Sylvia Forman
Agnes M. Rash

The Whole Truth About Whole Numbers

An Elementary Introduction to Number Theory

The Whole Truth About Whole Numbers

Sylvia Forman • Agnes M. Rash

The Whole Truth About Whole Numbers

An Elementary Introduction
to Number Theory

Sylvia Forman
Department of Mathematics
St. Joseph's University
Philadelphia, PA, USA

Agnes M. Rash
Department of Mathematics
St. Joseph's University
Philadelphia, PA, USA

This work is dedicated to my mother and role model for her inspiration and encouragement and to my husband for his unending support.

—Agnes M. Rash

To Sean, Carl, and Elinore

—Sylvia Forman

Preface to the Instructor

The Whole Truth About Whole Numbers

This textbook introduces the field of number theory at a level accessible to nonmath and nonscience majors. The target audience is students in either a liberal arts mathematics course or a course focused on elementary education majors at any college or university. The content of this book is similar to what is included in a standard introductory number theory course offered for mathematics majors, but the presentation is much different. The text includes an introduction to logic and proofs, at a level suitable for liberal arts majors, as well as major concepts in number theory accessible to students with 2 years of high-school algebra. This text is designed to be used in a one-semester (15-week) course.

Throughout the book, concepts have been linked and ordered to show connections between them. For example, the greatest common divisor is first defined in Chap. 2 and used to identify primitive Pythagorean triples in Chap. 3. In Chap. 4, the greatest common divisor is discussed in connection with prime factors, and then in Chap. 5 the Euclidean Algorithm is used to calculate greatest common divisors. Proof techniques and methods are introduced in Chap. 2 using the familiar concepts of *even* and *odd*, and then students continue to write proofs about each new topic they encounter throughout the text.

In Chap. 1, the importance of precise communication in mathematics is stressed, and some common problem-solving techniques are introduced. Examples are given using facts about integers, considering cases and looking for a pattern. Terms such as *even*, *odd*, *prime*, and *divisible* are discussed, but these are formally defined in Chap. 2 so that it is possible to omit Chap. 1.

Knowing how to verify whether a statement is true or false is basic to mathematics. Students must learn how to precisely state and justify ideas. Chapter 2 includes a brief introduction to logic including the basic logical connectives and the types of compound sentences formed using them. Section 2.4 includes formal definitions of some basic terms (even, odd, prime). Sections 2.5 and 2.6 illustrate some common

proof techniques, such as a direct proof, a proof by contradiction, and an indirect proof (proof by contrapositive). Proofs by contradiction come up again in Chap. 4, in the proof that there are infinitely many primes. The contrapositive of a statement is also used in Chap. 4 to formulate a primality test; however, indirect proofs are not necessary to the proofs in the rest of the text, so this topic could be skipped if desired. Proving statements false using a counterexample is also discussed in Chap. 2. The last section of Chap. 2 provides a review of divisibility rules which are useful throughout the text. Chapter 2 should be covered before proceeding to further chapters.

Chapter 3 is not essential for understanding the concepts presented later, but it gives students practice with elementary proofs through building on their knowledge of a familiar topic: right triangles. While discussing this material, the authors show NOVA's film *The Proof*, about Andrew Wiles' path to proving Fermat's Last Theorem. This provides the opportunity to remark that you never know when an idea will have a new application.

Chapter 4 on prime numbers is central to the study of number theory. Section 4.3 explores arithmetic in the even integers in order to show that the unique factorization property of the integers does not hold in every number system, and is optional. Section 4.5 discusses some unsolved questions in number theory as well as the search for larger primes and could also be omitted.

In Chap. 5, the division algorithm is discussed in detail in order to motivate the study of the Euclidean Algorithm as well as modular arithmetic described in Chap. 6. Section 6.4 is an application of congruences to check digits, so the rest of the material in the book is not dependent upon it. The Chinese Remainder Theorem in Section 6.5 is also not necessary for the remaining material. In Chap. 7, Section 7.5 could also be omitted to make time for covering cryptography. Euler's phi function and Euler's theorem in Sections 7.4 and 7.6 are needed for Chap. 8.

Chapter 8 introduces a modern application of number theory to public key cryptography but also includes several examples of private key codes in Sections 8.2 and 8.3 for contrast. If needed, these sections could be omitted to allow time for an introduction to the application of number theory to the RSA public key code, contained in Section 8.4.

Philadelphia, PA, USA   Sylvia Forman
Philadelphia, PA, USA   Agnes M. Rash

Preface to the Student

"Archimedes will be remembered when Aeschylus is forgotten, because languages die and mathematical ideas do not."

—G. H. Hardy (1877–1947)

Number theory is the study of whole numbers. Early in recorded history, humans began to count using the natural numbers 1, 2, 3, ... The earliest counting did not progress very far in this sequence, partially because numbers were associated with the items that could be counted on fingers (also called digits) and toes. Whole numbers (or integers) include natural numbers and their negatives as well as zero. These numbers and their properties have been studied extensively, at least since the time of the Babylonians and the golden age of Greece. Many learned people were fascinated with these numbers and proved theorems about whole numbers just for the personal satisfaction of finding the results. In the fifth century B.C., Pythagoras remarked "All is number" and, like many mathematicians, believed that numbers had special properties that could be used to describe or represent the world around them. For example, Pythagoras identified "1" as the number of reason and "10" as the number of the universe.

There is a certain satisfaction that one gets by accomplishing a goal, performing a difficult task, or discovering a new fact. Throughout the ages, this fascination with whole numbers has led to many great discoveries. Breakthroughs, discoveries, and new ideas often occur as an inspiration or an "aha" moment. When Archimedes had such an "aha" moment, the story goes that he leapt out of the bathtub and ran through the streets proclaiming "Eureka, I have found it!"

There are concepts that were discovered just for the fun of it that eventually turned out to be very useful and have had profound implications for modern times. One such example is the Euclidean Algorithm, discovered by Euclid in the third century B.C. This result is now widely used in cryptography and the design of secret codes discussed in Chap. 8.

We hope that you have "aha" moments, although hopefully less provocative than Archimedes', as we learn about number theory.

Develop a Plan for Learning Mathematics

In any human endeavor, to become proficient one must be dedicated. Think about a particular activity, such as playing a guitar or shooting a basketball. Whether it is a hobby or a profession, to be good at something requires practice. The more you practice, usually the better you become. The same is true for mathematics. Here are some suggestions to help you to be successful in understanding mathematical concepts and to be able to use them in the future.

Prior to the class, read the material that will be covered in class to get an idea of what the topic is and to know if there are new terms that you will have to learn. Be sure that you have done the homework and note down any questions that you want to ask about the assignment.

In class, ask questions about what is unclear. Professors are happy to help students understand concepts, clarify ideas, and eliminate errors in problems, whether they are small errors or large misunderstandings. Take notes during the class. Ask the instructor to repeat something if you missed it.

After class, read your notes and the class materials, with a pencil and paper. Take down notes and work out examples where necessary. Rewriting something makes it easier to remember later. Make sure that you understand the concepts and terms.

When reading an example, be sure you understand the problem. After you have read one example, try to solve the next example before reading its solution.

The more you practice, the better you will be. Pick out a couple of easy problems, moderately difficult problems, and problems that require extra effort, and see if you can solve them. Often, explaining a concept to a fellow student will help clarify the concept to yourself. When you read a theorem and its proof, be sure you know what the hypothesis is. Try to figure out what direction the proof might take before reading the proof. When you read the proof, you can see how close your ideas were to the proof in the text.

When studying for a test, start preparing several days before the test. Try to solve problems that you think might appear on the exam. Read over your notes and the text to determine the key concepts. Go through the problems that you had trouble with earlier, and be sure that you can solve them. If you have any difficulty, talk to your instructor and get help. A study group is also helpful in preparing for a test. Cramming might get you through one test, but by the time of the final exam, you will have forgotten the material.

Reading mathematics is an active process. You may have to go back and refresh your memory of a concept, definition, or theorem. Don't get discouraged; some concepts have taken centuries to develop, so it is not surprising if you don't understand them during your first reading.

During a test, begin by reading all of the problems. Find the ones that you can solve quickly and easily and do them first, leaving enough time to work on the other problems that require more effort. If you get stuck on a problem, take a deep breath and relax. Work on a different problem and come back to the difficult one later.

Philadelphia, PA, USA   Sylvia Forman
Philadelphia, PA, USA   Agnes M. Rash

Acknowledgments

Contents

Chapter 1
Introduction

*The single biggest problem in communication is the illusion
that it has taken place.*

—George Bernard Shaw, 1856–1950

1.1 Communication in Mathematics

In order to share information with one another, we must be able to clearly and
accurately communicate our thoughts and ideas. In the era of text messaging and
cryptic notes, the art of understanding a communication has changed. Many
parents and grandparents may be unable to understand a text message sent by
you or one of your friends. In mathematics, precise language is important so that
everyone can understand each other. This section introduces the meaning of
precise mathematical language and what is included in a good explanation in
mathematics.

Definitions are used to ensure that everyone is discussing the same concept.
Ill-defined words lead to confusion. For instance, the meaning of the word
terrific can be different in different contexts. In some sentences it means
something terrible (a terrific storm), and at other times it means something
wonderful (a terrific vacation). Words that have opposing meanings and depend
on context can create problems in interpretation. Mathematicians try to be
consistent and precise with the language that is used to describe objects and
concepts.

Think about a familiar term, such as an *even number*. Given some numbers, you
could probably identify which ones are even, and you can probably come up with a
test to determine whether or not a given number is even. There are different ways to
describe an even number, but the definition must make it clear what is an even
number and what is not. All even numbers must satisfy the definition and any

number that is not even cannot satisfy the definition. Part of this course will be learning precise definitions for mathematical concepts, some of which will be familiar, and some of which may be new.

The following list summarizes what makes a good explanation in mathematics.

Characteristics of Good Explanations in Mathematics
1. The explanation addresses the specific question or problem that was posed.
2. Each step is factually correct and clearly follows from the previous step(s) or prepares for the subsequent steps.
3. The explanation could be used to teach another person, possibly even one who is not in the class.
4. Key points are emphasized.
5. If applicable, supporting pictures, diagrams, examples, or equations are used appropriately and as needed to clarify a concept.

1.2 Problem Solving Strategies

Problem solving is central to all areas of endeavor. When learning something new for fun, whether it is a winning strategy for a game of cards or a new sport, you need a plan of action. You may need to solve a monetary problem, such as financing a college education or getting a mortgage to purchase a house. Each of these requires a strategy. Even determining how much sleep you need to feel your best, or determining if you can stop your vehicle (as the traffic light is turning red) before you get to a crosswalk, requires thought.

In mathematics, problem solving is essential, and therefore developing techniques to approach different problems is helpful. Looking at alternative strategies and selecting what seems to be the best one is a useful approach. One of the most famous problem-solving strategies was proposed by the mathematician George Polya in his classic book *How to Solve It*. The four-step strategy works for many types of problems. Here are his suggestions:

1. Understand the problem.
2. Devise a plan.
3. Carry out the plan.
4. Look back.

We will elaborate on Polya's strategy and add some helpful information.

1. Understand the problem:

   Do you understand all of the words and their definitions?
   Can you restate the problem in your own words?
   Do you know what the goal is? What are you asked to find out or show?

Can you work out some numerical examples (special cases) that would help
  make the problem clearer?
Is this problem similar to another problem that you have solved?

2. Devise a plan (there are many strategies that can be useful. Below is a partial
   list):

Make a table of information.
Guess and check, and then generalize from the examples.
Modify the problem or solve a simpler problem first.
Search for a pattern.
Work backwards.
Divide into cases.
Consider extreme cases.

3. Carry out the plan:

Carrying out the plan is usually easier than devising the plan, because you are
  actually using the method you have already thought of to solve the problem.
  Do not let yourself get discouraged if the first strategy you tried is not
  working; be persistent and try a different one. Take a break when you need
  to! A fresh start or new strategy can lead to success if you are still having
  difficulty.

4. Check your results:

Is your solution reasonable?
Can you check to see if your solution is correct?
Did you answer the question?
Is there an easier solution? Could you have done this problem another way?

Let us look at several examples.

Example 1.1 What are the possibilities for the missing digit so that the number
below is divisible by 3?

$$341725\_\_$$

Solution:
We will use Polya's strategy for solving this problem.

Step 1   Understand the problem.
We are asked to fill in the blank with a digit, which could be any of the values 0, 1,
2, 3, 4, 5, 6, 7, 8, or 9. Then, determine which of these digits produces a number
divisible by 3.

Step 2   Devise a plan.
There are 10 possible numbers to test in this problem, since there are 10 different
digits that could be filled in for the missing digit. We can make a list of them and
then divide each one by 3 to see which is a multiple of 3 and which is not.

Step 3 Carry out the plan.

The numbers we must check are listed below.

3417250	3417255
3417251	3417256
3417252	3417257
3417253	3417258
3417254	3417259

For instance, $341720/3 = 113906.666\ldots$, so 341720 is not divisible by 3. The next table shows the results of dividing by 3.

	Divisible by 3?		Divisible by 3?
3417250	N	3417255	Y
3417251	N	3417256	N
3417252	Y	3417257	N
3417253	N	3417258	Y
3417254	N	3417259	N

Looking at the table, you can see that the last digit could be 2, 5, or 8.

Step 4 Check your results.

Make sure that your arithmetic is correct. Then, when the problem is finished, and the answer has been given, look at the table to see if you can find any additional information. For example, it appears that when one number worked, every third number after this also worked.

◈

Example 1.2 Sophie has pennies, nickels, and dimes in her purse, at least four of each, and she pulls out four coins. What would be the different totals that Sophie could get?

Solution:

This is another example of a problem where listing all the possible values could be helpful in finding a solution. We will make a table of the possibilities.

Pennies	Nickels	Dimes	Total
4	0	0	4¢
3	1	0	8¢
3	0	1	13¢
2	2	0	12¢
2	0	2	22¢
2	1	1	17¢

(continued)

(continued)

Pennies	Nickels	Dimes	Total
1	3	0	16¢
1	0	3	31¢
1	1	2	26¢
1	2	1	21¢
0	4	0	20¢
0	0	4	40¢
0	3	1	25¢
0	1	3	35¢
0	2	2	30¢

From the last column, the possibilities for the total amount of money Sophie pulled out are 4¢, 8¢, 13¢, 12¢, 22¢, 17¢, 16¢, 31¢, 26¢, 21¢, 20¢, 40¢, 25¢, 35¢, and 30¢.

◈

Example 1.3 Without using a calculator, show that the square root of 4356 is an integer.

Solution:
First, square a few numbers to see if you can discover a pattern.

For example, $70^2 = 4900$, which is larger than 4356, but $60^2 = 3600$, which is smaller. Therefore, $\sqrt{4356}$ is between 60 and 70. At this point, we could just check each number between 60 and 70, but we can save some time by noticing that since the last digit of 4356 is a 6, the square of the units' digit of $\sqrt{4356}$ must be 6.

The units' digit can be 0, 1, 2, ..., 8, or 9. So, construct a table of the units' digits and their squares, as shown in Table 1.1.

Table 1.1 Squares of units digits

a	a^2
0	0
1	1
2	4
3	9
4	6
5	5
6	6
7	9
8	4
9	1

Only the numbers 4 and 6 have a square that ends in a 6. Therefore, testing 64 and 66, we find that $64^2 = 4096$ is too small, but $66^2 = 4356$. Thus, $\sqrt{4356} = 66$.

◈

Exercise Set 1.2

1. List the 3-digit numbers that can be written using each of 1, 3, and 5 once and only once. Which strategy did you use?
2. List the 4-digit numbers than can be written using each of the digits 2, 3, 4, and 6 once and only once. Which strategy did you use?
3. Four friends ran a race:

   - Carl finished 7 s ahead of Bernhard.
   - Niels finished 3 s behind Leonard.
   - Bernhard finished 5 s behind Niels.

   In what order did the friends finish the race?

Exercises 4–9. Without a calculator, determine what integer is the square root of each number.
4. 484
5. 8464
6. 2116
7. 676
8. 3249
9. 5041

10. Julia, Jay, and Pierre go out to eat. The total bill is $45, including the tip. They decide to split the bill evenly, so each person owes $15. Jay wants to put the total on a credit card and get cash or checks from the others. Pierre has only one check, three $1 bills, and a $5 bill. Julia has only a $10 bill and a $20 bill. Explain how the three can settle among themselves so that the waiter has to take only Jay's credit card for the total amount (and so that no one owes anything). Explain your reasoning.
11. Stacey had 32 coins in a jar. Some of the coins were nickels; the others were dimes. The total value of the coins was $2.80. Find out how many of each coin there were in the jar. What problem-solving strategy did you use?
12. The houses on Main Street are numbered consecutively from 1 to 150. How many house numbers contain at least one digit "7"?
13. The houses on Market Street are numbered consecutively from 1 to 150. How many house numbers contain at least one digit "4"?
14. Continue these numerical sequences by filling in the next three numbers in the pattern.

    (a) 1, 4, 7, 10, 13, _____, _____, _____
    (b) 19, 20, 22, 25, 29, _____, _____, _____
    (c) 2, 6, 18, 54, _____, _____, _____

15. In order to save the world, MacGyver must time exactly 3 min. All he was able to find in the kitchen of the evil genius planning to destroy the earth were two egg timers: one timer can time an interval of exactly 4 min, and the other can

time an interval of exactly 7 min. How can he use these two egg timers to time an interval of exactly 3 min?

16. There are two species of cicadas: one emerges every 13 years and the other every 17 years. Suppose both emerged in 2010.

    (a) When is the next time that both species emerge?
    (b) If the cicadas have a common predator that emerges every 2 years, and also emerged in 2010, when is the next time that all three emerge in the same year?

17. A professor buys a new car every 3 years; he bought his first one in 1981. He gets a sabbatical leave every 7 years, starting in 1992. When will he first get both?

18. Pierre and John are playing drums together, making a steady beat. Pierre beats his drum hard on beats that are multiples of 8. John beats his drum hard on beats that are multiples of 12. Find the first 4 beats on which both Pierre and John will beat their drums hard together. Explain.

Activities

1. Solving Sudoku puzzles is an exercise in logical and deductive reasoning. In Sudoku, a 9×9 grid is filled in with the numbers $1, 2, \ldots, 9$ such that no number appears more than once in any row, column, or 3-by-3 submatrix. These puzzles appear in newspapers, on the Internet, and in puzzle books. Find an easy Sudoku puzzle and solve the puzzle. Then,

    (a) Write an explanation of the strategy that you used to solve the puzzle.
    (b) Describe your strategy to a fellow student. If the person can solve the puzzle using your strategy, then your explanation was clear. If not, modify your explanation and try again.

2. Copy the figure below and place the digits 1, 2, 3, 4, and 5 in these circles so that the sums across (horizontally) and down (vertically) are the same. Is there more than one solution?
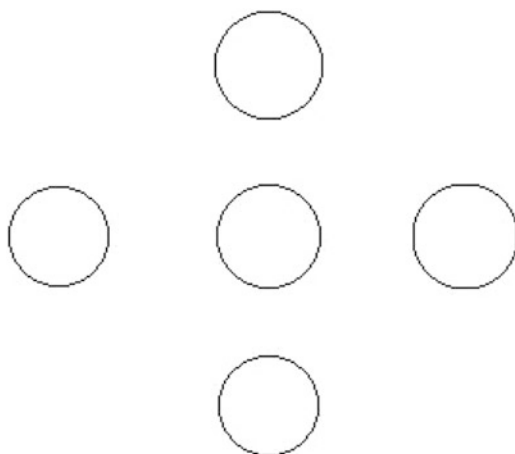
Chapter 2
Conjectures, Proofs, and Counterexamples

*Before we take to sea we walk on land. Before we create
we must understand.*

—Joseph-Louis Lagrange, 1736–1813

2.1   What Is Number Theory?

The collection of ***integers*** is defined to be the set of numbers

$$\{\ldots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots\}$$

where the dots indicate that the pattern continues indefinitely in each direction. The integers are also sometimes called the ***whole numbers***.[1] We will use these terms interchangeably.

To get the next integer to the right in the list above, add 1 to the previous number. To find the next integer on the left, subtract 1 from the preceding number. As you can see, the list of integers goes on forever in both the positive and negative directions. In other words, there is an infinite number of integers.

Mathematicians use symbols to represent ideas and concepts. For example, the letters a, b, m, and n usually represent integers. The symbol $\mathbb{Z}$ is used to represent the entire set of integers, so we can write

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

---

[1] The term *whole numbers* does not have a standard definition. It is sometimes used to represent the positive integers $(1,\ 2, \ldots)$, sometimes the non-negative integers $(0,\ 1,\ 2, \ldots)$ and sometimes the entire collection of integers. We will use *whole number* interchangeably with *integer* to emphasize that we are not including fractions.

Having defined the set of integers, we can consider what is in the set and what is not. For example, 81 is in the set $\mathbb{Z}$ of integers, but $\frac{2}{3}$ is not. The symbol $\in$ is used to mean "is in the set" or "is a member of." For example, $81 \in \mathbb{Z}$. To say that $\frac{2}{3}$ is not in the integers, we draw a line through the $\in$ symbol and write $\frac{2}{3} \notin \mathbb{Z}$.

Number theory is the study of the integers. Since the time of the ancient Greeks, over 2,000 years ago, people have been interested in properties of the integers and relationships between them. For a long time, number theory was thought of as an interesting field because it contains so many interesting problems that are very simple to state but incredibly difficult to solve; however, it was not believed to have much practical use. In fact, the American mathematician Leonard Dickson (1874–1954) who wrote a book called *History of the Theory of Numbers* once said, "Thank God that Number Theory is unsullied by any application." However, this view has changed since the advent of computers. In 1974, computer scientist Donald Knuth (1938–) said, "Virtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations." In addition to being important to basic computer design, scientists have found many modern applications for number theory, one of the most studied being cryptology.

As was discussed in Section 1.1, clear definitions are extremely important in mathematics. In Section 2.4, some formal mathematical definitions will be introduced. Many of the terms we work with in number theory are familiar since you have been working with the integers for most of your life. We will start by reviewing the concepts of *even*, *odd*, *divisible*, and *prime*. For now, the goal is to make sure you have a strong understanding of these concepts.

One of the most basic classifications of the integers is even or odd. What exactly do we mean by an even integer? You can probably list a few even numbers without referring to a definition and without any difficulty.

When first introducing evens and odds, however, one question that always comes up is, "What about zero? Is it even or odd?" Having precise definitions allows us to answer this question: If zero fits the definition for even, then it is even. If zero fits the definition for odd, then it is odd. If zero fits neither definition, then it is neither even nor odd.

There are different ways to describe an even number. One possibility is an even number is always equal to a whole number plus itself. Another possibility: an even number is divisible by 2. Can you think of others?

Example 2.1 Is the integer 0 even?

Solution
Using the characterizations of even stated before this example, we can confirm that zero is even, since $0 + 0 = 0$, or since $0 \div 2 = 0$.

◈

There are also different ways to describe odd integers. For example, one could say that an odd integer has to be an even integer plus one. Alternatively, odd integers are integers that are not divisible by 2. Can you think of any other ways to describe odd integers?

Example 2.2 Can odd numbers be negative?

Solution
Yes, using the description above, odd numbers can be negative since there are negative numbers which are not divisible by 2. For example, -7 and -81 are both odd.

◈

The idea of *divisible* is important for establishing relationships between integers, and even if you cannot state a definition for it right now, it is likely to be familiar. If you were asked whether 80 is divisible by 5, you would be able to answer correctly (nod head yes). If you were asked if 80 is divisible by 7, you would be able to answer correctly again (shake head no). Now, try to describe this property for each example: 80 is divisible by 5 because $\frac{80}{5}$ is an integer. Or, another way to say this is that 80 is divisible by 5 because $5 \times 16 = 80$ and 16 is an integer. Using the same idea, 80 is not divisible by 7 because $\frac{80}{7}$ is not an integer or because $7 \times \frac{80}{7} = 80$, and $\frac{80}{7}$ is not an integer.

Finally, let us discuss the concept of *prime* for integers. A prime number is often described as an integer that is only divisible by 1 and itself. While most people interpret this to mean that some examples of primes are 5, 7, 11, and 31, these numbers do not technically satisfy the description of primes given above. For example, the number 5 is divisible by 1 and itself, but 5 is also divisible by -5, since $-5 \cdot -1 = 5$ and -1 is an integer. To fix this problem, we can rewrite the statement to say that the only *positive* integers a prime number is divisible by are 1 and itself. In addition, negative numbers are not considered prime, even if their positive counterpart is prime. And, what about the number 1? It is only divisible by the positive values of 1 and itself, since 1 is itself; however, the integer 1 is not considered prime. Therefore, the formal definition of prime in Section 2.4 must make it clear that negative integers and the number 1 are not included as primes.

2.1.1 Unsolved Questions in Number Theory

We will close with some unsolved questions in number theory. Many fields of mathematics require a significant amount of background and terminology to understand the unsolved questions in the field. Since number theory is the study of the already familiar integers, you can understand many of the unsolved problems of number theory on the first day of the course. Finding solutions to these questions is another matter, but we will return to some of these questions throughout this book.

1. Are there infinitely many twin primes? Many pairs of primes differ by 2. For example, 3, 5; 5, 7; 11, 13; 17, 19. These pairs of primes are called **twin primes**. The Twin Prime Conjecture states that there are infinitely many such pairs, but so far no one has been able to prove it.
2. Are there infinitely many primes that can be expressed as $2^n + 1$? For example, $5 = 2^2 + 1$ and $17 = 2^4 + 1$.

3. Are there infinitely many primes that can be expressed as $2^n - 1$? For example, $3 = 2^2 - 1$, $7 = 2^3 - 1$. (These are called **Mersenne primes**.)

4. Are there infinitely many perfect numbers? A **perfect number** is an integer whose divisors other than the number itself add up to the number. For example, the divisors of 6 (other than 6 itself) are 1, 2, and 3. Adding these, we see that $1 + 2 + 3 = 6$. Similarly, the divisors of 28 (other than 28) are 1, 2, 4, 7, and 14. Adding, $1 + 2 + 4 + 7 + 14 = 28$.

