ways, but let's try writing the* n*th odd natural number as* $2n-1$*. Then the next odd natural number will be* $2n+1$*.*

$$P(n) := \text{“}(2n+1)^2 - (2n-1)^2 = 4\left(\frac{(2n-1)+(2n+1)}{2}\right).\text{”}$$

So we just verified $P(1)$ *above. Now let's show that* $P(n)$ *implies* $P(n+1)$*. We start by assuming* $P(n)$*, then we simplify both sides a bit...*

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

$$(4n^2+4n+1) - (4n^2-4n+1) = 4\left(\frac{4n}{2}\right) = 8n.$$

... but then we notice that if we continue simplifying, we just get that this is always true, and we didn't need to do induction in the first place! Distributing the minus sign and reordering the left hand side gives us

$$4n^2 - 4n^2 + 4n + 4n + 1 - 1 = 8n.$$

So we ended up showing that this is going to hold for any natural number n*, without actually using any inductive principles! We started an inductive proof, and by using those ideas to organize our information, we actually got a simpler proof.*

5.1.1 Homework

Problem 5.1.1. Use mathematical induction to show that for a real number a, and $n \in \mathbb{N}$:

$$\sum_{j=0}^{n-1} a = an.$$

Problem 5.1.2. Use mathematical induction to show that for real numbers a and r, with $a > 0$ and $r > 1$, and $n \in \mathbb{N}$:

$$\sum_{j=0}^{n-1} ar^j = a\frac{1-r^n}{1-r}.$$

Problem 5.1.3. Use mathematical induction to show that for any natural number $n \geq 2$:

$$n^2 \leq n^3 - n$$

Problem 5.1.4. Use mathematical induction to show that the sum of the first n odd numbers is n^2.

Problem 5.1.5. Use mathematical induction to show that for any natural number $n \geq 4$:

$$2^n \leq n!$$

Problem 5.1.6. Explain why it is not always enough to just add $n + 1$ to both sides for some induction proofs.

Problem 5.1.7. This problem may seem silly, but try it anyway. Use induction to prove that there are infinitely many natural numbers bigger than 42.

Problem 5.1.8. This problem may seem slightly less silly. Use induction to prove that there are infinitely many real numbers between 0 and 1.

6 Counting

6.1 Basic counting

HOMEWORK: 6.1 # 1–6

- Sum rule (or), product rule (and), subtraction rule (inclusion/exclusion), division rule (symmetry)

People often joke that counting is easy. I think a more accurate assessment is that straightforward counting is often easy, but counting tasks can get very difficult very quickly. We will begin slowly, but please take this section seriously, and read it very carefully.

6.1.1 Sum Rule

When some step in the decision making process affects later options, we have to take all of these separate possible paths and add them together. This is called the *sum rule*. It is for dealing with scenarios where we have to do this (exclusive) OR that.

Example 6.1.1. *Suppose that I have 3 movies I want to watch. How many different ways can I watch exactly one movie?*
Solution: *Three. Yep, there's not a whole lot going on here. I can either watch the first movie, and not the second or third, or I could watch the second movie, while ignoring the first and last, or, not surprisingly, I could forego the first two movies and just watch the third. These are all of my options.*

So, that might have been confusingly easy, so we'll spice things up just a bit.

Example 6.1.2. *Suppose that I have 3 pairs of shorts, and two pairs of jeans. How many different choices do I have for leg coverings?*
Solution: *I could either wear shorts (three ways) or jeans (two ways). So my total is 3+2=5 choices.*

One abstract way to think of this is the size of a set. If I have to select exactly one element from a set S then I have $|S|$ distinct ways to do that. While we're studying fashion so carefully, let's consider a top and a bottom. The next example is an illustration of the *product rule*. Basically, if I have several choices to make at each stage in a decision making process, and none affects the others, then I just multiply the number of choices at each step. The key to identifying these scenarios is if I have to do step one AND step two AND step three, etc...

Example 6.1.3. *Suppose that I have 3 shirts, and 2 pairs of shorts. How many outfits can I make, assuming they all match?*
Solution: *Well, for each choice of shorts, I have 3 shirts. So the answer is* $3 \times 2 = 6$ *total outfits.*

6.1.2 Product Rule

Taking the set theoretical viewpoint a bit further, we recall that all of the choices of one element from a set A and one element from a set B is exactly their Cartesian product, $A \times B$, and $|A \times B| = |A| \cdot |B|$. We now make things a bit more intricate.

Example 6.1.4. *How many five digit numbers are there (in standard decimal notation)?*
Solution: *The first digit can be any number between 1–9 (9 choices), and the rest are any number between 0–9 (10 choices). We choose the first digit AND the second AND the third AND the fourth AND the fifth, so we multiply the numbers of choices together.*
9 choices $\times$ *10 choices* $\times$ *10 choices* $\times$ *10 choices* $\times$ *10 choices* $= 90{,}000$.

