Contents

Preface

The mathematics in this book is not hard, but neither is it very interesting, unless you are an algebra nerd.
— Review in *The Economist* of *Lewis Carroll in Numberland* by Robin Wilson

Why should a student learn discrete mathematics? For me, there are two good reasons. One is that discrete mathematics is used in almost all areas of computer science, data science, actuarial science, logistics, and many other disciplines. So a student learning discrete mathematics has a good foundation from which they can excel in those other disciplines. But that, in my opinion, is the less important of the two reasons.

The second reason is the exposure to the wide array and variety of mathematical topics and structures outside the traditional algebra, geometry, trigonometry, and calculus sequence. Many students feel frustrated with factoring, confused by calculus, lost with logarithms, and triggered by trigonometry. Due to the vast amounts of symbolic manipulation and solution finding, some students come away from those traditional courses with the view that mathematics is all about computing an answer. Discrete mathematics shows these students that mathematics is no more about computation than literature is about grammar. Certainly, computations are important and useful, but calculations are not mathematics — just as knowing grammar is important, but grammar is not literature. With discrete mathematics, students finally get a chance to experience other important and fascinating areas of mathematics outside the traditional course sequence, and hopefully come away with an understanding that mathematics is more than just computation: it is about *proof*.

The topics included in this book reflect the growing importance of certain areas of mathematics, and my own personal favoritism towards some topics. The scope of the book is narrow on purpose. The choices of topics and applications are chosen with the student in mind to be relevant, interesting, and reflective of the mathematics they are learning. It would be easy to expand these topics further, but then I would have written a number theory textbook, or a graph theory textbook, or a combinatorics textbook, rather than an introduction to these topics. Your favorite topic or application may not be included, but by keeping the book slim, you have ample time to include it in your classes.

At my institution, students taking a course in discrete mathematics have already completed a course in differential calculus. They are taking discrete mathematics instead of more calculus because their intended major and careers do not require more calculus, or because they did not find calculus enjoyable (but want to know more mathematics), or because some are required to take discrete mathematics. As a result, this book is written with two broad types of student in mind: the student who has some mathematical sophistication, and the student who has struggled with the traditional mathematical course sequence. Thus, the textbook is intended to be read by students of varying backgrounds, and I wrote it with this goal in mind.

The variety of reasons for a student to take this course also results in a variety of difficulty levels in the problem sets. Most problems simply reinforce the concepts learned, and are straightforward – some are even (gasp!) rote. However, some problems require plenty of thought to put the pieces of mathematics and logic together to form a solution. There are supplemental problems at the end of each chapter, grouped by section. These are intended to give extra practice of concepts. I use problem and example titles to help students find similar problems in the supplemental problems to those in the problem sets at the end of each section, and to enable students to refer to examples more easily. There are also sample test questions at the end of each chapter which are not titled or grouped by section, thereby preparing students for how they would see problems presented on a test.

There are no answers in the back of the book. I went back and forth about including the answers in the back of the book. Some students use the answers as they should be used: a check on their progress. Most students, unfortunately, simply flip to the back of the book at the first hint of struggle with a problem, thereby never letting themselves think deeply and think through a problem. I considered putting all answers in the back except the proofs, but even a numerical answer in the back can short-circuit the problem-solving process. While the answers in the back could prove useful, I ultimately decided not to put them in the back of the book. A separate solutions manual is available from `lulu.com`.

Acknowledgements

Thanks to my wife, Julie, for putting up with me while this book was written (and for putting up with me in general).

Thanks to my in-person colleagues, Maurice Hendon, David Hornbeck, Julie Matthews, Debbie Poss, Chasen Smith, and David Stone.

Thanks to my virtual colleagues at *The Art of Problem Solving*, particularly Miles Dillon Edwards, Joshua Zucker, and David Patrick. Each one of these people has excellent instructional ideas, and they enabled me to become a better instructor.

The conversations with the late Steve Sigur concerning mathematics teaching continue to motivate me; I wish I could thank him in person.

I thank all my Discrete Math and Advanced Finite Math students over the years who have learned mathematics outside the normal algebra-trig-calculus track (some reluctantly, some ethusiastically).

Dedication

This book is dedicated to a few students who helped write this book without even knowing they did because they challenged me to think about how I teach discrete mathematics: Amy, Sophia, Raymond, Ashley, James, Jonathan, Zineb, Matt, Anika, Julia, Erin, Irene, Zariah, Danahyah, Kep, Payton, Sarah, Kwatcho, Patricia, Nylah, Zuri, and Maxwell.

Chuck Garner
Conyers, Georgia
June 2023

1 LOGIC and SETS

The title of this book is *Discrete Mathematics: A Gateway to the Mathematical Garden*. What does this mean? *Discrete* mathematics is the mathematics of concepts which are not continuous; concepts such as counting objects, properties of integers, logic, and proof. Some use this interchangably with the term *finite* mathematics. However, finite mathematics is about concepts which are not infinite. There are many interesting concepts of mathematics which can be classified as finite or discrete or both. The overwhelming majority of your mathematical education has focused on the continuous and infinite (indeed, this is what calculus is all about) while neglecting these other concepts. This book aims to address this imbalance.

This first chapter sets the stage for the rest of the course. There will be many new terms and ideas thrown at you very quickly. Just like any garden, you will need to get your hands dirty for things to bloom! Thus, it is best to have a pencil and your notebook with you to make note of the new terms and their definitions. You can easily spot the new terms because they are italicized and typeset in red, *like this*. You should read each section before you come to class, and you should have thought about the examples and their solutions.

A few of the new terms will appear in margin notes like this one, and some will appear in the problems.

Time to get started! Do you have your pencil and notebook? Are you sitting comfortably? Discrete mathematics awaits!

1.1 Statements

> *When dealing with people, remember you are not dealing with creatures of logic, but with creatures bristling with prejudice and motivated by pride and vanity.*
> — Dale Carnegie, *How to Win Friends and Influence People*

You will learn . . .

1: to determine whether a sentence is a statement;

2: to write statements from symbols to English and vice versa;

3: to represent the operations and, or, *and* not *using logical symbolism, and to determine whether statements involving these operations are true or false;*

4: to interpret if-then *statements.*

A *statement* is a declarative sentence that is either true or false, but not both. The adjective "declarative" rules out sentences such as commands or questions. Every statement has a *truth value*, either true (T) or false (F). If the truth value is ambiguous—perhaps the sentence expresses an opinion or contains ill-defined terms—then the sentence is not a statement.

▶ **Example 1.1.A – Some Statements.**

Which of the following sentences are statements? Determine the truth values of the ones that are statements.

(a) Mars is a planet.

(b) $6 > 1$.

(c) Lizzo is better than Taylor Swift.

(d) Buy tickets to the BTS concert.

(e) $x < 10$.

(f) $x^2 = 9$.

(g) $(x + y)^2 = x^2 + 2xy + y^2$.

(h) Who is calling me?

(i) $1 + 1 = 3$.

(j) Alexis has the highest SAT score in her school.

(k) Calculus is difficult.

(l) Her name is Cecily Strong.

(m) All of Halsey's email is spam.

(n) Our country is worse because of woke commie liberals.

(o) Our society is worse because of fascist right-wing nutjobs.

▷ **Solution.** Sentences (c), (k), (n), and (o) express opinions, and are therefore not statements. Sentence (d) is a command, and therefore not a statement. Sentence (h) is a question, and therefore not a statement. Sentences (e), (f), and (l) are ambiguous, and so are not statements because we do not know the value of the variables ("x" in the cases of (e) and (f), and "her" in (l)).

This leaves (a), (b), (g), (i), (j), and (m) as statements. Statements (a), (b), and (g) are true. Statement (i) is false. Statements (j) and (m) are certainly either true or false, and not both; however, we need more information to determine which!

Some logicians and mathematicians use the term proposition *instead of "statement."*

The statements in Example 1.1.A are *simple statements* because they can be represented by a single letter, such as p or q. For instance, we can write p = "Mars is a planet." Some propositions are combined using logical operators to create *compound statements*. The words “not,” “and,” and “or” are three such logical operators.

The “or” in everyday English is not the same as the logical or. Often in conversation, we do not allow both possibilities to be true. For instance, “Coke or Pepsi” is a choice between two options, not a logical statement. (And the right choice is neither Coke nor Pepsi, it’s RC. Fight me.) The choice between two options—p or q but not both—is called the exclusive or, while the logical or used here is the inclusive or.

▶ Example 1.1.B – A Compound Statement.

Both “Mars is a planet” and “Pluto is a planet” are statements. A compound statement would be “Mars is a planet or Pluto is a planet.” Another compound statement is “Pluto is not a planet.”

We use symbols for these logical operators when the statements are represented by single letters. Let p = “Mars is a planet” and q = “Pluto is a planet.” Then we can make the following compound statements.

The symbol $p \wedge q$ represents “Mars is a planet and Pluto is a planet.” The statement $p \wedge q$ is true only when p is true and q is true. If one of them or both are false, then $p \wedge q$ is false.

