Strong Induction

Investigate!

Start with a square piece of paper. You want to cut this square into smaller squares, leaving no waste (every piece of paper you end up with must be a square). Obviously it is possible to cut the square into 4 squares. You can also cut it into 9 squares. It turns out you can cut the square into 7 squares (although not all the same size). What other numbers of squares could you end up with?

Attempt the above activity before proceeding

Sometimes, to prove that $P(k+1)$ is true, it would be helpful to know that $P(k)$ *and* $P(k-1)$ *and* $P(k-2)$ are all true. Consider the following puzzle:

> You have a rectangular chocolate bar, made up of n identical squares of chocolate. You can take such a bar and break it along any row or column. How many times will you have to break the bar to reduce it to n single chocolate squares?

At first, this question might seem impossible. Perhaps I meant to ask for the *smallest* number of breaks needed? Let's investigate.

Start with some small cases. If $n = 2$, you must have a 1×2 rectangle, which can be reduced to single pieces in one break. With $n = 3$, we must have a 1×3 bar, which requires two breaks: the first break creates a single square and a 1×2 bar, which we know takes one (more) break.

What about $n = 4$? Now we could have a 2×2 bar, or a 1×4 bar. In the first case, break the bar into two 2×2 bars, each which require one more break (that's a total of three breaks required). If we started with a 1×4 bar, we have choices for our first break. We could break the bar in half, creating two 1×2 bars, or we could break off a single square, leaving a 1×3 bar. But either way, we still need two more breaks, giving a total of three.

It is starting to look like no matter how we break the bar (and no matter how the n squares are arranged into a rectangle), we will always have the same number of breaks required. It also looks like that number is one less than n:

Conjecture 2.5.4 *Given a n-square rectangular chocolate bar, it always takes $n-1$ breaks to reduce the bar to single squares.*

It makes sense to prove this by induction because after breaking the bar once, you are left with *smaller* chocolate bars. Reducing to smaller cases is what induction is all about. We can inductively assume we already know how to deal with these smaller bars. The problem is, if we are trying to prove the inductive case about a $(k+1)$-square bar, we don't know that after the first break the remaining bar will have k squares. So we really need to assume that our conjecture is true for all cases less than $k+1$.

Is it valid to make this stronger assumption? Remember, in induction we are attempting to prove that $P(n)$ is true for all n. What if that were not the case? Then there would be some first n_0 for which $P(n_0)$ was false. Since n_0 is the *first* counterexample, we know that $P(n)$ is true for all $n < n_0$. Now we proceed to prove that $P(n_0)$ is actually true, based on the assumption that $P(n)$ is true for all smaller n.

This is quite an advantage: we now have a stronger inductive hypothesis. We can assume that $P(1)$, $P(2)$, $P(3)$, ... $P(k)$ is true, just to show that $P(k+1)$ is true. Previously, we just assumed $P(k)$ for this purpose.

It is slightly easier if we change our variables for strong induction. Here is what the formal proof would look like:

Strong Induction Proof Structure.

Again, start by saying what you want to prove: "Let $P(n)$ be the statement..." Then establish two facts:

1. Base case: Prove that $P(0)$ is true.
2. Inductive case: Assume $P(k)$ is true for all $k < n$. Prove that $P(n)$ is true.

Conclude, "therefore, by strong induction, $P(n)$ is true for all $n > 0$."

Of course, it is acceptable to replace 0 with a larger base case if needed.[5]

Let's prove our conjecture about the chocolate bar puzzle:

Proof. Let $P(n)$ be the statement, "it takes $n-1$ breaks to reduce a n-square chocolate bar to single squares."

Base case: Consider $P(2)$. The squares must be arranged into a 1×2 rectangle, and we require $2-1=1$ breaks to reduce this to single squares.

Inductive case: Fix an arbitrary $n \geq 2$ and assume $P(k)$ is true for all $k < n$. Consider a n-square rectangular chocolate bar. Break the bar once along any row or column. This results in two chocolate bars, say of sizes a and b. That is, we have an a-square rectangular chocolate bar, a b-square rectangular chocolate bar, and $a + b = n$.

We also know that $a < n$ and $b < n$, so by our inductive hypothesis, $P(a)$ and $P(b)$ are true. To reduce the a-square bar to single squares takes

[5]Technically, strong induction does not require you to prove a separate base case. This is because when proving the inductive case, you must show that $P(0)$ is true, assuming $P(k)$ is true for all $k < 0$. But this is not any help so you end up proving $P(0)$ anyway. To be on the safe side, we will always include the base case separately.

$a-1$ breaks; to reduce the b-square bar to single squares takes $b-1$ breaks. Doing this results in our original bar being reduced to single squares. All together it took the initial break, plus the $a-1$ and $b-1$ breaks, for a total of $1+a-1+b-1=a+b-1=n-1$ breaks. Thus $P(n)$ is true.

Therefore, by strong induction, $P(n)$ is true for all $n \geq 2$. QED

Here is a more mathematically relevant example:

Example 2.5.5

Prove that any natural number greater than 1 is either prime or can be written as the product of primes.

Solution. First, the idea: if we take some number n, maybe it is prime. If so, we are done. If not, then it is composite, so it is the product of two smaller numbers. Each of these factors is smaller than n (but at least 2), so we can repeat the argument with these numbers. We have reduced to a smaller case.

Now the formal proof:

Proof. Let $P(n)$ be the statement, "n is either prime or can be written as the product of primes." We will prove $P(n)$ is true for all $n \geq 2$.

Base case: $P(2)$ is true because 2 is indeed prime.

Inductive case: assume $P(k)$ is true for all $k < n$. We want to show that $P(n)$ is true. That is, we want to show that n is either prime or is the product of primes. If n is prime, we are done. If not, then n has more than 2 divisors, so we can write $n = m_1 \cdot m_2$, with m_1 and m_2 less than n (and greater than 1). By the inductive hypothesis, m_1 and m_2 are each either prime or can be written as the product of primes. In either case, we have that n is written as the product of primes.

Thus by the strong induction, $P(n)$ is true for all $n \geq 2$. ■

Whether you use regular induction or strong induction depends on the statement you want to prove. If you wanted to be safe, you could always use strong induction. It really is *stronger*, so can accomplish everything "weak" induction can. That said, using regular induction is often easier since there is only one place you can use the induction hypothesis. There is also something to be said for *elegance* in proofs. If you can prove a statement using simpler tools, it is nice to do so.

As a final contrast between the two forms of induction, consider once more the stamp problem. Regular induction worked by showing how to increase postage by one cent (either replacing three 5-cent stamps with two 8-cent stamps, or three 8-cent stamps with five 5-cent stamps). We could give a slightly different proof using strong induction. First, we could show *five* base cases: it is possible to make 28, 29, 30, 31, and 32 cents (we would actually say how each of these is made). Now assume that it is possible to make k cents of postage for all $k < n$ as long as $k \geq 28$. As long as $n > 32$, this means in particular we can make $k = n - 5$ cents. Now add a 5-cent stamp to get make n cents.

Exercises

1. On the way to the market, you exchange your cow for some magic dark chocolate espresso beans. These beans have the property that every night at midnight, each bean splits into two, effectively doubling your collection. You decide to take advantage of this and each morning (around 8am) you eat 5 beans.

(a) Explain why it is true that *if* at noon on day n you have a number of beans ending in a 5, then at noon on day $n + 1$ you will still have a number of beans ending in a 5.

(b) Why is the previous fact not enough to conclude that you will always have a number of beans ending in a 5? What additional fact would you need?

(c) Assuming you have the additional fact in part (b), and have successfully proved the fact in part (a), how do you know that you will always have a number of beans ending in a 5? Illustrate what is going on by carefully explaining how the two facts above prove that you will have a number of beans ending in a 5 on *day 4* specifically. In other words, explain why induction works in this context.

2. Use induction to prove for all $n \in \mathbb{N}$ that $\displaystyle\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$.

3. Prove that $7^n - 1$ is a multiple of 6 for all $n \in \mathbb{N}$.

4. Prove that $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ for all $n \geq 1$.

5. Prove that $F_0 + F_2 + F_4 + \cdots + F_{2n} = F_{2n+1} - 1$ where F_n is the nth Fibonacci number.

6. Prove that $2^n < n!$ for all $n \geq 4$. (Recall, $n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n$.)

7. Prove, by mathematical induction, that $F_0 + F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$, where F_n is the nth Fibonacci number ($F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$).

8. Zombie Euler and Zombie Cauchy, two famous zombie mathematicians, have just signed up for Twitter accounts. After one day, Zombie Cauchy has more followers than Zombie Euler. Each day after that, the number of new followers of Zombie Cauchy is exactly the same as the number of new followers of Zombie Euler (and neither lose any followers). Explain how a proof by mathematical induction can show that on every day after the first day, Zombie Cauchy will have more followers than Zombie Euler. That is, explain what the base case and inductive case are, and why they together prove that Zombie Cauchy will have more followers on the 4th day.

9. Find the largest number of points which a football team cannot get exactly using just 3-point field goals and 7-point touchdowns (ignore the possibilities of safeties, missed extra points, and two point conversions). Prove your answer is correct by mathematical induction.

10. Prove that the sum of n squares can be found as follows

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

11. Prove that the sum of the interior angles of a convex n-gon is $(n-2)\cdot 180°$. (A convex n-gon is a polygon with n sides for which each interior angle is less than $180°$.)

12. What is wrong with the following "proof" of the "fact" that $n+3 = n+7$ for all values of n (besides of course that the thing it is claiming to prove is false)?
Proof. Let $P(n)$ be the statement that $n + 3 = n + 7$. We will prove that $P(n)$ is true for all $n \in \mathbb{N}$. Assume, for induction that $P(k)$ is true. That is, $k + 3 = k + 7$. We must show that $P(k + 1)$ is true. Now since $k + 3 = k + 7$, add 1 to both sides. This gives $k + 3 + 1 = k + 7 + 1$. Regrouping $(k+1)+3 = (k+1)+7$. But this is simply $P(k+1)$. Thus by the principle of mathematical induction $P(n)$ is true for all $n \in \mathbb{N}$. QED

13. The proof in the previous problem does not work. But if we modify the "fact," we can get a working proof. Prove that $n + 3 < n + 7$ for all values of $n \in \mathbb{N}$. You can do this proof with algebra (without induction), but the goal of this exercise is to write out a valid induction proof.

14. Find the flaw in the following "proof" of the "fact" that $n < 100$ for every $n \in \mathbb{N}$.
Proof. Let $P(n)$ be the statement $n < 100$. We will prove $P(n)$ is true for all $n \in \mathbb{N}$. First we establish the base case: when $n = 0$, $P(n)$ is true, because $0 < 100$. Now for the inductive step, assume $P(k)$ is true. That is, $k < 100$. Now if $k < 100$, then k is some number, like 80. Of course

$80 + 1 = 81$ which is still less than 100. So $k + 1 < 100$ as well. But this is what $P(k + 1)$ claims, so we have shown that $P(k) \to P(k + 1)$. Thus by the principle of mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$. QED

15. While the above proof does not work (it better not since the statement it is trying to prove is false!) we can prove something similar. Prove that there is a strictly increasing sequence $a_1, a_2, a_3, \ldots$ of numbers (not necessarily integers) such that $a_n < 100$ for all $n \in \mathbb{N}$. (By **strictly increasing** we mean $a_n < a_{n+1}$ for all n. So each term must be larger than the last.)

16. What is wrong with the following "proof" of the "fact" that for all $n \in \mathbb{N}$, the number $n^2 + n$ is odd?
Proof. Let $P(n)$ be the statement "$n^2 + n$ is odd." We will prove that $P(n)$ is true for all $n \in \mathbb{N}$. Suppose for induction that $P(k)$ is true, that is, that $k^2 + k$ is odd. Now consider the statement $P(k + 1)$. Now $(k + 1)^2 + (k + 1) = k^2 + 2k + 1 + k + 1 = k^2 + k + 2k + 2$. By the inductive hypothesis, $k^2 + k$ is odd, and of course $2k + 2$ is even. An odd plus an even is always odd, so therefore $(k + 1)^2 + (k + 1)$ is odd. Therefore by the principle of mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$. QED

17. Now give a valid proof (by induction, even though you might be able to do so without using induction) of the statement, "for all $n \in \mathbb{N}$, the number $n^2 + n$ is even."

18. Prove that there is a sequence of positive real numbers $a_0, a_1, a_2, \ldots$ such that the partial sum $a_0 + a_1 + a_2 + \cdots + a_n$ is strictly less than 2 for all $n \in \mathbb{N}$. Hint: think about how you could define what a_{k+1} is to make the induction argument work.

19. Prove that every positive integer is either a power of 2, or can be written as the sum of distinct powers of 2.

20. Prove, using strong induction, that every natural number is either a Fibonacci number or can be written as the *sum* of *distinct* Fibonacci numbers.

21. Use induction to prove that if n people all shake hands with each other, that the total number of handshakes is $\frac{n(n-1)}{2}$.

22. Suppose that a particular real number x has the property that $x + \frac{1}{x}$ is an integer. Prove that $x^n + \frac{1}{x^n}$ is an integer for all natural numbers n.

23. Use induction to prove that $\sum_{k=0}^{n} \binom{n}{k} = 2^n$. That is, the sum of the nth row of Pascal's Triangle is 2^n.

24. Use induction to prove $\binom{4}{0} + \binom{5}{1} + \binom{6}{2} + \cdots + \binom{4+n}{n} = \binom{5+n}{n}$. (This is an example of the hockey stick theorem.)

25. Use the product rule for logarithms ($\log(ab) = \log(a) + \log(b)$) to prove, by induction on n, that $\log(a^n) = n\log(a)$, for all natural numbers $n \geq 2$.

26. Let $f_1, f_2, \ldots, f_n$ be differentiable functions. Prove, using induction, that

$$(f_1 + f_2 + \cdots + f_n)' = f_1' + f_2' + \cdots + f_n'.$$

You may assume $(f + g)' = f' + g'$ for any differentiable functions f and g.

27. Suppose $f_1, f_2, \ldots, f_n$ are differentiable functions. Use mathematical induction to prove the generalized product rule:

$$(f_1 f_2 f_3 \cdots f_n)' = f_1' f_2 f_3 \cdots f_n + f_1 f_2' f_3 \cdots f_n + f_1 f_2 f_3' \cdots f_n + \cdots + f_1 f_2 f_3 \cdots f_n'.$$

You may assume the product rule for two functions is true.

28. You will prove that the Fibonacci numbers satisfy the identity $F_n^2 + F_{n+1}^2 = F_{2n+1}$. One way to do this is to prove the more general identity,

$$F_m F_n + F_{m+1} F_{n+1} = F_{m+n+1},$$

and realize that when $m = n$ we get our desired result.

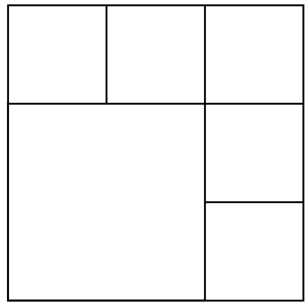
Note that we now have two variables, so we want to prove this for all $m \geq 0$ *and* all $n \geq 0$ at the same time. For each such pair (m, n), let $P(m, n)$ be the statement $F_m F_n + F_{m+1} F_{n+1} = F_{m+n+1}$

(a) First fix $m = 0$ and give a proof by mathematical induction that $P(0, n)$ holds for all $n \geq 0$. Note this proof will be very easy.

(b) Now fix an arbitrary n and give a proof by *strong* mathematical induction that $P(m, n)$ holds for all $m \geq 0$.

(c) You can now conclude that $P(m, n)$ holds for all $m, n \geq 0$. Do you believe that? Explain why this sort of induction is valid. For example, why do your proofs above guarantee that $P(2, 3)$ is true?

29. Given a square, you can cut the square into smaller squares by cutting along lines parallel to the sides of the original square (these lines do not need to travel the entire side length of the original square). For example, by cutting along the lines below, you will divide a square into 6 smaller squares:



Prove, using strong induction, that it is possible to cut a square into n smaller squares for any $n \geq 6$.

2.6 Chapter Summary

Investigate!

Each day your supply of magic chocolate covered espresso beans doubles (each one splits in half), but then you eat 5 of them. You have 10 at the start of day 0.

1. Write out the first few terms of the sequence. Then give a recursive definition for the sequence and explain how you know it is correct.

2. Prove, using induction, that the last digit of the number of beans you have on the nth day is always a 5 for all $n \geq 1$.

3. Find a closed formula for the nth term of the sequence and prove it is correct by induction.

Attempt the above activity before proceeding

In this chapter we explored sequences and mathematical induction. At first these might not seem entirely related, but there is a link: recursive reasoning. When we have many cases (maybe infinitely many), it is often easier to describe a particular case by saying how it relates to other cases, instead of describing it absolutely. For sequences, we can describe the nth term in the sequence by saying how it is related to the *previous* term. When showing a statement involving the variable n is true for all values of n, we can describe why the case for $n = k$ is true on the basis of why the case for $n = k - 1$ is true.

While thinking of problems recursively is often easier than thinking of them absolutely (at least after you get used to thinking in this way), our ultimate goal is to move beyond this recursive description. For sequences, we want to find *closed formulas* for the nth term of the sequence. For proofs, we want to know the statement is actually true for a particular n (not only under the assumption that the statement is true for the previous value of n). In this chapter we saw some methods for moving from recursive descriptions to absolute descriptions.

- If the terms of a sequence increase by a constant difference or constant ratio (these are both recursive descriptions), then the sequences are arithmetic or geometric, respectively, and we have closed formulas for each of these based on the initial terms and common difference or ratio.

- If the terms of a sequence increase at a polynomial rate (that is, if the differences between terms form a sequence with a polynomial closed formula), then the sequence is itself given by a polynomial closed formula (of degree one more than the sequence of differences).

- If the terms of a sequence increase at an exponential rate, then we expect the closed formula for the sequence to be exponential. These sequences often have relatively nice recursive formulas, and the *characteristic root technique* allows us to find the closed formula for these sequences.
- If we want to prove that a statement is true for all values of n (greater than some first small value), and we can describe why the statement being true for $n = k$ implies the statement is true for $n = k + 1$, then the *principle of mathematical induction* gives us that the statement is true for all values of n (greater than the base case).

Throughout the chapter we tried to understand *why* these facts listed above are true. In part, that is what proofs, by induction or not, attempt to accomplish: they explain why mathematical truths are in fact truths. As we develop our ability to reason about mathematics, it is a good idea to make sure that the methods of our reasoning are sound. The branch of mathematics that deals with deciding whether reasoning is good or not is *mathematical logic*, the subject of the next chapter.

Chapter Review

1. Find $3 + 7 + 11 + \cdots + 427$.

2. Consider the sequence $2, 6, 10, 14, \ldots, 4n + 6$.

(a) How many terms are there in the sequence?

(b) What is the second-to-last term?

(c) Find the sum of all the terms in the sequence.

3. Consider the sequence given by $a_n = 2 \cdot 5^{n-1}$.

(a) Find the first 4 terms of the sequence.

What sort of sequence is this?

(b) Find the *sum* of the first 25 terms. That is, compute $\sum_{k=1}^{25} a_k$.

4. Consider the sequence $5, 11, 19, 29, 41, 55, \ldots$. Assume $a_1 = 5$.

(a) Find a closed formula for a_n, the nth term of the sequence, by writing each term as a sum of a sequence. Hint: first find a_0, but ignore it when collapsing the sum.

(b) Find a closed formula again, this time using either polynomial fitting or the characteristic root technique (whichever is appropriate). Show your work.

(c) Find a closed formula once again, this time by recognizing the sequence as a modification to some well known sequence(s). Explain.

5. Use polynomial fitting to find a closed formula for the sequence $(a_n)_{n\geq 1}$:

$$4, 11, 20, 31, 44, \ldots.$$

6. Suppose the closed formula for a particular sequence is a degree 3 polynomial. What can you say about the closed formula for:

(a) The sequence of partial sums.

(b) The sequence of second differences.

7. Consider the sequence given recursively by $a_1 = 4$, $a_2 = 6$ and $a_n = a_{n-1} + a_{n-2}$.

(a) Write out the first 6 terms of the sequence.

(b) Could the closed formula for a_n be a polynomial? Explain.

8. The sequence $(a_n)_{n\geq 1}$ starts $-1, 0, 2, 5, 9, 14\ldots$ and has closed formula $a_n = \dfrac{(n+1)(n-2)}{2}$. Use this fact to find a closed formula for the sequence $(b_n)_{n\geq 1}$ which starts $4, 10, 18, 28, 40, \ldots$.

9. The in song *The Twelve Days of Christmas*, my true love gave to me first 1 gift, then 2 gifts and 1 gift, then 3 gifts, 2 gifts and 1 gift, and so on. How many gifts did my true love give me all together during the twelve days?

10. Consider the recurrence relation $a_n = 3a_{n-1} + 10a_{n-2}$ with first two terms $a_0 = 1$ and $a_1 = 2$.

(a) Write out the first 5 terms of the sequence defined by this recurrence relation.

(b) Solve the recurrence relation. That is, find a closed formula for a_n.

11. Consider the recurrence relation $a_n = 2a_{n-1} + 8a_{n-2}$, with initial terms $a_0 = 1$ and $a_1 = 3$.

(a) Find the next two terms of the sequence (a_2 and a_3).

(b) Solve the recurrence relation. That is, find a closed formula for the nth term of the sequence.

12. Your magic chocolate bunnies reproduce like rabbits: every large bunny produces 2 new mini bunnies each day, and each day every mini bunny born the previous day grows into a large bunny. Assume you start with 2 mini bunnies and no bunny ever dies (or gets eaten).

(a) Write out the first few terms of the sequence.

(b) Give a recursive definition of the sequence and explain why it is correct.

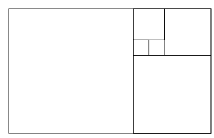
(c) Find a closed formula for the nth term of the sequence.

13. Consider the sequence of partial sums of *squares* of Fibonacci numbers: $F_1^2, F_1^2 + F_2^2, F_1^2 + F_2^2 + F_3^2, \ldots$. The sequences starts $1, 2, 6, 15, 40, \ldots$

(a) Guess a formula for the nth partial sum, in terms of Fibonacci numbers. Hint: write each term as a product.

(b) Prove your formula is correct by mathematical induction.

(c) Explain what this problem has to do with the following picture:



14. Prove the following statements by mathematical induction:

(a) $n! < n^n$ for $n \geq 2$

(b) $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n \cdot (n+1)} = \frac{n}{n+1}$ for all $n \in \mathbb{Z}^+$.

(c) $4^n - 1$ is a multiple of 3 for all $n \in \mathbb{N}$.

(d) The *greatest* amount of postage you *cannot* make exactly using 4 and 9 cent stamps is 23 cents.

(e) Every even number squared is divisible by 4.

15. Prove $1^3 + 2^3 + 3^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$ holds for all $n \geq 1$, by mathematical induction.

16. Suppose $a_0 = 1$, $a_1 = 1$ and $a_n = 3a_{n-1} - 2a_{n-1}$. Prove, using strong induction, that $a_n = 1$ for all n.

17. Prove using induction that every set containing n elements has 2^n different subsets for any $n \geq 1$.

Chapter 3

Symbolic Logic and Proofs

Logic is the study of consequence. Given a few mathematical statements or facts, we would like to be able to draw some conclusions. For example, if I told you that a particular real-valued function was continuous on the interval $[0,1]$, and $f(0) = -1$ and $f(1) = 5$, can we conclude that there is some point between $[0,1]$ where the graph of the function crosses the x-axis? Yes, we can, thanks to the Intermediate Value Theorem from Calculus. Can we conclude that there is exactly one point? No. Whenever we find an "answer" in math, we really have a (perhaps hidden) argument. Mathematics is really about proving general statements (like the Intermediate Value Theorem), and this too is done via an argument, usually called a proof. We start with some given conditions, the *premises* of our argument, and from these we find a consequence of interest, our *conclusion*.

The problem is, as you no doubt know from arguing with friends, not all arguments are *good* arguments. A "bad" argument is one in which the conclusion does not follow from the premises, i.e., the conclusion is not a consequence of the premises. Logic is the study of what makes an argument good or bad. In other words, logic aims to determine in which cases a conclusion is, or is not, a consequence of a set of premises.

By the way, "argument" is actually a technical term in math (and philosophy, another discipline which studies logic):

Arguments.

An **argument** is a set of statements, one of which is called the **conclusion** and the rest of which are called **premises**. An argument is said to be **valid** if the conclusion must be true whenever the premises are all true. An argument is **invalid** if it is not valid; it is possible for all the premises to be true and the conclusion to be false.

For example, consider the following two arguments:

	If Edith eats her vegetables, then she can have a cookie.
	Edith eats her vegetables.
∴	Edith gets a cookie.

	Florence must eat her vegetables in order to get a cookie.
	Florence eats her vegetables.
∴	Florence gets a cookie.

(The symbol "∴" means "therefore")

Are these arguments valid? Hopefully you agree that the first one is but the second one is not. Logic tells us why by analyzing the structure of the statements in the argument. Notice the two arguments above look almost identical. Edith and Florence both eat their vegetables. In both cases there is a connection between the eating of vegetables and cookies. But we claim that it is valid to conclude that Edith gets a cookie, but not that Florence does. The difference must be in the connection between eating vegetables and getting cookies. We need to be skilled at reading and comprehending these sentences. Do the two sentences mean the same thing? Unfortunately, in everyday language we are often sloppy, and you might be tempted to say they are equivalent. But notice that just because Florence *must* eat her vegetables, we have not said that doing so would be *enough* (she might also need to clean her room, for example). In everyday (non-mathematical) practice, you might be tempted to say this "other direction" is implied. In mathematics, we never get that luxury.

Before proceeding, it might be a good idea to quickly review Section 0.2 where we first encountered statements and the various forms they can take. The goal now is to see what mathematical tools we can develop to better analyze these, and then to see how this helps read and write proofs.

3.1 Propositional Logic

Investigate!

You stumble upon two trolls playing Stratego®. They tell you:

> Troll 1: If we are cousins, then we are both knaves.
>
> Troll 2: We are cousins or we are both knaves.

Could both trolls be knights? Recall that all trolls are either always-truth-telling knights or always-lying knaves.

Attempt the above activity before proceeding

A **proposition** is simply a statement. **Propositional logic** studies the ways statements can interact with each other. It is important to remember that propositional logic does not really care about the content of the statements. For example, in terms of propositional logic, the claims, "if the moon is made of cheese then basketballs are round," and "if spiders have eight legs then Sam walks with a limp" are exactly the same. They are both implications: statements of the form, $P \to Q$.

Truth Tables

Here's a question about playing Monopoly:

> If you get more doubles than any other player then you will lose, or if you lose then you must have bought the most properties.

True or false? We will answer this question, and won't need to know anything about Monopoly. Instead we will look at the logical *form* of the statement.

We need to decide when the statement $(P \to Q) \vee (Q \to R)$ is true. Using the definitions of the connectives in Section 0.2, we see that for this to be true, either $P \to Q$ must be true or $Q \to R$ must be true (or both). Those are true if either P is false or Q is true (in the first case) and Q is false or R is true (in the second case). So—yeah, it gets kind of messy. Luckily, we can make a chart to keep track of all the possibilities. Enter **truth tables**. The idea is this: on each row, we list a possible combination of T's and F's (for true and false) for each of the sentential variables, and then mark down whether the statement in question is true or false in that case. We do this for every possible combination of T's and F's. Then we can clearly see in which cases the statement is true or false. For complicated statements, we will first fill in values for each part of the statement, as a way of breaking up our task into smaller, more manageable pieces.

Since the truth value of a statement is completely determined by the truth values of its parts and how they are connected, all you really need to know is the truth tables for each of the logical connectives. Here they are:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

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

P	Q	$P \to Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

The truth table for negation looks like this:

P	$\neg P$
T	F
F	T

None of these truth tables should come as a surprise; they are all just restating the definitions of the connectives. Let's try another one.

Example 3.1.1

Make a truth table for the statement $\neg P \vee Q$.

Solution. Note that this statement is not $\neg(P \vee Q)$, the negation belongs to P alone. Here is the truth table:

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

We added a column for $\neg P$ to make filling out the last column easier. The entries in the $\neg P$ column were determined by the entries in the P column. Then to fill in the final column, look only at the column for Q and the column for $\neg P$ and use the rule for $\vee$.

Now let's answer our question about monopoly:

Example 3.1.2

Analyze the statement, "if you get more doubles than any other player you will lose, or that if you lose you must have bought the most properties," using truth tables.

Solution. Represent the statement in symbols as $(P \to Q) \vee (Q \to R)$, where P is the statement "you get more doubles than any other player," Q is the statement "you will lose," and R is the statement "you must have bought the most properties." Now make a truth table.

The truth table needs to contain 8 rows in order to account for every possible combination of truth and falsity among the three statements. Here is the full truth table:

P	Q	R	$P \to Q$	$Q \to R$	$(P \to Q) \vee (Q \to R)$
T	T	T	T	T	T
T	T	F	T	F	T
T	F	T	F	T	T
T	F	F	F	T	T
F	T	T	T	T	T
F	T	F	T	F	T
F	F	T	T	T	T
F	F	F	T	T	T

The first three columns are simply a systematic listing of all possible combinations of T and F for the three statements (do you see how you would list the 16 possible combinations for four statements?). The next two columns are determined by the values of P, Q, and R and the definition of implication. Then, the last column is determined by the values in the previous two columns and the definition of $\vee$. It is this final column we care about.

Notice that in each of the eight possible cases, the statement in question is true. So our statement about monopoly is true (regardless of how many properties you own, how many doubles you roll, or whether you win or lose).

The statement about monopoly is an example of a **tautology**, a statement which is true on the basis of its logical form alone. Tautologies are always true but they don't tell us much about the world. No knowledge about monopoly was required to determine that the statement was true. In fact, it is equally true that "If the moon is made of cheese, then Elvis is still alive, or if Elvis is still alive, then unicorns have 5 legs."

Logical Equivalence

You might have noticed in Example 3.1.1 that the final column in the truth table for $\neg P \vee Q$ is identical to the final column in the truth table for $P \rightarrow Q$:

P	Q	$P \rightarrow Q$	$\neg P \vee Q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

This says that no matter what P and Q are, the statements $\neg P \vee Q$ and $P \rightarrow Q$ either both true or both false. We therefore say these statements are **logically equivalent**.

Logical Equivalence.

Two (molecular) statements P and Q are **logically equivalent** provided P is true precisely when Q is true. That is, P and Q have the same truth value under any assignment of truth values to their atomic parts.

To verify that two statements are logically equivalent, you can make a truth table for each and check whether the columns for the two statements are identical.

Recognizing two statements as logically equivalent can be very helpful. Rephrasing a mathematical statement can often lend insight into what it is saying, or how to prove or refute it. By using truth tables we can systematically verify that two statements are indeed logically equivalent.

Example 3.1.3

Are the statements, "it will not rain or snow" and "it will not rain and it will not snow" logically equivalent?

Solution. We want to know whether $\neg(P \vee Q)$ is logically equivalent to $\neg P \wedge \neg Q$. Make a truth table which includes both statements:

P	Q	$\neg(P \vee Q)$	$\neg P \wedge \neg Q$
T	T	F	F
T	F	F	F
F	T	F	F
F	F	T	T

Since in every row the truth values for the two statements are equal, the two statements are logically equivalent.

Notice that this example gives us a way to "distribute" a negation over a disjunction (an "or"). We have a similar rule for distributing over conjunctions ("and"s):

De Morgan's Laws.

$\neg(P \wedge Q)$ is logically equivalent to $\neg P \vee \neg Q$.

$\neg(P \vee Q)$ is logically equivalent to $\neg P \wedge \neg Q$.

This suggests there might be a sort of "algebra" you could apply to statements (okay, there is: it is called *Boolean algebra*) to transform one statement into another. We can start collecting useful examples of logical equivalence, and apply them in succession to a statement, instead of writing out a complicated truth table.

De Morgan's laws do not do not directly help us with implications, but as we saw above, every implication can be written as a disjunction:

Implications are Disjunctions.

$P \rightarrow Q$ is logically equivalent to $\neg P \vee Q$.

Example: "If a number is a multiple of 4, then it is even" is equivalent to, "a number is not a multiple of 4 or (else) it is even."

With this and De Morgan's laws, you can take any statement and *simplify* it to the point where negations are only being applied to atomic propositions. Well, actually not, because you could get multiple negations stacked up. But this can be easily dealt with:

Double Negation.

$\neg\neg P$ is logically equivalent to P.

Example: “It is not the case that c is not odd” means “c is odd.”

Let’s see how we can apply the equivalences we have encountered so far.

Example 3.1.4

Prove that the statements $\neg(P \rightarrow Q)$ and $P \wedge \neg Q$ are logically equivalent without using truth tables.

Solution. We want to start with one of the statements, and transform it into the other through a sequence of logically equivalent statements. Start with $\neg(P \rightarrow Q)$. We can rewrite the implication as a disjunction this is logically equivalent to

$$\neg(\neg P \vee Q).$$

Now apply DeMorgan’s law to get

$$\neg\neg P \wedge \neg Q.$$

Finally, use double negation to arrive at $P \wedge \neg Q$

Notice that the above example illustrates that the negation of an implication is NOT an implication: it is a conjunction! We saw this before, in Section 0.2, but it is so important and useful, it warants a second blue box here:

Negation of an Implication.

The negation of an implication is a conjunction:

$\neg(P \rightarrow Q)$ is logically equivalent to $P \wedge \neg Q$.

That is, the only way for an implication to be false is for the hypothesis to be true *AND* the conclusion to be false.

To verify that two statements are logically equivalent, you can use truth tables or a sequence of logically equivalent replacements. The truth table method, although cumbersome, has the advantage that it can verify that two statements are NOT logically equivalent.

Example 3.1.5

Are the statements $(P \vee Q) \to R$ and $(P \to R) \vee (Q \to R)$ logically equivalent?

Solution. Note that while we could start rewriting these statements with logically equivalent replacements in the hopes of transforming one into another, we will never be sure that our failure is due to their lack of logical equivalence rather than our lack of imagination. So instead, let's make a truth table:

P	Q	R	$(P \vee Q) \to R$	$(P \to R) \vee (Q \to R)$
T	T	T	T	T
T	T	F	F	F
T	F	T	T	T
T	F	F	F	T
F	T	T	T	T
F	T	F	F	T
F	F	T	T	T
F	F	F	T	T

Look at the fourth (or sixth) row. In this case, $(P \to R) \vee (Q \to R)$ is true, but $(P \vee Q) \to R$ is false. Therefore the statements are not logically equivalent.

While we don't have logical equivalence, it is the case that whenever $(P \vee Q) \to R$ is true, so is $(P \to R) \vee (Q \to R)$. This tells us that we can *deduce* $(P \to R) \vee (Q \to R)$ from $(P \vee Q) \to R$, just not the reverse direction.

Deductions

Investigate!

Holmes owns two suits: one black and one tweed. He always wears either a tweed suit or sandals. Whenever he wears his tweed suit and a purple shirt, he chooses to not wear a tie. He never wears the tweed suit unless he is also wearing either a purple shirt or sandals. Whenever he wears sandals, he also wears a purple shirt. Yesterday, Holmes wore a bow tie. What else did he wear?

Attempt the above activity before proceeding

Earlier we claimed that the following was a valid argument:

> If Edith eats her vegetables, then she can have a cookie. Edith ate her vegetables. Therefore Edith gets a cookie.

How do we know this is valid? Let's look at the form of the statements. Let P denote "Edith eats her vegetables" and Q denote "Edith can have a cookie." The logical form of the argument is then:

$$\begin{array}{rc} & P \rightarrow Q \\ & P \\ \hline \therefore & Q \end{array}$$

This is an example of a **deduction rule**, an argument form which is always valid. This one is a particularly famous rule called *modus ponens*. Are you convinced that it is a valid deduction rule? If not, consider the following truth table:

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

This is just the truth table for $P \rightarrow Q$, but what matters here is that all the lines in the deduction rule have their own column in the truth table. Remember that an argument is valid provided the conclusion must be true given that the premises are true. The premises in this case are $P \rightarrow Q$ and P. Which *rows* of the truth table correspond to both of these being true? P is true in the first two rows, and of those, only the first row has $P \rightarrow Q$ true as well. And lo-and-behold, in this one case, Q is also true. So if $P \rightarrow Q$ and P are both true, we see that Q must be true as well.

Here are a few more examples.

Example 3.1.6

Show that

$$\begin{array}{rc} & P \rightarrow Q \\ & \neg P \rightarrow Q \\ \hline \therefore & Q \end{array}$$

is a valid deduction rule.

Solution. We make a truth table which contains all the lines of the argument form:

P	Q	$P \rightarrow Q$	$\neg P$	$\neg P \rightarrow Q$
T	T	T	F	T
T	F	F	F	T
F	T	T	T	T
F	F	T	T	F

(we include a column for $\neg P$ just as a step to help getting the column for $\neg P \to Q$).

Now look at all the rows for which both $P \to Q$ and $\neg P \to Q$ are true. This happens only in rows 1 and 3. Hey! In those rows Q is true as well, so the argument form is valid (it is a valid deduction rule).

Example 3.1.7

Decide whether

$$\begin{array}{rc} & P \to R \\ & Q \to R \\ & R \\ \hline \therefore & P \vee Q \end{array}$$

is a valid deduction rule.

Solution. Let's make a truth table containing all four statements.

P	Q	R	$P \to R$	$Q \to R$	$P \vee Q$
T	T	T	T	T	T
T	T	F	F	F	T
T	F	T	T	T	T
T	F	F	F	T	T
F	T	T	T	T	T
F	T	F	T	F	T
F	F	T	T	T	F
F	F	F	T	T	F

Look at the second to last row. Here all three premises of the argument are true, but the conclusion is false. Thus this is not a valid deduction rule.

While we have the truth table in front of us, look at rows 1, 3, and 5. These are the only rows in which all of the statements $P \to R$, $Q \to R$, and $P \vee Q$ are true. It also happens that R is true in these rows as well. Thus we have discovered a new deduction rule we know *is* valid:

$$\begin{array}{rc} & P \to R \\ & Q \to R \\ & P \vee Q \\ \hline \therefore & R \end{array}$$

Beyond Propositions

As we saw in Section 0.2, not every statement can be analyzed using logical connectives alone. For example, we might want to work with the statement:

> All primes greater than 2 are odd.

To write this statement symbolically, we must use quantifiers. We can translate as follows:

$$\forall x((P(x) \wedge x > 2) \rightarrow O(x)).$$

In this case, we are using $P(x)$ to denote "x is prime" and $O(x)$ to denote "x is odd." These are not propositions, since their truth value depends on the input x. Better to think of P and O as denoting *properties* of their input. The technical term for these is **predicates** and when we study them in logic, we need to use **predicate logic**.

It is important to stress that predicate logic *extends* propositional logic (much in the way quantum mechanics extends classical mechanics). You will notice that our statement above still used the (propositional) logical connectives. Everything that we learned about logical equivalence and deductions still applies. However, predicate logic allows us to analyze statements at a higher resolution, digging down into the individual propositions P, Q, etc.

A full treatment of predicate logic is beyond the scope of this text. One reason is that there is no systematic procedure for deciding whether two statements in predicate logic are logically equivalent (i.e., there is no analogue to truth tables here). Rather, we end with a two examples of logical equivalence and deduction, to pique your interest.

Example 3.1.8

Suppose we claim that there is no smallest number. We can translate this into symbols as

$$\neg\exists x\forall y(x \leq y)$$

(literally, "it is not true that there is a number x such that for all numbers y, x is less than or equal to y").

However, we know how negation interacts with quantifiers: we can pass a negation over a quantifier by switching the quantifier type (between universal and existential). So the statement above should be *logically equivalent* to

$$\forall x\exists y(y < x).$$

Notice that $y < x$ is the negation of $x \leq y$. This literally says, "for every number x there is a number y which is smaller than x." We see that this is another way to make our original claim.

Example 3.1.9

Can you switch the order of quantifiers? For example, consider the two statements:

$$\forall x \exists y P(x, y) \qquad \text{and} \qquad \exists y \forall x P(x, y).$$

Are these logically equivalent?

Solution. These statements are NOT logically equivalent. To see this, we should provide an interpretation of the predicate $P(x, y)$ which makes one of the statements true and the other false.

Let $P(x, y)$ be the predicate $x < y$. It is true, in the natural numbers, that for all x there is some y greater than that x (since there are infinitely many numbers). However, there is not a natural number y which is greater than every number x. Thus it is possible for $\forall x \exists y P(x, y)$ to be true while $\exists y \forall x P(x, y)$ is false.

We cannot do the reverse of this though. If there is some y for which every x satisfies $P(x, y)$, then certainly for every x there is some y which satisfies $P(x, y)$. The first is saying we can find one y that works for every x. The second allows different y's to work for different x's, but there is nothing preventing us from using the same y that work for every x. In other words, while we don't have logical equivalence between the two statements, we do have a valid deduction rule:

$$\begin{array}{rl} & \exists y \forall x P(x, y) \\ \hline \therefore & \forall x \exists y P(x, y) \end{array}$$

Put yet another way, this says that the single statement

$$\exists y \forall x P(x, y) \rightarrow \forall x \exists y P(x, y)$$

is always true. This is sort of like a tautology, although we reserve that term for necessary truths in propositional logic. A statement in predicate logic that is necessarily true gets the more prestigious designation of a **law of logic** (or sometimes **logically valid**, but that is less fun).

Exercises

1. Consider the statement about a party, "If it's your birthday or there will be cake, then there will be cake."

    (a) Translate the above statement into symbols. Clearly state which statement is P and which is Q.

    (b) Make a truth table for the statement.

    (c) Assuming the statement is true, what (if anything) can you conclude if there will be cake?

    (d) Assuming the statement is true, what (if anything) can you conclude if there will not be cake?

    (e) Suppose you found out that the statement was a lie. What can you conclude?

2. Make a truth table for the statement $(P \vee Q) \rightarrow (P \wedge Q)$.

3. Make a truth table for the statement $\neg P \wedge (Q \rightarrow P)$. What can you conclude about P and Q if you know the statement is true?

4. Make a truth table for the statement $\neg P \rightarrow (Q \wedge R)$.

5. Geoff Poshingten is out at a fancy pizza joint, and decides to order a calzone. When the waiter asks what he would like in it, he replies, "I want either pepperoni or sausage. Also, if I have sausage, then I must also include quail. Oh, and if I have pepperoni or quail then I must also have ricotta cheese."

    (a) Translate Geoff's order into logical symbols.

    (b) The waiter knows that Geoff is either a liar or a truth-teller (so either everything he says is false, or everything is true). Which is it?

    (c) What, if anything, can the waiter conclude about the ingredients in Geoff's desired calzone?

6. Determine whether the following two statements are logically equivalent: $\neg(P \rightarrow Q)$ and $P \wedge \neg Q$. Explain how you know you are correct.

7. Are the statements $P \rightarrow (Q \vee R)$ and $(P \rightarrow Q) \vee (P \rightarrow R)$ logically equivalent?

8. Simplify the following statements (so that negation only appears right before variables).

    (a) $\neg(P \rightarrow \neg Q)$.

    (b) $(\neg P \vee \neg Q) \rightarrow \neg(\neg Q \wedge R)$.

(c) $\neg((P \to \neg Q) \vee \neg(R \wedge \neg R))$.

(d) It is false that if Sam is not a man then Chris is a woman, and that Chris is not a woman.

9. Use De Morgan's Laws, and any other logical equivalence facts you know to simplify the following statements. Show all your steps. Your final statements should have negations only appear directly next to the sentence variables or predicates (P, Q, $E(x)$, etc.), and no double negations. It would be a good idea to use only conjunctions, disjunctions, and negations.

(a) $\neg((\neg P \wedge Q) \vee \neg(R \vee \neg S))$.

(b) $\neg((\neg P \to \neg Q) \wedge (\neg Q \to R))$ (careful with the implications).

(c) For both parts above, verify your answers are correct using truth tables. That is, use a truth table to check that the given statement and your proposed simplification are actually logically equivalent.

10. Consider the statement, "If a number is triangular or square, then it is not prime"

(a) Make a truth table for the statement $(T \vee S) \to \neg P$.

(b) If you believed the statement was *false*, what properties would a counterexample need to possess? Explain by referencing your truth table.

(c) If the statement were true, what could you conclude about the number 5657, which is definitely prime? Again, explain using the truth table.

11. Tommy Flanagan was telling you what he ate yesterday afternoon. He tells you, "I had either popcorn or raisins. Also, if I had cucumber sandwiches, then I had soda. But I didn't drink soda or tea." Of course you know that Tommy is the worlds worst liar, and everything he says is false. What did Tommy eat?

Justify your answer by writing all of Tommy's statements using sentence variables (P, Q, R, S, T), taking their negations, and using these to deduce what Tommy actually ate.