5. Are there any odd perfect numbers?

6. Is Goldbach's conjecture true? **Goldbach's conjecture**: Every even integer greater than 2 can be written as the sum of two primes. For example: $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, and $10 = 5 + 5$. This famous conjecture, proposed by Russian mathematician Christian Goldbach (1690–1764), has been tested for very large numbers, and has been true for all of them, but no one has been able to prove it is always true, despite a \$1,000,000 prize and a novel about the topic.[2]

Exercise Set 2.1

Exercises 1–4. Give an example of a number that fits the description of the term given in this section and one that does not fit the description. Explain your answer.

1. even
2. odd
3. divisible by 8
4. prime

Exercises 5–8. Translate the statement given in symbols into words.

5. $14 \in \mathbb{Z}$
6. $-7 \in \mathbb{Z}$
7. $\frac{4}{3} \notin \mathbb{Z}$
8. $0 \in \mathbb{Z}$

Exercises 9–12. Rewrite the statement in symbols.

9. 81 is an integer.
10. 3.14 is not an integer.
11. $\frac{2}{5}$ is not an integer.
12. -21 is an integer.

Exercises 13–18. There have been many attempts to find a formula that will generate only prime numbers, or at least infinitely many prime numbers. (See 2 and 3 in the list of unsolved questions in number theory.) For each expression, evaluate the expression, and then determine whether or not it is prime. Explain the method you use.

---

[2] The novel is called *Uncle Petros and Goldbach's Conjecture: A Novel of Mathematical Obsession* by Apostolos Doxiadis.

13. $2^6 - 1$
14. $2^6 + 1$
15. $2^7 - 1$
16. $2^7 + 1$
17. $2^9 - 1$
18. $2^9 + 1$

19. Determine whether or not 128 is a perfect number.
20. Determine whether or not 24 is a perfect number.
21. Find three examples of twin primes not already given in this section.
22. *Cousin primes* are primes that differ by 4. Find two pairs of cousin primes.
23. Show that Goldbach's conjecture is true for 20.
24. Show that Goldbach's conjecture is true for 32.

2.2 Inductive and Deductive Reasoning

Inductive and deductive reasoning are important mathematical tools, but they can also be used to make everyday decisions. For example, suppose that your professor has been five minutes late to class for each of the last three classes. You may conclude that you have time to stand in line for your coffee because she will be five minutes late again today. As another example, suppose you are applying for a public library card and must verify your address. You could provide a photo ID and an electric bill or a copy of your apartment lease to the librarian to confirm that you reside in the city limits.

Notice that the conclusions in each example above–that the professor will be late again and that you do live in the city limit–are not of the same type. In the first case, even if it is true that the professor was late for three classes in a row, it does not guarantee that she will be late again. The conclusion may be true, or she may be on time today. In the second case, however, assuming that the information you presented to the librarian was true, his conclusion is also true. You have verified that you do live in the city. This difference comes from the type of reasoning that was used to come to each conclusion.

In the first case, the conclusion was based on examples or past observations. Since the professor had a record of coming to class late, the student concluded that she would continue to be late. Each additional observation or example of a time the professor is late gives additional support to the claim that she will always be 5 min late, but even if she is late every single class up to the last day, it is still possible she will arrive at the last class on time. This type of reasoning, where conclusions are made by generalizing observations, is called **inductive reasoning**. Inductive reasoning is used whenever you make observations and use them to formulate a hypothesis or **conjecture**, a statement that you believe to be true. However, since inductive reasoning is based on specific examples, it will never result in a proof.

More examples provide more evidence, but they cannot prove that a general statement such as "This professor is always 5 min late" is true.

> ***Inductive reasoning*** is used when one observes specific examples, identifies patterns, and then formulates a conjecture based on these observations. Inductive reasoning generalizes from specific examples to a general statement.The goal of inductive reasoning is to develop a new conjecture or test an existing conjecture. Inductive reasoning can provide support for a conjecture, but it cannot be used to prove the conjecture is true.

In the case of the library card, information was presented to the librarian that allowed him to conclude definitively that you live in the city. The photo ID and the apartment lease taken together convinced the librarian of your residency. This is an example of ***deductive reasoning***. Deductive reasoning does not generalize specific examples. Instead, a deductive reasoning process begins with known facts and connects them using logic to reach a conclusion. The most important difference between inductive and deductive reasoning is that the conclusion of a deductive argument is guaranteed to be true, as long as the ***premises***, or the initial pieces of information used in the argument, are true. If a deductive argument begins with a false premise, such as $2+2=5$, then correctly applying a rule of algebra by adding 1 to both sides of the equation produces the equation $5=6$. This is false, but the reason is because the premise that $2+2=5$ is false, and not because the reasoning is incorrect.

> ***Deductive reasoning*** begins with known facts and uses logic to reach a conclusion. The goal of deductive reasoning is to prove that a statement is true. The conclusion of a deductive argument is guaranteed to be true as long as the initial information is also true.

In mathematics, statements that have been proven true are often called ***theorems***. Both of these types of reasoning are very useful. It is important to know the difference between these two types of reasoning, since each has a different purpose and leads to a different type of conclusion. Inductive reasoning is used to test statements to decide what might be true and what statements you might want to prove. Even if all examples support the truth of the statement, though, it still could be false in some case not yet tested. If the statement is indeed true, deductive reasoning is the tool used to prove it.

Example 2.3 Determine whether each example illustrates inductive reasoning or deductive reasoning:

(a)   Sarah concludes her grade for the semester will be a B, because her grades on the first two quizzes were Bs.
(b)   At the end of the semester, Julia averages her quiz grades and finds that her quiz average is an A-.

(c)   Scientists have learned a lot by studying Mars, so they will also learn a lot by studying Neptune.
(d)   Birds are dinosaurs and dinosaurs are reptiles, so birds must be reptiles.

Solution
(a)   This is an example of inductive reasoning, because Sarah generalized the examples of her grades on two quizzes to her grade for the semester.
(b)   This is deductive reasoning, since Julia used the formula for computing an average and the grading scale for the class to find her quiz average.
(c)   Since this argument generalizes from the example of Mars to another planet, this is inductive reasoning.
(d)   This is a deductive argument, starting with the premises that birds are dinosaurs and dinosaurs are reptiles. As for whether or not the premises and conclusion are true, you may need to consult your local paleontologist.

◈

Inductive reasoning is used to make new conjectures, as well as test existing conjectures. Examples 2.4 and 2.5 illustrate this.

Example 2.4 Test the following conjecture: All primes are odd.

Solution
One common application of inductive reasoning is to test conjectures by looking at examples to see if the conjecture is supported. For example, 3, 5, 7, and 11 are all prime and they are all odd. There are many more examples that support this statement such as 13, 17, 19, 23, 29, and 31. However, no number of examples that support this statement can prove that it is true. In fact, the conjecture is false because 2 is an even number and 2 is a prime.

◈

Notice that while testing examples cannot prove a general statement is true, Example 2.4 shows that an example can be used to prove it is false. This idea is more carefully discussed in Section 2.7.

Example 2.5 Make a conjecture about the result of adding two even numbers.

Solution
One way to formulate a conjecture is to try some examples and look for patterns. Choose some pairs of even integers:

$$6 + 4 = 10$$
$$0 + 8 = 8$$
$$-6 + 4 = -2$$
$$2 + 12 = 14$$

Notice that in every case, the sum of the two even integers was itself an even integer. These examples do not prove that this will always be the case, but they allow us to make a conjecture that we can then try to prove.

◈

Since the purpose in using deductive reasoning is to prove statements, we should establish exactly what is meant by a proof.

> **Definition 2.1: proof**
> A *proof* uses deductive reasoning and logic to connect a sequence of statements, definitions, and theorems to verify that a particular conclusion is true. The goal of a proof is to provide a clear and convincing argument that the conclusion is true.

In the next three sections, we will look carefully at all these components of a proof. In Section 2.3, we will examine statements and explain when different types of statements are true or false. In Section 2.4, some basic definitions related to the integers are introduced. Finally, in Section 2.5, these components are combined with rules of logic to write mathematical proofs.

> **Exercise Set 2.2**

Exercises 1–7. Determine which of the following situations involve inductive reasoning and which involve deductive reasoning.

1. It has rained for four of the last 5 days. Today is sunny, so I expect it to rain for the next few days.
2. Your low fuel light came on in your car. The last time this happened, you were able to drive for two more days without running out of gas, so this time you will be able to as well.
3. Your low fuel light came on in your car, so you get out the manual to see how many gallons of gas are left in the tank.
4. Robin has calculated the amount of money he earned over the summer and is now calculating whether any additional income tax will have to be paid over what was taken as a payroll deduction.
5. When budgeting for next month, Julia assumes the deductions from her paycheck will be the same as they were in the previous month.
6. The stock market has been going down for most of the past month. However, you have observed that the market rarely goes down 2 months in a row. So, you plan to invest some money in the market at the beginning of next month.
7. George liked the first three books by his favorite author, so he is ordering an advance copy of her latest book since he is sure to like it.

8. Consider the following conjecture:
   CONJECTURE: The sum of the squares of two odd integers cannot be a perfect square:

   (a) Test the conjecture on at least four examples, and use these examples to make a conclusion about whether the conjecture is true or false.

    (b)   What type of reasoning did you use to make the conclusion in part (a)?

    (c)   Is your conclusion in part (a) still a conjecture, or is it a theorem?

9. Add the pairs of numbers: $2 + 4$, $6 + 8$, $14 + - 10$, $2 + - 2$.

    (a)   Do you see a pattern in the numbers that were given? (Hint: Think about whether they are odd or even.)

    (b)   Do you notice a pattern in the sums?

    (c)   Make a conjecture about what you observed when these pairs of numbers are added.

10. Add the pairs of numbers: $7 + - 9$, $3 + - 11$, $9 + - 3$, $- 27 + 27$.

    (a)   Do you see a pattern in the numbers that were given? (Hint: Think about whether they are odd or even.)

    (b)   Do you notice a pattern in the sums?

    (c)   Make a conjecture about what you observed when these pairs of numbers are added.

11. Add the pairs of numbers: $6 + 3$, $9 + 4$, $16 + - 5$, $5 + - 10$, $58 + 21$.

    (a)   Do you see a pattern in the numbers that were given?

    (b)   Do you notice a pattern in the sums?

    (c)   Make a conjecture about what you observed when these pairs of numbers are added.

12. Use Exercises 9–11 to formulate a conjecture that covers all three cases. Create several new examples to test your conjecture and see if it is true in these new examples.

13. Multiply the pairs: 2×3, 5×8, 11×10, 124×9.

    (a)   Do you see a pattern in the numbers that were given?

    (b)   Do you notice a pattern in the products?

    (c)   Make a conjecture about what you observed when these pairs of numbers are multiplied.

14. Multiply at least three pairs of odd integers and make a conjecture about the product of two odd integers.

15. Multiply at least three pairs of even integers together and make a conjecture about the product of two even integers.

16. Use Exercises 13–15 to formulate a conjecture that covers all three cases. Create several new examples to test your conjecture and see if it is true in these new examples.

17. Multiply at least three sets of *three* odd integers and make a conjecture about the product of three odd integers.

18. Multiply at least three sets of *four* odd integers and make a conjecture about the product of four odd integers.

Exercises 19–21. Find a pattern in the sequences of integers, and make a conjecture about the next three integers in the sequence.

19. 1, 2, 3, 4, 5, ___, ___, ___, . . .
20. 2, 5, 9, ___, ___, ___, . . .
21. 1, 1, 2, 3, 5, 8, ___, ___, ___, . . .

22. Find all examples of inductive or deductive reasoning in the passage below from Induction and Analogy in Mathematics Volume 1 of Plausible Reasoning by George Polya (page 11–Chap. 1: Induction). In each case, determine whether the conclusion made matches the type of reasoning used.

   The Logician, the Mathematician, the Physicist, and the Engineer

   "Look at this mathematician," said the logician. "He observes that the first ninety-nine numbers are less than [a] hundred and infers hence, by what he calls induction, that all numbers are less than a hundred."

   "A physicist believes," said the mathematician, "that 60 is divisible by all numbers. He observes that 60 is divisible by 1, 2, 3, 4, 5, and 6. He examines a few more cases, as 10, 20, and 30, taken at random as he says. Since 60 is divisible also by these, he considers the experimental evidence sufficient."

   "Yes, but look at the engineers," said the physicist. "An engineer suspected that all odd numbers are prime numbers. At any rate, 1 can be considered as a prime number, he argued. Then there comes 3, 5, and 7, all indubitably primes. Then there comes 9; an awkward case, it does not seem to be a prime number. Yet 11 and 13 are certainly primes. 'Coming back to 9,' he said, 'I conclude that 9 must be an experimental error.'"

2.3   Statements and Connectives

An important part of mathematics is determining whether or not something is true. In mathematics, the word *statement* means a declarative sentence that is either true or false. Sentences or exclamations like "Really?," "Okay," or "Are you going to study math today?" do not qualify as statements.

There are both simple statements as well as compound statements, and our goal will be to understand exactly when each type of statement is true and when it is false. This is called the *truth value* of the statement. Since both the initial information in a proof as well as the conclusion to be shown are made up of statements, it is important to understand exactly what they mean.

A simple statement is the simplest declarative sentence. Some examples are:

Triangles have three sides.
Nine is a prime number.
Leonhard goes to the library to study every day.

The truth value of these simple statements is easy to determine provided you have the necessary information, such as the definition of a triangle or Leonhard's schedule. Compound statements are formed by joining simple statements with a connective word such as "and" or "or." There are many possible connectives in the English language, but all of them can be expressed in terms of the following five:

not
and
or
if...then...
...if and only if...

For this reason, these are the five connectives usually studied in logic, and these are the five used in this textbook.

We are especially interested in general statements, such as "The sum of any two even integers is even," or "Adding the same number to both sides of a true equation will produce a true equation." Our goal is to be able to prove such statements are either true or false.

When discussing their general properties, statements are usually represented with letters, such as p, q, or r. This allows us to easily represent different statements. If, for example, p represents the statement "Nine is a prime number" (which is false) and q represents the statement "Triangles have three sides" (which is true), we would show this assignment by:

p: Nine is a prime number.
q: Triangles have three sides.

Then we can apply connectives such as *not p*, *p and q*, and *if p, then q* to indicate different ways of combining these statements into compound statements.

2.3.1   Negations

The first connective on the list, "not," is the only one that does not link statements together.[3] The connective "not" is used to form the **negation** of a statement. The negation of a statement is a new statement that has the opposite truth value. For example, the negation of the statement "The integer a is even" is "The integer a is not even" or "The integer a is odd."

---

[3] Sometimes, the connective "not" is called a *unary connective* since it is applied to a single statement, rather than to connect two or more statements.

> **Definition 2.2: negation, ~ *p***
> The ***negation*** of a statement *p* is a statement with the opposite truth value of *p*.
> If *p* is true, then the negation is false, and if *p* is false, then the negation is true.
> The negation of *p* is written as *not p*, or in symbols as ~ *p*.

The negation of any statement can be formed by adding "It is not true that. . ." to the beginning of the sentence. So, for a statement *p*, the negation can be expressed as "It is not true that *p*." This is often awkward-sounding and difficult to use, but expressing the sentence this way first can be helpful in figuring out the correct negation for the statement.

Example 2.6 Write the negation of each simple statement in symbols and words, and determine whether the negation is true or false:

(a)   *t*: Triangles have three sides.
(b)   *n*: Nine is a prime number.
(c)   *w*: There are not 8 days in a week.
(d)   *s*: The sum of two even numbers is even.

Solution
(a)   ~ *t* Triangles *do not* have three sides.
      False (notice that the original statement was true).
(b)   ~ *n* Nine is *not* a prime number.
      True (notice that the original statement was false).
(c)   ~ *w* There are 8 days in a week.
      False (notice that the original was true).
(d)   ~ *s* The sum of two even numbers is not even.
      False (You may have convinced yourself that the original statement is true in Exercise 9 of Section 2.2, and we will prove this fact in Section 2.5.)

◈

Now, let us consider some examples of more complicated statements. When statements have quantifiers like *many*, *some*, or *all*, forming the negation is slightly more complicated.

Example 2.7 Determine which choice is the correct negation of the given statement and explain why.

Statement
Some people like math.

Possible Negations
(a)   All people like math.
(b)   Some people do not like math.
(c)   No people like math.

Solution

The negation of the statement "Some people like math" must have the opposite truth value. So, assuming that this original statement is true, the correct negation must always be false. Similarly, if the original statement is false, then the negation must be true. Keeping this in mind, we will examine the choices.

Choice (a) does not form the negation of the given statement. If it is true that all people like math, then there are definitely some who like math, so these statements do not have opposite truth values—they can both be true at the same time.

Choice (b) is appealing, but examining it closely shows that it does not form the negation of the given statement either. To see this, notice that if it is true that some people do not like math, it could still be true that there are some different people who do. Therefore, these two statements do not have opposite truth values.

This leaves Choice (c), which is the correct negation. To make the original statement "Some people do like math" false, there must be no people who like math. Therefore, the correct negation is "No people like math" or "All people do not like math," a sad state of affairs if it were true.

Therefore, the negation of a statement of the form **SOME *a* are *b*** is **It is not true that SOME *a* are *b***, which can also be expressed as **NO *a* are *b***.

◈

Example 2.8 Find the negation of the statement: "All apples are red."

Solution

One way to think about the negation is to think about what is necessary to make the statement false. If it is not true that all apples are red, then there would have to be an apple of another color. Therefore, the negation of "All apples are red" is "Some apples are not red."

The negation of a statement of the form **ALL *a* are *b*** is **It is not true that ALL *a* are *b***, which can be expressed as **SOME *a* are not *b*** or **AT LEAST ONE *a* is not *b***.

◈

Notice that for the statement "All apples are red" to be false, only one example of a non-red apple is needed (such as a green Granny Smith). This idea will be important in Section 2.7, which discusses how to prove that a statement is false.

Example 2.9 Find the negation of the following statement and determine the truth values of the statement and its negation:

All polygons are regular polygons.

Solution

To form the negation of this statement, first form the sentence, "It is not true that all polygons are regular polygons." This can be expressed more clearly by saying "Some polygons are not regular polygons."

To determine the truth values, remember that a polygon is just a closed shape with straight sides, and a regular polygon has sides of all the same length and angles of all

the same measure. The original statement is then false because there are examples of polygons such as rectangles or right triangles which are not regular polygons. This also shows the statement "Some polygons are not regular polygons" is true.

◈

2.3.2   Conjunctions

The next type of compound statement is a **_conjunction_**. A conjunction is formed by joining two (or more) statements with the connective "and." So, if p and q are statements, then the statement p _and_ q is a conjunction, also called an "and statement." The symbol $\wedge$ is used to represent the word "and."

Definition 2.3: conjunction, $p \wedge q$

The **_conjunction_** of two statements p and q is the statement p _and_ q, or in symbols $p \wedge q$. A conjunction or _and statement_ is true when both parts of the statement are true. Therefore, $p \wedge q$ is true when p is true and q is true. The statement $p \wedge q$ is false when either one of p or q is false.

Example 2.10 For each statement below, use the simple statements to convert symbols into words or words into symbols. Then determine whether each statement is true or false.

Simple statements:

p: Four is an even number. r: There are 12 months in a year.
q: Six is an odd number. s: A triangle has four sides.

(a)   Four is an even number and there are 12 months in a year.
(b)   Four is an even number and six is an odd number.
(c)   A triangle has four sides and six is not an odd number.
(d) $\sim s \wedge q$

Solution
(a)   In symbols, this statement is $p \wedge r$. Since both p and r are true, the conjunction $p \wedge r$ is also true.
(b)   In symbols, this statement is $p \wedge q$. Since q is a false statement, the conjunction $p \wedge q$ is false, even though p is true.
(c)   In symbols, this statement is $s \wedge \sim q$. Since s is a false statement, the conjunction is also false, even though $\sim q$ (six is not an odd number) is true.
(d)   In words, the statement $\sim s \wedge q$ is "A triangle does not have four sides and six is an odd number." This conjunction is false since six is even, not odd.

◈

We can also find negations of compound statements. The negation of a statement of the form $p \wedge q$ is a statement that is false when $p \wedge q$ is true. A conjunction is false

when *either* of the statements it contains is false. Therefore, the negation of "*p and q*" is "not *p or* not *q*."

Example 2.11 Write the negation of the statement "It is raining and I forgot my umbrella."

Solution
The negation of this statement is "It is not raining or I did not forget my umbrella."

◈

2.3.3   Disjunctions

A compound statement formed by joining two (or more) statements with the connective "or" is called a ***disjunction***. If *p* and *q* are statements, then the statement *p or q* is a disjunction, or an "or statement." The symbol $\vee$ is used to represent the connective "or."

> **Definition 2.4: disjunction, $p \vee q$**
> The ***disjunction*** of two statements *p* and *q* is the statement *p or q*, or $p \vee q$. The statement $p \vee q$ is true when either *p* is true, *q* is true, or both *p* and *q* are true. The only time the statement $p \vee q$ is false is if both *p* and *q* are false.

Sometimes an *or* statement can specify that both options cannot be true. This is called the ***exclusive or*** in logic. For example, with the *exclusive or*, the statement "You can have a cookie or a piece of cake" would mean that you can have one or the other, but not both. We will not use the exclusive or, so any statement of the form $p \vee q$ will be true when both *p* and *q* are true. If only one option is allowed, that will be indicated in the sentence, such as "You can do your homework or watch TV, but not both."

Example 2.12 Use the simple statements given below to write the compound statements in symbols, and then determine whether each compound statement is true or false.

Simple statements:
p: A square has five sides.	*r*: Three is a prime number.
q: A platypus is a mammal.	*s*: Nine is an even number.

Compound statements:
(a)   Three is a prime number or a platypus is a mammal.
(b)   A square has five sides or three is a prime number.
(c)   Nine is an even number or a square has five sides.
(d)   Nine is an even number or three is not a prime number.

Solution
(a) In symbols, this statement is $r \vee q$, which is true since three is prime and a platypus is one of the rare cases of an egg-laying mammal.
(b) In symbols, this statement is $p \vee r$, which is also true since even though p is false, r is true.
(c) In symbols, this statement is $s \vee p$, which is a false statement since it is false that nine is even and also false that a square has five sides.
(d) In symbols, this statement is $s \vee \sim r$ which is a false statement since both s and $\sim r$ are false.

◈

The negation of the statement "p or q" must be false when "p or q" is true. Since the only way for "p or q" to be false is for both p and q to be false, the negation is "not p **and** not q." In symbols, the negation of $p \vee q$ is $\sim p \wedge \sim q$.

Example 2.13 Find the negation of each of the compound statements in Example 2.12. Write the negations in words and symbols.

Solution
(a) Three is not a prime number and a platypus is not a mammal. $\sim r \wedge \sim q$
(b) A square does not have five sides and three is not a prime number. $\sim p \wedge \sim r$
(c) Nine is not an even number and a square does not have five sides. $\sim s \wedge \sim p$
(d) Nine is not an even number and three is a prime number. $\sim s \wedge r$

◈

Example 2.14 Write the negation of the statement from Example 2.11, "It is raining and I forgot my umbrella," using symbols.

Solution
We will start by labeling the two simple statements included in the given compound statement:

r: It is raining.
u: I forgot my umbrella.

Then, the original statement can be written as $r \wedge u$. To form the negation, either r or u must be false. In words, "It is not raining or I did not forget my umbrella," and in symbols, $\sim r \vee \sim u$.

◈

Note that Example 2.14 shows that the negation of any statement of the form $p \wedge q$ is $\sim p \vee \sim q$.

2.3.4 Conditionals

Conditional statements are formed when two statements are connected with the terms *if* and *then*. For statements p and q, one possible conditional statement is: *If p, then q*. The statement p that follows the "if" is called the **condition** and the

statement q that follows the "then" is called the **consequence** or **conclusion**. A second conditional statement is: *If q, then p*. Notice that this is a different statement with a different meaning, since now q is the condition and p is the consequence.

Statements of the form *if p, then q* are called conditionals because they only tell you what will happen if the condition is true. For example, consider the following statement: If she has a phenomenal interview, then she will get the job. What happens if she does not have a phenomenal interview? The conditional above does not apply to this situation. She may lose out on the job, or her qualifications might fit the position so well that she gets a job offer despite a disappointing interview. The statement above only specifies what happens in the event of an outstanding interview.

> **Definition 2.5: conditional, $p \Rightarrow q$**
> A **conditional statement** is a statement of the form *if p, then q*. In symbols, this is written as $p \Rightarrow q$, and is read as "if p, then q" or "p implies q". A conditional statement is true if the conclusion, q, is true whenever the condition, p, is true. For a conditional statement to be false, there must be an example when the condition p is true and the conclusion q is false.

Sometimes statements that are not written in the conditional form are actually conditional statements. It is useful to be able to rewrite statements in a conditional form since we will develop techniques to prove this type of statement in the next section. The following example shows some sentences which can be rewritten as conditionals.

Example 2.15 Rewrite each of the following statements as a conditional statement with the same meaning.

(a)   A line extends indefinitely in two directions.
(b)   All integers are real numbers.
(c)   The sum of two even integers is an even integer.

Solution
(a)   If L is a line, then L extends indefinitely in two directions.
(b)   If a is an integer, then a is a real number.
(c)   If a and b are two even integers, then their sum is an even integer.

◈

The negation of a conditional statement $p \Rightarrow q$ must be false when the conditional is true. Since a conditional only specifies what will happen when the condition is true, the only way to make a conditional false is for the condition to be true and the conclusion to be false. Therefore, the negation of $p \Rightarrow q$ is $p \wedge \sim q$.

Example 2.16 Write the negation of the statement: If you build it, they will come.

Solution
You did build it, and they did not come. (Note that the statement "You did build it, but they did not come" has the same meaning but uses an alternate connective.)

◈

2.3.5   Biconditionals

There is one additional connective to consider, the **biconditional**.

