To the Instructor

Please also read the "To the Student."

Why do we teach discrete mathematics? I think there are two good reasons. First, discrete mathematics is useful, especially to students whose interests lie in computer science and engineering, as well as those who plan to study probability, statistics, operations research, and other areas of modern applied mathematics. But I believe there is a second, more important reason to teach discrete mathematics. Discrete mathematics is an excellent venue for teaching students to write proofs.

Thus this book has two primary objectives:

- to teach students fundamental concepts in discrete mathematics (from counting to basic cryptography to graph theory) and
- to teach students proof-writing skills.

Audience and Prerequisites

This text is designed for an introductory-level course on discrete mathematics. The aim is to introduce students to the world of mathematics through the ideas and topics of discrete mathematics.

A course based on this text requires only core high school mathematics: algebra and geometry. No calculus is presupposed or necessary.

Serving the computer science/engineering student.

Discrete mathematics courses are taken by nearly all computer science and computer engineering students. Consequently, some discrete mathematics courses focus on topics such as logic circuits, finite state automata, Turing machines, algorithms, and so on. Although these are interesting, important topics, there is more that a computer scientist/engineer should know. We take a broader approach. All of the material in this book is directly applicable to computer science and engineering, but it is presented from a mathematician's perspective. As college instructors, our job is to educate students, not just to train them. We serve our computer science and engineering students better by giving them a broader approach, by exposing them to different ideas and perspectives, and, above all, by helping them to think and write clearly. To be sure, in this book you will find algorithms and their analysis, but the emphasis is on mathematics.

Topics Covered and Navigating the Sections

The topics covered in this book include

- the nature of mathematics (definition, theorem, proof, and counterexample),
- basic logic,
- lists and sets,
- relations and partitions,
- advanced proof techniques,
- recurrence relations,
- functions and their properties,
- permutations and symmetry,
- discrete probability theory,
- number theory,
- group theory,
- public-key cryptography,
- graph theory, and
- partially ordered sets.

Furthermore, enumeration (counting) and proof writing are developed throughout the text. Please consult the table of contents for more detail.

Each section of this book corresponds (roughly) to one classroom lecture. Some sections do not require this much attention, and others require two lectures.

There is enough material in this book for a year-long course in discrete mathematics. If you are teaching a year-long sequence, you can cover all the sections.

A semester course based on this text can be roughly divided into two halves. In the first half, core concepts are covered. This core consists of Sections 3 through 24 (optionally omitting Sections 18 and 19).

From there, the choice of topics depends on the needs and interests of the students.

Sample Course Outlines

Thanks to its plentiful selection of topics, this book can serve a variety of discrete mathematics courses. The following outlines provide some ideas on how to structure a course based on this book.

- **Computer science/engineering focus**: Cover sections 1–17, 20–24, 29, 30–34, 35–37, 47–50, and 52. This plan covers the core material, special computer science notation, discrete probability, essential number theory, and graph theory.
- **Abstract algebra focus**: Cover sections 1–17, 20–28, and 35–46. This plan covers the core material, permutations and symmetry, number theory, group theory, and cryptography.
- **Discrete structures focus**: Cover sections 1–27, 47–57, and 59. This plan includes the core material, inclusion-exclusion, multisets, permutations, graph theory, and partially ordered sets.
- **Broad focus**: Cover sections 1–17, 20–24, 26–27, 35–39, 43–46, and 47–53. This plan covers the core material, permutations, number theory, cryptography, and graph theory.

Special Features

- **Proof templates**: Many students find proof writing difficult. When presented with a task such as proving two sets are equal, they have trouble structuring their proof and don't know what to write first. (See Proof Template 5 on page 44.) The proof templates appearing throughout this book give students the basic skeleton of the proof as well as boilerplate language. A list of the proof templates appears on the inside front cover.
- **Growing proofs**: Experienced mathematicians can write proofs sentence by sentence in proper order. They are able to do so because they can see the entire proof in their minds before they begin. Novice mathematicians (our students) often cannot see the whole proof before they begin. It is difficult for a student to learn how to write a proof simply by studying completed examples. I instruct students to begin their proofs by first writing the first sentence and next writing the last sentence. We then work the proof from both ends until we (ideally) meet in the middle.

  This approach is presented in the text through ever-expanding proofs in which the new sentences appear in color. See, for example, the proof of Proposition 12.11 (pages 60–63).
- **Mathspeak**: Mathematicians write well. We are concerned with expressing our ideas clearly and precisely. However, we change the meaning of some words (e.g., *injection* and *group*) to suit our needs. We invent new words (e.g., *poset* and *bijection*), and we change the part of speech of others (e.g., we use the noun *maximum* and the preposition *onto* as adjectives). I point out and explain many of the idiosyncrasies of mathematical English in marginal notes flagged with the term *Mathspeak*. In addition, a new section on mathematical writing has been included in the first chapter.
- **Hints**: Appendix A contains an extensive collection of hints (and some answers). It is often difficult to give hints that point a student in the correct direction without revealing the full answer. Some hints may give away too much, and others may be cryptic, but on balance, students will find this section enormously helpful. They should be instructed to consult this section only after mounting a hearty first attack on the problems.
- **Answers**. An *Instructor's Manual* is available from the publisher (Cengage). Not only does this supplement give solutions to all the problems, it also gives helpful tips for

teaching each of the sections. I strongly encourage you to obtain a copy. The *Instructor's Manual* is not available to students.

- **Self tests**. Every chapter ends with a self test for students. Complete answers appear in Appendix B. These problems are of varying degrees of difficulty. Instructors may wish to specify which problems students should attempt in case not all sections of a chapter have been covered in class.

CHAPTER

1 Fundamentals

The cornerstones of mathematics are definition, theorem, and proof. *Definitions* specify precisely the concepts in which we are interested, *theorems* assert exactly what is true about these concepts, and *proofs* irrefutably demonstrate the truth of these assertions.

Before we get started, though, we ask a question: Why?

1 Joy

Why?

Please also read the *To the Student* preface, where we briefly address the questions: What is mathematics, and what is discrete mathematics? We also give important advice on how to read a mathematics book.

Before we roll up our sleeves and get to work in earnest, I want to share with you a few thoughts on the question: Why study mathematics?

Mathematics is incredibly useful. Mathematics is central to every facet of modern technology: the discovery of new drugs, the scheduling of airlines, the reliability of communication, the encoding of music and movies on CDs and DVDs, the efficiency of automobile engines, and on and on. Its reach extends far beyond the technical sciences. Mathematics is also central to all the social sciences, from understanding the fluctuations of the economy to the modeling of social networks in schools or businesses. Every branch of the fine arts—including literature, music, sculpture, painting, and theater—has also benefited from (or been inspired by) mathematics

Because mathematics is both flexible (new mathematics is invented daily) and rigorous (we can incontrovertibly prove our assertions are correct), it is the finest analytic tool humans have developed.

The unparalleled success of mathematics as a tool for solving problems in science, engineering, society, and the arts is reason enough to actively engage this wonderful subject. We mathematicians are immensely proud of the accomplishments that are fueled by mathematical analysis. However, for many of us, this is not the primary motivation to study mathematics.

The Agony and the Ecstasy

Why do mathematicians devote their lives to the study of mathematics? For most of us, it is because of the joy we experience when doing mathematics.

Mathematics is difficult for everyone. No matter what level of accomplishment or skill in this subject you (or your instructor) have attained, there is always a harder, more frustrating problem waiting around the bend. Demoralizing? Hardly! The greater the challenge, the greater the sense of accomplishment we experience when the challenge has been met. The best part of mathematics is the joy we experience in practicing this art.

Most art forms can be enjoyed by spectators. I can delight in a concert performed by talented musicians, be awestruck by a beautiful painting, or be deeply moved by literature. Mathematics, however, releases its emotional surge only for those who actually do the work.

Conversely, if you have solved this problem, do not offer your assistance to others; you don't want to spoil their fun.

I want you to feel the joy, too. So at the end of this short section there is a single problem for you to tackle. In order for you to experience the joy, **do not under any circumstances let anyone help you solve this problem**. I hope that when you first look at the problem, you do not immediately see the solution but, rather, have to struggle with it for a while. Don't feel bad: I've shown this problem to extremely talented mathematicians who did not see the solution right away. Keep working and thinking—the solution will come. My hope is that when you solve this puzzle, it will bring a smile to your face. Here's the puzzle:

1 Exercise **1.1.** Simplify the following algebraic expression:

$$(x-a)(x-b)(x-c)\cdots(x-z).$$

2 Speaking (and Writing) of Mathematics

Precisely!

Whether or not we enjoy mathematics, we all can admire one of its unique features: there are definitive answers. Few other endeavors from economics to literary analysis to history to psychology can make this boast. Furthermore, in mathematics we can speak (and write) with extreme precision. While endless books, songs, and poems have been written about love, it's far easier to make precise statements (and verify their truth) about mathematics than human relations.

Precise language is vital to the study of mathematics. Unfortunately, students sometimes see mathematics as an endless series of numeric and algebraic calculations in which letters are only used to name variables; the closest one comes to using actual words is "sin" or "log."

In fact, to communicate mathematics clearly and precisely we need far more than numbers, variables, operations, and relation symbols; we need words composed into meaningful sentences that exactly convey the meaning we intend. Mathematical sentences often include technical notation, but the rules of grammar apply fully. Arguably, until one expresses ideas in a coherent sentence, those ideas are only half baked.

In addition, the mental effort to convert mathematical ideas into language is vital to learning those concepts. Take the time to express your ideas clearly both verbally and in writing. To learn mathematics requires you to engage all routes into your brain: your hands, eyes, mouth, and ears all need to get in on the act. Say the ideas out loud and write them down. You will learn to express yourself more clearly and you will learn the concepts better.

A Bit of Help

Be sure to check with your instructor concerning what types of collaboration are permitted on your assignments.

Writing is difficult. The best way to learn is to practice, especially with the help of a partner. Most people find it difficult to edit their own writing; our brains know what we want to say and trick us into believing that what we put onto paper is exactly what we intend. If you resort to saying "well, you know what I mean" then you need to try again.

In this brief section we provide a few pointers and some warnings about some common mistakes.

- *A language of our own.* Scattered in the margins of this book you will find *Mathspeak* notes that explain some of the idiosyncratic ways in which mathematicians use ordinary words. Common words (such as *function* or *prime*) are used differently in mathematics than in general use. The good news is that when we co-opt words into mathematical service, the meanings we give them are razor sharp (see the next section of this book for more about this).
- *Complete sentences.* This is the most basic rule of grammar and it applies to mathematics as much as to any discipline. Mathematical notation must be part of a sentence.

  Bad: $3x + 5$.

  This is not a sentence! What about $3x + 5$? What is the writer trying to say?

  Good: When we substitute $x = -5/3$ into $3x + 5$ the result is 0.

- *Mismatch of categories.* This is one of the most common mistakes people commit in mathematical writing and speaking. A line segment isn't a number, a function isn't an equation, a set isn't an operation, and so on. Consider this sentence:

  Air Force One is the president of the United States.

  This, of course, is nonsense. No amount of "well, you know what I mean" or "you get the general idea" can undo the error of writing that an airplane is a human being. Yet, this is exactly the sort of error novice mathematical writers (and speakers) make frequently.

  Thus, don't write "the function is equal to 3" when you mean "when the function is evaluated at $x = 5$ the result is 3". Note that we don't have to be verbose. Don't write "$f = 3$", but do write "$f(5) = 3$."

  Bad: If the legs of a right triangle T have lengths 5 and 12, then $T = 30$.

  Good: If the legs of a right triangle T have lengths 5 and 12, then the area of T is 30.
- *Avoid pronouns.* It's easy to write a sentence full of pronouns that you—the writer—understand but which is incomprehensible to anyone else.

  Bad: If we move everything over, then it simplifies and that's our answer.

  Give the things you're writing about names (such as single letters for numbers and line numbers for equations).

  Good: When we move all terms involving x to the left in equation (12), we find that those terms cancel and that enables us to determine the value of y.
- *Rewrite.* It's nearly impossible to write well on a first draft. What's more, few mathematics problems can be solved correctly straight away. Unfortunately, some students (not you, of course) start solving a problem, cross out errors, draw arrows to new parts of the solution, and then submit this awful mess as a finished product. Yuck! As with all other forms of writing, compose a first draft, edit, and then rewrite.
- *Learn LaTeX.* The editing and rewriting process is made much easier by word processors. Unfortunately, it's much more difficult to type mathematics than ordinary prose. Some what-you-see-is-what-you-get [WYSIWYG] word processing programs, such as Microsoft Word, include an equation editor that allows the typist to insert mathematical formulas into documents. Indeed, many scientists and engineers use Word to compose technical papers replete with intricate formulas.

The word LaTeX is written with letters of various sizes on different levels, in part to distinguish it from latex, a type of rubber. Incidentally, this book was composed using LaTeX.