12. Determine if the following deduction rule is valid:

$$\begin{array}{rc} & P \vee Q \\ & \neg P \\ \hline \therefore & Q \end{array}$$

13. Determine if the following is a valid deduction rule:

$$\begin{array}{rc} & P \rightarrow (Q \vee R) \\ & \neg(P \rightarrow Q) \\ \hline \therefore & R \end{array}$$

14. Determine if the following is a valid deduction rule:

$$\begin{array}{rc} & (P \wedge Q) \rightarrow R \\ & \neg P \vee \neg Q \\ \hline \therefore & \neg R \end{array}$$

15. Can you chain implications together? That is, if $P \rightarrow Q$ and $Q \rightarrow R$, does that means the $P \rightarrow R$? Can you chain more implications together? Let's find out:

(a) Prove that the following is a valid deduction rule:

$$\begin{array}{rc} & P \rightarrow Q \\ & Q \rightarrow R \\ \hline \therefore & P \rightarrow R \end{array}$$

(b) Prove that the following is a valid deduction rule for any $n \geq 2$:

$$\begin{array}{rc} & P_1 \rightarrow P_2 \\ & P_2 \rightarrow P_3 \\ & \vdots \\ & P_{n-1} \rightarrow P_n \\ \hline \therefore & P_1 \rightarrow P_n. \end{array}$$

I suggest you don't go through the trouble of writing out a 2^n row truth table. Instead, you should use part (a) and mathematical induction.

16. We can also simplify statements in predicate logic using our rules for passing negations over quantifiers, and then applying propositional logical equivalence to the "inside" propositional part. Simplify the statements below (so negation appears only directly next to predicates).

(a) $\neg\exists x \forall y(\neg O(x) \vee E(y))$.

(b) $\neg\forall x \neg\forall y \neg(x < y \wedge \exists z(x < z \vee y < z))$.

(c) There is a number n for which no other number is either less n than or equal to n.

(d) It is false that for every number n there are two other numbers which n is between.

17. Simplify the statements below to the point that negation symbols occur only directly next to predicates.

(a) $\neg\forall x \forall y(x < y \vee y < x)$.

(b) $\neg(\exists x P(x) \to \forall y P(y))$.

18. Simplifying negations will be especially useful in the next section when we try to prove a statement by considering what would happen if it were false. For each statement below, write the *negation* of the statement as simply as possible. Don't just say, "it is false that . . . ".

(a) Every number is either even or odd.

(b) There is a sequence that is both arithmetic and geometric.

(c) For all numbers n, if n is prime, then $n + 3$ is not prime.

19. Suppose P and Q are (possibly molecular) propositional statements. Prove that P and Q are logically equivalent if any only if $P \leftrightarrow Q$ is a tautology.

20. Suppose $P_1, P_2, \ldots, P_n$ and Q are (possibly molecular) propositional statements. Suppose further that

$$\begin{array}{rl} & P_1 \\ & P_2 \\ & \vdots \\ & P_n \\ \hline \therefore & Q \end{array}$$

is a valid deduction rule. Prove that the statement

$$(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \to Q$$

is a tautology.

3.2 Proofs

Investigate!

Decide which of the following are valid proofs of the following statement:

If ab is an even number, then a or b is even.

1. Suppose a and b are odd. That is, $a = 2k + 1$ and $b = 2m + 1$ for some integers k and m. Then

$$\begin{aligned} ab &= (2k+1)(2m+1) \\ &= 4km + 2k + 2m + 1 \\ &= 2(2km + k + m) + 1. \end{aligned}$$

   Therefore ab is odd.

2. Assume that a or b is even - say it is a (the case where b is even is identical). That is, $a = 2k$ for some integer k. Then

$$\begin{aligned} ab &= (2k)b \\ &= 2(kb). \end{aligned}$$

   Thus ab is even.

3. Suppose that ab is even but a and b are both odd. Namely, $ab = 2n$, $a = 2k+1$ and $b = 2j+1$ for some integers n, k, and j. Then

$$\begin{aligned} 2n &= (2k+1)(2j+1) \\ 2n &= 4kj + 2k + 2j + 1 \\ n &= 2kj + k + j + 0.5. \end{aligned}$$

   But since $2kj + k + j$ is an integer, this says that the integer n is equal to a non-integer, which is impossible.

4. Let ab be an even number, say $ab = 2n$, and a be an odd number, say $a = 2k + 1$.

$$\begin{aligned} ab &= (2k+1)b \\ 2n &= 2kb + b \\ 2n - 2kb &= b \\ 2(n - kb) &= b. \end{aligned}$$

   Therefore b must be even.

Attempt the above activity before proceeding

Anyone who doesn't believe there is creativity in mathematics clearly has not tried to write proofs. Finding a way to convince the world that a particular statement is necessarily true is a mighty undertaking and can often be quite challenging. There is not a guaranteed path to success in the search for proofs. For example, in the summer of 1742, a German mathematician by the name of Christian Goldbach wondered whether every even integer greater than 2 could be written as the sum of two primes. Centuries later, we still don't have a proof of this apparent fact (computers have checked that "Goldbach's Conjecture" holds for all numbers less than 4×10^{18}, which leaves only infinitely many more numbers to check).

Writing proofs is a bit of an art. Like any art, to be truly great at it, you need some sort of inspiration, as well as some foundational technique. Just as musicians can learn proper fingering, and painters can learn the proper way to hold a brush, we can look at the proper way to construct arguments. A good place to start might be to study a classic.

Theorem 3.2.1 *There are infinitely many primes.*

Proof. Suppose this were not the case. That is, suppose there are only finitely many primes. Then there must be a last, largest prime, call it p. Consider the number

$$N = p! + 1 = (p \cdot (p-1) \cdot \dots \cdot 3 \cdot 2 \cdot 1) + 1.$$

Now N is certainly larger than p. Also, N is not divisible by any number less than or equal to p, since every number less than or equal to p divides $p!$. Thus the prime factorization of N contains prime numbers (possibly just N itself) all greater than p. So p is not the largest prime, a contradiction. Therefore there are infinitely many primes. QED

This proof is an example of a *proof by contradiction*, one of the standard styles of mathematical proof. First and foremost, the proof is an argument. It contains sequence of statements, the last being the *conclusion* which follows from the previous statements. The argument is valid so the conclusion must be true if the premises are true. Let's go through the proof line by line.

1. Suppose there are only finitely many primes. *[this is a premise. Note the use of "suppose."]*
2. There must be a largest prime, call it p. *[follows from line 1, by the definition of "finitely many."]*
3. Let $N = p! + 1$. *[basically just notation, although this is the inspired part of the proof; looking at* $p! + 1$ *is the key insight.]*
4. N is larger than p. *[by the definition of* $p!$*]*

5. N is not divisible by any number less than or equal to p. *[by definition, $p!$ is divisible by each number less than or equal to p, so $p! + 1$ is not.]*

6. The prime factorization of N contains prime numbers greater than p. *[since N is divisible by each prime number in the prime factorization of N, and by line 5.]*

7. Therefore p is not the largest prime. *[by line 6, N is divisible by a prime larger than p.]*

8. This is a contradiction. *[from line 2 and line 7: the largest prime is p and there is a prime larger than p.]*

9. Therefore there are infinitely many primes. *[from line 1 and line 8: our only premise lead to a contradiction, so the premise is false.]*

We should say a bit more about the last line. Up through line 8, we have a valid argument with the premise "there are only finitely many primes" and the conclusion "there is a prime larger than the largest prime." This is a valid argument as each line follows from previous lines. So if the premises are true, then the conclusion *must* be true. However, the conclusion is NOT true. The only way out: the premise must be false.

The sort of line-by-line analysis we did above is a great way to really understand what is going on. Whenever you come across a proof in a textbook, you really should make sure you understand what each line is saying and why it is true. Additionally, it is equally important to understand the overall structure of the proof. This is where using tools from logic is helpful. Luckily there are a relatively small number of standard proof styles that keep showing up again and again. Being familiar with these can help understand proof, as well as give ideas of how to write your own.

Direct Proof

The simplest (from a logic perspective) style of proof is a **direct proof**. Often all that is required to prove something is a systematic explanation of what everything means. Direct proofs are especially useful when proving implications. The general format to prove $P \to Q$ is this:

> Assume P. Explain, explain, ..., explain. Therefore Q.

Often we want to prove universal statements, perhaps of the form $\forall x(P(x) \to Q(x))$. Again, we will want to assume $P(x)$ is true and deduce $Q(x)$. But what about the x? We want this to work for *all* x. We accomplish this by fixing x to be an arbitrary element (of the sort we are interested in).

Here are a few examples. First, we will set up the proof structure for a direct proof, then fill in the details.

Example 3.2.2

Prove: For all integers n, if n is even, then n^2 is even.

Solution. The format of the proof will be this: Let n be an arbitrary integer. Assume that n is even. Explain explain explain. Therefore n^2 is even.

To fill in the details, we will basically just explain what it means for n to be even, and then see what that means for n^2. Here is a complete proof.

Proof. Let n be an arbitrary integer. Suppose n is even. Then $n = 2k$ for some integer k. Now $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Since $2k^2$ is an integer, n^2 is even. ■

Example 3.2.3

Prove: For all integers a, b, and c, if $a|b$ and $b|c$ then $a|c$. (Here $x|y$, read "x divides y" means that y is a multiple of x, i.e., that x will divide into y without remainder).

Solution. Even before we know what the divides symbol means, we can set up a direct proof for this statement. It will go something like this: Let a, b, and c be arbitrary integers. Assume that $a|b$ and $b|c$. Dot dot dot. Therefore $a|c$.

How do we connect the dots? We say what our hypothesis ($a|b$ and $b|c$) really means and why this gives us what the conclusion ($a|c$) really means. Another way to say that $a|b$ is to say that $b = ka$ for some integer k (that is, that b is a multiple of a). What are we going for? That $c = la$, for some integer l (because we want c to be a multiple of a). Here is the complete proof.

Proof. Let a, b, and c be integers. Assume that $a|b$ and $b|c$. In other words, b is a multiple of a and c is a multiple of b. So there are integers k and j such that $b = ka$ and $c = jb$. Combining these (through substitution) we get that $c = jka$. But jk is an integer, so this says that c is a multiple of a. Therefore $a|c$. ■

Proof by Contrapositive

Recall that an implication $P \to Q$ is logically equivalent to its contrapositive $\neg Q \to \neg P$. There are plenty of examples of statements which are hard to prove directly, but whose contrapositive can easily be proved directly. This is all that **proof by contrapositive** does. It gives a direct proof of the contrapositive of the implication. This is enough because the contrapositive is logically equivalent to the original implication.

The skeleton of the proof of $P \to Q$ by contrapositive will always look roughly like this:

Assume $\neg Q$. Explain, explain, ... explain. Therefore $\neg P$.

As before, if there are variables and quantifiers, we set them to be arbitrary elements of our domain. Here are two examples:

Example 3.2.4

Is the statement "for all integers n, if n^2 is even, then n is even" true?

Solution. This is the converse of the statement we proved above using a direct proof. From trying a few examples, this statement definitely appears to be true. So let's prove it.

A direct proof of this statement would require fixing an arbitrary n and assuming that n^2 is even. But it is not at all clear how this would allow us to conclude anything about n. Just because $n^2 = 2k$ does not in itself suggest how we could write n as a multiple of 2.

Try something else: write the contrapositive of the statement. We get, for all integers n, if n is odd then n^2 is odd. This looks much more promising. Our proof will look something like this:

Let n be an arbitrary integer. Suppose that n is not even. This means that .... In other words .... But this is the same as saying .... Therefore n^2 is not even.

Now we fill in the details:

Proof. We will prove the contrapositive. Let n be an arbitrary integer. Suppose that n is not even, and thus odd. Then $n = 2k + 1$ for some integer k. Now $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$. Since $2k^2 + 2k$ is an integer, we see that n^2 is odd and therefore not even. ■

Example 3.2.5

Prove: for all integers a and b, if $a + b$ is odd, then a is odd or b is odd.

Solution. The problem with trying a direct proof is that it will be hard to separate a and b from knowing something about $a + b$. On the other hand, if we know something about a and b separately, then combining them might give us information about $a + b$. The contrapositive of the statement we are trying to prove is: for all integers a and b, if a and b are even, then $a + b$ is even. Thus our proof will have the following format:

Let a and b be integers. Assume that a and b are both even. la la la. Therefore $a + b$ is even.

Here is a complete proof:

Proof. Let a and b be integers. Assume that a and b are even. Then $a = 2k$ and $b = 2l$ for some integers k and l. Now $a + b = 2k + 2l = 2(k + 1)$. Since $k + l$ is an integer, we see that $a + b$ is even, completing the proof. ■

Note that our assumption that a and b are even is really the negation of a or b is odd. We used De Morgan's law here.

We have seen how to prove some statements in the form of implications: either directly or by contrapositive. Some statements are not written as implications to begin with.

Example 3.2.6

Consider the following statement: for every prime number p, either $p = 2$ or p is odd. We can rephrase this: for every prime number p, if $p \neq 2$, then p is odd. Now try to prove it.

Solution.

Proof. Let p be an arbitrary prime number. Assume p is not odd. So p is divisible by 2. Since p is prime, it must have exactly two divisors, and it has 2 as a divisor, so p must be divisible by only 1 and 2. Therefore $p = 2$. This completes the proof (by contrapositive). ■

Proof by Contradiction

There might be statements which really cannot be rephrased as implications. For example, "$\sqrt{2}$ is irrational." In this case, it is hard to know where to start. What can we assume? Well, say we want to prove the statement P. What if we could prove that $\neg P \to Q$ where Q was false? If this implication is true, and Q is false, what can we say about $\neg P$? It must be false as well, which makes P true!

This is why **proof by contradiction** works. If we can prove that $\neg P$ leads to a contradiction, then the only conclusion is that $\neg P$ is false, so P is true. That's what we wanted to prove. In other words, if it is impossible for P to be false, P must be true.

Here are three examples of proofs by contradiction:

Example 3.2.7

Prove that $\sqrt{2}$ is irrational.

Solution.

Proof. Suppose not. Then $\sqrt{2}$ is equal to a fraction $\frac{a}{b}$. Without loss of generality, assume $\frac{a}{b}$ is in lowest terms (otherwise reduce the fraction). So,

$$2 = \frac{a^2}{b^2}$$
$$2b^2 = a^2.$$

Thus a^2 is even, and as such a is even. So $a = 2k$ for some integer k, and $a^2 = 4k^2$. We then have,

$$2b^2 = 4k^2$$
$$b^2 = 2k^2.$$

Thus b^2 is even, and as such b is even. Since a is also even, we see that $\frac{a}{b}$ is not in lowest terms, a contradiction. Thus $\sqrt{2}$ is irrational. ∎

Example 3.2.8

Prove: There are no integers x and y such that $x^2 = 4y + 2$.

Solution.

Proof. We proceed by contradiction. So suppose there *are* integers x and y such that $x^2 = 4y + 2 = 2(2y + 1)$. So x^2 is even. We have seen that this implies that x is even. So $x = 2k$ for some integer k. Then $x^2 = 4k^2$. This in turn gives $2k^2 = (2y + 1)$. But $2k^2$ is even, and $2y + 1$ is odd, so these cannot be equal. Thus we have a contradiction, so there must not be any integers x and y such that $x^2 = 4y + 2$. ∎

Example 3.2.9

The **Pigeonhole Principle**: If more than n pigeons fly into n pigeon holes, then at least one pigeon hole will contain at least two pigeons. Prove this!

Solution.

Proof. Suppose, contrary to stipulation, that each of the pigeon holes contain at most one pigeon. Then at most, there will be n pigeons. But we assumed that there are more than n pigeons, so this is impossible. Thus there must be a pigeonhole with more than one pigeon. ■

While we phrased this proof as a proof by contradiction, we could have also used a proof by contrapositive since our contradiction was simply the negation of the hypothesis. Sometimes this will happen, in which case you can use either style of proof. There are examples however where the contradiction occurs "far away" from the original statement.

Proof by (counter) Example

It is almost NEVER okay to prove a statement with just an example. Certainly none of the statements proved above can be proved through an example. This is because in each of those cases we are trying to prove that something holds of all integers. We claim that n^2 being even implies that n is even, *no matter what integer* n we pick. Showing that this works for $n = 4$ is not even close to enough.

This cannot be stressed enough. If you are trying to prove a statement of the form $\forall x P(x)$, you absolutely CANNOT prove this with an example.[1]

However, existential statements can be proven this way. If we want to prove that there is an integer n such that $n^2 - n + 41$ is not prime, all we need to do is find one. This might seem like a silly thing to want to prove until you try a few values for n.

n	1	2	3	4	5	6	7
$n^2 - n + 41$	41	43	47	53	61	71	83

So far we have gotten only primes. You might be tempted to conjecture, "For all positive integers n, the number $n^2 - n + 41$ is prime." If you wanted to prove this, you would need to use a direct proof, a proof by contrapositive, or another style of proof, but certainly it is not enough to give even 7 examples. In fact, we can prove this conjecture is *false* by proving its negation: "There is a positive integer n such that $n^2 - n + 41$ is not prime." Since this is an existential statement, it suffices to show that there does indeed exist such a number.

[1]This is not to say that looking at examples is a waste of time. Doing so will often give you an idea of how to write a proof. But the examples do not belong in the proof.

In fact, we can quickly see that $n = 41$ will give 41^2 which is certainly not prime. You might say that this is a counterexample to the conjecture that $n^2 - n + 41$ is always prime. Since so many statements in mathematics are universal, making their negations existential, we can often prove that a statement is false (if it is) by providing a counterexample.

Example 3.2.10

Above we proved, "for all integers a and b, if $a + b$ is odd, then a is odd or b is odd." Is the converse true?

Solution. The converse is the statement, "for all integers a and b, if a is odd or b is odd, then $a + b$ is odd." This is false! How do we prove it is false? We need to prove the negation of the converse. Let's look at the symbols. The converse is

$$\forall a \forall b((O(a) \vee O(b)) \rightarrow O(a + b)).$$

We want to prove the negation:

$$\neg \forall a \forall b((O(a) \vee O(b)) \rightarrow O(a + b)).$$

Simplify using the rules from the previous sections:

$$\exists a \exists b((O(a) \vee O(b)) \wedge \neg O(a + b)).$$

As the negation passed by the quantifiers, they changed from $\forall$ to $\exists$. We then needed to take the negation of an implication, which is equivalent to asserting the if part and not the then part.

Now we know what to do. To prove that the converse is false we need to find two integers a and b so that a is odd or b is odd, but $a + b$ is not odd (so even). That's easy: 1 and 3. (remember, "or" means one or the other or both). Both of these are odd, but $1 + 3 = 4$ is not odd.

Proof by Cases

We could go on and on and on about different proof styles (we haven't even mentioned induction or combinatorial proofs here), but instead we will end with one final useful technique: proof by cases. The idea is to prove that P is true by proving that $Q \rightarrow P$ and $\neg Q \rightarrow P$ for some statement Q. So no matter what, whether or not Q is true, we know that P is true. In fact, we could generalize this. Suppose we want to prove P. We know that at least one of the statements $Q_1, Q_2, \ldots, Q_n$ is true. If we can show that $Q_1 \rightarrow P$ and $Q_2 \rightarrow P$ and so on all the way to $Q_n \rightarrow P$, then we can conclude P. The key thing is that we want to be sure that one of our cases (the Q_i's) must be true no matter what.

If that last paragraph was confusing, perhaps an example will make things better.

Example 3.2.11

Prove: For any integer n, the number $(n^3 - n)$ is even.

Solution. It is hard to know where to start this, because we don't know much of anything about n. We might be able to prove that $n^3 - n$ is even if we knew that n was even. In fact, we could probably prove that $n^3 - n$ was even if n was odd. But since n must either be even or odd, this will be enough. Here's the proof.

Proof. We consider two cases: if n is even or if n is odd.

Case 1: n is even. Then $n = 2k$ for some integer k. This give

$$\begin{aligned} n^3 - n &= 8k^3 - 2k \\ &= 2(4k^2 - k), \end{aligned}$$

and since $4k^2 - k$ is an integer, this says that $n^3 - n$ is even.

Case 2: n is odd. Then $n = 2k + 1$ for some integer k. This gives

$$\begin{aligned} n^3 - n &= (2k+1)^3 - (2k+1) \\ &= 8k^3 + 6k^2 + 6k + 1 - 2k - 1 \\ &= 2(4k^3 + 3k^2 + 2k), \end{aligned}$$

and since $4k^3 + 3k^2 + 2k$ is an integer, we see that $n^3 - n$ is even again.

Since $n^3 - n$ is even in both exhaustive cases, we see that $n^3 - n$ is indeed always even. ■

Exercises

1. Consider the statement "for all integers a and b, if $a + b$ is even, then a and b are even"
   (a) Write the contrapositive of the statement.
   (b) Write the converse of the statement.
   (c) Write the negation of the statement.
   (d) Is the original statement true or false? Prove your answer.
   (e) Is the contrapositive of the original statement true or false? Prove your answer.
   (f) Is the converse of the original statement true or false? Prove your answer.
   (g) Is the negation of the original statement true or false? Prove your answer.

2. For each of the statements below, say what method of proof you should use to prove them. Then say how the proof starts and how it ends. Bonus points for filling in the middle.
   (a) There are no integers x and y such that x is a prime greater than 5 and $x = 6y + 3$.
   (b) For all integers n, if n is a multiple of 3, then n can be written as the sum of consecutive integers.
   (c) For all integers a and b, if $a^2 + b^2$ is odd, then a or b is odd.

3. Consider the statement: for all integers n, if n is even then $8n$ is even.
   (a) Prove the statement. What sort of proof are you using?
   (b) Is the converse true? Prove or disprove.

4. The game TENZI comes with 40 six-sided dice (each numbered 1 to 6). Suppose you roll all 40 dice.
   (a) Prove that there will be at least seven dice that land on the same number.
   (b) How many dice would you have to roll before you were guaranteed that some four of them would all match or all be different? Prove your answer.

5. Prove that for all integers n, it is the case that n is even if and only if $3n$ is even. That is, prove both implications: if n is even, then $3n$ is even, and if $3n$ is even, then n is even.

6. Prove that $\sqrt{3}$ is irrational.

7. Consider the statement: for all integers a and b, if a is even and b is a multiple of 3, then ab is a multiple of 6.

(a) Prove the statement. What sort of proof are you using?

(b) State the converse. Is it true? Prove or disprove.

8. Prove the statement: For all integers n, if $5n$ is odd, then n is odd. Clearly state the style of proof you are using.

9. Prove the statement: For all integers a, b, and c, if $a^2 + b^2 = c^2$, then a or b is even.

10. Suppose that you would like to prove the following implication:

For all numbers n, if n is prime then n is solitary.

Write out the beginning and end of the argument if you were to prove the statement,

(a) Directly

(b) By contrapositive

(c) By contradiction

You do not need to provide details for the proofs (since you do not know what solitary means). However, make sure that you provide the first few and last few lines of the proofs so that we can see that logical structure you would follow.

11. Suppose you have a collection of 5-cent stamps and 8-cent stamps. We saw earlier that it is possible to make any amount of postage greater than 27 cents using combinations of both these types of stamps. But, let's ask some other questions:

(a) Prove that if you only use an even number of both types of stamps, the amount of postage you make must be even.

(b) Suppose you made an even amount of postage. Prove that you used an even number of at least one of the types of stamps.

(c) Suppose you made exactly 72 cents of postage. Prove that you used at least 6 of one type of stamp.

12. Prove: $x = y$ if and only if $xy = \frac{(x+y)^2}{4}$. Note, you will need to prove two "directions" here: the "if" and the "only if" part.

13. Prove that $\log(7)$ is irrational.

14. Prove that there are no integer solutions to the equation $x^2 = 4y + 3$.

15. Prove that every prime number greater than 3 is either one more or one less than a multiple of 6.

16. Your "friend" has shown you a "proof" he wrote to show that $1 = 3$. Here is the proof:
Proof. I claim that $1 = 3$. Of course we can do anything to one side of an equation as long as we also do it to the other side. So subtract 2 from both sides. This gives $-1 = 1$. Now square both sides, to get $1 = 1$. And we all agree this is true. QED

What is going on here? Is your friend's argument valid? Is the argument a proof of the claim $1 = 3$? Carefully explain using what we know about logic.

17. A standard deck of 52 cards consists of 4 suites (hearts, diamonds, spades and clubs) each containing 13 different values (Ace, 2, 3, . . . , 10, J, Q, K). If you draw some number of cards at random you might or might not have a pair (two cards with the same value) or three cards all of the same suit. However, if you draw enough cards, you will be guaranteed to have these. For each of the following, find the smallest number of cards you would need to draw to be guaranteed having the specified cards. Prove your answers.

(a) Three of a kind (for example, three 7's).

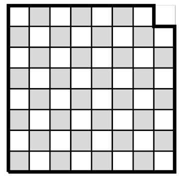
(b) A flush of five cards (for example, five hearts).

(c) Three cards that are either all the same suit or all different suits.

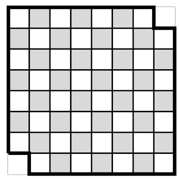
18. Suppose you are at a party with 19 of your closest friends (so including you, there are 20 people there). Explain why there must be least two people at the party who are friends with the same number of people at the party. Assume friendship is always reciprocated.

19. Your friend has given you his list of 115 best Doctor Who episodes (in order of greatness). It turns out that you have seen 60 of them. Prove that there are at least two episodes you have seen that are exactly four episodes apart on your friend's list.

20. Suppose you have an $n \times n$ chessboard but your dog has eaten one of the corner squares. Can you still cover the remaining squares with dominoes? What needs to be true about n? Give necessary and sufficient conditions (that is, say exactly which values of n work and which do not work). Prove your answers.



21. What if your $n \times n$ chessboard is missing two opposite corners? Prove that no matter what n is, you will not be able to cover the remaining squares with dominoes.



3.3 Chapter Summary

We have considered logic both as its own sub-discipline of mathematics, and as a means to help us better understand and write proofs. In either view, we noticed that mathematical statements have a particular logical form, and analyzing that form can help make sense of the statement.

At the most basic level, a statement might combine simpler statements using *logical connectives*. We often make use of variables, and *quantify* over those variables. How to resolve the truth or falsity of a statement based on these connectives and quantifiers is what logic is all about. From this, we can decide whether two statements are logically equivalent or if one or more statements (logically) imply another.

When writing proofs (in any area of mathematics) our goal is to explain why a mathematical statement is true. Thus it is vital that our argument implies the truth of the statement. To be sure of this, we first must know what it means for the statement to be true, as well as ensure that the statements that make up the proof correctly imply the conclusion. A firm understanding of logic is required to check whether a proof is correct.

There is, however, another reason that understanding logic can be helpful. Understanding the logical structure of a statement often gives clues as how to write a proof of the statement.

This is not to say that writing proofs is always straight forward. Consider again the *Goldbach conjecture*:

> Every even number greater than 2 can be written as the sum of two primes.

We are not going to try to prove the statement here, but we can at least say what a proof might look like, based on the logical form of the statement. Perhaps we should write the statement in an equivalent way which better highlights the quantifiers and connectives:

> For all integers n, if n is even and greater than 2, then there exists integers p and q such that p and q are prime and $n = p+q$.

What would a direct proof look like? Since the statement starts with a universal quantifier, we would start by, ``Let n be an arbitrary integer." The rest of the statement is an implication. In a direct proof we assume the "if" part, so the next line would be, "Assume n is greater than 2 and is even." I have no idea what comes next, but eventually, we would need to find two prime numbers p and q (depending on n) and explain how we know that $n = p + q$.

Or maybe we try a proof by contradiction. To do this, we first assume the negation of the statement we want to prove. What is the negation? From what we have studied we should be able to see that it is,

> There is an integer n such that n is even and greater than 2, but for all integers p and q, either p or q is not prime or $n \neq p + q$.

Could this statement be true? A proof by contradiction would start by assuming it was and eventually conclude with a contradiction, proving that our assumption of truth was incorrect. And if you can find such a contradiction, you will have proved the most famous open problem in mathematics. Good luck.

Chapter Review

1. Complete a truth table for the statement $\neg P \rightarrow (Q \wedge R)$.

2. Suppose you know that the statement "if Peter is not tall, then Quincy is fat and Robert is skinny" is false. What, if anything, can you conclude about Peter and Robert if you know that Quincy is indeed fat? Explain (you may reference problem 3.3.1).

3. Are the statements $P \rightarrow (Q \vee R)$ and $(P \rightarrow Q) \vee (P \rightarrow R)$ logically equivalent? Explain your answer.

4. Is the following a valid deduction rule? Explain.

$$\begin{array}{rl} & P \rightarrow Q \\ & P \rightarrow R \\ \hline \therefore & P \rightarrow (Q \wedge R). \end{array}$$

5. Write the negation, converse and contrapositive for each of the statements below.

(a) If the power goes off, then the food will spoil.

(b) If the door is closed, then the light is off.

(c) $\forall x(x < 1 \rightarrow x^2 < 1)$.

(d) For all natural numbers n, if n is prime, then n is solitary.

(e) For all functions f, if f is differentiable, then f is continuous.

(f) For all integers a and b, if $a \cdot b$ is even, then a and b are even.

(g) For every integer x and every integer y there is an integer n such that if $x > 0$ then $nx > y$.

(h) For all real numbers x and y, if $xy = 0$ then $x = 0$ or $y = 0$.

(i) For every student in Math 228, if they do not understand implications, then they will fail the exam.

6. Consider the statement: for all integers n, if n is even and $n \leq 7$ then n is negative or $n \in \{0, 2, 4, 6\}$.

(a) Is the statement true? Explain why.

(b) Write the negation of the statement. Is it true? Explain.

(c) State the contrapositive of the statement. Is it true? Explain.

(d) State the converse of the statement. Is it true? Explain.

7. Consider the statement: $\forall x(\forall y(x + y = y) \rightarrow \forall z(x \cdot z = 0))$.

(a) Explain what the statement says in words. Is this statement true? Be sure to state what you are taking the universe of discourse to be.

(b) Write the converse of the statement, both in words and in symbols. Is the converse true?

(c) Write the contrapositive of the statement, both in words and in symbols. Is the contrapositive true?

(d) Write the negation of the statement, both in words and in symbols. Is the negation true?

8. Simplify the following.

(a) $\neg(\neg(P \wedge \neg Q) \rightarrow \neg(\neg R \vee \neg(P \rightarrow R)))$.

(b) $\neg\exists x \neg\forall y \neg\exists z(z = x + y \rightarrow \exists w(x - y = w))$.

9. Consider the statement: for all integers n, if n is odd, then $7n$ is odd.

(a) Prove the statement. What sort of proof are you using?

(b) Prove the converse. What sort of proof are you using?

10. Suppose you break your piggy bank and scoop up a handful of 22 coins (pennies, nickels, dimes and quarters).

(a) Prove that you must have at least 6 coins of a single denomination.

(b) Suppose you have an odd number of pennies. Prove that you must have an odd number of at least one of the other types of coins.

(c) How many coins would you need to scoop up to be sure that you either had 4 coins that were all the same or 4 coins that were all different? Prove your answer.

11. You come across four trolls playing bridge. They declare:

Troll 1: All trolls here see at least one knave.

Troll 2: I see at least one troll that sees only knaves.

Troll 3: Some trolls are scared of goats.

Troll 4: All trolls are scared of goats.

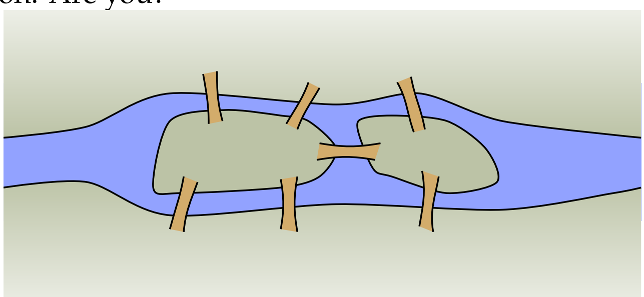
Are there any trolls that are not scared of goats? Recall, of course, that all trolls are either knights (who always tell the truth) or knaves (who always lie).

Chapter 4

Graph Theory

Investigate!

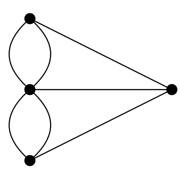
In the time of Euler, in the town of Königsberg in Prussia, there was a river containing two islands. The islands were connected to the banks of the river by seven bridges (as seen below). The bridges were very beautiful, and on their days off, townspeople would spend time walking over the bridges. As time passed, a question arose: was it possible to plan a walk so that you cross each bridge once and only once? Euler was able to answer this question. Are you?



Attempt the above activity before proceeding

Graph Theory is a relatively new area of mathematics, first studied by the super famous mathematician Leonhard Euler in 1735. Since then it has blossomed in to a powerful tool used in nearly every branch of science and is currently an active area of mathematics research.

The problem above, known as the *Seven Bridges of Königsberg*, is the problem that originally inspired graph theory. Consider a "different" problem: Below is a drawing of four dots connected by some lines. Is it possible to trace over each line once and only once (without lifting up your pencil, starting and ending on a dot)?



There is an obvious connection between these two problems. Any path in the dot and line drawing corresponds exactly to a path over the bridges of Königsberg.

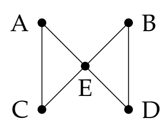
Pictures like the dot and line drawing are called **graphs**. Graphs are made up of a collection of dots called **vertices** and lines connecting those dots called **edges**. When two vertices are connected by an edge, we say they are **adjacent**. The nice thing about looking at graphs instead of pictures of rivers, islands and bridges is that we now have a mathematical object to study. We have distilled the "important" parts of the bridge picture for the purposes of the problem. It does not matter how big the islands are, what the bridges are made out of, if the river contains alligators, etc. All that matters is which land masses are connected to which other land masses, and how many times.

We will return to the question of finding paths through graphs later. But first, here are a few other situations you can represent with graphs:

Example 4.0.1

Al, Bob, Cam, Dan, and Euler are all members of the social networking website *Facebook*. The site allows members to be "friends" with each other. It turns out that Al and Cam are friends, as are Bob and Dan. Euler is friends with everyone. Represent this situation with a graph.

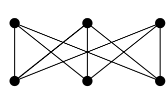
Solution. Each person will be represented by a vertex and each friendship will be represented by an edge. That is, two vertices will be adjacent (there will be an edge between them) if and only if the people represented by those vertices are friends.



Example 4.0.2

Each of three houses must be connected to each of three utilities. Is it possible to do this without any of the utility lines crossing?

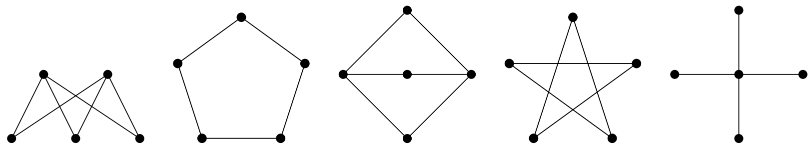
Solution. We will answer this question later. For now, notice how we would ask this question in the context of graph theory. We are really asking whether it is possible to redraw the graph below without any edges crossing (except at vertices). Think of the top row as the houses, bottom row as the utilities.



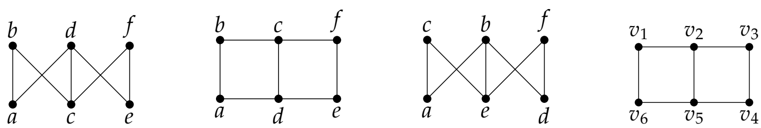
4.1 Definitions

Investigate!

Which (if any) of the graphs below are the same?



The graphs above are unlabeled. Usually we think of a graph as having a specific set of vertices. Which (if any) of the graphs below are the same?



Actually, all the graphs we have seen above are just *drawings* of graphs. A graph is really an abstract mathematical object consisting of two sets V and E where E is a set of 2-element subsets of V. Are the graphs below the same or different?

Graph 1:

$$V = \{a, b, c, d, e\},$$

$$E = \{\{a, b\}, \{a, c\}, \{a, d\}, \{a, e\}, \{b, c\}, \{d, e\}\}.$$

Graph 2:

$$V = \{v_1, v_2, v_3, v_4, v_5\},$$

$$E = \{\{v_1, v_3\}, \{v_1, v_5\}, \{v_2, v_4\}, \{v_2, v_5\}, \{v_3, v_5\}, \{v_4, v_5\}\}.$$

Attempt the above activity before proceeding

Before we start studying graphs, we need to agree upon what a graph is. While we almost always think of graphs as pictures (dots connected by lines) this is fairly ambiguous. Do the lines need to be straight? Does it matter how long the lines are or how large the dots are? Can there be two lines connecting the same pair of dots? Can one line connect three dots?

The way we avoid ambiguities in mathematics is to provide concrete and rigorous *definitions*. Crafting good definitions is not easy, but it is incredibly important. The definition is the agreed upon starting point from which all truths in mathematics proceed. Is there a graph with no edges? We have to look at the definition to see if this is possible.

We want our definition to be precise and unambiguous, but it also must agree with our intuition for the objects we are studying. It needs to be useful: we *could* define a graph to be a six legged mammal, but that would not let us solve any problems about bridges. Instead, here is the (now) standard definition of a graph.

Graph Definition.

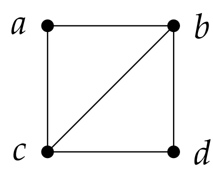
A **graph** is an ordered pair $G = (V, E)$ consisting of a nonempty set V (called the **vertices**) and a set E (called the **edges**) of two-element subsets of V.

Strange. Nowhere in the definition is there talk of dots or lines. From the definition, a graph could be

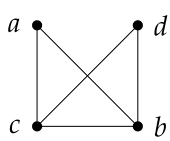
$$(\{a, b, c, d\}, \{\{a, b\}, \{a, c\}, \{b, c\}, \{b, d\}, \{c, d\}\}).$$

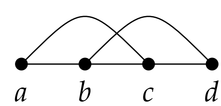
Here we have a graph with four vertices (the letters a, b, c, d) and five edges (the pairs $\{a, b\}, \{a, c\}, \{b, c\}, \{b, d\}, \{c, d\}$).

Looking at sets and sets of 2-element sets is difficult to process. That is why we often draw a representation of these sets. We put a dot down for each vertex, and connect two dots with a line precisely when those two vertices are one of the 2-element subsets in our set of edges. Thus one way to draw the graph described above is this:



However we could also have drawn the graph differently. For example either of these:





We should be careful about what it means for two graphs to be "the same." Actually, given our definition, this is easy: Are the vertex sets equal? Are the edge sets equal? We know what it means for sets to be equal, and graphs are nothing but a pair of two special sorts of sets.

Example 4.1.1

Are the graphs below equal?

$$G_1 = (\{a, b, c\}, \{\{a, b\}, \{b, c\}\}); \qquad G_2 = (\{a, b, c\}, \{\{a, c\}, \{c, b\}\}).$$

Solution. No. Here the vertex sets of each graph are equal, which is a good start. Also, both graphs have two edges. In the first graph, we have edges $\{a, b\}$ and $\{b, c\}$, while in the second graph we have edges $\{a, c\}$ and $\{c, b\}$. Now we do have $\{b, c\} = \{c, b\}$, so that is not the problem. The issue is that $\{a, b\} \neq \{a, c\}$. Since the edge sets of the two graphs are not equal (as sets), the graphs are not equal (as graphs).

Even if two graphs are not *equal*, they might be *basically* the same. The graphs in the previous example could be drawn like this:

Graphs that are basically the same (but perhaps not equal) are called **isomorphic**. We will give a precise definition of this term after a quick example:

Example 4.1.2

Consider the graphs:

$G_1 = (V_1, E_1)$ where $V_1 = \{a, b, c\}$ and $E_1 = \{\{a, b\}, \{a, c\}, \{b, c\}\}$;

$G_2 = (V_2, E_2)$ where $V_2 = \{u, v, w\}$ and $E_2 = \{\{u, v\}, \{u, w\}, \{v, w\}\}$.

Are these graphs the same?

Solution. The two graphs are NOT equal. It is enough to notice that $V_1 \neq V_2$ since $a \in V_1$ but $a \notin V_2$. However, both of these graphs consist of three vertices with edges connecting every pair of vertices. We can draw them as follows:

Clearly we want to say these graphs are basically the same, so while they are not equal, they will be *isomorphic*. We can rename the vertices of one graph and get the second graph as the result.

Intuitively, graphs are **isomorphic** if they are basically the same, or better yet, if they are the same except for the names of the vertices. To make the concept of renaming vertices precise, we give the following definitions:

Isomorphic Graphs.

An **isomorphism** between two graphs G_1 and G_2 is a bijection $f: V_1 \to V_2$ between the vertices of the graphs such that $\{a, b\}$ is an edge in G_1 if and only if $\{f(a), f(b)\}$ is an edge in G_2.

Two graphs are **isomorphic** if there is an isomorphism between them. In this case we write $G_1 \cong G_2$.

An isomorphism is simply a function which renames the vertices. It must be a bijection so every vertex gets a new name. These newly named vertices must be connected by edges precisely when they were connected by edges with their old names.

Example 4.1.3

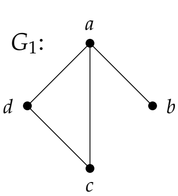
Decide whether the graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are equal or isomorphic.

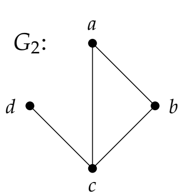
$V_1 = \{a, b, c, d\}$, $E_1 = \{\{a, b\}, \{a, c\}, \{a, d\}, \{c, d\}\}$
$V_2 = \{a, b, c, d\}$, $E_2 = \{\{a, b\}, \{a, c\}, \{b, c\}, \{c, d\}\}$

Solution. The graphs are NOT equal, since $\{a, d\} \in E_1$ but $\{a, d\} \notin E_2$. However, since both graphs contain the same number of vertices and same number of edges, they *might* be isomorphic (this is not enough in most cases, but it is a good start).

We can try to build an isomorphism. How about we say $f(a) = b$, $f(b) = c$, $f(c) = d$ and $f(d) = a$. This is definitely a bijection, but to make sure that the function is an isomorphism, we must make sure it *respects the edge relation*. In G_1, vertices a and b are connected by an edge. In G_2, $f(a) = b$ and $f(b) = c$ are connected by an edge. So far, so good, but we must check the other three edges. The edge $\{a, c\}$ in G_1 corresponds to $\{f(a), f(c)\} = \{b, d\}$, but here we have a problem. There is no edge between b and d in G_2. Thus f is NOT an isomorphism.

Not all hope is lost, however. Just because f is not an isomorphism does not mean that there is no isomorphism at all. We can try again. At this point it might be helpful to draw the graphs to see how they should match up.





Alternatively, notice that in G_1, the vertex a is adjacent to every other vertex. In G_2, there is also a vertex with this property: c. So build the bijection $g : V_1 \to V_2$ by defining $g(a) = c$ to start with. Next, where should we send b? In G_1, the vertex b is only adjacent to vertex a. There is exactly one vertex like this in G_2, namely d. So let $g(b) = d$. As for the last two, in this example, we have a free choice: let $g(c) = b$ and $g(d) = a$ (switching these would be fine as well).

We should check that this really is an isomorphism. It is definitely a bijection. We must make sure that the edges are respected. The four edges in G_1 are

$$\{a, b\}, \{a, c\}, \{a, d\}, \{c, d\}.$$

Under the proposed isomorphism these become

$$\{g(a), g(b)\}, \{g(a), g(c)\}, \{g(a), g(d)\}, \{g(c), g(d)\}$$

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

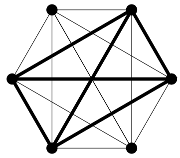
which are precisely the edges in G_2. Thus g is an isomorphism, so $G_1 \cong G_2$

Sometimes we will talk about a graph with a special name (like K_n or the *Peterson graph*) or perhaps draw a graph without any labels. In this case we are really referring to *all* graphs isomorphic to any copy of that particular graph. A collection of isomorphic graphs is often called an **isomorphism class**. [1]

There are other relationships between graphs that we care about, other than equality and being isomorphic. For example, compare the following pair of graphs:

These are definitely not isomorphic, but notice that the graph on the right looks like it might be part of the graph on the left, especially if we draw it like this:

[1] This is not unlike geometry, where we might have more than one copy of a particular triangle. There instead of *isomorphic* we say *congruent*.



We would like to say that the smaller graph is a *subgraph* of the larger.

We should give a careful definition of this. In fact, there are two reasonable notions for what a subgraph should mean.

Subgraphs.

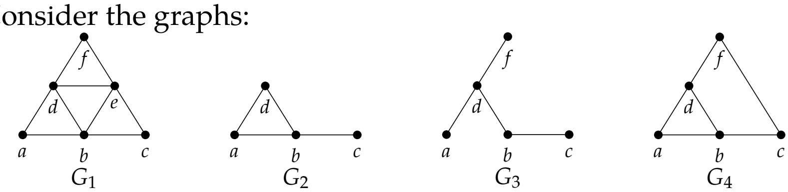
We say that $G' = (V', E')$ is a **subgraph** of $G = (V, E)$, and write $G' \subseteq G$, provided $V' \subseteq V$ and $E' \subseteq E$.

We say that $G' = (V', E')$ is an **induced subgraph** of $G = (V, E)$ provided $V' \subseteq V$ and every edge in E whose vertices are still in V' is also an edge in E'.

Notice that every induced subgraph is also an ordinary subgraph, but not conversely. Think of a subgraph as the result of deleting some vertices and edges from the larger graph. For the subgraph to be an induced subgraph, we can still delete vertices, but now we only delete those edges that included the deleted vertices.