Biconditional or "if and only if" statements have the form *p if and only if q*. The symbol ⇔ is used to represent "if and only if."

Definition 2.6: biconditional, $p \Leftrightarrow q$
The **biconditional** statement, *p if and only if q*, or $p \Leftrightarrow q$, means that both *p* and *q* are simultaneously true or simultaneously false. If $p \Leftrightarrow q$ is true, then *p* and *q* are called **logically equivalent**. For $p \Leftrightarrow q$ to be false, *p* or *q* must be true when the other is false.

One of the most important uses of "if and only if" statements is in mathematical definitions. In the next section formal definitions of some familiar terms about the integers–even, odd, and prime–are introduced.

Another way to think of an "if and only if" statement, $p \Leftrightarrow$ q, is as a combination of the two conditionals $p \Rightarrow q$ and $q \Rightarrow p$. For the biconditional $p \Leftrightarrow$ q to be true, both $p \Rightarrow q$ and $q \Rightarrow p$ must be true.

Example 2.17 Write the following biconditional statement in symbols, and determine its truth value.

A polygon is a triangle if and only if it has three sides.

Solution
If *p* represents the statement "A polygon is a triangle" and *t* represents "It has three sides," then in symbols the statement is $p \Leftrightarrow t$.

To determine whether the statement is true or false, look at the two conditionals combined in the biconditional:

$p \Rightarrow t$: If a polygon is a triangle, then it has three sides.
$t \Rightarrow p$: If it has three sides, then a polygon is a triangle.

Every triangle has three sides, so the first conditional, $p \Rightarrow t$, is true since whenever the condition is met, the conclusion is true.

Also, any polygon with three sides will be a triangle so the second conditional $t \Rightarrow p$ is also true.

Therefore, the biconditional statement $p \Leftrightarrow t$ is true.

◈

Example 2.18 Use the simple statements below to write out the "if and only if" statements $p \Leftrightarrow q$ and $r \Leftrightarrow t$ in words, and determine their truth values:

p: *S* has four sides.   r: The number *m* is an even integer.
q: *S* is a square.   t: *m* is divisible by 4.

Solution

$$p \Leftrightarrow q$$

In words: *S* has four sides if and only if *S* is a square.

To determine the truth value, look at the two conditionals combined in this statement.

$p \Rightarrow q$: If *S* has four sides, then *S* is a square.
$q \Rightarrow p$: If *S* is a square, then *S* has four sides.

The second conditional is true since every shape that is a square will have four sides. However, the first conditional is false. For example, if *S* is a rectangle, then it will have four sides, but they do not have to all have the same length, so *S* need not be a square. Since both conditionals are not true, the biconditional $p \Leftrightarrow q$ is false.

$$r \Leftrightarrow t$$

In words: The number *m* is an even integer if and only if *m* is divisible by 4.
Again, we can break this biconditional down into two conditionals.

$r \Rightarrow t$: If the number *m* is an even integer, then *m* is divisible by 4.
$t \Rightarrow r$: If *m* is divisible by 4, then *m* is an even integer.

The first conditional is false since 2 is an even number that is not divisible by 4. Therefore, the biconditional $r \Leftrightarrow t$ is false (even though the second conditional $t \Rightarrow r$ is true).

◈

Exercise Set 2.3

Exercises 1–7. Determine if the following pronouncements are statements.
 1. Calvin Butter is a math major.
 2. Eat your vegetables!
 3. Thank you!
 4. The clock is slow or the time is correct.
 5. How many answers are there for question #1?
 6. Heart disease is the leading killer of women.
 7. If you eat less and exercise more, you will lose weight.

Exercises 8–17. Form the negation of each of the following statements. Then determine the truth value of the original statement and the negation.
 8. The number nine is an odd number.
 9. A triangle has three sides.
10. All four-sided shapes are squares.

11. Today it is sunny outside.
12. Some birds do not fly.
13. Some amphibians do not swim.
14. The sum of two even numbers is even.
15. All dogs are friendly.
16. All prime numbers are odd.
17. Two and three are factors of six.

18. A crossword puzzle clue reads "cat or dog." Is the correct answer pet or pets? Why?
19. A crossword puzzle clue reads "Aretha and Ben." Is the correct answer Franklin or Franklins? Why?

Exercises 20–25. Using the simple statements below, write each compound statement in words, and decide whether the statement is true or false.

p: Two is an even number. r: Nine is a prime number.
q: Six is a multiple of 3. s: n is an odd number.

20. $p \wedge q$
21. $p \wedge \sim r$
22. $r \wedge s$
23. $p \wedge s$
24. $\sim q \wedge r$
25. $\sim r \wedge \sim p$

Exercises 26–31. Using the simple statements below, write each compound statement in words, and decide whether the statement is true or false. Compare the truth value to the corresponding statement in the previous section.

p: Two is an even number. r: Nine is a prime number.
q: Six is a multiple of 3. s: n is an odd number.

26. $p \vee q$
27. $p \vee \sim r$
28. $r \vee s$
29. $p \vee s$
30. $\sim q \vee r$
31. $\sim r \vee \sim p$

Exercises 32–36. For each pair of statements, do the following.

(a) Form the conditional statement $p \Rightarrow q$ and determine whether it is true or false. If the conditional statement is false, give an example that shows it is false.
(b) Form the conditional $q \Rightarrow p$ and determine whether it is true or false. If the conditional statement is false, give an example that shows it is false.
(c) Determine whether the biconditional statement $p \Leftrightarrow q$ is true or false.

32. p: a is even. q: a is divisible by 6.
33. p: The last digit of n is 0. q: n is even.
34. p: The last digit of n is 5. q: n is divisible by 5.

35. *p*: *a* is divisible by 3.   *q*: *a* is odd.
36. *p*: The last digit of *n* is 0.   *q*: *n* is divisible by 10.

Exercises 37–41. Determine whether the biconditional statement is true or false (it may be helpful to write out the two conditional statements combined in the biconditional).
37. A car's windshield wipers are on if and only if the headlights are on.
38. The sum of two integers is even if and only if the two integers are even.
39. An integer is prime if and only if it is odd.
40. *R* is a rectangle if and only if *R* has four sides.
41. The integer *m* is a perfect square if and only if the square root of *m* is an integer.

Exercises 42–45. Represent each simple statement with a letter and then write each compound statement below in symbols.
42. If *R* is a rectangle, then *R* has 4 right angles.
43. If two even integers are added, then their sum is an even integer.
44. If two odd integers are added, then their sum is an even integer.
45. If two even integers are multiplied, then the product is an even integer.

Exercises 46–49. Form the negation of each of the following statements.
46. If the grass is greener, then she will go to the other side of the fence.
47. The number three is prime and there are 12 months in a year.
48. I would like peas or carrots with dinner.
49. The integer *a* is odd or the integer *b* is odd.

2.4   Properties of the Integers

Two important components of a proof are *axioms* and *definitions*. Axioms are statements that are so basic they are accepted as true without proof. They provide a starting point for reasoning. Definitions make use of "if and only if" statements to provide a concrete characterization of mathematical terms so that everyone has the same understanding of what they mean. Since definitions are "if and only if" statements, the two sides are interchangeable and can be substituted for each other in a proof. This section introduces the formal definitions of even, odd, and prime, as well as an axiom about the integers.

> **Definition 2.7: even**
> An integer *a* is **even** if and only if $a = 2n$ for $n \in \mathbb{Z}$.

The "if and only if" in this definition means that the two sides of the statement are interchangeable: if an integer *a* is even, then *a* can be replaced with the formula $2n$. Also if you find that *a* can be written as $2n$ for an integer *n*, then you can conclude that *a* is even. This definition will be used repeatedly in proofs.

Example 2.19 Use the definition of even to show that 22 is even but 23 is not.

Solution
Since $22 = 2(11)$ and $11 \in \mathbb{Z}$, 22 satisfies the definition of even.
Since $23 = 2(11.5)$, and $11.5 \notin \mathbb{Z}$, 23 is not even.

◈

> **Definition 2.8: odd**
> An integer b is ***odd*** if and only if $b = 2n + 1$ for $n \in \mathbb{Z}$.

This means that if an integer b is odd, it can be replaced with the formula $2n + 1$, and that works in reverse as well: if you are able to show that an integer b can be written in the form of twice another integer plus 1, then you can conclude b is odd.

Example 2.20 Use the definition of odd to verify that 81 is odd but 80 is not odd.

Solution
Since $81 = 2(40) + 1$ and $40 \in \mathbb{Z}$, 81 is odd.
Since $80 = 2(39.5) + 1$, and $39.5 \notin \mathbb{Z}$, 80 is not odd. (In fact, since $80 = 2(40)$, 80 is even.)

◈

> **Definition 2.9: prime**
> An integer $p > 1$ is ***prime*** if and only if the only positive divisors of p are 1 and p.

Before beginning to write proofs about the integers, there is one more familiar fact that needs to be made explicit. Think about what happens when two integers are added; whether they are positive, negative, or zero, the result will be another integer. Similarly, if two integers are subtracted, the result will be another integer. Finally, if two integers are multiplied together, the result is still an integer. This property is called ***closure***. If a set is ***closed*** under an operation (like addition or subtraction), it means that when that operation is performed on members of the set, the result will still be in the set. This property is an axiom of integer arithmetic and is stated below.

> **Closure of $\mathbb{Z}$ Axiom**
> The integers are closed under addition, subtraction, and multiplication.

Notice that the operation division is missing from this list. That is because the integers are not closed under division. For example, $4 \div 2 = 2$, which is still in the

integers, but $4 \div 3 = \frac{4}{3}$, which is not an integer. Since the result of dividing an integer by an integer is not always an integer, the integers are not closed under division.

Example 2.21 If k and m are integers, determine whether or not $2(k + 2km + 1)$ must be an integer.

Solution
Since 2, k, m, and 1 are all integers, and they are combined using multiplication and addition, $2(k + 2km + 1)$ must be an integer because $\mathbb{Z}$ is closed under addition and multiplication.

◈

Example 2.22 If a and b are integers, use the definition of even to verify that $4a + 2$ is even.

Solution
Since $4a + 2 = 2(2a + 1)$, and $2a + 1 \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under addition and multiplication, $4a + 2$ is even by the definition of even.

◈

Exercise Set 2.4

Exercises 1–10. If a and b are integers, determine whether or not the given expression *must* represent an integer. Explain your work.

1. $a + b$
2. $a - b$
3. a/b
4. $a - 2b + 1$
5. πab (where $\pi = 3.14159\ldots$)
6. $10ab$
7. $2a + b + 1$
8. $4b - 2$
9. $\frac{a+b}{2}$
10. $\sqrt{2} \cdot ab$

11. For each term below, give an example that satisfies its definition and an example that does not. Explain using the definition:

    (a) even
    (b) odd
    (c) prime

Exercises 12–17. Determine whether each integer is even or odd. Justify your answer using the definitions.

12. 412
13. -25
14. 0
15. -34
16. 147
17. 2

Exercises 18–25. If a and b are integers, determine whether or not each expression is even or odd, if possible. Justify your answer using the definitions. If it is not possible to determine whether the expression is even or odd, explain why using examples.

18. $2a + 2b$
19. $a + 2$
20. $4a + 2b$
21. $2a + 2b + 3$
22. $a + b + 2ab$
23. $4b + 1$
24. $a^2 + b^2$
25. $2a + 4ab + 4$

26. Explain why 2 is the only even prime number, using the definitions in this section.

2.5 Rules of Logic and Direct Proofs

Now that we can determine whether a statement is true or false, and we have some definitions and the Closure of $\mathbb{Z}$ Axiom to work with, we will continue with some rules of logic. Remember that the statements that are given as true at the beginning of a proof are called **premises**. Premises are often facts that are given in the statement of the problem. In logic, a **valid argument** means that if the premises you start with are true, then the conclusion will also be true. The conclusion of a valid argument is called a **valid conclusion**. Proofs are an example of valid arguments, and logical rules explain how to construct a valid argument, based on the types of statements in the premises and the conclusion you want to show.

For example, if you know that "Philip has a pet dog and a pet rabbit" is a true statement, then it is valid to conclude that Phillip has a dog. (In fact, he has a rabbit as well.) On the other hand, if you are given that "Phillip has a pet dog *or* a pet rabbit" is a true statement, it would not be valid to conclude that Phillip has a pet dog, because the "or" statement above is still true if Phillip has only a pet rabbit.

These rules of logic, based on what makes a statement true or false, allow us to connect the definitions, theorems, and given information into a **mathematical proof**.

2.5.1   General Properties of a Proof

The purpose of a proof is to provide a clear argument that you or another person can read and follow to understand why the statement being proved is true. When writing a proof, the goal is always to connect the information known to be true to the conclusion you want to show is true. In order to make proofs as clear as possible, there are some general properties they all share.

- The beginning and end of the proof are always labeled, so that readers know when the argument starts and at what point they should be convinced the statement is true.
- The premises are clearly stated at the beginning of the proof.
- Each step in the proof is supported with a reason.
- The last line of the proof matches the conclusion you were to show.

The most common proof is a proof of a conditional statement: *If p, then q*. The most common type of proof is a ***direct proof***.

2.5.2   Direct Proofs

Often the type of statement to prove has a conditional form, "if p, then q". For a conditional to be true, the consequence q must be true whenever the condition p is true. Therefore, a conditional statement can be proven true by assuming the condition p is a true statement and showing that the conclusion q is also a true statement. This type of proof is called a ***direct proof***.

> **Proof Technique: Direct Proof**
> To prove a statement of the form: If p, then q:
>
> 1. Take p as a premise.
> 2. Logically connect definitions, theorems, and axioms to show that q must be true.

Note that if one is not able to fill in the middle to show that the statement q must be true, it could be for two reasons:

1. Possibly, q is not always true when p is true and *if p, then q* is actually a false statement (We will discuss what to do in this case in Section 2.7).
2. It is also possible that we have not put the information together in the right way yet, or there is a piece of information missing that is needed to complete the proof.

Whenever you are trying to better understand a statement, or determine whether it is actually true or false, inductive reasoning is very helpful.

The next example illustrates how all these ideas fit together to prove a statement about the integers.

Example 2.23 Prove that if two integers are even, then their sum is even.

Solution

This is a conditional statement of the form *if p, then q*. Therefore, the method of proof is to take p as the premise and show q is true.

In this case, the statement p is "two integers are even." To make this easier to work with, rewrite it in two parts: a is an even integer and b is an even integer. Our goal is then to show that q is true: the sum $a + b$ is even. Here are the steps in the proof. In each step of the proof, previous steps will be shown in italics to make it clear what has been changed.

1. Label the start of the proof, and write down the premises. Premises are often identified by the words "Let" or "Suppose" since they are the beginning assumptions of the proof. Also, write down what you want to show. Note that the column headed "Show" is an important tool to keep track of what we need to do but is not actually considered part of the proof.

Proof.	SHOW
Let a be an even integer.	$a + b$ is an even integer
Let b be an even integer.	

2. Check to see if any defined terms are included in the premises. In this case, *even* is a term that has been defined. If so, apply the definition to the premise.

Proof.	SHOW
Let a be an even integer.	*a + b is an even integer*
Let b be an even integer.	
$a = 2n$ for $n \in \mathbb{Z}$ by the definition of even	
$b = 2k$ for $k \in \mathbb{Z}$ by the definition of even	

Notice that when we applied the definition of even to the integers a and b, different letters, n and k, were used. This is necessary: using n in both cases would mean a and b were the same number. Changing the letter gives two different even numbers.

3. Compare what you are trying to show to the last step of the proof so far. If there is also a defined term in the desired conclusion, rewrite it in the "Show" column using the definition. (Remember: when you rewrite the conclusion on the right-hand side, this is not actually part of the proof. This is scratchwork that helps keep you on track and guides you in the best direction to go next).

Proof.	SHOW
Let a be an even integer.	*a + b is an even integer*
Let b be an even integer.
a = 2n for n ∈ ℤ by the definition of even	*a + b = 2x for an integer x*
b = 2k for k ∈ ℤ by the definition of even

Notice that once again, we used a different letter in the definition of even. All we know about x is that it must be an integer, but not exactly what form it will have.

4. The first three steps are the same in almost every single proof. Here is where the creative part of the proof begins! Compare the steps in the proof to the conclusion, looking for a way to relate them. In this example, we want information about the sum $a + b$, and the proof contains formulas for a and b, so it may be helpful to add a and b together and substitute the formulas.

Proof.	SHOW
Let a be an even integer.	*a + b is an even integer*
Let b be an even integer.
a = 2n for n ∈ ℤ by the definition of even	*a + b = 2x for an integer x*
b = 2k for k ∈ ℤ by the definition of even
$a + b = 2n + 2k$ by substitution

5. This looks promising! Continue to compare the steps of the proof to what you want to show, and use known information such as algebra rules, definitions, or theorems to connect them. In this case, algebra is helpful.

Proof.	SHOW
Let a be an even integer.	*a + b is an even integer*
Let b be an even integer.
a = 2n for n ∈ ℤ by the definition of even	*a + b = 2x for an integer*
b = 2k for k ∈ ℤ by the definition of even	*x*
$a + b = 2n + 2k$ by substitution
$a + b = 2(n + k)$ by algebra (factoring)

6. Continue to compare the lines of the proof to what you want to show, until you are able to reach the desired conclusion of the proof. In this example, the proof is close to done because the last line of the proof is very close to the last line in the Show column. It remains to show that $n + k$ is an integer. This is true because the integers are closed under addition, and n and k are both integers.

Proof.	SHOW
Let a be an even integer.	*a + b is an even integer*
Let b be an even integer.	
a = 2n for n ∈ ℤ by the definition of even	*a + b = 2x for an integer x*
b = 2k for k ∈ ℤ by the definition of even	
a + b = 2n + 2k by substitution	
a + b = 2(n + k) by algebra (factoring)	
$n + k \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under addition	

7. The last two lines of the proof verify the last line under the Show column. At this point, we can use the scratchwork to work back up to the desired conclusion of the proof. The final step is to state the conclusion and indicate that the proof is done. There are many ways to signify the end of a proof. A common way is a box placed at the end of the proof. Here is the complete proof.

Proof.	SHOW
Let a be an even integer.	*a + b is an even integer*
Let b be an even integer.	
a = 2n for n ∈ ℤ by the definition of even	*a + b = 2x for an integer x*
b = 2k for k ∈ ℤ by the definition of even	
a + b = 2n + 2k by substitution	
a + b = 2(n + k) by algebra (factoring)	
n + k ∈ ℤ because ℤ is closed under addition	
Therefore, $a + b$ is even by the definition of even.	
■	

◈

Example 2.24 Prove that the product of two odd integers is odd.

Solution
This statement is not in a conditional form but can be written so that it is:
   If a and b are odd integers, then their product ab is odd.

Therefore, the proof will have the same format as the last example, beginning with the premises that a is odd and b is odd. (For algebra review on the factoring and multiplying of these expressions, see Exercises 1–8 at the end of this section.)

Proof. | SHOW

Let a be an odd integer. ab is an odd integer
Let b be an odd integer.
$a = 2n + 1$ for $n \in \mathbb{Z}$ by the definition of odd $ab = 2x + 1$ for an integer x
$b = 2k + 1$ for $k \in \mathbb{Z}$ by the definition of odd
$ab = (2n + 1)(2k + 1)$ by substitution
$\quad = 4nk + 2n + 2k + 1$ using algebra
$\quad = 2(2nk + n + k) + 1$ by factoring out common terms
$2nk + n + k \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under addition
and multiplication
Therefore, ab is odd by the definition of odd.

■

◈

Proofs in textbooks (except for geometry textbooks) and mathematical articles are often written in paragraph form, rather than the column form shown in the two previous examples. The proofs still contain the same information (premises are clearly stated, and each step is justified with a reason), but it is presented in a different format. If you are writing a proof in this form yourself, it is often useful to start with a column proof to organize the information and then translate it into paragraph form. The proof for the statement in Example 2.24 is shown again in Example 2.25, written in a more traditional mathematical style.

Example 2.25 Write a proof of the statement "If a and b are odd integers, then their product ab is odd" in paragraph form.

Solution
Proof.
Let a and b be odd integers. Then, by the definition of odd, there are integers n and k such that $a = 2n + 1$ and $b = 2k + 1$. Multiplying a and b and substituting these formulas, we obtain:

$$ab = (2n + 1)(2k + 1)$$
$$= 4nk + 2n + 2k + 1$$
$$= 2(2nk + n + k) + 1.$$

Since $\mathbb{Z}$ is closed under multiplication and addition, $2nk + n + k \in \mathbb{Z}$. Therefore, ab is odd by the definition of odd.

■

◈

Example 2.26 Suppose you have the following two premises.

Sophie plays the piano or the violin.
Sophie plays the violin.

Can you make a valid conclusion about whether or not Sophie plays the piano? If so, what? If not, why not?

Solution
In this case, no valid conclusion can be drawn about whether or not Sophie plays the piano. The premises can both be true whether Sophie plays the violin or not.

On the other hand, if the second premise had been "Sophie does not play the violin," then it would have been valid to conclude that she does play the piano, because if she did not play either instrument, the first premise would not be true.

◈

Note that when an "or" statement is true, at least one of the component statements is true. If you know that one statement is false, then the other one must be true. This concept is illustrated again in Example 2.27 below.

Example 2.27 Prove that if $a + b$ is odd, then one of a or b is odd.

Solution
In this case, the conclusion is an "or" statement. One common technique to show that an "or" statement is true is to assume that one of the component statements is false. Then, if we are able to show that the other piece of the "or" statement must be true, that proves the original statement is true.

Proof.	SHOW
Let $a + b$ be odd.	a is odd or b is odd
Then $a + b = 2n + 1$ for $n \in \mathbb{Z}$ by the definition of odd.	
Suppose that a is even.	Show that b is odd.
$a = 2k$ for $k \in \mathbb{Z}$ by the definition of even	Show that $b = 2x + 1$ for an integer x.
$b = 2n + 1 - a$ by solving $a + b = 2n + 1$ for b	
$b = 2n + 1 - 2k$ by substitution	
$b = 2(n - k) + 1$ by factoring	
$n - k \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under subtraction	
Therefore, b is odd by the definition of odd.	
■	

◈

Example 2.28 Suppose that you have the following two premises:

1. If R is a rectangle, then pairs of opposite sides are parallel.
2. R, pictured below, is a rectangle.

Can you make a valid conclusion about sides AB and CD? If so, what? If not, why not?

Solution

In this case the premises do support a valid conclusion. If a conditional statement is true, then the consequence is true every time the condition is true. Since the shape R is a rectangle, the condition in the first premise is true for R. Therefore, the opposite sides AB and CD must be parallel.

◈

Exercise Set 2.5

Exercises 1–4. Factor the common factors out of the expression.
1. $2m + 4k$
2. $4mn + 2m + 2n + 1$
3. $2k + 2$
4. $10a + 6ab + 2$

Exercises 5–8. Multiply and simplify when possible.
5. $2(2k + 1)$
6. $2m \cdot 2n$
7. $(2k + 1)(2k + 1)$
8. $(2k + 1)(2m + 1)$

Exercises 9–12. Use the definition of even to verify that the expression is an even integer.
9. $6k$
10. $2m + 4n$
11. $4k + 2$
12. $6 - 4m$

Exercises 13–16. Use the definition of odd to verify that the expression is an odd integer.
13. $2m + 2n + 1$
14. $4k + 1$

15. $2k+5$
16. $2m+2k+3$

17. Complete the following to form a valid argument:

   (a)   If John is delivering the truck, then the shipment will arrive on time. The
         shipment will not arrive on time.
   (b)   If you get a C, then you will pass the class. You did not pass the class.

18. Prove that 0 is an even number.
19. Prove that if n is even, then $n+1$ is odd.
20. Prove that if n is odd, then $n+1$ is even.
21. Prove that if a is even and b is odd, then the sum of a and b is odd.
22. Prove that if two integers are odd, then their sum is even.
23. Prove that the product of an even number and an odd number is even.
24. Prove that the product of an even number and any integer is even.
25. Prove that the difference of two odd numbers is even.
26. Prove that the product of two even integers is divisible by 4.
27. Prove that the sum of two consecutive integers is odd.
28. Prove that the sum of three odd numbers is odd.

2.6   Indirect Proofs and Proofs by Contradiction

In Section 2.3, we saw that two conditionals could be formed from two statements
p and q: if p, then q, and if q, then p. In symbols, these are written as $p \Rightarrow q$ and
$q \Rightarrow p$. The conditional $q \Rightarrow p$ is called the ***converse*** of $p \Rightarrow q$.

> **Definition 2.10: converse**
> The ***converse*** of the conditional statement *If p*, *then q* is *If q*, *then p*.
> In symbols, the *converse* of $p \Rightarrow q$ is $q \Rightarrow p$.

If both $p \Rightarrow q$ and its converse $q \Rightarrow p$ are true (or if $p \Rightarrow q$ and $q \Rightarrow p$ are both
false), then the biconditional statement $p \Leftrightarrow q$ is true, and p and q are logically
equivalent. Sometimes a statement and its converse have the same truth value, and
sometimes they do not, as Examples 2.17 and 2.18 in Section 2.3 show.
   The ***contrapositive*** is another conditional that can be formed from "if p, then q."
The definition is stated below.

> **Definition 2.11: contrapositive**
> The ***contrapositive*** of the conditional statement "if p, then q" is "if not q, then
> not p." In symbols, the *contrapositive* of $p \Rightarrow q$ is $\sim q \Rightarrow \sim p$.

Notice that there are two steps to forming the contrapositive of $p \Rightarrow q$:

1. Switch the order of p and q (this is the converse).
2. Negate both p and q.

Example 2.29 Form the contrapositive of each of the following statements:

(a) If you play well, then your team will win.
(b) If S is a square, then S has four sides.
(c) If you get enough sleep, then you feel energetic and enthusiastic.

Solution
(a) Label p: "You play well" and q: "Your team will win." Then the form for the contrapositive is $\sim q \Rightarrow \sim p$. In words:

   If your team did not win, then you did not play well.