Example 6.1.5. *(a) How many bit strings of length 6 are there? (b) How many bit strings of length 8 end in "10"?*
Solution: *For part (a), we have to choose between two options six times. So the answer is* 2^6. *For part (b), the answer is the same, because we are still only making 6 choices.*

Now we combine the sum and product rules in the following example.

Example 6.1.6. *Suppose that a valid product code consists of either two letters and a one-digit number, or one letter a three one-digit numbers. How many total product codes are there?*
Solution:
We will deal with the two types of product codes separately, and add the totals together at the end. For the first type, we have 26 choices for the first letter, 26 choices for the second letter, and 10 choices for the number, for a total of $26^2 \cdot 10$. *Similar reasoning tells us that we have* $26 \cdot 10^3$ *choices for the second type. So the total number of available product codes is* $26^2 \cdot 10 + 26 \cdot 10^3$.

6.1.3 Subtraction Rule (Inclusion/Exclusion)

Given two sets, A and B, we have the following relationship, called **inclusion/exclusion** or **the subtraction rule**:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Sometimes, it is easier to over-count a desired quantity, and then go back later and correct ourselves. In some sense, that is what inclusion/exclusion does. We want to count $A \cup B$, so we count A and we count B, but we've counted the elements in both sets twice, so we correct for this by subtracting exactly the amour by which we have over-counted. Let's do a straightforward example of this.

Example 6.1.7. *Suppose* A *and* B *are sets with* $|A| = 8, |B| = 9$, *and* $|A \cap B| = 4$. *How big is* $A \cup B$*?*
Solution: *We apply the inclusion/exclusion formula to get*

$$|A \cup B| = |A| + |B| - |A \cap B| = 8 + 9 - 4 = 13.$$

Now we do a more involved example using inclusion/exclusion.

Example 6.1.8. *Suppose that I have ten total apps on my phone. Five are free and seven are games. Obviously, the only apps worth buying are games. How many free games do I have?*
Solution: *We start by calling the set of free apps F, and the set of games G. Now, because every app on my phone is either free or a game or both, the ten total apps can only consist of elements in either the set F or the set G, or both. That is,*

$$|F \cup G| = 10.$$

By inclusion/exclusion, we have that

$$|F \cup G| = |F| + |G| - |F \cap G|.$$

putting together everything we know gives us

$$10 = |F \cup G| = |F| + |G| - |F \cap G| = 5 + 7 - |F \cap G|,$$

which yields the final answer $|F \cap G| = 2$, the number of free games.

Example 6.1.9. *Consider the natural numbers 1–100. (a) How many are even? (b) How many are multiples of 3? (c) How many are multiples of either 2 or 3?*
Solution: *For part (a), we just need to divide 100 by two, as half are odd and half are even, and we get 50.*
For part (b), we know that one-third of the natural numbers 1–99 are multiples of 3, so there are 33 multiples of 3 between 1-99. Now, 100 is not a multiple of three, so the total number of multiples of 3 between 1–100 is also 33. For part (c), we call E the set of even numbers between 1-100, and call T the set of multiples of 3 between 1-100. The total number of multiples of either 2 or 3 will then be the set $E \cup T$. So, we appeal to inclusion/exclusion to get

$$|E \cup T| = |E| + |T| - |E \cap T|.$$

The set $E \cap T$ is the set of multiples of both 2 and 3, or the multiples of 6. Reasoning as above, we see that there are exactly 16 multiples of 6 between 1-96, and no more from 97–100. So $|E \cap T| = 16$. Plugging this into our previous equation gives us that

$$|E \cup T| = |E| + |T| - |E \cap T| = 50 + 33 - 16 = 67.$$

6.1.4 Division Rule

Sometimes we over-count by much, much more. The **division rule** helps us account for various symmetries. We illustrate it in the following examples.

Example 6.1.10. *In this example, we use the term 'word' to mean any string of characters, regardless of whether or not they are legal plays in Scrabble, Words With Friends, or even pronounceable. However, as in Scrabble, we cannot play a word with two of a given letter unless we have access to two of that letter. (a) How many words can be formed using the letters in 'BOX'? (b) How many words can be formed using the letters in 'BOO'? (c) How many words can be formed using the letters in 'CANNONBALL'?*
: Solution *For part (a), we have three choices for the first letter, two for the second (because we cannot repeat letters), and then only one letter remains, so the answer is* $3 \times 2 \times 1 = 6$.
For part (b), we will pretend that the two letter Os are distinct by labeling them O_1 *and* O_2*. Now, we can begin by counting the number of words formed by the letters in 'BOO' by considering four distinct letters, '*BO_1O_2*,' as we did in part (a). We get* $3 \times 2 \times 1$*, or 6. However, we have over-counted, as '*BO_1O_2*' and '*BO_2O_1*' are actually the same word, 'BOO.' If we were to write out a list of all of the words, but keep the words with* O_1 *to the left of* O_2 *on one side of the list, and keep the words with* O_2 *to the left of* O_1 *on one side of the list, we'd get two copies of the same list!*