Example 4.1.4

Consider the graphs:



Here both G_2 and G_3 are subgraphs of G_1. But only G_2 is an *induced* subgraph. Every edge in G_1 that connects vertices in G_2 is also an edge in G_2. In G_3, the edge $\{a, b\}$ is in E_1 but not E_3, even though vertices a and b are in V_3.

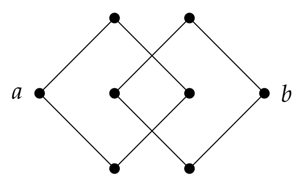
The graph G_4 is NOT a subgraph of G_1, even though it looks like all we did is remove vertex e. The reason is that in E_4 we have the edge $\{c, f\}$ but this is not an element of E_1, so we don't have the required $E_4 \subseteq E_1$.

Back to some basic graph theory definitions. Notice that all the graphs we have drawn above have the property that no pair of vertices is connected more than once, and no vertex is connected to itself. Graphs like these are sometimes called **simple**, although we will just call them *graphs*. This is because our definition for a graph says that the edges form a set of

2-element subsets of the vertices. Remember that it doesn't make sense to say a set contains an element more than once. So no pair of vertices can be connected by an edge more than once. Also, since each edge must be a set containing two vertices, we cannot have a single vertex connected to itself by an edge.

That said, there are times we want to consider double (or more) edges and single edge loops. For example, the "graph" we drew for the Bridges of Königsberg problem had double edges because there really are two bridges connecting a particular island to the near shore. We will call these objects **multigraphs**. This is a good name: a *multiset* is a set in which we are allowed to include a single element multiple times.

The graphs above are also **connected**: you can get from any vertex to any other vertex by following some path of edges. A graph that is not connected can be thought of as two separate graphs drawn close together. For example, the following graph is NOT connected because there is no path from a to b:



Vertices in a graph do not always have edges between them. If we add all possible edges, then the resulting graph is called **complete**. That is, a graph is complete if every pair of vertices is connected by an edge. Since a graph is determined completely by which vertices are adjacent to which other vertices, there is only one complete graph with a given number of vertices. We give these a special name: K_n is the complete graph on n vertices.

Each vertex in K_n is adjacent to $n-1$ other vertices. We call the number of edges emanating from a given vertex the **degree** of that vertex. So every vertex in K_n has degree $n-1$. How many edges does K_n have? One might think the answer should be $n(n-1)$, since we count $n-1$ edges n times (once for each vertex). However, each edge is incident to 2 vertices, so we counted every edge exactly twice. Thus there are $n(n-1)/2$ edges in K_n. Alternatively, we can say there are $\binom{n}{2}$ edges, since to draw an edge we must choose 2 of the n vertices.

In general, if we know the degrees of all the vertices in a graph, we can find the number of edges. The sum of the degrees of all vertices will always be *twice* the number of edges, since each edge adds to the degree of two vertices. Notice this means that the sum of the degrees of all vertices in any graph must be even!

This is our first example of a general result about all graphs. It seems innocent enough, but we will use it to prove all sorts of other statements. So let's give it a name and state it formally.

Lemma 4.1.5 Handshake Lemma. *In any graph, the sum of the degrees of vertices in the graph is always twice the number of edges.*

The handshake lemma[2] is sometimes called the *degree sum formula*, and can be written symbolically as

$$\sum_{v \in V} d(v) = 2e.$$

Here we are using the notation $d(v)$ for the degree of the vertex v.

One use for the lemma is to actually find the number of edges in a graph. To do this, you must be given the **degree sequence** for the graph (or be able to find it from other information). This is a list of every degree of every vertex in the graph, generally written in non-increasing order.

Example 4.1.6

How many vertices and edges must a graph have if its degree sequence is

$$(4, 4, 3, 3, 3, 2, 1)?$$

Solution. The number of vertices is easy to find: it is the number of degrees in the sequence: 7. To find the number of edges, we compute the degree sum:

$$4 + 4 + 3 + 3 + 3 + 2 + 1 = 20,$$

so the number of edges is half this: 10.

The handshake lemma also tells us what is not possible.

Example 4.1.7

At a recent math seminar, 9 mathematicians greeted each other by shaking hands. Is it possible that each mathematician shook hands with exactly 7 people at the seminar?

Solution. It seems like this should be possible. Each mathematician chooses one person to not shake hands with. But this cannot happen. We are asking whether a graph with 9 vertices can have each vertex have degree 7. If such a graph existed, the sum of the degrees of

[2] A *lemma* is a mathematical statement that is primarily of importance in that it is used to establish other results.

the vertices would be $9 \cdot 7 = 63$. This would be twice the number of edges (handshakes) resulting in a graph with 31.5 edges. That is impossible. Thus at least one (in fact an odd number) of the mathematicians must have shaken hands with an *even* number of people at the seminar.

We can generalize the previous example to get the following proposition.[3]

Proposition 4.1.8 *In any graph, the number of vertices with odd degree must be even.*

Proof. Suppose there were a graph with an odd number of vertices with odd degree. Then the sum of the degrees in the graph would be odd, which is impossible, by the handshake lemma. QED

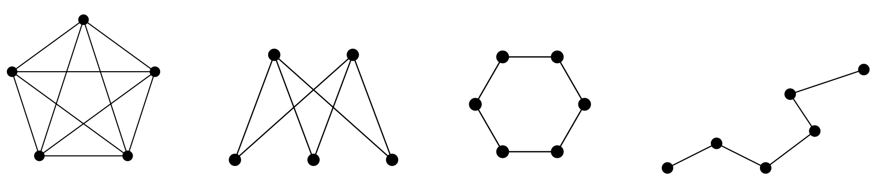
We will consider further applications of the handshake lemma in the exercises.

One final definition: we say a graph is **bipartite** if the vertices can be divided into two sets, A and B, with no two vertices in A adjacent and no two vertices in B adjacent. The vertices in A can be adjacent to some or all of the vertices in B. If each vertex in A is adjacent to all the vertices in B, then the graph is a **complete bipartite graph**, and gets a special name: $K_{m,n}$, where $|A| = m$ and $|B| = n$. The graph in the houses and utilities puzzle is $K_{3,3}$.

Named Graphs.

Some graphs are used more than others, and get special names.

- K_n The complete graph on n vertices.
- $K_{m,n}$ The complete bipartite graph with sets of m and n vertices.
- C_n The cycle on n vertices, just one big loop.
- P_n The path on $n+1$ vertices (so n edges), just one long path.



K_5 $K_{2,3}$ C_6 P_5

[3]A **proposition** is a general statement in mathematics, similar to a theorem, although generally of lesser importance.

Graph Theory Definitions.

There are a lot of definitions to keep track of in graph theory. Here is a glossary of the terms we have already used and will soon encounter.

Graph
: A collection of **vertices**, some of which are connected by **edges**. More precisely, a pair of sets V and E where V is a set of vertices and E is a set of 2-element subsets of V.

Adjacent
: Two vertices are **adjacent** if they are connected by an edge. Two edges are **adjacent** if they share a vertex.

Bipartite graph
: A graph for which it is possible to divide the vertices into two disjoint sets such that there are no edges between any two vertices in the same set.

Complete bipartite graph
: A bipartite graph for which every vertex in the first set is adjacent to every vertex in the second set.

Complete graph
: A graph in which every pair of vertices is adjacent.

Connected
: A graph is **connected** if there is a path from any vertex to any other vertex.

Chromatic number
: The minimum number of colors required in a proper vertex coloring of the graph.

Cycle
: A path (see below) that starts and stops at the same vertex, but contains no other repeated vertices.

Degree of a vertex
: The number of edges incident to a vertex.

Euler path
: A walk which uses each edge exactly once.

Euler circuit
: An Euler path which starts and stops at the same vertex.

Multigraph
: A **multigraph** is just like a graph but can contain multiple edges between two vertices as well as single edge loops (that is an edge from a vertex to itself).

Path A **path** is a walk that doesn't repeat any vertices (or edges) except perhaps the first and last. If a path starts and ends at the same vertex, it is called a **cycle**.

Planar
A graph which can be drawn (in the plane) without any edges crossing.

Subgraph
We say that H is a **subgraph** of G if every vertex and edge of H is also a vertex or edge of G. We say H is an **induced** subgraph of G if every vertex of H is a vertex of G and each pair of vertices in H are adjacent in H if and only if they are adjacent in G.

Tree A connected graph with no cycles. (If we remove the requirement that the graph is connected, the graph is called a **forest**.) The vertices in a tree with degree 1 are called **leaves**.

Vertex coloring
An assignment of colors to each of the vertices of a graph. A vertex coloring is **proper** if adjacent vertices are always colored differently.

Walk A sequence of vertices such that consecutive vertices (in the sequence) are adjacent (in the graph). A walk in which no edge is repeated is called a **trail**, and a trail in which no vertex is repeated (except possibly the first and last) is called a **path**.

Exercises

1. If 10 people each shake hands with each other, how many handshakes took place? What does this question have to do with graph theory?

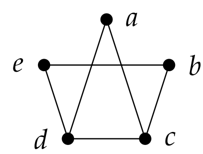
2. Among a group of 5 people, is it possible for everyone to be friends with exactly 2 of the people in the group? What about 3 of the people in the group?

3. Is it possible for two *different* (non-isomorphic) graphs to have the same number of vertices and the same number of edges? What if the degrees of the vertices in the two graphs are the same (so both graphs have vertices with degrees 1, 2, 2, 3, and 4, for example)? Draw two such graphs or explain why not.

4. Are the two graphs below equal? Are they isomorphic? If they are isomorphic, give the isomorphism. If not, explain.
   Graph 1:

$$V = \{a, b, c, d, e\}, E = \{\{a, b\}, \{a, c\}, \{a, e\}, \{b, d\}, \{b, e\}, \{c, d\}\}.$$

   Graph 2:



5. Consider the following two graphs:

G_1 $\quad V_1 = \{a, b, c, d, e, f, g\}$

$E_1 = \{\{a, b\}, \{a, d\}, \{b, c\}, \{b, d\}, \{b, e\}, \{b, f\}, \{c, g\}, \{d, e\}, \{e, f\}, \{f, g\}\}.$

G_2 $\quad V_2 = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\},$

$E_2 = \{\{v_1, v_4\}, \{v_1, v_5\}, \{v_1, v_7\}, \{v_2, v_3\}, \{v_2, v_6\}, \{v_3, v_5\}, \{v_3, v_7\}, \{v_4, v_5\}, \{v_5, v_6\}, \{v_5, v_7\}\}$

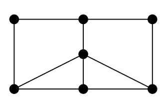
(a) Let $f : G_1 \to G_2$ be a function that takes the vertices of Graph 1 to vertices of Graph 2. The function is given by the following table:

x	a	b	c	d	e	f	g
$f(x)$	v_4	v_5	v_1	v_6	v_2	v_3	v_7

Does f define an isomorphism between Graph 1 and Graph 2?

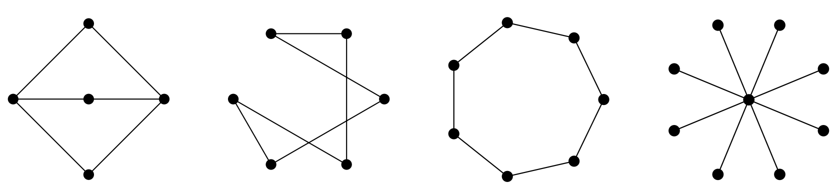
(b) Define a new function g (with $g \neq f$) that defines an isomorphism between Graph 1 and Graph 2.

(c) Is the graph pictured below isomorphic to Graph 1 and Graph 2? Explain.



6. What is the largest number of edges possible in a graph with 10 vertices? What is the largest number of edges possible in a *bipartite* graph with 10 vertices? What is the largest number of edges possible in a *tree* with 10 vertices?

7. Which of the graphs below are bipartite? Justify your answers.



8. For which $n \geq 3$ is the graph C_n bipartite?

9. For each of the following, try to give two *different* unlabeled graphs with the given properties, or explain why doing so is impossible.

(a) Two different trees with the same number of vertices and the same number of edges. A tree is a connected graph with no cycles.

(b) Two different graphs with 8 vertices all of degree 2.

(c) Two different graphs with 5 vertices all of degree 4.

(d) Two different graphs with 5 vertices all of degree 3.

10. Decide whether the statements below about subgraphs are true or false. For those that are true, briefly explain why (1 or 2 sentences). For any that are false, give a counterexample.

(a) Any subgraph of a complete graph is also complete.

(b) Any *induced* subgraph of a complete graph is also complete.

(c) Any subgraph of a bipartite graph is bipartite.

(d) Any subgraph of a tree is a tree.

11. Let $k_1, k_2, \ldots, k_j$ be a list of positive integers that sum to n (i.e., $\sum_{i=1}^{j} k_i = n$). Use two graphs containing n vertices to explain why

$$\sum_{i=1}^{j} \binom{k_i}{2} \leq \binom{n}{2}.$$

12. We often define graph theory concepts using set theory. For example, given a graph $G = (V, E)$ and a vertex $v \in V$, we define

$$N(v) = \{u \in V : \{v, u\} \in E\}.$$

We define $N[v] = N(v) \cup \{v\}$. The goal of this problem is to figure out what all this means.

(a) Let G be the graph with $V = \{a, b, c, d, e, f\}$ and $E = \{\{a, b\}, \{a, e\}, \{b, c\}, \{b, e\}, \{c, d\}, \{c, f\}, \{d, f\}, \{e, f\}\}$. Find $N(a)$, $N[a]$, $N(c)$, and $N[c]$.

(b) What is the largest and smallest possible values for $|N(v)|$ and $|N[v]|$ for the graph in part (a)? Explain.

(c) Give an example of a graph $G = (V, E)$ (probably different than the one above) for which $N[v] = V$ for some vertex $v \in V$. Is there a graph for which $N[v] = V$ for *all* $v \in V$? Explain.

(d) Give an example of a graph $G = (V, E)$ for which $N(v) = \emptyset$ for some $v \in V$. Is there an example of such a graph for which $N[u] = V$ for some other $u \in V$ as well? Explain.

(e) Describe in words what $N(v)$ and $N[v]$ mean in general.

13. A graph is a way of representing the relationships between elements in a set: an edge between the vertices x and y tells us that x is related to y (which we can write as $x \sim y$). Not all sorts of relationships can be represented by a graph though. For each relationship described below, either draw the graph or explain why the relationship cannot be represented by a graph.

(a) The set $V = \{1, 2, \ldots, 9\}$ and the relationship $x \sim y$ when $x - y$ is a non-zero multiple of 3.

(b) The set $V = \{1, 2, \ldots, 9\}$ and the relationship $x \sim y$ when y is a multiple of x.

(c) The set $V = \{1, 2, \ldots, 9\}$ and the relationship $x \sim y$ when $0 < |x - y| < 3$.

14. Consider graphs with n vertices. Remember, graphs do not need to be *connected*.

(a) How many edges must the graph have to guarantee at least one vertex has degree two or more? Prove your answer.

(b) How many edges must the graph have to guarantee all vertices have degree two or more? Prove your answer.

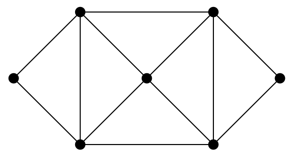
15. Prove that any graph with at least two vertices must have two vertices of the same degree.

16. Suppose G is a connected graph with $n > 1$ vertices and $n - 1$ edges. Prove that G has a vertex of degree 1.

4.2 Trees

Investigate!

Consider the graph drawn below.



1. Find a subgraph with the smallest number of edges that is still connected and contains all the vertices.
2. Find a subgraph with the largest number of edges that doesn't contain any cycles.
3. What do you notice about the number of edges in your examples above? Is this a coincidence?

Attempt the above activity before proceeding

One very useful and common approach to studying graph theory is to restrict your focus to graphs of a particular kind. For example, you could try to really understand just complete graphs or just bipartite graphs, instead of trying to understand all graphs in general. That is what we are going to do now, looking at *trees*. Hopefully by the end of this section we will have a better understanding of this class of graph, and also understand why it is important enough to warrant its own section.

Definition of a Tree.

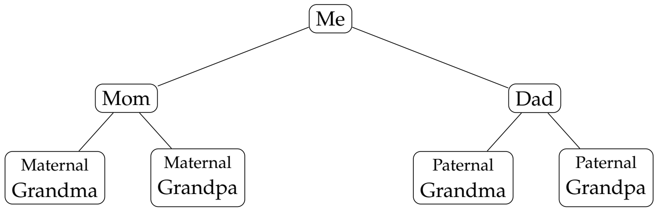
A **tree** is a connected graph containing no cycles.[4]

A **forest** is a graph containing no cycles. Note that this means that a connected forest is a tree.

Does the definition above agree with your intuition for what graphs we should call trees? Try thinking of examples of trees and make sure they satisfy the definition. One thing to keep in mind is that while the trees we study in graph theory are related to trees you might see in other subjects, the correspondence is not exact. For instance, in anthropology, you might study family trees, like the one below,

---

[4]Sometimes this is stated as "a tree is an acyclic connected graph;" "acyclic" is just a fancy word for "containing no cycles."



So far so good, but while your grandparents are (probably) not blood-relatives, if we go back far enough, it is likely that they did have *some* common ancestor. If you trace the tree back from you to that common ancestor, then down through your other grandparent, you would have a cycle, and thus the graph would not be a tree.

You might also have seen something called a *decision tree* (such as the algorithm for deciding whether a series converges or diverges). Sometimes these too contain cycles, as the decision for one node might lead you back to a previous step.

Both the examples of trees above also have another feature worth mentioning: there is a clear order to the vertices in the tree. In general, there is no reason for a tree to have this added structure, although we can impose such a structure by considering **rooted trees**, where we simply designate one vertex as the *root*. We will consider such trees in more detail later in this section.

Properties of Trees

We wish to really understand trees. This means we should discover properties of trees; what makes them special and what is special about them.

A tree is a connected graph with no cycles. Is there anything else we can say? It would be nice to have other equivalent conditions for a graph to be a tree. That is, we would like to know whether there are any graph theoretic properties that all trees have, and perhaps even that *only* trees have.

To get a feel for the sorts of things we can say, we will consider three *propositions* about trees. These will also illustrate important proof techniques that apply to graphs in general, and happen to be a little easier for trees.

Our first proposition gives an alternate definition for a tree. That is, it gives necessary and sufficient conditions for a graph to be a tree.

Proposition 4.2.1 *A graph T is a tree if and only if between every pair of distinct vertices of T there is a unique path.*

Proof. This is an "if and only if" statement, so we must prove two implications. We start by proving that if T is a tree, then between every pair of distinct vertices there is a unique path.

Assume T is a tree, and let u and v be distinct vertices (if T only has one vertex, then the conclusion is satisfied automatically). We must show two things to show that there is a unique path between u and v: that there is a path, and that there is not more than one path. The first of these is automatic, since T is a tree, it is connected, so there is a path between any pair of vertices.

To show the path is unique, we suppose there are two paths between u and v, and get a contradiction. The two paths might start out the same, but since they are different, there is some first vertex u' after which the two paths diverge. However, since the two paths both end and v, there is some first vertex after u' that they have in common, call it v'. Now consider the two paths from u' to v'. Taken together, these form a cycle, which contradicts our assumption that T is a tree.

Now we consider the converse: if between every pair of distinct vertices of T there is a unique path, then T is a tree. So assume the hypothesis: between every pair of distinct vertices of T there is a unique path. To prove that T is a tree, we must show it is connected and contains no cycles.

The first half of this is easy: T is connected, because there is a path between every pair of vertices. To show that T has no cycles, we assume it does, for the sake of contradiction. Let u and v be two distinct vertices in a cycle of T. Since we can get from u to v by going clockwise or counterclockwise around the cycle, there are two paths from u and v, contradicting our assumption.

We have established both directions so we have completed the proof.

QED

Read the proof above very carefully. Notice that both directions had two parts: the existence of paths, and the uniqueness of paths (which related to the fact that there were no cycles). In this case, these two parts were really separate. In fact, if we just considered graphs with no cycles (a forest), then we could still do the parts of the proof that explore the uniqueness of paths between vertices, even if there might not *exist* paths between vertices.

This observation allows us to state the following *corollary*:[5]

Corollary 4.2.2 *A graph F is a forest if and only if between any pair of vertices in F there is at most one path.*

We do not give a proof of the corollary (it is, after all, supposed to follow directly from the proposition) but for practice, you are asked to give a careful proof in the exercises. When you do so, try to use proof by contrapositive instead of proof by contradiction.

[5] A corollary is another sort of provable statement, like a proposition or theorem, but one that follows direction from another already established statement, or its proof.

Our second proposition tells us that all trees have **leaves**: vertices of degree one.

Proposition 4.2.3 *Any tree with at least two vertices has at least two vertices of degree one.*

Proof. We give a proof by contradiction. Let T be a tree with at least two vertices, and suppose, contrary to stipulation, that there are not two vertices of degree one.

Let P be a path in T of longest possible length. Let u and v be the endpoints of the path. Since T does not have two vertices of degree one, at least one of these must have degree two or higher. Say that it is u. We know that u is adjacent to a vertex in the path P, but now it must also be adjacent to another vertex, call it u'.

Where is u'? It cannot be a vertex of P, because if it was, there would be two distinct paths from u to u': the edge between them, and the first part of P (up to u'). But u' also cannot be outside of P, for if it was, there would be a path from u' to v that was longer than P, which has longest possible length.

This contradiction proves that there must be at least two vertices of degree one. In fact, we can say a little more: u and v must *both* have degree one. QED

The proposition is quite useful when proving statements about trees, because we often prove statements about trees by *induction*. To do so, we need to reduce a given tree to a smaller tree (so we can apply the inductive hypothesis). Getting rid of a vertex of degree one is an obvious choice, and now we know there is always one to get rid of.

To illustrate how induction is used on trees, we will consider the relationship between the number of vertices and number of edges in trees. Is there a tree with exactly 7 vertices and 7 edges? Try to draw one. Could a tree with 7 vertices have only 5 edges? There is a good reason that these seem impossible to draw.

Proposition 4.2.4 *Let T be a tree with v vertices and e edges. Then $e = v - 1$.*

Proof. We will give a proof by induction on the number of vertices in the tree. That is, we will prove that every tree with v vertices has exactly $v - 1$ edges, and then use induction to show this is true for all $v \geq 1$.

For the base case, consider all trees with $v = 1$ vertices. There is only one such tree: the graph with a single isolated vertex. This graph has $e = 0$ edges, so we see that $e = v - 1$ as needed.

Now for the inductive case, fix $k \geq 1$ and assume that all trees with $v = k$ vertices have exactly $e = k - 1$ edges. Now consider an arbitrary tree T with $v = k + 1$ vertices. By Proposition 4.2.3, T has a vertex v_0 of degree one. Let T' be the tree resulting from removing v_0 from T (together with its incident edge). Since we removed a leaf, T' is still a tree (the unique paths between pairs of vertices in T' are the same as the unique paths between them in T).

Now T' has k vertices, so by the inductive hypothesis, has $k-1$ edges. What can we say about T? Well, it has one more edge than T', so it has k edges. But this is exactly what we wanted: $v = k+1$, $e = k$ so indeed $e = v - 1$. This completes the inductive case, and the proof. QED

There is a very important feature of this induction proof that is worth noting. Induction makes sense for proofs about graphs because we can think of graphs as growing into larger graphs. However, this does NOT work. It would not be correct to start with a tree with k vertices, and then add a new vertex and edge to get a tree with $k+1$ vertices, and note that the number of edges also grew by one. Why is this bad? Because how do you know that *every* tree with $k+1$ vertices is the result of adding a vertex to your arbitrary starting tree? You don't!

The point is that whenever you give an induction proof that a statement about graphs that holds for all graphs with v vertices, you must start with an arbitrary graph with $v+1$ vertices, then *reduce* that graph to a graph with v vertices, to which you can apply your inductive hypothesis.

Rooted Trees

So far, we have thought of trees only as a particular kind of graph. However, it is often useful to add additional structure to trees to help solve problems. Data is often structured like a tree. This book, for example, has a tree structure: draw a vertex for the book itself. Then draw vertices for each chapter, connected to the book vertex. Under each chapter, draw a vertex for each section, connecting it to the chapter it belongs to. The graph will not have any cycles; it will be a tree. But a tree with clear hierarchy which is not present if we don't identify the book vertex as the "top".

As soon as one vertex of a tree is designated as the **root**, then every other vertex on the tree can be characterized by its position relative to the root. This works because there is a unique path between any two vertices in a tree. So from any vertex, we can travel back to the root in exactly one way. This also allows us to describe how distinct vertices in a rooted tree are related.

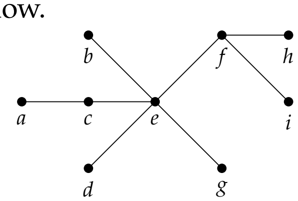
If two vertices are adjacent, then we say one of them is the **parent** of the other, which is called the **child** of the parent. Of the two, the parent is the vertex that is closer to the root. Thus the root of a tree is a parent, but is not the child of any vertex (and is unique in this respect: all non-root vertices have *exactly one* parent).

Not surprisingly, the child of a child of a vertex is called the **grandchild** of the vertex (and it is the **grandparent**). More in general, we say that a vertex v is a **descendent** of a vertex u provided u is a vertex on the path from v to the root. Then we would call u an **ancestor** of v.

For most trees (in fact, all except paths with one end the root), there will be pairs of vertices neither of which is a descendant of the other. We might call these cousins or siblings. In fact, vertices u and v are called **siblings** provided they have the same parent. Note that siblings are never adjacent (do you see why?).

Example 4.2.5

Consider the tree below.



If we designate vertex f as the root, then e, h, and i are the children of f, and are siblings of each other. Among the other things we cay say are that a is a child of c, and a descendant of f. The vertex g is a descendant of f, in fact, is a grandchild of f. Vertices g and d are siblings, since they have the common parent e.

Notice how this changes if we pick a different vertex for the root. If a is the root, then its lone child is c, which also has only one child, namely e. We would then have f the child of e (instead of the other way around), and f is the descendant of a, instead of the ancestor. f and g are now siblings.

All of this flowery language helps us describe how to *navigate* through a tree. Traversing a tree, visiting each vertex in some order, is a key step in many algorithms. Even if the tree is not rooted, we can always form a rooted tree by picking any vertex as the root. Here is an example of why doing so can be helpful.

Example 4.2.6

Explain why every tree is a bipartite graph.

Solution. To show that a graph is bipartite, we must divide the vertices into two sets A and B so that no two vertices in the same set are adjacent. Here is an algorithm that does just this.

Designate any vertex as the root. Put this vertex in set A. Now put all of the children of the root in set B. None of these children

> are adjacent (they are siblings), so we are good so far. Now put into A every child of every vertex in B (i.e., every grandchild of the root). Keep going until all vertices have been assigned one of the sets, alternating between A and B every "generation." That is, a vertex is in set B if and only if it is the child of a vertex in set A.

The key to how we partitioned the tree in the example was to know which vertex to assign to a set next. We chose to visit all vertices in the same generation before any vertices of the next generation. This is usually called a **breadth first search** (we say "search" because you often traverse a tree looking for vertices with certain properties).

In contrast, we could also have partitioned the tree in a different order. Start with the root, put it in A. Then look for one child of the root to put in B. Then find a child of that vertex, into A, and then find its child, into B, and so on. When you get to a vertex with no children, retreat to its parent and see if the parent has any other children. So we travel as far from the root as fast as possible, then backtrack until we can move forward again. This is called **depth first search**.

These algorithmic explanations can serve as a proof that every tree is bipartite, although care needs to be spent to prove that the algorithms are *correct*. Another approach to prove that all trees are bipartite, using induction, is requested in the exercises.

Spanning Trees

One of the advantages of trees is that they give us a few simple ways to travel through the vertices. If a connected graph is not a tree, then we can still use these traversal algorithms if we identify a subgraph that *is* a tree.

First we should consider if this even makes sense. Given any connected graph G, will there always be a subgraph that is a tree? Well, that is actually too easy: you could just take a single vertex of G. If we want to use this subgraph to tell us how to visit all vertices, then we want our subgraph to include all of the vertices. We call such a tree a **spanning tree**. It turns out that every connected graph has one (and usually many).

Spanning tree.

Given a connected graph G, a **spanning tree** of G is a subgraph of G which is a tree and includes all the vertices of G.

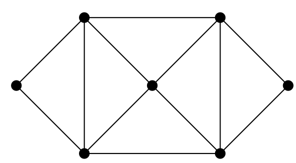
Every connected graph has a spanning tree.

How do we know? We can give an algorithm for *finding* a spanning tree! Start with a connected graph G. If there is no cycle, then G is already a tree and we are done. If there is a cycle, let e be any edge in that cycle and consider the new graph $G_1 = G - e$ (i.e., the graph you get by deleting e). This tree is still connected since e belonged to a cycle, there were at least two paths between its incident vertices. Now repeat: if G_1 has no cycles, we are done, otherwise define G_2 to be $G_1 - e_1$, where e_1 is an edge in a cycle in G_1. Keep going. This process must eventually stop, since there are only a finite number of edges to remove. The result will be a tree, and since we never removed any vertex, a *spanning* tree.

This is by no means the only algorithm for finding a spanning tree. You could have started with the empty graph and added edges that belong to G as long as adding them would not create a cycle. You have some choices as to which edges you add first: you could always add an edge adjacent to edges you have already added (after the first one, of course), or add them using some other order. Which spanning tree you end up with depends on these choices.

Example 4.2.7

Find two different spanning trees of the graph,



Solution. Here are two spanning trees.

Although we will not consider this in detail, these algorithms are usually applied to *weighted* graphs. Here every edge has some weight or cost assigned to it. The goal is to find a spanning tree that has the smallest possible combined weight. Such a tree is called a **minimum spanning tree**. Finding the minimum spanning tree uses basically the same algorithms as we described above, but when picking an edge to add, you always pick the smallest (or when removing an edge, you always remove the largest).[6]

[6] If you add the smallest edge adjacent to edges you have already added, you are doing *Prim's algorithm*. If you add the smallest edge in the entire graph, you are following *Kruskal's algorithm*.

Exercises

1. Which of the following graphs are trees?

   (a) $G = (V, E)$ with $V = \{a, b, c, d, e\}$ and $E = \{\{a, b\}, \{a, e\}, \{b, c\}, \{c, d\}, \{d, e\}\}$

   (b) $G = (V, E)$ with $V = \{a, b, c, d, e\}$ and $E = \{\{a, b\}, \{b, c\}, \{c, d\}, \{d, e\}\}$

   (c) $G = (V, E)$ with $V = \{a, b, c, d, e\}$ and $E = \{\{a, b\}, \{a, c\}, \{a, d\}, \{a, e\}\}$

   (d) $G = (V, E)$ with $V = \{a, b, c, d, e\}$ and $E = \{\{a, b\}, \{a, c\}, \{d, e\}\}$

2. For each degree sequence below, decide whether it must always, must never, or could possibly be a degree sequence for a tree. Remember, a degree sequence lists out the degrees (number of edges incident to the vertex) of all the vertices in a graph in non-increasing order.

   (a) $(4, 1, 1, 1, 1)$

   (b) $(3, 3, 2, 1, 1)$

   (c) $(2, 2, 2, 1, 1)$

   (d) $(4, 4, 3, 3, 3, 2, 2, 1, 1, 1, 1, 1, 1, 1)$

3. For each degree sequence below, decide whether it must always, must never, or could possibly be a degree sequence for a tree. Justify your answers.

   (a) $(3, 3, 2, 2, 2)$

   (b) $(3, 2, 2, 1, 1, 1)$

   (c) $(3, 3, 3, 1, 1, 1)$

   (d) $(4, 4, 1, 1, 1, 1, 1, 1)$

4. Suppose you have a graph with v vertices and e edges that satisfies $v = e + 1$. Must the graph be a tree? Prove your answer.

5. Prove that any graph (not necessarily a tree) with v vertices and e edges that satisfies $v > e + 1$ will NOT be connected.

6. If a graph G with v vertices and e edges is connected and has $v < e + 1$, must it contain a cycle? Prove your answer.

7. We define a **forest** to be a graph with no cycles.

   (a) Explain why this is a good name. That is, explain why a forest is a union of trees.

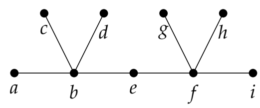
   (b) Suppose F is a forest consisting of m trees and v vertices. How many edges does F have? Explain.

   (c) Prove that any graph G with v vertices and e edges that satisfies $v < e + 1$ must contain a cycle (i.e., not be a forest).

8. Give a careful proof of Corollary 4.2.2: A graph is a forest if and only if there is at most one path between any pair of vertices. Use proof by contrapositive (and not a proof by contradiction) for both directions.

9. Give a careful proof by induction on the number of vertices, that every tree is bipartite.

10. Consider the tree drawn below.



(a) Suppose we designate vertex e as the root. List the children, parents and siblings of each vertex. Does any vertex other than e have grandchildren?

(b) Suppose e is *not* chosen as the root. Does our choice of root vertex change the *number* of children e has? The number of grandchildren? How many are there of each?

(c) In fact, pick any vertex in the tree and suppose it is not the root. Explain why the number of children of that vertex does not depend on which other vertex is the root.

(d) Does the previous part work for other trees? Give an example of a different tree for which it holds. Then either prove that it always holds or give an example of a tree for which it doesn't.

11. Let T be a rooted tree that contains vertices u, v, and w (among possibly others). Prove that if w is a descendant of both u and v, then u is a descendant of v or v is a descendant of u.

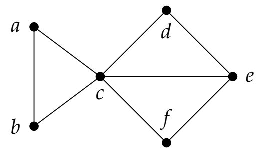
12. Unless it is already a tree, a given graph G will have multiple spanning trees. How similar or different must these be?

(a) Must all spanning trees of a given graph be isomorphic to each other? Explain why or give a counterexample.

(b) Must all spanning trees of a given graph have the same number of edges? Explain why or give a counterexample.

(c) Must all spanning trees of a graph have the same number of leaves (vertices of degree 1)? Explain why or give a counterexample.

13. Find all spanning trees of the graph below. How many different spanning trees are there? How many different spanning trees are there *up to isomorphism* (that is, if you grouped all the spanning trees by which are isomorphic, how many groups would you have)?



14. Give an example of a graph that has exactly 7 different spanning trees. Note, it is acceptable for some or all of these spanning trees to be isomorphic.

15. Prove that every connected graph which is not itself a tree must have at last three different (although possibly isomorphic) spanning trees.

16. Consider edges that must be in every spanning tree of a graph. Must every graph have such an edge? Give an example of a graph that has exactly one such edge.

4.3 Planar Graphs

Investigate!

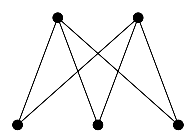
When a connected graph can be drawn without any edges crossing, it is called **planar**. When a planar graph is drawn in this way, it divides the plane into regions called **faces**.

1. Draw, if possible, two different planar graphs with the same number of vertices, edges, and faces.
2. Draw, if possible, two different planar graphs with the same number of vertices and edges, but a different number of faces.

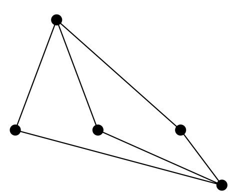
Attempt the above activity before proceeding

When is it possible to draw a graph so that none of the edges cross? If this *is* possible, we say the graph is **planar** (since you can draw it on the *plane*).

Notice that the definition of planar includes the phrase "it is possible to." This means that even if a graph does not look like it is planar, it still might be. Perhaps you can redraw it in a way in which no edges cross. For example, this is a planar graph:



That is because we can redraw it like this:



The graphs are the same, so if one is planar, the other must be too. However, the original drawing of the graph was not a **planar representation** of the graph.

When a planar graph is drawn without edges crossing, the edges and vertices of the graph divide the plane into regions. We will call each region a **face**. The graph above has 3 faces (yes, we *do* include the "outside" region as a face). The number of faces does not change no matter how you draw the graph (as long as you do so without the edges crossing), so it makes sense to ascribe the number of faces as a property of the planar graph.

WARNING: you can only count faces when the graph is drawn in a planar way. For example, consider these two representations of the same graph:

If you try to count faces using the graph on the left, you might say there are 5 faces (including the outside). But drawing the graph with a planar representation shows that in fact there are only 4 faces.

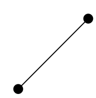
There is a connection between the number of vertices (v), the number of edges (e) and the number of faces (f) in any connected planar graph. This relationship is called Euler's formula.

Euler's Formula for Planar Graphs.

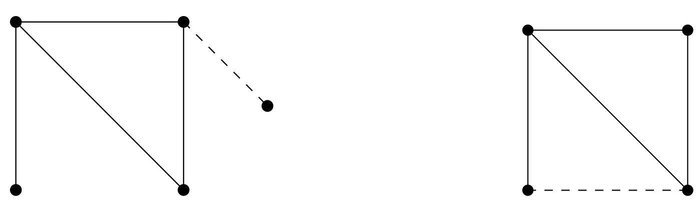
For any connected planar graph with v vertices, e edges and f faces, we have

$$v - e + f = 2.$$

Why is Euler's formula true? One way to convince yourself of its validity is to draw a planar graph step by step. Start with the graph P_2:



Any connected graph (besides just a single isolated vertex) must contain this subgraph. Now build up to your graph by adding edges and vertices. Each step will consist of either adding a new vertex connected by a new edge to part of your graph (so creating a new "spike") or by connecting two vertices already in the graph with a new edge (completing a circuit).



What do these "moves" do? When adding the spike, the number of edges increases by 1, the number of vertices increases by one, and the number of faces remains the same. But this means that $v - e + f$ does not change. Completing a circuit adds one edge, adds one face, and keeps the number of vertices the same. So again, $v - e + f$ does not change.

Since we can build any graph using a combination of these two moves, and doing so never changes the quantity $v - e + f$, that quantity will be the same for all graphs. But notice that our starting graph P_2 has $v = 2$, $e = 1$ and $f = 1$, so $v - e + f = 2$. This argument is essentially a proof by induction. A good exercise would be to rewrite it as a formal induction proof.

Non-planar Graphs

Investigate!

For the complete graphs K_n, we would like to be able to say something about the number of vertices, edges, and (if the graph is planar) faces. Let's first consider K_3:

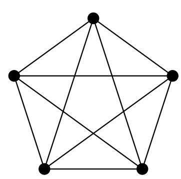
1. How many vertices does K_3 have? How many edges?
2. If K_3 is planar, how many faces should it have?

Repeat parts (1) and (2) for K_4, K_5, and K_{23}.

What about complete bipartite graphs? How many vertices, edges, and faces (if it were planar) does $K_{7,4}$ have? For which values of m and n are K_n and $K_{m,n}$ planar?

Attempt the above activity before proceeding

Not all graphs are planar. If there are too many edges and too few vertices, then some of the edges will need to intersect. The smallest graph where this happens is K_5.



If you try to redraw this without edges crossing, you quickly get into trouble. There seems to be one edge too many. In fact, we can prove that no matter how you draw it, K_5 will always have edges crossing.

Theorem 4.3.1 *K_5 is not planar.*

Proof. The proof is by contradiction. So assume that K_5 is planar. Then the graph must satisfy Euler's formula for planar graphs. K_5 has 5 vertices and 10 edges, so we get

$$5 - 10 + f = 2,$$

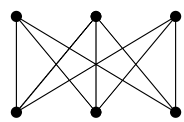
which says that if the graph is drawn without any edges crossing, there would be $f = 7$ faces.

Now consider how many edges surround each face. Each face must be surrounded by at least 3 edges. Let B be the total number of *boundaries* around all the faces in the graph. Thus we have that $3f \leq B$. But also $B = 2e$, since each edge is used as a boundary exactly twice. Putting this together we get

$$3f \leq 2e.$$

But this is impossible, since we have already determined that $f = 7$ and $e = 10$, and $21 \nleq 20$. This is a contradiction so in fact K_5 is not planar. QED

The other simplest graph which is not planar is $K_{3,3}$



Proving that $K_{3,3}$ is not planar answers the houses and utilities puzzle: it is not possible to connect each of three houses to each of three utilities without the lines crossing.

Theorem 4.3.2 $K_{3,3}$ *is not planar.*

Proof. Again, we proceed by contradiction. Suppose $K_{3,3}$ were planar. Then by Euler's formula there will be 5 faces, since $v = 6$, $e = 9$, and $6 - 9 + f = 2$.

How many boundaries surround these 5 faces? Let B be this number. Since each edge is used as a boundary twice, we have $B = 2e$. Also, $B \geq 4f$ since each face is surrounded by 4 or more boundaries. We know this is true because $K_{3,3}$ is bipartite, so does not contain any 3-edge cycles. Thus

$$4f \leq 2e.$$

But this would say that $20 \leq 18$, which is clearly false. Thus $K_{3,3}$ is not planar. QED

Note the similarities and differences in these proofs. Both are proofs by contradiction, and both start with using Euler's formula to derive the (supposed) number of faces in the graph. Then we find a relationship between the number of faces and the number of edges based on how many edges surround each face. This is the only difference. In the proof for K_5, we got $3f \leq 2e$ and for $K_{3,3}$ we go $4f \leq 2e$. The coefficient of f is the key. It is the smallest number of edges which could surround any face. If some number of edges surround a face, then these edges form a cycle. So that number is the size of the smallest cycle in the graph.

In general, if we let g be the size of the smallest cycle in a graph (g stands for *girth*, which is the technical term for this) then for any planar graph we have $gf \leq 2e$. When this disagrees with Euler's formula, we know for sure that the graph cannot be planar.

Polyhedra

Investigate!

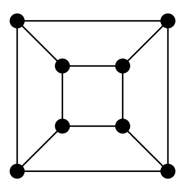
A cube is an example of a convex polyhedron. It contains 6 identical squares for its faces, 8 vertices, and 12 edges. The cube is a **regular polyhedron** (also known as a **Platonic solid**) because each face is an identical regular polygon and each vertex joins an equal number of faces.

There are exactly four other regular polyhedra: the tetrahedron, octahedron, dodecahedron, and icosahedron with 4, 8, 12 and 20 faces respectively. How many vertices and edges do each of these have?

STOP **Attempt the above activity before proceeding** STOP

Another area of mathematics where you might have heard the terms "vertex," "edge," and "face" is geometry. A **polyhedron** is a geometric solid made up of flat polygonal faces joined at edges and vertices. We are especially interested in **convex** polyhedra, which means that any line segment connecting two points on the interior of the polyhedron must be entirely contained inside the polyhedron.[7]

Notice that since $8 - 12 + 6 = 2$, the vertices, edges and faces of a cube satisfy Euler's formula for planar graphs. This is not a coincidence. We can represent a cube as a planar graph by projecting the vertices and edges onto the plane. One such projection looks like this:



In fact, *every* convex polyhedron can be projected onto the plane without edges crossing. Think of placing the polyhedron inside a sphere, with a light at the center of the sphere. The edges and vertices of the polyhedron cast a shadow onto the interior of the sphere. You can then cut a hole in the sphere in the middle of one of the projected faces and "stretch" the

[7]An alternative definition for convex is that the internal angle formed by any two faces must be less than 180 deg.

sphere to lie down flat on the plane. The face that was punctured becomes the "outside" face of the planar graph.

The point is, we can apply what we know about graphs (in particular planar graphs) to convex polyhedra. Since every convex polyhedron can be represented as a planar graph, we see that Euler's formula for planar graphs holds for all convex polyhedra as well. We also can apply the same sort of reasoning we use for graphs in other contexts to convex polyhedra. For example, we know that there is no convex polyhedron with 11 vertices all of degree 3, as this would make $33/2$ edges.

Example 4.3.3

Is there a convex polyhedron consisting of three triangles and six pentagons? What about three triangles, six pentagons and five heptagons (7-sided polygons)?

Solution. How many edges would such polyhedra have? For the first proposed polyhedron, the triangles would contribute a total of 9 edges, and the pentagons would contribute 30. However, this counts each edge twice (as each edge borders exactly two faces), giving $39/2$ edges, an impossibility. There is no such polyhedron.

The second polyhedron does not have this obstacle. The extra 35 edges contributed by the heptagons give a total of $74/2 = 37$ edges. So far so good. Now how many vertices does this supposed polyhedron have? We can use Euler's formula. There are 14 faces, so we have $v - 37 + 14 = 2$ or equivalently $v = 25$. But now use the vertices to count the edges again. Each vertex must have degree *at least* three (that is, each vertex joins at least three faces since the interior angle of all the polygons must be less that $180°$), so the sum of the degrees of vertices is at least 75. Since the sum of the degrees must be exactly twice the number of edges, this says that there are strictly more than 37 edges. Again, there is no such polyhedron.

To conclude this application of planar graphs, consider the regular polyhedra. We claimed there are only five. How do we know this is true? We can prove it using graph theory.

Theorem 4.3.4 *There are exactly five regular polyhedra.*

Proof. Recall that all the faces of a regular polyhedron are identical regular polygons, and that each vertex has the same degree. Consider four cases, depending on the type of regular polygon.