Nevertheless, the gold standard for mathematical typing is LaTeX. Learning to compose documents in LaTeX takes a significant initial investment of time, but no investment of cash as there many implementations of LaTeX that are free and run on most types of computers (Windows, Mac OS, linux). Documents produced in LaTeX are visually more appealing than the output of WYSIWIG systems and are easier to edit. In LaTeX one types special commands to produce mathematical notation. For example, to produce the quadratic formula

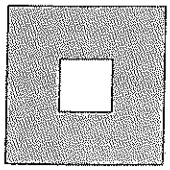
$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

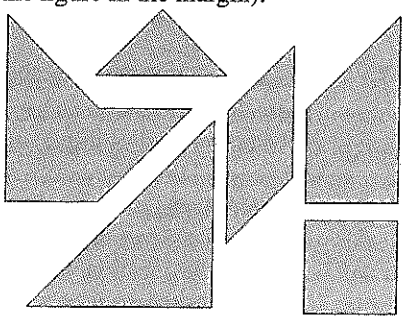
one types: `x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}`

There are many guides and books available for learning LaTeX including some that are available for free on the web.

2 Exercise

2.1. The six pieces below can be arranged to form a 3×3 square with the middle 1×1 square left empty (as in the figure in the margin).





Determine how to solve this puzzle and then write out clear instructions (without any diagrams!) so that another person can read your directions and properly fit the pieces together to arrive at the solution.

You may download a large, printable version of the puzzle pieces (so you can cut them out) from the author's website:

`www.ams.jhu.edu/~ers/mdi/puzzle.pdf`

3 Definition

Mathematics exists only in people's minds. There is no such "thing" as the number 6. You can draw the symbol for the number 6 on a piece of paper, but you can't physically hold a 6 in your hands. Numbers, like all other mathematical objects, are purely conceptual.

Mathematical objects come into existence by definitions. For example, a number is called *prime* or *even* provided it satisfies precise, unambiguous conditions. These highly specific conditions are the definition for the concept. In this way, we are acting like legislators, laying down specific criteria such as eligibility for a government program. The difference is that laws may allow for some ambiguity, whereas a mathematical definition must be absolutely clear.

Let's take a look at an example.

Definition 3.1 **(Even)** An integer is called *even* provided it is divisible by two.

In a definition, the word(s) being defined are typically set in *italic* type.

Clear? Not entirely. The problem is that this definition contains terms that we have not yet defined, in particular *integer* and *divisible*. If we wish to be terribly fussy, we can complain that we haven't defined the term *two*. Each of these terms—*integer*, *divisible*, and *two*—can be defined in terms of simpler concepts, but this is a game we cannot entirely win. If every term is defined in terms of simpler terms, we will be chasing definitions forever. Eventually we must come to a point where we say, "This term is undefined, but we think we understand what it means."

The situation is like building a house. Each part of the house is built up from previous parts. Before roofing and siding, we must build the frame. Before the frame goes up, there must be a foundation. As house builders, we think of pouring the foundation as the first step, but this is not really the first step. We also have to own the land and run electricity and water to the property. For there to be water, there must be wells and pipes laid in the ground. STOP! We have descended to a level in the process that really has little to do with building a house. Yes, utilities are vital to home construction, but it is not our job, as home builders, to worry about what sorts of transformers are used at the electric substation!

Let us return to mathematics and Definition 3.1. It is possible for us to define the terms *integer*, *two*, and *divisible* in terms of more basic concepts. It takes a great deal of work to define integers, multiplication, and so forth in terms of simpler concepts. What are we to do? Ideally, we should begin from the most basic mathematical object of all—the *set*—and work our way up to the integers. Although this is a worthwhile activity, in this book we build our mathematical house assuming the foundation has already been laid.

The symbol $\mathbb{Z}$ stands for the integers. This symbol is easy to draw, but often people do a poor job. Why? They fall into the following trap: They first draw a Z and then try to add an extra slash. That doesn't work! Instead, make a 7 and then an interlocking, upside-down 7 to draw $\mathbb{Z}$.

Where shall we begin? What may we assume? In this book, we take the integers as our starting point. The *integers* are the positive whole numbers, the negative whole numbers, and zero. That is, the set of integers, denoted by the letter $\mathbb{Z}$, is

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

We also assume that we know how to add, subtract, and multiply, and we need not prove basic number facts such as $3 \times 2 = 6$. We assume the basic algebraic properties of addition, subtraction, and multiplication and basic facts about order relations ($<$, $\leq$, $>$, and $\geq$). See Appendix D for more details on what you may assume.

Thus, in Definition 3.1, we need not define *integer* or *two*. However, we still need to define what we mean by *divisible*. To underscore the fact that we have not made this clear yet, consider the question: Is 3 divisible by 2? We want to say that the answer to this question is no, but perhaps the answer is yes since $3 \div 2$ is $1\frac{1}{2}$. So it is possible to divide 3 by 2 if we allow

fractions. Note further that in the previous paragraph we were granted basic properties of addition, subtraction, and multiplication, but not—and conspicuous by its absence—division. Thus we need a careful definition of *divisible*.

Definition 3.2 **(Divisible)** Let a and b be integers. We say that a is *divisible* by b provided there is an integer c such that $bc = a$. We also say b *divides* a, or b is a *factor* of a, or b is a *divisor* of a. The notation for this is $b|a$.

This definition introduces various terms (*divisible*, *factor*, *divisor*, and *divides*) as well as the notation $b|a$. Let's look at an example.

Example 3.3 Is 12 divisible by 4? To answer this question, we examine the definition. It says that $a = 12$ is divisible by $b = 4$ if we can find an integer c so that $4c = 12$. Of course, there is such an integer, namely, $c = 3$.

In this situation, we also say that 4 divides 12 or, equivalently, that 4 is a factor of 12. We also say 4 is a divisor of 12.

The notation to express this fact is $4|12$.

On the other hand, 12 is not divisible by 5 because there is no integer x for which $5x = 12$; thus $5|12$ is false.

Now Definition 3.1 is ready to use. The number 12 is even because $2|12$, and we know $2|12$ because $2 \times 6 = 12$. On the other hand, 13 is not even, because 13 is not divisible by 2; there is no integer x for which $2x = 13$. Note that we did not say that 13 is odd because we have yet to define the term *odd*. Of course, we know that 13 is an odd number, but we simply have not "created" odd numbers yet by specifying a definition for them. All we can say at this point is that 13 is not even. That being the case, let us define the term *odd*.

Definition 3.4 **(Odd)** An integer a is called *odd* provided there is an integer x such that $a = 2x + 1$.

Thus 13 is odd because we can choose $x = 6$ in the definition to give $13 = 2 \times 6 + 1$. Note that the definition gives a clear, unambiguous criterion for whether or not an integer is odd.

Please note carefully what the definition of *odd* does not say: It does not say that an integer is odd provided it is not even. This, of course, is true, and we prove it in a subsequent chapter. "Every integer is odd or even but not both" is a fact that we *prove*.

Here is a definition for another familiar concept.

Definition 3.5 **(Prime)** An integer p is called *prime* provided that $p > 1$ and the only positive divisors of p are 1 and p.

For example, 11 is prime because it satisfies both conditions in the definition: First, 11 is greater than 1, and second, the only positive divisors of 11 are 1 and 11.

However, 12 is not prime because it has a positive divisor other than 1 and itself; for example, $3|12$, $3 \neq 1$, and $3 \neq 12$.

Is 1 a prime? No. To see why, take $p = 1$ and see if p satisfies the definition of primality. There are two conditions: First we must have $p > 1$, and second, the only positive divisors of p are 1 and p. The second condition is satisfied: the only divisors of 1 are 1 and itself. However, $p = 1$ does not satisfy the first condition because $1 > 1$ is false. Therefore, 1 is not a prime.

We have answered the question: Is 1 a prime? The reason why 1 isn't prime is that the definition was specifically designed to make 1 nonprime! However, the real "why question" we would like to answer is: Why did we write Definition 3.5 to exclude 1?

I will attempt to answer this question in a moment, but there is an important philosophical point that needs to be underscored. The decision to exclude the number 1 in the definition was deliberate and conscious. In effect, the reason 1 is not prime is "because I said so!" In principle, you could define the word *prime* differently and allow the number 1 to be prime. The main problem with your using a different definition for prime is that the concept of a

prime number is well established in the mathematical community. If it were useful to you to allow 1 as a prime in your work, you ought to choose a different term for your concept, such as *relaxed prime* or *alternative prime*.

Now, let us address the question: Why did we write Definition 3.5 to exclude 1? The idea is that the prime numbers should form the "building blocks" of multiplication. Later, we prove the fact that every positive integer can be factored in a unique fashion into prime numbers. For example, 12 can be factored as $12 = 2 \times 2 \times 3$. There is no other way to factor 12 down to primes (other than rearranging the order of the factors). The prime factors of 12 are precisely 2, 2, and 3. Were we to allow 1 as a prime number, then we could also factor 12 down to "primes" as $12 = 1 \times 2 \times 2 \times 3$, a different factorization.

Since we have defined prime numbers, it is appropriate to define composite numbers.

Definition 3.6 **(Composite)** A positive integer a is called *composite* provided there is an integer b such that $1 < b < a$ and $b|a$.

For example, the number 25 is composite because it satisfies the condition of the definition: There is a number b with $1 < b < 25$ and $b|25$; indeed, $b = 5$ is the only such number.

Similarly, the number 360 is composite. In this case, there are several numbers b that satisfy $1 < b < 360$ and $b|360$.

Prime numbers are not composite. If p is prime, then, by definition, there can be no divisor of p between 1 and p (read Definition 3.5 carefully).

Furthermore, the number 1 is not composite. (Clearly, there is no number b with $1 < b < 1$.) Poor number 1! It is neither prime nor composite! (There is, however, a special term that is applied to the number 1—the number 1 is called a *unit*.)

Recap

In this section, we introduced the concept of a mathematical definition. Definitions typically have the form "An object X is called *the term being defined* provided it satisfies *specific conditions*." We presented the integers $\mathbb{Z}$ and defined the terms *divisible*, *odd*, *even*, *prime*, and *composite*.

---

3 Exercises

3.1. Please determine which of the following are true and which are false; use Definition 3.2 to explain your answers.

a. $3|100$.
b. $3|99$.
c. $-3|3$.
d. $-5|-5$.
e. $-2|-7$.
f. $0|4$.
g. $4|0$.
h. $0|0$.

3.2. Here is a possible alternative to Definition 3.2: We say that a is *divisible* by b provided $\frac{a}{b}$ is an integer. Explain why this alternative definition is different from Definition 3.2.

Here, *different* means that Definition 3.2 and the alternative definition specify *different concepts*. So, to answer this question, you should find integers a and b such that a is divisible by b according to one definition, but a is not divisible by b according to the other definition.

3.3. None of the following numbers is prime. Explain why they fail to satisfy Definition 3.5. Which of these numbers is composite?

a. 21.
b. 0.
c. π.
d. $\frac{1}{2}$.
e. -2.
f. -1.

The symbol $\mathbb{N}$ stands for the natural numbers.

3.4. The *natural numbers* are the nonnegative integers; that is,

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}.$$

Use the concept of natural numbers to create definitions for the following relations about integers: *less than* ($<$), *less than or equal to* ($\leq$), *greater than* ($>$), and *greater than or equal to* ($\geq$).

Note: Many authors define the natural numbers to be just the positive integers; for them, zero is not a natural number. To me, this seems unnatural ☺. The concepts *positive integers* and *nonnegative integers* are unambiguous and universally recognized among mathematicians. The term *natural number*, however, is not 100% standardized.

The symbol $\mathbb{Q}$ stands for the rational numbers.

3.5. A *rational number* is a number formed by dividing two integers a/b where $b \neq 0$. The set of all rational numbers is denoted $\mathbb{Q}$.

Explain why every integer is a rational number, but not all rational numbers are integers.

3.6. Define what it means for an integer to be a *perfect square*. For example, the integers 0, 1, 4, 9, and 16 are perfect squares. Your definition should begin

An integer x is called a *perfect square* provided....

3.7. Define what it means for one number to be the *square root* of another number.

3.8. Define the *perimeter* of a polygon.

3.9. Suppose the concept of distance between points in the plane is already defined. Write a careful definition for one point to be *between* two other points. Your definition should begin

Suppose A, B, C are points in the plane. We say that C is *between* A and B provided....

Note: Since you are crafting this definition, you have a bit of flexibility. Consider the possibility that the point C might be the same as the point A or B, or even that A and B might be the same point. Personally, if A and C were the same point, I would say that C is between A and B (regardless of where B may lie), but you may choose to design your definition to exclude this possibility. Whichever way you decide is fine, but be sure your definition does what you intend.

Note further: You do not need the concept of collinearity to define *between*. Once you have defined *between*, please use the notion of between to define what it means for three points to be collinear. Your definition should begin

Suppose A, B, C are points in the plane. We say that they are collinear provided....

Note even further: Now if, say, A and B are the same point, you certainly want your definition to imply that A, B, and C are collinear.

3.10. Define the *midpoint* of a line segment.

3.11. Some English words are difficult to define with mathematical precision (for example, *love*), but some can be tightly defined. Try writing definitions for these:

a. teenager.
b. grandmother.
c. leap year.
d. dime.
e. palindrome.
f. homophone.

You may assume more basic concepts (such as *coin* or *pronunciation*) are already defined.

3.12. Discrete mathematicians especially enjoy *counting problems*: problems that ask *how many*. Here we consider the question: How many positive divisors does a number have? For example, 6 has four positive divisors: 1, 2, 3, and 6.