The symbol $p \vee q$ represents “Mars is a planet or Pluto is a planet.” The statement $p \vee q$ is true when at least one of p or q is true. If both are false, then $p \vee q$ is false.

The symbol $\neg q$ represents “It is not the case that Pluto is a planet” or simply “Pluto is not a planet.” The statement $\neg q$ is true when q is false; $\neg q$ is false when q is true. We say that $\neg q$ is the *negation* of q.

The symbols $\sim q$, q', and $\overline{q}$ are also used to denote “not q.” Some computer languages use !q for “not q.”

▶ Example 1.1.C – Truth Value of a Compound Statement.

Let p = “Mars is a planet” and q = “Pluto is a planet.” Then $p \wedge \neg q$ represents “Mars is a planet and Pluto is not a planet.” It is true that Mars is a planet. It is false that Pluto is a planet, so it is true that Pluto is not a planet. So we have two true statements joined together with an “and.” Thus the statement $p \wedge \neg q$ has a truth value of T.

We can summarize the truth value of the compounding connectors in a *truth table*. The truth table lists every possible combination of T and F that p and q could have, and the corresponding values of the compound statement. Below are the truth tables for “not,” “and,” and “or.”

p	$\neg p$
T	F
F	T

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

▶ Example 1.1.D – Translating Symbols.

Let p, q, and r represent the following statements.

p = “It is raining.” q = “Dale is at the mall.” r = “It is sunny.”

Translate the following symbolic statement into proper English. Assuming that p, q, and r have the truth value T, determine the truth values of each symbolic statement.

(a) $p \vee r$

(b) $q \wedge \neg r$

(c) $\neg(p \wedge q)$

(d) $q \wedge (p \vee \neg r)$

▷ Solution.

(a) "It is raining or it is sunny." Since both p and r are true, then $p \vee r$ is true.

(b) "Dale is at the mall and it is not sunny" or "Dale is at the mall but it is not sunny." Given that r is true, then $\neg r$ is false. As long as one of the two is false, the entire and-statement is false.

(c) "It is not the case that it is raining and Dale is at the mall." Since p and q are true, then $p \wedge q$ is true. This makes $\neg(p \wedge q)$ false.

(d) "Dale is at the mall and it is raining or it is not sunny." Given that r is true, then $\neg r$ is false. But since p is true, $p \vee \neg r$ is still true. Since this is true and q is true, the statement $q \wedge (p \vee \neg r)$ has truth value T. However, notice the ambiguity here in the English translation. We could translate $(q \wedge p) \vee \neg r$ as "Dale is at the mall and it is raining or it is not sunny." The same English sentence can mean two different logical statements!

In everyday English, "but" suggests that the phrase following "but" is unexpected. However, logically, "but" and "and" are equivalent.

Is it any wonder people misunderstand each other?

Compound statements using the operators $\wedge$, $\vee$, and $\neg$ are not the only ones. There are also compound statements of the form "if p then q" and "p if and only if q." The statement "if p then q" is an *implication*, or a *conditional statement*. It is symbolized as $p \Rightarrow q$. In the statement $p \Rightarrow q$, we call p the *hypothesis* and q the *conclusion*. As such, $p \Rightarrow q$ is often read as "p implies q," but it could also be translated as

- "p *only if* q,"
- "p is *sufficient* for q,"
- "q is *necessary* for p," or
- "q *whenever* p."

However, "p if q" is equivalent to "If q then p" which is different from "p only if q"!

The statement "p if and only if q" is a *double implication*, or a *biconditional*. It is symbolized as $p \Leftrightarrow q$, and the English "if and only if" can be abbreviated to *iff*. The symbol $p \Leftrightarrow q$ is itself an abbreviation of what the statement actually means: $(p \Rightarrow q) \wedge (q \Rightarrow p)$. That is, p iff q means that p implies q and q implies p.

The truth tables for these statements are below.

p	q	$p \Rightarrow q$
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

Let's examine an implication to see why there is only one instance when $p \Rightarrow q$ could be false. Consider the following compound statement, where p = "I am late for my job" and q = "I will be fired":

"If I am late for my job, then I will be fired."

Now, suppose that you are late for your job, and your boss fires you. In this case p and q are both true, so we see that $p \Rightarrow q$ must also be true. That is, your boss followed through on their promise to fire you if you are late.

Now suppose that you are late but your boss doesn't fire you. In this case, p is true and q is false. In other words, the boss did not keep their word. So it is no longer true that p implies q since you weren't fired. Hence, $p \Rightarrow q$ is false.

In the third case, suppose you are not late and then your boss fires you. In this case p is false and q is true. You may think that $p \Rightarrow q$ must be false, but wait: your boss did not say under what *other* conditions you could be fired. Perhaps you stole money from the register, or you didn't lock the door when you left yesterday after closing, or the boss just doesn't like your attitude. In other words, the boss did not say that if you showed up on time that you would keep your job! In this case, $p \Rightarrow q$ is *vacuously true*, that is, *true by default*, since we do not know what would happen if you showed up on time.

In the fourth case, suppose you are not late and your boss doesn't fire you. Here, both p and q are false. But again, we do not know what would happen if you showed up on time. Thus, like the case before, this is vacuously true.

The take-away here is that a conditional statement is false only when the hypothesis is true and the conclusion is false!

Problems for §1.1

1 A Few Statements. For each of the following, determine whether the sentence is a statement. Determine the truth values of the ones that are statements.

(a) Video games are fun.

(b) The difference between two even integers is an even integer.

(c) There was a time in your life where your age in months was equal to your height in inches.

(d) Why are you calling me?

(e) Please do not call me.

(f) Hulu is better than Netflix.

(g) There are infinitely many prime numbers.

(h) The equation $x^2 = 9$ has two solutions.

(i) In a room full of 400 people, at least two people in the room share a birthday.

(j) Tom Holland is the best Spider-Man.

2 Truth Values. Determine all truth values for each statement for every possible combination of truth values of p and q. You may find it useful to create a truth table.

(a) $p \wedge (\neg p)$

(b) $(\neg p) \vee q$

(c) $\neg (p \wedge q)$

(d) $p \wedge (\neg q)$

3 Negations. Write the negations of the following statements.

(a) The equation $x^2 = 9$ has two solutions.

(b) A square is a rhombus.

(c) There are infinitely many prime numbers.

(d) Exponential functions are always positive.

4 Translations to English. Suppose p = "It is cold outside," q = "It is snowing," and r = "Kala is swimming." Write the English translations of the following symbolic statements, and, given that p, q, and r are true, determine the truth value of each statement.

(a) $(p \wedge q) \wedge r$

(b) $(p \wedge r) \wedge \neg q$

(c) $p \Rightarrow r$

(d) $(p \wedge q) \Rightarrow r$

(e) $r \Rightarrow (p \vee q)$

(f) $q \Rightarrow \neg r$

5 Translations to Symbols. Suppose p = "n is divisible by 2," q = "n is divisible by 9," and r = "n is divisible by 18." Translate the following

English statements to symbols and determine their truth value for all integers n.

(a) If n is divisible by 18, then n is divisible by 9.

(b) If n is divisible by 2 and by 9, then n is divisible by 18.

(c) n is divisible by 18 if and only if n is divisible by 2 and by 9.

(d) That n is divisible by 2 is sufficient for n to be divisible by 18.

6 Implications. Which of the following are other ways to express the statement "If I am late for my job, then I will be fired"?

(a) Being late for my job is sufficient for being fired.

(b) Being late for my job is necessary for being fired.

(c) I will be fired only if I am late for my job.

(d) I will be fired whenever I am late for my job.

(e) I will be fired if I am late for my job.

(f) Being late for my job implies that I will be fired.

7 Early Voting. To cast a ballot in Rockdale County, Georgia before election day, certain requirements must be met: you can only vote early on any non-holiday between 3 and 17 days prior to election day; you must be a legal resident of Rockdale County; you must be at least 18 years old; and you must have a valid form of identification. Let p = "You are allowed to vote early," q = "It must be between 3 and 17 days prior to election day," r = "It is a holiday," s = "You are a legal resident," t = "You are at least 18 years old," and u = "You have a valid ID." Construct a symbolic statement using q, r, s, t, and u that is equivalent to p.

1.2 Compound Statements

> *On its own, being a decent person is no guarantee that you will act well, which brings us back to the one protection we have against demagogues, tricksters, and the madness of crowds: clear and reasoned thinking.*
>
> — Christopher Paolini, *Eldest*

You will learn . . .

1: to construct truth tables that represent conditional statements, and use truth tables to determine whether a statement is true or false;

2: to translate conditional statements from logical symbolism to English and vice versa.

Assessing the truth value of a statement can be complicated, but that is mostly because the words we use in logic and mathematics have different meanings in everyday conversations. We have already mentioned the difference between the inclusive or and the exclusive or. Another reason is the lack of rigor in what we say and mean. Consider the following statement made by a parent to a child.