O_1 *to the left of* O_2	O_2 *to the left of* O_1
BO_1O_2	BO_2O_1
O_1BO_2	O_2BO_1
O_1O_2B	O_2O_1B

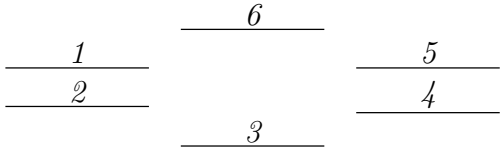
So, we have to divide by the number of symmetries of the letter Os. Since there would just be two symmetric lists, we will divide our previous answer by two. So the final answer for part (b) is 6/2 =3.
For part (c), we will take the same approach. First we compute the size of our total list,

$$10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 3,628,800.$$

Then we divide this number by the number of symmetries, or ways to arrange the letters N_1, N_2*, and* N_3 *(*$3 \times 2 \times 1 = 6$*), as well as the number of ways to arrange the letters* L_1 *and* L_2 *(*$2 \times 1 = 2$*), and the number of ways to arrange the letters* A_1 *and* A_2 *(*$2 \times 1 = 2$*). So if we wrote out all 3,628,800 words, there would be* $6 \times 2 \times 2 = 24$ *identical lists, with our subscripted letters being the only difference, so the final answer is 3,628,800/24=131,200.*

Example 6.1.11. *How neighbor-different seating arrangements are there for six people around a round table, if two seating arrangements are only*

neighbor-different if at least some person has different neighbors?
Solution: *Well, if we just count the number of different arrangements, ignoring the neighbor rules, we have six choices for the first seat (starting at the top and going clockwise), five for the second, and so on, yielding* $6 \times 5 \times 4 \times 3 \times 2 \times 1 = 720$.



Now we need to divide out by the number of different choices of first seat. Since there are six seats, there are six choices for first seat. Also, we need to divide by two because we could count clockwise or counterclockwise. So our final answer is

$$\frac{720}{12} = 60.$$

6.1.5 Homework

Problem 6.1.1. Suppose I have fifteen shirts and twenty-five pairs of shorts. How many outfits can I make?

Problem 6.1.2. Suppose I have seven shirts, and four pairs of shorts, and five pairs of jeans. Recall that I won't wear both shorts and jeans at the same time. How many outfits can I make?

Problem 6.1.3. Suppose a valid product code has the format of three letters followed by five single-digit numbers or by two more letters. How many valid product codes are there?

Problem 6.1.4. Suppose I have twenty books that are blue, and fifteen books that are about music. If exactly five of the blue books are about music, how many books do I have total that are either blue, about music, or both?

Problem 6.1.5. Let A, B, and C be sets. If $|A \cap C| = 7, |B \cap C| = 4$, and $|A \cap B \cap C| = 2$, how big is $|(A \cup B) \cap C|$?

Problem 6.1.6. How many numbers between 1 and 100 are either a multiple of 2 or a multiple of 5 or a multiple of both?

Problem 6.1.7. How many 'words' can one form by rearranging the letters in the word, 'REORDERING'?

Problem 6.1.8. (*) How many pairs of elements can you choose from a set with n elements? What if the order (which is first and which is second) doesn't matter?

Problem 6.1.9. Suppose a valid product code has the format of seven letters followed by three single-digit numbers or six letters followed by five single-digit numbers. How many valid product codes are there?

Problem 6.1.10. Suppose a valid product code has the format of four letters followed by four single-digit numbers or by two more letters. How many valid product codes are there?

Problem 6.1.11. How many 'words' can one form by rearranging the letters in the word, 'HABERDASHERY'?

6.2 Pigeonhole principle

HOMEWORK: 6.2 # 1–4

- Theorem 6.2.1 (PHP)

Suppose that you have ten pigeons, each of which is carefully (so as not to harm said pigeon) placed into exactly one of three holes. Then at least one of the holes has at least four pigeons in it. This is an example of the **pigeonhole principle (php)**. Now, since 'ten' rhymes with n, 'three' rhymes with t, and 'four' rhymes with $\lceil \frac{n}{t} \rceil$, we write the following theorem.