How many positive divisors does each of the following have?

a. 8.
b. 32.
c. 2^n where n is a positive integer.
d. 10.
e. 100.

hot and humid." Let me assure you, from personal experience, that this statement is true! Does this mean that every day in every July is hot and humid? No, of course not. It is not reasonable to expect such a rigid interpretation of a general statement about the weather.

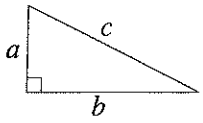
Consider the physicist's statement just presented: "When an object is dropped near the surface of the earth, it accelerates at a rate of 9.8 meter/sec^2." This statement is also true and is expressed with greater precision than our assertion about the climate in Baltimore. But this physics "law" is not absolutely correct. First, the value 9.8 is an approximation. Second, the term *near* is vague. From a galactic perspective, the moon is "near" the earth, but that is not the meaning of *near* that we intend. We can clarify *near* to mean "within 100 meters of the surface of the earth," but this leaves us with a problem. Even at an altitude of 100 meters, gravity is slightly less than at the surface. Worse yet, gravity at the surface is not constant; the gravitational pull at the top of Mount Everest is a bit smaller than the pull at sea level!

Despite these various objections and qualifications, the claim that objects dropped near the surface of the earth accelerate at a rate of 9.8 meter/sec^2 is true. As climatologists or physicists, we learn the limitations of our notion of truth. Most statements are limited in scope, and we learn that their truth is not meant to be considered absolute and universal.

However, in mathematics the word *true* is meant to be considered absolute, unconditional, and without exception.

Let us consider an example. Perhaps the most celebrated theorem in geometry is the following classical result of Pythagoras.

Theorem 4.1 **(Pythagorean)** If a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse, then



$$a^2 + b^2 = c^2.$$

The relation $a^2 + b^2 = c^2$ holds for the legs and hypotenuse of every right triangle, absolutely and without exception! We know this because we can prove this theorem (more on proofs later).

Is the Pythagorean Theorem really absolutely true? We might wonder: If we draw a right triangle on a piece of paper and measure the lengths of the sides down to a billionth of an inch, would we have exactly $a^2 + b^2 = c^2$? Probably not, because a drawing of a right triangle is not a right triangle! A drawing is a helpful visual aid for understanding a mathematical concept, but a drawing is just ink on paper. A "real" right triangle exists only in our minds.

On the other hand, consider the statement, "Prime numbers are odd." Is this statement true? No. The number 2 is prime but not odd. Therefore, the statement is false. We might like to say it is nearly true since all prime numbers except 2 are odd. Indeed, there are far more exceptions to the rule "July days in Baltimore are hot and humid" (a sentence regarded to be true) than there are to "Prime numbers are odd."

Mathematicians have adopted the convention that a statement is called *true* provided it is absolutely true without exception. A statement that is not absolutely true in this strict way is called *false*.

An engineer, a physicist, and a mathematician are taking a train ride through Scotland. They happen to notice some black sheep on a hillside.

"Look," shouts the engineer. "Sheep in this part of Scotland are black!"

"Really," retorts the physicist. "You mustn't jump to conclusions. All we can say is that in this part of Scotland there are some black sheep."

"Well, at least on one side," mutters the mathematician.

If-Then

Consider the mathematical and the ordinary usage of the word *prime*. When an economist says that the prime interest rate is now 8%, we are not upset that 8 is not a prime number!

Mathematicians use the English language in a slightly different way than ordinary speakers. We give certain words special meanings that are different from that of standard usage. Mathematicians take standard English words and use them as technical terms. We give words such as *set*, *group*, and *graph* new meanings. We also invent our own words, such as *bijection* and *poset*. (All these words are defined later in this book.)

Not only do mathematicians expropriate nouns and adjectives and give them new meanings, we also subtly change the meaning of common words, such as *or*, for our own purposes.

hot and humid." Let me assure you, from personal experience, that this statement is true! Does this mean that every day in every July is hot and humid? No, of course not. It is not reasonable to expect such a rigid interpretation of a general statement about the weather.

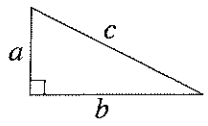
Consider the physicist's statement just presented: "When an object is dropped near the surface of the earth, it accelerates at a rate of 9.8 meter/sec^2." This statement is also true and is expressed with greater precision than our assertion about the climate in Baltimore. But this physics "law" is not absolutely correct. First, the value 9.8 is an approximation. Second, the term *near* is vague. From a galactic perspective, the moon is "near" the earth, but that is not the meaning of *near* that we intend. We can clarify *near* to mean "within 100 meters of the surface of the earth," but this leaves us with a problem. Even at an altitude of 100 meters, gravity is slightly less than at the surface. Worse yet, gravity at the surface is not constant; the gravitational pull at the top of Mount Everest is a bit smaller than the pull at sea level!

Despite these various objections and qualifications, the claim that objects dropped near the surface of the earth accelerate at a rate of 9.8 meter/sec^2 is true. As climatologists or physicists, we learn the limitations of our notion of truth. Most statements are limited in scope, and we learn that their truth is not meant to be considered absolute and universal.

However, in mathematics the word *true* is meant to be considered absolute, unconditional, and without exception.

Let us consider an example. Perhaps the most celebrated theorem in geometry is the following classical result of Pythagoras.

Theorem 4.1 **(Pythagorean)** If a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse, then



$$a^2 + b^2 = c^2.$$

The relation $a^2 + b^2 = c^2$ holds for the legs and hypotenuse of every right triangle, absolutely and without exception! We know this because we can prove this theorem (more on proofs later).

Is the Pythagorean Theorem really absolutely true? We might wonder: If we draw a right triangle on a piece of paper and measure the lengths of the sides down to a billionth of an inch, would we have exactly $a^2 + b^2 = c^2$? Probably not, because a drawing of a right triangle is not a right triangle! A drawing is a helpful visual aid for understanding a mathematical concept, but a drawing is just ink on paper. A "real" right triangle exists only in our minds.

On the other hand, consider the statement, "Prime numbers are odd." Is this statement true? No. The number 2 is prime but not odd. Therefore, the statement is false. We might like to say it is nearly true since all prime numbers except 2 are odd. Indeed, there are far more exceptions to the rule "July days in Baltimore are hot and humid" (a sentence regarded to be true) than there are to "Prime numbers are odd."

Mathematicians have adopted the convention that a statement is called *true* provided it is absolutely true without exception. A statement that is not absolutely true in this strict way is called *false*.

An engineer, a physicist, and a mathematician are taking a train ride through Scotland. They happen to notice some black sheep on a hillside.

"Look," shouts the engineer. "Sheep in this part of Scotland are black!"

"Really," retorts the physicist. "You mustn't jump to conclusions. All we can say is that in this part of Scotland there are some black sheep."

"Well, at least on one side," mutters the mathematician.

If-Then

Consider the mathematical and the ordinary usage of the word *prime*. When an economist says that the prime interest rate is now 8%, we are not upset that 8 is not a prime number!

Mathematicians use the English language in a slightly different way than ordinary speakers. We give certain words special meanings that are different from that of standard usage. Mathematicians take standard English words and use them as technical terms. We give words such as *set*, *group*, and *graph* new meanings. We also invent our own words, such as *bijection* and *poset*. (All these words are defined later in this book.)

Not only do mathematicians expropriate nouns and adjectives and give them new meanings, we also subtly change the meaning of common words, such as *or*, for our own purposes.

While we may be guilty of fracturing standard usage, we are highly consistent in how we do it. I call such altered usage of standard English *mathspeak*, and the most important example of mathspeak is the if-then construction.

In the statement "If A, then B," condition A is called the *hypothesis* and condition B is called the *conclusion*.

The vast majority of theorems can be expressed in the form "If A, then B." For example, the theorem "The sum of two even integers is even" can be rephrased "If x and y are even integers, then $x + y$ is also even."

In casual conversation, an if-then statement can have various interpretations. For example, I might say to my daughter, "If you mow the lawn, then I will pay you \$20." If she does the work, she will expect to be paid. She certainly wouldn't object if I gave her \$20 when she didn't mow the lawn, but she wouldn't expect it. Only one consequence is promised.

On the other hand, if I say to my son, "If you don't finish your lima beans, then you won't get dessert," he understands that unless he finishes his vegetables, no sweets will follow. But he also understands that if he does finish his lima beans, then he will get dessert. In this case two consequences are promised: one in the event he finishes his lima beans and one in the event he doesn't.

The mathematical use of if-then is akin to that of "If you mow the lawn, then I will pay you \$20." The statement "If A, then B" means: Every time condition A is true, condition B must be true as well. Consider the sentence "If x and y are even, then $x + y$ is even." All this sentence promises is that when x and y are both even, it must also be the case that $x + y$ is even. (The sentence does not rule out the possibility of $x + y$ being even despite x or y not being even. Indeed, if x and y are both odd, we know that $x + y$ is also even.)

In the statement "If A, then B," we might have condition A true or false, and we might have condition B true or false. Let us summarize this in a chart. If the statement "If A, then B" is true, we have the following.

Condition A	Condition B	
True	True	Possible
True	False	Impossible
False	True	Possible
False	False	Possible

All that is promised is that whenever A is true, B must be true as well. If A is not true, then no claim about B is asserted by "If A, then B."

Here is an example. Imagine I am a politician running for office, and I announce in public, "If I am elected, then I will lower taxes." Under what circumstances would you call me a liar?

- Suppose I am elected and I lower taxes. Certainly you would not call me a liar—I kept my promise.
- Suppose I am elected and I do not lower taxes. Now you have every right to call me a liar—I have broken my promise.
- Suppose I am not elected, but somehow (say, through active lobbying) I manage to get taxes lowered. You certainly would not call me a liar—I have not broken my promise.
- Finally, suppose I am not elected and taxes are not lowered. Again, you would not accuse me of lying—I promised to lower taxes only if I were elected.

The only circumstance under which "If (A) I am elected, then (B) I will lower taxes" is a lie is when A is true and B is false.

In summary, the statement "If A, then B" promises that condition B is true whenever A is true but makes no claim about B when A is false.

Alternative wordings for "If A, then B."

If-then statements pervade all of mathematics. It would be tiresome to use the same phrases over and over in mathematical writing. Consequently, there is an assortment of alternative ways to express "If A, then B." All of the following express exactly the same statement as "If A, then B."

- "A implies B." This can also be expressed in passive voice: "B is implied by A."
- "Whenever A, we have B." Also: "B, whenever A."
- "A is sufficient for B." Also: "A is a sufficient condition for B."
  This is an example of mathspeak. The word *sufficient* can carry, in standard English, the connotation of being "just enough." No such connotation should be ascribed here. The meaning is "Once A is true, then B must be true as well."

- "In order for B to hold, it is enough that we have A."
- "B is necessary for A."
  This is another example of mathspeak. The way to understand this wording is as follows: In order for A to be true, it is *necessarily* the case that B is also true.
- "A, only if B."
  The meaning is that A can happen *only if* B happens as well.
- "$A \Longrightarrow B$."
  The special arrow symbol $\Longrightarrow$ is pronounced "implies."
- "$B \Longleftarrow A$".
  The arrow $\Longleftarrow$ is pronounced "is implied by."

If and Only If

The vast majority of theorems are—or can readily be expressed—in the if-then form. Some theorems go one step further; they are of the form "If A then B, and if B then A." For example, we know the following is true:

If an integer x is even, then $x + 1$ is odd, and if $x + 1$ is odd, then x is even.

This statement is verbose. There are concise ways to express statements of the form "A implies B and B implies A" in which we do not have to write out the conditions A and B twice each. The key phrase is *if and only if*. The statement "If A then B, and if B then A" can be rewritten as "A if and only if B." The example just given is more comfortably written as follows:

An integer x is even if and only if $x + 1$ is odd.

What does an if-and-only-if statement mean? Consider the statement "A if and only if B." Conditions A and B may each be either true or false, so there are four possibilities that we can summarize in a chart. If the statement "A if and only if B" is true, we have the following table.

Condition A	Condition B	
True	True	Possible
True	False	Impossible
False	True	Impossible
False	False	Possible

It is impossible for condition A to be true while B is false, because $A \Longrightarrow B$. Likewise, it is impossible for condition B to be true while A is false, because $B \Longrightarrow A$. Thus the two conditions A and B must be both true or both false.

Let's revisit the example statement.

An integer x is even if and only if $x + 1$ is odd.

Condition A is "x is even" and condition B is "$x + 1$ is odd." For some integers (e.g., $x = 6$), conditions A and B are both true (6 is even and 7 is odd), but for other integers (e.g., $x = 9$), both conditions A and B are false (9 is not even and 10 is not odd).

Alternative wordings for "A if and only if B."

Just as there are many ways to express an if-then statement, so too are there several ways to express an if-and-only-if statement.

- "A iff B."
  Because the phrase "if and only if" occurs so frequently, the abbreviation "iff" is often used.
- "A is necessary and sufficient for B."
- "A is equivalent to B".
  The reason for the word *equivalent* is that condition A holds under exactly the same circumstances under which condition B holds.
- "A is true exactly when B is true."
  The word *exactly* means that the circumstances under which condition A hold are precisely the same as the circumstances under which B holds.
- "$A \Longleftrightarrow B$".
  The symbol $\Longleftrightarrow$ is an amalgamation of the symbols $\Longleftarrow$ and $\Longrightarrow$.