If you want dessert, then you will eat your vegetables!

Now suppose that the child eats their vegetables but doesn't get any dessert. Did the parent lie? *No!* The parent said what would happen *if the child wanted dessert*. The parent never indicated what would happen if the child ate the vegetables! The child (and possibly the parent) assumed the converse of the statement to be true when it does not necessarily have to be.

Due to our misuse of logic and language, we learn, from an early age, misguided reasoning. One way to combat this is to rely on the symbols and the truth tables to determine when a statement is true or false. This becomes quite crucial with more complicated compound statements.

▶ Example 1.2.A – Compound Statements.

Are the following statements true or false?

(a) Abraham Lincoln was President of the United States in 2021 or $3 + 4 = 7$.

(b) If the sky is purple, then New York City is a big city.

(c) If Google makes the iPhone, then buses can fly.

(d) If the capital of Georgia is Atlanta, then an equilateral triangle has equal side lengths.

▷ Solution.

(a) It is not true that Abraham Lincoln was President of the United States in 2021, and it is true that $3 + 4 = 7$. Hence, this statement has the form $p \vee q$, where p is false and q is true. This means that the statement $p \vee q$ is true since q is true.

(b) It is not true that the sky is purple, and it is true that New York City is a big city. Thus we have an implication of the form $p \Rightarrow q$, where p is false and q is true. This is one of the cases that is vacuously true, and so, $p \Rightarrow q$ is true. (We know this is true by the value in the truth table on page 4.)

(c) It is not true that Google makes the iPhone, and it is not true that buses can fly. So we have a statement of the form $p \Rightarrow q$ with both p and q false. However this is true, as this is another vacuously true case.

(d) This is a statement of the form $p \Rightarrow q$ where both p and q are true. So we must accept the statement $p \Rightarrow q$ as true.

In everyday conversation, we expect phrases linked together with "If"-"then" or with an "or" to be related somehow. However, whether the statement $p \Rightarrow q$ indicates a relationship between p and q is irrelevant to whether it is true or false, only whether the components of the satement are true or false matters. There is no obvious relationship between Atlanta being Georgia's capitol and the sides of an equilateral triangle being equal, but this does not mean that the statement's truth value is false.

Perhaps we should say "more compounded"?

As statements get more complicated, we rely more on the symbolic representation. Consider the statement

$$S : (\neg p \wedge q) \Rightarrow (p \vee q).$$

For a particular pair of truth values of p and q, we can determine the truth value of S. To do this, we plug in the truth values for T and F, and "compute" the truth value of S. The following example shows how we can do such a computation.

▶ Example 1.2.B – Truth Table for a Compound Statement.

Create a truth table for $S : (\neg\, p \wedge q) \;\Rightarrow\; (p \vee q)$.

▷ Solution. To create a truth table, we need to evaluate S at every possible of combination of the truth values of p and q. We will start with p and q both having the value T. We can then "plug in" these values for p and q and evaluate each part of the statement using the truth tables from §1.1. We have

$$\begin{aligned} S &= (\neg\, T \wedge T) \;\Rightarrow\; (T \vee T) \\ &= (F \wedge T) \;\Rightarrow\; (T \vee T) \\ &= F \;\Rightarrow\; T \\ &= F. \end{aligned}$$

So when $p = q = T$, $S = F$. Now we need to do this for the other three possible combinations of truth values. This can be accomplished in a more compact fashion by constructing the truth table column by column. Write columns for the various combinations of p and q, then write the columns for the "sub-statements" involved in S. This is shown below.

p	q	$\neg\, p$	$\neg\, p \wedge q$	$p \vee q$	S
T	T	F	F	T	F
T	F	F	F	T	F
F	T	T	T	T	T
F	F	T	F	F	T

The last column is obtained by evaluating the $\neg\, p \wedge q$ column entries and the $p \vee q$ column entries joined by $\Rightarrow$.

It is possible that we could have more than two simple statements in a compound statement. For instance, the compound statement

$$S : (p \wedge \neg\, q) \;\Leftrightarrow\; (r \vee p)$$

involves three statements p, q, and r. To create a truth table for S, we need to consider all possible combinations of the values of T and F for p, q, and r:

$$\begin{array}{cccc} TTT & TTF & TFT & TFF \\ FTT & FTF & FFT & FFF. \end{array}$$

Once the columns for p, q, and r are written, we move to the next "sub-statement" which would be $\neg\, q$. Then we evaluate $p \wedge \neg\, q$, then $r \vee p$, and finally, $(p \wedge \neg\, q) \;\Leftrightarrow\; (r \vee p)$. The complete truth table is in Figure 1.1 on page 9.

How do we decide which order to evaluate the sub-statements? How do we order the columns in the truth table? Just as with arithmetic and algebra, there is an *order of operations* for these logical symbols. The order is

$$\neg, \quad \wedge, \quad \vee, \quad \Rightarrow, \quad \Leftrightarrow.$$

p	q	r	$\neg q$	$p \wedge \neg q$	$r \vee p$	S
T	T	T	F	F	T	F
T	T	F	F	F	T	F
T	F	T	T	T	T	T
T	F	F	T	T	T	T
F	T	T	F	F	T	F
F	T	F	F	F	F	T
F	F	T	T	F	T	F
F	F	F	T	F	F	T

Figure 1.1 – The truth table for the statement $S : (p \wedge \neg q) \Leftrightarrow (r \vee p)$.

With an understanding of this order, we do not have to write the parentheses in the statement

$$S : (p \wedge \neg q) \Leftrightarrow (r \vee p).$$

We can simply write

$$S : p \wedge \neg q \Leftrightarrow r \vee p.$$

Besides, there is an infinite supply of parentheses!

Parentheses are encouraged if it helps bring clarity to symbols, and it is never wrong to correctly place as many parentheses as you want. From here on out, we will no longer write unneeded parentheses in this book. That means $\neg p \wedge q$ is unambiguously different from $\neg(p \wedge q)$.

Problems for §1.2

1 Tautology and Contradiction. A compound statement that has a truth value of T for all truth values of the simple statements is called a *tautology*. A compound statement that has a truth value of F for all truth values of the simple statements is called a *contradiction*. The statement $p \wedge (\neg p)$ from §1.1, Problem **2**(a) is a contradiction because the result column of the truth table was always F. There is a related statement that is a tautology—what is the statement?

2 Interesting Implications.

(a) Compare your answer to §1.1, Problem **2**(b) and the truth table for $p \Rightarrow q$ on page 4. What does this imply about $p \Rightarrow q$ and $\neg p \vee q$?

(b) Find a way to write "It is not raining or I am at the mall" in a logically equivalent form using "if" and "then."

(c) Create a truth table for the statement $\neg p \vee \neg q$. Compare this to the truth table from §1.1, Problem **2**(c). What conclusions can you draw about the statements $\neg p \vee \neg q$ and $\neg(p \wedge q)$?

(d) Find a way to write "It is not the case that I was late for my job and that I got fired" in a logically equivalent form using an "or" statement.

3 Conditionals, Tautologies, and Contradictions. Suppose p and q are statements. What can be said of the conditional statement $p \Rightarrow q$ in each case?

(a) p is a contradiction.

(b) p is a tautology.

(c) q is a contradiction.

(d) q is a tautology.

4 More Truth Tables. Create a truth table for each statement. (Recall the order of operations for these symbols!)

(a) $\neg(p \vee q)$

(b) $\neg p \wedge \neg q$

(c) $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$

(d) $p \wedge q \vee \neg r \Rightarrow q$

(e) $p \wedge \neg r \Leftrightarrow q \vee \neg p$

5 Do You Notice. . . .

(a) Identify any of the statements in Problem 4 that are tautologies.

(b) The truth tables in Problems 4(a) and 4(b) are identical. What does this indicate?

(c) How many rows would there need to be in a truth table for the compound statement $p \wedge q \Rightarrow r \vee s$? How many rows would there need to be for five simple statements? For six? Generalize: how many rows are needed for n simple statements?

6 The Exclusive Or. The *exclusive or*, also shortened to *xor*, is the logical operator used to mean that one can have p or q but not both. Many people use many different symbols for the exclusive or; in this book, we will use $p \veebar q$. (Another symbol used often is $p \oplus q$.) The truth table for the exclusive or is below.

p	q	$p \veebar q$
T	T	F
T	F	T
F	T	T
F	F	F

Show that $(p \vee q) \wedge \neg(p \wedge q)$ is logically equivalent to $p \veebar q$ by creating a truth table and verifying the last column matches the last column of the truth table given for $p \veebar q$.

7 Even More Translations. Let p = "the Declaration of Independence was signed in Philadelphia," s = "the Declaration of Independence was signed in 1776," and r = "the Declaration of Independence started the American Revolution." Translate the following from English to symbols, or from symbols to English.

(a) If the Declaration of Independence was signed in 1776, then it started the American Revolution.