Case 1: Each face is a triangle. Let f be the number of faces. There are then $3f/2$ edges. Using Euler's formula we have $v - 3f/2 + f = 2$ so $v = 2 + f/2$. Now each vertex has the same degree, say k. So the number of edges is also $kv/2$. Putting this together gives

$$e = \frac{3f}{2} = \frac{k(2 + f/2)}{2},$$

which says

$$k = \frac{6f}{4 + f}.$$

Both k and f must be positive integers. Note that $\frac{6f}{4+f}$ is an increasing function for positive f, bounded above by a horizontal asymptote at $k = 6$. Thus the only possible values for k are 3, 4, and 5. Each of these are possible. To get $k = 3$, we need $f = 4$ (this is the tetrahedron). For $k = 4$ we take $f = 8$ (the octahedron). For $k = 5$ take $f = 20$ (the icosahedron). Thus there are exactly three regular polyhedra with triangles for faces.

Case 2: Each face is a square. Now we have $e = 4f/2 = 2f$. Using Euler's formula we get $v = 2 + f$, and counting edges using the degree k of each vertex gives us

$$e = 2f = \frac{k(2 + f)}{2}.$$

Solving for k gives

$$k = \frac{4f}{2 + f} = \frac{8f}{4 + 2f}.$$

This is again an increasing function, but this time the horizontal asymptote is at $k = 4$, so the only possible value that k could take is 3. This produces 6 faces, and we have a cube. There is only one regular polyhedron with square faces.

Case 3: Each face is a pentagon. We perform the same calculation as above, this time getting $e = 5f/2$ so $v = 2 + 3f/2$. Then

$$e = \frac{5f}{2} = \frac{k(2 + 3f/2)}{2},$$

so

$$k = \frac{10f}{4 + 3f}.$$

Now the horizontal asymptote is at $\frac{10}{3}$. This is less than 4, so we can only hope of making $k = 3$. We can do so by using 12 pentagons, getting the dodecahedron. This is the only regular polyhedron with pentagons as faces.

Case 4: Each face is an n-gon with $n \geq 6$. Following the same procedure as above, we deduce that

$$k = \frac{2nf}{4 + (n - 2)f},$$

which will be increasing to a horizontal asymptote of $\frac{2n}{n-2}$. When $n = 6$, this asymptote is at $k = 3$. Any larger value of n will give an even smaller asymptote. Therefore no regular polyhedra exist with faces larger than pentagons.[8] QED

Exercises

1. Is it possible for a planar graph to have 6 vertices, 10 edges and 5 faces? Explain.

2. The graph G has 6 vertices with degrees $2, 2, 3, 4, 4, 5$. How many edges does G have? Could G be planar? If so, how many faces would it have. If not, explain.

3. Is it possible for a connected graph with 7 vertices and 10 edges to be drawn so that no edges cross and create 4 faces? Explain.

4. Is it possible for a graph with 10 vertices and edges to be a connected planar graph? Explain.

5. Is there a connected planar graph with an odd number of faces where every vertex has degree 6? Prove your answer.

6. I'm thinking of a polyhedron containing 12 faces. Seven are triangles and four are quadralaterals. The polyhedron has 11 vertices including those around the mystery face. How many sides does the last face have?

7. Consider some classic polyhedrons.
   (a) An *octahedron* is a regular polyhedron made up of 8 equilateral triangles (it sort of looks like two pyramids with their bases glued together). Draw a planar graph representation of an octahedron. How many vertices, edges and faces does an octahedron (and your graph) have?
   (b) The traditional design of a soccer ball is in fact a (spherical projection of a) truncated icosahedron. This consists of 12 regular pentagons and 20 regular hexagons. No two pentagons are adjacent (so the edges of each pentagon are shared only by hexagons). How many vertices, edges, and faces does a truncated icosahedron have? Explain how you arrived at your answers. Bonus: draw the planar graph representation of the truncated icosahedron.

[8] Notice that you can tile the plane with hexagons. This is an infinite planar graph; each vertex has degree 3. These infinitely many hexagons correspond to the limit as $f \to \infty$ to make $k = 3$.

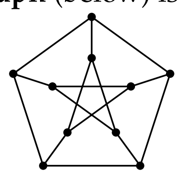
(c) Your "friend" claims that he has constructed a convex polyhedron out of 2 triangles, 2 squares, 6 pentagons and 5 octagons. Prove that your friend is lying. Hint: each vertex of a convex polyhedron must border at least three faces.

8. Prove Euler's formula using induction on the number of edges in the graph.

9. Prove Euler's formula using induction on the number of *vertices* in the graph.

10. Euler's formula ($v - e + f = 2$) holds for all *connected* planar graphs. What if a graph is not connected? Suppose a planar graph has two components. What is the value of $v - e + f$ now? What if it has k components?

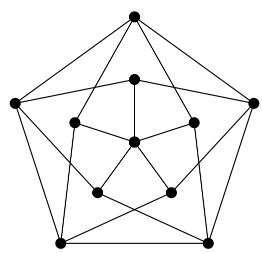
11. Prove that the **Petersen graph** (below) is not planar.



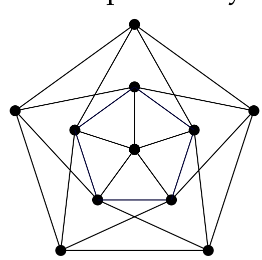
12. Prove that any planar graph with v vertices and e edges satisfies $e \leq 3v - 6$.

13. Prove that any planar graph must have a vertex of degree 5 or less.

14. Give a careful proof that the graph below is not planar.



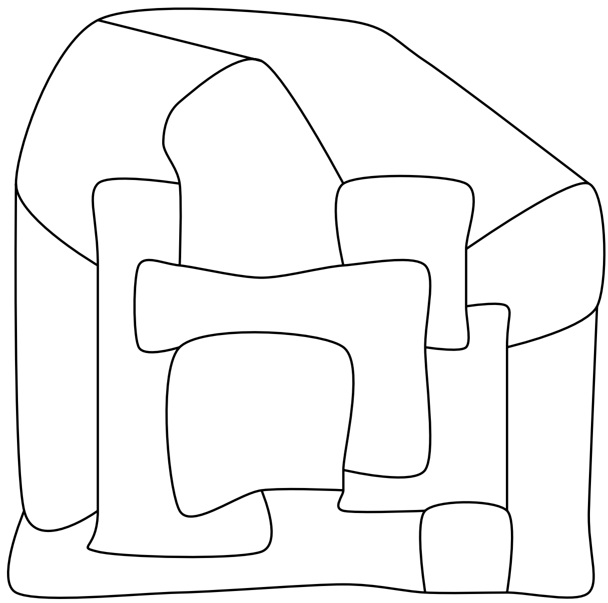
15. Explain why we cannot use the same sort of proof we did in Exercise 4.3.14 to prove that the graph below is not planar. Then explain how you know the graph is not planar anyway.



4.4 Coloring

Investigate!

Mapmakers in the fictional land of Euleria have drawn the borders of the various dukedoms of the land. To make the map pretty, they wish to color each region. Adjacent regions must be colored differently, but it is perfectly fine to color two distant regions with the same color. What is the fewest colors the mapmakers can use and still accomplish this task?



Attempt the above activity before proceeding

Perhaps the most famous graph theory problem is how to color maps.

> Given any map of countries, states, counties, etc., how many colors are needed to color each region on the map so that neighboring regions are colored differently?

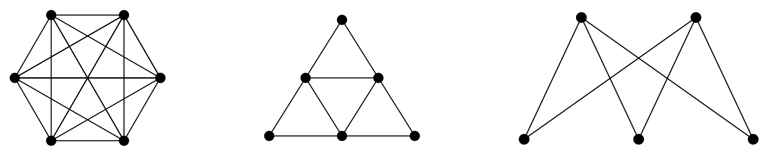
Actual map makers usually use around seven colors. For one thing, they require watery regions to be a specific color, and with a lot of colors it is easier to find a permissible coloring. We want to know whether there is a smaller palette that will work for any map.

How is this related to graph theory? Well, if we place a vertex in the center of each region (say in the capital of each state) and then connect two vertices if their states share a border, we get a graph. Coloring regions on the map corresponds to coloring the vertices of the graph. Since neighboring regions cannot be colored the same, our graph cannot have vertices colored the same when those vertices are adjacent.

In general, given any graph G, a coloring of the vertices is called (not surprisingly) a **vertex coloring**. If the vertex coloring has the property that adjacent vertices are colored differently, then the coloring is called **proper**. Every graph has a proper vertex coloring. For example, you could color every vertex with a different color. But often you can do better. The smallest number of colors needed to get a proper vertex coloring is called the **chromatic number** of the graph, written $\chi(G)$.

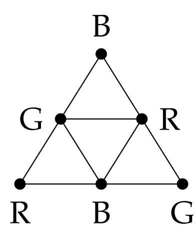
Example 4.4.1

Find the chromatic number of the graphs below.



Solution. The graph on the left is K_6. The only way to properly color the graph is to give every vertex a different color (since every vertex is adjacent to every other vertex). Thus the chromatic number is 6.

The middle graph can be properly colored with just 3 colors (Red, Blue, and Green). For example:



There is no way to color it with just two colors, since there are three vertices mutually adjacent (i.e., a triangle). Thus the chromatic number is 3.

The graph on the right is just $K_{2,3}$. As with all bipartite graphs, this graph has chromatic number 2: color the vertices on the top row red and the vertices on the bottom row blue.

It appears that there is no limit to how large chromatic numbers can get. It should not come as a surprise that K_n has chromatic number n. So how could there possibly be an answer to the original map coloring question? If the chromatic number of graph can be arbitrarily large, then it seems like there would be no upper bound to the number of colors needed for any map. But there is.

The key observation is that while it is true that for any number n, there is a graph with chromatic number n, only some graphs arrive as representations of maps. If you convert a map to a graph, the edges between vertices correspond to borders between the countries. So you should be able to connect vertices in such a way where the edges do not cross. In other words, the graphs representing maps are all *planar*!

So the question is, what is the largest chromatic number of any planar graph? The answer is the best known theorem of graph theory:

Theorem 4.4.2 The Four Color Theorem. *If G is a planar graph, then the chromatic number of G is less than or equal to 4. Thus any map can be properly colored with 4 or fewer colors.*

We will not prove this theorem. Really. Even though the theorem is easy to state and understand, the proof is not. In fact, there is currently no "easy" known proof of the theorem. The current best proof still requires powerful computers to check an *unavoidable set* of 633 *reducible configurations*. The idea is that every graph must contain one of these reducible configurations (this fact also needs to be checked by a computer) and that reducible configurations can, in fact, be colored in 4 or fewer colors.

Coloring in General

Investigate!

The math department plans to offer 10 classes next semester. Some classes cannot run at the same time (perhaps they are taught by the same professor, or are required for seniors).

Class:	Conflicts with:
A	D I
B	D I J
C	E F I
D	A B F
E	C H I
F	C D I
G	J
H	E I J
I	A B C E F H
J	B G H

How many different time slots are needed to teach these classes (and which should be taught at the same time)? More importantly, how could we use graph coloring to answer this question?

Attempt the above activity before proceeding

Cartography is certainly not the only application of graph coloring. There are plenty of situations in which you might wish to partition the objects in question so that related objects are not in the same set. For example, you might wish to store chemicals safely. To avoid explosions, certain pairs of chemicals should not be stored in the same room. By coloring a graph (with vertices representing chemicals and edges representing potential negative interactions), you can determine the smallest number of rooms needed to store the chemicals.

Here is a further example:

Example 4.4.3

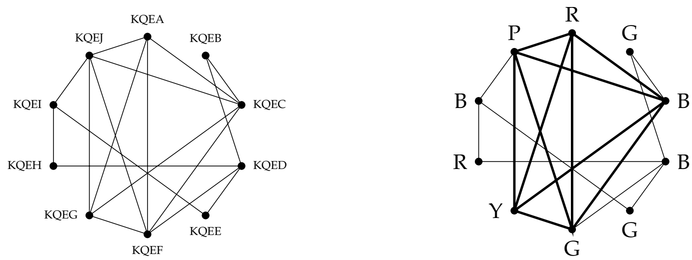
Radio stations broadcast their signal at certain frequencies. However, there are a limited number of frequencies to choose from, so nationwide many stations use the same frequency. This works because the stations are far enough apart that their signals will not interfere; no one radio could pick them up at the same time.

Suppose 10 new radio stations are to be set up in a currently unpopulated (by radio stations) region. The radio stations that are close enough to each other to cause interference are recorded in the table below. What is the fewest number of frequencies the stations could use.

	KQEA	KQEB	KQEC	KQED	KQEE	KQEF	KQEG	KQEH	KQEI	KQEJ
KQEA			X			X	X			X
KQEB			X	X						
KQEC	X					X	X			X
KQED		X			X	X		X		
KQEE				X					X	
KQEF	X		X	X			X			X
KQEG	X		X			X				X
KQEH				X					X	
KQEI					X			X		X
KQEJ	X		X			X	X		X	

Solution. Represent the problem as a graph with vertices as the stations and edges when two stations are close enough to cause interference. We are looking for the chromatic number of the graph. Vertices that are colored identically represent stations that can have the same frequency.

This graph has chromatic number 5. A proper 5-coloring is shown on the right. Notice that the graph contains a copy of the complete graph K_5 so no fewer than 5 colors can be used.



In the example above, the chromatic number was 5, but this is not a counterexample to the Four Color Theorem 4.4.2, since the graph representing the radio stations is not planar. It would be nice to have some quick way to find the chromatic number of a (possibly non-planar) graph. It turns out nobody knows whether an efficient algorithm for computing chromatic numbers exists.

While we might not be able to find the exact chromatic number of graph easily, we can often give a reasonable range for the chromatic number. In other words, we can give upper and lower bounds for chromatic number.

This is actually not very difficult: for every graph G, the chromatic number of G is at least 1 and at most the number of vertices of G.

What? You want *better* bounds on the chromatic number? Well you are in luck.

A **clique** in a graph is a set of vertices all of which are pairwise adjacent. In other words, a clique of size n is just a copy of the complete graph K_n. We define the **clique number** of a graph to be the largest n for which the graph contains a clique of size n. Any clique of size n cannot be colored with fewer than n colors, so we have a nice lower bound:

Theorem 4.4.4 *The chromatic number of a graph G is at least the clique number of G.*

There are times when the chromatic number of G is *equal* to the clique number. These graphs have a special name; they are called **perfect**. If you know that a graph is perfect, then finding the chromatic number is simply a matter of searching for the largest clique.[9] However, not all graphs are perfect.

For an upper bound, we can improve on "the number of vertices" by looking to the degrees of vertices. Let $\Delta(G)$ be the largest degree of any vertex in the graph G. One reasonable guess for an upper bound on the chromatic number is $\chi(G) \leq \Delta(G) + 1$. Why is this reasonable? Starting with any vertex, it together with all of its neighbors can always be colored in $\Delta(G)+1$ colors, since at most we are talking about $\Delta(G)+1$ vertices in this

[9] There are special classes of graphs which can be proved to be perfect. One such class is the set of **chordal** graphs, which have the property that every cycle in the graph contains a **chord**—an edge between two vertices in of the cycle which are not adjacent in the cycle.

set. Now fan out! At any point, if you consider an already colored vertex, some of its neighbors might be colored, some might not. But no matter what, that vertex and its neighbors could all be colored distinctly, since there are at most $\Delta(G)$ neighbors, plus the one vertex being considered.

In fact, there are examples of graphs for which $\chi(G) = \Delta(G) + 1$. For any n, the complete graph K_n has chromatic number n, but $\Delta(K_n) = n - 1$ (since every vertex is adjacent to every *other* vertex). Additionally, any *odd* cycle will have chromatic number 3, but the degree of every vertex in a cycle is 2. It turns out that these are the only two types of examples where we get equality, a result known as Brooks' Theorem.

Theorem 4.4.5 Brooks' Theorem. *Any graph G satisfies $\chi(G) \leq \Delta(G)$, unless G is a complete graph or an odd cycle, in which case $\chi(G) = \Delta(G) + 1$.*

The proof of this theorem is *just* complicated enough that we will not present it here (although you are asked to prove a special case in the exercises). The adventurous reader is encouraged to find a book on graph theory for suggestions on how to prove the theorem.

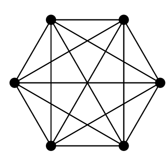
Coloring Edges

The chromatic number of a graph tells us about coloring vertices, but we could also ask about coloring edges. Just like with vertex coloring, we might insist that edges that are adjacent must be colored differently. Here, we are thinking of two edges as being adjacent if they are incident to the same vertex. The least number of colors required to properly color the edges of a graph G is called the **chromatic index** of G, written $\chi'(G)$.

Example 4.4.6

Six friends decide to spend the afternoon playing chess. Everyone will play everyone else once. They have plenty of chess sets but nobody wants to play more than one game at a time. Games will last an hour (thanks to their handy chess clocks). How many hours will the tournament last?

Solution. Represent each player with a vertex and put an edge between two players if they will play each other. In this case, we get the graph K_6:



We must color the edges; each color represents a different hour. Since different edges incident to the same vertex will be colored differently, no player will be playing two different games (edges) at the same time. Thus we need to know the chromatic index of K_6.

Notice that for sure $\chi'(K_6) \geq 5$, since there is a vertex of degree 5. It turns out 5 colors is enough (go find such a coloring). Therefore the friends will play for 5 hours.

Interestingly, if one of the friends in the above example left, the remaining 5 chess-letes would still need 5 hours: the chromatic index of K_5 is also 5.

In general, what can we say about chromatic index? Certainly $\chi'(G) \geq \Delta(G)$. But how much higher could it be? Only a little higher.

Theorem 4.4.7 Vizing's Theorem. *For any graph G, the chromatic index $\chi'(G)$ is either $\Delta(G)$ or $\Delta(G) + 1$.*

At first this theorem makes it seem like chromatic index might not be very interesting. However, deciding which case a graph is in is not always easy. Graphs for which $\chi'(G) = \Delta(G)$ are called *class 1*, while the others are called *class 2*. Bipartite graphs always satisfy $\chi'(G) = \Delta(G)$, so are class 1 (this was proved by König in 1916, decades before Vizing proved his theorem in 1964). In 1965 Vizing proved that all planar graphs with $\Delta(G) \geq 8$ are of class 1, but this does not hold for all planar graphs with $2 \leq \Delta(G) \leq 5$. Vizing conjectured that all planar graphs with $\Delta(G) = 6$ or $\Delta(G) = 7$ are class 1; the $\Delta(G) = 7$ case was proved in 2001 by Sanders and Zhao; the $\Delta(G) = 6$ case is still open.

Ramsey Theory.

There is another interesting way we might consider coloring edges, quite different from what we have discussed so far. What if we colored every edge of a graph either red or blue. Can we do so without, say, creating a *monochromatic* triangle (i.e., an all red or all blue triangle)? Certainly for some graphs the answer is yes. Try doing so for K_4. What about K_5? K_6? How far can we go?

The problem above is not too difficult and is a fun exercise. We could extend the question in a variety of ways. What if we had three colors? What if we were trying to avoid other graphs. Surprisingly, very little is known about these questions. For example, we know that you need to go up to K_{17} in order to force a monochromatic triangle using three colors, but nobody knows how big you need to go with more colors. Similarly, we know that using two colors K_{18} is the smallest graph that forces a monochromatic copy of K_4, but the best we have to force a monochromatic

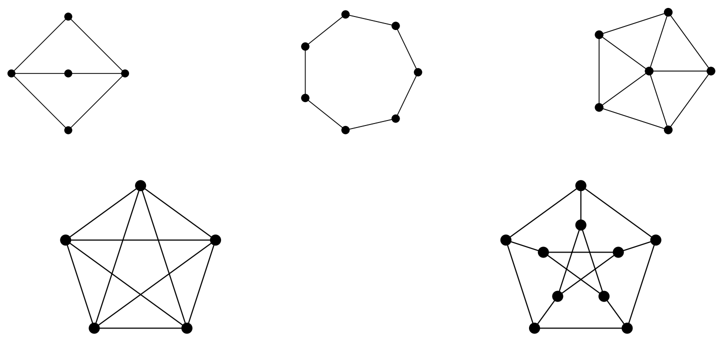
K_5 is a range, somewhere from K_{43} to K_{49}. If you are interested in these sorts of questions, this area of graph theory is called Ramsey theory. Check it out.

Exercises

1. What is the smallest number of colors you need to properly color the vertices of $K_{4,5}$? That is, find the chromatic number of the graph.

2. Draw a graph with chromatic number 6 (i.e., which requires 6 colors to properly color the vertices). Could your graph be planar? Explain.

3. Find the chromatic number of each of the following graphs.



4. A group of 10 friends decides to head up to a cabin in the woods (where nothing could possibly go wrong). Unfortunately, a number of these friends have dated each other in the past, and things are still a little awkward. To get to the cabin, they need to divide up into some number of cars, and no two people who dated should be in the same car.

   (a) What is the smallest number of cars you need if all the relationships were strictly heterosexual? Represent an example of such a situation with a graph. What kind of graph do you get?

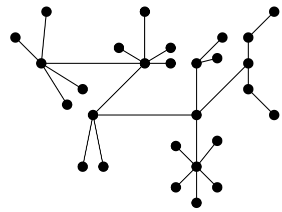
   (b) Because a number of these friends dated there are also conflicts between friends of the same gender, listed below. Now what is the smallest number of conflict-free cars they could take to the cabin?

Friend	A	B	C	D	E	F	G	H	I	J
Conflicts	CFJ	J	AEF	H	CFG	ACEGI	EFI	D	AFG	B

5. What is the smallest number of colors that can be used to color the vertices of a cube so that no two adjacent vertices are colored identically?

6. Prove the chromatic number of any tree is two. Recall, a tree is a connected graph with no cycles.

(a) Describe a procedure to color the tree below.



(b) The chromatic number of C_n is two when n is even. What goes wrong when n is odd?

(c) Prove that your procedure from part (a) always works for any tree.

(d) Now, prove using induction that every tree has chromatic number 2.

7. The two problems below can be solved using graph coloring. For each problem, represent the situation with a graph, say whether you should be coloring vertices or edges and why, and use the coloring to solve the problem.

(a) Your Quidditch league has 5 teams. You will play a tournament next week in which every team will play every other team once. Each team can play at most one match each day, but there is plenty of time in the day for multiple matches. What is the fewest number of days over which the tournament can take place?

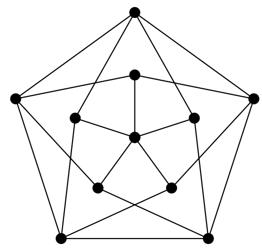
(b) Ten members of Math Club are driving to a math conference in a neighboring state. However, some of these students have dated in the past, and things are still a little awkward. Each student lists which other students they refuse to share a car with; these conflicts are recorded in the table below. What is the fewest number of cars the club needs to make the trip? Do not worry about running out of seats, just avoid the conflicts.

Student	A	B	C	D	E	F	G	H	I	J
Conflicts	BEJ	ADG	HJ	BF	AI	DJ	B	CI	EHJ	ACFI

8. Prove the 6-color theorem: every planar graph has chromatic number 6 or less. Do not assume the 4-color theorem (whose proof is MUCH harder), but you may assume the fact that every planar graph contains a vertex of degree at most 5.

9. Not all graphs are perfect. Give an example of a graph with chromatic number 4 that does not contain a copy of K_4. That is, there should be no 4 vertices all pairwise adjacent.

10. Find the chromatic number of the graph below and prove you are correct.



11. Prove by induction on vertices that any graph G which contains at least one vertex of degree less than $\Delta(G)$ (the maximal degree of all vertices in G) has chromatic number at most $\Delta(G)$.

12. You have a set of magnetic alphabet letters (one of each of the 26 letters in the alphabet) that you need to put into boxes. For obvious reasons, you don't want to put two consecutive letters in the same box. What is the fewest number of boxes you need (assuming the boxes are able to hold as many letters as they need to)?

13. Suppose you colored edges of a graph either red or blue (not requiring that adjacent edges be colored differently). What must be true of the graph to guarantee some vertex is incident to three edges of the same color? Prove your answer.

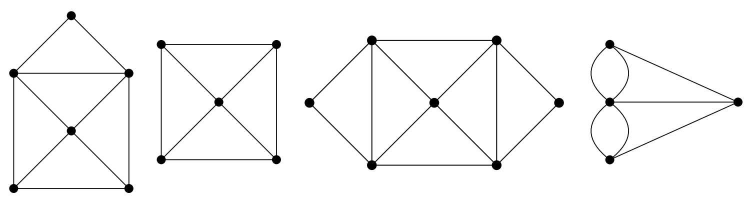
14. Prove that if you color every edge of K_6 either red or blue, you are guaranteed a monochromatic triangle (that is, an all red or an all blue triangle).

4.5 Euler Paths and Circuits

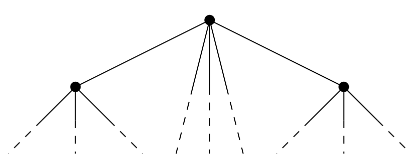
Investigate!

An **Euler path**, in a graph or multigraph, is a walk through the graph which uses every edge exactly once. An **Euler circuit** is an Euler path which starts and stops at the same vertex. Our goal is to find a quick way to check whether a graph (or multigraph) has an Euler path or circuit.

1. Which of the graphs below have Euler paths? Which have Euler circuits?



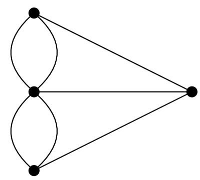
2. List the degrees of each vertex of the graphs above. Is there a connection between degrees and the existence of Euler paths and circuits?
3. Is it possible for a graph with a degree 1 vertex to have an Euler circuit? If so, draw one. If not, explain why not. What about an Euler path?
4. What if every vertex of the graph has degree 2. Is there an Euler path? An Euler circuit? Draw some graphs.
5. Below is *part* of a graph. Even though you can only see some of the vertices, can you deduce whether the graph will have an Euler path or circuit?



Attempt the above activity before proceeding

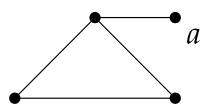
If we start at a vertex and trace along edges to get to other vertices, we create a *walk* through the graph. More precisely, a **walk** in a graph is a sequence of vertices such that every vertex in the sequence is adjacent to the vertices before and after it in the sequence. If the walk travels along every edge exactly once, then the walk is called an **Euler path** (or **Euler walk**). If, in addition, the starting and ending vertices are the same (so you trace along every edge exactly once and end up where you started), then the walk is called an **Euler circuit** (or **Euler tour**). Of course if a graph is not connected, there is no hope of finding such a path or circuit. For the rest of this section, assume all the graphs discussed are connected.

The bridges of Königsberg problem is really a question about the existence of Euler paths. There will be a route that crosses every bridge exactly once if and only if the graph below has an Euler path:



This graph is small enough that we could actually check every possible walk that does not reuse edges, and in doing so convince ourselves that there is no Euler path (let alone an Euler circuit). On small graphs which do have an Euler path, it is usually not difficult to find one. Our goal is to find a quick way to check whether a graph has an Euler path or circuit, even if the graph is quite large.

One way to guarantee that a graph does *not* have an Euler circuit is to include a "spike," a vertex of degree 1.



The vertex a has degree 1, and if you try to make an Euler circuit, you see that you will get stuck at the vertex. It is a dead end. That is, unless you start there. But then there is no way to return, so there is no hope of finding an Euler circuit. There is however an Euler path. It starts at the vertex a, then loops around the triangle. You will end at the vertex of degree 3.

You run into a similar problem whenever you have a vertex of any odd degree. If you start at such a vertex, you will not be able to end there (after traversing every edge exactly once). After using one edge to leave the starting vertex, you will be left with an even number of edges emanating from the vertex. Half of these could be used for returning to the vertex, the other half for leaving. So you return, then leave. Return, then leave. The only way to use up all the edges is to use the last one by leaving the vertex. On the other hand, if you have a vertex with odd degree that you do not start a path at, then you will eventually get stuck at that vertex. The path will use pairs of edges incident to the vertex to arrive and leave again. Eventually all but one of these edges will be used up, leaving only an edge to arrive by, and none to leave again.

What all this says is that if a graph has an Euler path and two vertices with odd degree, then the Euler path must start at one of the odd degree vertices and end at the other. In such a situation, every other vertex *must* have an even degree since we need an equal number of edges to get to those vertices as to leave them. How could we have an Euler circuit? The graph could not have any odd degree vertex as an Euler path would have to start there or end there, but not both. Thus for a graph to have an Euler circuit, all vertices must have even degree.

The converse is also true: if all the vertices of a graph have even degree, then the graph has an Euler circuit, and if there are exactly two vertices with odd degree, the graph has an Euler path. To prove this is a little tricky, but the basic idea is that you will never get stuck because there is an "outbound" edge for every "inbound" edge at every vertex. If you try to make an Euler path and miss some edges, you will always be able to "splice in" a circuit using the edges you previously missed.

Euler Paths and Circuits.

- A graph has an Euler circuit if and only if the degree of every vertex is even.
- A graph has an Euler path if and only if there are at most two vertices with odd degree.

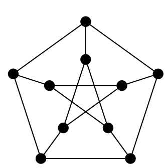
Since the bridges of Königsberg graph has all four vertices with odd degree, there is no Euler path through the graph. Thus there is no way for the townspeople to cross every bridge exactly once.

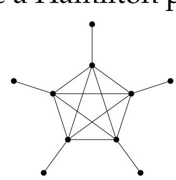
Hamilton Paths

Suppose you wanted to tour Königsberg in such a way that you visit each land mass (the two islands and both banks) exactly once. This can be done. In graph theory terms, we are asking whether there is a path which visits every vertex exactly once. Such a path is called a **Hamilton path** (or **Hamiltonian path**). We could also consider **Hamilton cycles**, which are Hamilton paths which start and stop at the same vertex.

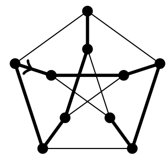
Example 4.5.1

Determine whether the graphs below have a Hamilton path.





Solution. The graph on the left has a Hamilton path (many different ones, actually), as shown here:

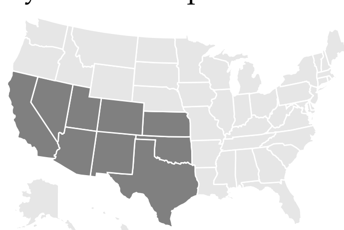


The graph on the right does not have a Hamilton path. You would need to visit each of the "outside" vertices, but as soon as you visit one, you get stuck. Note that this graph does not have an Euler path, although there are graphs with Euler paths but no Hamilton paths.

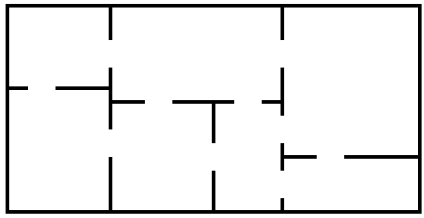
It appears that finding Hamilton paths would be easier because graphs often have more edges than vertices, so there are fewer requirements to be met. However, nobody knows whether this is true. There is no known simple test for whether a graph has a Hamilton path. For small graphs this is not a problem, but as the size of the graph grows, it gets harder and harder to check wither there is a Hamilton path. In fact, this is an example of a question which as far as we know is too difficult for computers to solve; it is an example of a problem which is NP-complete.

Exercises

1. You and your friends want to tour the southwest by car. You will visit the nine states below, with the following rather odd rule: you must cross each border between neighboring states exactly once (so, for example, you must cross the Colorado-Utah border exactly once). Can you do it? If so, does it matter where you start your road trip? What fact about graph theory solves this problem?



2. Which of the following graphs contain an Euler path? Which contain an Euler circuit?
   (a) K_4 (b) K_5. (c) $K_{5,7}$ (d) $K_{2,7}$ (e) C_7 (f) P_7
3. Edward A. Mouse has just finished his brand new house. The floor plan is shown below:



(a) Edward wants to give a tour of his new pad to a lady-mouse-friend. Is it possible for them to walk through every doorway exactly once? If so, in which rooms must they begin and end the tour? Explain.

(b) Is it possible to tour the house visiting each room exactly once (not necessarily using every doorway)? Explain.

(c) After a few mouse-years, Edward decides to remodel. He would like to add some new doors between the rooms he has. Of course, he cannot add any doors to the exterior of the house. Is it possible for each room to have an odd number of doors? Explain.

4. For which n does the graph K_n contain an Euler circuit? Explain.

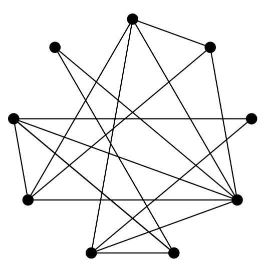
5. For which m and n does the graph $K_{m,n}$ contain an Euler path? An Euler circuit? Explain.

6. For which n does K_n contain a Hamilton path? A Hamilton cycle? Explain.

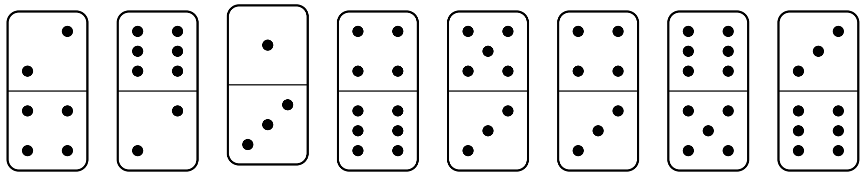
7. For which m and n does the graph $K_{m,n}$ contain a Hamilton path? A Hamilton cycle? Explain.

8. A bridge builder has come to Königsberg and would like to add bridges so that it *is* possible to travel over every bridge exactly once. How many bridges must be built?

9. Below is a graph representing friendships between a group of students (each vertex is a student and each edge is a friendship). Is it possible for the students to sit around a round table in such a way that every student sits between two friends? What does this question have to do with paths?



10. On the table rest 8 dominoes, as shown below. If you were to line them up in a single row, so that any two sides touching had matching numbers, what would the sum of the two end numbers be?

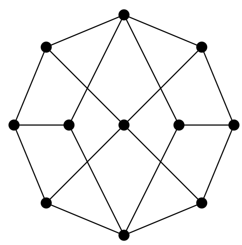


11. Is there anything we can say about whether a graph has a Hamilton path based on the degrees of its vertices?

(a) Suppose a graph has a Hamilton path. What is the maximum number of vertices of degree one the graph can have? Explain why your answer is correct.

(b) Find a graph which does not have a Hamilton path even though no vertex has degree one. Explain why your example works.

12. Consider the following graph:



(a) Find a Hamilton path. Can your path be extended to a Hamilton cycle?

(b) Is the graph bipartite? If so, how many vertices are in each "part"?

(c) Use your answer to part (b) to prove that the graph has no Hamilton cycle.

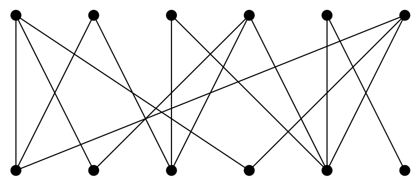
(d) Suppose you have a bipartite graph G in which one part has at least two more vertices than the other. Prove that G does not have a Hamilton path.

4.6 Matching in Bipartite Graphs

Investigate!

Given a bipartite graph, a **matching** is a subset of the edges for which every vertex belongs to exactly one of the edges. Our goal in this activity is to discover some criterion for when a bipartite graph has a matching.

Does the graph below contain a matching? If so, find one.



Not all bipartite graphs have matchings. Draw as many fundamentally different examples of bipartite graphs which do NOT have matchings. Your goal is to find all the possible obstructions to a graph having a perfect matching. Write down the *necessary* conditions for a graph to have a matching (that is, fill in the blank: If a graph has a matching, then ________). Then ask yourself whether these conditions are sufficient (is it true that if ________, then the graph has a matching?).

Attempt the above activity before proceeding

We conclude with one more example of a graph theory problem to illustrate the variety and vastness of the subject.

Suppose you have a bipartite graph G. This will consist of two sets of vertices A and B with some edges connecting some vertices of A to some vertices in B (but of course, no edges between two vertices both in A or both in B). A **matching of** A is a subset of the edges for which each vertex of A belongs to exactly one edge of the subset, and no vertex in B belongs to more than one edge in the subset. In practice we will assume that $|A| = |B|$ (the two sets have the same number of vertices) so this says that every vertex in the graph belongs to exactly one edge in the matching.[10]

Some context might make this easier to understand. Think of the vertices in A as representing students in a class, and the vertices in B as representing presentation topics. We put an edge from a vertex $a \in A$ to a vertex $b \in B$ if student a would like to present on topic b. Of course, some students would want to present on more than one topic, so their vertex

[10]Note: what we are calling a *matching* is sometimes called a *perfect matching* or *complete matching*. This is because in it interesting to look at non-perfect matchings as well. We will call those *partial* matchings.

would have degree greater than 1. As the teacher, you want to assign each student their own unique topic. Thus you want to find a matching of A: you pick some subset of the edges so that each student gets matched up with exactly one topic, and no topic gets matched to two students.[11]

The question is: when does a bipartite graph contain a matching of A? To begin to answer this question, consider what could prevent the graph from containing a matching. This will not necessarily tell us a condition when the graph *does* have a matching, but at least it is a start.

One way G could not have a matching is if there is a vertex in A not adjacent to any vertex in B (so having degree 0). What else? What if two students both like the same one topic, and no others? Then after assigning that one topic to the first student, there is nothing left for the second student to like, so it is very much as if the second student has degree 0. Or what if three students like only two topics between them. Again, after assigning one student a topic, we reduce this down to the previous case of two students liking only one topic. We can continue this way with more and more students.

It should be clear at this point that if there is every a group of n students who as a group like $n - 1$ or fewer topics, then no matching is possible. This is true for any value of n, and any group of n students.

To make this more graph-theoretic, say you have a set $S \subseteq A$ of vertices. Define $N(S)$ to be the set of all the **neighbors** of vertices in S. That is, $N(S)$ contains all the vertices (in B) which are adjacent to at least one of the vertices in S. (In the student/topic graph, $N(S)$ is the set of topics liked by the students of S.) Our discussion above can be summarized as follows:

Matching Condition.

If a bipartite graph $G = \{A, B\}$ has a matching of A, then

$$|N(S)| \geq |S|$$

for all $S \subseteq A$.

Is the converse true? Suppose G satisfies the matching condition $|N(S)| \geq |S|$ for all $S \subseteq A$ (every set of vertices has at least as many neighbors than vertices in the set). Does that mean that there is a matching?

[11]The standard example for matchings used to be the *marriage problem* in which A consisted of the men in the town, B the women, and an edge represented a marriage that was agreeable to both parties. A matching then represented a way for the town elders to marry off everyone in the town, no polygamy allowed. We have chosen a more progressive context for the sake of political correctness.

Surprisingly, yes. The obvious necessary condition is also sufficient.[12] This is a theorem first proved by Philip Hall in 1935.[13]

Theorem 4.6.1 Hall's Marriage Theorem. *Let G be a bipartite graph with sets A and B. Then G has a matching of A if and only if*

$$|N(S)| \geq |S|$$

for all $S \subseteq A$.

There are quite a few different proofs of this theorem – a quick internet search will get you started.

In addition to its application to marriage and student presentation topics, matchings have applications all over the place. We conclude with one such example.

Example 4.6.2

Suppose you deal 52 regular playing cards into 13 piles of 4 cards each. Prove that you can always select one card from each pile to get one of each of the 13 card values Ace, 2, 3, . . . , 10, Jack, Queen, and King.

Solution. Doing this directly would be difficult, but we can use the matching condition to help. Construct a graph G with 13 vertices in the set A, each representing one of the 13 card values, and 13 vertices in the set B, each representing one of the 13 piles. Draw an edge between a vertex $a \in A$ to a vertex $b \in B$ if a card with value a is in the pile b. Notice that we are just looking for a matching of A; each value needs to be found in the piles exactly once.

We will have a matching if the matching condition holds. Given any set of card values (a set $S \subseteq A$) we must show that $|N(S)| \geq |S|$. That is, the number of piles that contain those values is at least the number of different values. But what if it wasn't? Say $|S| = k$. If $|N(S)| < k$, then we would have fewer than $4k$ different cards in those piles (since each pile contains 4 cards). But there are $4k$ cards with the k different values, so at least one of these cards must be in another pile, a contradiction. Thus the matching condition holds, so there is a matching, as required.

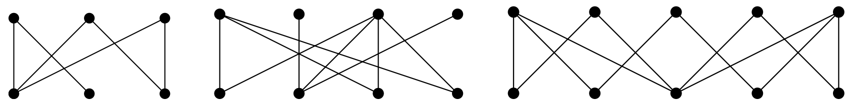
---

[12]This happens often in graph theory. If you can avoid the obvious counterexamples, you often get what you want.

[13]There is also an infinite version of the theorem which was proved by Marshal Hall, Jr. The name is a coincidence though as the two Halls are not related.

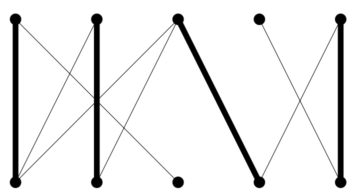
Exercises

1. Find a matching of the bipartite graphs below or explain why no matching exists.



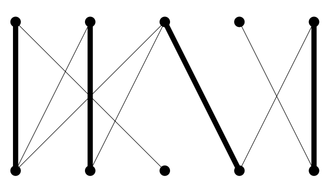
2. A bipartite graph that doesn't have a matching might still have a **partial matching**. By this we mean a set of *edges* for which no vertex belongs to more than one edge (but possibly belongs to none). Every bipartite graph (with at least one edge) has a partial matching, so we can look for the largest partial matching in a graph.

   Your "friend" claims that she has found the largest partial matching for the graph below (her matching is in bold). She explains that no other edge can be added, because all the edges not used in her partial matching are connected to matched vertices. Is she correct?

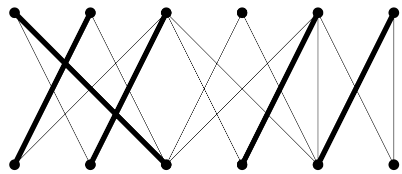


3. One way you might check to see whether a partial matching is maximal is to construct an **alternating path**. This is a sequence of adjacent edges, which alternate between edges in the matching and edges not in the matching (no edge can be used more than once). If an alternating path starts and stops with an edge *not* in the matching, then it is called an **augmenting path**.

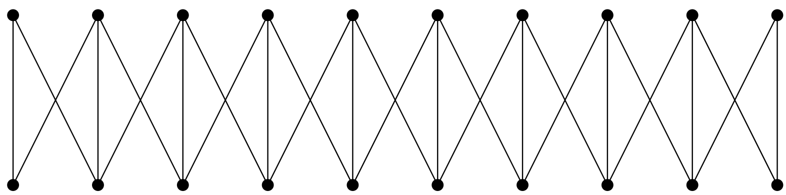
   (a) Find the largest possible alternating path for the partial matching of your friend's graph. Is it an augmenting path? How would this help you find a larger matching?



   (b) Find the largest possible alternating path for the partial matching below. Are there any augmenting paths? Is the partial matching the largest one that exists in the graph?



4. The two richest families in Westeros have decided to enter into an alliance by marriage. The first family has 10 sons, the second has 10 girls. The ages of the kids in the two families match up. To avoid impropriety, the families insist that each child must marry someone either their own age, or someone one position younger or older. In fact, the graph representing agreeable marriages looks like this:



The question: how many different acceptable marriage arrangements which marry off all 20 children are possible?

(a) How many marriage arrangements are possible if we insist that there are exactly 6 boys marry girls not their own age?

(b) Could you generalize the previous answer to arrive at the total number of marriage arrangements?

(c) How do you know you are correct? Try counting in a different way. Look at smaller family sizes and get a sequence.

(d) Can you give a recurrence relation that fits the problem?

5. We say that a set of vertices $A \subseteq V$ is a **vertex cover** if every edge of the graph is incident to a vertex in the cover (so a vertex cover covers the *edges*). Since V itself is a vertex cover, every graph has a vertex cover. The interesting question is about finding a **minimal** vertex cover, one that uses the fewest possible number of vertices.

(a) Suppose you had a matching of a graph. How can you use that to get a minimal vertex cover? Will your method always work?

(b) Suppose you had a minimal vertex cover for a graph. How can you use that to get a partial matching? Will your method always work?

(c) What is the relationship between the size of the minimal vertex cover and the size of the maximal partial matching in a graph?

6. For many applications of matchings, it makes sense to use bipartite graphs. You might wonder, however, whether there is a way to find matchings in graphs in general.

(a) For which n does the complete graph K_n have a matching?

(b) Prove that if a graph has a matching, then $|V|$ is even.

(c) Is the converse true? That is, do all graphs with $|V|$ even have a matching?

(d) What if we also require the matching condition? Prove or disprove: If a graph with an even number of vertices satisfies $|N(S)| \geq |S|$ for all $S \subseteq V$, then the graph has a matching.

4.7 Chapter Summary

Hopefully this chapter has given you some sense for the wide variety of graph theory topics as well as why these studies are interesting. There are many more interesting areas to consider and the list is increasing all the time; graph theory is an active area of mathematical research.