And, Or, and Not

Mathematicians use the words *and*, *or*, and *not* in very precise ways. The mathematical usage of *and* and *not* is essentially the same as that of standard English. The usage of *or* is more idiosyncratic.

Mathematical use of *and*.

The statement "A and B" means that both statements A and B are true. For example, "Every integer whose ones digit is 0 is divisible by 2 *and* by 5." This means that a number that ends in a zero, such as 230, is divisible both by 2 and by 5. The use of *and* can be summarized in the following chart.

A	B	A and B
True	True	True
True	False	False
False	True	False
False	False	False

Mathematical use of *not*.

The statement "not A" is true if and only if A is false. For example, the statement "All primes are odd" is false. Thus the statement "Not all primes are odd" is true. Again, we can summarize the use of *not* in a chart.

A	not A
True	False
False	True

Mathematical use of *or*.

Thus the mathematical usage of *and* and *not* corresponds closely with standard English. The use of *or*, however, does not. In standard English, *or* often suggests a choice of one option or the other, but not both. Consider the question, "Tonight, when we go out for dinner, would you like to have pizza or Chinese food?" The implication is that we'll dine on one or the other, but not both.

In contradistinction, the mathematical *or* allows the possibility of *both*. The statement "A or B" means that A is true, or B is true, or both A and B are true. For example, consider the following:

> *Suppose x and y are integers with the property that $x|y$ and $y|x$. Then $x = y$ or $x = -y$.*

The conclusion of this result says that we may have any one of the following:

- $x = y$ but not $x = -y$ (e.g., take $x = 3$ and $y = 3$).
- $x = -y$ but not $x = y$ (e.g., take $x = -5$ and $y = 5$).
- $x = y$ *and* $x = -y$, which is possible only when $x = 0$ and $y = 0$.

Here is a chart for *or* statements.

A	B	A or B
True	True	True
True	False	True
False	True	True
False	False	False

What Theorems Are Called

The word *theorem* should not be confused with the word *theory*. A *theorem* is a specific statement that can be proved. A *theory* is a broader assembly of ideas on a particular issue.

Some theorems are more important or more interesting than others. There are alternative nouns that mathematicians use in place of *theorem*. Each has a slightly different connotation. The word *theorem* conveys importance and generality. The Pythagorean Theorem certainly deserves to be called a *theorem*. The statement "The square of an even integer is also even" is also a theorem, but perhaps it doesn't deserve such a profound name. And the statement "$6 + 3 = 9$" is technically a theorem but does not merit such a prestigious appellation.

Here we list words that are alternatives to *theorem* and offer a guide to their usage.

Result A modest, generic word for a theorem. There is an air of humility in calling your theorem merely a "result." Both important and unimportant theorems can be called results.

Fact A very minor theorem. The statement "$6 + 3 = 9$" is a fact.

Proposition A minor theorem. A proposition is more important or more general than a fact but not as prestigious as a theorem.

Lemma A theorem whose main purpose is to help prove another, more important theorem. Some theorems have complicated proofs. Often one can break down the job of proving a such theorems into smaller parts. The lemmas are the parts, or tools, used to build the more elaborate proof.

Corollary A result with a short proof whose main step is the use of another, previously proved theorem.

Claim Similar to lemma. A claim is a theorem whose statement usually appears inside the proof of a theorem. The purpose of a claim is to help organize key steps in a proof. Also, the statement of a claim may involve terms that make sense only in the context of the enclosing proof.

Vacuous Truth

What are we to think of an if-then statement in which the hypothesis is impossible? Consider the following.

Statement 4.2 **(Vacuous)** If an integer is both a perfect square and prime, then it is negative.

Is this statement true or false?

The statement is not nonsense. The terms *perfect square* (see Exercise 3.6), *prime*, and *negative* properly apply to integers.

We might be tempted to say that the statement is false because square numbers and prime numbers cannot be negative. However, for a statement of the form "If A, then B" to be declared *false*, we need to find an instance in which clause A is true and clause B is false. In the case of Statement 4.2, condition A is impossible; there are no numbers that are both a perfect square and prime. So we can never find an integer that renders condition A true and condition B false. Therefore, Statement 4.2 is true!

Statements of the form "If A, then B" in which condition A is impossible are called *vacuous*, and mathematicians consider such statements true because they have no exceptions.

Recap

This section introduced the notion of a *theorem*: a declarative statement about mathematics that has a proof. We discussed the absolute nature of the word *true* in mathematics. We examined the if-then and if-and-only-if forms of theorems, as well as alternative language to express such results. We clarified the way in which mathematicians use the words *and*, *or*, and *not*. We presented a number of synonyms for *theorem* and explained their connotations. Finally, we discussed vacuous if-then statements and noted that mathematicians regard such statements as true.

---

4 Exercises

4.1. Each of the following statements can be recast in the if-then form. Please rewrite each of the following sentences in the form "If A, then B."

a. The product of an odd integer and an even integer is even.

b. The square of an odd integer is odd.

c. The square of a prime number is not prime.

d. The product of two negative integers is negative. (This, of course, is false.)

e. The diagonals of a rhombus are perpendicular.

f. Congruent triangles have the same area.

g. The sum of three consecutive integers is divisible by three.

4.2. Below you will find pairs of statements A and B. For each pair, please indicate which of the following three sentences are true and which are false:

- If A, then B.
- If B, then A.
- A if and only if B.

Note: You do not need to prove your assertions.

a. A: Polygon $PQRS$ is a rectangle. B: Polygon $PQRS$ is a square.

b. A: Polygon $PQRS$ is a rectangle. B: Polygon $PQRS$ is a parallelogram.

c. A: Joe is a grandfather. B: Joe is male.

d. A: Ellen resides in Los Angeles. B: Ellen resides in California.

e. A: This year is divisible by 4. B: This year is a leap year.

f. A: Lines ℓ_1 and ℓ_2 are parallel. B: Lines ℓ_1 and ℓ_2 are perpendicular.

For the remaining items, x and y refer to real numbers.

g. A: $x > 0$. B: $x^2 > 0$.

h. A: $x < 0$. B: $x^3 < 0$.

i. A: $xy = 0$. B: $x = 0$ or $y = 0$.

j. A: $xy = 0$. B: $x = 0$ and $y = 0$.

k. A: $x + y = 0$. B: $x = 0$ and $y = 0$.

The statement "If B, then A" is called the *converse* of the statement "If A, then B."

4.3. It is a common mistake to confuse the following two statements:

a. If A, then B.

b. If B, then A.

Find two conditions A and B such that statement (a) is true but statement (b) is false.

4.4. Consider the two statements

a. If A, then B.

b. (not A) or B.

Under what circumstances are these statements true? When are they false? Explain why these statements are, in essence, identical.

The statement "If (not B), then (not A)" is called the *contrapositive* of the statement "If A, then B."

4.5. Consider the two statements

a. If A, then B.

b. If (not B), then (not A).

Under what circumstances are these statements true? When are they false? Explain why these statements are, in essence, identical.

4.6. Consider the two statements

a. A iff B.

b. (not A) iff (not B).

Under what circumstances are these statements true? Under what circumstances are they false? Explain why these statements are, in essence, identical.

4.7. Consider an equilateral triangle whose side lengths are $a = b = c = 1$. Notice that in this case $a^2 + b^2 \neq c^2$. Explain why this is not a violation of the Pythagorean Theorem.

A side of a spherical triangle is an arc of a great circle of the sphere on which it is drawn.

4.8. Explain how to draw a triangle on the surface of a sphere that has three right angles. Do the legs and hypotenuse of such a right triangle satisfy the condition $a^2 + b^2 = c^2$? Explain why this is not a violation of the Pythagorean Theorem.

4.9. Consider the sentence "A line is the shortest distance between two points." Strictly speaking, this sentence is nonsense.

Find two errors with this sentence and rewrite it properly.

4.10. Consider the following rather grotesque claim: "If you pick a guinea pig up by its tail, then its eyes will pop out." Is this true?

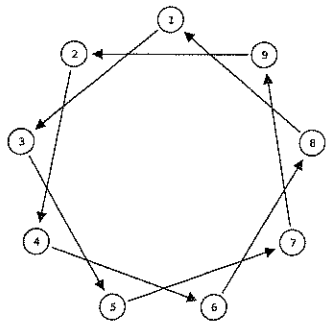
4.11. What are the two plurals of the word *lemma*?

4.12. **More about conjectures.** Where do new theorems come from? They are the creations of mathematicians that begin as *conjectures*: statements about mathematics whose truth we have yet to establish. In other words, conjectures are guesses (usually, educated guesses). By looking at many examples and hunting for patterns, mathematicians express their observations as statements they hope to prove.

The following items are designed to lead you through the process of making conjectures. In each case, try out several examples and attempt to formulate your observations as a theorem to be proved. *You do not have to prove these statements*; for now we simply want you to express what you find in the language of mathematics.

a. What can you say about the sum of consecutive odd numbers starting with 1? That is, evaluate 1, $1+3$, $1+3+5$, $1+3+5+7$, and so on, and formulate a conjecture.

b. What can you say about the sum of consecutive perfect cubes, starting with 1. That is, what can you say about 1^3, $1^3 + 3^3$, $1^3 + 3^3 + 5^3$, $1^3 + 3^3 + 5^3 + 7^3$, and so on.



c. Let n be a positive integer. Draw n lines (no two of which are parallel) in the plane. How many regions are formed?

d. Place n points evenly around a circle. Starting at one point, draw a path to every other point around the circle until returning to start. In some instances, every point is visited and in some instances some are missed. Under what circumstances is every point visited (as in the figure with $n = 9$)?

Suppose instead of jumping to every second point, we jump to every third point. For what values of n does the path touch every point?

Finally, suppose we visit every k^{th} point (where k is between 1 and n). When does the path touch every point?

e. A school has a long hallway of lockers numbered 1, 2, 3, and so on up to 1000. In this problem we'll refer to *flipping* a locker to mean opening a closed locker or closing an open locker. That is, to *flip* a locker is to change its closed/open state.

- Student #1 walks down the hallway and closes all the lockers.
- Student #2 walks down the hallway and flips all the even numbered lockers. So now, the odd lockers are closed and the even lockers are open.
- Student #3 walks down the hall and flips all the lockers that are divisible by 3.
- Student #4 walks down the hall and flips all the lockers that are divisible by 4.
- Likewise students 5, 6, 7, and so on walk down the hall in turn, each flipping lockers divisible by their own number until finally student 1000 flips the (one and only) locker divisible by 1000 (the last locker).

Which lockers are open and which are closed? Generalize to any number of lockers.

Note: We ask you to prove your conjecture later; see Exercise 24.19.

5 Proof

We create mathematical concepts via definitions. We then posit assertions about mathematical notions, and then we try to prove our ideas are correct.

What is a *proof*?

In science, truth is borne out through experimentation. In law, truth is ascertained by a trial and decided by a judge and/or jury. In sports, the truth is the ruling of referees to the best of their ability. In mathematics, we have *proof*.

Truth in mathematics is not demonstrated through experimentation. This is not to say that experimentation is irrelevant for mathematics—quite the contrary! Trying out ideas and examples helps us to formulate statements we believe to be true (conjectures); we then try to prove these statements (thereby converting conjectures to theorems).

For example, recall the statement "All prime numbers are odd." If we start listing the prime numbers beginning with 3, we find hundreds and thousands of prime numbers, and they are all odd! Does this mean all prime numbers are odd? Of course not! We simply missed the number 2.

Let us consider a far less obvious example.

Conjecture 5.1 **(Goldbach)** Every even integer greater than two is the sum of two primes.

Let's see that this statement is true for the first few even numbers. We have

$$4 = 2 + 2 \qquad 6 = 3 + 3 \qquad 8 = 3 + 5 \qquad 10 = 3 + 7$$
$$12 = 5 + 7 \qquad 14 = 7 + 7 \qquad 16 = 11 + 5 \qquad 18 = 11 + 7.$$

Mathspeak! A proof is often called an *argument*. In standard English, the word *argument* carries a connotation of disagreement or controversy. No such negative connotation should be associated with a mathematical argument. Indeed, mathematicians are honored when their proofs are called "beautiful arguments."

One could write a computer program to verify that the first few billion even numbers (starting with 4) are each the sum of two primes. Does this imply Goldbach's Conjecture is true? No! The numerical evidence makes the conjecture believable, but it does not prove that it is true. To date, no proof has been found for Goldbach's Conjecture, so we simply do not know whether it is true or false.

A proof is an essay that incontrovertibly shows that a statement is true. Mathematical proofs are highly structured and are written in a rather stylized manner. Certain key phrases

and logical constructions appear frequently in proofs. In this and subsequent sections, we show how proofs are written.

The theorems we prove in this section are all rather simple. Indeed, you won't learn any facts about numbers you probably didn't already know quite well. The point in this section is not to learn new information about numbers; the point is to learn how to write proofs. So without further ado, let's start writing proofs!

We prove the following:

Proposition 5.2 The sum of two even integers is even.

We write the proof here in full, and then discuss how this proof was created. In this proof, each sentence is numbered so we can examine the proof piece by piece. Normally we would write this short proof as a single paragraph and not number the sentences.