(b) The Declaration of Independence was signed in 1776 or in Philadelphia, but not both.

(c) The Declaration of Independence started the American Revolution but it was signed in 1776.

(d) $(p \wedge s) \Rightarrow r$.

(e) $s \wedge p \wedge \neg r$.

(f) $\neg r \vee r$.

(g) The Declaration of Independence started the American Revolution only if it was signed in 1776 but not if it was signed in Philadelphia.

1.3 Conditional Statements

> *There can be no doubt that the knowledge of logic is of considerable practical importance for everyone who desires to think and to infer correctly.*
>
> — Alfred Tarski, *Introduction to Logic and to the Methodology of the Deductive Sciences*

You will learn . . .

1: to write the negation, converse, inverse, and contrapositive of a conditional statement and determine the truth value of each;

2: to use DeMorgan's laws to write the negation of "and" and "or" statements;

3: to determine whether two statements are logically equivalent.

We saw conditional statements in the previous section; they are statements of the form $p \Rightarrow q$ or of the form $p \Leftrightarrow q$. In this section, we will work more with conditional statements. But first, we will define what it means for two logical statements to be *logically equivalent*.

In Example 1.2.B, we created a truth table for the statement $S : (\neg p \wedge q) \Rightarrow (p \vee q)$. It is reproduced below.

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

Examine the final column $(\neg p \wedge q) \Rightarrow (p \vee q)$ and the column $\neg p$. These columns are identical. When this happens, we say that the compound statement $(\neg p \wedge q) \Rightarrow (p \vee q)$ is *logically equivalent* to $\neg p$. That is, these two compound statements have the same truth value for every truth value of the simple statements p and q. In symbols, we denote logical equivalence with $\equiv$. In this example, we would write

$$(\neg p \wedge q) \Rightarrow (p \vee q) \equiv \neg p.$$

The $\equiv$ symbol is called the equivalence symbol.

Examining a truth table is one way to prove whether two statements are logically equivalent.

▶ Example 1.3.A – The Negation of a Negation.

Show that $\neg(\neg p) \equiv p$.

▷ Solution. Let's create a truth table for $\neg(\neg p)$.

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

Since the last column is identical to the column for p, we do have $\neg(\neg p) \equiv p$.

Two sets of important logical equivalences are known as *De Morgan's laws*.

Named after 19th century English logician and mathematician Augustus De Morgan. He was fond of obscure numerical facts and liked to say that he was x years old in the year x^2.

THEOREM 1 — De Morgan's Laws.

Let p and q be simple statements. Then

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

and

$$\neg(p \vee q) \equiv \neg p \wedge \neg q.$$

Proof. You have already proven these to be true! See §1.2, Problem **2**(c) for the first equivalence and Problems **4**(a) and **4**(b) for the second equivalence. ■

▶ Example 1.3.B – Using De Morgan's Laws.

Write the negation of the statement "Riri is a computer science major and Shuri is an engineering major."

▷ Solution. The statement is of the form $r \wedge s$, so by De Morgan's laws, the negation is $\neg(r \wedge s) \equiv \neg r \vee \neg s$. Thus, the negation is "Riri is not a computer science major or Shuri is not an engineering major."

There are other useful properties that allow us to rewrite compound statements. These other useful properties—listed in the theorem on the next page—can be proved with truth tables. However, to save a few pages, we will omit the proof of these properties.

THEOREM 2 — Some Logical Equivalences.

Suppose p, q, and r are simple statements. Then we have the following logical equivalences.

1. $p \wedge q \equiv q \wedge p$
2. $p \vee q \equiv q \vee p$ *(The commutative laws.)*
3. $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
4. $(p \vee q) \vee r \equiv p \vee (q \vee r)$ *(The associative laws.)*
5. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
6. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ *(The distributive laws.)*
7. $p \vee (p \wedge q) \equiv p$
8. $p \wedge (p \vee q) \equiv p$ *(The absorption laws.)*

Logical equivalences enable one to replace a complicated compound statement with an equivalent simpler statement. This can aid in reasoning, in writing, and in thinking. The logical equivalence of a conditional statement $p \Rightarrow q$ with its *contrapositive* $\neg q \Rightarrow \neg p$ is often useful. Indeed, we may show these are logically equivalent with a truth table, as shown below.

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

Comparing the last column of this truth table with that of the truth table for $p \Rightarrow q$ on page 4, shows that

$$p \Rightarrow q \equiv \neg q \Rightarrow \neg p.$$

Being logically equivalent, a conditional statement and its contrapositive will always have the same truth value.

▶ Example 1.3.C – Using the Contrapositive.

Consider the statement

If a person is innocent of a crime, then they are not a suspect.

This sounds like it could be true. But let's examine the contrapositive of this statement. The contrapositive is

If a person is a suspect, then they are not innocent of a crime.

The contrapositive is certainly false, as someone could be a suspect and still be found innocent of a crime. Hence, the original statement must also be false.

Besides the contrapositive, we may also form the *converse* and the *inverse* of a conditional statement. Given the statement $p \Rightarrow q$, the converse is $q \Rightarrow p$ and the inverse is $\neg p \Rightarrow \neg q$. The converse of the statement in Example 1.3.C is

If a person is not a suspect, then they are innocent of a crime.

The inverse is

If a person is not innocent of a crime, then they are a suspect.

Are the converse and inverse true?

Note that the inverse is the contrapositive of the converse, so the inverse and converse are logically equivalent; i.e.,

$$q \Rightarrow p \equiv \neg p \Rightarrow \neg q.$$

▶ Example 1.3.D – Rewriting a Conditional Statement.

Consider the statement "If you paid full price, then you didn't buy it at Stan's Club." Write the contrapositive, converse, and inverse of this conditional statement in symbols and in English.

▷ Solution. Let f = "you paid full price" and s = "you bought it at Stan's Club." Then the original statement is $f \Rightarrow \neg s$. Then

$$\begin{aligned} \text{the contrapositive is} \quad & s \Rightarrow \neg f, \\ \text{the converse is} \quad & \neg s \Rightarrow f, \\ \text{and the inverse is} \quad & \neg f \Rightarrow s. \end{aligned}$$

In English, the contrapositive is

If you bought it at Stan's Club, then you didn't pay full price.

The converse is

If you didn't buy it at Stan's Club, then you paid full price.

The inverse is

If you didn't pay full price, then you bought it at Stan's Club.

Many would probably think that the negation of a conditional statement would mean that we negate the hypothesis and the conclusion. However, this is not correct! We can see why if we rewrite the conditional statement according to what we did in §1.2, Problem **2**(a). There, we found that the conditional statement $p \Rightarrow q$ is logically equivalent to $\neg p \vee q$. Thus, to negate a conditional statement, we negate $\neg p \vee q$. To do this, we make use of the properties introduced thus far.

$$\begin{aligned} \neg(\neg p \vee q) &\equiv \neg(\neg p) \wedge \neg q && \text{(by De Morgan's Laws)} \\ &\equiv p \wedge \neg q. && \text{(by Example 1.3.A)} \end{aligned}$$

Thus, the negation of a conditional statement is *not* another conditional, but it is an "and" statement!

▶ Example 1.3.E – Negation of a Conditional.

Consider the statement “If you paid full price, then you didn’t buy it at Stan’s Club.” Write the negation of this conditional statement in symbols and in English.

▷ Solution. Let f = “you paid full price” and s = “you bought it at Stan’s Club.” Our statement symbolically is $f \Rightarrow \neg s \equiv \neg f \vee \neg s$. The negation is therefore $\neg(\neg f \vee \neg s) \equiv f \wedge s$. In English, this is “You paid full price and you did buy it at Stan’s Club.”

▶ Example 1.3.F – A Taxing Contrapositive.

Consider the statement “If your filing status is single or married filing jointly and if your adjusted gross income is less than \$100,000 and if you claim no dependents and if you do not itemize your deductions, then you are eligible to file your income taxes with a Form 1040EZ.” Write the contrapositive of this statement.

This is not an exhaustive list of conditions one must meet in order to file using Form 1040EZ!

▷ Solution. There is so much here that going straight to the contrapositive in English is too complicated. We would be wise to write this in symbols, find the contrapositive of the symbolic statement, and then translate that to English. To that end, let s = “your filing status is single,” m = “your filing status is married filing jointly,” a = “your adjusted gross income is less than \$100,000,” d = “you claim no dependents,” i = “you itemize your deductions,” and f = “you are eligible to file your income taxes with a Form 1040EZ.” Then the statement in symbols is

$$(s \vee m) \wedge a \wedge d \wedge \neg i \Rightarrow f.$$

Thus, the contrapositive is

$$\begin{aligned} \neg f \Rightarrow \neg((s \vee m) \wedge a \wedge d \wedge \neg i) \\ &\equiv \neg f \Rightarrow (\neg(s \vee m)) \vee \neg a \vee \neg d \vee \neg(\neg i) \\ &\equiv \neg f \Rightarrow (\neg s \wedge \neg m) \vee \neg a \vee \neg d \vee i. \end{aligned}$$

In English, this becomes the statement “If you are not eligible to file your income taxes with a Form 1040EZ, then you are not single and not married filing jointly, or your adjusted gross income is not less than \$100,000, or you claim dependents, or you itemize your deductions.”