One reason graph theory is such a rich area of study is that it deals with such a fundamental concept: any pair of objects can either be related or not related. What the objects are and what "related" means varies on context, and this leads to many applications of graph theory to science and other areas of math. The objects can be countries, and two countries can be related if they share a border. The objects could be land masses which are related if there is a bridge between them. The objects could be websites which are related if there is a link from one to the other. Or we can be completely abstract: the objects are vertices which are related if their is an edge between them.

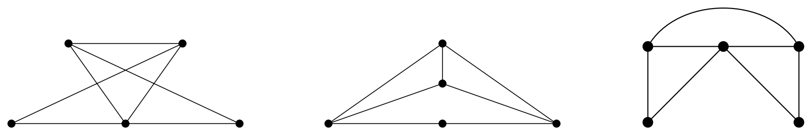
What question we ask about the graph depends on the application, but often leads to deeper, general and abstract questions worth studying in their own right. Here is a short summary of the types of questions we have considered:

- Can the graph be drawn in the plane without edges crossing? If so, how many regions does this drawing divide the plane into?
- Is it possible to color the vertices of the graph so that related vertices have different colors using a small number of colors? How many colors are needed?
- Is it possible to trace over every edge of a graph exactly once without lifting up your pencil? What other sorts of "paths" might a graph posses?
- Can you find subgraphs with certain properties? For example, when does a (bipartite) graph contain a subgraph in which all vertices are only related to one other vertex?

Not surprisingly, these questions are often related to each other. For example, the chromatic number of a graph cannot be greater than 4 when the graph is planar. Whether the graph has an Euler path depends on how many vertices each vertex is adjacent to (and whether those numbers are always even or not). Even the existence of matchings in bipartite graphs can be proved using paths.

Chapter Review

1. Which (if any) of the graphs below are the same? Which are different? Explain.



2. Which of the graphs in the previous question contain Euler paths or circuits? Which of the graphs are planar?

3. Draw a graph which has an Euler circuit but is not planar.

4. Draw a graph which does not have an Euler path and is also not planar.

5. Consider the graph $G = (V, E)$ with $V = \{a, b, c, d, e, f, g\}$ and $E = \{ab, ac, af, bg, cd, ce\}$ (here we are using the shorthand for edges: ab really means $\{a, b\}$, for example).

   (a) Is the graph G isomorphic to $G' = (V', E')$ with $V' = \{t, u, v, w, x, y, z\}$ and $E' = \{tz, uv, uy, uz, vw, vx\}$? If so, give the isomoprhism. If not, explain how you know.

   (b) Find a graph G'' with 7 vertices and 6 edges which is NOT isomorphic to G, or explain why this is not possible.

   (c) Write down the *degree sequence* for G. That is, write down the degrees of all the vertices, in decreasing order.

   (d) Find a connected graph G''' with the same degree sequence of G which is NOT isomorphic to G, or explain why this is not possible.

   (e) What kind of graph is G? Is G complete? Bipartite? A tree? A cycle? A path? A wheel?

   (f) Is G planar?

   (g) What is the chromatic number of G? Explain.

   (h) Does G have an Euler path or circuit? Explain.

6. If a graph has 10 vertices and 10 edges and contains an Euler circuit, must it be planar? How many faces would it have?

7. Suppose G is a graph with n vertices, each having degree 5.

   (a) For which values of n does this make sense?

(b) For which values of n does the graph have an Euler path?

(c) What is the smallest value of n for which the graph might be planar? (tricky)

8. At a school dance, 6 girls and 4 boys take turns dancing (as couples) with each other.

(a) How many couples danced if every girl dances with every boy?

(b) How many couples danced if everyone danced with everyone else (regardless of gender)?

(c) Explain what graphs can be used to represent these situations.

9. Among a group of n people, is it possible for everyone to be friends with an odd number of people in the group? If so, what can you say about n?

10. Your friend has challenged you to create a convex polyhedron containing 9 triangles and 6 pentagons.

(a) Is it possible to build such a polyhedron using *only* these shapes? Explain.

(b) You decide to also include one heptagon (seven-sided polygon). How many vertices does your new convex polyhedron contain?

(c) Assuming you are successful in building your new 16-faced polyhedron, could every vertex be the joining of the same number of faces? Could each vertex join either 3 or 4 faces? If so, how many of each type of vertex would there be?

11. Is there a convex polyhedron which requires 5 colors to properly color the vertices of the polyhedron? Explain.

12. How many edges does the graph $K_{n,n}$ have? For which values of n does the graph contain an Euler circuit? For which values of n is the graph planar?

13. The graph G has 6 vertices with degrees $1, 2, 2, 3, 3, 5$. How many edges does G have? If G was planar how many faces would it have? Does G have an Euler path?

14. What is the smallest number of colors you need to properly color the vertices of K_7. Can you say whether K_7 is planar based on your answer?

15. What is the smallest number of colors you need to properly color the vertices of $K_{3,4}$? Can you say whether $K_{3,4}$ is planar based on your answer?

16. Prove that $K_{3,4}$ is not planar. Do this using Euler's formula, not just by appealing to the fact that $K_{3,3}$ is not planar.

17. A dodecahedron is a regular convex polyhedron made up of 12 regular pentagons.

(a) Suppose you color each pentagon with one of three colors. Prove that there must be two adjacent pentagons colored identically.

(b) What if you use four colors?

(c) What if instead of a dodecahedron you colored the faces of a cube?

18. Decide whether the following statements are true or false. Prove your answers.

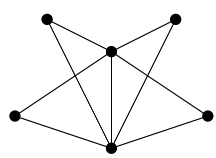
(a) If two graph G_1 and G_2 have the same chromatic number, then they are isomorphic.

(b) If two graphs G_1 and G_2 have the same number of vertices and edges and have the same chromatic number, then they are isomorphic.

(c) If two graphs are isomorphic, then they have the same chromatic number.

19. If a planar graph G with 7 vertices divides the plane into 8 regions, how many edges must G have?

20. Consider the graph below:



(a) Does the graph have an Euler path or circuit? Explain.

(b) Is the graph planar? Explain.

(c) Is the graph bipartite? Complete? Complete bipartite?

(d) What is the chromatic number of the graph.

21. For each part below, say whether the statement is true or false. Explain why the true statements are true, and give counterexamples for the false statements.

(a) Every bipartite graph is planar.

(b) Every bipartite graph has chromatic number 2.

(c) Every bipartite graph has an Euler path.

(d) Every vertex of a bipartite graph has even degree.

(e) A graph is bipartite if and only if the sum of the degrees of all the vertices is even.

22. Consider the statement "If a graph is planar, then it has an Euler path."

(a) Write the converse of the statement.

(b) Write the contrapositive of the statement.

(c) Write the negation of the statement.

(d) Is it possible for the contrapositive to be false? If it was, what would that tell you?

(e) Is the original statement true or false? Prove your answer.

(f) Is the converse of the statement true or false? Prove your answer.

23. Let G be a connected graph with v vertices and e edges. Use mathematical induction to prove that if G contains exactly one cycle (among other edges and vertices), then $v = e$.

Note: this is asking you to prove a special case of Euler's formula for planar graphs, so do not use that formula in your proof.

Chapter 5

Additional Topics

5.1 Generating Functions

There is an extremely powerful tool in discrete mathematics used to manipulate sequences called the generating function. The idea is this: instead of an infinite sequence (for example: $2, 3, 5, 8, 12, \ldots$) we look at a single function which encodes the sequence. But not a function which gives the nth term as output. Instead, a function whose power series (like from calculus) "displays" the terms of the sequence. So for example, we would look at the power series $2+3x+5x^2+8x^3+12x^4+\cdots$ which displays the sequence $2, 3, 5, 8, 12, \ldots$ as coefficients.

An infinite power series is simply an infinite sum of terms of the form $c_n x^n$ were c_n is some constant. So we might write a power series like this:

$$\sum_{k=0}^{\infty} c_k x^k.$$

or expanded like this

$$c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4 + c_5 x^5 + \cdots.$$

When viewed in the context of generating functions, we call such a power series a *generating series*. The generating series generates the sequence

$$c_0, c_1, c_2, c_3, c_4, c_5, \ldots.$$

In other words, the sequence generated by a generating series is simply the sequence of *coefficients* of the infinite polynomial.

Example 5.1.1

What sequence is represented by the generating series $3+8x^2+x^3+\frac{x^5}{7}+100x^6+\cdots$?

Solution. We just read off the coefficients of each x^n term. So $a_0 = 3$ since the coefficient of x^0 is 3 ($x^0 = 1$ so this is the constant term). What is a_1? It is NOT 8, since 8 is the coefficient of x^2, so 8 is the term a_2 of the sequence. To find a_1 we need to look for the coefficient of x^1 which in this case is 0. So $a_1 = 0$. Continuing, we have $a_2 = 8$,

$a_3 = 1$, $a_4 = 0$, and $a_5 = \frac{1}{7}$. So we have the sequence

$$3, 0, 8, 1, 0, \frac{1}{7}, 100, \ldots.$$

Note that when discussing generating functions, we always start our sequence with a_0.

Now you might very naturally ask why we would do such a thing. One reason is that encoding a sequence with a power series helps us keep track of which term is which in the sequence. For example, if we write the sequence $1, 3, 4, 6, 9, \ldots, 24, 41, \ldots$ it is impossible to determine which term 24 is (even if we agreed that the first term was supposed to be a_0). However, if we wrote the generating series instead, we would have $1 + 3x + 4x^2 + 6x^3 + 9x^4 + \cdots + 24x^{17} + 41x^{18} + \cdots$. Now it is clear that 24 is the 17th term of the sequence (that is, $a_{17} = 24$). Of course to get this benefit we could have displayed our sequence in any number of ways, perhaps $\boxed{1}_0 \boxed{3}_1 \boxed{4}_2 \boxed{6}_3 \boxed{9}_4 \cdots \boxed{24}_{17} \boxed{41}_{18} \cdots$, but we do not do this. The reason is that the generating series looks like an ordinary power series (although we are interpreting it differently) so we can do things with it that we ordinarily do with power series such as write down what it converges to.

For example, from calculus we know that the power series $1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \cdots + \frac{x^n}{n!} + \cdots$ converges to the function e^x. So we can use e^x as a way of talking about the sequence of coefficients of the power series for e^x. When we write down a nice compact function which has an infinite power series that we view as a generating series, then we call that function a *generating function*. In this example, we would say

$$1, 1, \frac{1}{2}, \frac{1}{6}, \frac{1}{24}, \ldots, \frac{1}{n!}, \ldots \text{ has generating function } e^x.$$

Building Generating Functions

The e^x example is very specific. We have a rather odd sequence, and the only reason we know its generating function is because we happen to know the Taylor series for e^x. Our goal now is to gather some tools to build the generating function of a particular given sequence.

Let's see what the generating functions are for some very simple sequences. The simplest of all: $1, 1, 1, 1, 1, \ldots$. What does the *generating series* look like? It is simply $1 + x + x^2 + x^3 + x^4 + \cdots$. Now, can we find a closed formula for this power series? Yes! This particular series is really just a geometric series with common ratio x. So if we use our "multiply, shift and subtract" technique from Section 2.2, we have

$$\begin{array}{rl} S &= 1 + x + x^2 + x^3 + \cdots \\ - \quad xS &= \quad\; x + x^2 + x^3 + x^4 + \cdots \\ \hline (1-x)S &= 1 \end{array}$$

Therefore we see that

$$1 + x + x^2 + x^3 \cdots = \frac{1}{1-x}.$$

You might remember from calculus that this is only true on the interval of convergence for the power series, in this case when $|x| < 1$. That is true for us, but we don't care. We are never going to plug anything in for x, so as long as there is some value of x for which the generating function and generating series agree, we are happy. And in this case we are happy.

$1, 1, 1, \ldots$.

The generating function for $1, 1, 1, 1, 1, 1, \ldots$ is $\dfrac{1}{1-x}$

Let's use this basic generating function to find generating functions for more sequences. What if we replace x by $-x$. We get

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + \cdots \text{ which generates } 1, -1, 1, -1, \ldots.$$

If we replace x by $3x$ we get

$$\frac{1}{1-3x} = 1 + 3x + 9x^2 + 27x^3 + \cdots \text{ which generates } 1, 3, 9, 27, \ldots.$$

By replacing the x in $\frac{1}{1-x}$ we can get generating functions for a variety of sequences, but not all. For example, you cannot plug in anything for x to get the generating function for $2, 2, 2, 2, \ldots$. However, we are not lost yet. Notice that each term of $2, 2, 2, 2, \ldots$ is the result of multiplying the terms of $1, 1, 1, 1, \ldots$ by the constant 2. So multiply the generating function by 2 as well.

$$\frac{2}{1-x} = 2 + 2x + 2x^2 + 2x^3 + \cdots \text{ which generates } 2, 2, 2, 2, \ldots.$$

Similarly, to find the generating function for the sequence $3, 9, 27, 81, \ldots$, we note that this sequence is the result of multiplying each term of $1, 3, 9, 27, \ldots$ by 3. Since we have the generating function for $1, 3, 9, 27, \ldots$ we can say

$$\frac{3}{1-3x} = 3 \cdot 1 + 3 \cdot 3x + 3 \cdot 9x^2 + 3 \cdot 27x^3 + \cdots \text{ which generates } 3, 9, 27, 81, \ldots.$$

What about the sequence $2, 4, 10, 28, 82, \ldots$? Here the terms are always 1 more than powers of 3. That is, we have added the sequences $1, 1, 1, 1, \ldots$ and $1, 3, 9, 27, \ldots$ term by term. Therefore we can get a generating function by adding the respective generating functions:

$$\begin{aligned} 2 + 4x + 10x^2 + 28x^3 + \cdots &= (1+1) + (1+3)x + (1+9)x^2 + (1+27)x^3 + \cdots \\ &= 1 + x + x^2 + x^3 + \cdots + 1 + 3x + 9x^2 + 27x^3 + \cdots \\ &= \frac{1}{1-x} + \frac{1}{1-3x} \end{aligned}$$

The fun does not stop there: if we replace x in our original generating function by x^2 we get

$$\frac{1}{1-x^2} = 1 + x^2 + x^4 + x^6 \cdots \text{ which generates } 1, 0, 1, 0, 1, 0, \ldots.$$

How could we get $0, 1, 0, 1, 0, 1, \ldots$? Start with the previous sequence and *shift* it over by 1. But how do you do this? To see how shifting works, let's first try to get the generating function for the sequence $0, 1, 3, 9, 27, \ldots$. We know that $\frac{1}{1-3x} = 1 + 3x + 9x^2 + 27x^3 + \cdots$. To get the zero out front, we need the generating series to look like $x + 3x^2 + 9x^3 + 27x^4 + \cdots$ (so there is no constant term). Multiplying by x has this effect. So the generating function for $0, 1, 3, 9, 27, \ldots$ is $\frac{x}{1-3x}$. This will also work to get the generating function for $0, 1, 0, 1, 0, 1, \ldots$:

$$\frac{x}{1-x^2} = x + x^3 + x^5 + \cdots \text{ which generates } 0, 1, 0, 1, 0, 1 \ldots.$$

What if we add the sequences $1, 0, 1, 0, 1, 0, \ldots$ and $0, 1, 0, 1, 0, 1, \ldots$ term by term? We should get $1, 1, 1, 1, 1, 1 \ldots$. What happens when we add the generating functions? It works (try it)!

$$\frac{1}{1-x^2} + \frac{x}{1-x^2} = \frac{1}{1-x}.$$

Here's a sneaky one: what happens if you take the *derivative* of $\frac{1}{1-x}$? We get $\frac{1}{(1-x)^2}$. On the other hand, if we differentiate term by term in the power series, we get $(1 + x + x^2 + x^3 + \cdots)' = 1 + 2x + 3x^2 + 4x^3 + \cdots$ which is the generating series for $1, 2, 3, 4, \ldots$. This says

$1, 2, 3, \ldots$.

The generating function for $1, 2, 3, 4, 5, \ldots$ is $\dfrac{1}{(1-x)^2}$.

Take a second derivative: $\frac{2}{(1-x)^3} = 2 + 6x + 12x^2 + 20x^3 + \cdots$. So $\frac{1}{(1-x)^3} = 1 + 3x + 6x^2 + 10x^3 + \cdots$ is a generating function for the triangular numbers, $1, 3, 6, 10\ldots$ (although here we have $a_0 = 1$ while $T_0 = 0$ usually).

Differencing

We have seen how to find generating functions from $\frac{1}{1-x}$ using multiplication (by a constant or by x), substitution, addition, and differentiation. To use each of these, you must notice a way to transform the sequence $1, 1, 1, 1, 1\ldots$ into your desired sequence. This is not always easy. It is also not really the way we have analyzed sequences. One thing we have considered often is the sequence of differences between terms of a sequence. This will turn out to be helpful in finding generating functions as well. The sequence of differences is often simpler than the original sequence. So if we know a generating function for the differences, we would like to use this to find a generating function for the original sequence.

For example, consider the sequence $2, 4, 10, 28, 82, \ldots$. How could we move to the sequence of first differences: $2, 6, 18, 54, \ldots$? We want to subtract 2 from the 4, 4 from the 10, 10 from the 28, and so on. So if we subtract (term by term) the sequence $0, 2, 4, 10, 28, \ldots$ from $2, 4, 10, 28\ldots$, we will be set. We can get the generating function for $0, 2, 4, 10, 28, \ldots$ from the generating function for $2, 4, 10, 28\ldots$ by multiplying by x. Use A to represent the generating function for $2, 4, 10, 28, 82, \ldots$ Then:

$$\begin{array}{rl} A &= 2 + 4x + 10x^2 + 28x^3 + 82x^4 + \cdots \\ - \quad xA &= 0 + 2x + 4x^2 + 10x^3 + 28x^4 + 82x^5 + \cdots \\ \hline (1-x)A &= 2 + 2x + 6x^2 + 18x^3 + 54x^4 + \cdots \end{array}$$

While we don't get exactly the sequence of differences, we do get something close. In this particular case, we already know the generating function A (we found it in the previous section) but most of the time we will use this differencing technique to *find* A: if we have the generating function for the sequence of differences, we can then solve for A.

Example 5.1.2

Find a generating function for $1, 3, 5, 7, 9, \ldots$.

Solution. Notice that the sequence of differences is constant. We know how to find the generating function for any constant sequence. So denote the generating function for $1, 3, 5, 7, 9, \ldots$ by A. We have

$$\begin{array}{rl} A &= 1 + 3x + 5x^2 + 7x^3 + 9x^4 + \cdots \\ - \quad xA &= 0 + x + 3x^2 + 5x^3 + 7x^4 + 9x^5 + \cdots \\ \hline (1-x)A &= 1 + 2x + 2x^2 + 2x^3 + 2x^4 + \cdots \end{array}$$

We know that $2x + 2x^2 + 2x^3 + 2x^4 + \cdots = \frac{2x}{1-x}$. Thus

$$(1-x)A = 1 + \frac{2x}{1-x}.$$

Now solve for A:

$$A = \frac{1}{1-x} + \frac{2x}{(1-x)^2} = \frac{1+x}{(1-x)^2}.$$

Does this makes sense? Before we simplified the two fractions into one, we were adding the generating function for the sequence $1, 1, 1, 1, \ldots$ to the generating function for the sequence $0, 2, 4, 6, 8, 10, \ldots$ (remember $\frac{1}{(1-x)^2}$ generates $1, 2, 3, 4, 5, \ldots$, multiplying by $2x$ shifts it over, putting the zero out front, and doubles each term). If we add these term by term, we get the correct sequence $1, 3, 5, 7, 9, \ldots$.

Now that we have a generating function for the odd numbers, we can use that to find the generating function for the squares:

Example 5.1.3

Find the generating function for $1, 4, 9, 16, \ldots$. Note we take $1 = a_0$.

Solution. Again we call the generating function for the sequence A. Using differencing:

$$\begin{array}{rl} A &= 1 + 4x + 9x^2 + 16x^3 + \cdots \\ - \quad xA &= 0 + x + 4x^2 + 9x^3 + 16x^4 + \cdots \\ \hline (1-x)A &= 1 + 3x + 5x^2 + 7x^3 + \cdots \end{array}$$

Since $1 + 3x + 5x^2 + 7x^3 + \cdots = \frac{1+x}{(1-x)^2}$ we have $A = \frac{1+x}{(1-x)^3}$.

In each of the examples above, we found the difference between consecutive terms which gave us a sequence of differences for which we knew a generating function. We can generalize this to more complicated relationships between terms of the sequence. For example, if we know that the sequence satisfies the recurrence relation $a_n = 3a_{n-1} - 2a_{n-2}$? In other words, if we take a term of the sequence and subtract 3 times the previous term and then add 2 times the term before that, we get 0 (since $a_n - 3a_{n-1} + 2a_{n-2} = 0$). That will hold for all but the first two terms of the sequence. So after the first two terms, the sequence of results of these calculations would be a sequence of 0's, for which we definitely know a generating function.

Example 5.1.4

The sequence $1, 3, 7, 15, 31, 63, \ldots$ satisfies the recurrence relation $a_n = 3a_{n-1} - 2a_{n-2}$. Find the generating function for the sequence.

Solution. Call the generating function for the sequence A. We have

$$\begin{aligned} A &= 1 + 3x + 7x^2 + 15x^3 + 31x^4 + \cdots + a_n x^n + \cdots \\ -3xA &= 0 - 3x - 9x^2 - 21x^3 - 45x^4 - \cdots - 3a_{n-1}x^n - \cdots \\ +\ \ 2x^2A &= 0 + 0x + 2x^2 + 6x^3 + 14x^4 + \cdots + 2a_{n-2}x^n + \cdots \\ \hline (1 - 3x + 2x^2)A &= 1 \end{aligned}$$

We multiplied A by $-3x$ which shifts every term over one spot and multiplies them by -3. On the third line, we multiplied A by $2x^2$, which shifted every term over two spots and multiplied them by 2. When we add up the corresponding terms, we are taking each term, subtracting 3 times the previous term, and adding 2 times the term before that. This will happen for each term after a_1 because $a_n - 3a_{n-1} + 2a_{n-2} = 0$. In general, we might have two terms from the beginning of the generating series, although in this case the second term happens to be 0 as well.

Now we just need to solve for A:

$$A = \frac{1}{1 - 3x + 2x^2}.$$

Multiplication and Partial Sums

What happens to the sequences when you multiply two generating functions? Let's see: $A = a_0 + a_1 x + a_2 x^2 + \cdots$ and $B = b_0 + b_1 x + b_2 x^2 + \cdots$. To multiply A and B, we need to do a lot of distributing (infinite FOIL?) but keep in mind we will group like terms and only need to write down the first few terms to see the pattern. The constant term is $a_0 b_0$. The coefficient of x is $a_0 b_1 + a_1 b_0$. And so on. We get:

$$AB = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)x^3 + \cdots.$$

Example 5.1.5

"Multiply" the sequence $1, 2, 3, 4, \ldots$ by the sequence $1, 2, 4, 8, 16, \ldots$.

Solution. The new constant term is just $1 \cdot 1$. The next term will be $1 \cdot 2 + 2 \cdot 1 = 4$. The next term: $1 \cdot 4 + 2 \cdot 2 + 3 \cdot 1 = 11$. One more: $1 \cdot 8 + 2 \cdot 4 + 3 \cdot 2 + 4 \cdot 1 = 26$. The resulting sequence is

$$1, 4, 11, 26, 57, \ldots.$$

Since the generating function for $1, 2, 3, 4, \ldots$ is $\frac{1}{(1-x)^2}$ and the generating function for $1, 2, 4, 8, 16, \ldots$ is $\frac{1}{1-2x}$, we have that the generating function for $1, 4, 11, 26, 57, \ldots$ is $\frac{1}{(1-x)^2(1-2x)}$

Consider the special case when you multiply a sequence by $1, 1, 1, \ldots$. For example, multiply $1, 1, 1, \ldots$ by $1, 2, 3, 4, 5 \ldots$. The first term is $1 \cdot 1 = 1$. Then $1 \cdot 2 + 1 \cdot 1 = 3$. Then $1 \cdot 3 + 1 \cdot 2 + 1 \cdot 1 = 6$. The next term will be 10. We are getting the triangular numbers. More precisely, we get the sequence of partial sums of $1, 2, 3, 4, 5, \ldots$. In terms of generating functions, we take $\frac{1}{1-x}$ (generating $1, 1, 1, 1, 1 \ldots$) and multiply it by $\frac{1}{(1-x)^2}$ (generating $1, 2, 3, 4, 5, \ldots$) and this give $\frac{1}{(1-x)^3}$. This should not be a surprise as we found the same generating function for the triangular numbers earlier.

The point is, if you need to find a generating function for the sum of the first n terms of a particular sequence, and you know the generating function for *that* sequence, you can multiply it by $\frac{1}{1-x}$. To go back from the sequence of partial sums to the original sequence, you look at the sequence of differences. When you get the sequence of differences you end up multiplying by $1 - x$, or equivalently, dividing by $\frac{1}{1-x}$. Multiplying by $\frac{1}{1-x}$ gives partial sums, dividing by $\frac{1}{1-x}$ gives differences.

Solving Recurrence Relations with Generating Functions

We conclude with an example of one of the many reasons studying generating functions is helpful. We can use generating functions to solve recurrence relations.

Example 5.1.6

Solve the recurrence relation $a_n = 3a_{n-1} - 2a_{n-2}$ with initial conditions $a_0 = 1$ and $a_1 = 3$.

Solution. We saw in an example above that this recurrence relation gives the sequence $1, 3, 7, 15, 31, 63, \ldots$ which has generating function $\dfrac{1}{1 - 3x + 2x^2}$. We did this by calling the generating function A

and then computing $A - 3xA + 2x^2A$ which was just 1, since every other term canceled out.

But how does knowing the generating function help us? First, break up the generating function into two simpler ones. For this, we can use partial fraction decomposition. Start by factoring the denominator:

$$\frac{1}{1-3x+2x^2} = \frac{1}{(1-x)(1-2x)}.$$

Partial fraction decomposition tells us that we can write this faction as the sum of two fractions (we decompose the given fraction):

$$\frac{1}{(1-x)(1-2x)} = \frac{a}{1-x} + \frac{b}{1-2x} \quad \text{for some constants } a \text{ and } b.$$

To find a and b we add the two decomposed fractions using a common denominator. This gives

$$\frac{1}{(1-x)(1-2x)} = \frac{a(1-2x)+b(1-x)}{(1-x)(1-2x)}.$$

so

$$1 = a(1-2x) + b(1-x).$$

This must be true for all values of x. If $x = 1$, then the equation becomes $1 = -a$ so $a = -1$. When $x = \frac{1}{2}$ we get $1 = b/2$ so $b = 2$. This tells us that we can decompose the fraction like this:

$$\frac{1}{(1-x)(1-2x)} = \frac{-1}{1-x} + \frac{2}{1-2x}.$$

This completes the partial fraction decomposition. Notice that these two fractions are generating functions we know. In fact, we should be able to expand each of them.

$$\frac{-1}{1-x} = -1-x-x^2-x^3-x^4-\cdots \text{ which generates } -1,-1,-1,-1,-1,\ldots.$$

$$\frac{2}{1-2x} = 2+4x+8x^2+16x^3+32x^4+\cdots \text{ which generates } 2,4,8,16,32,\ldots.$$

We can give a closed formula for the nth term of each of these sequences. The first is just $a_n = -1$. The second is $a_n = 2^{n+1}$. The sequence we are interested in is just the sum of these, so the solution to the recurrence relation is

$$a_n = 2^{n+1} - 1.$$

We can now add generating functions to our list of methods for solving recurrence relations.

Exercises

1. Find the generating function for each of the following sequences by relating them back to a sequence with known generating function.
   (a) $4, 4, 4, 4, 4, \ldots$.
   (b) $2, 4, 6, 8, 10, \ldots$.
   (c) $0, 0, 0, 2, 4, 6, 8, 10, \ldots$.
   (d) $1, 5, 25, 125, \ldots$.
   (e) $1, -3, 9, -27, 81, \ldots$.
   (f) $1, 0, 5, 0, 25, 0, 125, 0, \ldots$.
   (g) $0, 1, 0, 0, 2, 0, 0, 3, 0, 0, 4, 0, 0, 5, \ldots$.
2. Find the sequence generated by the following generating functions:
   (a) $\dfrac{4x}{1-x}$.
   (b) $\dfrac{1}{1-4x}$.
   (c) $\dfrac{x}{1+x}$.
   (d) $\dfrac{3x}{(1+x)^2}$.
   (e) $\dfrac{1+x+x^2}{(1-x)^2}$ (Hint: multiplication).
3. Show how you can get the generating function for the triangular numbers in three different ways:
   (a) Take two derivatives of the generating function for $1, 1, 1, 1, 1, \ldots$
   (b) Use differencing.
   (c) Multiply two known generating functions.
4. Use differencing to find the generating function for $4, 5, 7, 10, 14, 19, 25, \ldots$.
5. Find a generating function for the sequence with recurrence relation $a_n = 3a_{n-1} - a_{n-2}$ with initial terms $a_0 = 1$ and $a_1 = 5$.
6. Use the recurrence relation for the Fibonacci numbers to find the generating function for the Fibonacci sequence.

7. Use multiplication to find the generating function for the sequence of partial sums of Fibonacci numbers, $S_0, S_1, S_2, \ldots$ where $S_0 = F_0$, $S_1 = F_0 + F_1$, $S_2 = F_0 + F_1 + F_2$, $S_3 = F_0 + F_1 + F_2 + F_3$ and so on.

8. Find the generating function for the sequence with closed formula $a_n = 2(5^n) + 7(-3)^n$.

9. Find a closed formula for the nth term of the sequence with generating function $\dfrac{3x}{1-4x} + \dfrac{1}{1-x}$.

10. Find a_7 for the sequence with generating function $\dfrac{2}{(1-x)^2} \cdot \dfrac{x}{1-x-x^2}$.

11. Explain how we know that $\dfrac{1}{(1-x)^2}$ is the generating function for $1, 2, 3, 4, \ldots$.

12. Starting with the generating function for $1, 2, 3, 4, \ldots$, find a generating function for each of the following sequences.

(a) $1, 0, 2, 0, 3, 0, 4, \ldots$.

(b) $1, -2, 3, -4, 5, -6, \ldots$.

(c) $0, 3, 6, 9, 12, 15, 18, \ldots$.

(d) $0, 3, 9, 18, 30, 45, 63, \ldots$. (Hint: relate this sequence to the previous one.)

13. You may assume that $1, 1, 2, 3, 5, 8, \ldots$ has generating function $\dfrac{1}{1-x-x^2}$ (because it does). Use this fact to find the sequence generated by each of the following generating functions.

(a) $\frac{x^2}{1-x-x^2}$.

(b) $\frac{1}{1-x^2-x^4}$.

(c) $\frac{1}{1-3x-9x^2}$.

(d) $\frac{1}{(1-x-x^2)(1-x)}$.

14. Find the generating function for the sequence $1, -2, 4, -8, 16, \ldots$.

15. Find the generating function for the sequence $1, 1, 1, 2, 3, 4, 5, 6, \ldots$.

16. Suppose A is the generating function for the sequence $3, 5, 9, 15, 23, 33, \ldots$.

(a) Find a generating function (in terms of A) for the sequence of differences between terms.

(b) Write the sequence of differences between terms and find a generating function for it (without referencing A).

(c) Use your answers to parts (a) and (b) to find the generating function for the original sequence.

5.2 Introduction to Number Theory

We have used the natural numbers to solve problems. This was the right set of numbers to work with in discrete mathematics because we always dealt with a whole number of things. The natural numbers have been a tool. Let's take a moment now to inspect that tool. What mathematical discoveries can we make *about* the natural numbers themselves?

This is the main question of number theory: a huge, ancient, complex, and above all, beautiful branch of mathematics. Historically, number theory was known as the Queen of Mathematics and was very much a branch of *pure* mathematics, studied for its own sake instead of as a means to understanding real world applications. This has changed in recent years however, as applications of number theory have been unearthed. Probably the most well known example of this is RSA cryptography, one of the methods used in encrypt data on the internet. It is number theory that makes this possible.

What sorts of questions belong to the realm of number theory? Here is a motivating example. Recall in our study of induction, we asked:

> Which amounts of postage can be made exactly using just 5-cent and 8-cent stamps?

We were able to prove that *any* amount greater than 27 cents could be made. You might wonder what would happen if we changed the denomination of the stamps. What if we instead had 4- and 9-cent stamps? Would there be some amount after which all amounts would be possible? Well, again, we could replace two 4-cent stamps with a 9-cent stamp, or three 9-cent stamps with seven 4-cent stamps. In each case we can create one more cent of postage. Using this as the inductive case would allow us to prove that any amount of postage greater than 23 cents can be made.

What if we had 2-cent and 4-cent stamps. Here it looks less promising. If we take some number of 2-cent stamps and some number of 4-cent stamps, what can we say about the total? Could it ever be odd? Doesn't look like it.

Why does 5 and 8 work, 4 and 9 work, but 2 and 4 not work? What is it about these numbers? If I gave you a pair of numbers, could you tell me right away if they would work or not? We will answer these questions, and more, after first investigating some simpler properties of numbers themselves.

Divisibility

It is easy to add and multiply natural numbers. If we extend our focus to all integers, then subtraction is also easy (we need the negative numbers so we can subtract any number from any other number, even larger from smaller). Division is the first operation that presents a challenge. If we wanted to extend our set of numbers so any division would be possible (maybe excluding division by 0) we would need to look at the rational numbers (the set of all numbers which can be written as fractions). This would be going too far, so we will refuse this option.

In fact, it is a good thing that not every number can be divided by other numbers. This helps us understand the structure of the natural numbers and opens the door to many interesting questions and applications.

If given numbers a and b, it is possible that $a \div b$ gives a whole number. In this case, we say that b *divides* a, in symbols, we write $b \mid a$. If this holds, then b is a divisor or factor of a, and a is a multiple of b. In other words, if $b \mid a$, then $a = bk$ for some integer k (this is saying a is some multiple of b).

The Divisibility Relation.

Given integers m and n, we say "m divides n" and write

$$m \mid n$$

provided $n \div m$ is an integer. Thus the following assertions mean the same thing:

1. $m \mid n$
2. $n = mk$ for some integer k
3. m is a factor (or divisor) of n
4. n is a multiple of m.

Notice that $m \mid n$ is a statement. It is either true or false. On the other hand, $n \div m$ or n/m is some number. If we want to claim that n/m is not an integer, so m does not divide n, then we can write $m \nmid n$.

Example 5.2.1

Decide whether each of the statements below are true or false.

1. $4 \mid 20$
2. $20 \mid 4$
3. $0 \mid 5$
4. $5 \mid 0$
5. $7 \mid 7$
6. $1 \mid 37$
7. $-3 \mid 12$
8. $8 \mid 12$
9. $1642 \mid 136299$

Solution.

1. True. 4 "goes into" 20 five times without remainder. In other words, $20 \div 4 = 5$, an integer. We could also justify this by saying that 20 is a multiple of 4: $20 = 4 \cdot 5$.
2. False. While 20 is a multiple of 4, it is false that 4 is a multiple of 20.
3. False. $5 \div 0$ is not even defined, let alone an integer.
4. True. In fact, $x \mid 0$ is true for all x. This is because 0 is a multiple of every number: $0 = x \cdot 0$.
5. True. In fact, $x \mid x$ is true for all x.
6. True. 1 divides every number (other than 0).
7. True. Negative numbers work just fine for the divisibility relation. Here $12 = -3 \cdot 4$. It is also true that $3 \mid -12$ and that $-3 \mid -12$.
8. False. Both 8 and 12 are divisible by 4, but this does not mean that 12 is divisible by 8.
9. False. See below.

This last example raises a question: how might one decide whether $m \mid n$? Of course, if you had a trusted calculator, you could ask it for the value of $n \div m$. If it spits out anything other than an integer, you know $m \nmid n$. This seems a little like cheating though: we don't have division, so should we really use division to check divisibility?

While we don't really know how to divide, we do know how to multiply. We might try multiplying m by larger and larger numbers until we get close to n. How close? Well, we want to be sure that if we multiply m by the next larger integer, we go over n.

For example, let's try this to decide whether $1642 \mid 136299$. Start finding multiples of 1642:

$$1642 \cdot 2 = 3284 \qquad 1642 \cdot 3 = 4926 \qquad 1642 \cdot 4 = 6568 \qquad \cdots.$$

All of these are well less than 136299. I suppose we can jump ahead a bit:

$$1642 \cdot 50 = 82100 \qquad 1642 \cdot 80 = 131360 \qquad 1642 \cdot 85 = 139570.$$

Ah, so we need to look somewhere between 80 and 85. Try 83:

$$1642 \cdot 83 = 136286.$$

Is this the best we can do? How far are we from our desired 136299? If we subtract, we get $136299 - 136286 = 13$. So we know we cannot go up to

84, that will be too much. In other words, we have found that

$$136299 = 83 \cdot 1642 + 13.$$

Since $13 < 1642$, we can now safely say that $1642 \nmid 136299$.

It turns out that the process we went through above can be repeated for any pair of numbers. We can always write the number a as some multiple of the number b plus some remainder. We know this because we know about **division with remainder** from elementary school. This is just a way of saying it using multiplication. Due to the procedural nature that can be used to find the remainder, this fact is usually called the **division algorithm**:

The Division Algorithm.

Given any two integers a and b, we can always find an integer q such that

$$a = qb + r$$

where r is an integer satisfying $0 \leq r < |b|$

The idea is that we can always take a large enough multiple of b so that the remainder r is as small as possible. We do allow the possibility of $r = 0$, in which case we have $b \mid a$.

Remainder Classes

The division algorithm tells us that there are only b possible remainders when dividing by b. If we fix this divisor, we can group integers by the remainder. Each group is called a **remainder class modulo b** (or sometimes **residue class**).

Example 5.2.2

Describe the remainder classes modulo 5.

Solution. We want to classify numbers by what their remainder would be when divided by 5. From the division algorithm, we know there will be exactly 5 remainder classes, because there are only 5 choices for what r could be ($0 \leq r < 5$).

First consider $r = 0$. Here we are looking for all the numbers divisible by 5 since $a = 5q + 0$. In other words, the multiples of 5. We get the infinite set

$$\{\ldots, -15, -10, -5, 0, 5, 10, 15, 20, \ldots\}.$$

Notice we also include negative integers.

Next consider $r = 1$. Which integers, when divided by 5, have remainder 1? Well, certainly 1, does, as does 6, and 11. Negatives? Here we must be careful: -6 does NOT have remainder 1. We can write $-6 = -2 \cdot 5 + 4$ or $-6 = -1 \cdot 5 - 1$, but only one of these is a "correct" instance of the division algorithm: $r = 4$ since we need r to be non-negative. So in fact, to get $r = 1$, we would have -4, or -9, etc. Thus we get the remainder class

$$\{\ldots, -14, -9, -4, 1, 6, 11, 16, 21, \ldots\}.$$

There are three more to go. The remainder classes for 2, 3, and 4 are, respectively

$$\{\ldots, -13, -8, -3, 2, 7, 12, 17, 22, \ldots\}$$

$$\{\ldots, -12, -7, -2, 3, 8, 13, 18, 23, \ldots\}$$

$$\{\ldots, -11, -6, -1, 4, 9, 14, 19, 24, \ldots\}.$$

Note that in the example above, *every* integer is in exactly one remainder class. The technical way to say this is that the remainder classes modulo b form a **partition** of the integers.[1] The most important fact about partitions, is that it is possible to define an **equivalence relation** from a partition: this is a relationship between pairs of numbers which acts in all the important ways like the "equals" relationship.[2]

All fun technical language aside, the idea is really simple. If two numbers belong to the same remainder class, then in some way, they are the same. That is, they are the same *up to division by b*. In the case where $b = 5$ above, the numbers 8 and 23, while not the same number, are the same when it comes to dividing by 5, because both have remainder 3.

It matters what the divisor is: 8 and 23 are the same up to division by 5, but not up to division by 7, since 8 has remainder of 1 when divided by 7 while 23 has a remainder of 2.

With all this in mind, let's introduce some notation. We want to say that 8 and 23 are basically the same, even though they are not equal. It would be wrong to say $8 = 23$. Instead, we write $8 \equiv 23$. But this is not always true. It works if we are thinking division by 5, so we need to denote that somehow. What we will actually write is this:

$$8 \equiv 23 \pmod{5}$$

[1] It is possible to develop a mathematical theory of partitions, prove statements about all partitions in general and then apply those observations to our case here.

[2] Again, there is a mathematical theory of equivalence relations which applies in many more instances than the one we look at here.

which is read, "8 is congruent to 23 modulo 5" (or just "mod 5"). Of course then we could observe that

$$8 \not\equiv 23 \pmod{7}.$$

Congruence Modulo n.

We say a **is congruent to** b **modulo** n, and write,

$$a \equiv b \pmod{n}$$

provided a and b have the same remainder when divided by n. In other words, provided a and b belong to the same remainder class modulo n.

Many books define congruence modulo n slightly differently. They say that $a \equiv b \pmod{n}$ if and only if $n \mid a - b$. In other words, two numbers are congruent modulo n, if their difference is a multiple of n. So which definition is correct? Turns out, it doesn't matter: they are equivalent.

To see why, consider two numbers a and b which are congruent modulo n. Then a and b have the same remainder when divided by n. We have

$$a = q_1 n + r \qquad\qquad b = q_2 n + r.$$

Here the two r's really are the same. Consider what we get when we take the difference of a and b:

$$a - b = q_1 n + r - (q_2 n + r) = q_1 n - q_2 n = (q_1 - q_2)n.$$

So $a - b$ is a multiple of n, or equivalently, $n \mid a - b$.

On the other hand, if we assume first that $n \mid a - b$, so $a - b = kn$, then consider what happens if we divide each term by n. Dividing a by n will leave some remainder, as will dividing b by n. However, dividing kn by n will leave 0 remainder. So the remainders on the left-hand side must cancel out. That is, the remainders must be the same.

Thus we have:

Congruence and Divisibility.

For any integers a, b, and n, we have

$$a \equiv b \pmod{n} \qquad \text{if and only if} \qquad n \mid a - b.$$

It will also be useful to switch back and forth between congruences and regular equations. The above fact helps with this. We know that $a \equiv b \pmod{n}$ if and only if $n \mid a - b$, if and only if $a - b = kn$ for some integer k. Rearranging that equation, we get $a = b + kn$. In other words, if a and b

are congruent modulo n, then a is b more than some multiple of n. This conforms with our earlier observation that all the numbers in a particular remainder class are the same amount larger than the multiples of n.

Congruence and Equality.

For any integers a, b, and n, we have

$$a \equiv b \pmod{n} \qquad \text{if and only if} \qquad a = b + kn \text{ for some integer } k.$$

Properties of Congruence

We said earlier that congruence modulo n behaves, in many important ways, the same way equality does. Specifically, we could prove that congruence modulo n is an **equivalence relation**, which would require checking the following three facts:

Congruence Modulo n is an Equivalence Relation.

Given any integers a, b, and c, and any positive integer n, the following hold:

1. $a \equiv a \pmod{n}$.
2. If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.
3. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

In other words, congruence modulo n is reflexive, symmetric, and transitive, so is an equivalence relation.

You should take a minute to convince yourself that each of the properties above actually hold of congruence. Try explaining each using both the remainder and divisibility definitions.

Next, consider how congruence behaves when doing basic arithmetic. We already know that if you subtract two congruent numbers, the result will be congruent to 0 (be a multiple of n). What if we add something congruent to 1 to something congruent to 2? Will we get something congruent to 3?

Congruence and Arithmetic.

Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then the following hold:

1. $a + c \equiv b + d \pmod{n}$.
2. $a - c \equiv b - d \pmod{n}$.

3. $ac \equiv bd \pmod{n}$.

The above facts might be written a little strangely, but the idea is simple. If we have a true congruence, and we add the same thing to both sides, the result is still a true congruence. This sounds like we are saying:

If $a \equiv b \pmod{n}$ then $a + c \equiv b + c \pmod{n}$.

Of course this is true as well, it is the special case where $c = d$. But what we have works in more generality. Think of congruence as being "basically equal." If we have two numbers which are basically equal, and we add basically the same thing to both sides, the result will be basically equal.

This seems reasonable. Is it really true? Let's prove the first fact:

Proof. Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. That means $a = b + kn$ and $c = d + jn$ for integers k and j. Add these equations:

$$a + c = b + d + kn + jn.$$

But $kn + jn = (k + j)n$, which is just a multiple of n. So $a + c = b + d + (j + k)n$, or in other words, $a + c \equiv b + d \pmod{n}$ QED

The other two facts can be proved in a similar way.

One of the important consequences of these facts about congruences, is that we can basically replace any number in a congruence with any other number it is congruent to. Here are some examples to see how (and why) that works:

Example 5.2.3

Find the remainder of 3491 divided by 9.

Solution. We could do long division, but there is another way. We want to find x such that $x \equiv 3491 \pmod{9}$. Now $3491 = 3000 + 400 + 90 + 1$. Of course $90 \equiv 0 \pmod{9}$, so we can replace the 90 in the sum with 0. Why is this okay? We are actually subtracting the "same" thing from both sides:

$$\begin{aligned} x &\equiv 3000 + 400 + 90 + 1 \pmod{9} \\ - \quad 0 &\equiv 90 \pmod{9} \\ x &\equiv 3000 + 400 + 0 + 1 \pmod{9}. \end{aligned}$$

Next, note that $400 = 4 \cdot 100$, and $100 \equiv 1 \pmod{9}$ (since $9 \mid 99$). So we can in fact replace the 400 with simply a 4. Again, we are appealing to our claim that we can replace congruent elements, but we are really appealing to property 3 about the arithmetic of congruence: we know $100 \equiv 1 \pmod{9}$, so if we multiply both sides by 4, we get $400 \equiv 4 \pmod{9}$.