Proof Proposition 5.2

1. We show that if x and y are even integers, then $x + y$ is an even integer.
2. Let x and y be even integers.
3. Since x is even, we know by Definition 3.1 that x is divisible by 2 (i.e., $2|x$).
4. Likewise, since y is even, $2|y$.
5. Since $2|x$, we know, by Definition 3.2, that there is an integer a such that $x = 2a$.
6. Likewise, since $2|y$, there is an integer b such that $y = 2b$.
7. Observe that $x + y = 2a + 2b = 2(a + b)$.
8. Therefore there is an integer c (namely, $a + b$) such that $x + y = 2c$.
9. Therefore (Definition 3.2) $2|(x + y)$.
10. Therefore (Definition 3.1) $x + y$ is even. ■

Let us examine exactly how this proof was written.

Convert the statement to if-then form.

- The first step is to convert the statement of the proposition into the if-then form.

  The statement reads, "The sum of two even integers is even."

  We convert the statement into if-then form as follows:

  "If x and y are even integers, then $x + y$ is an even integer."

  Note that we introduced letters (x and y) to name the two even integers. These letters come in handy in the proof.

  Observe that the first sentence of the proof spells out the proposition in if-then form.

  Sentence 1 announces the structure of this proof. The hypothesis (the "if" part) tells the reader that we will assume that x and y are even integers, and the conclusion (the "then" part) tells the reader that we are working to prove that $x + y$ is even.

  Sentence 1 can be regarded as a preamble to the proof. The proof starts in earnest at sentence 2.

Write the first and last sentences using the hypothesis and conclusion of the statement.

- The next step is to write the very beginning and the very *end* of the proof.

  The hypothesis of sentence 1 tells us what to write next. It says, "... if x and y are even integers...," so we simply write, "Let x and y be even integers." (Sentence 2)

  Immediately after we write the first sentence, we write the very last sentence of the proof. The last sentence of the proof is a rewrite of the conclusion of the if-then form of the statement.

  "Therefore, $x + y$ is even." (Sentence 10)

  The basic skeleton of the proof has been constructed. We know where we begin (x and y are even), and we know where we are heading ($x + y$ is even).

Unravel definitions.

- The next step is to unravel definitions. We do this at both ends of the proof.

  Sentence 2 tells us that x is even. What does this mean? To find out, we check (or we remember) the definition of the word *even*. (Take a quick look at Definition 3.1 on page 4.) It says that an integer is even provided it is divisible by 2. So we know that x is divisible by 2, and we can also write that as $2|x$; this gives sentence 3.

  Sentence 4 does the same job as sentence 3. Since the reasoning in sentence 4 is identical to that of sentence 3, we use the word *likewise* to flag this parallel construction.

  We now unravel the definition of *divisible*. We consult Definition 3.2 to learn that $2|x$ means there is an integer—we need to give that integer a name and we call it a—so that

$x = 2a$. So sentence 5 just unravels sentence 3. Similarly (*likewise*!) sentence 6 unravels the fact that $2|y$ (sentence 4), and we know we have an integer b such that $y = 2b$.

At this point, we are stuck. We have unraveled all the definitions at the beginning of the proof, so now we return to the end of the proof and work backward!

We are still in the "unravel definitions" phase of writing this proof. The last sentence of the proof says, "Therefore $x + y$ is even." How do we prove an integer is even? We turn to the definition of *even*, and we see that we need to prove that $x + y$ is divisible by 2. So we know that the penultimate sentence (number 9) should say that $x + y$ is divisible by 2.

How do we get to sentence 9? To show that an integer (namely, $x + y$) is divisible by 2, we need to show there is an integer—let's call it c—such that $(x + y) = 2c$. This gives sentence 8.

Now we have unraveled definitions from both ends of the proof. Let's pause a moment to see what we have. The proof (written more tersely here) reads:

> We show that if x and y are even integers, then $x + y$ is an even integer.
>
> Let x and y be even integers. By definition of *even*, we know that $2|x$ and $2|y$. By definition of *divisibility*, we know there are integers a and b such that $x = 2a$ and $y = 2b$.
>
> ⋮
>
> Therefore there is an integer c such that $x + y = 2c$; hence $2|(x + y)$, and therefore $x + y$ is even.

What do we know? What do we need? Make the ends meet.

- The next step is to think. What do we know and what do we need?

We know $x = 2a$ and $y = 2b$. We need an integer c such that $x + y = 2c$. So in this case, it is easy to see that we can take $c = a + b$ because the sum of two integers is an integer. We fill in the middle of the proof with sentence 7 and we are finished! To celebrate, and to mark the end of the proof, we append an end-of-proof symbol to the end of the proof: ■

This middle step—which was quite easy—is actually the hardest part of the proof. The translation of the statement of the proposition into if-then form and the unraveling of definitions are routine; once you have written several proofs, you will find these steps are easily produced. The hard part comes when you try to make ends meet!

The proof of Proposition 5.2 is the most basic type of proof; it is called a *direct* proof. The steps in writing a direct proof of an if-then statement are summarized in Proof Template 1.

Proof Template 1 Direct proof of an if-then theorem.

- Write the first sentence(s) of the proof by restating the hypothesis of the result. Invent suitable notation (e.g., assign letters to stand for variables).
- Write the last sentence(s) of the proof by restating the conclusion of the result.
- Unravel the definitions, working forward from the beginning of the proof and backward from the end of the proof.
- Figure out what you know and what you need. Try to forge a link between the two halves of your argument.

Let's use the direct proof technique to prove another result.

Proposition 5.3 Let a, b, and c be integers. If $a|b$ and $b|c$, then $a|c$.

The first step in creating the proof of this proposition is to write the first and last sentences based on the hypothesis and conclusion. This gives

> Suppose a, b, and c are integers with $a|b$ and $b|c$.
> ...
> Therefore $a|c$. ■

Next we unravel the definition of divisibility.

> Suppose a, b, and c are integers with $a|b$ and $b|c$. Since $a|b$, there is an integer x such that $b = ax$. Likewise there is an integer y such that $c = by$.
> ...
> Therefore there is an integer z such that $c = az$. Therefore $a|c$. ■

We have unraveled the definitions. Let's consider what we have and what we need.

$$\text{We have } a, b, c, x, \text{ and } y \text{ such that:} \quad b = ax \text{ and } c = by.$$
$$\text{We want to find } z \text{ such that:} \quad c = az.$$

Now we have to think, but fortunately the problem is not too hard. Since $b = ax$, we can substitute ax for b in $c = by$ and get $c = axy$. So the z we need is $z = xy$. We can use this to finish the proof of Proposition 5.3.

> Suppose a, b, and c are integers with $a|b$ and $b|c$. Since $a|b$, there is an integer x such that $b = ax$. Likewise there is an integer y such that $c = by$. Let $z = xy$. Then $az = a(xy) = (ax)y = by = c$.
> Therefore there is an integer z such that $c = az$. Therefore $a|c$. ■

A More Involved Proof

Propositions 5.2 and 5.3 are rather simple and not particularly interesting. Here we develop a more interesting proposition and its proof.

One of the most intriguing and most difficult issues in mathematics is the pattern of prime and composite numbers. Here is one pattern for you to consider. Pick a positive integer, cube it, and then add one. Some examples:

$$3^3 + 1 = 27 + 1 = 28,$$
$$4^3 + 1 = 64 + 1 = 65,$$
$$5^3 + 1 = 125 + 1 = 126, \text{ and}$$
$$6^3 + 1 = 216 + 1 = 217.$$

Notice that the results are all composite. (Note that $217 = 7 \times 31$.) Try a few more examples on your own.

Let us try to convert this observation into a proposition for us to prove. Here's a first (but incorrect) draft: "If x is an integer, then $x^3 + 1$ is composite." This is a good start, but when we examine Definition 3.6, we note that the term *composite* applies only to positive integers. If x is negative, then $x^3 + 1$ is either negative or zero.

Fortunately, it's easy to repair the draft statement; here is a second version: "If x is a positive integer, then $x^3 + 1$ is composite." This looks better, but we're in trouble already when $x = 1$ because, in this case, $x^3 + 1 = 1^3 + 1 = 2$, which is prime. This makes us worry about the entire idea, but we note that when $x = 2$, $x^3 + 1 = 2^3 + 1 = 9$, which is composite, and we can try many other examples with $x > 1$ and always meet with success.

The case $x = 1$ turns out to be the only positive exception, and this leads us to a third (and correct) version of the proposition we wish to prove.

Proposition 5.4 Let x be an integer. If $x > 1$, then $x^3 + 1$ is composite.

Let's write down the basic outline of the proof.

> Let x be an integer and suppose $x > 1$.
> ...
> Therefore $x^3 + 1$ is composite. ■

To reach the conclusion that $x^3 + 1$ is composite, we need to find a factor of $x^3 + 1$ that is strictly between 1 and $x^3 + 1$. With luck, the word *factor* makes us think about factoring the polynomial $x^3 + 1$ as a polynomial. Recall from basic algebra that

$$x^3 + 1 = (x + 1)(x^2 - x + 1).$$

You might have the following concern: "I forgot that $x^3 + 1$ factors. How would I ever come up with this proof?" One idea is to look for patterns in the factors. We saw that $6^3 + 1 = 7 \times 31$, so $6^3 + 1$ is divisible by 7. Trying more examples, you may notice that $7^3 + 1$ is divisible by 8, $8^3 + 1$ is divisible by 9, $9^3 + 1$ is divisible by 10, and so on. With luck, that will help you realize that $x^3 + 1$ is divisible by $x + 1$, and then you can complete the factorization $x^3 + 1 = (x + 1) \times ?$.

This is the "Aha!" insight we need. Both $x + 1$ and $x^2 - x + 1$ are factors of $x^3 + 1$. For example, when $x = 6$, the factors $x + 1$ and $x^2 - x + 1$ evaluate to 7 and 31, respectively. Let's add this insight to our proof.

> Let x be an integer and suppose $x > 1$. Note that $x^3 + 1 = (x + 1)(x^2 - x + 1)$.
> ...
> Since $x + 1$ is a divisor of $x^3 + 1$, we have that $x^3 + 1$ is composite. ■

To correctly say that $x + 1$ is a divisor of $x^3 + 1$, we need the fact that both $x + 1$ and $x^2 - x + 1$ are integers. This is clear, because x itself is an integer. Let's be sure we include this detail in our proof.

> Let x be an integer and suppose $x > 1$. Note that $x^3 + 1 = (x + 1)(x^2 - x + 1)$. Because x is an integer, both $x + 1$ and $x^2 - x + 1$ are integers. Therefore $(x + 1) | (x^3 + 1)$.
> ...
> Since $x + 1$ is a divisor of $x^3 + 1$, we have that $x^3 + 1$ is composite. ■

The proof isn't quite finished yet. Consult Definition 3.6; we need that the divisor be strictly between 1 and $x^3 + 1$, and we have not proved that yet. So let's figure out what we need to do. We must prove

$$1 < x + 1 < x^3 + 1.$$

The first part is easy. Since $x > 1$, adding 1 to both sides gives

$$x + 1 > 1 + 1 = 2 > 1.$$

Showing that $x + 1 < x^3 + 1$ is only slightly more difficult. Working backward, to show $x + 1 < x^3 + 1$, it will be enough if we can prove that $x < x^3$. Notice that since $x > 1$, multiplying both sides by x gives $x^2 > x$, and since $x > 1$, we have $x^2 > 1$. Multiplying both sides of this by x gives $x^3 > x$. Let's take these ideas and add them to the proof.

Let x be an integer and suppose $x > 1$. Note that $x^3+1 = (x+1)(x^2-x+1)$. Because x is an integer, both $x + 1$ and $x^2 - x + 1$ are integers. Therefore $(x + 1)|(x^3 + 1)$.

Since $x > 1$, we have $x + 1 > 1 + 1 = 2 > 1$.

Also $x > 1$ implies $x^2 > x$, and since $x > 1$, we have $x^2 > 1$. Multiplying both sides by x again yields $x^3 > x$. Adding 1 to both sides gives $x^3 + 1 > x + 1$.

Thus $x + 1$ is an integer with $1 < x + 1 < x^3 + 1$.

Since $x + 1$ is a divisor of $x^3 + 1$ and $1 < x + 1 < x^3 + 1$, we have that $x^3 + 1$ is composite. ■

Proving If-and-Only-If Theorems

The basic technique for proving a statement of the form "A iff B" is to prove two if-then statements. We prove both "If A, then B" and "If B, then A." Here is an example:

Proposition 5.5 Let x be an integer. Then x is even if and only if $x + 1$ is odd.

The basic skeleton of the proof is as follows:

Let x be an integer.

($\Rightarrow$) Suppose x is even. ... Therefore $x + 1$ is odd.

($\Leftarrow$) Suppose $x + 1$ is odd. ... Therefore x is even. ■

Notice that we flag the two sections of the proof with the symbols ($\Rightarrow$) and ($\Leftarrow$). This lets the reader know which section of the proof is which.

Now we unravel the definitions at the front of each part of the proof. (Recall the definition of *odd*; see Definition 3.4 on page 5.)

Let x be an integer.

($\Rightarrow$) Suppose x is even. This means that $2|x$. Hence there is an integer a such that $x = 2a$. ... Therefore $x + 1$ is odd.