Problems for §1.3

1 The Contrapositive. Write the contrapositive of each conditional statement below.

(a) If $x \geq 2$, then $x^2 \geq 4$.

(b) If n is an even integer, then n^2 is divisible by 4.

(c) If today is Labor Day, then tomorrow is Tuesday.

(d) If it ain't broke, don't fix it.

(e) If you want something done right, you have to do it yourself.

(f) If these problems are not easy, then my head will ache.

(g) If a person has not done anything wrong, then they have nothing to hide.

(h) If a person did not vote in the election, then they have no right to complain about politics.

(i) If you don't care that China has access to your phone's data, then use TikTok.

2 Translations to Symbols. Suppose s = "n is divisible by 7," and t = "n is divisible by 21." Consider the statement

If n is divisible by 21,
then n is divisible by 7.

Translate this into symbols, write the converse, inverse, and contrapositive of each statement in symbols and in English, and then determine their truth values for all integers n.

3 Conditionals. Given the statement

If n is an odd integer,
then $n^2 + 1$ is divisible by 8,

write the converse, inverse, and contrapositive of the statement. Which of these four statements (the original, the converse, the inverse, or the contrapositive) do you think are true?

4 Conditional Equivalence. Are the following two statements logically equivalent?

(1) A real number is less than 1 only if its reciprocal is greater than 1.

(2) Having a reciprocal greater than 1 is a sufficient condition for a real number to be less than 1.

Justify your answer.

5 Symbolic Statements. Write the contrapositive and the negation of each statement in symbols.

(a) $(p \Rightarrow q) \Rightarrow r$

(b) $(p \vee q) \Rightarrow r$

(c) $p \Rightarrow (q \vee r)$

(d) $\neg p \Rightarrow (q \wedge r)$

6 More Negations. Write the negation of each statement.

(a) Clark is a reporter and Bruce is a millionaire.

(b) The HDMI connector is loose or the projector is unplugged.

(c) If n is divisible by 5, then the units digit of n is 0 or 5.

(d) If you eat your vegetables, then you may have cake or cookies for dessert.

(e) If $x^2 \leq 9$, then $x \geq -3$ and $x \leq 3$.

(f) If a person has not done anything wrong, then they have nothing to hide.

(g) Jeff is wealthy and generous, or Jeff is insane.

7 Unless. In everyday English, we say statements with the word "unless." Logically, to say p *unless* q means that as long as q does not happen, then p will happen. In symbols,

$$p \text{ unless } q \equiv \neg q \Rightarrow p.$$

Write the statement "The door will not open unless you have the passcode" in if-then form. What is the contrapositive of this statement?

8 Various Conditionals. Consider the following statement: "If the solution is not boiling, then its temperature must be less than 302°F." Assuming that this statement is true, which of the following must also be true?

A) If the temperature of the solution is less than 302°F, then the solution is not boiling.

B) If the temperature of the solution is at least 302°F, then the solution is boiling.

C) The solution will boil only if its temperature is less than 302°F.

D) If the solution is boiling, then its temperature is at least 302°F.

E) A necessary condition for the solution to not boil is that its temperature be less than 302°F.

F) A sufficient condition for the solution to not boil is that its temperature be less than 302°F.

G) The temperature of the solution is less than 302°F unless the solution is boiling.

2.8 Linear Combinations

> *To some extent the beauty of number theory seems to be related to the contradiction between the simplicity of the integers and the complicated structure of the primes, their building blocks. This has always attracted people.*
>
> — Andreas Knauf, *Number Theory, Dynamical Systems and Statistical Mechanics*

You will learn . . .

1: to write the gcd of two positive integers as a linear combination of those two positive integers;

2: to apply the linear combination of the gcd to prove statements about the gcd.

The Euclidean algorithm not only provides a way to find the greatest common divisor of two integers a and b. It also helps us write the greatest common divisor of a and b in the form $ax + by$ for some integers x and y. This form is called the *linear combination* of a and b. It turns out that this form is quite useful for many different things, and we will call upon a linear combination of a and b often.

Indeed, we have already seen linear combinations at work. Recall from §2.2 the problem of proving that all amounts of money greater than 11 cents can be made using only 3-cent and 7-cent coins (Theorem 24). We noted that 13 cents can be made with two 3-cent coins and one 7-cent coin. This is a linear combination: 13 is the linear combination of 3 and 7, since $13 = 3 \cdot 2 + 7 \cdot 1$. Additionally, 14 is the linear combination of 3 and 7, since $14 = 3 \cdot 0 + 7 \cdot 2$, and 15 is the linear combination of 3 and 7, since $15 = 3 \cdot 5 + 7 \cdot 0$.

If we allow negative integers as possible values of x and y (which removes this from the "practical" coin problem), then we may also write 11 as a linear combination of 3 and 7 as $11 = 3 \cdot 55 + 7 \cdot (-22)$. We can also write 1 as a linear combination of 3 and 7 as $1 = 3 \cdot 5 + 7 \cdot (-2)$.

However, writing any integer as a linear combination of any other pair of integers does not always work. For instance, there is no way to write 1 as a linear combination of 6 and 9. Let's justify this. For the sake of contradiction, suppose we could. Then there are integers x and y such that $1 = 6x + 9y$. Then $1 = 3(2x + 3y)$. However, the right side, $3(2x + 3y)$, is divisible by 3, but the left side is not; this is impossible. Thus, $1 \neq 6x + 9y$. Now, if the number on the right was a multiple of 3, this would be possible! Certainly, $3 = 6x + 9y$ for $x = 2$ and $y = -1$. But notice that we can divide both sides of $3 = 6x + 9y$ by 3, giving us $1 = 2x + 3y$ which is satisfied by $x = -1$ and $y = 1$. That is, we can reduce $3 = 6x + 9$ by the greatest common factor of 6 and 9. This leads us to the next theorem.

THEOREM 40 — GCD and Linear Combinations.

Let $a, b \in \mathbb{Z}$, $b \neq 0$, and let $d = \gcd(a, b)$. Then d is the smallest positive linear combination of a and b, and all other linear combinations of a and b equal multiples of d.

Proof. Let $a, b \in \mathbb{Z}$, $b \neq 0$, and let $d = \gcd(a, b)$. In using the Euclidean algorithm to compute d, we find that $d = r_{n-1}$, the last nonzero remainder. The equation resulting from the $(n-1)$th division is $r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}$. From this, we can write

$$d = r_{n-1} = r_{n-3} - r_{n-2}q_{n-1} = r_{n-3} \cdot 1 + r_{n-2} \cdot (-q_{n-1}).$$

Thus, d is a linear combination of r_{n-3} and r_{n-2}. Now we take the equation resulting from the $(n-2)$th division, $r_{n-4} = r_{n-3}q_{n-2} + r_{n-2}$. Solving this equation for r_{n-2}, we then have

$$\begin{aligned} d = r_{n-1} &= r_{n-3} \cdot 1 + r_{n-2} \cdot (-q_{n-1}) \\ &= r_{n-3} \cdot 1 + (r_{n-4} - r_{n-3}q_{n-2} \cdot (-q_{n-1}) \\ &= r_{n-3} - r_{n-4}q_{n-1} + r_{n-3}q_{n-2}q_{n-1} \\ &= r_{n-3}(1 + q_{n-2}q_{n-1}) + r_{n-4} \cdot (-q_{n-1}). \end{aligned}$$

Thus, d is a linear combination of r_{n-3} and r_{n-4}. Expressing r_{n-3} from the $(n-3)$th division and substituting, we will arrive at the fact that d is a linear combination of r_{n-4} and r_{n-5}. Continue this process—going "backwards" through the Euclidean algorithm—and we will obtain in the final step that d is a linear combination of a and b. This must be the smallest positive linear combination: if there were one smaller, then that would be the greatest common divisor of a and b.

Now consider $as + bt$ for some integers s and t. Since $d \mid a$ and $d \mid b$, then $d \mid (as + bt)$. Hence, $\exists\ k \in \mathbb{Z}$ s.t. $dk = as + bt$. Therefore any other linear combination of a and b is a multiple of d. ■

The proof of the previous theorem shows how to actually find a linear combination of $\gcd(a, b)$ in terms of a and b. We do this in the next example.

▶ Example 2.8.A – Finding a Linear Combination.