Similarly, we can replace 3000 with 3, since $1000 = 1 + 999 \equiv 1 \pmod{9}$. So our original congruence becomes

$$x \equiv 3 + 4 + 0 + 1 \pmod{9}$$

$$x \equiv 8 \pmod{9}.$$

Therefore 3491 divided by 9 has remainder 8.

The above example should convince you that the well known divisibility test for 9 is true: the sum of the digits of a number is divisible by 9 if and only if the original number is divisible by 9. In fact, we now know something more: any number is congruent to the sum of its digits, modulo 9.[3]

Let's try another:

Example 5.2.4

Find the remainder when 3^{123} is divided by 7.

Solution. Of course, we are working with congruence because we want to find the smallest positive x such that $x \equiv 3^{123} \pmod{7}$. Now first write $3^{123} = (3^3)^{41}$. We have:

$$3^{123} = 27^{41} \equiv 6^{41} \pmod{7},$$

since $27 \equiv 6 \pmod{7}$. Notice further that $6^2 = 36$ is congruent to 1 modulo 7. Thus we can simplify further:

$$6^{41} = 6 \cdot (6^2)^{20} \equiv 6 \cdot 1^{20} \pmod{7}.$$

But $1^{20} = 1$, so we are done:

$$3^{123} \equiv 6 \pmod{7}.$$

In the above example, we are using the fact that if $a \equiv b \pmod{n}$, then $a^p \equiv b^p \pmod{n}$. This is just applying property 3 a bunch of times.

So far we have seen how to add, subtract and multiply with congruences. What about division? There is a reason we have waited to discuss it. It turns out that we cannot simply divide. In other words, even if $ad \equiv bd$

[3]This works for 3 as well, but definitely not for any modulus in general.

$\pmod{n}$, we do not know that $a \equiv b \pmod{n}$. Consider, for example:

$$18 \equiv 42 \pmod{8}.$$

This is true. Now 18 and 42 are both divisible by 6. However,

$$3 \not\equiv 7 \pmod{8}.$$

While this doesn't work, note that $3 \equiv 7 \pmod{4}$. We cannot divide 8 by 6, but we can divide 8 by the greatest common factor of 8 and 6. Will this always happen?

Suppose $ad \equiv bd \pmod{n}$. In other words, we have $ad = bd + kn$ for some integer k. Of course ad is divisible by d, as is bd. So kn must also be divisible by d. Now if n and d have no common factors (other than 1), then we must have $d \mid k$. But in general, if we try to divide kn by d, we don't know that we will get an integer multiple of n. Some of the n might get divided as well. To be safe, let's divide as much of n as we can. Take the largest factor of both d and n, and cancel that out from n. The rest of the factors of d will come from k, no problem.

We will call the largest factor of both d and n the $\gcd(d,n)$, for *greatest common divisor*. In our example above, $\gcd(6,8) = 2$ since the greatest divisor common to 6 and 8 is 2.

Congruence and Division.

Suppose $ad \equiv bd \pmod{n}$. Then $a \equiv b \pmod{\frac{n}{\gcd(d,n)}}$.

If d and n have no common factors then $\gcd(d,n) = 1$, so $a \equiv b \pmod{n}$.

Example 5.2.5

Simplify the following congruences using division: (a) $24 \equiv 39 \pmod{5}$ and (b) $24 \equiv 39 \pmod{15}$.

Solution. (a) Both 24 and 39 are divisible by 3, and 3 and 5 have no common factors, so we get

$$8 \equiv 13 \pmod{5}.$$

(b) Again, we can divide by 3. However, doing so blindly gives us $8 \equiv 13 \pmod{15}$ which is no longer true. Instead, we must also divide the modulus 15 by the greatest common factor of 3 and 15, which is 3. Again we get

$$8 \equiv 13 \pmod{5}.$$

Solving Congruences

Now that we have some algebraic rules to govern congruence relations, we can attempt to solve for an unknown in a congruence. For example, is there a value of x that satisfies,

$$3x + 2 \equiv 4 \pmod{5},$$

and if so, what is it?

In this example, since the modulus is small, we could simply try every possible value for x. There are really only 5 to consider, since any integer that satisfied the congruence could be replaced with any other integer it was congruent to modulo 5. Here, when $x = 4$ we get $3x + 2 = 14$ which is indeed congruent to 4 modulo 5. This means that $x = 9$ and $x = 14$ and $x = 19$ and so on will each also be a solution because as we saw above, replacing any number in a congruence with a congruent number does not change the truth of the congruence.

So in this example, simply compute $3x+2$ for values of $x \in \{0, 1, 2, 3, 4\}$. This gives 2, 5, 8, 11, and 14 respectively, for which only 14 is congruent to 4.

Let's also see how you could solve this using our rules for the algebra of congruences. Such an approach would be much simpler than the trial and error tactic if the modulus was larger. First, we know we can subtract 2 from both sides:

$$3x \equiv 2 \pmod{5}.$$

Then to divide both sides by 3, we first add 0 to both sides. Of course, on the right-hand side, we want that 0 to be a 10 (yes, 10 really is 0 since they are congruent modulo 5). This gives,

$$3x \equiv 12 \pmod{5}.$$

Now divide both sides by 3. Since $\gcd(3, 5) = 1$, we do not need to change the modulus:

$$x \equiv 4 \pmod{5}.$$

Notice that this in fact gives the *general solution*: not only can $x = 4$, but x can be any number which is congruent to 4. We can leave it like this, or write "$x = 4 + 5k$ for any integer k."

Example 5.2.6

Solve the following congruences for x.

1. $7x \equiv 12 \pmod{13}$.
2. $84x - 38 \equiv 79 \pmod{15}$.

3. $20x \equiv 23 \pmod{14}$.

Solution.

1. All we need to do here is divide both sides by 7. We add 13 to the right-hand side repeatedly until we get a multiple of 7 (adding 13 is the same as adding 0, so this is legal). We get 25, 38, 51, 64, 77 – got it. So we have:

$$\begin{aligned} 7x &\equiv 12 \pmod{13} \\ 7x &\equiv 77 \pmod{13} \\ x &\equiv 11 \pmod{13}. \end{aligned}$$

2. Here, since we have numbers larger than the modulus, we can reduce them prior to applying any algebra. We have $84 \equiv 9$, $38 \equiv 8$ and $79 \equiv 4$. Thus,

$$\begin{aligned} 84x - 38 &\equiv 79 \pmod{15} \\ 9x - 8 &\equiv 4 \pmod{15} \\ 9x &\equiv 12 \pmod{15} \\ 9x &\equiv 72 \pmod{15}. \end{aligned}$$

We got the 72 by adding $0 \equiv 60 \pmod{15}$ to both sides of the congruence. Now divide both sides by 9. However, since $\gcd(9, 15) = 3$, we must divide the modulus by 3 as well:

$$x \equiv 8 \pmod{5}.$$

So the solutions are those values which are congruent to 8, or equivalently 3, modulo 5. This means that in some sense there are 3 solutions modulo 15: 3, 8, and 13. We can write the solution:

$$x \equiv 3 \pmod{15}; \;\; x \equiv 8 \pmod{15}; \;\; x \equiv 13 \pmod{15}.$$

3. First, reduce modulo 14:

$$20x \equiv 23 \pmod{14}$$

$$6x \equiv 9 \pmod{14}.$$

We could now divide both sides by 3, or try to increase 9 by a multiple of 14 to get a multiple of 6. If we divide by 3, we get,

$$2x \equiv 3 \pmod{14}.$$

Now try adding multiples of 14 to 3, in hopes of getting a number we can divide by 2. This will not work! Every time we add 14 to the right side, the result will still be odd. We will never get an even number, so we will never be able to divide by 2. Thus there are no solutions to the congruence.

The last congruence above illustrates the way in which congruences might not have solutions. We could have seen this immediately in fact. Look at the original congruence:

$$20x \equiv 23 \pmod{14}.$$

If we write this as an equation, we get

$$20x = 23 + 14k,$$

or equivalently $20x - 14k = 23$. We can easily see there will be no solution to this equation in integers. The left-hand side will always be even, but the right-hand side is odd. A similar problem would occur if the right-hand side was divisible by *any* number the left-hand side was not.

So in general, given the congruence

$$ax \equiv b \pmod{n},$$

if a and n are divisible by a number which b is not divisible by, then there will be no solutions. In fact, we really only need to check one divisor of a and n: the greatest common divisor. Thus, a more compact way to say this is:

Congruences with no solutions.

If $\gcd(a,n) \nmid b$, then $ax \equiv b \pmod{n}$ has no solutions.

Solving Linear Diophantine Equations

Discrete math deals with whole numbers of things. So when we want to solve equations, we usually are looking for *integer* solutions. Equations which are intended to only have integer solutions were first studied by in the third century by the Greek mathematician Diophantus of Alexandria, and as such are called *Diophantine equations*. Probably the most famous example of a Diophantine equation is $a^2 + b^2 = c^2$. The integer solutions to this equation are called **Pythagorean triples**. In general, solving Diophantine equations is hard (in fact, there is provably no general algorithm for deciding whether a Diophantine equation has a solution, a result known as Matiyasevich's Theorem). We will restrict our focus to *linear* Diophantine equations, which are considerably easier to work with.

Diophantine Equations.

An equation in two or more variables is called a **Diophantine equation** if only integers solutions are of interest. A **linear** Diophantine equation takes the form $a_1x_1 + a_2x_x + \cdots + a_nx_n = b$ for constants $a_1, \ldots, a_n, b$.

A **solution** to a Diophantine equation is a solution to the equation consisting only of integers.

We have the tools we need to solve linear Diophantine equations. We will consider, as a main example, the equation

$$51x + 87y = 123.$$

The general strategy will be to convert the equation to a congruence, then solve that congruence.[4] Let's work this particular example to see how this might go.

First, check if perhaps there are no solutions because a divisor of 51 and 87 is not a divisor of 123. Really, we just need to check whether $\gcd(51, 87) \mid 123$. This greatest common divisor is 3, and yes $3 \mid 123$. At this point, we might as well factor out this greatest common divisor. So instead, we will solve:

$$17x + 29y = 41.$$

Now observe that if there are going to be solutions, then for those values of x and y, the two sides of the equation must have the same remainder as each other, no matter what we divide by. In particular, if we divide both sides by 17, we must get the same remainder. Thus we can safely write

$$17x + 29y \equiv 41 \pmod{17}.$$

We choose 17 because $17x$ will have remainder 0. This will allow us to reduce the congruence to just one variable. We could have also moved to a congruence modulo 29, although there is usually a good reason to select the smaller choice, as this will allow us to reduce the other coefficient. In our case, we reduce the congruence as follows:

$$\begin{aligned} 17x + 29y &\equiv 41 \pmod{17} \\ 0x + 12y &\equiv 7 \pmod{17} \\ 12y &\equiv 24 \pmod{17} \\ y &\equiv 2 \pmod{17}. \end{aligned}$$

[4]This is certainly not the only way to proceed. A more common technique would be to apply the **Euclidean algorithm**. Our way can be a little faster, and is presented here primarily for variety.

Now at this point we know $y = 2 + 17k$ will work for any integer k. If we haven't made a mistake, we should be able to plug this back into our original Diophantine equation to find x:

$$\begin{aligned} 17x + 29(2 + 17k) &= 41 \\ 17x &= -17 - 29 \cdot 17k \\ x &= -1 - 29k. \end{aligned}$$

We have now found all solutions to the Diophantine equation. For each k, $x = -1 - 29k$ and $y = 2 + 17k$ will satisfy the equation. We could check this for a few cases. If $k = 0$, the solution is $(-1, 2)$, and yes, $-17 + 2 \cdot 29 = 41$. If $k = 3$, the solution is $(-88, 53)$. If $k = -2$, we get $(57, -32)$.

To summarize this process, to solve $ax + by = c$, we,

1. Divide both sides of the equation by $\gcd(a, b)$ (if this does not leave the right-hand side as an integer, there are no solutions). Let's assume that $ax + by = c$ has already been reduced in this way.
2. Pick the smaller of a and b (here, assume it is b), and convert to a congruence modulo b:
   $$ax + by \equiv c \pmod{b}.$$
   This will reduce to a congruence with one variable, x:
   $$ax \equiv c \pmod{b}.$$
3. Solve the congruence as we did in the previous section. Write your solution as an equation, such as,
   $$x = n + kb.$$
4. Plug this into the original Diophantine equation, and solve for y.
5. If we want to know solutions in a particular range (for example, $0 \leq x, y \leq 20$), pick different values of k until you have all required solutions.

Here is another example:

Example 5.2.7

How can you make \$6.37 using just 5-cent and 8-cent stamps? What is the smallest and largest number of stamps you could use?

Solution. First, we need a Diophantine equation. We will work in numbers of cents. Let x be the number of 5-cent stamps, and y be the number of 8-cent stamps. We have:

$$5x + 8y = 637.$$

Convert to a congruence and solve:

$$\begin{aligned} 8y &\equiv 637 \pmod 5 \\ 3y &\equiv 2 \pmod 5 \\ 3y &\equiv 12 \pmod 5 \\ y &\equiv 4 \pmod 5. \end{aligned}$$

Thus $y = 4 + 5k$. Then $5x + 8(4 + 5k) = 637$, so $x = 121 - 8k$.

This says that one way to make \$6.37 is to take 121 of the 5-cent stamps and 4 of the 8-cent stamps. To find the smallest and largest number of stamps, try different values of k.

k	(x, y)	Stamps
-1	(129, -1)	not possible
0	(121, 4)	125
1	(113, 9)	122
2	(105, 13)	119
⋮	⋮	⋮

This is no surprise. Having the most stamps means we have as many 5-cent stamps as possible, and to get the smallest number of stamps would require have the least number of 5-cent stamps. To minimize the number of 5-cent stamps, we want to pick k so that $121 - 8k$ is as small as possible (but still positive). When $k = 15$, we have $x = 1$ and $y = 79$.

Therefore, to make \$6.37, you can us as few as 80 stamps (1 5-cent stamp and 79 8-cent stamps) or as many as 125 stamps (121 5-cent stamps and 4 8-cent stamps).

Using this method, as long as you can solve linear congruences in one variable, you can solve linear Diophantine equations of two variables. There are times though that solving the linear congruence is a lot of work. For example, suppose you need to solve,

$$13x \equiv 6 \pmod{51}.$$

You *could* keep adding 51 to the right side until you get a multiple of 13: You would get 57, 108, 159, 210, 261, 312, and 312 is the first of these that is divisible by 13. This works, but is really too much work. Instead we could convert *back* to a Diophantine equation:

$$13x = 6 + 51k.$$

Now solve *this* like we have in this section. Write it as a congruence modulo 13:

$$\begin{aligned} 0 &\equiv 6 + 51k \pmod{13} \\ -12k &\equiv 6 \pmod{13} \\ 2k &\equiv -1 \pmod{13} \\ 2k &\equiv 12 \pmod{13} \\ k &\equiv 6 \pmod{13}. \end{aligned}$$

so $k = 6 + 13j$. Now go back and figure out x:

$$\begin{aligned} 13x &= 6 + 51(6 + 13j) \\ x &= 24 + 51j. \end{aligned}$$

Of course you could do this switching back and forth between congruences and Diophantine equations as many times as you like. If you *only* used this technique, you would essentially replicate the Euclidean algorithm, a more standard way to solve Diophantine equations.

Exercises

1. Suppose a, b, and c are integers. Prove that if $a \mid b$, then $a \mid bc$.

2. Suppose a, b, and c are integers. Prove that if $a \mid b$ and $a \mid c$ then $a \mid b + c$ and $a \mid b - c$.

3. Write out the remainder classes for $n = 4$.

4. What is the largest n such that 16 and 25 are in the same remainder class modulo n? Write out the remainder class they both belong to and give an example of a number more than 100 in that class.

5. Let a, b, c, and n be integers. Prove that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a - c \equiv b - d \pmod{n}$.

6. Find the remainder of 3^{456} when divided by

(a) 2. (b) 5. (c) 7. (d) 9.

7. Repeat the previous exercise, this time dividing 2^{2019}.

8. Determine which of the following congruences have solutions, and find any solutions (between 0 and the modulus) by trial and error.

(a) $4x \equiv 5 \pmod{6}$.

(b) $6x \equiv 3 \pmod{9}$.

(c) $x^2 \equiv 2 \pmod{4}$.

9. Determine which of the following congruences have solutions, and find any solutions (between 0 and the modulus) by trial and error.

(a) $4x \equiv 5 \pmod{7}$.

(b) $6x \equiv 4 \pmod{9}$.

(c) $x^2 \equiv 2 \pmod{7}$.

10. Solve the following congruence $5x + 8 \equiv 11 \pmod{22}$. That is, describe the general solution.

11. Solve the congruence: $6x \equiv 4 \pmod{10}$.

12. Solve the congruence: $4x \equiv 24 \pmod{30}$.

13. Solve the congruence: $341x \equiv 2941 \pmod{9}$.

14. I'm thinking of a number. If you multiply my number by 7, add 5, and divide the result by 11, you will be left with a remainder of 2. What remainder would you get if you divided my original number by 11?

15. Solve the following linear Diophantine equation, using modular arithmetic (describe the general solutions).

$$6x + 10y = 32.$$

16. Solve the following linear Diophantine equation, using modular arithmetic (describe the general solutions).

$$17x + 8y = 31.$$

17. Solve the following linear Diophantine equation, using modular arithmetic (describe the general solutions).

$$35x + 47y = 1.$$

18. You have a 13 oz. bottle and a 20 oz. bottle, with which you wish to measure exactly 2 oz. However, you have a limited supply of water. If any water enters either bottle and then gets dumped out, it is gone forever. What is the least amount of water you can start with and still complete the task?

Appendix A

Selected Hints

0.2 Exercises

0.2.18. Try an example. What if $P(x)$ was the predicate, "x is prime"? What if it was "if x is divisible by 4, then it is even"? Of course examples are not enough to prove something in general, but that is entirely the point of this question.

0.2.19. First figure out what each statement is saying. For part (c), you don't need to assume the domain is an infinite set.

0.3 Exercises

0.3.7. You should be able to write all of them out. Don't forget A and B, which are also candidates for C.

0.3.14. It might help to think about what the union $A_2 \cup A_3$ is first. Then think about what numbers are *not* in that union. What will happen when you also include A_5?

0.3.17. We are looking for a set containing 16 sets.

0.3.18. Write these out, or at least start to and look for a pattern.

0.3.29. It looks like you should be able to define the set A like this. But consider the two possible values for $|A|$.

0.4 Exercises

0.4.20. Work with some examples. What if $f = \begin{pmatrix} 1 & 2 & 3 \\ a & a & b \end{pmatrix}$ and $g = \begin{pmatrix} a & b & c \\ 5 & 6 & 7 \end{pmatrix}$?

0.4.25. To find the recurrence relation, consider how many *new* handshakes occur when person $n + 1$ enters the room.

0.4.29. One of these is not always true. Try some examples!

1.1 Exercises

1.1.9. To find out how many numbers are divisible by 6 and 7, for example, take 500/42 and round down.

1.1.11. For part (a) you could use the formula for PIE, but for part (b) you might be better off drawing a Venn diagram.

1.1.13. You could consider cases. For example, any number of the form ODD-ODD-EVEN will have an even sum. Alternatively, how many three digit numbers have the sum of their digits even if the first two digits are 54? What if the first two digits are 19?

1.1.14. For a simpler example, there are 4 divisors of $6 = 2 \cdot 3$. They are $1 = 2^0 \cdot 3^0$, $2 = 2^1 \cdot 3^0$, $3 = 2^0 \cdot 3^1$ and $6 = 2^1 \cdot 3^1$.

1.2 Exercises

1.2.5. Pennies are sort of like 0′s and nickels are sort of like 1′s.

1.2.7. Break the question into five cases.

1.3 Exercises

1.3.4. Which question should have the larger answer? One of these is a combination, the other is a permutation.

1.3.6. If you pick any three points, you can get a triangle, unless those three points are all on the x-axis or on the y-axis. There are other ways to start this as well, and any correct method should give the same answer.

1.3.8. We just need a string of 7 letters: 4 of one type, 3 of the other.

1.3.11. There are 10 people seated around the table, but it does not matter where King Arthur sits, only who sits to his left, two seats to his left, and so on. So the answer is not 10!.

1.4 Exercises

1.4.3. There will be 185 triangles. But to find them . . .

(a) How many vertices of the triangle can be on the horizontal axis?

(b) Will *any* three dots work as the vertices?

1.4.4. The answer is 120.

1.4.6. Try Exercise 1.4.5

1.4.7. What if you wanted a pair of co-maids-of-honor?

1.4.8. For the combinatorial proof: what if you don't yet know how many bridesmaids you will have?

1.4.9. Count handshakes.

1.4.13. This one might remind you of Example 1.4.6

1.4.14. For the lattice paths, think about what sort of paths 2^n would count. Not all the paths will end at the same point, but you could describe the set of end points as a line.

1.6 Exercises

1.6.4. Instead, count the solutions to $y_1 + y_2 + y_3 + y_4 = 7$ with $0 \le y_i \le 3$. Why is this equivalent?

1.6.13. This is a sneaky way to ask for the number of derangements on 5 elements. Do you see why?

1.7 Chapter Review

1.7.16. Stars and bars.

2.1 Exercises

2.1.11. You will want to write out the sequence, guess a closed formula, and then verify that you are correct.

2.1.12. Write out the sequence, guess a recursive definition, and verify that the closed formula is a solution to that recursive definition.

2.1.15. Try an example: when you draw the 4th line, it will cross three other lines, so will be divided into four segments, two of which are infinite. Each segment will divide a previous region into two.

2.1.16. Consider three cases: the last digit is a 0, a 1, or a 2. Two of these should be easy to count, but strings ending in 0 cannot be proceeded by a 2, so require a little more work.

2.1.18. Think recursively, like you did in Pascal's triangle.

2.1.19. There is only one way to tile a 2×1 board, and two ways to tile a 2×2 board (you can orient the dominoes in two ways). In general, consider the two ways the domino covering the top left corner could be oriented.

2.4 Exercises

2.4.3. Use telescoping or iteration.

2.5 Exercises

2.5.9. It is not possible to score exactly 11 points. Can you prove that you can score n points for any $n \ge 12$?

2.5.11. Start with $(k+1)$-gon and divide it up into a k-gon and a triangle.

2.5.15. For the inductive step, you can assume you have a strictly increasing sequence up to a_k where $a_k < 100$. Now you just need to find the next term a_{k+1} so that $a_k < a_{k+1} < 100$. What should a_{k+1} be?

2.5.17. For the inductive case, you will need to show that $(k+1)^2 + (k+1)$ is even. Factor this out and locate the part of it that is $k^2 + k$. What have you assumed about that quantity?

2.5.18. This is similar to Exercise 2.5.15, although there you were showing that a sequence had all its terms less than some value, and here you are showing that the sum is less than some value. But the partial sums forms a sequence, so this is actually very similar.

2.5.20. As with the previous question, we will want to subtract something from n in the inductive step. There we subtracted the largest power of 2 less than n. So what should you subtract here?

Note, you will still need to take care here that the sum you get from the inductive hypothesis, together with the number you subtracted will be a sum of *distinct* Fibonacci numbers. In fact, you could prove that the Fibonacci numbers in the sum are non-consecutive!

2.5.21. We have already proved this without using induction, but looking at it inductively sheds light onto the problem (and is fun).

The question you need to answer to complete the inductive step is, how many new handshakes take place when a person $k + 1$ enters the room. Why does adding this give you the correct formula?

2.5.22. You will need to use strong induction. For the inductive case, try multiplying $\left(x^k + \frac{1}{x^k}\right)\left(x + \frac{1}{x}\right)$ and collect which terms together are integers.

2.5.23. Here's the idea: since every entry in Pascal's Triangle is the sum of the two entries above it, we can get the $k + 1$st row by adding up all the pairs of entry from the kth row. But doing this uses each entry on the kth row twice. Thus each time we drop to the next row, we double the total. Of course, row 0 has sum $1 = 2^0$ (the base case). Now try to make this precise with a formal induction proof. You will use the fact that $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ for the inductive case.

2.5.24. To see why this works, try it on a copy of Pascal's triangle. We are adding up the entries along a diagonal, starting with the 1 on the left-hand side of the 4th row. Suppose we add up the first 5 entries on this diagonal. The claim is that the sum is the entry below and to the left of the last of these 5 entries. Note that if this is true, and we instead add up the first 6 entries, we will need to add the entry one spot to the right of the previous sum. But these two together give the entry below them, which is below and left of the last of the 6 entries on the diagonal. If you follow that, you can see what is going on. But it is not a great proof. A formal induction proof is needed.

2.5.26. You are allowed to assume the base case. For the inductive case, group all but the last function together as one sum of functions, then apply the usual sum of derivatives rule, and then the inductive hypothesis.

2.5.27. For the inductive step, we know by the product rule for two functions that

$$(f_1 f_2 f_3 \cdots f_k f_{k+1})' = (f_1 f_2 f_3 \cdots f_k)' f_{k+1} + (f_1 f_2 f_3 \cdots f_k) f'_{k+1}.$$

Then use the inductive hypothesis on the first summand, and distribute.

2.5.29. You will need three base cases. This is a very good hint actually, as it suggests that to prove $P(n)$ is true, you would want to use the fact that $P(n-3)$ is true. So somehow you need to increase the number of squares by 3.

2.6 Chapter Review

2.6.14.

(a) Hint: $(n+1)^{n+1} > (n+1) \cdot n^n$.

(b) Hint: This should be similar to the other sum proofs. The last bit comes down to adding fractions.

(c) Hint: Write $4^{k+1} - 1 = 4 \cdot 4^k - 4 + 3$.

(d) Hint: one 9-cent stamp is 1 more than two 4-cent stamps, and seven 4-cent stamps is 1 more than three 9-cent stamps.

(e) Careful to actually use induction here. The base case: $2^2 = 4$. The inductive case: assume $(2n)^2$ is divisible by 4 and consider $(2n+2)^2 = (2n)^2 + 4n + 4$. This is divisible by 4 because $4n + 4$ clearly is, and by our inductive hypothesis, so is $(2n)^2$.

2.6.15. This is a straight forward induction proof. Note you will need to simplify $\left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3$ and get $\left(\frac{(n+1)(n+2)}{2}\right)^2$.

2.6.16. There are two base cases $P(0)$ and $P(1)$. Then, for the inductive case, assume $P(k)$ is true for all $k < n$. This allows you to assume $a_{n-1} = 1$ and $a_{n-2} = 1$. Apply the recurrence relation.

3.1 Exercises

3.1.4. Like above, only now you will need 8 rows instead of just 4.

3.1.5. You should write down three statements using the symbols P, Q, R, S. If Geoff is a truth-teller, then all three statements would be true. If he was a liar, then all three statements would be false. But in either case, we don't yet know whether the four atomic statements are true or false, since he hasn't said them by themselves.

A truth table might help, although is probably not entirely necessary.

3.1.10.

(a) There will be three rows in which the statement is false.

(b) Consider the three rows that evaluate to false and say what the truth values of T, S, and P are there.

(c) You are looking for a row in which P is true, and the whole statement is true.

3.1.11. Write down three statements, and then take the negation of each (since he is a liar). You should find that Tommy ate one item and drank one item. (Q is for cucumber sandwiches.)

3.1.15. For the second part, you can inductively assume that from the first $n-2$ implications you can deduce $P_1 \to P_{n-1}$. Then you are back in the case in part (a) again.

3.1.18. It might help to translate the statements into symbols and then use the formulaic rules to simplify negations (i.e., rules for quantifiers and De Morgan's laws). After simplifying, you should get $\forall x(\neg E(x) \wedge \neg O(x))$, for the first one, for example. Then translate this back into English.

3.1.19. What do these concepts mean in terms of truth tables?

3.2 Exercises

3.2.5. One of the implications will be a direct proof, the other will be a proof by contrapositive.

3.2.6. This is really an exercise in modifying the proof that $\sqrt{2}$ is irrational. There you proved things were even; here they will be multiples of 3.

3.2.7. Part (a) should be a relatively easy direct proof. Look for a counterexample for part (b).

3.2.9. A proof by contradiction would be reasonable here, because then you get to assume that both a *and* b are odd. Deduce that c^2 is even, and therefore a multiple of 4 (why? and why is that a contradiction?).

3.2.11. Use a different style of proof for each part. The last part should remind you of the pigeonhole principle, so mimicking that proof might be helpful.

3.2.13. Note that if $\log(7) = \frac{a}{b}$, then $7 = 10^{\frac{a}{b}}$. Can any power of 7 be the same as a power of 10?

3.2.14. What if there were? Deduce that x must be odd, and continue towards a contradiction.

3.2.15. Prove the contrapositive by cases. There will be 4 cases to consider.

3.2.16. Your friend's proof a proof, but of what? What implication follows from the given proof? Is that helpful?

3.2.18. Consider the set of *numbers* of friends that everyone has. If everyone had a different number of friends, this set must contain 20 elements. Is that possible? Why not?

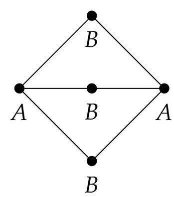
3.2.19. This feels like the pigeonhole principle, although a bit more complicated. At least, you could try to replicate the style of proof used by the pigeonhole principle. How would the episodes need to be spaced out so that no two of your sixty were exactly 4 apart?

4.1 Exercises

4.1.3. Both situations are possible. Go find some examples.

4.1.6. The bipartite graph is a little tricky. You will definitely want a complete bipartite graph, but it could be $K_{5,5}$ or maybe $K_{1,9}$, or . . .

4.1.7. The first graph is bipartite, which can be seen by labeling it as follows.



Two of the remaining three are also bipartite.

4.1.8. C_4 is bipartite; C_5 is not. What about all the other values of n?

4.1.11. How many edges does K_n have? One of the two graphs will not be connected (unless $j = 1$).

4.1.12. You should be able to deduce everything directly from the definition. However, perhaps it would be helpful to know that the N stands for **neighborhood**.

4.1.13. Be careful to make sure the edges are not "directed." In a graph, if a is adjacent to b, then b is adjacent to a. In the language of relations, we say that the edge relation is **symmetric**.

4.1.14. You might want to answer the questions for some specific values of n to get a feel for them, but your final answers should be in terms of n.

4.1.15. Try a small example first: any graph with 8 vertices must have two vertices of the same degree. If not, what would the degree sequence be?

4.1.16. Use the handshake lemma 4.1.5. What would happen if all the vertices had degree 2?

4.2 Exercises

4.2.3. Careful: the graphs might not be connected.

4.2.4. Try Exercise 4.2.2.

4.2.5. Try a proof by contradiction and consider a spanning tree of the graph.

4.2.7. For part (b), trying some simple examples should give you the formula. Then you just need to prove it is correct.

4.2.8. Examining the proof of Proposition 4.2.1 gives you most of what you need, but make sure to just give the relevant parts, and take care to not use proof by contradiction.

4.2.9. You will need to remove a vertex of degree one, apply the inductive hypothesis to the result, and then say which set the degree one vertex to.

4.2.10. If e is the root, then b will have three children (a, c, and d), all of which will be siblings, and have b as their parent. a will not have any children.

In general, how can you determine the number of children a vertex will have, if it is not a root?

4.2.14. There is an example with 7 edges.

4.2.15. The previous exercise will be helpful.

4.2.16. Note that such an edge, if removed, would disconnect the graph. We call graphs that have an edge like this **1-connected**.

4.3 Exercises

4.3.3. What would Euler's formula tell you?

4.3.5. You can use the handshake lemma to find the number of edges, in terms of v, the number of vertices.

4.3.11. What is the length of the shortest cycle? (This quantity is usually called the **girth** of the graph.)

4.3.14. The girth of the graph is 4.

4.3.15. What has happened to the girth? Careful: we have a different number of edges as well. Better check Euler's formula.

4.4 Exercises

4.4.7. For (a), you will want the teams to be vertices and games to be edges. Which does it make sense to color?

4.4.10. The chromatic number is 4. Now prove this!

Note that you cannot use the 4-color theorem, or Brooke's theorem, or the clique number here. In fact, this graph, called the *Grötzsch graph* is the smallest graph with chromatic number 4 that does not contain any triangles.

4.4.13. You can color K_5 in such a way that every vertex is adjacent to exactly two blue edges and two red edges. However, there is a graph with only 5 edges that will result in a vertex incident to three edges of the same color no matter how they are colored. What is it, and how can you generalize?

4.4.14. The previous exercise is useful as a starting point.

4.5 Exercises

4.5.7. This is harder than the previous three questions. Think about which "side" of the graph the Hamilton path would need to be on every other step.

4.5.9. If you read off the names of the students in order, you would need to read each student's name exactly once, and the last name would need to be of a student who was friends with the first. What sort of a cycle is this?

4.5.10. Draw a graph with 6 vertices and 8 edges. What sort of path would be appropriate?

4.7 Chapter Review

4.7.23. You might want to give the proof in two parts. First prove by induction that the cycle C_n has $v = e$. Then consider what happens if the graph is more than just the cycle.

5.1 Exercises

5.1.10. You should "multiply" the two sequences.

5.2 Exercises

5.2.13. First reduce each number modulo 9, which can be done by adding up the digits of the numbers.

5.2.18. Solve the Diophantine equation $13x + 20y = 2$ (why?). Then consider which value of k (the parameter in the solution) is optimal.

Appendix B

Selected Solutions

0.2 Exercises

0.2.1.

(a) This is not a statement. It is an imperative sentence, but is not either true or false. It doesn't matter that this might actually be the rule or not. Note that "The rule is that all customers must wear shoes" *is* a statement.

(b) This is a statement, as it is either true or false. It is an atomic statement because it cannot be divided into smaller statements.

(c) This is again a statement, but this time it is molecular. In fact, it is a conjunction, as we can write it as "The customers wore shoes and the customers wore socks."

0.2.3.

(a) $P \wedge Q$.

(b) $P \rightarrow \neg Q$.

(c) Jack passed math or Jill passed math (or both).

(d) If Jack and Jill did not both pass math, then Jill did.

(e) i. Nothing else.

ii. Jack did not pass math either.

0.2.4.

(a) It is impossible to tell. The hypothesis of the implication is true. Thus the implication will be true if the conclusion is true (if 13 *is* my favorite number) and false otherwise.

(b) This is true, no matter whether 13 is my favorite number or not. Any implication with a true conclusion is true.

(c) This is true, again, no matter whether 13 is my favorite number or not. Any implication with a false hypothesis is true.

(d) For a disjunction to be true, we just need one or the other (or both) of the parts to be true. Thus this is a true statement.

(e) We cannot tell. The statement would be true if 13 is my favorite number, and false if not (since a conjunction needs both parts to be true to be true).

(f) This is definitely false. 13 is prime, so its negation (13 is not prime) is false. At least one part of the conjunction is false, so the whole statement is false.

(g) This is true. Either 13 is my favorite number or it is not, but whichever it is, at least one part of the disjunction is true, so the whole statement is true.

0.2.5. The main thing to realize is that we don't know the colors of these two shapes, but we do know that we are in one of three cases: We could have a blue square and green triangle. We could have a square that was not blue but a green triangle. Or we could have a square that was not blue and a triangle that was not green. The case in which the square is blue but the triangle is not green cannot occur, as that would make the statement false.

(a) This must be false. In fact, this is the negation of the original implication.

(b) This might be true or might be false.

(c) True. This is the contrapositive of the original statement, which is logically equivalent to it.

(d) We do not know. This is the converse of the original statement. In particular, if the square is not blue but the triangle is green, then the original statement is true but the converse is false.

(e) True. This is logically equivalent to the original statement.

0.2.6. The only way for an implication $P \rightarrow Q$ to be true but its converse to be false is for Q to be true and P to be false. Thus:

(a) False.

(b) True.

(c) False.

(d) True.

0.2.7. The converse is "If I will give you magic beans, then you will give me a cow." The contrapositive is "If I will not give you magic beans, then you will not give me a cow." All the other statements are neither the converse nor contrapositive.

0.2.9.

(a) Equivalent to the converse.

(b) Equivalent to the original theorem.

(c) Equivalent to the converse.

(d) Equivalent to the original theorem.

(e) Equivalent to the original theorem.

(f) Equivalent to the converse.

(g) Equivalent to the converse.

(h) Equivalent to the original theorem.

0.2.10.

(a) If you have lost weight, then you exercised.

(b) If you exercise, then you will lose weight.

(c) If you are American, then you are patriotic.

(d) If you are patriotic, then you are American.

(e) If a number is rational, then it is real.

(f) If a number is not even, then it is prime. (Or the contrapositive: if a number is not prime, then it is even.)

(g) If the Broncos don't win the Super Bowl, then they didn't play in the Super Bowl. Alternatively, if the Broncos play in the Super Bowl, then they will win the Super Bowl.

0.2.12. $P(5)$ is the statement "$3 \cdot 5 + 1$ is even", which is true. Thus the statement $\exists x P(x)$ is true (for example, 5 is such an x). However, we cannot tell anything about $\forall x P(x)$ since we do not know the truth value of $P(x)$ for *all* elements of the domain of discourse. In this case, $\forall x P(x)$ happens to be false (since $P(4)$ is false, for example).

0.2.14.

(a) The claim that $\forall x P(x)$ means that $P(n)$ is true no matter what n you consider in the domain of discourse. Thus the only way to prove that $\forall x P(x)$ is true is to check or otherwise argue that $P(n)$ is true for all n in the domain.

(b) To prove $\forall x P(x)$ is false all you need is one example of an element in the domain for which $P(n)$ is false. This is often called a counterexample.

(c) We are simply claiming that there is some element n in the domain of discourse for which $P(n)$ is true. If you can find one such element, you have verified the claim.

(d) Here we are claiming that no element we find will make $P(n)$ true. The only way to be sure of this is to verify that *every* element of the domain makes $P(n)$ false. Note that the level of proof needed for this statement is the same as to prove that $\forall x P(x)$ is true.

0.2.15.

(a) $\forall x \exists y P(x, y)$ is false because when $x = 4$, there is no y which makes $P(4, y)$ true.

(b) $\forall y \exists x P(x, y)$ is true. No matter what y is (i.e., no matter what column we are in) there is some x for which $P(x, y)$ is true. In fact, we can always take x to be 3.

(c) $\exists x \forall y P(x, y)$ is true. In particular $x = 3$ is such a number, so that no matter what y is, $P(x, y)$ is true.

(d) $\exists y \forall x P(x, y)$ is false. In fact, no matter what y (column) we look at, there is always some x (row) which makes $P(x, y)$ false.

0.2.16.

(a) $\neg \exists x (E(x) \wedge O(x))$.

(b) $\forall x (E(x) \rightarrow O(x + 1))$.

(c) $\exists x (P(x) \wedge E(x))$ (where $P(x)$ means "x is prime").

(d) $\forall x \forall y \exists z (x < z < y \vee y < z < x)$.

(e) $\forall x \neg \exists y (x < y < x + 1)$.

0.2.17.

(a) Any even number plus 2 is an even number.

(b) For any x there is a y such that $\sin(x) = y$. In other words, every number x is in the domain of sine.

(c) For every y there is an x such that $\sin(x) = y$. In other words, every number y is in the range of sine (which is false).

(d) For any numbers, if the cubes of two numbers are equal, then the numbers are equal.

0.3 Exercises

0.3.1.

(a) $\{1, 3, 4, 6, 9, 10\}$.

(b) $\{1\}$.

(c) $\{4, 9\}$.

(d) $\{3, 6, 10\}$.

0.3.2.

(a) This is the set $\{3, 4, 5, \ldots\}$ since we need each element to be a natural number whose square is at least three more than 2. Since $3^2 - 3 = 6$ but $2^2 - 3 = 1$ we see that the first such natural number is 3.

(b) We get the same set as we did in the previous part, and the smallest non-negative number for which $n^2 - 5$ is a natural numbers is 3.

Note that if we didn't specify $n \in \mathbb{N}$ then any integer less than -3 would also be in the set, so there would not be a least element.

(c) This is the set $\{1, 2, 5, 10, \ldots\}$, namely the set of numbers that are the *result* of squaring and adding 1 to a natural number. ($0^2 + 1 = 1$, $1^2 + 1 = 2$, $2^2 + 1 = 5$ and so on.) Thus the least element of the set is 1.

(d) Now we are looking for natural numbers that are equal to taking some natural number, squaring it and adding 1. That is, $\{1, 2, 5, 10, \ldots\}$, the same set as the previous part. So again, the least element is 1.

0.3.3.

(a) 34. Note that $37 - 4 = 33$, but this calculation would not include 4 itself.

(b) 103. Again, you could compute this by $100 - (-2) + 1$, or simply count: 100 numbers from 1 through 100, plus -2, -1, and 0.

(c) 8. There are 8 primes not greater than 20: $\{2, 3, 5, 7, 11, 13, 17, 19\}$.

0.3.4. $\{2, 4\}$.

0.3.5. $\{1, 2, 3, 4, 5, 6, 8, 10\}$

0.3.6. 11.

0.3.7. There will be exactly 4 such sets: $\{2, 3, 4\}$, $\{1, 2, 3, 4\}$, $\{2, 3, 4, 5\}$ and $\{1, 2, 3, 4, 5\}$.

0.3.8.

(a) $A \cap B = \{3, 4, 5\}$.

(b) $A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$.

(c) $A \setminus B = \{1, 2\}$.

(d) $A \cap \overline{(B \cup C)} = \{1\}$.

0.3.9.

(a) $A \cap B$ will be the set of natural numbers that are both at least 4 and less than 12, and even. That is, $A \cap B = \{x \in \mathbb{N} : 4 \leq x < 12 \wedge x \text{ is even}\} = \{4, 6, 8, 10\}$.

(b) $A \setminus B$ is the set of all elements that are in A but not B. So this is $\{x \in \mathbb{N} : 4 \leq x < 12 \wedge x \text{ is odd}\} = \{5, 7, 9, 11\}$.

Note this is the same set as $A \cap \overline{B}$.

0.3.11. For example, $A = \{2, 3, 5, 7, 8\}$ and $B = \{3, 5\}$.

0.3.12. For example, $A = \{1, 2, 3\}$ and $B = \{1, 2, 3, 4, 5, \{1, 2, 3\}\}$

0.3.13.

(a) No.

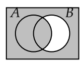
(b) No.

(c) $2\mathbb{Z} \cap 3\mathbb{Z}$ is the set of all integers which are multiples of both 2 and 3 (so multiples of 6). Therefore $2\mathbb{Z} \cap 3\mathbb{Z} = \{x \in \mathbb{Z} : \exists y \in \mathbb{Z}(x = 6y)\}$.

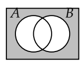
(d) $2\mathbb{Z} \cup 3\mathbb{Z}$.

0.3.15.

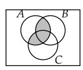
(a) $A \cup \overline{B}$:



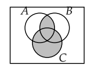
(b) $\overline{(A \cup B)}$:



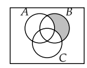
(c) $A \cap (B \cup C)$:



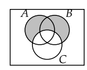
(d) $(A \cap B) \cup C$:



(e) $\overline{A} \cap B \cap \overline{C}$:



(f) $(A \cup B) \setminus C$:



0.3.17.

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}\{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, \{a, b, c, d\}\}.$$

0.3.20. For example, $A = \{1, 2, 3, 4\}$ and $B = \{5, 6, 7, 8, 9\}$ gives $A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

0.3.28. We need to be a little careful here. If B contains 3 elements, then A contains just the number 3 (listed twice). So that would make $|A| = 1$, which would make $B = \{1, 3\}$, which only has 2 elements. Thus $|B| \neq 3$. This means that $|A| = 2$, so B contains at least the elements 1 and 2. Since $|B| \neq 3$, we must have $|B| = 2$, which agrees with the definition of B.

Therefore it must be that $A = \{2, 3\}$ and $B = \{1, 2\}$

0.4 Exercises

0.4.1.

(a) $f(1) = 4$, since 4 is the number below 1 in the two-line notation.

(b) Such an n is $n = 2$, since $f(2) = 1$. Note that 2 is above a 1 in the notation.

(c) $n = 4$ has this property. We say that 4 is a fixed point of f. Not all functions have such a point.

(d) Such an element is 2 (in fact, that is the only element in the codomain that is not in the range). In other words, 2 is not the image of any element under f; nothing is sent to 2.

0.4.2.

(a) This is neither injective nor surjective. It is not injective because more than one element from the domain has 3 as its image. It is not surjective because there are elements of the codomain (1, 2, 4, and 5) that are not images of anything from the domain.

(b) This is a bijection. Every element in the codomain is the image of *exactly* one element of the domain.

(c) This is a bijection. Note that we can write this function in two line notation as $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$.

(d) In two line notation, this function is $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 2 & 2 & 3 \end{pmatrix}$. From this we can quickly see it is neither injective (for example, 1 is the image of both 1 and 2) nor surjective (for example, 4 is not the image of anything).