Theorem 6.2.1 (Pigeonhole principle)**.** *Suppose that you have n pigeons, each of which is carefully (so as not to harm said pigeon) placed into exactly one of t holes. Then at least one of the holes has at least $\lceil \frac{n}{t} \rceil$ pigeons in it.*

Proof. By way of contradiction, suppose that every hole has fewer than $\lceil \frac{n}{t} \rceil$ pigeons in it. The total number of pigeons is less than the number of holes times the maximum number pigeons in any hole, so

$$n \leq t \cdot \left(\left\lceil \frac{n}{t} \right\rceil - 1 \right) < t \cdot \left(\frac{n}{t} + 1 - 1 \right) = n,$$

but n cannot be strictly less than itself, contradiction. □

Here's another example, which might be a bit clearer.

Example 6.2.1. *In any group of thirteen people, at least two people were born in the same month. Why? Well, there are twelve months (holes) in a year. So each person (pigeon) is classified by which month is their birth month (put into exactly one hole). Since there are thirteen pigeons put into twelve holes, there must be a month (hole) with at least $\lceil \frac{13}{12} \rceil = 2$ people (pigeons), by the pigeonhole principle.*

While the setup may appear a bit strange, the idea behind this is probably something that you already understand.

Example 6.2.2. *Prove that in a class of any size, if the average on a quiz is 7 points out of 10 points total, then at least one person must have scored at least 7 points on the quiz.*
Solution: *Suppose that there are n students in the class, and that their scores are s_1 for student 1, s_2 for student 2, ..., and s_n for student n. We can compute the average by summing all of their scores, and dividing by the number of students. That is, the average score is:*

$$7 = \frac{\sum_{j=1}^{n} s_j}{n}.$$

Multiplying both sides of this by n gives us that the total number of points scored by all of the students put together is $7n$. These $7n$ points are our pigeons, and their holes are the individual student scores. So by the pigeonhole principle, there must be at least one hole (student score) with at least $\frac{7n}{n} = 7$ pigeons (points).

Now we present some examples where the pigeonhole principle is an integral component of the solution, but there are more steps to complete.

Example 6.2.3. *Prove that in any party with six people, there are at least three mutual acquaintances, or at least three mutual strangers.*
Solution: *Pick one person from any of the people at the party and call her Alice. There are five people besides Alice. Now, either Alice knows these people or she doesn't. So there is one hole for people she knows, and another hole for people she does not know. There are five people to be put in these categories, so either she knows at least $\lceil \frac{5}{2} \rceil = 3$ people, or she does not know at least $\lceil \frac{5}{2} \rceil = 3$ people, by php.*
If she knows at least three people, choose three of the people she knows. Call them Bob, Charlie, and Dave. If any of them know one another, then that pair, along with Alice, forms a triple of acquainted people. If none of Bob, Charlie, and Dave know one another, then they form a triple of strangers.
If she does not know at least three people, choose three of the people she does not know. Call them Brandi, Candi, and Delores. If any of them do not know one another, then that pair, along with Alice, forms a triple of mutually unacquainted people. If none of Brandi, Candi, and Delores are unacquainted, then they form a triple of friends.

The following example is more involved, but it is worth going through carefully.

Example 6.2.4. *Suppose that a company sends out no more than 45 letters in a given 30-day period, at least one each day. Show that there is a period of consecutive days during which exactly 14 letters are sent out.*
Solution: *Define the set* $A := \{a_j : j = 1, \dots 30\}$*, where* a_j *denotes the total number of letters sent by the end of day* j*. Let* $b_j = a_j + 14$ *for* $j = 1, \dots, 30$*, and* $B := \{b_j : j = 1, \dots 30\}$*. Notice that both of the sets* A *and* B *are subsets of the interval* $[1, 59]$*, as they sent out no more than 45 total letters, and 59=45+14, the largest possible value of the set* B*. Now, by definition,* $|A| = |B| = 30$*. So there are 60 total elements to consider. However, all 60 of these are natural numbers between 1 and 59, inclusive. So there are 60 pigeons, and 59 holes. Therefore, by the pigeonhole principle, there must be a hole with at least* $\left\lceil \frac{60}{59} \right\rceil = 2$ *pigeons in it. That means that there must be two elements that are actually the same number. Now, since the company sends out at least one letter every day, there cannot be distinct* i *and* j *such that* $a_i = a_j$*. Similarly, there cannot be distinct* i *and* j *such that* $b_i = b_j$*, as the elements of* B *are just elements of* A *plus 14. So if two of the elements are equal, it must be that for some* k *and* ℓ*,* $a_k = b_\ell$*. However, recall that* $b_\ell = a_\ell + 14$*, which means that* $a_k = a_\ell + 14$*, or that the company sent out exactly 14 letters between days* k *and* ℓ*.*

6.2.1 Homework

Problem 6.2.1. One week, I sold 25 pies at my bakery. Prove that there must have been a day where I sold at least four pies.

Problem 6.2.2. Suppose that instead of writing down any student's name in my grade book, I just write the first letter of their first name. Will this scheme work if I have 27 students in my class?