(b) The contrapositive is, "If S does not have four sides, then S is not a square." Notice that both the original conditional and the contrapositive are true statements.
(c) In this example, the conclusion is an "and" statement: You will feel energetic and enthusiastic. The negation is "You do not feel energetic *or* you do not feel enthusiastic." Therefore, the contrapositive is, "If you do not feel energetic or you do not feel enthusiastic, then you did not get enough sleep."

◈

2.6.1   Indirect Proofs

The contrapositive of a conditional statement is very useful because, unlike the converse, the contrapositive is logically equivalent to the original conditional statement. In other words, $p \Rightarrow q$ and $\sim q \Rightarrow \sim p$ are either both true or both false. This means that an alternative to proving the statement "if p, then q" using a direct proof is to prove that the contrapositive is true instead. This method is called an ***indirect proof***. Although a direct proof is the first method to try, if it is not working, sometimes proving the contrapositive is easier.

> **Definition 2.12: indirect proof**
> An ***indirect proof*** of the conditional statement $p \Rightarrow q$ is a proof of the statement $\sim q \Rightarrow \sim p$.

To prove a statement "if p, then q" using an indirect proof, you would first assume that $\sim q$ is true and then show that $\sim p$ is true.

Proof Technique: Indirect Proof

To prove a statement of the form "if p, then q", prove the contrapositive "if $\sim q$, then $\sim p$".

1. Take $\sim q$ as a premise.
2. Logically connect definitions, theorems, and axioms to show that $\sim p$ must be true.

At the end of this section, we will examine why a conditional and its contrapositive are logically equivalent, but before that let us look at an example of a proof where the contrapositive is useful.

Example 2.30 Prove that if $3a + 5$ is odd, then a is even.

Solution

Using the direct approach to a proof, the premise is that $3a + 5$ is odd. Applying the definition of odd, this can be written as $3a + 5 = 2k + 1$ for an integer k. Since the conclusion is that a is even, we must show that $a = 2n$ for an integer n. However, in attempting to solve the equation above for a, we get stuck with $3a = 2k - 4$. It may be possible to continue by dividing the problem up between when k is even and k is odd, but instead let us see if proving the contrapositive is easier.

The contrapositive of the statement is: If a is odd, then $3a + 5$ is even. Notice that the premise is much simpler this time. We will now proceed with the proof.

Proof (of the contrapositive).	SHOW
Let a be an odd integer.	$3a + 5$ is even
Then $a = 2n + 1$ for $n \in \mathbb{Z}$ by the definition of odd.	Show that $3a + 5 = 2x$ for an integer x
$3a + 5 = 3(2n + 1) + 1$ by substitution	
$3a + 5 = 6n + 3 + 1$ by distributing through the parentheses	
$3a + 5 = 6n + 4$ by combining like terms	
$3a + 5 = 2(3n + 2)$ by factoring out common factors	
$3n + 2 \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under addition and multiplication	
Therefore, $3a + 5$ is even by the definition of even.	
∎	

◈

2.6.2   Proof by Contradiction

Another proof technique very closely related to an indirect proof is called a ***proof by contradiction***. Sometimes rewriting a statement as its contrapositive does not make a proof more approachable. In this case, a proof by contradiction can be helpful because it gives you an extra premise to work with. Proofs by contradiction are often useful when you are trying to prove that something is not true or does not exist.

In order to prove a statement using a proof by contradiction, start by stating the premise or premises, as you would in a direct proof. Where this method differs is that we also assume that the desired conclusion is false. Then use the original premises as well as this extra piece of information to reach an impossible statement (such as one of the premises being false). Since the premises are given as true, it follows that the assumption that the conclusion is false is incorrect. Therefore, the conclusion must be true.

Proof Technique: Proof by Contradiction

1. Start by stating any premises.
2. Assume that the desired conclusion is false.
3. Logically connect definitions, theorems, and axioms to find a contradiction of one of the premises or some other fact known to be true.
4. Conclude that the conclusion cannot be false as assumed and must in fact be true.

Example 2.31 Consider the following statement: The difference of two primes is never 13.

(a) Test this statement on some examples to convince yourself it is true.
(b) Prove that the statement is true.

Solution
(a) In symbols, the statement says that if p and q are primes, then $p - q \neq 13$. Another way to say this is that if $a - b = 13$, then a and b cannot both be prime. The second statement may be a more useful way to think about testing the statement. Choose a prime value for b. Then, $a = 13 + b$. If a is not a prime number, this supports the statement that a difference of two primes cannot yield 13. If a is prime, then this would be a counterexample which would prove the statement false. Here are some examples.

$$b = 2, \qquad a = 13 + 2 = 15 \text{ which is not prime}$$
$$b = 3, \qquad a = 13 + 3 = 16 \text{ which is not prime}$$
$$b = 5, \qquad a = 13 + 5 = 18 \text{ which is not prime}$$

In fact, notice that if b is an odd prime, then a will be even since the sum of two odd numbers is even.

(b) Notice that this is an example of proving that something cannot happen, a good candidate for a proof by contradiction.

Proof (by contradiction).
We are asked to show that if p and q are primes, then $p - q \neq 13$. We will assume the opposite. So, suppose that there actually are two primes p and q such that $p - q = 13$. Since 13 is odd, either p is odd and q is even or p is even and q is odd. Otherwise, their difference would be even. We will examine the two possibilities separately.

Case 1. Suppose that p is odd and q is even. Then, since q is prime, q must equal 2. Substituting into $p - q = 13$, we obtain $p - 2 = 13$, which means that $p = 15$. This contradicts the premise that p is prime.

Case 2. Suppose that p is even and q is odd. Then, since p is prime, p must be equal to 2. Substituting again into $p - q = 13$, we obtain $2 - q = 13$, which means that $q = -11$. This also contradicts the premise that q is prime since primes are defined to be greater than 1.

In each case, we reached a contradiction of one of the premises of the proof. Therefore, the assumption that primes p and q exist such that $p - q = 13$ must be false. Therefore, there are no primes with a difference of 13.

■

◈

Finally, we will show that a conditional and its contrapositive are logically equivalent. Remember that two statements are logically equivalent if they always have the same truth values, so there are two parts to this proof. First, if $p \Rightarrow q$ is true, then we must show $\sim q \Rightarrow \sim p$ is also true. Second, if $\sim q \Rightarrow \sim p$ is true, then we must show $p \Rightarrow q$ is true. This result is stated in Theorem 2.1 below.

> **Theorem 2.1**
> A conditional statement "if p, then q" is logically equivalent to its contrapositive "if $\sim q$, then $\sim p$." In symbols, the statements $p \Rightarrow q$ and $\sim q \Rightarrow \sim p$ are logically equivalent.

Proof.
Part I. Show that if $p \Rightarrow q$ is true, then $\sim q \Rightarrow \sim p$ is true.
Let $p \Rightarrow q$ be true. To show that $\sim q \Rightarrow \sim p$ is true, show that when $\sim q$ is true, $\sim p$ is also true. So, assume that $\sim q$ is true. This means that q must be false since a statement and its negation always have opposite truth values. Now, since $p \Rightarrow q$ is a true statement, q is true whenever p is true. Since we know q is false, p must also be false. Therefore, $\sim p$ is true. This verifies that $\sim q \Rightarrow \sim p$ is true.

Part II. Show that if $\sim q \Rightarrow \sim p$ is true, then $p \Rightarrow q$ is true.

Let $\sim q \Rightarrow \sim p$ be true. Since this statement is a conditional, we will apply the result proved in Part I, which tells us that if we reverse the order and negate each piece of this conditional, we will still get a true statement. Therefore, $\sim(\sim p) \Rightarrow \sim(\sim q)$ is also a true statement. Since $\sim(\sim p) = p$ and $\sim(\sim q) = q$, the statement $\sim(\sim p) \Rightarrow \sim(\sim q)$ is the same as $p \Rightarrow q$. Therefore, $p \Rightarrow q$ is true.

∎

To put this result in context, suppose that the following is a true statement: If you are late to the concert, then you will miss the opening act. The contrapositive of this statement is: If you do not miss the opening act, then you were not late to the concert. If one of these statements is true, then the other has to be as well. The original conditional and its contrapositive are giving you the same information, but in two different forms.

Exercise Set 2.6

Exercises 1–7. Write the contrapositive of the statement and decide if the statement (and its contrapositive) is true or false.

1. If the shoe fits, then she will wear it.
2. If you are not there, then you cannot vote.
3. If at first you do not succeed, then try again.
4. If n is odd, then 2 does not divide n.
5. If n is even, then 2 does not divide n.
6. If p is prime, then p is odd.
7. If p is odd, then p is prime.

8. Prove that every prime number greater than 2 is odd. (Note that you were asked to explain why this is true in Exercise 26 in Section 2.4. Now, write a formal proof of this fact.)
9. Prove that if $5b - 1$ is even, then b is odd.
10. Prove that if $7a + 2$ is even, then a is even.

2.7   Counterexamples: Proving a Statement Is False

To show that a general statement is false, you need to find one example for which the statement fails to be true, called a ***counterexample***. For example, consider the statement "All prime numbers are odd." To be convinced that this statement is false, we need only one example of a prime number that is not odd, and the number 2 fits the bill since 2 is even and also prime. Even though there are many prime numbers that are odd, the statement is false because it is not true for the prime 2. Therefore,

the number 2 is a counterexample to the statement that "All prime numbers are odd." Now consider the example below.

Example 2.32 Show that the statement "All multiples of 3 are multiples of 6" is false.

Solution
Start by rewriting the statement as a conditional:
    If x is a multiple of 3, then x is a multiple of 6.

To show this statement is false, we need only one choice for x that makes the statement false. Any choice for x that makes the statement false is called a counterexample. For a conditional, this means that the condition is true for x, but the conclusion is false.
For example, if $x = 9$, then it is true that 9 is a multiple of 3 because $3 \cdot 3 = 9$, so the condition is true. But it is false that 9 is a multiple of 6 since there is no integer that can be multiplied by 6 to equal 9. Therefore, $x = 9$ is a counterexample for the given statement.
Notice that even though the statement is true for some values of x, such as $x = 12$ or $x = 24$, it is still a false statement since it is not true for all values of x. Also, notice that 9 is not the only possible counterexample. The values $x = 15$ or $x = 3$ are also counterexamples to the statement. (Make sure that you can justify that they are actually counterexamples.)

◈

There are two parts to providing a complete counterexample: first, the example itself and second, the explanation of why it shows the statement is false.

Example 2.33 The following statement is false. Provide a counterexample and explain why it is a counterexample.

    "The product of two primes is odd."

Solution
Again, one can find many examples that make the statement true, for instance, 3×5, 7×11, 3×73. However, this statement is false. Here is a counterexample:
    2 is a prime number and 3 is a prime number, but $2 \times 3 = 6$, and 6 is even, not odd.

◈

Example 2.34 Disprove the statement: The sum of an even number and an odd number is even.

Solution
Disproving a statement means to show that the statement is false, so we need a counterexample. One counterexample is the pair of integers 2 and 3; 2 is even and 3 is odd, but the sum $2 + 3 = 5$ which is odd, not even. Therefore the statement is false.

◈

Exercises 1–13. Prove that the statement is false by providing a counterexample and explaining why the example shows the statement is false.

1. If you are a college student, then you must be under 22.
2. If you are a millionaire, then you have a college degree.
3. If you have a college degree, then you are a millionaire.
4. All organic food is healthy.
5. The sum of an odd number and an odd number is an odd number.
6. If n is a multiple of 4, then n is also a multiple of 8.
7. If the sum $a + b$ is even, then a and b must both be even.
8. All odd numbers are prime.
9. The sum of two prime numbers is even.
10. The sum of an even number and an odd number is an even number.
11. The difference of two prime numbers is even.
12. The formula $n^2 + n + 5$ is a prime number for all integers $n > 0$.
13. All multiples of 6 are multiples of 12.

2.8   Divisors and the Greatest Common Divisor

We end this chapter with a discussion of divisors and common divisors in Section 2.8, and a review of divisibility rules in Section 2.9. These are central to number theory and will be used in every chapter of this book. They are also very important in modern applications of mathematics in a variety of settings, including cryptography which is studied in Chap. 8.

We will start with an important definition.

Definition 2.13: divides
An integer d **divides** an integer m if and only if $m = dk$ for some integer k.

The notation for "d divides m" is $d|m$. Because this is such an important and useful concept, there are many ways to express the information "d divides m". Some common alternatives include:

d is a factor of m.
d is a divisor of m.
d divides m evenly.
m is a multiple of d.

Example 2.35 Determine whether each of the following statements are true or false:

(a) $8|72$ (b) $6|20$ (c) $2|4326$ (d) $6|3$ (e) $5|0$

Solution

(a)   Since $72 = 8(9)$, and 9 is an integer, $8|72$ is true.
(b)   Since $20 = 6(3) + 2$, 6 does not divide 20 evenly, so $6|20$ is false. Another way to see this is that $20 = 6\left(\frac{10}{3}\right)$, and $\frac{10}{3}$ is not an integer.
(c)   Since $4326 = 2(2163)$, $2|4326$ is true.
(d)   Since $3 = 6\left(\frac{1}{2}\right)$, $6|3$ is false (Note that $3|6$ is true, but reversing the order makes a false statement since an integer cannot be a divisor of a smaller integer).
(e)   Since $0 = 5(0)$, $5|0$ is true!

◆

Example 2.36   Determine whether each of the following statements is true or false:

(a) $-8|72$ (b) $2|(6n + 4)$ (c) $0|11$ (d) $4|(-128)$ (e) $0|0$

Solution

(a)   True, because $72 = -8(9)$.
(b)   True, because $6n + 4 = 2(3n + 2)$. Notice that it doesn't matter whether 2 divides n, since we can factor a 2 out of the entire expression.
(c)   This statement is false. We would need $11 = 0 \cdot k$ for an integer k, but $0 \cdot k$ is always 0.
(d)   True, because $-128 = 4(-32)$.
(e)   True, because $0 \cdot 0 = 0$.

◆

Parts (e) of Example 2.35 and Example 2.36 may seem surprising, because there are issues with dividing by zero. It is important to understand the difference between the symbols $a|b$ and a/b. The "divides" symbol is a vertical line, not a slanted line. When we write $a|b$, this is actually a shorthand representation of the statement "a divides b" that is either true or false. On the other hand, a/b represents a particular number: the one that is equal to the value of a divided by b. These concepts are different, but related. For example, if a/b is an integer, that means that $b|a$. Since we are working only in the integers, we will generally avoid division because the integers are not closed under division.

In Part (a) of Examples 2.35 and of Example 2.36, we saw that $8|72$ and $-8|72$ are both true. In the next example, we will prove that this relationship is true in general.

Example 2.37 Prove that if $a|b$, then $-a|b$.

Solution
Proof.
Let $a|b$. Then, using the definition of divides, we know that $b = ak$ for some $k \in \mathbb{Z}$. Notice that $ak = (-a)(-k)$, so $b = (-a)(-k)$. Since $-k$ is also an integer (because

$-k = -1 \cdot k$ and $\mathbb{Z}$ is closed under multiplication), we can conclude that $-a|b$ by the definition of divides.

■

◈

Example 2.38 Prove that if 6 divides n, then 2 divides n and 3 divides n.

Solution
Notice that the conclusion we are asked to prove is an "and" statement, so to complete the proof, we have to verify that both $2|n$ and $3|n$ are true. The proof of this statement is shown below in column form. In Exercise 60, you are asked to rewrite it in paragraph form.

Proof.	SHOW
Let $6|n$.	$2|n$ and $3|n$
Then $n = 6k$ for $k \in \mathbb{Z}$ by the definition of divides	$n = 2x$ and
	$n = 3y$
$n = 2 \cdot 3k$ by factoring	for integers
	x and y
Therefore, $n = 2(3k)$ and $n = 3(2k)$ because multiplication is associative and commutative.	
$3k$ and $2k$ are integers because $\mathbb{Z}$ is closed under multiplication	
Therefore, $2|n$ and $3|n$ by the definition of divides.	
■	

◈

Example 2.39 Determine if the following conjecture is true or false. If it is false, give a counterexample. If the conjecture is true, provide a proof.

CONJECTURE: If $3|a$ and $6|a$, then $18|a$.

Solution
Since we do not know whether this statement is true or false, we will test a few choices for a to develop an opinion. If a choice for a makes the statement false, then it is a counterexample. If, on the other hand, all of the choices for a make the statement true, then we can either test more examples or try to write a proof.

Start with $a = 36$. Then the condition is met since $3|36$ and $6|36$ are both true. However, $18|36$ is also true, so this example provides support for the conjecture.

Now, try $a = 9$. This choice for a will not provide a counterexample or evidence that the statement is true since the condition is not satisfied: while it is true that $3|9$, $6|9$ is false. Since the condition is false, this example provides no information.

As another example, let $a = 12$. The condition is true in this case, because $3|12$ (since $12 = 3(4)$) and $6|12$ (since $12 = 6(2)$). However, $18 \nmid 12$ since $18\left(\frac{2}{3}\right) = 12$ and $\frac{2}{3} \notin \mathbb{Z}$, so the conclusion is false. Therefore, the conjecture is false and $a = 12$ is a counterexample.

◈

The next theorem shows that divides is transitive: if $a|b$ and $b|c$, then $a|c$.

Theorem 2.2
Prove that if $a|b$ and $b|c$, then $a|c$.

Proof.
Let $a|b$ and $b|c$. Then by the definition of divides, there are integers m and k such that $b = am$, and $c = bk$. Substituting for b in the second equation,

$$c = bk$$
$$= (am)k$$
$$= a(mk).$$

Because $\mathbb{Z}$ is closed under multiplication, $mk \in \mathbb{Z}$. Therefore, $a|c$ by the definition of divides.

∎

◈

Often we are interested in what divisors are shared by two (or more) integers. Any pair of integers will have at least one shared positive divisor since 1 divides every integer. These shared divisors are called ***common divisors***, and the largest of the common divisors of two integers is called their ***greatest common divisor***. The definitions of these two terms are given below.

Definition 2.14: common divisor
An integer d is a ***common divisor*** of a and b if and only if $d|a$ and $d|b$.

The following theorem is a useful property of common divisors. We will use this property in Chap. 5, and you are asked to prove similar statements in Exercises 53 and 54 of this section.

Theorem 2.3
If d is a common divisor of m and n, then for any integers a and b, $d|(am + bn)$.

Proof.
Let d be a common divisor of m and n. Then by the definition of common divisor, $d|m$ and $d|n$. Therefore, by the definition of divides, $m = dk$ for $k \in \mathbb{Z}$ and $n = dl$ for $l \in \mathbb{Z}$. Substituting for m and n in the expression $am + bn$, we obtain:

$$am + bn = a(dk) + b(dl)$$
$$= d(ak + bl).$$

Since $\mathbb{Z}$ is closed under addition and multiplication, $ak + bl \in \mathbb{Z}$. Therefore, $d \mid (am + bn)$.

∎

> **Definition 2.15: greatest common divisor**
> An integer d is the **greatest common divisor of a and b** if and only if d is a common divisor of a and b and d is the largest common divisor of a and b. The notation for the **greatest common divisor of a and b** is gcd(a, b).

Notice that since 1 is a common divisor of every pair of integers (positive or negative), we only need to consider the positive divisors when looking for the greatest common divisor of two integers, since any common negative divisors will be less than 1.

Example 2.41 Find the greatest common divisors of the following pairs of numbers:

  gcd(18, 4)
  gcd(21, 4)
  gcd(16, 40)

Solution
(a) Since the positive divisors of 4 are 1, 2, and 4, the greatest common divisor will be one of these numbers. Since 4 is not a divisor of 18, but both 1 and 2 are divisors of 18, gcd(18, 4) = 2.
(b) The divisors of 4 are again 1, 2, and 4. The only value on this list that also divides 21 is 1, so gcd(4, 21) = 1.
(c) The divisors of 16 are 1, 2, 4, 8, and 16. From this list, 1, 2, 4, and 8 are also divisors of 40. Therefore, the greatest common divisor of 16 and 40 is gcd(16, 40) = 8.

◆

Example 2.42 Find gcd(124, 216).

Solution
The positive divisors of 124 are 1, 2, 4, 31, 64, and 124. The positive divisors of 216 are 1, 2, 3, 4, 6, 9, 27, 36, 54, and 72. Comparing these lists, the largest divisor on both lists is 4, so gcd(124, 216) = 4.

◆

In the examples above, we looked only at greatest common divisors of positive integers. Here is another example with negative numbers.

Example 2.43 Find gcd(12, −18).

Solution
Notice that −18 has the same positive divisors as 18: 1, 2, 3, 6, 9, and 18. The common divisors between −18 and 12 are then 1, 2, 3, and 6. Since 6 is the largest of these that also divides 12, gcd(12, −18)=6.

◈

These examples show that it is possible to find all the positive factors of each number and then look at the lists of factors to find the greatest integer common to both lists. However, as numbers become large, it may be difficult to find all of the factors. Chaps. 4 and 5 will introduce alternate methods for finding the greatest common divisor of two numbers.

Example 2.44 Formulate a conjecture about the value of gcd $(a, 0)$.

Solution
To formulate a conjecture, we will choose some values for a to look for a pattern. Try choosing a variety of values: a prime, a non-prime, and maybe a negative value.

$$a = 7$$

The positive divisors of $a = 7$ are 1 and 7, and both of these also divide 0 since $1 \cdot 0 = 0$ and $7 \cdot 0 = 0$. Therefore, gcd(7, 0)=7.

$$a = 15$$

The positive divisors of a are 1, 3, 5, and 15, and again all of these also divide 0, so gcd(15, 0)=15.

$$a = -6$$

The positive divisors of -6 are 1, 2, 3, and 6, and you have probably picked up on the pattern here. Since $0 \cdot m = 0$ for any integer m, the divisors of a will also always be divisors of 0. So, again, gcd(−6, 0)=6. Notice that in this case, gcd(−6, 0)=|−6|.

Based on the examples above, the following conjecture seems reasonable.

CONJECTURE: If a is an integer, then gcd(a, 0)=|a|.

Notice that if a is positive, then $|a| = a$, so this conjecture says that for a positive a, gcd(a, 0)=a.

◈

Example 2.45   Test the conjecture from Example 2.44 on the value $a = 0$.

Solution
If $a = 0$, we are looking for the value of $\gcd(0, 0)$. Since $a \cdot 0 = 0$ for every integer a, every integer is a divisor of 0. Therefore, there is no largest common divisor, and $\gcd(0, 0)$ does not exist. Therefore, we will revise the conjecture from Example 2.44.

   CONJECTURE: If a is an integer not equal to 0, then $\gcd(a, 0) = |a|$.

◈

   The version of the conjecture in Example 2.45 is true and is stated for positive integers in Theorem 2.4 below.

Theorem 2.4
If a is a positive integer not equal to 0, then $\gcd(a, 0) = a$.

Proof.
Let a be a positive integer that is not 0. Then, $a|a$, so a is its own largest divisor. Since $a \cdot 0 = 0$, a is a common divisor of a and 0. Therefore, $\gcd(a, 0) = a$.

■

   In Exercise 59, you are asked to look at why this proof will not work if $a = 0$.
   One particularly interesting case is when two numbers have no common divisors besides 1. When two numbers share this property, they are called ***relatively prime***. The definition is stated below.

Definition 2.16: relatively prime
Two integers a and b are ***relatively prime*** if and only if $\gcd(a, b) = 1$.

   A related topic to the greatest common divisor is the least common multiple which is defined below.

Definition 2.17: least common multiple
The integer m is the ***least common multiple*** of two integers a and b if and only if m is the smallest positive multiple of both a and b. The least common multiple is denoted by $lcm(a, b)$.

   For example, $lcm(5, 12) = 60$ since 60 is the smallest number that both numbers divide. On the other hand, $lcm(12, 18) = 36$ since both numbers divide 36 but they do not both divide any number between 18 and 36.

Exercise Set 2.8

Exercises 1–4. Rewrite each of the following statements using the notation $a|b$.
 1. 24 is a multiple of 8.
 2. 16 divides 32.
 3. 5 is a factor of 70.
 4. 7 is a divisor of 49.

Exercises 5–12. Determine whether the statement is true or false. Explain your answer.
 5. 8 divides 56.
 6. 27 is a multiple of 6.
 7. 9 is a factor of 108.
 8. 2 is a divisor of 67.
 9. 21 is a multiple of 7.
10. 7 is a multiple of 21.
11. 6 is a factor of 76.
12. 35 divides 7.

Exercises 13–19. Determine whether the statement is true or false. Justify your answer using the definition of *divides*.
13. $7|63$
14. $9|0$
15. $2|3426$
16. $14|4988$
17. $0|18$
18. $6|2$
19. $2|(4n+2)$

Exercises 20–23. Test the statement to develop a conjecture about whether it is true or false. Explain your answer.
20. If 6 divides a and 12 divides a, then 72 divides a.
21. If $2|a$ and $4|a$, then $8|a$.
22. If $2|a$ and $7|a$, then $14|a$.
23. If $6|n$, then $3|n$.

24. Find an integer d that divides 15 but does not divide 25.
25. Find an integer d that divides 20 but does not divide 26.
26. Write the contrapositive of the statement proved in Example 2.38: If 6 divides n, then 2 divides n and 3 divides n.
27. Consider the statement: "If m is not even, then m is not divisible by 4."

   (a) Write the contrapositive of the statement.
   (b) Prove the statement using an indirect proof. (In other words, prove the original statement by proving its contrapositive).

Exercises 28–38. Find the greatest common divisor.
28. gcd(42, 130)
29. gcd(15, 421)
30. gcd(3289, 561)
31. gcd(45, 75)
32. gcd(4, 67)
33. gcd(183, 27)
34. gcd(513, 315)
35. gcd(432, 234)
36. gcd(803, 154)
37. gcd(235, 5665)
38. gcd(34, 35)

Exercises 39–49. Find the least common multiple of each pair of numbers from Exercises 28–38.

50. Find a value for a so that a and 12 are relatively prime.
51. Find a counterexample to the following statement, and explain your example:

    If a $\nmid$ b and b $\nmid$ a, then a and b are relatively prime.