0.4.5. There are 8 functions, including 6 surjective and zero injective functions.

0.4.7.

(a) f is not injective, since $f(2) = f(5)$; two different inputs have the same output.

(b) f is surjective, since every element of the codomain is an element of the range.

(c) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 2 \end{pmatrix}$.

0.4.9. $f(10) = 1024$. To find $f(10)$, we need to know $f(9)$, for which we need $f(8)$, and so on. So build up from $f(0) = 1$. Then $f(1) = 2$, $f(2) = 4$, $f(3) = 8$, ... In fact, it looks like a closed formula for f is $f(n) = 2^n$. Later we will see how to prove this is correct.

0.4.10. For each case, you must use the recurrence to find $f(1)$, $f(2)$ ... $f(5)$. But notice each time you just add three to the previous. We do this 5 times.

(a) $f(5) = 15$.

(b) $f(5) = 16$.

(c) $f(5) = 17$.

(d) $f(5) = 115$.

0.4.12.

(a) f is injective, but not surjective (since 0, for example, is never an output).

(b) f is injective and surjective. Unlike in the previous question, every integers is an output (of the integer 4 less than it).

(c) f is injective, but not surjective (10 is not 8 less than a multiple of 5, for example).

(d) f is not injective, but is surjective. Every integer is an output (of twice itself, for example) but some integers are outputs of more than one input: $f(5) = 3 = f(6)$.

0.4.13.

(a) f is not injective. To prove this, we must simply find two different elements of the domain which map to the same element of the codomain. Since $f(\{1\}) = 1$ and $f(\{2\}) = 1$, we see that f is not injective.

(b) f is not surjective. The largest subset of A is A itself, and $|A| = 10$. So no natural number greater than 10 will ever be an output.

(c) $f^{-1}(1) = \{\{1\}, \{2\}, \{3\}, \ldots \{10\}\}$ (the set of all the singleton subsets of A).

(d) $f^{-1}(0) = \{\emptyset\}$. Note, it would be wrong to write $f^{-1}(0) = \emptyset$ - that would claim that there is no input which has 0 as an output.

(e) $f^{-1}(12) = \emptyset$, since there are no subsets of A with cardinality 12.

0.4.16.

(a) $|f^{-1}(3)| \leq 1$. In other words, either $f^{-1}(3)$ is the empty set or is a set containing exactly one element. Injective functions cannot have two elements from the domain both map to 3.

(b) $|f^{-1}(3)| \geq 1$. In other words, $f^{-1}(3)$ is a set containing at least one elements, possibly more. Surjective functions must have something map to 3.

(c) $|f^{-1}(3)| = 1$. There is exactly one element from X which gets mapped to 3, so $f^{-1}(3)$ is the set containing that one element.

0.4.17. X can really be any set, as long as $f(x) = 0$ or $f(x) = 1$ for every $x \in X$. For example, $X = \mathbb{N}$ and $f(n) = 0$ works.

0.4.21.

(a) f is injective.

Proof. Let x and y be elements of the domain $\mathbb{Z}$. Assume $f(x) = f(y)$. If x and y are both even, then $f(x) = x + 1$ and $f(y) = y + 1$. Since $f(x) = f(y)$, we have $x + 1 = y + 1$ which implies that $x = y$. Similarly, if x and y are both odd, then $x - 3 = y - 3$ so again $x = y$. The only other possibility is that x is even an y is odd (or visa-versa). But then $x + 1$ would be odd and $y - 3$ would be even, so it cannot be that $f(x) = f(y)$. Therefore if $f(x) = f(y)$ we then have $x = y$, which proves that f is injective. QED

(b) f is surjective.

Proof. Let y be an element of the codomain $\mathbb{Z}$. We will show there is an element n of the domain ($\mathbb{Z}$) such that $f(n) = y$. There are two cases: First, if y is even, then let $n = y + 3$. Since y is even, n is odd, so $f(n) = n - 3 = y + 3 - 3 = y$ as desired. Second, if y is odd, then let $n = y - 1$. Since y is odd, n is even, so $f(n) = n + 1 = y - 1 + 1 = y$ as needed. Therefore f is surjective. QED

0.4.22. Yes, this is a function, if you choose the domain and codomain correctly. The domain will be the set of students, and the codomain will be the set of possible grades. The function is almost certainly not injective, because it is likely that two students will get the same grade. The function might be surjective – it will be if there is at least one student who gets each grade.

0.4.24. This is not a function.

0.4.25. The recurrence relation is $f(n + 1) = f(n) + n$.

0.4.26. In general, $|A| \geq |f(A)|$, since you cannot get more outputs than you have inputs (each input goes to exactly one output), but you could have fewer outputs if the function is not injective. If the function is injective, then $|A| = |f(A)|$, although you can have equality even if f is not injective (it must be injective *restricted* to A).

0.4.27. In general, there is no relationship between $|B|$ and $|f^{-1}(B)|$. This is because B might contain elements that are not in the range of f, so we might even have $f^{-1}(B) = \emptyset$. On the other hand, there might be lots of elements from the domain that all get sent to a few elements in B, making $f^{-1}(B)$ larger than B.

More specifically, if f is injective, then $|B| \geq |f^{-1}(B)|$ (since every element in B must come from at most one element from the domain). If f is surjective, then $|B| \leq |f^{-1}(B)|$ (since every element in B must come from at least one element of the domain). Thus if f is bijective then $|B| = |f^{-1}(B)|$.

1.1 EXERCISES

1.1.1. There are 255 outfits. Use the multiplicative principle.

1.1.2.

(a) 8 ties. Use the additive principle.

(b) 15 ties. Use the multiplicative principle

(c) $5 \cdot (4 + 3) + 7 = 42$ outfits.

1.1.3.

(a) For example, 16 is the number of choices you have if you want to watch one movie, either a comedy or horror flick.

(b) For example, 63 is the number of choices you have if you will watch two movies, first a comedy and then a horror.

1.1.5.

(a) To maximize the number of elements in common between A and B, make $A \subset B$. This would give $|A \cap B| = 10$.

(b) A and B might have no elements in common, giving $|A \cap B| = 0$.

(c) $15 \leq |A \cup B| \leq 25$. In fact, when $|A \cap B| = 0$ then $|A \cup B| = 25$ and when $|A \cap B| = 10$ then $|A \cup B| = 15$.

1.1.6. $|A \cup B| + |A \cap B| = 13$. Use PIE: we know $|A \cup B| = 8 + 5 - |A \cap B|$.

1.1.7. 39 students. Use Venn diagram or PIE: $28+19+24-16-14-10+8 = 39$.

1.1.8. 6 students *don't* like potatoes.

1.1.9. 215 values of n.

1.1.12.

(a) $8^5 = 32768$ words.

(b) $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 = 6720$ words.

(c) $8 \cdot 8 = 64$ words.

(d) $64 + 64 - 0 = 128$ words.

(e) $(8 \cdot 7 \cdot 6 \cdot 5 \cdot 4) - 3 \cdot (5 \cdot 4) = 6660$ words.

1.2 EXERCISES

1.2.1.

(a) $2^6 = 64$ subsets. We need to select yes/no for each of the six elements.

(b) $2^3 = 8$ subsets. We need to select yes/no for each of the remaining three elements.

(c) $2^6 - 2^3 = 56$ subsets. There are 8 subsets which do not contain any odd numbers (select yes/no for each even number).

(d) $3 \cdot 2^3 = 24$ subsets. First pick the even number. Then say yes or no to each of the odd numbers.

1.2.2.

(a) $\binom{6}{4} = 15$ subsets.

(b) $\binom{3}{1} = 3$ subsets. We need to select 1 of the 3 remaining elements to be in the subset.

(c) $\binom{6}{4} = 15$ subsets. All subsets of cardinality 4 must contain at least one odd number.

(d) $\binom{3}{1} = 3$ subsets. Select 1 of the 3 even numbers. The remaining three odd numbers of S must all be in the set.

1.2.3.

(a) There are 512 subsets.

(b) $\displaystyle\binom{9}{5} = 126.$

(c) $2^4 = 16$. (Note, if you wish to exclude the empty set - it does not contain odd numbers, but no evens either - then you could subtract 1).

(d) 256.

1.2.4.

(a) $2^6 = 64$.

(b) $\displaystyle\binom{6}{3} = 20.$

(c) 176.

(d) 51.

1.2.5.

(a) We will need $6 \cdot 20 = 120$ coins (60 of each).

(b) We need $6 \cdot 64 = 384$ coins (192 of each).

1.2.6. $\binom{10}{6} + \binom{10}{7} + \binom{10}{8} + \binom{10}{9} + \binom{10}{10} = 386$ strings.

1.2.9. $\binom{14}{9} + \binom{15}{6}2^9$.

1.2.10.

(a) $\binom{14}{7} = 3432$ paths.

(b) $\binom{6}{2}\binom{8}{5} = 840$ paths.

(c) $\binom{14}{7} - \binom{6}{2}\binom{8}{5}$ paths.

1.2.11.

(a) $\binom{18}{9}$.

(b) $\binom{12}{7}\binom{6}{2}$.

(c) $$\binom{18}{9} - \binom{3}{1}\binom{14}{8}$$

(d) $$\binom{3}{1}\binom{15}{8} + \binom{12}{7}\binom{6}{2} - \binom{3}{1}\binom{9}{6}\binom{6}{2}$$

1.2.12.

(a) $\binom{11}{3} = 165$ choices, since you have to select a 3-element subset of the set of 11 toppings.

(b) $\binom{10}{3} = 120$ choices, since you must select 3 of the 10 non-pineapple toppings.

(c) $\binom{10}{2} = 45$ choices, since you must select 2 of the remaining 10 non-pineapple toppings to have in addition to the pineapple.

(d) $165 = 120 + 45$ choices, which makes sense because every 3-topping pizza either has pineapple or does not have pineapple as a topping.

1.3 Exercises

1.3.1.

(a) $\binom{10}{3} = 120$ pizzas. We must choose (in no particular order) 3 out of the 10 toppings.

(b) $2^{10} = 1024$ pizzas. Say yes or no to each topping.

(c) $P(10, 5) = 30240$ ways. Assign each of the 5 spots in the left column to a unique pizza topping.

1.3.2. Despite its name, we are not looking for a combination here. The order in which the three numbers appears matters. There are $P(40, 3) = 40 \cdot 39 \cdot 38$ different possibilities for the "combination". This is assuming you cannot repeat any of the numbers (if you could, the answer would be 40^3).

1.3.3.

(a) This is just the multiplicative principle. There are 7 digits which we can select for each of the 5 positions, so we have $7^5 = 16807$ such numbers.

(b) Now we have 7 choices for the first number, 6 for the second, etc. So there are $7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = P(7, 5) = 2520$ such numbers.

(c) To build such a number we simply must select 5 different digits. After doing so, there will only be one way to arrange them into a 5-digit number. Thus there are $\binom{7}{5} = 21$ such numbers.

(d) The permutation is in part (b), while the combination is in part (c). At first this seems backwards, since usually we use combinations for when order does not matter. Here it looks like in part (c) that order does matter. The better way to distinguish between combinations and permutations is to ask whether we are counting different arrangements as different outcomes. In part (c), there is only one arrangement of any set of 5 digits, while in part (b) each set of 5 digits gives 5! different outcomes.

1.3.5. You can make $\binom{7}{2}\binom{7}{2} = 441$ quadrilaterals.

There are 5 squares.

There are $\binom{7}{2}$ rectangles.

There are $\binom{7}{2} + (\binom{7}{2} - 1) + (\binom{7}{2} - 3) + (\binom{7}{2} - 6) + (\binom{7}{2} - 10) + (\binom{7}{2} - 15) = 91$ parallelograms.

All of the quadrilaterals are trapezoids. To count the non-parallelogram trapezoids, compute $441 - 91 = 350$.

1.3.6. 120.

1.3.7. Since there are 15 different letters, we have 15 choices for the first letter, 14 for the next, and so on. Thus there are 15! anagrams.

1.3.8. There are $\binom{7}{2} = 21$ anagrams starting with "a".

1.3.9. First, decide where to put the "a"s. There are 7 positions, and we must choose 3 of them to fill with an "a". This can be done in $\binom{7}{3}$ ways. The remaining 4 spots all get a different letter, so there are 4! ways to finish off the anagram. This gives a total of $\binom{7}{3} \cdot 4!$ anagrams. Strangely enough, this is 840, which is also equal to $P(7,4)$. To get the answer that way, start by picking one of the 7 *positions* to be filled by the "n", one of the remaining 6 positions to be filled by the "g", one of the remaining 5 positions to be filled by the "r", one of the remaining 4 positions to be filled by the "m" and then put "a"s in the remaining 3 positions.

1.3.10.

(a) $\binom{20}{4}\binom{16}{4}\binom{12}{4}\binom{8}{4}\binom{4}{4}$ ways.

(b) $5!\binom{15}{3}\binom{12}{3}\binom{9}{3}\binom{6}{3}\binom{3}{3}$ ways.

1.3.11. 9!.

1.3.12.

(a) 17^{10} functions. There are 17 choices for the image of each element in the domain.

(b) $P(17,10)$ injective functions. There are 17 choices for image of the first element of the domain, then only 16 choices for the second, and so on.

1.3.13.

(a) $6^4 = 1296$ functions.

(b) $P(6,4) = 6 \cdot 5 \cdot 4 \cdot 3 = 360$ functions.

(c) $\binom{6}{4} = 15$ functions.

1.4 Exercises

1.4.1.

Proof. Question: How many 2-letter words start with a, b, or c and end with either y or z?

Answer 1: There are two words that start with a, two that start with b, two that start with c, for a total of $2 + 2 + 2$.

Answer 2: There are three choices for the first letter and two choices for the second letter, for a total of $3 \cdot 2$.

Since the two answers are both answers to the same question, they are equal. Thus $2 + 2 + 2 = 3 \cdot 2$. ■

1.4.5.

(a) She has $\binom{15}{6}$ ways to select the 6 bridesmaids, and then for each way, has 6 choices for the maid of honor. Thus she has $\binom{15}{6}6$ choices.

(b) She has 15 choices for who will be her maid of honor. Then she needs to select 5 of the remaining 14 friends to be bridesmaids, which she can do in $\binom{14}{5}$ ways. Thus she has $15\binom{14}{5}$ choices.

(c) We have answered the question (how many wedding parties can the bride choose from) in two ways. The first way gives the left-hand side of the identity and the second way gives the right-hand side of the identity. Therefore the identity holds.

1.4.7.

Proof. Question: You have a large container filled with ping-pong balls, all with a different number on them. You must select k of the balls, putting two of them in a jar and the others in a box. How many ways can you do this?

Answer 1: First select 2 of the n balls to put in the jar. Then select $k - 2$ of the remaining $n - 2$ balls to put in the box. The first task can be completed in $\binom{n}{2}$ different ways, the second task in $\binom{n-2}{k-2}$ ways. Thus there are $\binom{n}{2}\binom{n-2}{k-2}$ ways to select the balls.

Answer 2: First select k balls from the n in the container. Then pick 2 of the k balls you picked to put in the jar, placing the remaining $k - 2$ in the box. The first task can be completed in $\binom{n}{k}$ ways, the second task in $\binom{k}{2}$ ways. Thus there are $\binom{n}{k}\binom{k}{2}$ ways to select the balls.

Since both answers count the same thing, they must be equal and the identity is established. ■

1.5 Exercises

1.5.1.

(a) $\binom{10}{5}$ sets. We must select 5 of the 10 digits to put in the set.

(b) Use stars and bars: each star represents one of the 5 elements of the set, each bar represents a switch between digits. So there are 5 stars and 9 bars, giving us $\binom{14}{9}$ sets.

1.5.2.

(a) There are $\binom{7}{5}$ numbers. We simply choose five of the seven digits and once chosen put them in increasing order.

(b) This requires stars and bars. Use a star to represent each of the 5 digits in the number, and use their position relative to the bars to say what numeral fills that spot. So we will have 5 stars and 6 bars, giving $\binom{11}{6}$ numbers.

1.5.3.

(a) You take 3 strawberry, 1 lime, 0 licorice, 2 blueberry and 0 bubblegum.

(b) This is backwards. We don't want the stars to represent the kids because the kids are not identical, but the stars are. Instead we should use 5 stars (for the lollipops) and use 5 bars to switch between the 6 kids. For example,

$$* * || * * * |||$$

would represent the outcome with the first kid getting 2 lollipops, the third kid getting 3, and the rest of the kids getting none.

(c) This is the word AAAEOO.

(d) This doesn't represent a solution. Each star should represent one of the 6 units that add up to 6, and the bars should *switch* between the different variables. We have one too many bars. An example of a correct diagram would be

$$*| * *|| * * * ,$$

representing that $x_1 = 1$, $x_2 = 2$, $x_3 = 0$, and $x_4 = 3$.

1.5.4.

(a) $\binom{18}{4}$ ways. Each outcome can be represented by a sequence of 14 stars and 4 bars.

(b) $\binom{13}{4}$ ways. First put one ball in each bin. This leaves 9 stars and 4 bars.

1.5.5.

(a) $\binom{7}{2}$ solutions. After each variable gets 1 star for free, we are left with 5 stars and 2 bars.

(b) $\binom{10}{2}$ solutions. We have 8 stars and 2 bars.

(c) $\binom{19}{2}$ solutions. This problem is equivalent to finding the number of solutions to $x' + y' + z' = 17$ where x', y' and z' are non-negative. (In fact, we really just do a substitution. Let $x = x' - 3$, $y = y' - 3$ and $z = z' - 3$).

1.5.6. $\binom{10}{5}$ outcomes.

1.5.7. There are $\binom{10}{3} = 120$ different combinations of coins possible. Thus you have a 1 in 120 chance of guessing correctly.

1.5.8. $\binom{18}{15}$ solutions. Distribute 10 units to the variables before finding all solutions to $x_1' + x_2' + x_3' + x_4' = 15$ in non-negative integers.

1.5.10.

(a) $\binom{10}{5}$. Note that a strictly increasing function is automatically injective.

(b) $\displaystyle\binom{14}{9}$.

1.5.11.

(a) $\binom{20}{4}$ sodas (order does not matter and repeats are not allowed).

(b) $P(20, 4) = 20 \cdot 19 \cdot 18 \cdot 17$ sodas (order matters and repeats are not allowed).

(c) $\binom{23}{4}$ sodas (order does not matter and repeats are allowed; 4 stars and 19 bars).

(d) 20^4 sodas (order matters and repeats are allowed; 20 choices 4 times).

1.6 Exercises

1.6.1.

(a) $\binom{9}{3}$ meals. First spend \$7 to buy one of each item, then use 3 stars to select items between 6 bars.

(b) $\binom{16}{6}$ meals. Here you have 10 stars and 6 bars (separating the 7 items).

(c) $\binom{16}{6} - \left[\binom{7}{1}\binom{13}{6} - \binom{7}{2}\binom{10}{6} + \binom{7}{3}\binom{7}{6}\right]$ meals. Use PIE to subtract all the meals in which you get 3 or more of a particular item.

1.6.3. $\binom{18}{4} - \left[\binom{5}{1}\binom{11}{4} - \binom{5}{2}\binom{4}{4}\right]$.

1.6.4. There are $\binom{10}{7} - \binom{4}{1}\binom{6}{3}$ solutions.

1.6.5. Without any restriction, there would be $\binom{19}{7}$ ways to distribute the stars. Now we must use PIE to eliminate all distributions in which one or more student gets more than one star:

$$\binom{19}{7} - \left[\binom{13}{1}\binom{17}{5} - \binom{13}{2}\binom{15}{3} + \binom{13}{3}\binom{13}{1}\right] = 1716.$$

Interestingly enough, this number is also the value of $\binom{13}{7}$, which makes sense: if each student can have at most one star, we must just pick the 7 out of 13 students to receive them.

1.6.7. The 9 derangements are: 2143, 2341, 2413, 3142, 3412, 3421, 4123, 4312, 4321.

1.6.8. First pick one of the five elements to be fixed. For each such choice, derange the remaining four, using the standard advanced PIE formula. We get $\binom{5}{1}\left(4! - \left[\binom{4}{1}3! - \binom{4}{2}2! + \binom{4}{3}1! - \binom{4}{4}0!\right]\right)$ permutations.

1.6.9. $\binom{10}{6}\left(4! - \left[\binom{4}{1}3! - \binom{4}{2}2! + \binom{4}{3}1! - \binom{4}{4}0!\right]\right)$ ways. We choose 6 of the 10 ladies to get their own hat, and the multiply by the number of ways the remaining hats can be deranged.

1.6.11. There are $5 \cdot 6^3$ functions for which $f(1) \neq a$ and another $5 \cdot 6^3$ functions for which $f(2) \neq b$. There are $5^2 \cdot 6^2$ functions for which both $f(1) \neq a$ and $f(2) \neq b$. So the total number of functions for which $f(1) \neq a$ or $f(2) \neq b$ or both is

$$5 \cdot 6^3 + 5 \cdot 6^3 - 5^2 \cdot 6^2 = 1260.$$

1.6.12. $5^{10} - \left[\binom{5}{1}4^{10} - \binom{5}{2}3^{10} + \binom{5}{3}2^{10} - \binom{5}{4}1^{10}\right]$ functions. The 5^{10} is all the functions from A to B. We subtract those that aren't surjective. Pick one of the five elements in B to not have in the range (in $\binom{5}{1}$ ways) and count all those functions (4^{10}). But this overcounts the functions where two elements from B are excluded from the range, so subtract those. And so on, using PIE.

1.6.13. $5! - \left[\binom{5}{1}4! - \binom{5}{2}3! + \binom{5}{3}2! - \binom{5}{4}1! + \binom{5}{5}0!\right]$ functions.

1.7 Chapter Review

1.7.1.

(a) $\binom{8}{5}$ ways, after giving one present to each kid, you are left with 5 presents (stars) which need to be divide among the 4 kids (giving 3 bars).

(b) $\binom{12}{9}$ ways. You have 9 stars and 3 bars.

(c) 4^9. You have 4 choices for whom to give each present. This is like making a function from the set of presents to the set of kids.

(d) $4^9 - \left[\binom{4}{1}3^9 - \binom{4}{2}2^9 + \binom{4}{3}1^9\right]$ ways. Now the function from the set of presents to the set of kids must be surjective.

1.7.2.

(a) Neither. $\binom{14}{4}$ paths.

(b) $\binom{10}{4}$ bow ties.

(c) $P(10,4)$, since order is important.

(d) Neither. Assuming you will wear each of the 4 ties on just 4 of the 7 days, without repeats: $\binom{10}{4}P(7,4)$.

(e) $P(10,4)$.

(f) $\binom{10}{4}$.

(g) Neither. Since you could repeat letters: 10^4. If no repeats are allowed, it would be $P(10,4)$.

(h) Neither. Actually, "k" is the 11th letter of the alphabet, so the answer is 0. If "k" was among the first 10 letters, there would only be 1 way - write it down.

(i) Neither. Either $\binom{9}{3}$ (if every kid gets an apple) or $\binom{13}{3}$ (if appleless kids are allowed).

(j) Neither. Note that this could not be $\binom{10}{4}$ since the 10 things and 4 things are from different groups. 4^{10}, assuming each kid eats one type of cerial.

(k) $\binom{10}{4}$ - don't be fooled by the "arrange" in there - you are picking 4 out of 10 *spots* to put the 1's.

(l) $\binom{10}{4}$ (assuming order is irrelevant).

(m) Neither. 16^{10} (each kid chooses yes or no to 4 varieties).

(n) Neither. 0.

(o) Neither. $4^{10} - [\binom{4}{1}3^{10} - \binom{4}{2}2^{10} + \binom{4}{3}1^{10}]$.

(p) Neither. $10 \cdot 4$.

(q) Neither. 4^{10}.

(r) $\binom{10}{4}$ (which is the same as $\binom{10}{6}$).

(s) Neither. If all the kids were identical, and you wanted no empty teams, it would be $\binom{10}{4}$. Instead, this will be the same as the number of surjective functions from a set of size 11 to a set of size 5.

(t) $\binom{10}{4}$.

(u) $\binom{10}{4}$.

(v) Neither. 4!.

(w) Neither. It's $\binom{10}{4}$ if you won't repeat any choices. If repetition is allowed, then this becomes $x_1 + x_2 + \cdots + x_{10} = 4$, which has $\binom{13}{9}$ solutions in non-negative integers.

(x) Neither. Since repetition of cookie type is allowed, the answer is 10^4. Without repetition, you would have $P(10, 4)$.

(y) $\binom{10}{4}$ since that is equal to $\binom{9}{4} + \binom{9}{3}$.

(z) Neither. It will be a complicated (possibly PIE) counting problem.

1.7.3.

(a) $2^8 = 256$ choices. You have two choices for each tie: wear it or don't.

(b) You have 7 choices for regular ties (the 8 choices less the "no regular tie" option) and 31 choices for bow ties (32 total minus the "no bow tie" option). Thus total you have $7 \cdot 31 = 217$ choices.

(c) $\binom{3}{2}\binom{5}{3} = 30$ choices.

(d) Select one of the 3 bow ties to go on top. There are then 4 choices for the next tie, 3 for the tie after that, and so on. Thus $3 \cdot 4! = 72$ choices.

1.7.4. You own 8 purple bow ties, 3 red bow ties, 3 blue bow ties and 5 green bow ties. How many ways can you select one of each color bow tie to take with you on a trip? $8 \cdot 3 \cdot 3 \cdot 5$ ways. How many choices do you have for a single bow tie to wear tomorrow? $8 + 3 + 3 + 5$ choices.

1.7.5.

(a) 4^5 numbers.

(b) $4^4 \cdot 2$ numbers (choose any digits for the first four digits - then pick either an even or an odd last digit to make the sum even).

(c) We need 3 or more even digits. 3 even digits: $\binom{5}{3}2^3 2^2$. 4 even digits: $\binom{5}{4}2^4 2$. 5 even digits: $\binom{5}{5}2^5$. So all together: $\binom{5}{3}2^3 2^2 + \binom{5}{4}2^4 2 + \binom{5}{5}2^5$ numbers.

1.7.6. 51 passengers. We are asking for the size of the union of three non-disjoint sets. Using PIE, we have $25 + 30 + 20 - 10 - 12 - 7 + 5 = 51$.

1.7.7.

(a) 2^8 strings.

(b) $\binom{8}{5}$ strings.

(c) $\binom{8}{5}$ strings.

(d) There is a bijection between subsets and bit strings: a 1 means that element in is the subset, a 0 means that element is not in the subset. To get a subset of an 8 element set we have an 8-bit string. To make sure the subset contains exactly 5 elements, there must be 5 1's, so the weight must be 5.

1.7.8. $\binom{13}{10} + \binom{17}{8}$.

1.7.9. With repeated letters allowed, we select which 5 of the 8 letters will be vowels, then pick one of the 5 vowels for each spot, and finally pick one of the other 21 letters for each of the remaining 3 spots. Thus, $\binom{8}{5}5^5 21^3$ words.

Without repeats, we still pick the positions of the vowels, but now each time we place one there, there is one fewer choice for the next one. Similarly, we cannot repeat the consonants. We get $\binom{8}{5}5!P(21,3)$ words.

1.7.10.

(a) $\binom{5}{2}\binom{11}{6}$ paths.

(b) $\binom{16}{8} - \binom{12}{7}\binom{4}{1}$ paths.

(c) $\binom{5}{2}\binom{11}{6} + \binom{12}{5}\binom{4}{3} - \binom{5}{2}\binom{7}{3}\binom{4}{3}$ paths.

1.7.11. $\binom{18}{8}\left(\binom{18}{8} - 1\right)$ routes. For each of the $\binom{18}{8}$ routes to work there is exactly one fewer route back.

1.7.12. $2^7 + 2^7 - 2^4$ strings (using PIE).

1.7.13. $\binom{7}{3} + \binom{7}{4} - \binom{4}{1}$ strings.

1.7.14. There are 4 spots to start the word, and then there are 3! ways to arrange the other letters in the remaining three spots. Thus the number of words avoiding the sub-word "bad" in consecutive letters is $6! - 4 \cdot 3!$.

If we now need to avoid words that put "b" before "a" before "d", we must choose which spots those letters go (in that order) and then arrange the remaining three letters. Thus, $6! - \binom{6}{3}3!$ words.

1.7.15. 2^n is the number of lattice paths which have length n, since for each step you can go up or right. Such a path would end along the line

$x + y = n$. So you will end at $(0, n)$, or $(1, n-1)$ or $(2, n-2)$ or ... or $(n, 0)$. Counting the paths to each of these points separately, give $\binom{n}{0}$, $\binom{n}{1}$, $\binom{n}{2}$, ..., $\binom{n}{n}$ (each time choosing which of the n steps to be to the right). These two methods count the same quantity, so are equal.

1.7.16.

(a) $\binom{19}{15}$ ways.

(b) $\binom{24}{20}$ ways.

(c) $\binom{19}{15} - \left[\binom{5}{1}\binom{12}{8} - \binom{5}{2}\binom{5}{1}\right]$ ways.

1.7.17.

(a) $5^4 + 5^4 - 5^3$ functions.

(b) $4 \cdot 5^4 + 5 \cdot 4 \cdot 5^3 - 4 \cdot 4 \cdot 5^3$ functions.

(c) $5! - [4! + 4! - 3!]$ functions. Note we use factorials instead of powers because we are looking for injective functions.

(d) Note that being surjective here is the same as being injective, so we can start with all 5! injective functions and subtract those which have one or more "fixed point". We get $5! - \left[\binom{5}{1}4! - \binom{5}{2}3! + \binom{5}{3}2! - \binom{5}{4}1! + \binom{5}{5}0!\right]$ functions.

1.7.18. $4^6 - \left[\binom{4}{1}3^6 - \binom{4}{2}2^6 + \binom{4}{3}1^6\right]$.

1.7.19.

(a) $\binom{10}{4}$ combinations. You need to choose 4 of the 10 cookie types. Order doesn't matter.

(b) $P(10, 4) = 10 \cdot 9 \cdot 8 \cdot 7$ ways. You are choosing and arranging 4 out of 10 cookies. Order matters now.

(c) $\binom{21}{12}$ choices. You must switch between cookie type 9 times as you make your 12 cookies. The cookies are the stars, the switches between cookie types are the bars.

(d) 10^{12} choices. You have 10 choices for the "1" cookie, 10 choices for the "2" cookie, and so on.

(e) $10^{12} - \left[\binom{10}{1}9^{12} - \binom{10}{2}8^{12} + \cdots - \binom{10}{10}0^{12}\right]$ choices. We must use PIE to remove all the ways in which one or more cookie type is not selected.

1.7.20.

(a) You are giving your professor 4 types of cookies coming from 10 different types of cookies. This does not lend itself well to a function interpretation. We *could* say that the domain contains the 4 types you will give your professor and the codomain contains the 10 you can choose from, but then counting injections would be too much (it doesn't matter if you pick type 3 first and type 2 second, or the other way around, just that you pick those two types).

(b) We want to consider injective functions from the set {most, second most, second least, least} to the set of 10 cookie types. We want injections because we cannot pick the same type of cookie to give most and least of (for example).

(c) This is not a good problem to interpret as a function. The problem is that the domain would have to be the 12 cookies you bake, but these elements are indistinguishable (there is not a first cookie, second cookie, etc.).

(d) The domain should be the 12 shapes, the codomain the 10 types of cookies. Since we can use the same type for different shapes, we are interested in counting all functions here.

(e) Here we insist that each type of cookie be given at least once, so now we are asking for the number of surjections of those functions counted in the previous part.

2.1 Exercises

2.1.1.

(a) Note that if we subtract 1 from each term, we get the square numbers. Thus $a_n = n^2 + 1$.

(b) These look like the triangular numbers, only shifted by 1. We get: $a_n = \frac{n(n+1)}{2} - 1$.

(c) If you subtract 2 from each term, you get triangular numbers, only starting with 6 instead of 1. So we must shift vertically and horizontally. $a_n = \frac{(n+2)(n+3)}{2} + 2$.

(d) These seem to grow very quickly. Further, if we add 1 to each term, we find the factorials, although starting with 2 instead of 1. This gives, $a_n = (n+1)! - 1$ (where $n! = 1 \cdot 2 \cdot 3 \cdots n$).

2.1.3.

(a) $a_0 = 0$, $a_1 = 1$, $a_2 = 3$, $a_3 = 6$ $a_4 = 10$. The sequence was described by a closed formula. These are the triangular numbers. A recursive definition is: $a_n = a_{n-1} + n$ with $a_0 = 0$.

(b) This is a recursive definition. We continue $a_2 = 2$, $a_3 = 3$, $a_4 = 4$, $a_5 = 5$, and so on. A closed formula is $a_n = n$.

(c) We have $a_0 = 1$, $a_1 = 1$, $a_2 = 2$, $a_3 = 6$, $a_4 = 24$, $a_5 = 120$, and so on. The closed formula is $a_n = n!$.

2.1.4.

(a) The recursive definition is $a_n = a_{n-1} + 2$ with $a_1 = 1$. A closed formula is $a_n = 2n - 1$.

(b) The sequence of partial sums is $1, 4, 9, 16, 25, 36, \ldots$. A recursive definition is (as always) $b_n = b_{n-1} + a_n$ which in this case is $b_n = b_{n-1} + 2n - 1$. It appears that the closed formula is $b_n = n^2$

2.1.5.

(a) $0, 1, 2, 4, 7, 12, 20, \ldots$.

(b) $F_0 + F_1 + \cdots + F_n = F_{n+2} - 1$.

2.1.6. The sequences all have the same recurrence relation: $a_n = a_{n-1} + a_{n-2}$ (the same as the Fibonacci numbers). The only difference is the initial conditions.

2.1.7. $3, 10, 24, 52, 108, \ldots$. The recursive definition for $10, 24, 52, \ldots$ is $a_n = 2a_{n-1} + 4$ with $a_1 = 10$.

2.1.8. $-1, -1, 1, 5, 11, 19, \ldots$ Thus the sequence $0, 2, 6, 12, 20, \ldots$ has closed formula $a_n = (n+1)^2 - 3(n+1) + 2$.

2.1.9. This closed formula would have $a_{n-1} = 3 \cdot 2^{n-1} + 7 \cdot 5^{n-1}$ and $a_{n-2} = 3 \cdot 2^{n-2} + 7 \cdot 5^{n-2}$. Then we would have

$$\begin{aligned}
7a_{n-1} - 10a_{n-2} &= 7(3 \cdot 2^{n-1} + 7 \cdot 5^{n-1}) - 10(3 \cdot 2^{n-2} + 7 \cdot 5^{n-2}) \\
&= 21 \cdot 2^{n-1} + 49 \cdot 5^{n-1} - 30 \cdot 2^{n-2} - 70 \cdot 5^{n-2}) \\
&= 21 \cdot 2^{n-1} + 49 \cdot 5^{n-1} - 15 \cdot 2^{n-1} - 14 \cdot 5^{n-1}) \\
&= 6 \cdot 2^{n-1} + 35 \cdot 5^{n-1} \\
&= 3 \cdot 2^n + 7 \cdot 5^n = a_n.
\end{aligned}$$

So the closed formula agrees with the recurrence relation. The closed formula has initial terms $a_0 = 10$ and $a_1 = 41$.

2.1.13.

(a) $\displaystyle\sum_{k=1}^{n} 2k$.

(b) $\displaystyle\sum_{k=1}^{107} (1 + 4(k-1))$.

(c) $\displaystyle\sum_{k=1}^{50} \frac{1}{k}$.

(d) $\displaystyle\prod_{k=1}^{n} 2k$.

(e) $\displaystyle\prod_{k=1}^{100} \frac{k}{k+1}$.

2.1.14.

(a) $\sum_{k=1}^{100}(3+4k) = 7+11+15+\cdots+403.$

(b) $\sum_{k=0}^{n} 2^k = 1+2+4+8+\cdots+2^n.$

(c) $\sum_{k=2}^{50} \frac{1}{(k^2-1)} = 1+\frac{1}{3}+\frac{1}{8}+\frac{1}{15}+\cdots+\frac{1}{2499}.$

(d) $\prod_{k=2}^{100} \frac{k^2}{(k^2-1)} = \frac{4}{3}\cdot\frac{9}{8}\cdot\frac{16}{15}\cdots\frac{10000}{9999}.$

(e) $\prod_{k=0}^{n}(2+3k) = (2)(5)(8)(11)(14)\cdots(2+3n).$

2.2 Exercises

2.2.1.

(a) $a_n = a_{n-1}+4$ with $a_1 = 5$.

(b) $a_n = 5+4(n-1)$.

(c) Yes, since $2013 = 5+4(503-1)$ (so $a_{503} = 2013$).

(d) 133

(e) $\frac{538\cdot 133}{2} = 35777$.

(f) $b_n = 1+\frac{(4n+6)n}{2}$.

2.2.2.

(a) 32, which is 26 + 6.

(b) The sequence is arithmetic, with $a_0 = 8$ and constant difference 6, so $a_n = 8+6n$.

(c) 30500. We want $8+14+\cdots+602$. Reverse and add to get 100 sums of 610, a total of 61000, which is twice the sum we are looking for.

2.2.3.

(a) 36.

(b) $\frac{253\cdot 36}{2} = 4554$.

2.2.4.

(a) $n+2$ terms, since to get 1 using the formula $6n+7$ we must use $n=-1$. Thus we have n terms, plus two, when $n=0$ and $n=-1$.

(b) $6n + 1$, which is 6 less than $6n + 7$ (or plug in $n - 1$ for n).

(c) $\frac{(6n+8)(n+2)}{2}$. Reverse and add. Each sum gives the constant $6n + 8$ and there are $n + 2$ terms.

2.2.5. 68117.

2.2.6. $\frac{5 \cdot 3^{21} - 5}{2}$. Let the sum be S, and compute $S - 3S = -2S$, which causes terms except 5 and $-5 \cdot 3^{21}$ to cancel. Then solve for S.

2.2.7. $\frac{1 + \frac{2^{31}}{3^{31}}}{5/3}$. This time compute $S + \frac{2}{3}S$.

2.2.8. For arithmetic: $x = 55/3$, $y = 29/3$. For geometric: $x = 9$ and $y = 3$.

2.2.9. For arithmetic: $x = 14$, $y = 23$. For geometric: $x = 5 * (32/5)^(1/3)$ and $y = 5 * (32/5)^(2/3)$.

2.2.11. We have $2 = 2$, $7 = 2 + 5$, $15 = 2 + 5 + 8$, $26 = 2 + 5 + 8 + 11$, and so on. The terms in the sums are given by the arithmetic sequence $b_n = 2 + 3n$. In other words, $a_n = \sum_{k=0}^{n}(2 + 3k)$. To find the closed formula, we reverse and add. We get $a_n = \frac{(4+3n)(n+1)}{2}$ (we have $n + 1$ there because there are $n + 1$ terms in the sum for a_n).

2.3 Exercises

2.3.1. $a_n = n^2 + n$. Here we know that we are looking for a quadratic because the second differences are constant. So $a_n = an^2 + bn + c$. Since $a_0 = 0$, we know $c = 0$. So just solve the system

$$2 = a + b$$
$$6 = 4a + 2b$$

2.3.2. $a_n = \frac{1}{6}(n^3 + 5n + 6)$.

2.3.3. $a_n = \frac{1}{6}(n^3 + 6n^2 + 11n + 12)$.

2.3.4. $a_n = \frac{1}{6}(n^3 + 6n^2 + 11n + 18)$.

2.3.6. $a_n = n^2 - n + 1$.

2.3.7. $a_n = n^3 + n^2 - n + 1$

2.3.8. $a_{n-1} = (n-1)^2 + 3(n-1) + 4 = n^2 + n + 2$. Thus $a_n - a_{n-1} = 2n + 2$. Note that this is linear (arithmetic). We can check that we are correct. The sequence a_n is $4, 8, 14, 22, 32, \ldots$ and the sequence of differences is thus $4, 6, 8, 10, \ldots$ which agrees with $2n + 2$ (if we start at $n = 1$).

2.3.9. $a_{n-1} = a(n-1)^2 + b(n-1) + c = an^2 - 2an + a + bn - b + c$. Therefore $a_n - a_{n-1} = 2an - a + b$, which is arithmetic. Notice that this is not quite the derivative of a_n, which would be $2an + b$, but it is close.

2.3.10. No. The sequence of differences is the same as the original sequence so no differences will be constant.

2.3.11. No. The sequence is geometric, and in fact has closed formula $2 \cdot 3^n$. This is an exponential function, which is not equal to any polynomial of any degree. If the nth sequence of differences was constant, then the closed formula for the original sequence would be a degree n polynomial.

2.4 Exercises

2.4.1. 171 and 341. $a_n = a_{n-1} + 2a_{n-2}$ with $a_0 = 3$ and $a_1 = 5$. Closed formula: $a_n = \frac{8}{3}2^n + \frac{1}{3}(-1)^n$. To find this solve the characteristic equation, $x^2 - x - 2 = 0$, to get characteristic roots $x = 2$ and $x = -1$. Then solve the system

$$3 = a + b$$
$$5 = 2a - b$$

2.4.3. $a_n = 3 + 2^{n+1}$. We should use telescoping or iteration here. For example, telescoping gives

$$\begin{aligned} a_1 - a_0 &= 2^1 \\ a_2 - a_1 &= 2^2 \\ a_3 - a_2 &= 2^3 \\ &\vdots \\ a_n - a_{n-1} &= 2^n \end{aligned}$$

which sums to $a_n - a_0 = 2^{n+1} - 2$ (using the multiply-shift-subtract technique from Section 3.2 for the right-hand side). Substituting $a_0 = 5$ and solving for a_n completes the solution.

2.4.4. We claim $a_n = 4^n$ works. Plug it in: $4^n = 3(4^{n-1}) + 4(4^{n-2})$. This works - just simplify the right-hand side.

2.4.5. By the Characteristic Root Technique. $a_n = 4^n + (-1)^n$.

2.4.6. $a_n = \frac{13}{5}4^n + \frac{12}{5}(-1)^n$.

2.4.7. $a_n = \frac{19}{7}(-2)^n + \frac{9}{7}5^n$.

2.4.10.

(a) $a_n = 4a_{n-1} + 5a_{n-2}$.

(b) 4, 21, 104, 521, 2604, 13021

(c) $a_n = \frac{5}{6}5^n + \frac{1}{6}(-1)^n$.

2.4.12. We have characteristic polynomial $x^2 - 2x + 1$, which has $x = 1$ as the only repeated root. Thus using the characteristic root technique for repeated roots, the general solution is $a_n = a + bn$ where a and b depend on the initial conditions.

(a) $a_n = 1 + n$.

(b) For example, we could have $a_0 = 21$ and $a_1 = 22$.

(c) For every x. Take $a_0 = x - 9$ and $a_1 = x - 8$.

2.5 Exercises

2.5.1.

(a) If we have a number of beans ending in a 5 and we double it, we will get a number of beans ending in a 0 (since $5 \cdot 2 = 10$). Then if we subtract 5, we will once again get a number of beans ending in a 5. Thus if on any day we have a number ending in a 5, the next day will also have a number ending in a 5.

(b) If you don't *start* with a number of beans ending in a 5 (on day 1), the above reasoning is still correct but not helpful. For example, if you start with a number ending in a 3, the next day you will have a number ending in a 1.

(c) Part (b) is the base case and part (a) is the inductive case. If on day 1 we have a number ending in a 5 (by part (b)), then on day 2 we will also have a number ending in a 5 (by part (a)). Then by part (a) again, we will have a number ending in a 5 on day 3. By part (a) again, this means we will have a number ending in a 5 on day 4

The proof by induction would say that on *every* day we will have a number ending in a 5, and this works because we can start with the base case, then use the inductive case over and over until we get up to our desired n.

2.5.2.

Proof. We must prove that $1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1$ for all $n \in \mathbb{N}$. Thus let $P(n)$ be the statement $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$. We will prove that $P(n)$ is true for all $n \in \mathbb{N}$. First we establish the base case, $P(0)$, which claims that $1 = 2^{0+1} - 1$. Since $2^1 - 1 = 2 - 1 = 1$, we see that $P(0)$ is true. Now for the inductive case. Assume that $P(k)$ is true for an arbitrary $k \in \mathbb{N}$. That is, $1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$. We must show that $P(k + 1)$ is true (i.e., that $1 + 2 + 2^2 + \cdots + 2^{k+1} = 2^{k+2} - 1$). To do this, we start with the left-hand side of $P(k + 1)$ and work to the right-hand side:

$$\begin{aligned} 1 + 2 + 2^2 + \cdots + 2^k + 2^{k+1} &= 2^{k+1} - 1 + 2^{k+1} \quad \text{by inductive hypothesis} \\ &= 2 \cdot 2^{k+1} - 1 \end{aligned}$$

$$= 2^{k+2} - 1$$

Thus $P(k+1)$ is true so by the principle of mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$. ∎

2.5.3.