Problem 6.2.3. Suppose I improve upon the scheme from the previous problem and instead write the first letter of the first name then the first letter of the last name of each student (for example, David Gilmour would be coded DG). What is the maximum number of students I could possibly have before there would necessarily be a problem?

Problem 6.2.4. For natural numbers n and m, suppose I have a set of n points, each on at least one of m lines in the plane. Prove that there must be a line with at least $\frac{n}{m}$ points on it.

Problem 6.2.5. (*) Prove that any polytope must have at least two faces with the same number of edges.

Problem 6.2.6. For natural numbers n and m, suppose I have a set of n points, each on at least one of m lines in space. Prove that there must be a line with at least $\frac{n}{m}$ points on it.

Problem 6.2.7. Suppose I make stuffed animals. One day, I decided to make three punk-rock pigeon dolls, with pierced ears. All together, they had ten piercings. Prove there must be at least one pigeon with at least four holes.

6.3 Permutations and combinations

HOMEWORK: 6.3 # 1–4

- permutation, $P(n,r)$, combination, $C(n,r)$, $\binom{n}{r}$, double counting

A *permutation* of r elements chosen from n is an **ordered** list of r of the n elements. Recall that for a natural number, n, $n! = n \times (n-1) \times \cdots \times 2 \times 1$, and $0! = 1$. The number of permutations of r elements chosen from n is

$$P(n,r) = \frac{n!}{(n-r)!} = \underbrace{n \times (n-1) \times \cdots \times (n-(r-1))}_{r \text{ factors}}.$$

To see this, suppose that you have n objects, and you want to put your top favorite r in order. Well, you have n choices for your favorite, $(n-1)$ choices for your second favorite, and so on, until you have made r selections. Because we have to choose the first AND the second AND the third, etc. we apply the product rule. We can also write this as

$$P(n,n) = \frac{n!}{(n-r)!} = \frac{n!}{0!} = \frac{n!}{1} = n!$$

Example 6.3.1. *How many ways can the top three medals be handed out for a race run by ten people?*
Solution: *We are putting three people in order, chosen from ten total, so the answer is*

$$P(10,3) = 10 \times 9 \times 8 = 720.$$

A *combination* is like a permutation, but we do not care about the order. The number of ways to choose r objects from n (irrespective of the order in which they were chosen) is written $C(n,r)$ or $\binom{n}{r}$, read "n choose r."

$$C(n,r) = \binom{n}{r} = \frac{P(n,r)}{r!} = \frac{n!}{r!(n-r)!}.$$

To count the number of ways to choose r objects from n, you can think of it as counting the permutations, $P(n, r)$, and then using the division rule to divide out by the number of symmetries, which is the number of lists of the same elements, but in different orders. So we need to divide by the number of ways to order r elements chosen from r, or $r!$.

Example 6.3.2. *How many different triples of people can get medals (irrespective of order) in a race run by ten people?*
Solution: *We are choosing three people from ten, so the answer is*

$$\binom{10}{3} = \frac{10!}{3!(10-3)!} = \frac{10 \times 9 \times 8 \times 7!}{3!7!} = \frac{10 \times 9 \times 8}{3!} = \frac{10 \times 9 \times 8}{3 \times 2 \times 1} = 120.$$

It isn't always so obvious whether or not order matters. Consider the next two examples.

Example 6.3.3. *I could make 10! different playlists by reordering ten songs every possible way.*

Example 6.3.4. *There are $\binom{52}{5}$ hands of poker, because it doesn't matter what order you receive your cards (at least for determining who wins).*

Example 6.3.5. *While these straightforward applications are useful, it's also important to fit these into a larger context. Prove that*

$$\binom{n}{r} = \binom{n}{(n-r)}.$$

Solution 1: *We can just write out the definition to see*

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{n!}{(n-(n-r))!(n-r)!} = \binom{n}{(n-r)}.$$

Solution 2: *The number of ways to choose r objects from n is $\binom{n}{r}$. However, choosing r objects is the same as* **not** *choosing $(n-r)$ objects from n, which has $\binom{n}{n-r}$ possibilities.*

In both of the next two examples, the second solution given is done by *double counting*, that is, counting a particular quantity twice, in two different ways, to establish an otherwise non-obvious relationship.