52. For what integers a is $1|a$ true? Justify your answer.
53. Prove that if $d|m$ and $d|n$, then $d|(m+n)$.
54. Prove that if $d|m$ and $d|n$, then $d|(m-n)$.
55. Prove that if a is an integer, then $a|0$.
56. Consider the following conjecture:
    CONJECTURE: If $a|b$ and $b|c$, then $a|(b+c)$.

    (a) Try some examples to determine whether the conjecture seems to be true or false.
    (b) Either prove the conjecture true, or give a counterexample to show it is false.

57. Consider the following conjecture:
    CONJECTURE: If $a|b$ and $b|c$, then $ab|c$.

    (a) Try some examples to determine whether the conjecture seems to be true or false.
    (b) Either prove the conjecture true, or give a counterexample to show it is false.

58. Consider the following conjecture:
    CONJECTURE: If $a|m$ and $b|m$, then $ab|m$.

    (a) Try some examples to determine whether the conjecture seems to be true or false.
    (b) Either prove the conjecture true, or give a counterexample to show it is false.

59. (a) Rewrite the proof of **Theorem 2.3** in the column form introduced in
       Section 2.5.
    (b) Explain why the proof of **Theorem 2.3** fails if $a = 0$.

60. Rewrite the proof of Example 2.38 in paragraph form.
61. When is it true that $a|b$ and $b|a$? Explain.
62. The following statement is false: If $a|c$ and $b|c$ then $ab|c$. Find a counterexample and explain your example.
63. Prove that the sum of three consecutive even integers is divisible by six.
64. Prove that the product of three even numbers is divisible by eight.
65. Prove that if $a \in \mathbb{Z}$, then $a|a^2$.
66. Prove that if $a|b$, then $-a|b$.
67. Prove that if $a|b$ and $c|d$, then $ac|bd$.
68. If a, b, c, and d are integers, prove that if $d|a$ and $d|b$, then $d^2|ab$.
69. (a) Fill in the table below and make a conjecture about the relationship among
       the values in each row.

a	b	$\gcd(a, b)$	$lcm(a, b)$	ab
3	7			
4	26			
24	48			
15	35			
36	142			
101	123			

    (b) Test the conjecture from part a) on two more pairs of integers.
    (c) If the conjecture in a) is true, how could it be used?

70. Find the $lcm(m, m+1)$ for any positive integer m.
71. What is the value of $lcm(0, 5)$? Explain your answer.
72. What is the value of $lcm(0, 0)$? Explain your answer.

2.9 Divisibility Rules

In this section, we state some divisibility rules that can be used to test whether or not one integer is divisible by another. They will be used throughout the textbook, so they are listed here for reference. Some are probably familiar and others may be new. It is often useful to be able to quickly check to see whether a particular integer divides another. You will see that some of the rules will simplify this work, while others are more complicated. We will state them using the term *divides* which was defined in Section 2.8. Also, notice that each of these rules is an "if and only if" statement.

Let *a* be any integer:

$2|a$ if and only if the last digit of *a* is even (0, 2, 4, 6, 8).

$3|a$ if and only if the sum of the digits of *a* is divisible by 3.

$4|a$ if and only if the number formed from the last two digits of *a* is divisible by 4.

$5|a$ if and only if the last digit of *a* is 0 or 5.

$6|a$ if and only if $2|a$ and $3|a$.

$7|a$ if and only if when you double the last digit of *a* and subtract that from the number that remains after removing the last digit of *a*, that value is divisible by 7.

$8|a$ if and only if the number formed by the last three digits of *a* is divisible by 8.

$9|a$ if and only if the sum of the digits of *a* is divisible by 9.

$10|a$ if and only if the last digit of *a* is a 0.

$11|a$ if and only if the number formed by alternately subtracting and adding the digits of *a* is divisible by 11.

$12|a$ if and only if $3|a$ and $4|a$.

The most complicated tests on this list are the ones for checking divisibility by 7 and by 11. They are less useful than the others because they are more complex and harder to remember, but it may be interesting to think about why all of these tests work. The tests for 7 and 11 are illustrated in the examples below.

Example 2.46 Does $7|1876$?

Solution
Using the divisibility test, we need to know if 7 divides the number $187 - 2(6) = 175$. Since 175 is still fairly large, we can apply the test again to get $17 - 2(5) = 7$. It is true that $7|7$, and therefore $7|1876$.

◈

Example 2.47 Does $11|5212$?

Solution
Applying the divisibility test for 11, form the number $5 - 2 + 1 - 2 = 2$. Since 11 does not divide 2, $11 \nmid 5212$ either.

◈

Example 2.48 According to the divisibility test for 12, it is enough to check that a number is divisible by both 3 and 4 to ensure divisibility by 12. Test the following conjecture for an alternate divisibility test for 12.

CONJECTURE: If $2|a$ and $6|a$, then $12|a$.

Solution

To test this statement, choose some values for a that make the condition "$2|a$ and $3|a$" true. If the conclusion that $12|a$ also holds true, this is evidence supporting the conjecture. If we find an example where the conclusion is false, then we have a counterexample.

Let us try $a = 6$. Then the condition is true since $2|6$ and $3|6$. However, $12|6$ is false since $6 = 12\left(\frac{1}{2}\right)$ and $\frac{1}{2} \notin \mathbb{Z}$. Therefore, the conjecture is false, and $a = 6$ is a counterexample.

◈

Exercise Set 2.9

Exercises 1–9. Determine whether 516 is divisible by each of the following numbers using the divisibility tests in this section.

1. 2
2. 3
3. 4
4. 5
5. 6
6. 7
7. 8
8. 9
9. 11

10. Let p and q be the statements below:

$p : n$ is divisible by 3.
$q : n$ is divisible by 9.

   (a)   Form the statement $p \Rightarrow q$ and determine whether it is true or false. If it is false, provide a counterexample.
   (b)   Form the statement $q \Rightarrow p$ and determine whether it is true or false. If it is false, provide a counterexample.
   (c)   What do parts (a) and (b) tell you about the truth value of $p \Leftrightarrow q$?

11. Let p and q be the statements below:

$p : n$ is divisible by 2.
$q : n$ is divisible by 6.

(a) Form the statement $p \Rightarrow q$ and determine whether it is true or false. If it is false, provide a counterexample.

(b) Form the statement $q \Rightarrow p$ and determine whether it is true or false. If it is false, provide a counterexample.

(c) What do parts (a) and (b) tell you about the truth value of $p \Leftrightarrow q$?

12. Which of the following numbers are divisible by 9?

(a) 784
(b) 7,668
(c) 1,327
(d) 8,964

13. Which of the following numbers are divisible by 3?

(a) 657
(b) 791
(c) 3,334
(d) 3,336

Exercises 14–21. Determine whether the statement is true or false, and explain.

14. 137 is a prime number.
15. 141 is a prime number.
16. 149 is a prime number.
17. 151 is a prime number.
18. 153 is a prime number.
19. 119 is a prime number.
20. 861 is a prime number.
21. 2,401 is a prime number.

22. Use the divisibility test to determine whether 3,459 is divisible by 11.
23. Use the divisibility test to determine whether 4,675 is divisible by 11.

2.10 Summary and Review Exercises

2.10.1 Vocabulary and Symbols

integers, $\mathbb{Z}$	conditional statement, $p \Rightarrow q$
whole numbers	biconditional statement, $p \Leftrightarrow q$
$\in$	logically equivalent
divisible	even
twin primes	odd
Mersenne primes	prime
perfect number	closed
Goldbach's Conjecture	Closure of $\mathbb{Z}$ Axiom

(continued)

inductive reasoning	direct proof
conjecture	converse
deductive reasoning	contrapositive
premises	indirect proof
proof	counterexample
truth value	divides
negation, $\sim$	common divisor
conjunction, $p \wedge q$	greatest common divisor
disjunction, $p \vee q$	least common multiple
	relatively prime

2.10.2   Suggested Readings

Dodge, Clayton W. *What is a Proof*? **Pi Mu Epsilon Journal** Vol. 10, (Fall, 1998) pp 725–727.

   Lamport, Leslie. *How to Write a Proof.* **The American Mathematical Monthly.** Vol. 102, (Aug–Sept, 1995) pp 600–608.

2.10.3   Review Exercises

1. What does each symbol represent?
      $\Leftrightarrow$, $\wedge$, $\vee$, $\Rightarrow$, $\sim$, $\mathbb{Z}$
2. Write the following statement symbolically using *p: n is an integer* and *q: n^2 is negative*.

   If *n* is an integer, then n^2 is not a negative number.

3. Explain the difference between *a|b* and *a/b*. Give an example of each.
4. Give an example of two non-prime integers that are relatively prime.

Exercises 5–9.   Write the contrapositive of the statement, eliminating any occurrences of "not not." Then state whether the pair of statements is true or false.

5. If *n* is odd, then 2 does not divide *n*.
6. If *n* is even, then 2 does not divide *n*.
7. If *a* and *b* are even, then the product *ab* is divisible by 4.
8. If *n* is prime, then *n* is odd.
9. If *n* is odd, then *n* is prime.

10. Label each of the following statements as true or false. If false, give a counterexample. If the statement is true, provide a proof.

(a)   If 10 divides ab, then 10 divides a or 10 divides b.
(b)   If $a|b$, then $a^2|b^2$.
(c)   If 4 divides ab, then $4|a$ or $4|b$.

11. Find the greatest common divisor and the least common multiple of each of the following pairs of integers:

(a)   216, 288
(b)   675, 1125
(c)   234, 233
(d)   356, 32

12. Find all $d > 0$ such that $18|d$ and $d|216$.
13. Find all $d > 0$ such that $20|d$ and $d|300$.
14. If p and q are distinct primes, find all positive divisors of pq.
15. Find the smallest integer $n > 0$ such that n has exactly 6 divisors.
16. Prove or disprove the following conjecture:
    CONJECTURE: If $b|c$, then $\gcd(a, b) \le \gcd(a, c)$.
17. Prove that a and $-a$ have the same divisors and the same multiples.
18. Prove that zero is an even number.
19. Prove that if $a|b$ and $a|c$, then $a|(b+c)$.
20. Prove that the square of an even number is even.
21. Prove that the sum of any three odd numbers is an even number.
22. Prove that the product of any two even numbers is an even number.
23. Prove that the product of any two consecutive integers is even.
24. Is the square of an odd number always odd or can it be an even number? Prove your answer.
25. Prove that the sum of two consecutive odd primes is never twice a prime. (Hint: Try some examples to convince yourself this is true. To prove it, try a proof by contradiction).

2.10.4   Activities

1. *Multi-Sudoku Puzzles*

The game of *Multi-Sudoku* is an extension of the usual Sudoku game. In Multi-Sudoku, the numbers in the grid are d, $2d$, $3d$, ..., $9d$, where $d > 1$ is a common factor for all of the nine numbers. Thus, the goal is to fill in each row, each column, and each 3 by 3 subset with the values d, $2d$, $3d$, ..., $9d$. Your first task is to find the greatest common divisor of all of the entries in the grid. Next, use any puzzle-solving strategy for ordinary Sudoku puzzles to solve the Multi-Sudoku puzzles below.

10		16			6			18
14	8	6	16			4		10
		18		10				
	10	14			4	2		
8					10		16	
16			14	2				4
	18		10					
		10	6	12	16	8		2
6		2	18		8	14		

Puzzle 1

		12				6		
		27	6		12	24		
15				24			9	27
	6	21	12		24		18	
		18				9		
	27		9		15		12	
24	18			12			6	21
		9	15		18	27		
		15				18		

Puzzle 2

2. Now, create your own Multi-Sudoku puzzle and challenge your friends to solve the puzzle.

Chapter 3
Pythagorean Triples

I had this rare privilege of being able to pursue in my adult life, what had been my childhood dream.

—Andrew Wiles, 1953–present

3.1   Review of Right Triangles and the Pythagorean Theorem

This chapter begins with a brief review of right triangle geometry, before exploring how these triangles come up in number theory. Triangles such as the two pictured below, in which one angle is a right angle, or a 90° angle, are called ***right triangles***. Remember from geometry that the side opposite the right angle is called the ***hypotenuse***, and the other two sides are called the ***legs*** of the right triangle.
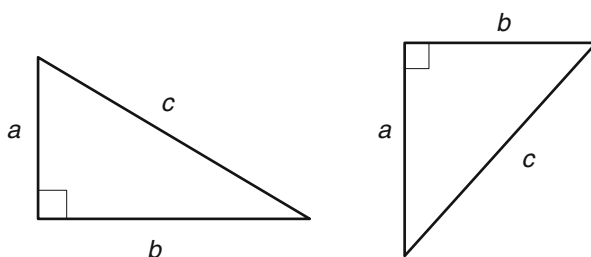

You may also remember the "special triangles" such as the $45° - 45° - 90°$ or the $30° - 60° - 90°$ triangles, where you can find the lengths of two missing sides if you know the length of one side. However, the most familiar property of right triangles is the Pythagorean Theorem, which is used to find a missing side of any right triangle when the lengths of the other two sides are known.

The well-known theorem says:

Theorem 3.1 Pythagorean Theorem
If a and b are the lengths of the two legs of a right triangle, and c is the length of the hypotenuse, then $a^2 + b^2 = c^2$.

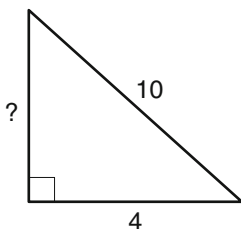**Example 3.1** Find the missing side of the right triangle below.
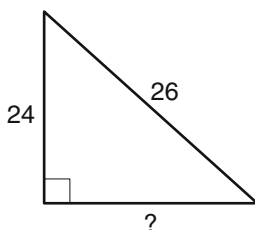
Solution
The Pythagorean Theorem can be used to find the missing side. Since one of the legs is missing, we will let b be the unknown, the other leg, $a = 24$, and the hypotenuse, $c = 26$. Substituting into the Pythagorean Theorem gives:

$$24^2 + b^2 = 26^2$$
$$576 + b^2 = 676$$
$$b^2 = 676 - 576$$
$$b^2 = 100$$
$$b = 10$$

Therefore, the length of the missing side is 10.

◈

Example 3.2 Find the missing side of the right triangle below.

Solution
Use the Pythagorean Theorem to find the missing side. Since one of the legs is missing, we will let b be the unknown, the other leg, $a = 4$, and the hypotenuse, $c = 10$. Substituting into the Pythagorean Theorem, we get:

$$4^2 + b^2 = 10^2$$
$$16 + b^2 = 100$$
$$b^2 = 100 - 16$$
$$b^2 = 84$$
$$b = \sqrt{84} \approx 9.17$$

Therefore, the length of the missing side is $\sqrt{84}$, or about 9.17.

◈

The Pythagorean Theorem can also be used to form a test to determine whether or not a triplet of three numbers forms the sides of a right triangle. This test is stated here.

Right Triangle Test
Suppose you have three positive numbers, a, b, and c, with c bigger than both a and b:

1. If $a^2 + b^2 = c^2$, then the numbers a, b, and c form the sides of a right triangle.
2. If $a^2 + b^2 \neq c^2$, then the numbers a, b, and c **do not** form the sides of a right triangle.

Note that the part 1 of the Right Triangle Test is the converse of the Pythagorean Theorem. While the converse of a statement is not always true, the converse of the Pythagorean Theorem is true. The proof is included as Exercise 36. Part 2 of the Right Triangle Test is the contrapositive of the Pythagorean Theorem. Recall from Section 2.6 that the contrapositive of a true statement is also true.

Right triangles are often identified by their three sides, so we will write the triangle with legs a and b, and hypotenuse c, as the triple $a - b - c$.

From Example 3.2 above, one can see that the lengths of sides of right triangles do not have to be integers. Since number theory only deals with whole numbers, we are interested in the right triangles whose sides are all whole numbers.

Right triangles whose sides are whole numbers are sometimes called ***Pythagorean triangles***, and triples of integers $a - b - c$ that represent Pythagorean triangles are called ***Pythagorean triples***. These terms will be used interchangeably since each Pythagorean triple represents a Pythagorean triangle. The formal definition is given below.

Definition 3.1: Pythagorean triple

The triple of positive integers $a - b - c$ is a ***Pythagorean triple*** if and only if $a^2 + b^2 = c^2$.

One such triangle appeared in Example 3.1. Are there more right triangles whose sides are all integers? The answer, of course, is YES! At this point, some people may be thinking of $3 - 4 - 5$. Is anyone thinking of $20 - 21 - 29$?

Example 3.3 Use the Right Triangle Test to confirm that $3 - 4 - 5$ and $20 - 21 - 29$ are both right triangles. Then determine whether or not $6 - 13 - 17$ is a right triangle.

Solution
Since $3^2 + 4^2 = 9 + 16 = 25$, and $5^2 = 25$, $3 - 4 - 5$ is a right triangle and also a Pythagorean triangle or Pythagorean triple, since the sides are integers.

Since $20^2 + 21^2 = 841$, and $29^2 = 841$, $20 - 21 - 29$ is a right triangle and also a Pythagorean triple.

Since $6^2 + 13^2 = 205$, and $17^2 = 289$, $6 - 13 - 17$ **does not** form a right triangle.

◈

Now that you know there are at least three Pythagorean triples (or right triangles with whole number sides), some other questions come up right away. You may be able to add some more questions to the list:

Question 1 How many Pythagorean triples are there?

Question 2 Is there a formula to find Pythagorean triples?

Starting with a Pythagorean triple such as $3 - 4 - 5$, we can create more Pythagorean triples by multiplying each side by the same number.

Example 3.4 Show that $6 - 8 - 10$ and $9 - 12 - 15$ are also Pythagorean triples, and explain how they are related to the Pythagorean triple $3 - 4 - 5$.

Solution
Since $6^2 + 8^2 = 36 + 64 = 100$, and $10^2 = 100$, $6 - 8 - 10$ is a Pythagorean triple.

$6 - 8 - 10$ came from multiplying the lengths of each side of the $3 - 4 - 5$ triangle by 2.

Since $9^2 + 12^2 = 81 + 144 = 225$, and $15^2 = 225$, $9 - 12 - 15$ is a Pythagorean triple.

$9 - 12 - 15$ came from multiplying the lengths of each side of the $3 - 4 - 5$ triangle by 3.

◈

From the example above, we can see that even though we have three different right triangles, they are all related. In geometry, triangles with this type of relationship are called ***similar*** triangles. When the word "similar" is in italics, it will

indicate we are using it in the geometry sense. *Similar* triangles are triangles that have the same basic shape but are of different sizes. *Similar* triangles have the same angles, and corresponding sides are proportional. This means that to get from the sides of one triangle to the sides of a *similar* triangle, you simply multiply (or divide) the three sides by the same number.

A list of triangles *similar* to the right triangle $3 - 4 - 5$ can be found by multiplying the sides by each positive integer k. Exercise 33 asks you to show that if k is a positive integer, then the triple $3k - 4k - 5k$ is a Pythagorean triple, and therefore, there is another Pythagorean triple *similar* to the triangle $3 - 4 - 5$ for each integer $k > 1$.

In fact, if $a - b - c$ is any Pythagorean triple, then if we multiply the sides by a common positive integer, we will get another (*similar*) Pythagorean triple. This result is stated in Theorem 3.2.

Theorem 3.2
If $a - b - c$ is a Pythagorean triple and k is a positive integer, then $(ka) - (kb) - (kc)$ is also a Pythagorean triple.

Proof.   Let $a - b - c$ be a Pythagorean triple. Then $a^2 + b^2 = c^2$. If k is a positive integer, then

$$(ka)^2 + (kb)^2 = k^2 a^2 + k^2 b^2$$
$$= k^2 (a^2 + b^2)$$
$$= k^2 (c^2)$$
$$= (kc)^2$$

Therefore, $(ka) - (kb) - (kc)$ is a Pythagorean triple.

∎

The converse of this theorem is also true. Starting with a Pythagorean triple and factoring out a common factor will result in values that will also form a Pythagorean triple.

Theorem 3.3
If $a - b - c$ is a Pythagorean triple and k is a positive common divisor of a, b, and c, then the triple resulting from factoring k out of a, b, and c will still be a Pythagorean triple.

Proof. Let $a - b - c$ be a Pythagorean triple, and let k be a positive common divisor of a, b, and c. Then, by the definition of common divisor:

$$k \,|\, a,$$
$$k \,|\, b,$$
$$k \,|\, c$$

By the definition of divides,

$$a = km \text{ for } m \in \mathbb{Z},$$
$$b = kn \text{ for } n \in \mathbb{Z},$$
$$c = kl \text{ for } l \in \mathbb{Z}$$

By the definition of Pythagorean triple, $a^2 + b^2 = c^2$. Therefore, substituting and simplifying, we obtain:

$$(km)^2 + (kn)^2 = (kl)^2$$
$$k^2 m^2 + k^2 n^2 = k^2 l^2$$
$$k^2 (m^2 + n^2) = k^2 l^2$$

Since k is a positive integer, $k^2 \neq 0$. Therefore,

$$m^2 + n^2 = l^2.$$

Therefore, by the definition of Pythagorean triple, the triple $m - n - l$ resulting from factoring k out of $a - b - c$ is a Pythagorean triple.

∎

This answers *Question 1*: there are infinitely many Pythagorean triples. However, our answer is not completely satisfying because the new Pythagorean triangles we have found are all *similar* to ones already known.

Let us rewrite the first question as follows:

Question 1 How many Pythagorean triples are there that are not *similar* to each other?

At this point, let us also update *Question 2*. Since we can always get *similar* triangles by multiplying all three sides by the same number, we are most interested in a formula that will produce *non-similar* Pythagorean triples.

Question 2 Are there formulas to find *non-similar* Pythagorean triples?

Both of these questions will be answered in Section 3.2.

So far, we have found two *non-similar* Pythagorean triples: $3 - 4 - 5$ and $20 - 21 - 29$. Can you come up with a few others on your own?

In order to easily tell when two triangles are *similar* as well as describe when they are not *similar*, we need the idea of common factors, or common divisors, discussed in Chap. 2.

From Example 3.4, we know that $6-8-10$ is a right triangle *similar* to $3-4-5$, and that $6-8-10$ came from multiplying each side of $3-4-5$ by 2. In fact, 2 is the largest integer that divides all three sides of the $6-8-10$ triangle. In the next definition, the idea of the greatest common divisor of two numbers is extended to more than two numbers.

Definition 3.2: greatest common divisor

A collection of integers, $a, b, c, \ldots$, has a ***common divisor d*** if d divides every integer in the collection. The largest of the common divisors is the ***greatest common divisor of a, b, c,*** ....

We will use the same notation for greatest common divisors of more than two numbers, so the greatest common divisor of the numbers 6, 8, and 10 is written $\gcd(6,\ 8,\ 10) = 2$.

Being able to find the common divisors of three numbers is useful in the search for *non-similar* Pythagorean triples. Since *similar* triangles have sides that are proportional, triangles whose sides share a common factor greater than 1 are *similar* to triangles where the common divisor has been factored out.

Example 3.5 Find the greatest common divisor of each collection of numbers below:

(a) $\gcd(4,\ 6,\ 10)$
(b) $\gcd(3,\ 5,\ 15)$
(c) $\gcd(16,\ 24,\ 40)$

Solution
(a) $\gcd(4,\ 6,\ 10) = 2$, since 2 is the largest number that divides all three of the numbers in the list.
(b) Even though 3 is a divisor of both 3 and 15, and 5 is a divisor of both 5 and 15, the greatest common divisor between all three numbers is 1, so $\gcd(3,\ 5,\ 15) = 1$.
(c) Right away, notice that 2 is a common divisor of these three numbers. One way to ensure getting the greatest common divisor is to list all divisors of each number.

Divisors of 16:	1,	2,		4,			8,		16	
Divisors of 24:	1,	2,	3,	4,		6,	8,		12,	24
Divisors of 40:	1,	2,		4,	5,		8,	10,	20,	40

From the chart above, we can see that 1, 2, 4, and 8 are all common divisors of these three numbers, and the largest common divisor is 8, so $\gcd(16, 24, 40) = 8$.

◆

In the examples above, notice that as the numbers get larger, it is harder to tell whether or not you have found the greatest common divisor. Listing out all divisors of each number and then comparing the lists will always work to find the greatest common divisor, but it will become very cumbersome for larger numbers. In Chaps. 4 and 5, other methods to find greatest common divisors will allow us to work more easily with larger numbers.

Example 3.6 Show that $18 - 24 - 30$ is a Pythagorean triple. Then find two *similar* triangles by factoring out common divisors.

Solution
First, since $18^2 + 24^2 = 900$ and $30^2 = 900$, $18 - 24 - 30$ is a Pythagorean triple.

Since 3 is a common divisor of 18, 24, and 30, factor out a 3 to get the triangle $6 - 8 - 10$. Since this triangle is *similar* to $18 - 24 - 30$, we know it is also a Pythagorean triple.

Since 2 is also a common divisor of 18, 24, and 30, factor out a 2 to get the Pythagorean triple $9 - 12 - 15$.

Note that Theorem 3.3 says that these new triples are also Pythagorean triples.

◆

Notice that for each of the *similar* triangles found above, the sides do not have a greatest common divisor of 1. That is because we factored out common divisors, but not the greatest common divisor of 18, 24, and 30. The greatest common divisor of these three numbers is $\gcd(18, 24, 30) = 6$, and factoring out a 6 produces another *similar* triangle $3 - 4 - 5$, which has $\gcd(3, 4, 5) = 1$. We will focus on Pythagorean triples with this property in the next section.

Exercise Set 3.1

Exercises 1–5. Find the missing side of the right triangle with legs a and b, and hypotenuse c. Note: In this problem, all sides of triangles are not necessarily integers.
  1. $a = $?, $b = 7$, $c = 12$
  2. $a = 16$, $b = $?, $c = 34$
  3. $a = 5$, $b = 6$, $c = $?
  4. $a = 11$, $b = 15$, $c = $?
  5. $a = 4$, $b = $?, $c = 5$

  6. State the converse of the Pythagorean Theorem.
  7. State the contrapositive of the Pythagorean Theorem.

Exercises 8–13. Use the Right Triangle Test to determine whether the triple is a Pythagorean triple. In each case, state whether you are using the converse or the contrapositive of the Pythagorean Theorem.