Proof. Let $P(n)$ be the statement "$7^n - 1$ is a multiple of 6." We will show $P(n)$ is true for all $n \in \mathbb{N}$. First we establish the base case, $P(0)$. Since $7^0 - 1 = 0$, and 0 is a multiple of 6, $P(0)$ is true. Now for the inductive case. Assume $P(k)$ holds for an arbitrary $k \in \mathbb{N}$. That is, $7^k - 1$ is a multiple of 6, or in other words, $7^k - 1 = 6j$ for some integer j. Now consider $7^{k+1} - 1$:

$$\begin{aligned} 7^{k+1} - 1 &= 7^{k+1} - 7 + 6 && \text{by cleverness: } -1 = -7 + 6 \\ &= 7(7^k - 1) + 6 && \text{factor out a 7 from the first two terms} \\ &= 7(6j) + 6 && \text{by the inductive hypothesis} \\ &= 6(7j + 1) && \text{factor out a 6} \end{aligned}$$

Therefore $7^{k+1} - 1$ is a multiple of 6, or in other words, $P(k+1)$ is true. Therefore by the principle of mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$. ∎

2.5.4.

Proof. Let $P(n)$ be the statement $1 + 3 + 5 + \cdots + (2n - 1) = n^2$. We will prove that $P(n)$ is true for all $n \geq 1$. First the base case, $P(1)$. We have $1 = 1^2$ which is true, so $P(1)$ is established. Now the inductive case. Assume that $P(k)$ is true for some fixed arbitrary $k \geq 1$. That is, $1 + 3 + 5 + \cdots + (2k - 1) = k^2$. We will now prove that $P(k+1)$ is also true (i.e., that $1 + 3 + 5 + \cdots + (2k + 1) = (k + 1)^2$). We start with the left-hand side of $P(k+1)$ and work to the right-hand side:

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) &= k^2 + (2k + 1) && \text{by ind. hyp.} \\ &= (k + 1)^2 && \text{by factoring} \end{aligned}$$

Thus $P(k+1)$ holds, so by the principle of mathematical induction, $P(n)$ is true for all $n \geq 1$. ∎

2.5.5.

Proof. Let $P(n)$ be the statement $F_0 + F_2 + F_4 + \cdots + F_{2n} = F_{2n+1} - 1$. We will show that $P(n)$ is true for all $n \geq 0$. First the base case is easy because $F_0 = 0$ and $F_1 = 1$ so $F_0 = F_1 - 1$. Now consider the inductive case. Assume $P(k)$ is true, that is, assume $F_0 + F_2 + F_4 + \cdots + F_{2k} = F_{2k+1} - 1$. To establish $P(k+1)$ we work from left to right:

$$\begin{aligned} F_0 + F_2 + \cdots + F_{2k} + F_{2k+2} &= F_{2k+1} - 1 + F_{2k+2} && \text{by ind. hyp.} \\ &= F_{2k+1} + F_{2k+2} - 1 \end{aligned}$$

$$= F_{2k+3} - 1 \qquad \text{by recursive def.}$$

Therefore $F_0 + F_2 + F_4 + \cdots + F_{2k+2} = F_{2k+3} - 1$, which is to say $P(k+1)$ holds. Therefore by the principle of mathematical induction, $P(n)$ is true for all $n \geq 0$. ■

2.5.6.

Proof. Let $P(n)$ be the statement $2^n < n!$. We will show $P(n)$ is true for all $n \geq 4$. First, we check the base case and see that yes, $2^4 < 4!$ (as $16 < 24$) so $P(4)$ is true. Now for the inductive case. Assume $P(k)$ is true for an arbitrary $k \geq 4$. That is, $2^k < k!$. Now consider $P(k+1)$: $2^{k+1} < (k+1)!$. To prove this, we start with the left side and work to the right side.

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &< 2 \cdot k! && \text{by the inductive hypothesis} \\ &< (k+1) \cdot k! && \text{since } k+1 > 2 \\ &= (k+1)! \end{aligned}$$

Therefore $2^{k+1} < (k+1)!$ so we have established $P(k+1)$. Thus by the principle of mathematical induction $P(n)$ is true for all $n \geq 4$. ■

2.5.12. The only problem is that we never established the base case. Of course, when $n = 0$, $0 + 3 \neq 0 + 7$.

2.5.13.

Proof. Let $P(n)$ be the statement that $n + 3 < n + 7$. We will prove that $P(n)$ is true for all $n \in \mathbb{N}$. First, note that the base case holds: $0 + 3 < 0 + 7$. Now assume for induction that $P(k)$ is true. That is, $k + 3 < k + 7$. We must show that $P(k+1)$ is true. Now since $k + 3 < k + 7$, add 1 to both sides. This gives $k + 3 + 1 < k + 7 + 1$. Regrouping $(k+1) + 3 < (k+1) + 7$. But this is simply $P(k+1)$. Thus by the principle of mathematical induction $P(n)$ is true for all $n \in \mathbb{N}$. ■

2.5.14. The problem here is that while $P(0)$ is true, and while $P(k) \rightarrow P(k+1)$ for *some* values of k, there is at least one value of k (namely $k = 99$) when that implication fails. For a valid proof by induction, $P(k) \rightarrow P(k+1)$ must be true for all values of k greater than or equal to the base case.

2.5.16. We once again failed to establish the base case: when $n = 0$, $n^2 + n = 0$ which is even, not odd.

2.5.19. The proof will be by strong induction.

Proof. Let $P(n)$ be the statement "n is either a power of 2 or can be written as the sum of distinct powers of 2." We will show that $P(n)$ is true for all $n \geq 1$.

Base case: $1 = 2^0$ is a power of 2, so $P(1)$ is true.

Inductive case: Suppose $P(k)$ is true for all $k < n$. Now if n is a power of 2, we are done. If not, let 2^x be the largest power of 2 strictly less than n. Consider $n - 2^x$, which is a smaller number, in fact smaller than both n and 2^x. Thus $n - 2^x$ is either a power of 2 or can be written as the sum of distinct powers of 2, but none of them are going to be 2^x, so the together with 2^x we have written n as the sum of distinct powers of 2.

Therefore, by the principle of (strong) mathematical induction, $P(n)$ is true for all $n \geq 1$. ∎

2.5.25. The idea here is that if we take the logarithm of a^n, we can increase n by 1 if we multiply by another a (inside the logarithm). This results in adding 1 more $\log(a)$ to the total.

Proof. Let $P(n)$ be the statement $\log(a^n) = n\log(a)$. The base case, $P(2)$ is true, because $\log(a^2) = \log(a \cdot a) = \log(a) + \log(a) = 2\log(a)$, by the product rule for logarithms. Now assume, for induction, that $P(k)$ is true. That is, $\log(a^k) = k\log(a)$. Consider $\log(a^{k+1})$. We have

$$\log(a^{k+1}) = \log(a^k \cdot a) = \log(a^k) + \log(a) = k\log(a) + \log(a),$$

with the last equality due to the inductive hypothesis. But this simplifies to $(k+1)\log(a)$, establishing $P(k+1)$. Therefore by the principle of mathematical induction, $P(n)$ is true for all $n \geq 2$. ∎

2.6 Chapter Review

2.6.1. $\frac{430 \cdot 107}{2} = 23005$.

2.6.2.

(a) $n + 2$ terms.

(b) $4n + 2$.

(c) $\dfrac{(4n+8)(n+2)}{2}$.

2.6.3.

(a) $2, 10, 50, 250, \ldots$ The sequence is geometric.

(b) $\dfrac{2 - 2 \cdot 5^{25}}{-4}$.

2.6.5. $a_n = n^2 + 4n - 1$.

2.6.6.

(a) The sequence of partial sums will be a degree 4 polynomial (its sequence of differences will be the original sequence).

(b) The sequence of second differences will be a degree 1 polynomial - an arithmetic sequence.

2.6.7.

(a) $4, 6, 10, 16, 26, 42, \ldots$.

(b) No, taking differences gives the original sequence back, so the differences will never be constant.

2.6.8. $b_n = (n + 3)n$.

2.6.10.

(a) $1, 2, 16, 68, 364, \ldots$.

(b) $a_n = \frac{3}{7}(-2)^n + \frac{4}{7}5^n$.

2.6.11.

(a) $a_2 = 14$. $a_3 = 52$.

(b) $a_n = \frac{1}{6}(-2)^n + \frac{5}{6}4^n$.

2.6.12.

(a) On the first day, your 2 mini bunnies become 2 large bunnies. On day 2, your two large bunnies produce 4 mini bunnies. On day 3, you have 4 mini bunnies (produced by your 2 large bunnies) plus 6 large bunnies (your original 2 plus the 4 newly matured bunnies). On day 4, you will have 12 mini bunnies (2 for each of the 6 large bunnies) plus 10 large bunnies (your previous 6 plus the 4 newly matured). The sequence of total bunnies is $2, 2, 6, 10, 22, 42 \ldots$ starting with $a_0 = 2$ and $a_1 = 2$.

(b) $a_n = a_{n-1} + 2a_{n-2}$. This is because the number of bunnies is equal to the number of bunnies you had the previous day (both mini and large) plus 2 times the number you had the day before that (since all bunnies you had 2 days ago are now large and producing 2 new bunnies each).

(c) Using the characteristic root technique, we find $a_n = a2^n + b(-1)^n$, and we can find a and b to give $a_n = \frac{4}{3}2^n + \frac{2}{3}(-1)^n$.

2.6.17. Let $P(n)$ be the statement, "every set containing n elements has 2^n different subsets." We will show $P(n)$ is true for all $n \geq 1$. Base case: Any set with 1 element $\{a\}$ has exactly 2 subsets: the empty set and the set itself. Thus the number of subsets is $2 = 2^1$. Thus $P(1)$ is true. Inductive case: Suppose $P(k)$ is true for some arbitrary $k \geq 1$. Thus every set containing exactly k elements has 2^k different subsets. Now consider a set containing $k + 1$ elements: $A = \{a_1, a_2, \ldots, a_k, a_{k+1}\}$. Any subset of A must either contain a_{k+1} or not. In other words, a subset of A is just a subset of $\{a_1, a_2, \ldots, a_k\}$ with or without a_{k+1}. Thus there are 2^k subsets of A which contain a_{k+1} and another 2^{k+1} subsets of A which do not contain

a^{k+1}. This gives a total of $2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$ subsets of A. But our choice of A was arbitrary, so this works for any subset containing $k+1$ elements, so $P(k+1)$ is true. Therefore, by the principle of mathematical induction, $P(n)$ is true for all $n \geq 1$.

3.1 Exercises

3.1.1.

(a) P: it's your birthday; Q: there will be cake. $(P \vee Q) \to Q$

(b) Hint: you should get three T's and one F.

(c) Only that there will be cake.

(d) It's NOT your birthday!

(e) It's your birthday, but the cake is a lie.

3.1.2.

P	Q	$(P \vee Q) \to (P \wedge Q)$
T	T	T
T	F	F
F	T	F
F	F	T

3.1.3.

P	Q	$\neg P \wedge (Q \to P)$
T	T	F
T	F	F
F	T	F
F	F	T

If the statement is true, then both P and Q are false.

3.1.6. Make a truth table for each and compare. The statements are logically equivalent.

3.1.8.

(a) $P \wedge Q$.

(b) $(\neg P \vee \neg R) \to (Q \vee \neg R)$ or, replacing the implication with a disjunction first: $(P \wedge Q) \vee (Q \vee \neg R)$.

(c) $(P \wedge Q) \wedge (R \wedge \neg R)$. This is necessarily false, so it is also equivalent to $P \wedge \neg P$.

(d) Either Sam is a woman and Chris is a man, or Chris is a woman.

3.1.12. The deduction rule is valid. To see this, make a truth table which contains $P \vee Q$ and $\neg P$ (and P and Q of course). Look at the truth value of Q in each of the rows that have $P \vee Q$ and $\neg P$ true.

3.1.16.

(a) $\forall x \exists y(O(x) \wedge \neg E(y))$.

(b) $\exists x \forall y(x \geq y \vee \forall z(x \geq z \wedge y \geq z))$.

(c) There is a number n for which every other number is strictly greater than n.

(d) There is a number n which is not between any other two numbers.

3.2 Exercises

3.2.1.

(a) For all integers a and b, if a or b is not even, then $a + b$ is not even.

(b) For all integers a and b, if a and b are even, then $a + b$ is even.

(c) There are numbers a and b such that $a + b$ is even but a and b are not both even.

(d) False. For example, $a = 3$ and $b = 5$. $a + b = 8$, but neither a nor b are even.

(e) False, since it is equivalent to the original statement.

(f) True. Let a and b be integers. Assume both are even. Then $a = 2k$ and $b = 2j$ for some integers k and j. But then $a+b = 2k+2j = 2(k+j)$ which is even.

(g) True, since the statement is false.

3.2.2.

(a) Proof by contradiction. Start of proof: Assume, for the sake of contradiction, that there are integers x and y such that x is a prime greater than 5 and $x = 6y+3$. End of proof: ... this is a contradiction, so there are no such integers.

(b) Direct proof. Start of proof: Let n be an integer. Assume n is a multiple of 3. End of proof: Therefore n can be written as the sum of consecutive integers.

(c) Proof by contrapositive. Start of proof: Let a and b be integers. Assume that a and b are even. End of proof: Therefore $a^2 + b^2$ is even.

3.2.3.

(a) Direct proof.

Proof. Let n be an integer. Assume n is even. Then $n = 2k$ for some integer k. Thus $8n = 16k = 2(8k)$. Therefore $8n$ is even. QED

(b) The converse is false. That is, there is an integer n such that $8n$ is even but n is odd. For example, consider $n = 3$. Then $8n = 24$ which is even but $n = 3$ is odd.

3.2.4.

(a) This is an example of the pigeonhole principle. We can prove it by contrapositive.

Proof. Suppose that each number only came up 6 or fewer times. So there are at most six 1's, six 2's, and so on. That's a total of 36 dice, so you must not have rolled all 40 dice. QED

(b) We can have 9 dice without any four matching or any four being all different: three 1's, three 2's, three 3's. We will prove that whenever you roll 10 dice, you will always get four matching or all being different.

Proof. Suppose you roll 10 dice, but that there are NOT four matching rolls. This means at most, there are three of any given value. If we only had three different values, that would be only 9 dice, so there must be 4 different values, giving 4 dice that are all different. QED

3.3 Chapter Review

3.3.1.

P	Q	R	$\neg P \to (Q \wedge R)$
T	T	T	T
T	T	F	T
T	F	T	T
T	F	F	T
F	T	T	T
F	T	F	F
F	F	T	F
F	F	F	F

3.3.2. Peter is not tall and Robert is not skinny. You must be in row 6 in the truth table above.

3.3.3. Yes. To see this, make a truth table for each statement and compare.

3.3.4. Make a truth table that includes all three statements in the argument:

P	Q	R	$P \to Q$	$P \to R$	$P \to (Q \wedge R)$
T	T	T	T	T	T
T	T	F	T	F	F
T	F	T	F	T	F
T	F	F	F	F	F
F	T	T	T	T	T
F	T	F	T	T	T
F	F	T	T	T	T
F	F	F	T	T	T

Notice that in every row for which both $P \to Q$ and $P \to R$ is true, so is $P \to (Q \wedge R)$. Therefore, whenever the premises of the argument are true, so is the conclusion. In other words, the deduction rule is valid.

3.3.5.

(a) Negation: The power goes off and the food does not spoil.

Converse: If the food spoils, then the power went off.

Contrapositive: If the food does not spoil, then the power did not go off.

(b) Negation: The door is closed and the light is on.

Converse: If the light is off then the door is closed.

Contrapositive: If the light is on then the door is open.

(c) Negation: $\exists x(x < 1 \wedge x^2 \geq 1)$

Converse: $\forall x(x^2 < 1 \to x < 1)$

Contrapositive: $\forall x(x^2 \geq 1 \to x \geq 1)$.

(d) Negation: There is a natural number n which is prime but not solitary.

Converse: For all natural numbers n, if n is solitary, then n is prime.

Contrapositive: For all natural numbers n, if n is not solitary then n is not prime.

(e) Negation: There is a function which is differentiable and not continuous.

Converse: For all functions f, if f is continuous then f is differentiable.

Contrapositive: For all functions f, if f is not continuous then f is not differentiable.

(f) Negation: There are integers a and b for which $a \cdot b$ is even but a or b is odd.

Converse: For all integers a and b, if a and b are even then ab is even.

Contrapositive: For all integers a and b, if a or b is odd, then ab is odd.

(g) Negation: There are integers x and y such that for every integer n, $x > 0$ and $nx \leq y$.

Converse: For every integer x and every integer y there is an integer n such that if $nx > y$ then $x > 0$.

Contrapositive: For every integer x and every integer y there is an integer n such that if $nx \leq y$ then $x \leq 0$.

(h) Negation: There are real numbers x and y such that $xy = 0$ but $x \neq 0$ and $y \neq 0$.

Converse: For all real numbers x and y, if $x = 0$ or $y = 0$ then $xy = 0$

Contrapositive: For all real numbers x and y, if $x \neq 0$ and $y \neq 0$ then $xy \neq 0$.

(i) Negation: There is at least one student in Math 228 who does not understand implications but will still pass the exam.

Converse: For every student in Math 228, if they fail the exam, then they did not understand implications.

Contrapositive: For every student in Math 228, if they pass the exam, then they understood implications.

3.3.6.

(a) The statement is true. If n is an even integer less than or equal to 7, then the only way it could not be negative is if n was equal to 0, 2, 4, or 6.

(b) There is an integer n such that n is even and $n \leq 7$ but n is not negative and $n \notin \{0, 2, 4, 6\}$. This is false, since the original statement is true.

(c) For all integers n, if n is not negative and $n \notin \{0, 2, 4, 6\}$ then n is odd or $n > 7$. This is true, since the contrapositive is equivalent to the original statement (which is true).

(d) For all integers n, if n is negative or $n \in \{0, 2, 4, 6\}$ then n is even and $n \leq 7$. This is false. $n = -3$ is a counterexample.

3.3.7.

(a) For any number x, if it is the case that adding any number to x gives that number back, then multiplying any number by x will give 0. This is true (of the integers or the reals). The "if" part only holds if $x = 0$, and in that case, anything times x will be 0.

(b) The converse in words is this: for any number x, if everything times x is zero, then everything added to x gives itself. Or in symbols: $\forall x(\forall z(x \cdot z = 0) \rightarrow \forall y(x + y = y))$. The converse is true: the only number which when multiplied by any other number gives 0 is $x = 0$. And if $x = 0$, then $x + y = y$.

(c) The contrapositive in words is: for any number x, if there is some number which when multiplied by x does not give zero, then there is some number which when added to x does not give that number. In symbols: $\forall x(\exists z(x \cdot z \neq 0) \rightarrow \exists y(x + y \neq y))$. We know the contrapositive must be true because the original implication is true.

(d) The negation: there is a number x such that any number added to x gives the number back again, but there is a number you can multiply x by and not get 0. In symbols: $\exists x(\forall y(x + y = y) \wedge \exists z(x \cdot z \neq 0))$. Of course since the original implication is true, the negation is false.

3.3.8.

(a) $(\neg P \vee Q) \wedge (\neg R \vee (P \wedge \neg R))$.

(b) $\forall x \forall y \forall z(z = x + y \wedge \forall w(x - y \neq w))$.

3.3.9.

(a) Direct proof.

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

$$7n = 7(2k + 1) = 14k + 7 = 2(7k + 3) + 1.$$

Since $7k + 3$ is an integer, we see that $7n$ is odd. QED

(b) The converse is: for all integers n, if $7n$ is odd, then n is odd. We will prove this by contrapositive.

Proof. Let n be an integer. Assume n is not odd. Then $n = 2k$ for some integer k. So $7n = 14k = 2(7k)$ which is to say $7n$ is even. Therefore $7n$ is not odd. QED

3.3.10.

(a) Suppose you only had 5 coins of each denomination. This means you have 5 pennies, 5 nickels, 5 dimes and 5 quarters. This is a total of 20 coins. But you have more than 20 coins, so you must have more than 5 of at least one type.

(b) Suppose you have 22 coins, including $2k$ nickels, $2j$ dimes, and $2l$ quarters (so an even number of each of these three types of coins). The number of pennies you have will then be

$$22 - 2k - 2j - 2l = 2(11 - k - j - l).$$

But this says that the number of pennies is also even (it is 2 times an integer). Thus we have established the contrapositive of the statement, "If you have an odd number of pennies then you have an odd number of at least one other coin type."

(c) You need 10 coins. You could have 3 pennies, 3 nickels, and 3 dimes. The 10th coin must either be a quarter, giving you 4 coins that are all different, or else a 4th penny, nickel or dime. To prove this, assume you don't have 4 coins that are all the same or all different. In particular, this says that you only have 3 coin types, and each of those types can only contain 3 coins, for a total of 9 coins, which is less than 10.

4.1 Exercises

4.1.1. This is asking for the number of edges in K_{10}. Each vertex (person) has degree (shook hands with) 9 (people). So the sum of the degrees is 90. However, the degrees count each edge (handshake) twice, so there are 45 edges in the graph. That is how many handshakes took place.

4.1.2. It is possible for everyone to be friends with exactly 2 people. You could arrange the 5 people in a circle and say that everyone is friends with the two people on either side of them (so you get the graph C_5). However, it is not possible for everyone to be friends with 3 people. That would lead to a graph with an odd number of odd degree vertices which is impossible since the sum of the degrees must be even.

4.1.4. The graphs are not equal. For example, graph 1 has an edge $\{a, b\}$ but graph 2 does not have that edge. They are isomorphic. One possible isomorphism is $f : G_1 \to G_2$ defined by $f(a) = d$, $f(b) = c$, $f(c) = e$, $f(d) = b$, $f(e) = a$.

4.1.9.

(a) For example:

(b) This is not possible if we require the graphs to be connected. If not, we could take C_8 as one graph and two copies of C_4 as the other.

(c) Not possible. If you have a graph with 5 vertices all of degree 4, then every vertex must be adjacent to every other vertex. This is the graph K_5.

(d) This is not possible. In fact, there is not even one graph with this property (such a graph would have $5 \cdot 3/2 = 7.5$ edges).

4.1.10.

(a) False. (b) True. (c) True. (d) False.

4.2 Exercises

4.2.1.

(a) This is not a tree since it contains a cycle. Note also that there are too many edges to be a tree, since we know that all trees with v vertices have $v - 1$ edges.

(b) This is a tree since it is connected and contains no cycles (which you can see by drawing the graph). All paths are trees.

(c) This is a tree since it is connected and contains no cycles (draw the graph). All stars are trees.

(d) This is a not a tree since it is not connected. Note that there are not enough edges to be a tree.

4.2.2.

(a) This must be the degree sequence for a tree. This is because the vertex of degree 4 must be adjacent to the four vertices of degree 1 (there are no other vertices for it to be adjacent to), and thus we get a star.

(b) This cannot be a tree. Each degree 3 vertex is adjacent to all but one of the vertices in the graph. Thus each must be adjacent to one of the degree 1 vertices (and not the other). That means both degree 3 vertices are adjacent to the degree 2 vertex, and to each other, so that means there is a cycle.

Alternatively, count how many edges there are!

(c) This might or might not be a tree. The length 4 path has this degree sequence (this is a tree), but so does the union of a 3-cycle and a length 1 path (which is not connected, so not a tree).

(d) This cannot be a tree. The sum of the degrees is 28, so there are 14 edges. But there are 14 vertices as well, so we don't have $v = e + 1$, meaning this cannot be a tree.

4.2.6. Yes. We will prove the contrapositive. Assume G does not contain a cycle. Then G is a tree, so would have $v = e + 1$, contrary to stipulation.

4.2.12.

(a) No, although there are graphs for which this is true. For example, K_4 has a spanning tree that is a path (of three edges) and also a spanning tree that is a star (with center vertex of degree 3).

(b) Yes. For a fixed graph, we have a fixed number v of vertices. Any spanning tree of the graph will also have v vertices, and since it is a tree, must have $v - 1$ edges.

(c) No, although there are graph for which this is true (note that if all spanning trees are isomorphic, then all spanning trees will have the same number of leaves). Again, K_4 is a counterexample. One spanning tree is a path, with only two leaves, another spanning tree is a star with 3 leaves.

4.3 Exercises

4.3.1. No. A (connected) planar graph must satisfy Euler's formula: $v - e + f = 2$. Here $v - e + f = 6 - 10 + 5 = 1$.

4.3.2. G has 10 edges, since $10 = \frac{2+2+3+4+4+5}{2}$. It could be planar, and then it would have 6 faces, using Euler's formula: $6 - 10 + f = 2$ means $f = 6$. To make sure that it is actually planar though, we would need to draw a graph with those vertex degrees without edges crossing. This can be done by trial and error (and is possible).

4.3.6. Say the last polyhedron has n edges, and also n vertices. The total number of edges the polyhedron has then is $(7 \cdot 3 + 4 \cdot 4 + n)/2 = (37 + n)/2$. In particular, we know the last face must have an odd number of edges. We also have that $v = 11$. By Euler's formula, we have $11 - (37 + n)/2 + 12 = 2$, and solving for n we get $n = 5$, so the last face is a pentagon.

4.3.8.

Proof. Let $P(n)$ be the statement, "every connected planar graph containing n edges satisfies $v - n + f = 2$." We will show $P(n)$ is true for all $n \geq 0$.

Base case: there is only one graph with zero edges, namely a single isolated vertex. In this case $v = 1$, $f = 1$ and $e = 0$, so Euler's formula holds.

Inductive case: Suppose $P(k)$ is true for some arbitrary $k \geq 0$. Now consider an arbitrary graph containing $k + 1$ edges (and v vertices and f faces). No matter what this graph looks like, we can remove a single edge to get a graph with k edges which we can apply the inductive hypothesis to.

There are two cases: either the graph contains a cycle or it does not. If the graph contains a cycle, then pick an edge that is part of this cycle, and remove it. This will not disconnect the graph, and will decrease the number of faces by 1 (since the edge was bordering two distinct faces). So by the inductive hypothesis we will have $v - k + f - 1 = 2$. Adding the edge back will give $v - (k+1) + f = 2$ as needed.

If the graph does not contain a cycle, then it is a tree, so has a vertex of degree 1. Then we can pick the edge to remove to be incident to such a degree 1 vertex. In this case, also remove that vertex. The smaller graph will now satisfy $v - 1 - k + f = 2$ by the induction hypothesis (removing the edge and vertex did not reduce the number of faces). Adding the edge and vertex back gives $v - (k+1) + f = 2$, as required.

Therefore, by the principle of mathematical induction, Euler's formula holds for all planar graphs. ■

4.3.12.

Proof. We know in any planar graph the number of faces f satisfies $3f \leq 2e$ since each face is bounded by at least three edges, but each edge borders two faces. Combine this with Euler's formula:

$$v - e + f = 2$$
$$v - e + \frac{2e}{3} \geq 2$$
$$3v - e \geq 6$$
$$3v - 6 \geq e.$$

■

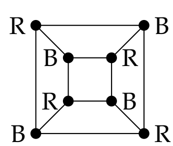
4.4 Exercises

4.4.1. 2, since the graph is bipartite. One color for the top set of vertices, another color for the bottom set of vertices.

4.4.2. For example, K_6. If the chromatic number is 6, then the graph is not planar; the 4-color theorem states that all planar graphs can be colored with 4 or fewer colors.

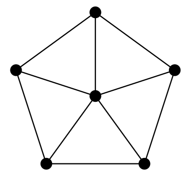
4.4.3. The chromatic numbers are 2, 3, 4, 5, and 3 respectively from left to right.

4.4.5. The cube can be represented as a planar graph and colored with two colors as follows:



Since it would be impossible to color the vertices with a single color, we see that the cube has chromatic number 2 (it is bipartite).

4.4.9. The wheel graph below has this property. The outside of the wheel forms an odd cycle, so requires 3 colors, the center of the wheel must be different than all the outside vertices.



4.4.12. If we drew a graph with each letter representing a vertex, and each edge connecting two letters that were consecutive in the alphabet, we would have a graph containing two vertices of degree 1 (A and Z) and the remaining 24 vertices all of degree 2 (for example, D would be adjacent to both C and E). By Brooks' theorem, this graph has chromatic number at most 2, as that is the maximal degree in the graph and the graph is not a complete graph or odd cycle. Thus only two boxes are needed.

4.4.13.

4.5 Exercises

4.5.1. This is a question about finding Euler paths. Draw a graph with a vertex in each state, and connect vertices if their states share a border. Exactly two vertices will have odd degree: the vertices for Nevada and Utah. Thus you must start your road trip at in one of those states and end it in the other.

4.5.2.

(a) K_4 does not have an Euler path or circuit.

(b) K_5 has an Euler circuit (so also an Euler path).

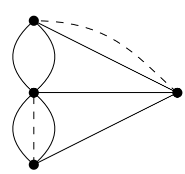
(c) $K_{5,7}$ does not have an Euler path or circuit.

(d) $K_{2,7}$ has an Euler path but not an Euler circuit.

(e) C_7 has an Euler circuit (it is a circuit graph!)

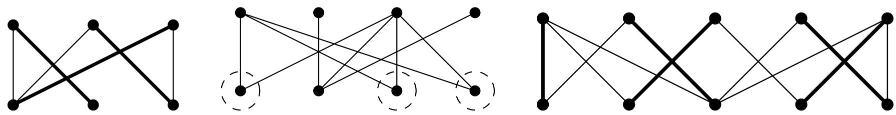
(f) P_7 has an Euler path but no Euler circuit.

4.5.8. If we build one bridge, we can have an Euler path. Two bridges must be built for an Euler circuit.



4.6 Exercises

4.6.1. The first and third graphs have a matching, shown in bold (there are other matchings as well). The middle graph does not have a matching. If you look at the three circled vertices, you see that they only have two neighbors, which violates the matching condition $|N(S)| \geq |S|$ (the three circled vertices form the set S).



4.7 Chapter Review

4.7.1. The first and the third graphs are the same (try dragging vertices around to make the pictures match up), but the middle graph is different (which you can see, for example, by noting that the middle graph has only one vertex of degree 2, while the others have two such vertices).

4.7.2. The first (and third) graphs contain an Euler path. All the graphs are planar.

4.7.3. For example, K_5.

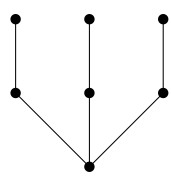
4.7.4. For example, $K_{3,3}$.

4.7.5.

(a) Yes, the graphs are isomorphic, which you can see by drawing them. One isomorphism is:

$$f = \begin{pmatrix} a & b & c & d & e & f & g \\ u & z & v & x & w & y & t \end{pmatrix}.$$

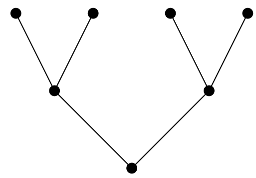
(b) This is easy to do if you draw the picture. Here is such a graph:



Any labeling of this graph will be not isomorphic to G. For example, we could take $V'' = \{a, b, c, d, e, f, g\}$ and $E'' = \{ab, ac, ad, be, cf, dg\}$.

(c) The degree sequence for G is $(3, 3, 2, 1, 1, 1, 1)$.

(d) In general this should be possible: the degree sequence does not determine the graph's isomorphism class. However, in this case, I was almost certain this was not possible. That is, until I stumbled up this:



(e) G is a tree (there are no cycles) and as such also bipartite.

(f) Yes, all trees are planar. You can draw them in the plane without edges crossing.

(g) The chromatic number of G is 2. It shouldn't be hard to give a 2-coloring (for example, color a, d, e, g red and b, c, f blue), but we know that all bipartite graphs have chromatic number 2.

(h) It is clear from the drawing that there is no Euler path, let alone an Euler circuit. Also, since there are more than 2 vertices of odd degree, we know for sure there is no Euler path.

4.7.6. Yes. According to Euler's formula it would have 2 faces. It does. The only such graph is C_{10}.

4.7.7.

(a) Only if $n \geq 6$ and is even.

(b) None.

(c) 12. Such a graph would have $\frac{5n}{2}$ edges. If the graph is planar, then $n - \frac{5n}{2} + f = 2$ so there would be $\frac{4+3n}{2}$ faces. Also, we must have $3f \leq 2e$, since the graph is simple. So we must have $3\left(\frac{4+3n}{2}\right) \leq 5n$. Solving for n gives $n \geq 12$.

4.7.8.

(a) There were 24 couples: 6 choices for the girl and 4 choices for the boy.

(b) There were 45 couples: $\binom{10}{2}$ since we must choose two of the 10 people to dance together.

(c) For part (a), we are counting the number of edges in $K_{4,6}$. In part (b) we count the edges of K_{10}.

4.7.9. Yes, as long as n is even. If n were odd, then corresponding graph would have an odd number of odd degree vertices, which is impossible.

4.7.10.

(a) No. The 9 triangles each contribute 3 edges, and the 6 pentagons contribute 5 edges. This gives a total of 57, which is exactly twice the number of edges, since each edge borders exactly 2 faces. But 57 is odd, so this is impossible.

(b) Now adding up all the edges of all the 16 polygons gives a total of 64, meaning there would be 32 edges in the polyhedron. We can then use Euler's formula $v - e + f = 2$ to deduce that there must be 18 vertices.

(c) If you add up all the vertices from each polygon separately, we get a total of 64. This is not divisible by 3, so it cannot be that each vertex belongs to exactly 3 faces. Could they all belong to 4 faces? That would mean there were $64/4 = 16$ vertices, but we know from Euler's formula that there must be 18 vertices. We can write $64 = 3x + 4y$ and solve for x and y (as integers). We get that there must be 10 vertices with degree 4 and 8 with degree 3. (Note the number of faces joined at a vertex is equal to its degree in graph theoretic terms.)

4.7.11. No. Every polyhedron can be represented as a planar graph, and the Four Color Theorem says that every planar graph has chromatic number at most 4.

4.7.12. $K_{n,n}$ has n^2 edges. The graph will have an Euler circuit when n is even. The graph will be planar only when $n < 3$.

4.7.13. G has 8 edges (since the sum of the degrees is 16). If G is planar, then it will have 4 faces (since $6 - 8 + 4 = 2$). G does not have an Euler path since there are more than 2 vertices of odd degree.

4.7.14. 7 colors. Thus K_7 is not planar (by the contrapositive of the Four Color Theorem).

4.7.15. The chromatic number of $K_{3,4}$ is 2, since the graph is bipartite. You cannot say whether the graph is planar based on this coloring (the converse of the Four Color Theorem is not true). In fact, the graph is *not* planar, since it contains $K_{3,3}$ as a subgraph.

4.7.16. We have that $K_{3,4}$ has 7 vertices and 12 edges (each vertex in the group of 3 has degree 4). Then by Euler's formula we have that $7 - 12 + f = 2$ so if the graph were planar, it would have $f = 7$ faces. However, since the girth of the graph is 4 (there are no cycles of length 3) we get that $4f \leq 2e$. But this would mean that $28 \leq 24$, a contradiction.

4.7.17. For all these questions, we are really coloring the vertices of a graph. You get the graph by first drawing a planar representation of the polyhedron and then taking its planar dual: put a vertex in the center of each face (including the outside) and connect two vertices if their faces share an edge.

(a) Since the planar dual of a dodecahedron contains a 5-wheel, it's chromatic number is at least 4. Alternatively, suppose you could color the faces using 3 colors without any two adjacent faces colored the same. Take any face and color it blue. The 5 pentagons bordering this blue pentagon cannot be colored blue. Color the first one red. Its two neighbors (adjacent to the blue pentagon) get colored green. The remaining 2 cannot be blue or green, but also cannot both be red since they are adjacent to each other. Thus a 4th color is needed.

(b) The planar dual of the dodecahedron is itself a planar graph. Thus by the 4-color theorem, it can be colored using only 4 colors without two adjacent vertices (corresponding to the faces of the polyhedron) being colored identically.

(c) The cube can be properly 3-colored. Color the "top" and "bottom" red, the "front" and "back" blue, and the "left" and "right" green.

4.7.18.

(a) False. To prove this, we can give an example of a pair of graphs with the same chromatic number that are not isomorphic. For example, $K_{3,3}$ and $K_{3,4}$ both have chromatic number 2, but are not isomorphic.

(b) False. The previous example does not work, but you can easily draw two trees that have the same number of vertices and edges but are not isomorphic. Since all trees have chromatic number 2, this is a counterexample.

(c) True. If there is an isomorphism from G_1 to G_2, then we have a bijection that tells us how to match up vertices between the graph. Any proper vertex coloring of G_1 will tell us how to properly color G_2, simply by coloring $f(v_i)$ the same color as v_i, for each vertex $v_i \in V$. That is, color the vertices in G_2 exactly how you color the corresponding vertices in G_1. Similarly, any proper vertex coloring of G_2 corresponds to a proper vertex coloring of G_1. Thus the smallest number of colors needed to properly color G_1 cannot be smaller than the smallest number of colors needed to properly color G_2, and vice-versa, so the chromatic numbers must be equal.

4.7.19. G has 13 edges, since we need $7 - e + 8 = 2$.

4.7.20.

(a) The graph does have an Euler path, but not an Euler circuit. There are exactly two vertices with odd degree. The path starts at one and ends at the other.

(b) The graph is planar. Even though as it is drawn edges cross, it is easy to redraw it without edges crossing.

(c) The graph is not bipartite (there is an odd cycle), nor complete.

(d) The chromatic number of the graph is 3.

4.7.21.

(a) False. For example, $K_{3,3}$ is not planar.

(b) True. The graph is bipartite so it is possible to divide the vertices into two groups with no edges between vertices in the same group. Thus we can color all the vertices of one group red and the other group blue.

(c) False. $K_{3,3}$ has 6 vertices with degree 3, so contains no Euler path.

(d) False. $K_{3,3}$ again.

(e) False. The sum of the degrees of all vertices is even for *all* graphs so this property does not imply that the graph is bipartite.

4.7.22.

(a) If a graph has an Euler path, then it is planar.

(b) If a graph does not have an Euler path, then it is not planar.

(c) There is a graph which is planar and does not have an Euler path.

(d) Yes. In fact, in this case it is because the original statement is false.

(e) False. K_4 is planar but does not have an Euler path.

(f) False. K_5 has an Euler path but is not planar.

5.1 Exercises

5.1.1.

(a) $\dfrac{4}{1-x}$.

(b) $\dfrac{2}{(1-x)^2}$.

(c) $\dfrac{2x^3}{(1-x)^2}$.

(d) $\dfrac{1}{1-5x}$.

(e) $\dfrac{1}{1+3x}$.

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

(g) $\dfrac{x}{(1-x^3)^2}$.

5.1.2.

(a) $0, 4, 4, 4, 4, 4, \ldots$.

(b) $1, 4, 16, 64, 256, \ldots$.

(c) $0, 1, -1, 1, -1, 1, -1, \ldots$.

(d) $0, 3, -6, 9, -12, 15, -18, \ldots$.

(e) $1, 3, 6, 9, 12, 15, \ldots$.

5.1.4. Call the generating function A. Compute $A - xA = 4 + x + 2x^2 + 3x^3 + 4x^4 + \cdots$. Thus $A - xA = 4 + \dfrac{x}{(1-x)^2}$. Solving for A gives $\dfrac{4}{1-x} + \dfrac{x}{(1-x)^3}$.

5.1.5. $\dfrac{1+2x}{1-3x+x^2}$.

5.1.6. Compute $A - xA - x^2A$ and the solve for A. The generating function will be $\dfrac{x}{1-x-x^2}$.

5.1.7. $\dfrac{x}{(1-x)(1-x-x^2)}$.

5.1.8. $\dfrac{2}{1-5x} + \dfrac{7}{1+3x}$.

5.1.9. $a_n = 3 \cdot 4^{n-1} + 1$.

5.1.12.

(a) $\frac{1}{(1-x^2)^2}$.

(b) $\frac{1}{(1+x)^2}$.

(c) $\frac{3x}{(1-x)^2}$.

(d) $\frac{3x}{(1-x)^3}$. (partial sums).

5.1.13.

(a) $0, 0, 1, 1, 2, 3, 5, 8, \ldots$.

(b) $1, 0, 1, 0, 2, 0, 3, 0, 5, 0, 8, 0, \ldots$.

(c) $1, 3, 18, 81, 405, \ldots$.

(d) $1, 2, 4, 7, 12, 20, \ldots$.

5.1.15. $\frac{x^3}{(1-x)^2} + \frac{1}{1-x}$.

5.2 Exercises

5.2.1.

Proof. Suppose $a \mid b$. Then b is a multiple of a, or in other words, $b = ak$ for some k. But then $bc = akc$, and since kc is an integer, this says bc is a multiple of a. In other words, $a \mid bc$. ■

5.2.3. $\{\ldots, -8, -4, 0, 4, 8, 12, \ldots\}$, $\{\ldots, -7, -3, 1, 5, 9, 13, \ldots\}$, $\{\ldots, -6, -2, 2, 6, 10, 14, \ldots\}$, and $\{\ldots, -5, -1, 3, 7, 11, 15, \ldots\}$.

5.2.5.

Proof. Assume $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. This means $a = b + kn$ and $c = d + jn$ for some integers k and j. Consider $a - c$. We have:

$$a - c = b + kn - (d + jn) = b - d + (k - j)n.$$

In other words, $a - c$ is $b - d$ more than some multiple of n, so $a - c \equiv b - d \pmod{n}$. ■

5.2.6.

(a) $3^{456} \equiv 1^{456} = 1 \pmod{2}$.

(b) $3^{456} = 9^{228} \equiv (-1)^{228} = 1 \pmod{5}$.

(c) $3^{456} = 9^{228} \equiv 2^{228} = 8^{76} \equiv 1^{76} = 1 \pmod{7}$.

(d) $3^{456} = 9^{228} \equiv 0^{228} = 0 \pmod{9}$.

5.2.8. For all of these, just plug in all integers between 0 and the modulus to see which, if any, work.

(a) No solutions.

(b) $x = 2$, $x = 5$, $x = 8$.

(c) No solutions.

5.2.10. $x = 5 + 22k$ for $k \in \mathbb{Z}$.

5.2.12. $x = 6 + 15k$ for $k \in \mathbb{Z}$.

5.2.14. We must solve $7x + 5 \equiv 2 \pmod{11}$. This gives $x \equiv 9 \pmod{11}$. In general, $x = 9 + 11k$, but when you divide any such x by 11, the remainder will be 9.

5.2.15. Divide through by 2: $3x + 5y = 16$. Convert to a congruence, modulo 3: $5y \equiv 16 \pmod{3}$, which reduces to $2y \equiv 1 \pmod{3}$. So $y \equiv 2 \pmod{3}$ or $y = 2 + 3k$. Plug this back into $3x + 5y = 16$ and solve for x, to get $x = 2 - 5k$. So the general solution is $x = 2 - 5k$ and $y = 2 + 3k$ for $k \in \mathbb{Z}$.

List of Symbols

Symbol	Description	Page
$P, Q, R, S, \ldots$	propositional (sentential) variables	6
$\wedge$	logical "and" (conjunction)	6
$\vee$	logical "or" (disjunction)	6
$\neg$	logical negation	6
$\exists$	existential quantifier	15
$\forall$	universal quantifier	15
$\emptyset$	the empty set	27
$\mathcal{U}$	universe set (domain of discourse)	27
$\mathbb{N}$	the set of natural numbers	27
$\mathbb{Z}$	the set of integers	27
$\mathbb{Q}$	the set of rational numbers	27
$\mathbb{R}$	the set of real numbers	27
$\mathcal{P}(A)$	the power set of A	27
$\{,\}$	braces, to contain set elements.	27
$:$	"such that"	27
$\in$	"is an element of"	27
$\subseteq$	"is a subset of"	27
$\subset$	"is a proper subset of"	27
$\cap$	set intersection	27
$\cup$	set union	27
$\times$	Cartesian product	27
$\setminus$	set difference	27
$\overline{A}$	the complement of A	27
$\|A\|$	cardinality (size) of A	27
$A \times B$	the Cartesian product of A and B	33
$f(A)$	the image of A under f.	48
$f^{-1}(B)$	the inverse image of B under f.	48
$\mathbf{B}^n$	the set of length n bit strings	72
$\mathbf{B}^n_k$	the set of length n bit strings with weight k.	72
$(a_n)_{n\in\mathbb{N}}$	the sequence $a_0, a_1, a_2, \ldots$	136
T_n	the nth triangular number	140
F_n	the nth Fibonacci number	145
Δ^k	the kth differences of a sequence	161

(Continued on next page)

Index

Colophon

This book was authored in PreTeXt.

Mathematics

This gentle introduction to discrete mathematics is written for first and second year math majors, especially those who intend to teach. The text began as a set of lecture notes for the discrete mathematics course at the University of Northern Colorado. This course serves both as an introduction to topics in discrete math and as the "introduction to proof" course for math majors. The course is usually taught with a large amount of student inquiry, and this text is written to help facilitate this.

Four main topics are covered: counting, sequences, logic, and graph theory. Along the way proofs are introduced, including proofs by contradiction, proofs by induction, and combinatorial proofs. The book contains over 470 exercises, including 275 with solutions and another 100 or so with hints. Exercises range from elementary to quite challenging.

While there are many fine discrete math textbooks available, this text has the following advantages:

- It is written to be used in an inquiry rich course.
- It is written to be used in a course for future math teachers.
- It is open source, with low cost print editions and free electronic editions.

To download the current version, or for information on obtaining the PreTeXt source, visit:
`http://discrete.openmathbooks.org/`.