($\Leftarrow$) Suppose $x + 1$ is odd. So there is an integer b such that $x + 1 = 2b + 1$. ... Therefore x is even. ■

The next steps are clear. In the first part of the proof, we have $x = 2a$, and we want to prove $x + 1$ is odd. We just add 1 to both sides of $x = 2a$ to get $x + 1 = 2a + 1$, and that shows that $x + 1$ is odd.

In the second part of the proof, we know $x + 1 = 2b + 1$, and we want to prove that x is even. We subtract 1 from both sides and we are finished.

Let x be an integer.

($\Rightarrow$) Suppose x is even. This means that $2|x$. Hence there is an integer a such that $x = 2a$. Adding 1 to both sides gives $x + 1 = 2a + 1$. By the definition of *odd*, $x + 1$ is odd.

($\Leftarrow$) Suppose $x + 1$ is odd. So there is an integer b such that $x + 1 = 2b + 1$. Subtracting 1 from both sides gives $x = 2b$. This shows that $2|x$ and therefore x is even. ■

Proof Template 2 shows the basic method for proving an if-and-only-if theorem.

Proof Template 2 Direct proof of an if-and-only-if theorem.

To prove a statement of the form "A iff B":

- ($\Rightarrow$) Prove "If A, then B."
- ($\Leftarrow$) Prove "If B, then A."

When is it safe to skip steps?

As you become more comfortable writing proofs, you may find yourself getting bored writing the same steps over and over again. We have seen the sequence (1) x is even, so (2) x is divisible by 2, so (3) there is an integer a such that $x = 2a$ several times already. You may be tempted to skip step (2) and just write "x is even, so there is an integer a such that $x = 2a$." The decision about skipping steps requires some careful judgment, but here are some guidelines.

- Would it be easy (and perhaps boring) for you to fill in the missing steps? Are the missing steps obvious? If you answer yes, then omit the steps.
- Does the same sequence of steps appear several times in your proof(s), but the sequence of steps is not very easy to reconstruct? Here you have two choices:
  - Write the sequence of steps out once, and the next time the same sequence appears, use an expression such as "as we saw before" or "likewise."
  - Alternatively, if the consequence of the sequence of steps can be described in a statement, first prove that statement, calling it a *lemma*. Then invoke (refer to) your lemma whenever you need to repeat those steps.
- When in doubt, write it out.

Let us illustrate the idea of explicitly separating off a portion of a proof into a lemma. Consider the following statement.

Proposition 5.6 Let a, b, c, and d be integers. If $a|b$, $b|c$, and $c|d$, then $a|d$.

Here is the proof as suggested by Proof Template 1.

Let a, b, c, and d be integers with $a|b$, $b|c$, and $c|d$.
Since $a|b$, there is an integer x such that $ax = b$.
Since $b|c$, there is an integer y such that $by = c$.
Since $c|d$, there is an integer z such that $cz = d$.
Note that $a(xyz) = (ax)(yz) = b(yz) = (by)z = cz = d$.
Therefore there is an integer $w = xyz$ such that $aw = d$.
Therefore $a|d$. ■

There is nothing wrong with this proof, but there is a simpler, less verbose way to handle it. We have already shown that $a|b,\ b|c \Rightarrow a|c$ in Proposition 5.3. Let us use this proposition to prove Proposition 5.6.

Here is the alternative proof.

Let a, b, c, and d be integers with $a|b$, $b|c$, and $c|d$.
Since $a|b$ and $b|c$, by Proposition 5.3 we have $a|c$.
Now, since $a|c$ and $c|d$, again by Proposition 5.3 we have $a|d$. ■

The key idea is to use Proposition 5.3 twice. Once it was applied to a, b, and c to get $a|c$. When we have established that $a|c$, we can use Proposition 5.3 again on the integers a, c, and d to finish the proof.

Proposition 5.3 serves as a lemma in the proof of Proposition 5.6.

Proving Equations and Inequalities

The basic algebraic manipulations you already know are valid steps in a proof. It is not necessary for you to prove that $x + x = 2x$ or that $x^2 - y^2 = (x - y)(x + y)$. In your proofs, feel free to use standard algebraic steps without detailed comment.

However, even these simple facts can be proved using the fundamental properties of numbers and operations (see Appendix D). We show how here, simply to illustrate that algebraic manipulations can be justified in terms of more basic principles.

For $x + x = 2x$:

$$\begin{aligned} x + x &= 1 \cdot x + 1 \cdot x && \text{1 is the identity element for multiplication} \\ &= (1 + 1)x && \text{distributive property} \\ &= 2x && \text{because } 1 + 1 = 2. \end{aligned}$$

For $(x - y)(x + y) = x^2 - y^2$:

$$\begin{aligned} (x - y)(x + y) &= x(x + y) - y(x + y) && \text{distributive property} \\ &= x^2 + xy - yx - y^2 && \text{distributive property} \\ &= x^2 + xy - xy - y^2 && \text{commutative property for multiplication} \\ &= x^2 + 1xy - 1xy - y^2 && \text{1 is the identity element for multiplication} \\ &= x^2 + (1 - 1)xy - y^2 && \text{distributive property} \\ &= x^2 + 0xy - y^2 && \text{because } 1 - 1 = 0 \\ &= x^2 + 0 - y^2 && \text{because anything multiplied by 0 is 0} \\ &= x^2 - y^2 && \text{0 is the identity element for addition.} \end{aligned}$$

Working with inequalities may be less familiar, but the basic steps are the same. For example, suppose you are asked to prove the following statement: If $x > 2$ then $x^2 > x + 1$. Here is a proof:

We need to comment that x is positive because multiplying both sides of an inequality by a negative number reverses the inequality.

Proof. We are given that $x > 2$. Since x is positive, multiplying both sides by x gives $x^2 > 2x$. So we have

$$\begin{aligned} x^2 &> 2x \\ &= x + x \\ &> x + 2 && \text{because } x > 2 \\ &> x + 1 && \text{because } 2 > 1. \end{aligned}$$

Therefore, by transitivity, $x^2 > x + 1$. ∎

See the discussion of Ordering in Appendix D for a review of *transitivity*.

Recap

We introduced the concept of proof and presented the basic technique of writing a direct proof for an if-then statement. For if-and-only-if statements, we apply this basic technique to both the forward ($\Rightarrow$) and the backward ($\Leftarrow$) implications.

5 Exercises

5.1. Prove that the sum of two odd integers is even.
5.2. Prove that the sum of an odd integer and an even integer is odd.
5.3. Prove that if n is an odd integer, then $-n$ is also odd.
5.4. Prove that the product of two even integers is even.
5.5. Prove that the product of an even integer and an odd integer is even.
5.6. Prove that the product of two odd integers is odd.
5.7. Prove that the square of an odd integer is odd.
5.8. Prove that the cube of an odd integer is odd.
5.9. Suppose a, b, and c are integers. Prove that if $a|b$ and $a|c$, then $a|(b + c)$.
5.10. Suppose a, b, and c are integers. Prove that if $a|b$, then $a|(bc)$.
5.11. Suppose a, b, d, x, and y are integers. Prove that if $d|a$ and $d|b$, then $d|(ax + by)$.
5.12. Suppose a, b, c, and d are integers. Prove that if $a|b$ and $c|d$, then $(ac)|(bd)$.

Note that Exercise 5.14 provides an alternative to Definition 3.4. To show that a number x is odd we can either look for an integer a so that $x = 2a + 1$ (using the definition) or we can look for an integer b so that $x = 2b - 1$ (using the result you prove here).

5.13. Let x be an integer. Prove that x is odd if and only if $x + 1$ is even.

5.14. Let x be an integers. Prove that x is odd if and only if there is an integer b such that $x = 2b - 1$.

5.15. Let x be an integer. Prove that $0|x$ if and only if $x = 0$.

5.16. Let a and b be integers. Prove that $a < b$ if and only if $a \leq b - 1$.

5.17. Let a be a number with $a > 1$. Prove that a number x is strictly between 1 and $\sqrt{a}$ if and only if a/x is strictly between $\sqrt{a}$ and a.

You may assume that $1 < \sqrt{a} < a$. (We ask you to prove this later; see Exercise 20.10.)

By *consecutive perfect squares* we mean numbers such as 3^2 and 4^2 or 12^2 and 13^2.

5.18. Prove that the difference between consecutive perfect squares is odd.

5.19. Let a be a perfect square. Prove that a is the square on a nonnegative integer.

5.20. For real numbers a and b, prove that if $0 < a < b$, then $a^2 < b^2$.

5.21. Prove that the difference between distinct, nonconsecutive perfect squares is composite.

5.22. Prove that an integer is odd if and only if it is the sum of two consecutive integers.

5.23. Suppose you are asked to prove a statement of the form "If A or B, then C." Explain why you need to prove (a) "If A, then C" and also (b) "If B, then C." Why is it not enough to prove only one of (a) and (b)?

5.24. Suppose you are asked to prove a statement of the form "A iff B." The standard method is to prove both $A \Rightarrow B$ and $B \Rightarrow A$.

Consider the following alternative proof strategy: Prove both $A \Rightarrow B$ and (not A) $\Rightarrow$ (not B). Explain why this would give a valid proof.

6 Counterexample

In the previous section, we developed the notion of proof: a technique to demonstrate irrefutably that a given statement is true. Not all statements about mathematics are true! Given a statement, how do we show that it is false? Disproving false statements is often simpler than proving theorems. The typical way to disprove an if-then statement is to create a *counterexample*. Consider the statement "If A, then B." A counterexample to such a statement would be an instance where A is true but B is false.

For example, consider the statement "If x is a prime, then x is odd." This statement is false. To prove that it is false, we just have to give an example of an integer that is prime but is not odd. The integer 2 has the requisite properties.

Let's consider another false statement.

Statement 6.1 **(false)** Let a and b be integers. If $a|b$ and $b|a$, then $a = b$.

This statement appears plausible. It seems that if $a|b$, then $a \leq b$, and if $b|a$, then $b \leq a$, and so $a = b$. But this reasoning is incorrect.

To disprove Statement 6.1, we need to find integers a and b that, on the one hand, satisfy $a|b$ and $b|a$ but, on the other hand, do not satisfy $a = b$.

Here is a counterexample: Take $a = 5$ and $b = -5$. To check that this is a counterexample, we simply note that, on the one hand, $5|-5$ and $-5|5$ but, on the other hand, $5 \neq -5$.

Proof Template 3 Refuting a false if-then statement via a counterexample.

To disprove a statement of the form "If A, then B":

Find an instance where A is true but B is false.

Refuting false statements is usually easier than proving true statements. However, finding counterexamples can be tricky. To create a counterexample, I recommend you try creating several instances where the hypothesis of the statement is true and check each to see whether or not the conclusion holds. All it takes is one counterexample to disprove a statement.

Unfortunately, it is easy to get stuck in a thinking rut. For Statement 6.1, we might consider $3|3$ and $4|4$ and $5|5$ and never think about making one number positive and the other negative.

Try to break out of such a rut by creating strange examples. Don't forget about the number 0 (which acts strangely) and negative numbers. Of course, following that advice, we might still be stuck in the rut $0|0, -1|-1, -2|-2$, and so on.

A strategy for finding counterexamples.

Here is a strategy for finding counterexamples. Begin by trying to prove the statement; when you get stuck, try to figure out what the problem is and look there to build a counterexample.

Let's apply this technique to Statement 6.1. We start, as usual, by converting the hypothesis and conclusion of the statement into the beginning and end of the proof.

> Let a and b be integers with $a|b$ and $b|a$. ... Therefore $a = b$. ■

Next we unravel definitions.

> Let a and b be integers with $a|b$ and $b|a$. Since $a|b$, there is an integer x such that $b = ax$. Since $b|a$, there is an integer y such that $a = by$. ... Therefore $a = b$. ■

Now we ask: What do we know? What do we need? We know

$$b = ax \qquad \text{and} \qquad a = by$$

and we want to show $a = b$. To get there, we can try to show that $x = y = 1$. Let's try to solve for x or y.

Since we have two expressions in terms of a and b, we can try substituting one in the other. We use the fact that $b = ax$ to eliminate b from $a = by$. We get

$$a = by \quad \Rightarrow \quad a = (ax)y \quad \Rightarrow \quad a = (xy)a.$$

It now looks quite tempting to divide both sides of the last equation by a, but we need to worry that perhaps, $a = 0$. Let's ignore the possibility of $a = 0$ for just a moment and go ahead and write $xy = 1$. We see that we have two integers whose product is 1. And we realize at this point that there are two ways that can happen: either $1 = 1 \times 1$ or $1 = -1 \times -1$. So although we know $xy = 1$, we can't conclude that $x = y = 1$ and finish the proof. We're stuck and now we consider the possibility that Statement 6.1 is false. We ask: What if $x = y = -1$? We see that this would imply that $a = -b$; for example, $a = 5$ and $b = -5$. And then we realize that in such a case, $a|b$ and $b|a$ but $a \neq b$. We have found a counterexample. Do we need to go back to our worry that perhaps $a = 0$? No! We have refuted the statement with our counterexample. The attempted proof served only to help us find a counterexample.

Recap

This section showed how to disprove an if-then statement by finding an example that satisfies the hypothesis of the statement but not the conclusion.