8. $4 - 5 - 6$
9. $25 - 60 - 65$
10. $11 - 60 - 61$
11. $8 - 15 - 17$
12. $32 - 44 - 56$
13. $10 - 15 - 25$

14. (a) Show that $a = \frac{3}{2}$, $b = 2$, $c = \frac{5}{2}$ give the sides of a right triangle.
    (b) Explain why the values for a, b, and c above are not a Pythagorean triple.
    (c) Find a Pythagorean triple that is similar to the triangle in (a).
15. (a) Show that $27 - 36 - 45$ is a Pythagorean triple.
    (b) Find two Pythagorean triangles similar to $27 - 36 - 45$: one whose corresponding sides are longer and one whose corresponding sides are shorter.
16. (a) Show that $30 - 72 - 78$ is a Pythagorean triple.
    (b) Find all possible similar Pythagorean triples with corresponding sides shorter than $30 - 72 - 78$.
    (c) Find one similar Pythagorean triple with corresponding sides longer than $30 - 72 - 78$.
17. (a) Show that $24 - 32 - 40$ is a Pythagorean triple.
    (b) Find all possible similar Pythagorean triples with corresponding sides shorter than $24 - 32 - 40$.
    (c) Find one similar Pythagorean triple with corresponding sides longer than $24 - 32 - 40$.
18. Given the Pythagorean triple $a = 15$, $b = 8$, $c = 17$, find two more: one where side a is less than 50 and one where side a is greater than 50.
19. Find a Pythagorean triple with $c > 250$.
20. Find a Pythagorean triple with $b > 100$.

Exercises 21–30. Find the greatest common divisor of each collection of numbers.
21. gcd(10, 20, 25)
22. gcd(4, 8, 15)
23. gcd(12, 8, 6)
24. gcd(385, 435, 660)
25. gcd(6, 8, 25)
26. gcd(11, 21, 31)
27. gcd(21, 33, 66)
28. gcd(28, 42, 14)
29. gcd(15, 45, 54)
30. gcd(231, 273, 399)

31. Combine **Theorem 3.2** and **Theorem 3.3** into one "if and only if" statement.
32. Rewrite the proof of **Theorem 3.2** in the column format introduced in Section 2.5.
33. Prove that if k is a positive integer, then $(3k) - (4k) - (5k)$ is a Pythagorean triple.

34. Consider the following conjecture.
    CONJECTURE: If $\gcd(a, b) = d$ and $d|c$, then $\gcd(a, b, c) = d$.

    (a) Test the conjecture on three different choices for a, b, and c.
    (b) Either prove the conjecture true, or clearly explain how you know it is false.

35. Prove that if $\gcd(a, b) = d$ and $\gcd(b, c) = d$, then $\gcd(a, b, c) = d$.
36. The converse of the Pythagorean Theorem states that if $a^2 + b^2 = c^2$, then a, b, and c are the sides of a right triangle (with c the hypotenuse). Prove that this is true. (Hint: Form a right triangle with legs a and b. Then show that the triangle must have a hypotenuse of c).

3.2   Primitive Pythagorean Triples

In the last section, we saw that if all three sides of a right triangle are multiplied or divided by a common factor, the result is a right triangle *similar* to the original triangle. Therefore, two Pythagorean right triangles, each of whose sides has a greatest common divisor of 1, will not be *similar*, because they cannot be obtained from each other by multiplying or dividing by a common factor.

Since the goal is to answer the question of how many *non-similar* Pythagorean triangles there are, in this section we will study Pythagorean triples $a - b - c$, where $\gcd(a, b, c) = 1$. Pythagorean triples of this type are called primitive Pythagorean triples. Here is the formal definition.

Definition 3.3: primitive Pythagorean triple (PPT)

The triple of positive integers $a - b - c$ is a ***primitive Pythagorean triple*** if and only if $a^2 + b^2 = c^2$ and the greatest common divisor of a, b, and c is 1, written as $\gcd(a, b, c) = 1$. A primitive Pythagorean triple is abbreviated as PPT.

A ***primitive Pythagorean triangle*** is a triangle whose side lengths form a primitive Pythagorean triple, so the two terms are used interchangeably.

Example 3.7 Find a primitive Pythagorean triple that is similar to the Pythagorean triple $42 - 144 - 150$.

Solution
Since $\gcd(42, 144, 150) = 6$, the triple $7 - 24 - 25$ obtained by dividing each side of $42 - 144 - 150$ by 6 is a similar triangle and a primitive Pythagorean triple.

Since Theorem 3.3 tells us that $7 - 24 - 25$ will still be a Pythagorean triple, we do not have to check separately that $7^2 + 24^2 = 25^2$.

◈

Notice that *Questions 1 and 2* from the last section can now be rephrased as:

Question 1 How many primitive Pythagorean triples are there?

Question 2 Are there formulas that will always produce primitive Pythagorean triples?

One example of a primitive Pythagorean triple is $3 - 4 - 5$, since $gcd(3, 4, 5) = 1$, and $3^2 + 4^2 = 5^2$.

Table 3.1 provides more examples of primitive Pythagorean triples.

Table 3.1 Primitive Pythagorean triples

a	b	c
3	4	5
5	12	13
21	20	29
15	8	17
7	24	25

Test each of these examples to confirm that they are in fact primitive Pythagorean triples. (Remember there are two things to check: first, that they satisfy $a^2 + b^2 = c^2$ and second, that $gcd(a, b, c) = 1$).

Now, can you find another primitive Pythagorean triple? What about two more? Ten more? How will we know when all of them have been found? In order to know whether we have all primitive Pythagorean triples, a systematic approach to finding them is needed. Here are some questions to answer. The first two are the questions from the end of the previous section.

Question 1 How many primitive Pythagorean triples are there? If there is a fixed number of possible primitive Pythagorean triples—maybe 100 or 1,000 or 12,000,000—mathematicians call that **finitely many**. If that is the case, then we can actually write them all down and the list will come to an end. On the other hand, if the list of different primitive Pythagorean triples is endless, there are **infinitely many**.

Question 2 Are there formulas that will always produce primitive Pythagorean triples? (Is it possible to find formulas for a, b, and c so that the formulas always produce values that form a PPT?)

Question 3 If the answer to *Question 2* above is "yes," then is there a set of formulas that will produce all possible primitive Pythagorean triples?

Question 4 Do the primitive Pythagorean triples follow any patterns? From the definition, if $a - b - c$ is a PPT, then $a^2 + b^2 = c^2$ and $gcd(a, b, c) = 1$, but are there any other common properties that all PPTs share?

Starting with the last question, let us look for patterns in Table 3.1. If there is a pattern that all primitive Pythagorean triples must follow, we may be able to use it to define formulas. Having equations that always give primitive Pythagorean triples would make it much easier to find more.

Here are some examples of possible conjectures based on the PPTs in Table 3.1.

> **Conjecture 3.1:** The hypotenuse of a PPT is always odd.

> **Conjecture 3.2:** At least one side of a PPT must be prime.

> **Conjecture 3.3:** The greatest common divisor of any two sides of a PPT is 1.

Notice that **Conjecture 3.3** is not the same as the definition which says that the greatest common divisor of all three sides is 1. Exercise 19 asks you to find an example where $\gcd(a, b, c) = 1$, but none of $\gcd(a, b)$, $\gcd(b, c)$, and $\gcd(a, c)$ are 1.

> **Conjecture 3.4:** One side of a PPT is even, and the other two sides are odd.

> **Conjecture 3.5:** The even side of a PPT is always divisible by 4.

Before using these conjectures to try to find formulas for PPTs, we need to know whether they are true or false. To prove any of these conjectures false, we need a counterexample. To prove a conjecture true requires a general proof showing that the statement is true for all primitive Pythagorean triples. Although additional examples will never give us a proof, they can provide support for suspecting it is true.

Example 3.8

(a) Verify that the triple $63 - 16 - 65$ is a primitive Pythagorean triple.
(b) Test each of the five conjectures above to see if they are true or false for the PPT $63 - 16 - 65$.

Solution
(a) Since $63^2 + 16^2 = 4225$ and $65^2 = 4225$, $63 - 16 - 65$ is a Pythagorean triple.

Now, to show $\gcd(63, 16, 65) = 1$. Starting with 16 (because it is the smallest), the positive divisors of 16 are 1, 2, 4, 8, and 16. Only 1 divides 63 and 65, so the only common divisor for all three numbers is 1. Therefore, $\gcd(63, 16, 65) = 1$.

(b) Now we will test each conjecture on the PPT $63 - 16 - 65$.

Test **Conjecture 3.1:** This conjecture is true for this example since the hypotenuse, 65, is odd.

Test **Conjecture 3.2:** This conjecture is **false**, since none of 63, 16, or 65 are prime numbers. Therefore, we have found a counterexample for **Conjecture 3.2**.

Test **Conjecture 3.3:** Checking every pair of sides, $\gcd(63, 16) = 1$, $\gcd(16, 65) = 1$, and $\gcd(63, 65) = 1$, so this conjecture is true in this example.

Test **Conjecture 3.4:** This conjecture is true for this example since 16 is even while 63 and 65 are both odd.

Test **Conjecture 3.5:** Since 16 is divisible by 4, this conjecture is true for this example.

◆

In the next section we will prove that the answers to both **Question 2** and **Question 3** are yes: there are formulas which always produce PPTs and every primitive Pythagorean triple can be found using these formulas. This will also give us the answer to **Question 1**: since each time a different value is substituted into the formulas, we obtain a different primitive Pythagorean triple; there are infinitely many.

Before that, though, we will introduce formulas that generate primitive Pythagorean triples so that you can see how useful they are. For the remainder of this section, we will work with these formulas. There are two components to the formulas to generate primitive Pythagorean triples: the actual equations for a, b, and c and the rules explaining what integers can be substituted into the equations to produce PPTs.

Formulas for Primitive Pythagorean Triples

Choose integers s and t using the following rules:

  (i) s and t are odd.
  (ii) $s > t \geq 1$.
  (iii) $\gcd(s, t) = 1$ (in words, s and t are relatively prime).

Then, if

$$a = st, \qquad b = \frac{s^2 - t^2}{2}, \qquad c = \frac{s^2 + t^2}{2},$$

$a - b - c$ is a primitive Pythagorean triple.

Theorem 3.4

If s and t are odd integers such that $s > t \geq 1$, $\gcd(s, t) = 1$, and $a = st$,

$b = \dfrac{s^2 - t^2}{2}$, and $c = \dfrac{s^2 + t^2}{2}$, then $a - b - c$ is a primitive Pythagorean triple.

For now, we will simply confirm that values for a, b, and c chosen in this way are actually a Pythagorean triple.

Partial Proof. Suppose that s and t are odd, positive integers such that $\gcd(s, t) = 1$ and $s > t$.

Let a, b, and c be integers such that $a = st$, $b = \dfrac{s^2 - t^2}{2}$, and $c = \dfrac{s^2 + t^2}{2}$.

Step 1 *Show that a, b, and c are all positive integers.*

First, since s and t are both odd, s^2 and t^2 are also both odd. Therefore the sum and difference, $s^2 + t^2$ and $s^2 - t^2$, are even. This means that b and c will both be integers. Since a is just the product of two integers, a is also an integer. (This shows why the first condition on s and t is needed.)

Second, since $s > t$, $s^2 - t^2 > 0$, so b will be positive. Since s and t are both positive, they are both at least 1, so a and c will also be positive.

Step 2 *Show that $a^2 + b^2 = c^2$.*

Substituting the formulas for a and b into $a^2 + b^2$ gives the following:

$$
\begin{aligned}
a^2 + b^2 &= (st)^2 + \left(\tfrac{s^2 - t^2}{2}\right)^2 \\
&= s^2 t^2 + \frac{s^4 - 2s^2 t^2 + t^4}{4} \\
&= \frac{4s^2 t^2 + s^4 - 2s^2 t^2 + t^4}{4} \\
&= \frac{s^4 + 2s^2 t^2 + t^4}{4} \\
&= \frac{(s^2 + t^2)^2}{4} \\
&= \left(\tfrac{s^2 + t^2}{2}\right)^2 \\
&= c^2
\end{aligned}
$$

■

Notice that only two of the three conditions on s and t have been used: we needed them to both be odd so that b and c would be integers, and we needed $s > t \geq 1$ so that we would get positive integers for a, b, and c, the sides of the triangle. (If t were larger than s, then b would be negative.)

What about the condition that $\gcd(s, t) = 1$? In fact, choosing $s = 9$ and $t = 3$ and applying the formulas results in the following triple:

$$a = 27, \quad b = \frac{81 - 9}{2} = 36, \quad c = \frac{81 + 9}{2} = 45.$$

This is a Pythagorean triple, but not a **primitive** Pythagorean triple, because gcd $(27, 36, 45) = 9$.

Now, on to some examples of how these formulas can be used.

Example 3.9 Find the PPT corresponding to the values $s = 11$ and $t = 7$.

Solution

Using the PPT formulas, we have $a = 11 \cdot 7 = 77$, $b = \frac{11^2 - 7^2}{2} = \frac{72}{3} = 36$, and $c = \frac{11^2 + 7^2}{2} = \frac{170}{2} = 85$. Therefore, the PPT is $77 - 36 - 85$.

◆

Example 3.10 Find all values of s and t that make $a = 21$. Then, find the corresponding PPTs.

Solution

Since $a = 21 = 7 \times 3 = 1 \times 21$, there are two choices for s and t: either $s = 7$, $t = 3$, or $s = 21$, $t = 1$. Using the values $s = 7$ and $t = 3$, the resulting PPT is the triple $21 - 20 - 29$. Using $s = 21$ and $t = 1$, the PPT is the triple $21 - 120 - 121$.

◆

Example 3.11 Find all values of s and t that make $a = 75$, and find the corresponding PPTs.

Solution

Even though $75 = 1 \cdot 75 = 5 \cdot 15 = 3 \cdot 25$, there are still only two choices for s and t that produce PPTs. If $s = 15$ and $t = 5$, then $\gcd(s, t) = 5 \neq 1$ so this choice will not produce a PPT. The two resulting PPTs are:

$75 - 2812 - 2813$ (when $s = 75$, $t = 1$)
$75 - 308 - 317$ (when $s = 25$, $t = 3$)

◆

Example 3.12 Suppose that you choose the values $s = 2$ and $t = 1$:

(a)   Which rule for s and t does this choice break?
(b)   What happens if you substitute $s = 2$ and $t = 1$ into the PPT formulas? Do you get a Pythagorean triple? Is it primitive?

Solution

(a)   This breaks the first rule which states that both s and t must be odd.
(b)   Applying the PPT formulas, we have $a = 2$, $b = \frac{3}{2}$, and $c = \frac{5}{2}$. The first thing to notice is that this is definitely not a PPT; in fact it is not even a Pythagorean triple. (Why not? Look back at the definition to see.) But it does specify the

sides of a right triangle because $2^2 + \left(\frac{3}{2}\right)^2 = 4 + \frac{9}{4} = \frac{25}{4} = \left(\frac{5}{2}\right)^2$. This empha-
sizes why we must have both s and t odd in the PPT formulas.   ◆

Example 3.13 Find an example of a PPT with $c > 50$.

Solution

The formula for computing c is $c = \frac{s^2 + t^2}{2}$. To make c greater than 50, choose s and
t so that $s^2 + t^2$ is greater than 100. Suppose $t = 5$. Then $s^2 + t^2 = s^2 + 25$, so we need
an odd integer s not divisible by 5 so that s^2 is greater than 75. One possible choice
is $s = 9$. Using $s = 9$, $t = 5$ to compute the PPT, we have

$$a = 45, \quad b = 28, \quad c = 53$$

◆

Exercise Set 3.2

Exercises 1–6. Determine whether or not the given triple is a Pythagorean triple.
Explain your answer.
  1. $10 - 24 - 26$
  2. $6 - 8 - 12$
  3. $1 - 2 - 3$
  4. $30 - 40 - 50$
  5. $40 - 76 - 86$
  6. $9 - 40 - 41$

  7. Which of the triples in Exercises 1–6 are **primitive** Pythagorean triples?
      Explain your answer.

Exercises 8–12. Find a triangle similar to the Pythagorean triple whose sides form
a primitive Pythagorean triple (PPT).
  8. $27 - 36 - 45$
  9. $45 - 24 - 51$
 10. $350 - 120 - 370$
 11. $126 - 120 - 174$
 12. $135 - 72 - 153$

Exercises 13–18. Determine whether or not the triple is a primitive Pythagorean
triple (PPT). (Remember there are two things to check.)
 13. $3 - 4 - 7$
 14. $6 - 8 - 10$
 15. $45 - 28 - 53$
 16. $5 - 12 - 13$
 17. $10 - 24 - 26$
 18. $15 - 20 - 25$

19. Give an example of integers a, b, and c such that $\gcd(a, b, c) = 1$ but none of $\gcd(a, b)$, $\gcd(b, c)$, and $\gcd(a, c)$ are 1.

Exercises 20–22. Find the PPT corresponding to the choice of s and t.
20. $s = 11, t = 5$
21. $s = 27, t = 1$
22. $s = 13, t = 11$

23. Find all pairs s and t that make $a = 11$. Then find the PPT corresponding to each set of values.
24. Find all pairs s and t that make $a = 19$. Then find the PPT corresponding to each set of values.
25. Find all pairs s and t that make $a = 63$. Then find the PPT corresponding to each set of values.
26. Find all pairs s and t that make $a = 27$. Then find the PPT corresponding to each set of values.
27. Find all pairs s and t that make $a = 45$. Then find the PPT corresponding to each set of values.
28. Find all pairs s and t that make $a = 65$. Then find the PPT corresponding to each set of values.
29. Find s and t that yield the PPT $9 - 40 - 41$.
30. Find s and t that yield the PPT $25 - 312 - 313$.
31. (a) Create a table of PPTs with $t = 1$ and different values of s. Make a conjecture about the relationship between t and the PPT.
    (b) Test the conjecture from part (a) on $t = 3$ using several values of s. If your conjecture is not true in this case, revise it.
    (c) Test your latest conjecture when $t = 5$. Is either the original or the revised conjecture still true?
32. Prove that if $t = 1$ and $s > t$, then a PPT generated by s and t has the property that $c = b + 1$.
33. Is $100 - 621 - 629$ a PPT? Explain your answer and how you found it.
34. Find a primitive Pythagorean triple with $c > 250$.
35. Find a primitive Pythagorean triple with $b > 100$.
36. Find all primitive Pythagorean triples with $c < 50$.
37. Find all primitive Pythagorean triples with $a < 20$.
38. Find all Pythagorean triples containing 12 (Note: They do not have to be primitive).
39. Prove that any odd positive integer greater than 1 can be a leg of a PPT.
40. Prove that if $a - b - c$ is a PPT with one odd leg and one even leg, then the hypotenuse c must be odd.
41. If s and t are odd integers with $s > t \geq 1$, prove that $\frac{s^2 - t^2}{2}$ is always a positive integer.

3.3   Computing Primitive Pythagorean Triples: The Formulas Work!

In this section, we will develop the outline of the proof of the claims about the primitive Pythagorean triple formulas that were made in Section 3.2. For reference, the formulas are included below.

Formulas for Primitive Pythagorean Triples

Choose integers s and t using the following rules:

(i) s and t are odd.
(ii) $s > t \geq 1$.
(iii) $\gcd(s, t) = 1$ (in other words, s and t are relatively prime).

Then, if

$$a = st, \quad b = \frac{s^2 - t^2}{2}, \quad c = \frac{s^2 + t^2}{2},$$

$a - b - c$ is a primitive Pythagorean triple.

In Section 3.2, it was verified that these formulas do produce Pythagorean triples. Now, there are two remaining things to show:

1. Show that if s and t are chosen according to the given rules, the resulting values for a, b, and c will be a primitive Pythagorean triple. Since the partial proof of Theorem 3.4 shows that they form a Pythagorean triple, it remains to show that $\gcd(a, b, c) = 1$.
2. Show that for any primitive Pythagorean triple, there are values for s and t meeting the conditions given above such that substituting them into the formulas produces that exact PPT. This means that the formulas above generate all possible primitive Pythagorean triples.

Parts of the proofs of these statements can be proven now, but some parts use tools to be developed in Chaps. 4 and 5. At the end of Chap. 5, we will return to these results and fill in the details of the proofs.

Theorem 3.5 states the first result listed above: that the formulas produce primitive Pythagorean triples.

Theorem 3.5
If s and t are positive integers such that $s > t$, s and t are odd, and $gcd(s, t) = 1$, and if $a = st$, $b = \frac{s^2-t^2}{2}$, and $c = \frac{s^2+t^2}{2}$, then the integers a, b, and c are a primitive Pythagorean triple.

The proof that the Pythagorean triples will be primitive relies on properties of prime numbers which will be studied in Chap. 4. We will return to this proof at the end of Chap. 5.

Now we will outline a proof of the second claim: if $a - b - c$ is a PPT, then it is possible to find $s > t \geq 1$ with s and t both odd and $\gcd(s, t) = 1$ such that $a = st$, $b = \frac{s^2 - t^2}{2}$, and $c = \frac{s^2 + t^2}{2}$.

We will start with two properties of the sides of a primitive Pythagorean triple. Lemma 3.1 is ***Conjecture 3.3*** from Section 3.2, and the Lemma 3.2 comes from ***Conjecture 3.4***. The smaller results that contribute to the proof of a major result, or theorem, are called lemmas.

Lemma 3.1
If $a - b - c$ is a Primitive Pythagorean triple, then the greatest common divisor of any two sides is 1.

The proof of Lemma 3.1 requires material developed later. We will return to this proof at the end of Chap. 5.

Lemma 3.2
If $a -b- c$ is a PPT, then one of the legs, a or b, is odd and the other is even.

Proof.   There are three possibilities for the legs of the triangle. Either:

  (i) Both legs are even.
 (ii) Both legs are odd.
(iii) One is odd and one is even.

The third option is the one we want to show is true. To do this, we will show that both of the other cases are impossible. (Since we are going to show something is impossible, we will use a proof by contradiction in each case.) Then, because one of these cases must be true, it will have to be iii).

Proof that i) cannot happen: Suppose that both legs of the PPT are even, so a and b are both even. Then these two legs share a common divisor of 2. But, by Lemma 3.1, $\gcd(a, b) = 1$. Therefore, 2 cannot divide both a and b, and so a and b cannot both be even.

Proof that ii) cannot happen: Suppose that both legs of the PPT are odd, so a and b are both odd. Then a^2 and b^2 are also odd. Therefore, since $c^2 = a^2 + b^2$, c^2 is even, so c is even.

From the definitions of odd and even, there are integers k, l, and m such that

$$a = 2k + 1, \quad b = 2l + 1, \quad c = 2m$$

Then, substituting these expressions into $a^2 + b^2 = c^2$ and simplifying, we obtain the following:

$$(2k + 1)^2 + (2l + 1)^2 = (2m)^2$$
$$4k^2 + 4k + 1 + 4l^2 + 4l + 1 = 4m^2$$
$$4k^2 + 4k + 4l^2 + 4l + 2 = 4m^2$$
$$2(2k^2 + 2k + 2l^2 + 2l + 1) = 2(2m^2)$$

Then,

$$2k^2 + 2k + 2l^2 + 2l + 1 = 2m^2$$
$$2(k^2 + 2 + l^2 + l) + 1 = 2m^2$$

But this equation cannot be true because the left side is odd, while the right side is even. Therefore, it is not possible for both legs of a PPT to be odd.

Since we have shown that both i) and ii) are impossible, iii) must be true, and all PPTs have one odd leg and one even leg.

∎

To match the formulas for primitive Pythagorean triples stated in Section 3.2, we will label the odd leg of a PPT as a, and the even leg as b.

Notice that since one leg is even and the other is odd, the hypotenuse c must be odd. The proof of this fact is Exercise 41 in Section 3.2. This exercise proves the last claim from **Conjecture 3.4**. We include the result here as a lemma, with a proof using Lemmas 3.1 and 3.2.

Lemma 3.3
The hypotenuse of a primitive Pythagorean triangle is always odd.

Proof.   Let $a - b - c$ be a PPT, with c the hypotenuse. By Lemma 3.2, one leg is odd and one leg is even. We will call the odd leg a and the even leg b. Since b is even, $b = 2m$ for $m \in \mathbb{Z}$, and so $2|b$. Now, by Lemma 3.1, $\gcd(b, c) = 1$. Therefore, 2 cannot divide c since if it did, it would be a common divisor of b and c. Therefore, c must be odd.

∎

Now, suppose $a - b - c$ is a primitive Pythagorean triple. Then $\gcd(a, b, c) = 1$, and $a^2 + b^2 = c^2$. By Lemma 3.2, one of the legs of the PPT must be odd (a) and the other must be even (b). Finally, the hypotenuse, c, is also odd by Lemma 3.3.

In order to show that a, b, and c can be expressed in terms of the PPT formulas, we need to find an alternate equation for a, b, or c that we can work with.

One way to start is to solve the equation $a^2 + b^2 = c^2$ to get another expression for a^2:

$$a^2 = c^2 - b^2$$
$$a^2 = (c + b)(c - b)$$

From this equation for a^2, you can see that if s and t are chosen so that $c + b = s^2$ and $c - b = t^2$, then a will be equal to st. We will prove this is possible in a series of steps proving facts about $(c + b)$ and $(c - b)$. To see what properties might be true about $(c + b)$ and $(c - b)$, we will look at some examples of PPTs.

	PPT			
a	b	c	$(c+b)$	$(c-b)$
3	4	5	9	1
5	12	13	25	1
21	20	29	49	9
15	8	17	25	9
7	24	25	49	1

One of the first things to notice is that $(c + b)$ and $(c - b)$ are both always odd. Here are some conjectures based on the table above.

Conjecture 3.6:: If $a - b - c$ is a PPT, then $(c + b)$ and $(c - b)$ are both odd.