Example 6.3.6. *Prove that*

$$\binom{n+1}{r} = \binom{n}{(r-1)} + \binom{n}{r}.$$

Solution 1: *We can just write out the definitions to see*

$$\begin{aligned}
\binom{n}{(r-1)} + \binom{n}{r} &= \frac{n!}{(r-1)!(n-(r-1))!} + \frac{n!}{r!(n-r)!} \\
&= \frac{n!}{(r-1)!(n-r+1)!} + \frac{n!}{r!(n-r)!} \\
&= \frac{n!r}{(r-1)!(n-r+1)!r} + \frac{n!(n-r+1)}{r!(n-r)!(n-r+1)} \\
&= \frac{n!(n+1)}{r!(n-r+1)!} \\
&= \frac{(n+1)!}{r!((n+1)-r)!} \\
&= \binom{n+1}{r}.
\end{aligned}$$

Solution 2: *We can count the number of ways to choose r objects from $n+1$ two different ways. First, we say that it is the definition of $\binom{n+1}{r}$. Then we count it a second way. We pick one object arbitrarily and call it x. If x is chosen, then we are choosing $r-1$ objects from the remaining n, which has $\binom{n}{r-1}$ possibilities. If we did not choose x, then we have r objects to choose from the remaining n objects. Since we either choose x or we do not choose x, but we cannot do both, we appeal to the sum rule, and add these two possibilities to get the total number of ways to choose r objects from $n+1$.*

We finish with a result that you are likely to see in the future.

Theorem 6.3.1 (Binomial Theorem)**.** *Given $a, b \in \mathbb{R}$, and $n \in \mathbb{N}$,*

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^j b^{n-j}.$$

Proof. Here, we merely sketch the proof. Basically, for each factor of the product

$$\underbrace{(x+y)(x+y)\cdots(x+y)}_{n \text{ factors}},$$

we have to choose either x or y. So we consider all possible strings of length n consisting of the letters x or y. These are then grouped by how many xs or ys appear in each string. How many strings have k copies of y? Precisely the number of ways to choose k of the factors to contribute a y, out of n total factors, or $\binom{n}{k}$. The value of that monomial will be $x^{n-k}y^k$. This holds for all values of k, and the theorem follows. □

Example 6.3.7. *Find the coefficient of the x^9y^6 term in the polynomial $(x+y)^{15}$.*
Solution: *We could either FOIL ourselves to death, or use the Binomial Theorem to see that the coefficient will be $\binom{15}{6}$.*

6.3.1 Homework

Problem 6.3.1. How many ways can I arrange the numbers from 1 to n, for a natural number n?

Problem 6.3.2. How many ways can I color one number blue, a different number red, and yet a third number green, with numbers chosen from 1 to n, for a natural number $n \geq 3$?

Problem 6.3.3. Suppose a valid product code consists of three single-digit numbers, followed by the letters A, B, and C, in some order. How many valid product codes are there?

Problem 6.3.4. Prove that for any natural numbers n, with $n > 2$, we have that $\binom{n}{2} \leq P(n, 2)$.

Problem 6.3.5. (*) Prove that for natural numbers n and k, with $n > k > 2$, we have that $\binom{2n}{k} \geq 2\binom{n}{k}$.

Problem 6.3.6. How possible combinations are there for a combination lock numbered 1 to 60, assuming the numbers cannot repeat?

Problem 6.3.7. How many ways can I arrange the numbers from m to n, for natural numbers $m < n$?

7 EXTRA TOPICS

7.1 Graph theory

- graph, vertex, edge, simple, connected, complete, planar, Euler's formula

A **graph** is a pair of sets, V, the **vertices** (plural of **vertex**), and E, the **edges**, where E consists entirely of two-element subsets of V. A graph is **simple** if every edge is between two *different* vertices, and no pair of vertices has more than one edge. A **subgraph** of a graph G is a graph whose vertex set is a subset of the vertices of G, and whose edges are a subset of the edges of G. A graph is **connected** if one can get from any vertex to any other vertex

by a path of vertices connected by edges in the graph. A graph is planar if it can be drawn without any two edges crossing. A graph is **complete** if every possible edge is present. We write K_n to denote the complete graph on n vertices.

Proposition 7.1.1 (Euler's formula)**.** *Suppose G is a simple, connected, planar graph with v vertices, $e \geq 1$ edges, and f faces, then $v + f = e + 2$.*

Proof. Proceed by induction on the number of edges. Start with a graph consisting of only one edge. Notice that it has two vertices and one face, satisfying the formula. For our induction hypothesis, suppose that the formula holds for all simple, connected, planar graphs with n edges. Now, to show that the formula will hold for any simple, connected, planar graph with $n+1$ edges, we watch what happens whenever we add an edge. Notice that any time you add an edge, you either add a vertex or a face. Therefore, we are done, by induction. □

Proposition 7.1.2. *Suppose G is a simple, connected, planar graph with $e \geq 2$ edges, and f faces, then $3f \leq 2e$.*

Proof. Draw the graph. For each edge in the graph, draw a little dog ear on each side, so that each edge looks like a wiener dog. Observe that there are two dog ears on each edge, so the number of dog ears is exactly $2e$. Notice that each face needs **at least** three dog ears, so the number of dog ears is $\geq 3f$. □

Combining Propositions 7.1.1 and 7.1.2 yields the following corollary.