6 Exercises

6.1. Disprove: If a and b are integers with $a|b$, then $a \leq b$.

6.2. Disprove: If a and b are nonnegative integers with $a|b$, then $a \leq b$.
Note: A counterexample to this statement would also be a counterexample for the previous problem, but not necessarily vice versa.

6.3. Disprove: If a, b, and c are positive integers with $a|(bc)$, then $a|b$ or $a|c$.

6.4. Disprove: If a, b, and c are positive integers, then $a^{(b^c)} = (a^b)^c$.

6.5. Disprove: If p and q are prime, then $p + q$ is composite.

6.6. Disprove: If p is prime, then $2^p - 1$ is also prime.

6.7. Disprove: If n is a nonnegative integer, then $2^{(2^n)} + 1$ is prime.

6.8. An integer is a *palindrome* if it reads the same forwards and backwards when expressed in base-10. For example, 1331 is a palindrome.
Disprove: All palindromes with two or more digits are divisible by 11.

6.9. Consider the polynomial $n^2 + n + 41$.
(a) Calculate the value of this polynomial for $n = 1, 2, 3, \ldots, 10$.
Notice that all the numbers you computed are prime.
(b) Disprove: If n is a positive integer, then $n^2 + n + 41$ is prime.

6.10. What does it mean for an if-and-only-if statement to be false? What properties should a counterexample for an if-and-only-if statement have?

6.11. Disprove: An integer x is positive if and only if $x + 1$ is positive.

6.12. Disprove: Two right triangles have the same area if and only if the lengths of their hypotenuses are the same.

6.13. Disprove: A positive integer is composite if and only if it has two different prime factors.

7 Boolean Algebra

Algebra is useful for reasoning about *numbers*. An algebraic relationship, such as $x^2 - y^2 = (x - y)(x + y)$, describes a general relationship that holds for any numbers x and y.

In a similar way, Boolean algebra provides a framework for dealing with *statements*. We begin with basic statements, such as "x is prime," and combine them using connectives such as *if-then*, *and*, *or*, *not*, and so on.

For example, in Section 4 you were asked (see Exercise 4.4) to explain why the statements "If A, then B" and "(not A) or B" mean essentially the same thing. In this section, we present a simple method for showing that such sentences have the same meaning.

In an ordinary algebraic expression, such as $3x - 4$, letters stand for numbers, and the operations are the familiar ones of addition, subtraction, multiplication, and so forth. The value of the expression $3x - 4$ depends on the number x. When $x = 1$, the value of the expression is -1, and if $x = 10$, the value is 26.

Variables stand for TRUE and FALSE.

Boolean algebra also has expressions containing letters and operations. Letters (variables) in a Boolean expression do not stand for numbers. Rather, they stand for the values TRUE and FALSE. Thus letters in a Boolean algebraic expression can only have two values!

The basic operations of Boolean algebra are $\wedge$, $\vee$, and $\neg$. These operations are also present in many computer languages. Since computer keyboards typically do not have these symbols, the symbols & (for $\wedge$), | (for $\vee$), and $\sim$ (for $\neg$) are often used instead.

There are several operations we can perform on the values TRUE and FALSE. The most basic operations are called *and* (symbol: $\wedge$), *or* (symbol: $\vee$), and *not* (symbol: $\neg$).

We begin with $\wedge$. To define $\wedge$, we need to define the value of $x \wedge y$ for all possible values of x and y. Since there are only two possible values for each of x and y, this is not hard. Without further ado, here is the definition of the operation $\wedge$.

$$\begin{aligned} \text{TRUE} \wedge \text{TRUE} &= \text{TRUE} \\ \text{TRUE} \wedge \text{FALSE} &= \text{FALSE} \\ \text{FALSE} \wedge \text{TRUE} &= \text{FALSE} \\ \text{FALSE} \wedge \text{FALSE} &= \text{FALSE}. \end{aligned}$$

In other words, the value of the expression $x \wedge y$ is TRUE when both x and y are TRUE and is FALSE otherwise. A convenient way to write all this is in a *truth table*, which is a chart showing the value of a Boolean expression depending on the values of the variables. Here is a truth table for the operation $\wedge$.

x	y	$x \wedge y$
TRUE	TRUE	TRUE
TRUE	FALSE	FALSE
FALSE	TRUE	FALSE
FALSE	FALSE	FALSE

The definition of the operation $\wedge$ is designed to mirror exactly the mathematical use of the English word *and*. Similarly, the Boolean operation $\vee$ is designed to mirror exactly the mathematical use of the English word *or*. Here is the definition of $\vee$.

$$\begin{aligned} \text{TRUE} \vee \text{TRUE} &= \text{TRUE} \\ \text{TRUE} \vee \text{FALSE} &= \text{TRUE} \\ \text{FALSE} \vee \text{TRUE} &= \text{TRUE} \\ \text{FALSE} \vee \text{FALSE} &= \text{FALSE}. \end{aligned}$$

In other words, the value of the expression $x \vee y$ is TRUE in all cases except when both x and y are FALSE. We summarize this in a truth table.

x	y	$x \vee y$
TRUE	TRUE	TRUE
TRUE	FALSE	TRUE
FALSE	TRUE	TRUE
FALSE	FALSE	FALSE

The third operation, $\neg$, is designed to reproduce the mathematical use of the English word *not*:

$$\neg\text{TRUE} = \text{FALSE}$$
$$\neg\text{FALSE} = \text{TRUE}.$$

In truth table form, $\neg$ is as follows:

x	$\neg x$
TRUE	FALSE
FALSE	TRUE

Ordinary algebraic expressions (e.g., $3\times 2-4$) may combine several operations. Likewise we can combine the Boolean operations. For example, consider

$$\text{TRUE} \wedge ((\neg\text{FALSE}) \vee \text{FALSE}).$$

Let us calculate the value of this expression step by step:

$$\begin{aligned}\text{TRUE} \wedge ((\neg\text{FALSE}) \vee \text{FALSE}) &= \text{TRUE} \wedge (\text{TRUE} \vee \text{FALSE}) \\ &= \text{TRUE} \wedge \text{TRUE} \\ &= \text{TRUE}.\end{aligned}$$

In algebra we learn how to manipulate formulas so we can derive identities such as

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

In Boolean algebra we are interested in deriving similar identities. Let us begin with a simple example:

$$x \wedge y = y \wedge x.$$

What does this mean? The ordinary algebraic identity $(x + y)^2 = x^2 + 2xy + y^2$ means that once we choose (numeric) values for x and y, the two expressions $(x+y)^2$ and $x^2+2xy+y^2$ must be equal. Similarly, the identity $x \wedge y = y \wedge x$ means that once we choose (truth) values for x and y, the results $x \wedge y$ and $y \wedge x$ must be the same.

Now it would be ridiculous to try to prove an identity such as $(x + y)^2 = x^2 + 2xy + y^2$ by trying to substitute all possible values for x and y—there are infinitely many possibilities! However, it is not hard to try all the possibilities to prove a Boolean algebraic identity. In the case of $x \wedge y = y \wedge x$, there are only four possibilities. Let us summarize these in a truth table.

x	y	$x \wedge y$	$y \wedge x$
TRUE	TRUE	TRUE	TRUE
TRUE	FALSE	FALSE	FALSE
FALSE	TRUE	FALSE	FALSE
FALSE	FALSE	FALSE	FALSE

By running through all possible combinations of values for x and y, we have a *proof* that $x \wedge y = y \wedge x$.

Logical equivalence.

When two Boolean expressions, such as $x \wedge y$ and $y \wedge x$, are equal for all possible values of their variables, we call these expressions *logically equivalent*. The simplest method to show that two Boolean expressions are logically equivalent is to run through all the possible values for the variables in the two expressions and to check that the results are the same in every case.

Let us consider a more interesting example.

Proposition 7.1 The Boolean expressions $\neg(x \wedge y)$ and $(\neg x) \vee (\neg y)$ are logically equivalent.

Proof. To show this is true, we construct a truth table for both expressions. To save space, we write T for TRUE and F for FALSE.

x	y	$x \wedge y$	$\neg(x \wedge y)$	$\neg x$	$\neg y$	$(\neg x) \vee (\neg y)$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

The important thing to notice is that the columns for $\neg(x \wedge y)$ and $(\neg x) \vee (\neg y)$ are exactly the same. Therefore, no matter how we choose the values for x and y, the expressions $\neg(x \wedge y)$ and $(\neg x) \vee (\neg y)$ evaluate to the same truth value. Therefore the expressions $\neg(x \wedge y)$ and $(\neg x) \vee (\neg y)$ are logically equivalent. ■

Proof Template 4 Truth table proof of logical equivalence

To show that two Boolean expressions are logically equivalent:
Construct a truth table showing the values of the two expressions for all possible values of the variables.
Check to see that the two Boolean expressions always have the same value.

Proofs by means of truth tables are easy but dull. The following result summarizes the basic algebraic properties of the operations $\wedge$, $\vee$, and $\neg$. In several cases, we give names for the properties.

Theorem 7.2

- $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$. (Commutative properties)
- $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ and $(x \vee y) \vee z = x \vee (y \vee z)$. (Associative properties)
- $x \wedge \text{TRUE} = x$ and $x \vee \text{FALSE} = x$. (Identity elements)
- $\neg(\neg x) = x$.
- $x \wedge x = x$ and $x \vee x = x$.
- $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ and $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$. (Distributive properties)
- $x \wedge (\neg x) = \text{FALSE}$ and $x \vee (\neg x) = \text{TRUE}$.
- $\neg(x \wedge y) = (\neg x) \vee (\neg y)$ and $\neg(x \vee y) = (\neg x) \wedge (\neg y)$. (DeMorgan's Laws)

All of these logical equivalences are easily proved via truth tables. In some of these identities, there is only one variable (e.g., $x \wedge \neg x = \text{FALSE}$); in this case, there would be only two rows in the truth table (one for $x = \text{TRUE}$ and one for $x = \text{FALSE}$). In the cases where there are three variables, there are eight rows in the truth table as (x, y, z) take on the possible values (T, T, T), (T, T, F), (T, F, T), (T, F, F), (F, T, T), (F, T, F), (F, F, T), and (F, F, F).

More Operations

The operations $\wedge$, $\vee$, and $\neg$ were created to replicate mathematicians' use of the words *and*, *or*, and *not*. We now introduce two more operations, $\rightarrow$ and $\leftrightarrow$, designed to model statements of the form "If A, then B" and "A if and only if B," respectively. The simplest way to define these is through truth tables.

x	y	$x \to y$
TRUE	TRUE	TRUE
TRUE	FALSE	FALSE
FALSE	TRUE	TRUE
FALSE	FALSE	TRUE

and

x	y	$x \leftrightarrow y$
TRUE	TRUE	TRUE
TRUE	FALSE	FALSE
FALSE	TRUE	FALSE
FALSE	FALSE	TRUE

The expression $x \to y$ models an if-then statement. We have $x \to y =$ TRUE except when $x =$ TRUE and $y =$ FALSE. Likewise the statement "If A, then B" is true unless there is an instance in which A is true but B is false. Indeed, the arrow $\to$ reminds us of the implication arrow $\Rightarrow$.

Similarly, the expression $x \leftrightarrow y$ models the statement "A if and only if B." The expression $x \leftrightarrow y$ is true provided x and y are either both true or both false. Likewise the statement "$A \iff B$" is true provided that in every instance A and B are both true or both false.

Let us revisit the issue that the statements "If A, then B" and "(not A) or B" mean the same thing (see Exercise 4.4).

Proposition 7.3 The expressions $x \to y$ and $(\neg x) \vee y$ are logically equivalent.

Proof. We construct a truth table for both expressions.

x	y	$x \to y$	$\neg x$	y	$(\neg x) \vee y$
TRUE	TRUE	TRUE	FALSE	TRUE	TRUE
TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
FALSE	TRUE	TRUE	TRUE	TRUE	TRUE
FALSE	FALSE	TRUE	TRUE	FALSE	TRUE

The columns for $x \to y$ and $(\neg x) \vee y$ are the same, and therefore these expressions are logically equivalent. ∎

Proposition 7.3 shows how the operation $\to$ can be reexpressed just in terms of the basic operations $\vee$ and $\neg$. Similarly, the operation $\leftrightarrow$ can be expressed in terms of the basic operations $\wedge$, $\vee$, and $\neg$ (see Exercise 7.15).

Recap

This section presented Boolean algebra as "arithmetic" with the values TRUE and FALSE. The basic operations are $\wedge$, $\vee$, and $\neg$. Two Boolean expressions are logically equivalent provided they always yield the same values when we substitute for their variables. We can prove Boolean expressions are logically equivalent using truth tables. We concluded this section by defining the operations $\to$ and $\leftrightarrow$.

7 Exercises

7.1. Do the following calculations:

a. TRUE $\wedge$ TRUE $\wedge$ TRUE $\wedge$ TRUE $\wedge$ FALSE.

b. $(\neg$TRUE$)$ $\vee$ TRUE.

c. $\neg$(TRUE $\vee$ TRUE).

d. (TRUE $\vee$ TRUE) $\wedge$ FALSE.

e. TRUE $\vee$ (TRUE $\wedge$ FALSE).