Conjecture 3.7:: If $a - b - c$ is a PPT, then $(c + b)$ and $(c - b)$ are relatively prime.

Conjecture 3.8:: If $a - b - c$ is a PPT, then $(c + b)$ and $(c - b)$ are both perfect squares.

Each of these conjectures is true for all PPTs, and they are used to show the PPT formulas stated at the beginning of this chapter to generate any PPT. To prove the second two conjectures, we need tools from Chaps. 4 and 5. We are ready to prove the first conjecture now, and it is stated in the lemma below.

Lemma 3.4
If $a - b - c$ is a primitive Pythagorean triple, then $(c + b)$ and $(c - b)$ are both odd.

Proof. Let $a - b - c$ be a PPT. By Lemma 3.2, one of the legs is odd. Call the odd leg a and the even leg b. By Lemma 3.3, the hypotenuse, c, must be odd. Since an odd integer plus or minus an even integer is odd, both $(c + b)$ and $(c - b)$ are odd integers. ∎

Lemma 3.5

If $a - b - c$ is a primitive Pythagorean triple, then $(c + b)$ and $(c - b)$ are relatively prime.

The proof of Lemma 3.5 requires results to be studied in Chap. 5. We will return to this Lemma at the end of Chap. 5.

Lemma 3.6

If $a - b - c$ is a primitive Pythagorean triple, then $(c + b)$ and $(c - b)$ are both squares.

The proof of Lemma 3.6 depends on material covered later. We will return to the proof at the end of Chap. 5.

The results above are summarized here in Theorem 3.6.

Theorem 3.6

If $a - b - c$ is a PPT, then there exist integers $s > t \geq 1$ with s and t odd and $\gcd(s, t) = 1$ such that $a = st$, $b = \frac{s^2 - t^2}{2}$, $c = \frac{s^2 + t^2}{2}$.

In addition to using the lemmas in this section, the proof of Theorem 3.6 uses tools developed in Chap. 4 when we study primes. We will return to the proof at the end of Chap. 5.

Combining Theorems 3.5 and 3.6, we obtain the following result.

Theorem 3.7

The triple of integers a, b, c forms a PPT if and only if $a = st$, $b = \frac{s^2 - t^2}{2}$, and $c = \frac{s^2 + t^2}{2}$ where s and t are odd integers such that $s > t \geq 1$ and $\gcd(s, t) = 1$.

Proof.

The proof of Theorem 3.5 proves the reverse direction of this if and only if statement.

The proof of Theorem 3.6 proves the forward direction of this if and only if statement.

■

3.4   Summary and Review Exercises

3.4.1   Vocabulary and Symbols

Pythagorean theorem
Pythagorean triangle
Pythagorean triple, $a - b - c$
similar triangles
common divisor
greatest common divisor
primitive Pythagorean triple
primitive Pythagorean triangle
finitely many
infinitely many

3.4.2   Suggested Readings

"Andrew Wiles on Solving Fermat," and interview with NOVA, http://www.pbs.org/wgbh/nova/physics/andrew-wiles-fermat.html.
   Cox, D.A. Introduction to Fermat's Last Theorem. The American Mathematical Monthly. vol. 101, pp 3–14 (1994).

3.4.3   Review Exercises

1. Explain what $a - b - c$ represents.
2. Explain the difference between Pythagorean triangles and primitive Pythagorean triangles.
3. What is the relationship between a Pythagorean triangle and a Pythagorean triple?
4. For each of the triples of numbers given below, determine if the numbers are a primitive Pythagorean triple. Explain your answer.

   (a) $78 - 120 - 340$
   (b) $9 - 12 - 15$
   (c) $12 - 35 - 37$
   (d) $7 - 15 - 35$

5. For each of the primitive Pythagorean triples, find the integers s and t from which a, b, and c are found.

   (a) $119 - 120 - 169$
   (b) $69 - 260 - 269$

(c) $13 - 84 - 85$
(d) $45 - 28 - 53$

6. For each of the pairs of values, s and t, find the corresponding primitive Pythagorean triple.

(a) $s = 15, t = 7$
(b) $s = 25, t = 3$
(c) $s = 27, t = 11$
(d) $s = 31, t = 1$

7. Find a Pythagorean triple $a - b - c$ with side b larger than 1,000.
8. Find a PPT $a - b - c$ with side b larger than 1,000.
9. Show that for every odd number $a \geq 3$, there is a PPT with a side of length a.
10. Find five primitive Pythagorean triples such that the length of the hypotenuse is one more than the length of one of the legs.
11. How many primitive Pythagorean triples with $a = 45$ are there, and what are they?
12. Is there a primitive Pythagorean triple such that $a = 23$? If so, find one. If not, why not?
13. Is there a primitive Pythagorean triple such that $a = 31$? If so, find one. If not, why not?
14. Give four new examples of primitive Pythagorean triples $a - b - c$ where a is odd and b is even. In your examples, determine the remainders when b is divided by 4 and make a conjecture based on what you observe.

Chapter 4
Prime Numbers

Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate.

—Leonhard Euler, 1707–1783

God may not play dice with the universe, but something strange is going on with the prime numbers.

—Carl Pomerance, 1944–present

4.1 What Are Prime Numbers?

While prime numbers were introduced in Chap. 2, this chapter will provide a more in-depth study of primes. Let us begin by reviewing the definition.

> **Definition 4.1: prime**
> An integer $p > 1$ is **prime** if and only if the only positive divisors of p are 1 and p.

An integer greater than 1, which is not prime, is called **composite.** The term composite can also be defined directly, as opposed to not being prime.

> **Definition 4.2: composite**
> An integer $m > 1$ is **composite** if and only if $m = a \cdot b$ where both $1 < a < m$ and $1 < b < m$.

Since the definitions of prime and composite both specify an integer greater than 1, the integer 1 is neither prime nor composite.

Example 4.1 Determine whether each number is prime or composite:

(a) 20
(b) 29
(c) 121
(d) 703

Solution

(a) 20 is composite, because 20 can be written as $20 = 5 \cdot 4$ or $2 \cdot 10$.
(b) 29 is prime, because 29 can only be factored as $29 = 1 \cdot 29$, which means the only positive divisors of 29 are 1 and 29.
(c) 121 is composite, because $121 = 11 \cdot 11$.
(d) 703 is composite, because $703 = 19 \cdot 37$.

◈

Working with primes does not just produce intriguing mathematical problems; knowing whether or not a large number is prime as well as being able to factor large numbers into primes are both very useful. One extremely important application of finding large prime numbers is cryptography, which we will study in Chap. 8.

Notice from Example 4.1 that determining whether or not a number is prime tends to take longer as numbers get larger. If asked to figure out whether 997 or 7429 were primes, it would likely take even longer than the examples above (See Exercise 25). You can always determine whether or not a number has any divisors by checking all positive integers less than or equal to the number, but this would become incredibly time-consuming when the number gets large. Shortcuts for finding divisors will be helpful.

In each of the examples above, notice that each time a number was composite, one of the divisors was always smaller than or equal to the square root of the number. For example, $\sqrt{20} \approx 4.47$, and 20 factored as $2 \cdot 10$ and $4 \cdot 5$. This property will always hold true: when a number is factored, one of the factors must be less than or equal to the square root of the number. To convince yourself of this, think about a perfect square like $36 = 6 \cdot 6$. The divisors or factors of 36 are 1, 2, 3, 4, 6, 9, 12, 18, and 36. Notice that each factor larger than 6 (the square root of 36) is paired with a factor less than six: $36 = 36 \cdot 1 = 18 \cdot 2 = 12 \cdot 3 = 9 \cdot 4 = 6 \cdot 6$.

Now, try it yourself on a number that is not a perfect square, like 42. Again, the divisors larger than the square root are always paired with another divisor smaller than the square root. As numbers get larger, however, testing **all** numbers less than the square root to see if they are divisors will be too time-consuming to be practical, even with the use of computers.

To get around this problem, mathematicians have developed tests called *Primality Tests*. Primality Tests provide shortcuts to check whether or not a number is prime; in other words, they are methods to determine whether or not a specific number is prime, without having to check all the possible divisors.

One of the simplest Primality Tests uses prime divisors of a number, rather than considering all divisors. To develop this test, we must first confirm that every

integer greater than 1 actually has a prime divisor. This fact is stated in the following lemma.

> **Lemma 4.1**
> Every integer greater than 1 has at least one prime divisor.

Proof.   Let k be an integer greater than 1. Then, k must be either a prime number or a composite number. First, look at what happens if k is prime: since every integer divides itself, k is its own prime divisor.

Now, what if k is composite? We will use a proof by contradiction to prove k must have a prime divisor. Suppose that there exists at least one composite integer greater than 1 with no prime divisors. Pick the smallest of these integers, and call it n.[1]

Then $n = ab$ with both a and b greater than 1 and less than n. Now, since n was chosen to be the smallest integer with no prime divisor, and $a < n$, a must have a prime divisor, p. But, since $p|a$ and $a|n$, it is also true that $p|n$, a contradiction. Therefore, there cannot be any integers greater than 1 with no prime divisors.

∎

The next theorem leads us to a Primality Test.

> **Theorem 4.1**
> If n is a composite number, then n must have a prime divisor p such that $p \leq \sqrt{n}$.

Proof.   Let n be a composite number. Then, $n = ab$, where $a \leq b$ and both a and b are greater than 1 and less than n. In symbols, $1 < a < n$ and $1 < b < n$. By Lemma 4.1, a has a prime divisor p.

Since $a \leq b$ there are two possibilities: either $a = b$, or $a < b$. In both cases it must be true that $a \leq \sqrt{n}$; otherwise, if $a > \sqrt{n}$, then $ab > \sqrt{n} \cdot \sqrt{n} = n$, which is not possible since $ab = n$. Then, since $p|a$ and $a|n$ implies that $p|n$, p is a prime divisor of n, and $p \leq \sqrt{n}$.

∎

Now, suppose we want to test an integer $n > 1$ to see whether it is prime or composite. By Theorem 4.1, if n is composite, then n must have a prime divisor $p \leq \sqrt{n}$. Using the contrapositive of Theorem 4.1, if n does not have a prime divisor $p \leq \sqrt{n}$, then n must not be composite, which means n is prime. Therefore, to test to see if a number is prime, it is sufficient to check to see if any prime less than or

---

[1] This is a special property of the integers called the **Well-Ordering Principle:** every nonempty set of positive integers has a smallest element. This is not true for all sets of numbers. For example, the Well-Ordering Principle is not true for the set of real numbers.

equal to the square root of the number is a divisor. If none of these are divisors, then the number is prime. This leads to the following statement.

Primality Test If an integer $n > 1$ has no prime divisor p such that $p \leq \sqrt{n}$, then n is prime.

Example 4.2 Use the Primality Test to determine whether each positive integer is prime or composite.

a) 149   b) 161

Solution

(a) 149

Since $\sqrt{149} \approx 12.2$, by the Primality Test, we check to see if any of the primes 2, 3, 5, 7, or 11 divide 149. The first three (2, 3, and 5) can be ruled out quickly using the divisibility tests from Section 2.9. Checking 7 and 11 shows that neither of these is a divisor of 149, either. Therefore, 149 is prime.

(b) 161

Since $\sqrt{161} \approx 12.7$, once again check the primes less than 12.7 to see if they divide 161. These primes are 2, 3, 5, 7, or 11. Again, the first three (2, 3, and 5) can be ruled out quickly. Checking 7 shows that $161 = 7 \cdot 23$. Therefore, 161 is composite, not prime.

◈

The Greek mathematician Eratosthenes (276–194 B.C.) was famous for his writings in many different fields, from mathematics to literary criticism, as well as serving as the head librarian at the Museum Library in Alexandria. One of his most impressive accomplishments was to accurately calculate the circumference of the earth using only geometry. Among other things, he developed a method for finding all primes less than a given integer n, which is based on the Primality Test above. This is still one of the most efficient methods to find "small primes" (primes less than 1 million).

Eratosthenes' method for finding primes is known as the *Sieve of Eratosthenes*. To see how his method works, suppose we want to find all primes less than the number 50. By the Primality Test, any composite number less than or equal to 50 must have a prime divisor less than or equal to $\sqrt{50}$, or about 7.1. The primes less than 7.1 are 2, 3, 5, and 7. Therefore, by deleting all multiples of these prime numbers (not including these numbers themselves) from the collection of numbers from 2 to 50, we will have deleted all composite numbers, and the remaining numbers must be prime. Table 4.1 shows the results of the completed Sieve of Eratosthenes for n = 50. The shaded numbers are the primes whose multiples we had to check. The different colors are to distinguish why numbers were removed.

◈

This process filters or "sieves" out the composite numbers, and any remaining number that has not been crossed off is prime. Note that we did not have to separately check the multiples of any prime higher than 7; for example, the multiples of 11 included in the table (22, 33, and 44) are all already crossed off even though we did not specifically look for multiples of 11. In Table 4.2, the primes less than 50 are circled. They are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, and 47.

Table 4.1 Sieve of Eratosthenes, $n = 50$

🟦	Number removed because it was a multiple of 2
🟩	Number removed because it was a multiple of 3
🟨	Number removed because it was a multiple of 5
🟪	Number removed because it was a multiple of 7

Sieve of Eratosthenes

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Table 4.2 Primes less than 50

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Exercise Set 4.1

1. Find the smallest prime factor of each of the following numbers (the divisibility tests in Section 2.9 may be helpful).

   (a)   1234566
   (b)   135795

Exercises 2–5. When using the Primality Test on the given number, what is the largest value that has to be checked to confirm whether or not the number is prime?

  2. 461

  3. 127

  4. 449

  5. 517

Exercises 6–24. Use the Primality Test to determine whether the number is prime or composite.

  6. 461

  7. 127

  8. 449

  9. 517

10. 91

11. 101

12. 113

13. 119

14. 139

15. 361

16. 143

17. 213

18. 221

19. 754

20. 3649

21. 441

22. 127

23. 131

24. 289

25. Show that 997 is prime, but 7429 is not.
26. Find all primes less than 30 using the Sieve of Eratosthenes.
27. Find all primes less than 70 using the Sieve of Eratosthenes.
28. Find all primes less than 100 using the Sieve of Eratosthenes. (A grid of integers from 1 to 100 is included in Table 4.3.)
29. Suppose you want to find all primes less than 250 using the Sieve of Eratosthenes. What are the dimensions of the number grid you would need? What are the primes whose multiples you would have to cross off to guarantee that you have found all the primes less than 250?
30. Prove or disprove the following conjecture:
    CONJECTURE: If p and q are odd primes, then $pq + 1$ is never prime.

Table 4.3   Sieve of Eratosthenes, n = 100

Sieve of Eratosthenes									
	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

4.2   The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic states that any integer greater than 1 can be written as a product of primes in exactly one way, if different orders of the prime numbers are not counted as different products. The product of primes equal to a given integer is called its ***prime factorization***. This is why primes are sometimes called the "building blocks" of integers—each positive integer can be "built" from a particular collection of prime numbers. (For an entertaining and artistic description of this fact, read the book *You Can Count on Monsters* by Richard Evan Schwartz.)

This section explains the Fundamental Theorem of Arithmetic and provides some examples of how prime factorizations are used. In Section 4.3, an example of a number system different from the integers where this familiar property of unique factorizations into primes is not true will be given. Then, in Section 4.4, we will finally prove that the Fundamental Theorem of Arithmetic is true in the set of integers.

> **Theorem 4.2. The Fundamental Theorem of Arithmetic**
> Every integer $n > 1$ can be factored into a product of primes $n = p_1 p_2 \ldots p_r$ in exactly one way. (Note: Arranging the factors in a different order is not a new factorization.)

The product $p_1 p_2 \ldots p_r$ is called the ***prime factorization of n***. Each of the symbols p_1, p_2, and so on represents a prime number in the factorization of n. For example, if $n = 28$, then $28 = 2 \cdot 2 \cdot 7$, so $p_1 = 2$, $p_2 = 2$, and $p_3 = 7$. A general term of the prime factorization (not necessarily the first or second prime in the product) is commonly represented by p_i. The Fundamental Theorem of Arithmetic tells us that this factorization is unique, except for the order of the primes. In other words, $28 = 2 \cdot 2 \cdot 7$, which also could be written as $2 \cdot 7 \cdot 2$, but since the lists contain exactly the same primes, they are not considered different factorizations.

Prime factorizations are usually written with like primes grouped together, to make it easier to see the components of the number. So, the factorization of 28 would be written as $2^2 \cdot 7$. Prime factorizations in this form are sometimes called *prime power factorizations*. In general notation, a prime power factorization is written as $n = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$. In this case, if $n = 28$, then $p_1 = 2$, $p_2 = 7$, and the exponents are $n_1 = 2$ and $n_2 = 1$. Notice that, since repeated primes are grouped in powers, each of the p_i's will be different.

Also, note that a prime is considered its own factorization, so, for example, 5 just factors into primes as 5.

Example 4.3 Find the prime factorization of 320.

Solution
Since prime factorizations are unique, starting with any factors of 320 will produce the same final answer. Here is one way to get to the prime factorization.

$$320 = 10 \cdot 32 = (2 \cdot 5)(2^5) = 2^6 \cdot 5$$

Note that starting with different factors still ends at the same prime factorization:

$$320 = 2 \cdot 160 = 2 \cdot (8 \cdot 20) = 2 \cdot 2^3 \cdot (4 \cdot 5) = 2 \cdot 2^3 \cdot 2^2 \cdot 5 = 2^6 \cdot 5$$

◈

Example 4.4 Find the prime factorization of 1134.

Solution
You may notice right away that 1134 is divisible by 2, 3, and 9 (If you aren't sure why, review the divisibility tests for these numbers in Section 2.9). Starting with any one of these factors will lead to the same final prime factorization. Here are two ways to get to the prime factorization of 1134:

$$1134 = 3 \cdot 378 = 3 \cdot 2 \cdot 189 = 3 \cdot 2 \cdot 9 \cdot 21 = 3 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7 = 2 \cdot 3^4 \cdot 7$$
$$1134 = 2 \cdot 567 = 2 \cdot 9 \cdot 63 = 2 \cdot 3 \cdot 3 \cdot 7 \cdot 9 = 2 \cdot 3 \cdot 3 \cdot 7 \cdot 3 \cdot 3 = 2 \cdot 3^4 \cdot 7$$

◈

Example 4.5 Find the prime factorization of 113.

Solution
In this example, it may not be obvious whether 113 has any divisors or is prime. In that case, we can always go back to the Primality Test to reduce the work of looking for divisors. If 113 is composite, then it must have at least one prime divisor less than or equal to $\sqrt{113} \approx 10.6$. Check to see if one of 2, 3, 5, or 7 is a divisor of 113. Since none of these divide 113, 113 is prime and is its own prime factorization.

◈

Example 4.6 Find the prime factorization of 143.

Solution

Again, the divisors that are easy to check using the divisibility tests do not evenly divide 143. According to the Primality Test, since $\sqrt{143} \approx 11.9$, check the primes 2, 3, 5, 7, and 11 to see if any of them divide 143. From this list, 11 divides 143, and this gives us the prime factorization of 143.

$$143 = 11 \cdot 13$$

◈

The previous examples show how numbers are broken down into their prime factors.

The last part of this section contains examples of ways to use unique prime factorizations. They can be useful in proving other general statements about a number and also to do calculations with specific numbers. We will start with a familiar example: Find the greatest common divisor of two integers. In Chap. 3, greatest common divisors were used to determine whether or not a Pythagorean triple was a primitive Pythagorean triple. Prime factorizations provide a more systematic way to find greatest common divisors.

Example 4.7 Find gcd (126, 540).

Solution

First, find the prime factorizations for 126 and for 540:

$$126 = 2 \cdot 3^2 \cdot 7$$
$$540 = 2^2 \cdot 3^3 \cdot 5$$

The primes 2 and 3 are in the prime factorizations of both 126 and 540, but 126 and 540 do not share any other prime factors. Now, 540 is divisible by $2^2 = 4$, but 126 is divisible only by 2, so 2 will be a factor of the greatest common divisor. Also, 540 is divisible by 3^3 but 126 is divisible only by 3^2, so 3^2 will be a factor of the greatest common divisor. Therefore, the greatest common divisor is gcd $(126, 540) = 2 \cdot 3^2 = 18$.

◈

Notice how the primes appearing in the prime factorizations of two numbers can be used to build the prime factorization of the greatest common divisor of those two numbers. This technique is summarized here.

Using Prime Power Factorizations to find gcd(a, b)

1. Write the prime power factorizations for both a and b.
2. Find the prime factors that a and b have in common.
3. The greatest common divisor of a and b will be the product of the prime factors shared by a and b, with the smaller exponent from the prime factorizations of a and b.

Example 4.8 Find gcd(4200, 720).

Solution
First, find the prime factorizations of 4200 and 720.

$$4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$$
$$720 = 2^4 \cdot 3^2 \cdot 5$$

Both numbers have prime factors of 2, 3, and 5. The smallest exponent for the factor of 2 is 3, the smallest exponent for the factor of 3 is 1, and the smallest exponent for the factor of 5 is 1. The prime 7 is not included in the greatest common divisor since 7 is not a factor of 720. Therefore, gcd(4200, 720) $= 2^3 \cdot 3 \cdot 5 = 120$. ◈

Example 4.9 Is $100 - 621 - 629$ a primitive Pythagorean triple?

Solution
To answer this question, two things need to be checked: first, that the numbers given satisfy the Pythagorean Theorem and second, that gcd(100, 621, 629) $= 1$.

Since $100^2 + 621^2 = 395641$ and $629^2 = 395641$, these numbers do represent a Pythagorean triple.

Now, use prime factorizations to find the gcd(100, 621, 629) (Remember the Primality Test may be helpful in finding prime factorizations.)

$$100 = 2^2 \cdot 5^2$$
$$621 = 3^3 \cdot 23$$
$$629 = 17 \cdot 37$$

Since these three numbers don't share any prime factors, they have no divisors in common except for 1, so gcd(100, 621, 629) $= 1$.

Note: This question is Exercise 34 from Section 3.2, before a systematic method for finding greatest common divisors. If you did this problem before, compare the two solutions. ◈

Example 4.10 Find $lcm(60, 126)$.

Solution
Remember that the *lcm* or least common multiple of two integers is the smallest number that both integers divide. Prime factorizations can also be used to find the least common multiple of two numbers. For this example, look at the prime factorizations of 60 and 126.

$$60 = 2^2 \cdot 3 \cdot 5$$
$$126 = 2 \cdot 3^2 \cdot 7$$

If 60 divides a number, that number must also be divisible by 2^2, 3, and 5. Likewise, if 126 divides a number, it must be divisible by 2, 3^2, and 7. To find the smallest number both 60 and 126 divide, include the largest power of each prime factor appearing in either number's factorization. Therefore,

$$lcm(60, \ 126) \ = \ 2^2 \cdot 3^2 \cdot 5 \cdot 7 = 1260$$

◈

From Example 4.10, you can see that prime power factorizations are also useful to find the least common multiple of two integers. Summarizing the process of using prime power factorizations to find the least common multiple of two integers is left as Exercise 29.

Example 4.11 Find all positive divisors of 315.

Solution
We will use the prime factorization $315 = 3^2 \cdot 5 \cdot 7$ to keep track of all of the divisors. The divisors of 315 are made up of all combinations of these prime factors (as well as the number 1, which doesn't show up in the prime factorization). Here is a list of the divisors:

1	$3 \cdot 3 = 9$	$3 \cdot 3 \cdot 5 = 45$	$3 \cdot 3 \cdot 5 \cdot 7 = 315$
3	$3 \cdot 5 = 15$	$3 \cdot 3 \cdot 7 = 63$	
5	$3 \cdot 7 = 21$	$3 \cdot 5 \cdot 7 = 105$	
7	$5 \cdot 7 = 35$		

◈

Example 4.12 Find a and b such that $a > 1000$, $b > 1000$, and $gcd(a, b) = 15$.

Solution
If $gcd(a, b) = 15 = 3 \cdot 5$, then $3 \cdot 5$ must be part of the prime factorization of both a and b. Also, since 15 is the greatest common divisor of a and b, they cannot have any other prime factors in common. One way to choose a and b is to multiply each one by different prime factors to make each number big enough. For example, $a = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$ and $b = 3 \cdot 5 \cdot 13 \cdot 17 = 3315$. Now, $gcd(a, \ b) = 15$ and both a and b are greater than 1000, as required. Can you find another correct solution?

◈

Prime factorizations can be useful in proving results about divisibility. The next two theorems use prime factorizations in their proofs. Theorem 4.3 is used again at the end of Chap. 5, to prove the PPT formulas from Chap. 3 do produce all primitive Pythagorean triples. Before the theorems are introduced, we introduce Lemma 4.2 which is useful in the proof.

> **Lemma 4.2**
> If $a|b$, then the prime factors of a are also prime factors of b.

Proof. Let $a|b$ and let p be a prime factor of a. Then, $p|a$. Therefore, since $p|a$ and $a|b$, we have that $p|b$. (This was proved in Theorem 2.2.) Therefore, p is also a prime factor of b.

∎

Notice that this means that if $a|b$, then each prime factor of a must be contained in the prime factorization of b.

> **Theorem 4.3**
> If $c, d > 1$ and $c^2|d^2$, then $c|d$.