Corollary 7.1.3. *Suppose G is a planar graph with $e \geq 2$ edges, and v vertices, then $e - 3v + 6 \leq 0$.*

Note that the complete graph on four vertices is planar, as it can be drawn without any edges crossing, but the complete graph on five vertices is NOT planar, as it has five vertices and ten edges, and therefore fails to obey the inequality in Corollary 7.1.3.

A graph is called **bipartite** if the set of vertices can be written as a union of two disjoint subsets, V_1 and V_2, so that no pair of vertices are adjacent in V_1 and no pair of vertices are adjacent in V_2. That is, all of the edges are of the form $\{v_1, v_2\}$ where $v_1 \in V_1$, and $v_2 \in V_2$. Moreover, we write $K_{s,t}$ to denote the bipartite graph with the maximum number of edges between two disjoint vertex sets of sizes s and t. This graph is called the **complete bipartite** graph on s and t vertices, even though it is technically not complete unless $s, t \leq 1$.

7.1.1 Homework

Problem 7.1.1. Prove that a bipartite graph cannot have K_3 as a subgraph.

Problem 7.1.2. (*) Modify the proof of Proposition 7.1.2 to get a tighter bound for bipartite graphs, then prove a stronger version of Corollary 7.1.3 to show that $K_{3,3}$ must have a crossing.

7.2 Relations

- relation, reflexive, symmetric, transitive, equivalence relation

A **binary relation**, $\mathcal{R}$, (often just called a relation) from a set A to a set B is a subset of the Cartesian product, $A \times B$. If $B = A$, we will call $\mathcal{R}$ a relation on A. If $(x, y) \in \mathcal{R}$, we will write $x\mathcal{R}y$, and say that, "a is related to y under $\mathcal{R}$." Here are some *possible* attributes of a relation, $\mathcal{R}$, on A:

name	description
reflexivity	$\forall a \in A, a\mathcal{R}a$
symmetry	$\forall a, b \in A, a\mathcal{R}b \to b\mathcal{R}a$
transitivity	$\forall a, b, c \in A, a\mathcal{R}b, b\mathcal{R}c \to a\mathcal{R}c$

I like to remember these properties with the mnemonic "RST,123," because Reflexivity concerns 1 element at a time, Symmetry concerns 2 elements at a time, and Transitivity concerns 3 elements at a time. You still have to remember how said elements are related for each property to hold though.

Example 7.2.1. *Let A be the set $\{a, b, c\}$. So any relation on A will be a subset of the Cartesian product,*

$$A \times A = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}.$$

Define the relation $\mathcal{R}_1$ to be $\{(a, a), (a, b), (a, c), (b, b), (b, c), (c, c)\}$. We have that R_1 is symmetric, because every element is related to itself. It's also transitive. However, it is NOT symmetric, because although $a\mathcal{R}_1b$, we do not have that $b\mathcal{R}_1a$. Define the relation $\mathcal{R}_2$ to be $\{(a, a), (a, b), (b, a), (b, b), (b, c), (c, b)\}$. We have that R_2 is NOT symmetric, because c is not related to itself under $\mathcal{R}_2$. It NOT transitive, because we have $a\mathcal{R}_2b$, and $b\mathcal{R}_2c$, but we do not have $a\mathcal{R}_2c$. However, it is symmetric.

Example 7.2.2. *Consider the relation "$\leq$" on the real numbers. Notice that it is reflexive and transitive, but not symmetric, as $1 \leq 2$, but $2 \not\leq 1$.*

If a relation is reflexive, symmetric, and transitive, then it is called an **equivalence relation**. Some notable examples of equivalence relations are "$=$" on just about any set we can imagine, and congruence modulo a natural number on the set of integers. Notice that by this definition, "$\leq$" is NOT an equivalence relation, as it is not symmetric.

7.2.1 Homework

Problem 7.2.1. Give an example of an equivalence relation on the set $\{a, b, c\}$.

Problem 7.2.2. Give an example of a relation on the set $\{a, b, c\}$ that is transitive, but not symmetric.

7.3 Systems of Equations

HOMEWORK:

- row vector, column vector, matrix addition, matrix multiplication, substitution, identity matrix, augmented matrices, elementary row operations

Example 7.3.1. *Solve*

$$\begin{cases} x+2y &= 5 \\ 3x\ -y &= 1 \end{cases}$$

Example 7.3.2. *Solve*

$$\begin{cases} x+2y &= 5 \\ 2x\ +4y &= 10 \end{cases}$$

Example 7.3.3. *Solve*

$$\begin{cases} x+y &= 5 \\ 3x\ +3y &= 10 \end{cases}$$

A **matrix** is just a box of numbers, like this:

$$\begin{bmatrix} 1 & 1 & -3 \\ 3 & 10 & 0 \end{bmatrix}$$

That is a **size** 2×3 matrix. It has two rows and three columns. We rowed boats before we built columns... which is why rows come before columns... or at least that's how I remember it. A matrix of one row is called a **row vector**, and a matrix of one column is called a **column vector**.