The point of the last four is that the order in which you do the operations matters! Compare the expressions in (b)–(c) and (d)–(e) and note that they are the same except for the placement of the parentheses.

Now rethink your answer to (a). Does your answer to (a) depend on the order in which you do the operations?

7.2. Prove by use of truth tables as many parts of Theorem 7.2 as you can tolerate.

7.3. Prove: $(x \wedge y) \vee (x \wedge \neg y)$ is logically equivalent to x.

An if-then statement is logically equivalent to its contrapositive.

7.4. Prove: $x \to y$ is logically equivalent to $(\neg y) \to (\neg x)$.

7.5. Prove: $x \leftrightarrow y$ is logically equivalent to $(\neg x) \leftrightarrow (\neg y)$.

7.6. Prove: $x \leftrightarrow y$ is logically equivalent to $(x \to y) \wedge (y \to x)$.

7.7. Prove: $x \leftrightarrow y$ is logically equivalent to $(x \rightarrow y) \wedge ((\neg x) \rightarrow (\neg y))$.

7.8. Prove: $(x \vee y) \rightarrow z$ is logically equivalent to $(x \rightarrow z) \wedge (y \rightarrow z)$.

7.9. Suppose we have two Boolean expressions that involve ten variables. To prove that these two expressions are logically equivalent, we construct a truth table. How many rows (besides the "header" row) would this table have?

7.10. How would you disprove a logical equivalence? Show the following:

An if-then statement is not logically equivalent to its converse.

a. $x \rightarrow y$ is not logically equivalent to $y \rightarrow x$.

b. $x \rightarrow y$ is not logically equivalent to $x \leftrightarrow y$.

c. $x \vee y$ is not logically equivalent to $(x \wedge \neg y) \vee ((\neg x) \wedge y)$.

7.11. A *tautology* is a Boolean expression that evaluates to TRUE for all possible values of its variables. For example, the expression $x \vee \neg x$ is TRUE both when $x =$ TRUE and when $x =$ FALSE. Thus $x \vee \neg x$ is a tautology.

Explain how to use a truth table to prove that a Boolean expression is a tautology and prove that the following are tautologies.

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

b. $(x \wedge (x \rightarrow y)) \rightarrow y$.

c. $(\neg(\neg x)) \leftrightarrow x$.

d. $x \rightarrow x$.

e. $((x \rightarrow y) \wedge (y \rightarrow z)) \rightarrow (x \rightarrow z)$.

f. FALSE $\rightarrow x$.

g. $(x \rightarrow$ FALSE$) \rightarrow \neg x$.

h. $((x \rightarrow y) \wedge (x \rightarrow \neg y)) \rightarrow \neg x$.

7.12. In the previous problem you proved that certain Boolean formulas are tautologies by creating truth tables. Another method is to use the properties listed in Theorem 7.2 together with the fact that $x \rightarrow y$ is equivalent to $(\neg x) \vee y$ (Proposition 7.3).

For example, part (b) asks you to establish that the formula $(x \wedge (x \rightarrow y)) \rightarrow y$ is a tautology. Here is a derivation of that fact:

$$
\begin{aligned}
(x \wedge (x \rightarrow y)) \rightarrow y &= [x \wedge (\neg x \vee y)] \rightarrow y && \text{translate } \rightarrow \\
&= [(x \wedge \neg x) \vee (x \wedge y)] \rightarrow y && \text{distributive} \\
&= [\text{FALSE} \vee (x \wedge y)] \rightarrow y \\
&= (x \wedge y) \rightarrow y && \text{identity element} \\
&= (\neg(x \wedge y)) \vee y && \text{translate } \rightarrow \\
&= (\neg x \vee \neg y) \vee y && \text{De Morgan} \\
&= \neg x \vee (\neg y \vee y) && \text{associative} \\
&= \neg x \vee \text{TRUE} \\
&= \text{TRUE} && \text{identity.}
\end{aligned}
$$

Use this technique to prove that the other formulas in Exercise 7.11 are tautologies.

You may replace $x \leftarrow y$ with $y \rightarrow x$ (which, in turn, is equivalent to $\neg y \vee x$) and you may replace $x \leftrightarrow y$ with $(x \rightarrow y) \wedge (y \rightarrow x)$.

7.13. A *contradiction* is a Boolean expression that evaluates to FALSE for all possible values of its variables. For example, $x \wedge \neg x$ is a contradiction.

Prove that the following are contradictions:

a. $(x \vee y) \wedge (x \vee \neg y) \wedge \neg x$.

b. $x \wedge (x \rightarrow y) \wedge (\neg y)$.

c. $(x \rightarrow y) \wedge ((\neg x) \rightarrow y) \wedge \neg y$.

7.14. Suppose A and B are Boolean expressions—that is, A and B are formulas involving variables (x, y, z, etc.) and Boolean operations ($\wedge$, $\vee$, $\neg$, etc.).

Prove: A is logically equivalent to B if and only if $A \leftrightarrow B$ is a tautology.

7.15. The expression $x \rightarrow y$ can be rewritten in terms of only the basic operations $\wedge$, $\vee$, and $\neg$; that is, $x \rightarrow y = (\neg x) \vee y$.

Find an expression that is logically equivalent to $x \leftrightarrow y$ and uses only the basic operations $\wedge$, $\vee$, and $\neg$ (and prove that you are correct).

The phrase *exclusive or* is sometimes written as *xor*.

7.16. Here is another Boolean operation called *exclusive or*; it is denoted by the symbol $\veebar$. It is defined in the following table.

x	y	$x \veebar y$
TRUE	TRUE	FALSE
TRUE	FALSE	TRUE
FALSE	TRUE	TRUE
FALSE	FALSE	FALSE

Please do the following:

a. Prove that $\veebar$ obeys the commutative and associative properties; that is, prove the logical equivalences $x \veebar y = y \veebar x$ and $(x \veebar y) \veebar z = x \veebar (y \veebar z)$.

b. Prove that $x \veebar y$ is logically equivalent to $(x \wedge \neg y) \vee ((\neg x) \wedge y)$. (Thus $\veebar$ can be expressed in terms of the basic operations $\wedge$, $\vee$, and $\neg$.)

c. Prove that $x \veebar y$ is logically equivalent to $(x \vee y) \wedge (\neg(x \wedge y))$. (This is another way that $\veebar$ can be expressed in terms of $\wedge$, $\vee$, and $\neg$.)

d. Explain why the operation $\veebar$ is called *exclusive or*.

A binary operation is an operation that combines two values. The operation $\neg$ is not binary because it works on just one value at a time; it is called *unary*.

7.17. We have discussed several binary Boolean operations: $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, and (in the previous problem) $\veebar$. How many different binary Boolean operations can there be? In other words, in how many different ways can we complete the following chart?

x	y	$x * y$
TRUE	TRUE	?
TRUE	FALSE	?
FALSE	TRUE	?
FALSE	FALSE	?

There aren't too many possibilities, and, in worst case, you can try writing out all of them. Be sure to organize your list carefully so you don't miss any or accidentally list the same operation twice.

7.18. We have seen that the operations $\rightarrow$, $\leftrightarrow$, and $\veebar$ can be reexpressed in terms of the basic operations $\wedge$, $\vee$, and $\neg$. Show that all binary Boolean operations (see the previous problem) can be expressed in terms of these basic three.

7.19. Prove that $x \vee y$ can be reexpressed in terms of just $\wedge$ and $\neg$ so all binary Boolean operations can be reduced to just two basic operations.

Nand.

7.20. Here is yet another Boolean operation called *nand*; it is denoted by the symbol $\overline{\wedge}$. We define $x \overline{\wedge} y$ to be $\neg(x \wedge y)$.

Please do the following:

a. Construct a truth table for $\overline{\wedge}$.

b. Is the operation $\overline{\wedge}$ commutative? Associative?

c. Show how the operations $x \wedge y$ and $\neg x$ can be reexpressed just in terms of $\overline{\wedge}$.

d. Conclude that all binary Boolean operations can be reexpressed just in terms of $\overline{\wedge}$ alone.

Chapter 1 Self Test

1. True or false: Every positive integer is either prime or composite. Explain your answer.

2. Find all integers x for which $x|(x+2)$. You do not need to prove your answer.

3. Let a and b be positive integers. Explain why the notation $a|b+1$ can be interpreted only as $a|(b+1)$ and not as $(a|b)+1$.

It is not known whether every perfect number is even, but it is conjectured that there are no odd perfect numbers.

4. Write the following statement in if-then form: "Every perfect integer is even."

5. Write the converse of the statement "If you love me, then you will marry me."

6. Determine which of the following statements are true and which are false. You should base your reply on your common knowledge of mathematics; you do not need to prove your answers.

a. Every integer is positive or negative.

b. Every integer is even and odd.

c. If x is an integer and $x > 2$ and x is prime, then x is odd.

d. Let x and y be integers. We have $x^2 = y^2$ if and only if $x = y$.

e. The sides of a triangle are all congruent to each other if and only if its three angles are all 60°.

f. If an integer x satisfies $x = x + 1$, then $x = 6$.

7. Consider the following statement (which you are not expected to understand): "If a matroid is graphic, then it is representable."

Write the first and last lines of a direct proof of this statement.

It is customary to use the letter M to stand for a matroid.

8. The following statement is false: If x, y, and z are integers and $x > y$, then $xz > yz$.

Please do the following:

a. Find a counterexample.

b. Modify the hypothesis of the statement by adding a condition concerning z so that the edited statement is true.

9. Prove or disprove the following statements:

a. Let a, b, c be integers. If $a|c$ and $b|c$, then $(a + b)|c$.

b. Let a, b, c be integers. If $a|b$, then $(ac)|(bc)$.

10. Consider the following proposition. Let N be a two-digit number and let M be the number formed from N by reversing N's digits. Now compare N^2 and M^2. The digits of M^2 are precisely those of N^2, but reversed.

For example:

$$10^2 = 100 \qquad 01^2 = 001$$
$$11^2 = 121 \qquad 11^2 = 121$$
$$12^2 = 144 \qquad 21^2 = 441$$
$$13^2 = 169 \qquad 31^2 = 961$$

and so on.

Here is a proof of the proposition:

Proof. Since N is a two-digit number, we can write $N = 10a + b$ where a and b are the digits of N. Since M is formed from N by reversing digits, $M = 10b + a$.

Note that $N^2 = (10a + b)^2 = 100a^2 + 20ab + b^2 = (a^2) \times 100 + (2ab) \times 10 + (b^2) \times 1$, so the digits of N^2 are, in order, $a^2, 2ab, b^2$.

Likewise, $M^2 = (10b + a)^2 = (b^2) \times 100 + (2ab) \times 10 + (a^2) \times 1$, so the digits of M^2 are, in order, $b^2, 2ab, a^2$, exactly the reverse of N^2. ∎

Your job: Show that the proposition is false and explain why the proof is invalid.

11. Suppose we are asked to prove the following identity:

$$x(x + y - 1) - y(x + 1) = x(x - 1) - y.$$

The identity is true (i.e., the equation is valid for all real numbers x and y).

The following "proof" is incorrect. Explain why.

Proof. We begin with

$$x(x + y - 1) - y(x + 1) = x(x - 1) - y$$

and expand the terms (using the distributive property)

$$x^2 + xy - x - yx - y = x^2 - x - y.$$

We cancel the terms x^2, $-x$, and $-y$ from both sides to give

$$xy - yx = 0,$$

and finally xy and $-yx$ cancel to give

$$0 = 0,$$

which is correct. ∎

12. Are the Boolean expressions $x \to \neg y$ and $\neg(x \to y)$ logically equivalent? Justify your answer.

13. Is the Boolean expression $(x \to y) \vee (x \to \neg y)$ a tautology? Justify your answer.

14. Prove that the sum of any three consecutive integers is divisible by three.

15. In the previous problem you were asked to prove that the sum of any three consecutive integers is divisible by three. Note, however, that the sum of any four consecutive integers is never divisible by four. For example, $10 + 11 + 12 + 13 = 46$, which is not divisible by four.

For which positive integers a is the sum of a consecutive integers divisible by a? That is, complete the following sentence to give a true statement:

> Let a be a positive integer. The sum of a consecutive integers is divisible by a if and only if ....

You need not prove your conjecture.

16. Let a be an integer. Prove: If $a \geq 3$, then $a^2 > 2a + 1$.

17. Suppose a is a perfect square and $a \geq 9$. Prove that $a - 1$ is composite.

See Exercise 3.6 and its solution on page 409 for the definition of *perfect square*.

18. Consider the following definition:

A pair of positive integers, x and y, are called *square mates* if their sum, $x + y$ is a perfect square. (The concept of square mates was contrived just for this test, problems 18 to 20.)

For example, 4 and 5 are square mates because $4 + 5 = 9 = 3^2$. Likewise, 8 and 8 are square mates because $8 + 8 = 16 = 4^2$. However, 3 and 8 are not square mates.

Explain why 10 and -1 are not square mates.

19. Let x be a positive integer. Prove that there is an integer y that is greater than x such that x and y are square mates.

20. Prove that if x is an integer and $x \geq 5$, then x has a square mate y with $y < x$.

You may use the following fact in your proof. If x is a positive integer, then x lies between two consecutive perfect squares; that is, there is a positive integer a such that $a^2 \leq x < (a + 1)^2$.