In Example 2.7.C, we found that $\gcd(23408, 171304) = 1064$. Thus we can write 1064 as a linear combination of 23408 and 171304. Solving the equation $23408 = 7448 \cdot 3 + 1064$ for 1064, we get $1064 = 23408 + 7448 \cdot (-3)$. Solving the equation $171304 = 23408 \cdot 7 + 7448$ for 7448, we get $7448 = 171304 + 23408 \cdot (-7)$. Now we substitute.

$$\begin{aligned} 1064 &= 23408 + 7448 \cdot (-3) \\ &= 23408 + (171304 + 23408 \cdot (-7)) \cdot (-3) \\ &= 23408 + 171304 \cdot (-3) + 23408 \cdot (-7) \cdot (-3) \\ &= 23408 \cdot (1 + (-7) \cdot (-3)) + 171304(-3) \\ &= 23408 \cdot 22 + 171304 \cdot (-3). \end{aligned}$$

Hence, $1064 = 23408 \cdot 22 + 171304 \cdot (-3)$.

▶ Example 2.8.B – Finding a Linear Combination.

In Example 2.7.D, we found that $\gcd(2027, 5040) = 1$. Thus we can write 1 as a linear combination of 2027 and 5040. Solving the equation $4 = 3 \cdot 1 + 1$ for the remainder 1, we get $1 = 4 + 3 \cdot (-1)$. Solving the equation $51 = 4 \cdot 12 + 3$ for 3, we get $3 = 51 + 4 \cdot (-12)$. Now we substitute.

$$\begin{aligned} 1 &= 4 + 3 \cdot (-1) \\ &= 4 + (51 + 4 \cdot (-12)) \cdot (-1) \\ &= 4 \cdot 13 + 51 \cdot (-1). \end{aligned}$$

Next, we solve $55 = 51 \cdot 1 + 4$ for 4 to get $4 = 55 + 51 \cdot (-1)$. Now substitute:

$$\begin{aligned} &= (55 + 51 \cdot (-1)) \cdot 13 + 51 \cdot (-1) \\ &= 55 \cdot 13 + 51 \cdot (-14) \end{aligned}$$

Now we move to the equation $986 = 55 \cdot 17 + 51$, which we solve for 51: $51 = 986 + 55 \cdot (-17)$. Then

$$\begin{aligned} &= 55 \cdot 13 + (986 + 55 \cdot (-17)) \cdot (-14) \\ &= 55 \cdot 251 + 986 \cdot (-14) \end{aligned}$$

From $2027 = 986 \cdot 2 + 55$ we write $55 = 2027 + 986 \cdot (-2)$. Then

$$\begin{aligned} &= (2027 + 986 \cdot (-2)) \cdot 251 + 986 \cdot (-14) \\ &= 2027 \cdot 251 + 986 \cdot (-516) \end{aligned}$$

Finally, we use $5040 = 2027 \cdot 2 + 986$ to write $986 = 5040 + 2027 \cdot (-2)$. We get

$$\begin{aligned} &= 2027 \cdot 251 + (5040 + 2027 \cdot (-2)) \cdot (-516) \\ &= 2027 \cdot 1283 + 5040 \cdot (-516). \end{aligned}$$

Hence, $1 = 2027 \cdot 1283 + 5040 \cdot (-516)$.

The fact that we can write the greatest common divisor of a and b as a linear combination of a and b implies the following: $a \perp b$ if and only if 1 can be written as a linear combination of a and b.

The fact that we can write the greatest common divisor of a and b as a linear combination of a and b also allows us to prove some rather interesting facts.

THEOREM 41.

Let $a, b, c \in \mathbb{Z}^+$. If $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$, then $\gcd(ab, c) = 1$.

Proof. Let $a, b, c \in \mathbb{Z}^+$ s.t. $\gcd(a, c) = \gcd(b, c) = 1$. Then by Theorem 40, $\exists\ s, t, x, y \in \mathbb{Z}$ s.t. $1 = as + ct$ and $1 = bx + cy$. Multiply these equations together. This gives us

$$\begin{aligned} 1 &= (as + ct)(bx + cy) \\ &= (as)(bx) + (as)(cy) + (ct)(bx) + (ct)(cy) \\ &= (ab)(sx) + c(asy + tbx + cty). \end{aligned}$$

The integers are closed, so $sx \in \mathbb{Z}$ and $asy + tbx + cty \in \mathbb{Z}$. Let $m = sx$ and $n = asy + tbx + cty$. Then $1 = (ab)m + cn$ expresses 1 as a linear combination of ab and c. Therefore, $\gcd(ab, c) = 1$. ■

THEOREM 42.

For $a, b \in \mathbb{Z}$, $\gcd(a, b) = d$ if and only if $\gcd(a/d, b/d) = 1$.

Proof. Let $a, b \in \mathbb{Z}$ s.t. $\gcd(a, b) = d$. Then by Theorem 40, $\exists\ x, y \in \mathbb{Z}$ s.t. $d = ax + by$. However, since $d \mid a$ and $d \mid b$, we may divide the equation $d = ax + by$ by d to get $1 = (a/d)x + (b/d)y$. Hence, $\gcd(a/d, b/d) = 1$.

Now assume $\gcd(a/d, b/d) = 1$. Then by Theorem 40, $\exists\ s, t \in \mathbb{Z}$ s.t. $1 = (a/d)s + (b/d)t$. Multiplying both sides of this equation by d yields $d = as + by$. Hence, $\gcd(a, b) = d$. ■

Important? Some would say it's fundamental!

Finally, we have all we need to prove an important result about the prime factorization of an integer.

THEOREM 43 — The Fundamental Theorem of Arithmetic.

Every integer greater than 1 is either prime or can be expressed uniquely (disregarding the order of the factors) as a product of primes.

Proof. Let $n \in \mathbb{Z}$ where $n > 1$. We will use strong induction. *Strong Basis.* If $n = 2$, the statement is true since 2 is prime.

Strong inductive hypothesis. Assume the statement is true for all n where $2 \leq n < m$. That is, assume that n is either prime or can be expressed uniquely as a product of primes for all values of n from 2 to $m - 1$.

Proof of strong induction. By Theorem 25, m is either a prime or a product of primes. If m is prime, we are done. So assume m is a product of primes. For the sake of contradiction, let m have the two prime factorizations

$$m = p_1 \cdot p_2 \cdot p_3 \cdots p_i = q_1 \cdot q_2 \cdot q_3 \cdots q_k,$$

where the primes are not necessarily distinct. We want to show that this assumption leads to a contradiction. Now, since $p_1 \mid m$ and $p_1 \mid q_1 \cdot q_2 \cdot q_3 \cdots q_k$, then $p_1 \mid q_j$ for some j, $1 \leq j \leq k$. But q_j is prime as well, so $p_1 = q_j$. Relabeling q_j as q_1, we have $p_1 = q_1$. Now consider the integer

$$\frac{n}{p_1} = p_2 \cdot p_3 \cdots p_i = q_2 \cdot q_3 \cdots q_k < n.$$

The integer n/p_1, being less than n, is covered by the inductive hypothesis, so n/p_1 is a unique product of primes. Hence, $i = k$, and after a suitable rearrangement, $p_j = q_j$ for $j = 2, 3, \ldots, k$. This is the contradiction we seek; indeed, multiplying by p_1 we get

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_k = p_1 \cdot q_2 \cdot q_3 \cdots q_k.$$

Therefore, the prime factorization is unique. ■

Problems for §2.8

1 Linear Combinations. For each pair of integers a, b in §2.7, Problem **1**, find integers x and y such that $ax + by = \gcd(a, b)$.

2 Integer Solutions. Does $637x + 5005y = 91$ have an integer solution? How do you know without actually finding the solution?

3 Proofs. Prove the following statements.

(a) Let $a, b, c \in \mathbb{Z}$. If $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$. (This result is known as Euclid's Lemma.)

(b) Let $a, b, c \in \mathbb{Z}$. If $a \mid c$, $b \mid c$, and $\gcd(a, b) = 1$, then $ab \mid c$.

(c) Let $a, b \in \mathbb{Z}, n \in \mathbb{Z}^+$, and $ab \equiv 1 \bmod n$. Prove that $a \perp n$ and $b \perp n$.

(d) Let $a \in \mathbb{Z}, n \in \mathbb{Z}^+$, and $a \perp n$. Prove $\exists\ b \in \mathbb{Z}$ s.t. $ab \equiv 1 \bmod n$.

4 More Linear Combinations. Find integers x, y, and z such that $78x + 403y + 754z = 13$. (*Hint:* Remember §2.7, Problem **3**?)

5 A Throwback. How many points (x, y) with integer coordinates lie on the line $5x + 7y = 1$ where x and y are each greater than -100 and each less than 100?

6 Least Common Multiple. The *least common multiple* of two integers a and b is the smallest integer which both a and b divide. We denote this by $\operatorname{lcm}(a, b)$.

(a) Let $a, b \in \mathbb{Z}^+$. Prove that $ab/\gcd(a, b) = \operatorname{lcm}(a, b)$.

(b) Use part (a) to find $\operatorname{lcm}(12, 30)$.

(c) Use part (a) to find $\operatorname{lcm}(56, 88)$.

(d) Use part (a) to find $\operatorname{lcm}(385, 1001)$.