We can add two matrices of the same size componentwise.

Example 7.3.4.

$$\begin{bmatrix} 1 & 1 & -3 \\ 3 & 1 & 6 \end{bmatrix} + \begin{bmatrix} 5 & -1 & 7 \\ 4 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 0 & 4 \\ 7 & 2 & 7 \end{bmatrix}$$

We can also do matrix multiplication between an $\ell \times m$ matrix and an $m \times n$ matrix. The resultant matrix will be of size $\ell \times n$. The entry in location (i, j) will be formed by taking the elements of row i from the first matrix and multiplying them by the elements of column j of the second matrix, and adding those products together.

Example 7.3.5.

$$\begin{bmatrix} 1 & 1 & -3 \\ 3 & 1 & 6 \end{bmatrix} \times \begin{bmatrix} 5 \\ 1 \\ 2 \end{bmatrix} = \begin{bmatrix} (1)(5)+(1)(1)+(-3)(2) \\ (3)(5)+(1)(1)+(6)(2) \end{bmatrix} = \begin{bmatrix} 0 \\ 28 \end{bmatrix}$$

We can also multiply a matrix by a constant. To do this, we can think of multiplying the matrix by a 1×1 matrix consisting of just the constant.

Example 7.3.6.

$$4 \begin{bmatrix} 1 & 0 & -1 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 0 & -4 \\ 12 & 8 & 4 \end{bmatrix}.$$

For each natural number n, there is a special $n \times n$ matrix called the **identity matrix,** usually denoted I or I_n. It has ones down the diagonal and zeros everywhere else. If you multiply a matrix by the appropriately-sized identity, you will get the original matrix back.

Example 7.3.7.

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \times \begin{bmatrix} 5 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 1 \end{bmatrix}$$

We can also produce special matrices called **augmented matrices**, which are formed by using the coefficients of systems of linear equations, as well as the constant term. We can often solve a system of equations by using special rules (listed below) to try to get the left hand side of the augmented matrix to look like an identity matrix. The special rules are called **elementary row operations**:

1. Swap two rows
2. Multiply a row by a constant
3. Replace a row by its sum with a constant multiple of another row

Example 7.3.8. *We can write this system as an augmented matrix.*

$$\begin{cases} x+2y &= 5 \\ 3x-y &= 1 \end{cases}$$

We just write down the coefficients, and put a vertical bar where the equals signs are.

$$\left[\begin{array}{cc|c} 1 & 2 & 5 \\ 3 & -1 & 1 \end{array}\right]$$

Now we will use elementary row operations to solve the system. We start by adding negative three times the first row to the second row, to get

$$\left[\begin{array}{cc|c} 1 & 2 & 5 \\ 0 & -7 & -14 \end{array}\right]$$

Next, we multiply the bottom row by -1/7 to get

$$\left[\begin{array}{cc|c} 1 & 2 & 5 \\ 0 & 1 & 2 \end{array}\right]$$

Now we add negative two times the bottom row to the top row to get

$$\left[\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 2 \end{array}\right]$$

This can be converted back into equations to yield the solution

$$\left\{\begin{array}{ll} x+(0)y & = 1 \\ (0)x+y & = 2 \end{array}\right.$$

That is, $x = 1$ *and* $y = 2$.

7.3.1 Homework

$$\left[\begin{array}{ccc} 1 & 1 & -3 \\ 3 & 1 & 6 \end{array}\right] + \left[\begin{array}{ccc} 5 & -1 & 7 \\ 4 & 1 & 1 \end{array}\right] = \left[\begin{array}{ccc} 6 & 0 & 4 \\ 7 & 2 & 7 \end{array}\right]$$

Problem 7.3.1. Compute

$$\left[\begin{array}{ccc} 1 & 0 & -1 \\ 2 & -5 & 6 \end{array}\right] + \left[\begin{array}{ccc} 0 & -2 & 9 \\ 0 & -1 & 1 \end{array}\right]$$

Problem 7.3.2. Compute

$$\left[\begin{array}{ccc} 1 & 0 & 1 \\ 2 & 0 & -1 \end{array}\right] \times \left[\begin{array}{cc} 0 & -2 \\ 0 & 1 \\ 2 & 3 \end{array}\right]$$

Problem 7.3.3. Solve

$$\left\{\begin{array}{ll} x+y & = 7 \\ 3x-2y & = 3 \end{array}\right.$$

Problem 7.3.4. Solve

$$\left\{\begin{array}{llll} x & +y & +z & = 6 \\ x & -2y & & = 0 \\ & y & +2z & = 8 \end{array}\right.$$