(e) Use part (a) to find $\operatorname{lcm}(1739, 29341)$.

2.9 Linear Congruences

> *Mathematics is the queen of the sciences and number theory is the queen of mathematics.*
> *She often condescends to render service to astronomy and other natural sciences,*
> *but in all relations she is entitled to the first rank.*
>
> — Karl Gauss, quoted in *Gauss, zum Gedächtnis,* by Wolfgang von Waltershausen

You will learn . . .
1: to solve linear congruences;
2: to find the inverse of an integer for a certain modulus.

What integer leaves a remainder of 4 when divided by 7? That seems like an easy problem. A moment's thought and we can easily come up with and an answer: 11. But there are more: 18, 25, 32, and so on. And let's not forget 4 as a solution! And of course, the problem did not specify that the integer we want had to be positive! That means -3 works, as does -10, -17, -24, and so on. In fact, every integer that can be represented as $7n+4$ for $n \in \mathbb{Z}$ is a solution to this problem. Hence, the solution set is $\{x \in \mathbb{Z} \mid x = 7n+4\ \ \forall\ n \in \mathbb{Z}\}$.

This problem really asks us to find an integer that is congruent to 4 modulo 7. That is, we are asked to solve the *linear congruence* $x \equiv 4 \bmod 7$. We have found the solution to be $x = 7n + 4$ for $n \in \mathbb{Z}$. We can also get this solution using the definition of congruent. Since

3.8 Trees

It has been said that combinatorics is both the easiest and hardest field of mathematics. Easy since a lot of it requires no prerequisite knowledge. Hence a High School Student can do work in it. Hard because a lot of it requires no prerequisite knowledge. Hence you can't easily apply continuous techniques.

— William Gasarch, Open Problems Column, *SIGACT News*, March 2020

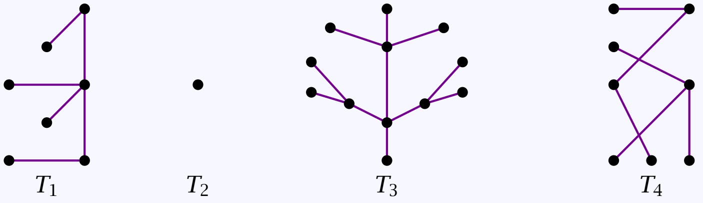
You will learn . . .

1: to use properties of trees to prove statements about them;
2: to compute the number of distinct labeled trees on n vertices;
3: to find a spanning tree of a graph.

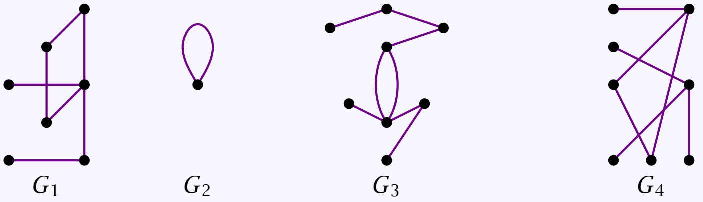
Now we will focus on a particular type of graph called a *tree*. A tree is a connected graph that has no circuits; in other words, a tree is a connected graph that is *circuit-free*. It is possible for a non-connected graph to have connected components that are trees. If that is the case, then the graph with each connected component a tree is called – wait for it – a *forest*.

▶ Example 3.8.A – Some Trees.

The following graphs are trees. Note that the graph T_4 is not connected, but each component is a tree. Hence T_4 is a forest.



The following graphs are not trees. Notice that they contain at least one circuit.



Trees have useful and interesting properties.

THEOREM 68.

Any tree with more than one vertex has a vertex of degree 1.

Proof. For the sake of contradiction, suppose G is a tree with more than one vertex that has no vertices of degree 1. Then each vertex has degree at least 2. It follows that G has a circuit, but this contradicts the fact that G is a tree. Hence, G must have at least one vertex of degree 1. ∎

THEOREM 69 — The Tree Theorem.

Let $n \in \mathbb{Z}^+$ and let G be a connected graph on n vertices. G is a tree if and only if G has $n-1$ edges.

Proof. Let $n \in \mathbb{Z}^+$ and let G be a connected graph on n vertices. Suppose G is a tree. We will show that G has $n-1$ edges.

Basis. There is only one tree on one vertex, and it has $1-1=0$ edges. The statement is true for $n=1$.

Induction hypothesis. Assume the statement is true for $n=k$. That is, assume that a tree on k vertices has $k-1$ edges.

Proof of induction. Now we must show the statement true for $n=k+1$. That is, we must show that a tree on $k+1$ vertices has $k+1-1=k$ edges. Consider the tree G on $k+1$ vertices. By Theorem 68, there is at least one vertex of G with degree 1. Let v be a vertex of G with degree 1, and consider the graph T formed by removing vertex v and its incident edge. Then T is a tree on k vertices. By the induction hypothesis, T has $k-1$ edges. Adding vertex v and its incident edge back to the tree, the result is a graph with one more vertex and one more edge. Hence, G has $k+1$ vertices and $k-1+1=k$ edges.

Now suppose G has $n-1$ edges. We will show that G is a tree. For the sake of contradiction, assume that G is not a tree; that is, assume that G has a circuit. Remove edges from the circuit until we obtain a connected graph H without a circuit. Suppose we remove m such edges. Then H is a tree on n vertices with $n-1-m$ edges. However, this contradicts the fact that a tree on n vertices must have $n-1$ edges. Therefore, G must be a tree. ■

Trees can be used to model many practical situations, such as ancestry, computer database searching, and many others. We have seen one example already at the beginning of this chapter (Figure 3.1 on page 124), which is known as a decision tree. Another fascinating example of the uses of trees is chemistry. Consider the two chemicals methylpropane and butane, shown below in Figure 3.16.

Both methylpropane and butane have the chemical formula C_4H_{10}, but they are different molecules because of the way the carbon atoms are connected. Viewing the molecules as a graph, we could create an adjacency matrix for such a molecule. Certain properties of the matrix (which we will not go into here) correspond to certain properties of the molecule. This field of study is called *spectral graph theory*.

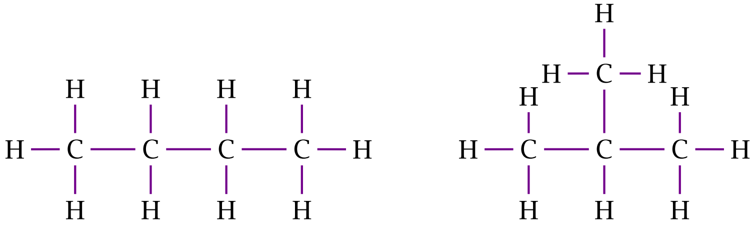


Figure 3.16 – The chemicals butane (left) and methylpropane (right) both have the same chemical formula.

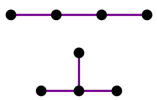


Figure 3.17 – The two non-isomorphic trees on 4 vertices.

Without going into adjacency matrices, we can see that each carbon atom must have degree 4. However, to maintain this degree, the carbon atoms themselves must form a tree! Then the question naturally arises: How many other molecules are there with 4 carbon atoms and 10 hydrogren atoms? That is, how many other non-isomorphic trees are there on 4 vertices? As it turns out, there are only 2. The number of non-isomorphic trees on n vertices is an open research problem; that is, no one has been able to find a formula in terms of n for this number. However, the numbers of such graphs have been computed for very large values of n.

For instance there are 11 non-isomorphic trees on 7 vertices, but there are 823065 on 20 vertices! For a list, see sequence A000055 in The On-Line Encyclopedia of Integer Sequences.

One question that we can answer is the total number of trees (whether isomorphic or not) on n distinct vertices. We count trees on distinct vertices by considering each vertex to be labeled. In this way, we count the possible ways to join distinct vertices with an edge. So what we are really counting is how to assign degrees to each vertex. For instance, a tree on 3 vertices must have degrees 1, 1, and 2, but there are 3 ways to assign which distinct vertex gets the degree of 2. This creates 3 possible ways to create a tree on 3 distinct vertices. To prove this requires the fact that the total degree of any tree on n vertices is $2n - 2$. (You will prove this fact in Problem **5**.)

If the vertex is left unlabeled - that is, if we did not consider them distinct - there is only 1 tree on 3 vertices.

THEOREM 70 — The Number of Trees of Given Vertex Degrees.

Let $n \in \mathbb{Z}^+$ and let $d_1, d_2, \ldots, d_n$ be a sequence of n postitive integers such that $d_1 + d_2 + \cdots + d_n = 2n - 2$. Then there are

$$\binom{n-2}{d_1 - 1, d_2 - 1, \ldots, d_n - 1}$$

labeled trees on n vertices, where $\deg(v_k) = d_k$ for $k = 1, 2, \ldots, n$.

Proof. Let $n \in \mathbb{Z}^+$ and let $d_1, d_2, \ldots, d_n$ be a sequence of n postitive integers such that $d_1 + d_2 + \cdots + d_n = 2n - 2$. *Basis.* Let $n = 2$. Then there is 1 tree on 2 vertices. This tree has two vertices and one edge, so $\deg(v_1) = d_1 = 1$ and $\deg(v_2) = d_2 = 1$. We also have

$$\binom{2-2}{1-1, 1-1} = \binom{0}{0, 0} = \frac{0!}{0!0!} = 1.$$

Thus, the statement is true for $n = 2$.

Induction hypothesis. Assume the statement is true for $n = m$. That is, assume that there are

$$\binom{m-2}{d_1 - 1, d_2 - 1, \ldots, d_m - 1}$$

trees on m vertices where $\deg(v_k) = d_k$ for $k = 1, 2, \ldots, m$.

Proof of induction. Now we show the statement is true for $n = m + 1$. That is, we will prove that there are

$$\binom{m-1}{d_1 - 1, d_2 - 1, \ldots, d_{m+1} - 1}$$

trees on $m+1$ vertices where $\deg(v_k) = d_k$ for $k = 1, 2, \ldots, m+1$. By Theorem 68, there is some vertex of degree 1. Let v_1 be this vertex. Any of the other m vertices could be adjacent to v_1. Hence, of the m other vertices, one of the them has degree one less. Thus, by the induction hypothesis, the number of trees on m vertices is

If v_1 is not a vertex of degree 1, we can re-label the vertices so that v_1 becomes a vertex of degree 1.

$$\binom{m-2}{d_2-2, d_3-1, \ldots, d_m-1} + \binom{m-2}{d_2-1, d_3-2, \ldots, d_m-1} + \cdots + \binom{m-2}{d_2-1, d_3-1, \ldots, d_m-2}$$

since v_1 could be adjacent to any of the other vertices. Finally, by Theorem 59, this sum is

$$\binom{m-1}{d_2-1, d_3-1, \ldots, d_m} = \binom{m-1}{0, d_2-1, d_3-1, \ldots, d_m} = \binom{m-1}{d_1-1, d_2-1, \ldots, d_m}.$$

Note that $d_1 = 1$ so that $d_1 - 1 = 0$, and thus $\deg(v_k) = d_k$ for $k = 1, 2, \ldots, m+1$. Therefore, the statement is true for $n \in \mathbb{Z}^+$. ■

Now we are able to use Theorem 70 to help us prove a statement concerning the total number of trees on any number of distinct vertices.

THEOREM 71 — The Number of Trees.

The number of trees on n labeled vertices is n^{n-2}.

Proof. Let $n \in \mathbb{Z}^+$. Suppose n vertices are labeled $v_1, v_2, \ldots, v_n$, and the degree of vertex v_i is d_i for $i = 1, 2, \ldots, n$. The total degree is therefore $d_1 + d_2 + \cdots + d_n = 2n - 2$. Note that

$$d_1 - 1 + d_2 - 1 + \cdots + d_n - 1 = 2n - 2 - n = n - 2.$$

Then the number of all possible trees is the sum

$$\sum_{\substack{d_1, d_2, \ldots, d_n \geq 1 \\ d_1 + d_2 + \cdots + d_n = 2n-2}} \binom{n-2}{d_1-1, d_2-1, \ldots, d_n-1}.$$

This sum represents the sum of all $n-2$ multinomial coefficients. By Problem 5(e) of §3.3, this is n^{n-2}. ■

Using ideas from combinatorics to determine facts about graphs is the field of *combinatorial graph theory*. What we have introduced so far in counting the number of trees on n vertices is the tip of the iceberg of this growing field of study. There is also an overlap of techniques and topics with spectral graph theory which adds to the interest.

This was my own research interest for my post-graduate degrees.

▶ Example 3.8.B – The Number of Trees.

How many trees are there on 5 vertices with degrees 1, 1, 1, 2, and 3? How many trees are there on 5 distinct vertices?

▷ Solution. By Theorem 70, there are

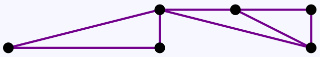
$$\left(\begin{matrix}5-2\\0,0,0,1,2\end{matrix}\right)=\left(\begin{matrix}3\\1,2\end{matrix}\right)=\frac{3!}{1!2!}=3$$

trees on 5 vertices with degrees 1, 1, 1, 2, and 3. By Theorem 71, there are $5^{5-2}=5^3=125$ trees on 5 distinct vertices.

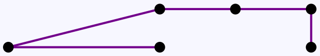
Trees can be found in many places, even in other graphs! Consider a graph G on n vertices. A tree that contains every vertex of G is called a *spanning tree*.

▶ Example 3.8.C – A Spanning Tree.

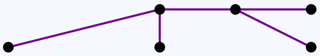
In the graph G, below find a spanning tree.



▷ Solution. One such spanning tree is below.



Of course, there are others. Another one is below.



Note that the spanning trees are, by definition, subgraphs of G.

One question we can ask about spanning trees concerns how many spanning trees a given graph can have. Unfortunately, there is no simple formula for this either! The formulas involve altering the adjacency matrix of the graph and then computing certain quantities; so an operation exists to find this number, but no simple formula. However, there are simple formulas for certain kinds of graphs.

THEOREM 72 — Number of Spanning Trees in Complete Bipartite Graphs.

Let $n, m \in \mathbb{Z}^+$. The number of spanning trees on the complete bipartite graph $K_{m,n}$ is $m^{n-1}n^{m-1}$.

Proof. Let $n, m \in \mathbb{Z}^+$. The vertices of $K_{m,n}$ are split into two disjoint subsets such that each of the m vertices is adjacent to each of the n vertices. Note that the total degree of every spanning tree of $K_{m,n}$ is $2(m+n)-2$. Thus the sum of the degrees of the m vertices is

$d_1 + d_2 + \cdots + d_m = m + n - 1$, and the sum of the degrees of the n vertices $d_{m+1} + d_{m+2} + \cdots + d_{m+n} = m + n - 1$. Now we use Theorems 70 and 71. Note that $d_1 - 1 + d_2 - 1 + \cdots + d_m - 1 = m + n - 1 - m = n - 1$. Summing all possible trees on the m vertices, we get

$$\sum_{\substack{d_1, d_2, \ldots, d_m \geq 1 \\ d_1 + d_2 + \cdots + d_m = n-1}} \binom{n-1}{d_1 - 1, d_2 - 1, \ldots, d_m - 1} = m^{n-1}.$$

Now for the other vertices. Note that $d_{m+1} - 1 + d_{m+2} - 1 + \cdots + d_{m+n} - 1 = m + n - 1 - n = m - 1$. Summing all possible trees on the n vertices, we get

$$\sum_{\substack{d_1, d_2, \ldots, d_n \geq 1 \\ d_{m+1} + d_{m+2} + \cdots + d_{m+n} = m-1}} \binom{m-1}{d_{m+1} - 1, d_{m+2} - 1, \ldots, d_{m+n} - 1} = n^{m-1}.$$

By the multiplication rule, the total number of spanning trees of $K_{m,n}$ is $m^{n-1} n^{m-1}$. ■

Problems for §3.8

1 Trees. Which of the graphs in §3.6, Problem 2 are trees? Which, if any, are forests?

2 Chemistry. There are three possible ways to draw a graph representing C_5H_{12}. Draw them, assuming each carbon atom has the maximum number of hydrogen atoms.

3 Number of Trees. Compute the number of

(a) trees on 6 vertices of degrees 1, 1, 2, 2, 2, 2.

(b) trees on 6 vertices of degrees 1, 1, 1, 1, 2, 4.

(c) trees on 8 vertices of degrees 1, 1, 1, 1, 1, 3, 3, 3.

(d) trees on 2 distinctly-labeled vertices.

(e) trees on 6 distinctly-labeled-vertices.

(f) trees on 8 distinctly-labeled-vertices.

(g) spanning trees on $K_{3,4}$.

(h) spanning trees on $K_{5,5}$.

4 Spanning Trees. Suppose the graph G has 15 vertices and 22 edges. How many edges would need to be removed to obtain a spanning tree of G?

5 Proofs. Prove the following statements about trees.

(a) The total degree of any tree on n vertices is $2n - 2$.

(b) Every edge of a tree is a bridge.

(c) If G is a tree, then there is a unique path between any two vertices of G.

(d) If there is a unique path between any two vertices of a connected graph G, then G is a tree.

(e) If a connected graph G has n vertices and m edges, where $m \geq n$, then G has a circuit.

(f) The total number of spanning trees of the complete graph K_n is n^{n-2}.

(g) The total number of spanning trees of the cycle graph C_n is n.

6 Trees and Degrees. Suppose T is a tree on n vertices. What is the largest possible degree of a vertex of T?

7 Chemistry. Let G be a graph representing a molecule made from c carbon atoms and h hydrogen atoms, where there are the maximum number of hydrogen atoms for each carbon atom. What is the total degree, in terms of c and h, of G?