Proof. Let $c^2|d^2$. Let $c = p_1^{c_1} \cdot p_2^{c_2} \cdot p_3^{c_3} \cdot p_4^{c_4} \cdots p_k^{c_k}$ and let $d = q_1^{d_1} \cdot q_2^{d_2} \cdot q_3^{d_3} \cdot q_4^{d_4} \cdots q_m^{d_m}$. Then the prime factorizations of c^2 and d^2 are:

$$c^2 = p_1^{2c_1} \cdot p_2^{2c_2} \cdot p_3^{2c_3} \cdot p_4^{2c_4} \cdots p_k^{2c_k},$$
$$d^2 = q_1^{2d_1} \cdot q_2^{2d_2} \cdot q_3^{2d_3} \cdot q_4^{2d_4} \cdots q_m^{2d_m}.$$

Since $c^2|d^2$, the prime factorization of c^2 must be contained in the prime factorization of d^2 by Lemma 4.2. Therefore, we can rearrange the factors of d^2 to write the factors common to c^2 first, obtaining

$$d^2 = p_1^{2c_1} \cdot p_2^{2c_2} \cdot p_3^{2c_3} \cdot p_4^{2c_4} \cdots p_k^{2c_k} \cdot q_{k+1}^{2d_{k+1}} \cdots q_m^{2d_m}$$

Using this factorization to find d, we see that

$$d = p_1^{c_1} \cdot p_2^{c_2} \cdot p_3^{c_3} \cdot p_4^{c_4} \cdots p_k^{c_k} \cdot q_{k+1}^{d_{k+1}} \cdots q_m^{d_m}$$

Notice that the first part is just the prime factorization of c, so

$$d = c \cdot q_{k+1}^{d_{k+1}} \cdots q_m^{d_m}$$

Therefore, $c|d$.

∎

Theorem 4.4
If $s, t > 1$ and $\gcd(s, t) = 1$, then $\gcd(s^2, t^2) = 1$.

Proof. Let $\gcd(s, t) = 1$. Then there must not be any primes in both the prime factorization of s and the prime factorization of t. Writing out the prime power factorizations, we will use p_i's to represent the primes in the factorization of s and q_i's to represent the primes in the factorization of t:

$$s = p_1^{s_1} \cdot p_2^{s_2} \cdot \cdots \cdot p_m^{s_m}$$

and

$$t = q_1^{t_1} \cdot q_2^{t_2} \cdot \cdots \cdot q_n^{t_n}$$

where none of the p_i's are equal to the q_j's. Now, square s and t to obtain the following:

$$s^2 = \left(p_1^{s_1} \cdot p_2^{s_2} \cdot \cdots \cdot p_m^{s_m} \right)^2 = p_1^{2s_1} \cdot p_2^{2s_2} \cdot \cdots \cdot p_m^{2s_m}$$

and

$$t^2 = \left(q_1^{t_1} \cdot q_2^{t_2} \cdot \cdots \cdot q_n^{t_n} \right)^2 = q_1^{2t_1} \cdot q_2^{2t_2} \cdot \cdots \cdot q_n^{2t_n}$$

Since no new primes were introduced into the prime factorizations of s^2 and t^2, the greatest common divisor is still 1. Therefore $\gcd(s^2, t^2) = 1$

■

Exercise Set 4.2

1. Remember that a prime integer must be greater than 1, so 1 is not considered a prime number. Explain why the Fundamental Theorem of Arithmetic would not be true if 1 were a prime number.
2. Find the prime factorization of 294, and then use it to list all the divisors of 294.
3. Find the prime factorization of 140 and then use it to list all the divisors of 140.

Exercises 4–8.   Find the prime factorization of the following integers. Write the prime power factorization, with the smallest primes first, grouped in powers (e.g., write $3 \cdot 2 \cdot 2$ as $2^2 \cdot 3$).
4. 108
5. 315
6. 1040
7. 7429

8. 561

9. Determine whether 3649 is prime. If not, find its prime factorization.
10. Describe all integers with exactly two positive divisors. Provide some specific examples and a general formula.
11. Describe all integers with exactly three positive divisors. Provide some specific examples and a general formula.
12. Describe all integers with exactly four positive divisors. Provide some specific examples and a general formula.
13. Find all positive divisors of the integer n if $n = p^3$ where p is prime.
14. Find all positive divisors of the integer n if $n = 5q$ where q is prime.

Exercises 15–20.   Find the greatest common divisor.
15. gcd(44, 130)
16. gcd($2^4 \cdot 5^3 \cdot 7^3 \cdot 11$, $2^5 \cdot 7^2 \cdot 11^3 \cdot 13$)
17. gcd(561, 3289)
18. gcd(221, 323)
19. gcd($2^2 \cdot 3^3 \cdot 5 \cdot 7, 2^2 \cdot 3^2 \cdot 5 \cdot 7^2$)
20. gcd(15, 421)

21. Find two numbers a and b such that gcd(a, b) = 14, $a > 1200$, and $b > 4000$.
22. Find two numbers a and b such that gcd(a, b) = 14, $a > 1200$, and $b > 4000$, **and the only prime divisors of a and b are 2 and 7**.

Exercises 23–28.   Find an integer that is relatively prime to the given integer.
23. 840
24. 1260
25. 12,870
26. 2310
27. 273
28. 56,595

29. Write a step-by-step process for finding the least common multiple of two integers using their prime power factorizations. Test the process on at least two different pairs of integers.
30. Consider the following conjecture: If a divides b and p is part of the prime factorization of a, then p divides b.

   (a) Rewrite the conjecture using symbols when possible.
   (b) Choose two sets of values for a, b, and p and show that the statement is true in both cases.
   (c) Prove that the conjecture is true.

31. Explain how to get the prime factorization of c^2 from the prime factorization of c that was used in the proof of **Theorem 4.3**.
32. Look at the prime factorizations of several perfect squares. Organize your examples in a table. Include at least two perfect squares that have more than one prime factor (e.g., 36). Make a conjecture about the properties of prime

factorizations of perfect squares, based on your examples. Can you prove your
conjecture?

33. The following statement is false: If $\gcd(s, t) = 4$, then $\gcd(s^2, t^2) = 4$. Find a
counterexample, and explain your example.

34. Prove the converse of **Theorem 4.4**: If $\gcd(s^2, t^2) = 1$, then $\gcd(s, t) = 1$.

35. Test the following conjecture using several examples. Then, try to either prove
or disprove the conjecture.
CONJECTURE: If $\gcd(s, t) = n$, then $\gcd(s^2, t^2) = n^2$.

36. Prove or disprove: If $a > 0$ and $a | b$, then $\gcd(a, b) = a$. **Hint:** To prove this
statement, you need a general proof. To disprove the statement, you need a
counterexample. Try several examples first to decide whether you think it is
true or false.

4.3 The Even Integers

The fact that every number has a unique prime factorization is probably very
familiar to you. In the past, you have worked with primes, made prime factor
trees for integers, and you probably believe that if a group of people individually
came up with a prime factorization for 300, they would all come up with the same
answer ($300 = 2^2 \cdot 3 \cdot 5^2$).

However, this familiar algebraic property actually sets the positive integers apart
from other collections of numbers. A field of mathematics called Abstract Algebra,
which is closely related to number theory, studies different collections of numbers
or objects and explores what properties they do or do not have. The collections
studied in Abstract Algebra can be familiar, like the integers, or some subset of the
integers, or they can be less familiar. In either case, the basic arithmetic operations
of addition and multiplication are defined on the objects of interest. After doing
that, two important questions to ask are "What do the primes look like?" and "Do
you get unique factorization?" In this section, we will study these questions using
the example of the even integers.

Call the collection of even integers $2\mathbb{Z}$. Then, the elements of the set are
$2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}$. Just as in the integers, $\mathbb{Z}$, there are no fractions,
when we look at $2\mathbb{Z}$, there are no odds. Before going on, let us see which standard
operations can be performed inside the set $2\mathbb{Z}$. Remember that a set is called *closed*
under an operation if the number resulting from performing the operation is still in
the set. By checking each operation, you will find that $2\mathbb{Z}$ is closed under $+$, $-$, and
$\times$, but not under $\div$, just as was true for $\mathbb{Z}$. This property was stated in the Closure of
$\mathbb{Z}$ Axiom in Chap. 2.

As an example, we can show that $2\mathbb{Z}$ is closed under $+$. Since the elements of $2\mathbb{Z}$
are just the evens, any two elements will have the form $2m$ and $2k$, with m and
$k \in \mathbb{Z}$. Adding shows that $2m + 2k = 2(m + k) \in 2\mathbb{Z}$, since $m + k$ is an integer (Notice
that this proof is the same as showing that the sum of an even and an even is still an
even number).

To discuss primes and prime factorizations in $2\mathbb{Z}$, we need to understand what it means for an element of $2\mathbb{Z}$ to divide another so that the concept of prime in $2\mathbb{Z}$ can be defined.

First, in the integers, $a \mid b$ if and only if $b = ak$ for some $k \in \mathbb{Z}$. So, it is true that $6 \mid 12$ because $12 = 6 \cdot 2$, but it is false that $6 \mid 15$ because $15 = 6 \cdot \left(\frac{5}{2}\right)$, but $\frac{5}{2} \notin \mathbb{Z}$. In $2\mathbb{Z}$, we have the following definition:

> **Definition 4.3: a divides b in 2$\mathbb{Z}$**
> If $a \in 2\mathbb{Z}$, then **a divides b in 2$\mathbb{Z}$** if and only if $b = ak$ for some $k \in 2\mathbb{Z}$. The notation for a divides b in $2\mathbb{Z}$ is still $a|b$ in $2\mathbb{Z}$.

Let us look at some examples.

Example 4.13

(a) $6 \mid 12$ in $2\mathbb{Z}$ because $12 = 6(2)$ and $2 \in 2\mathbb{Z}$.
(b) $6 \nmid 18$ in $2\mathbb{Z}$ because $18 = 6(3)$ and $3 \notin 2\mathbb{Z}$.
(c) $4 \nmid 22$ in $2\mathbb{Z}$ because $22 = 4\left(\frac{11}{2}\right)$ and $\frac{11}{2} \notin 2\mathbb{Z}$ (or in $\mathbb{Z}$, for that matter).
(d) $4 \nmid 20$ in $2\mathbb{Z}$ because $20 = 4(5)$ and $5 \notin 2\mathbb{Z}$.
(e) $8 \mid 80$ in $2\mathbb{Z}$ because $80 = 8(10)$ and $10 \in 2\mathbb{Z}$.

◈

Now that we have a good idea of what it means for one number to divide another in $2\mathbb{Z}$; let us explore how to define "prime" in $2\mathbb{Z}$. The definition cannot be exactly the same definition as in $\mathbb{Z}$—that a prime numbers only positive divisors are one and itself—because 1 is not in $2\mathbb{Z}$, and therefore, no elements of $2\mathbb{Z}$ are divisible by themselves. Instead, we will use the following definition in $2\mathbb{Z}$:

> **Definition 4.4: prime in 2$\mathbb{Z}$**
> An element $p \geq 2$ of $2\mathbb{Z}$ is **prime in 2$\mathbb{Z}$** if and only if p is not divisible by any element in $2\mathbb{Z}$.

Another way to say this is that p is prime in $2\mathbb{Z}$ if and only if p cannot be written as a product of even numbers (elements of $2\mathbb{Z}$).

Example 4.14 Determine which of the following are prime in $2\mathbb{Z}$:
            (a) 2   (b)4   (c)6   (d)12

Solution

(a) 2 is prime in $2\mathbb{Z}$ because $2 = 2(1)$ and $1 \notin 2\mathbb{Z}$.
(b) 4 is not prime in $2\mathbb{Z}$ because 4 can be written as $4 = 2(2)$, so $2|4$ in $2\mathbb{Z}$.
(c) 6 is prime in $2\mathbb{Z}$, because 6 can be factored as $6 = 1(6) = 2(3)$, but neither is a factorization in $2\mathbb{Z}$.
(d) 12 is not prime in $2\mathbb{Z}$, because even though $12 = 4(3)$ and $3 \notin 2\mathbb{Z}$, it is also true that $12 = 2(6)$, so both 2 and 6 divide 12 in $2\mathbb{Z}$.

◈

The first 10 primes in $2\mathbb{Z}$ are 2, 6, 10, 14, 18, 22, 26, 30, 34, and 38. Notice that the primes on this list are spaced 4 apart. Think about whether you can show that this pattern continues or whether there is a counterexample somewhere.

Finally, now that we know how to find primes in $2\mathbb{Z}$, we can answer the question of whether or not $2\mathbb{Z}$ has unique factorization into primes. Unfortunately, the answer is no. For example, $60 = 6(10) = 2(30)$, two factorizations of different primes. Can you find another example?

Exercise Set 4.3

1. Prove that $2\mathbb{Z}$ is closed under $-$ and $\cdot$, but not under $\div$.
2. Find an example of an element of $2\mathbb{Z}$ that factors into primes in more than one way.
3. Consider the collection of all odd integers: $Odd\mathbb{Z} = \{\ldots, -5, -3, -1, 1, 3, 5, 7,\ldots\}$. Determine whether $Odd\mathbb{Z}$ is closed under $+$, $\cdot$, $-$, or $\div$.
4. Consider the set of numbers $3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$.

   (a) Show that $3\mathbb{Z}$ is closed under $+$, $-$, and $\cdot$.
   (b) Show that $3\mathbb{Z}$ is not closed under $\div$.
   (c) State the definition of $a|b$ in $3\mathbb{Z}$.
   (d) In each case below, determine whether the expression is true or false in $3\mathbb{Z}$. Explain your answers.

      (i) $6 \mid 12$
      (ii) $3 \mid 15$
      (iii) $6 \mid 18$
      (iv) $9 \mid 18$
      (v) $9 \mid 27$

5. Define an element of $3\mathbb{Z}$ to be prime if it is not divisible by any element of $3\mathbb{Z}$.

   (a) Make a list of the first ten primes in $3\mathbb{Z}$
   (b) Make a conjecture about whether $3\mathbb{Z}$ has unique factorization into primes, and test your conjecture.

4.4 Proving the Fundamental Theorem of Arithmetic

Knowing that the property of unique factorization into primes is not automatic in all number systems, we will return to $\mathbb{Z}$ and look at why it is true here. The Fundamental Theorem of Arithmetic actually has two parts: first, that each integer greater than 1 has a prime factorization and second, that each number has only one prime factorization—that prime factorizations are unique (Remember that the prime factorization of a prime is just the prime itself.) This theorem is restated here.

> **The Fundamental Theorem of Arithmetic**
> Every integer $n > 1$ can be factored into a product of primes $n = p_1 p_2 \cdots p_n$ in exactly one way. (Note: Arranging the factors in a different order does not count as a new factorization.)

Proof. First, prove that every integer $n > 1$ has a prime factorization, using a proof by contradiction. So, suppose that there exists at least one integer greater than 1 that cannot be written as a product of primes. Pick the smallest of these integers and call it k.[2] Then k cannot be prime, because if it were, it would be its own prime factorization. Therefore, k must be composite. Then k can be written as $k = ab$, where both a and b are greater than 1 and less than k. Now, k was chosen to be the smallest integer greater than 1 not having a prime factorization, so since a and b are both greater than 1 and less than k, a and b must both have prime factorizations. But since $k = ab$, k has a prime factorization also. This contradicts the choice of k. Therefore, there are no integers greater than 1 that do not have a prime factorization.

To prove the second part of the theorem, we must prove that prime factorizations are unique. To prove this part of the theorem, write out two prime factorizations for an integer, and then show that they have to contain the same primes. Start by assuming that there is an integer $n > 1$ such that $n = p_1 p_2 p_3 \ldots p_k = q_1 q_2 q_3 \ldots q_r$, where each of the p_i and q_i are primes, listed in increasing order. Now, by the definition of divides, $p_1 \mid q_1 q_2 q_3 \ldots q_r$, $p_2 \mid q_1 q_2 q_3 \ldots q_r$, and so on. Since p_1 is prime, it must be true that p_1 divides one of the q_i's. Since the smallest primes are first, $p_1 \mid q_1$. (This is the generalized version of Euclid's Lemma (Theorem 5.3) discussed in Exercise 22 of Section . For now, see if you can convince yourself that it is reasonable by looking at a few examples.) Since p_1 and q_1 are both prime and the only divisors of q_1 are 1 and q_1 itself, p_1 and q_1 must be equal. Similarly, p_2 must divide one of the q_i's, so $p_2 \mid q_2$, which implies that $p_2 = q_2$. Continuing in this manner, we will get that $p_i = q_i$ for each of the primes, and therefore, there is only one way to factor n into primes.
∎

4.5   The Search for Primes

One question that has not yet been answered is, "How many primes are there?" If there is a fixed number of primes–maybe 100 or 1000 or even 50,000,000–then there are *finitely many* primes. If that is the case, then they can all be written down,

---

[2] We are using the Well-Ordering Principle again here.

and the list of primes would come to an end. There would be a biggest prime out there, and no integer larger than it could be prime. On the other hand, if the list of primes goes on forever, with no largest prime, then there are *infinitely many* primes.

Mathematicians are searching for larger and larger primes, and they keep track of the largest integers that have been proven to be primes. In 2008, mathematicians confirmed that the nearly 13 million digit number $2^{43112609} - 1$ was prime, and this number held the honor of being the largest known prime until 2013 when it was overshadowed by $2^{57885161} - 1$, with over 17 million digits. Primes of this form $(2^n - 1)$ are called ***Mersenne primes***. Can we be sure that primes larger than this one exist, even if we haven't actually found them? Thanks to Euclid, we know that the answer is yes!

Euclid's proof that there must be infinitely many primes is one of the most famous proofs in number theory. This proof is a good example of an ideal time to use a proof by contradiction, because the statement of the theorem does not contain any given information. The proof depends on a fact proved in Lemma 4.1: that every integer greater than 1 must have at least one prime divisor. Euclid was able to show that if you did have a finite number of primes, it would always be possible to create a number that couldn't possibly be divisible by any of them. Here is the statement of the theorem and the proof.

Theorem 4.5
There are infinitely many primes.

Proof (by contradiction).
Suppose that there are finitely many primes, say n of them. Then they could be listed in order as follows: p_1, p_2, p_3, ..., p_n. Now, consider the integer $N = p_1 p_2 p_3 \cdots p_n + 1$. Then, since N is a positive integer greater than 1, N must have a prime divisor by Lemma 4.1. But, on the other hand, each of the primes listed will leave a remainder of 1 when divided into N. Therefore, there must be a prime not included on the list above, since N must have a prime divisor. This is a contradiction since we claimed to have listed all the primes. Therefore, there must be infinitely many primes.

■

Since there are infinitely many primes, another interesting question is whether or not there is a pattern to the occurrence of primes. For example, some questions that come up are:

1. Do primes occur regularly throughout the integers? (Is every 10th, or 100th, or *kth* integer prime?)
2. Is it possible to find a formula that will generate all primes, or that will always give a prime number, either when any integer or a certain type of integer is substituted into the formula?
3. If a formula that always gives a prime is not possible, then is it possible to find a formula that will give a prime number infinitely often, but not every time?

(In other words, is there a formula that will result in a prime number when infinitely many different integers are substituted into the formula?

To answer the first question, think about finding a sequence of two consecutive composite integers. This is not hard to do; for example, 8 and 9 or 9 and 10 both work. To find three consecutive composite integers, we can put together 8, 9, and 10. To find a longer string of consecutive composites, say seven in a row, the smallest sequence of numbers that works is 90, 91, 92, 93, 94, 95, and 96. To find even longer strings of consecutive composites, we would have to use larger numbers. This illustrates that as numbers get bigger, the primes get more spread out.

In fact, we can generate a list of consecutive composite numbers of any length. We will look at how to do this using an example (Note that this method will not necessarily provide the sequence of the smallest possible integers that work, but it is easily adapted to any desired sequence length).

Before going through the method, let us take a moment to review *factorials*. Remember that the factorial of a number is the product of that number and the positive integers less than that number. So, for example, $3! = 3 \cdot 2 \cdot 1$, and $10! = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$. Notice that each positive integer less than or equal to n will be a divisor of $n!$ (although this is not a complete list of the divisors).

To see how this method works, start with a small example. Suppose you want to find 4 consecutive composite integers. Since $4! = 4 \cdot 3 \cdot 2 \cdot 1$, we see right away that 2, 3, and 4 are all divisors of 4!. Since we want 4 consecutive integers, begin with $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ so that 2, 3, 4, and 5 are divisors. To make consecutive numbers, form the sequence 5! + 2, 5! + 3, 5! + 4, and 5! + 5 or 122, 123, 124, and 125. Notice that the first number will be divisible by 2 since it divides both terms of the sum, the second will be divisible by 3, and so on.

Example 4.15 Find eight consecutive composite integers.

Solution
To get eight consecutive integers, start with 9! + 9 and work down to 9! + 2. The list of integers is:

$$9! + 9, \quad 9! + 8, \quad 9! + 7, \quad 9! + 6, \quad 9! + 5, \quad 9! + 4, \quad 9! + 3, \quad 9! + 2$$

Then, the first integer is divisible by 9, the second by 8, the third by 7, and so on, guaranteeing that all values on this list are composite.   ◈

Since the technique in the example above can be adapted for any number of consecutive composite integers, we can find a gap between primes of any length.

The second question is whether or not there is a formula that will always generate primes. Take a few minutes to test the following conjecture related to this question:

Conjecture 4.1: The formula $6n + 5$ is prime for all values of $n \geq 1$.

No one has been able to find a practical formula which generates only primes (If you did not find a non-prime result testing the conjecture above, go back and try a few more examples). The next best thing is a formula that will generate primes infinitely often; such a formula may not produce a prime every time an integer is substituted, but there is a never-ending collection of integers that will result in a prime when substituted into the formula. Several formulas or types of formulas which generate primes infinitely often have been found. In some cases, it has been proven that the formula will generate infinitely many primes, and in other cases it is still a conjecture. The following are some examples of conjectures about primes:

1. **Landau Problems**
   At the 1912 International Congress of Mathematicians, a large mathematics conference held every four years, the German mathematician Edmund Landau listed four statements or questions about primes that sounded simple but had not yet been proven true or false. As of 2012, no one has yet been able to definitively answer the question of whether each of these statements is true or false:

   (a) **Goldbach's conjecture:** Every even integer greater than 2 can be written as the sum of two primes.
       This statement is very approachable—you can start checking even integers right now. Even though it is easy to work with, no one has been able to prove it true or false.

   (b) **Twin prime conjecture:** There are infinitely many primes p such that p and $p+2$ are both prime.
       Although people have found very large pairs of twin primes, and mathematicians suspect this statement is true, no one has been able to prove it true or false.

   (c) **Legendre's conjecture:** There always exists at least one prime between two consecutive perfect squares (n^2 and $(n+1)^2$).
       This is another conjecture you can start testing right away. For example, if $n = 2$, then we are looking for a prime between 4 and 9. There are two in this case: 5 and 7. Mathematicians suspect this conjecture is true, but it has yet to be proven.

   (d) **Near-square prime conjecture:** There infinitely many primes of the form $n^2 + 1$.
       We can find some primes of this form: if $n = 1$, then $n^2 + 1 = 2$, and if $n = 2$, then $n^2 + 1 = 5$. Primes of this form are called ***near-square primes***, because if $p = n^2 + 1$, then $p - 1 = n^2$, a perfect square. Once again, no one has been able to prove that this statement is true, but mathematicians believe there are infinitely many near-square primes.

2. **Mersenne primes**
   What about formulas of the form $a^n - 1$? Is it possible to find a value of a so that $a^n - 1$ will be a prime number for infinitely many values of n? The French mathematician Marin Mersenne (1588–1648) searched for a formula to generate prime numbers and studied numbers of the form $2^n - 1$ to look for primes.

Mersenne realized that if $2^n - 1$ was prime, then n was necessarily prime and also that the converse was false: a prime value of n does not guarantee that $2^n - 1$ is prime.

Mathematicians believe that there are infinitely many Mersenne primes, but this has not been proven even though extremely large Mersenne primes have been found.

3. **Fermat primes**

The French mathematician Pierre de Fermat studied numbers of the form $2^{2^n} + 1$, for $n \geq 0$. Numbers with this form are called **Fermat numbers** since Fermat was the first person known to study them. The first three Fermat numbers are 3, 5, and 17 (Make sure you understand the formula by computing these numbers yourself). A Fermat number which is prime is called a **Fermat prime**. From the list above, one can see that the first three Fermat numbers are prime. The fourth and fifth Fermat numbers, 257 and 65537, are prime as well. In fact, in 1650, Fermat made the conjecture that all Fermat numbers are prime. Unfortunately, every Fermat number larger than the first five that has been tested has turned out to be composite. This proves Fermat's claim false, and it seems unlikely that more Fermat primes will be found.

Exercise Set 4.5

1. (a) Find 10 consecutive composite integers.
   (b) It is possible to find any number of consecutive composite numbers. What does this tell you about the placement of primes in the integers?

2. Explain how to find 100 consecutive composite integers (Note: You do not need to write out all the numbers, but explain how to construct them).

3. Test the following conjecture and develop a hypothesis about whether it is true or false. Are you able to prove your hypothesis?
   CONJECTURE: the expression $2n^2 + 11$ is prime for all positive integers n.

4. The French mathematician Joseph Bertrand made the following conjecture in 1845.
   CONJECTURE: For every positive integer n, there is a prime p such that $n < p < 2n$:

   (a) Test the conjecture for $n = 3$, $n = 7$, and $n = 10$.
   (b) Find the smallest prime satisfying the conjecture for $n = 73$, and verify that the p you found is prime.

5. Consider the formula 9n + 16, where n is a positive integer. What is the smallest prime that can be expressed in this way? What value of n gives this prime?

6. Do an Internet search to find the largest known prime and the largest known Mersenne prime. Are they the same? How were they found?

Exercises 7–15. Test the conjecture and make a hypothesis about whether it is true or false. If possible, prove your hypothesis (Remember that a counterexample can prove a conjecture is false, but a general proof is needed to prove it is true).

7. CONJECTURE: There are infinitely many primes of the form $n^2 + 1$.
8. CONJECTURE: There are infinitely many primes of the form $n^2 - 1$.
9. CONJECTURE: There are infinitely many primes of the form $n^2 - 2$.
10. CONJECTURE: There are infinitely many primes of the form $n^2 + 5n + 6$.
11. CONJECTURE: There are infinitely many primes of the form $n^2 - 9$.
12. CONJECTURE: There are infinitely many primes of the form $n^2 + 9$.
13. CONJECTURE: There are infinitely many primes of the form $n^2 + n + 1$.
14. CONJECTURE: There are infinitely many primes of the form $n^2 + 2n + 1$.
15. CONJECTURE: There are infinitely many primes of the form $n^2 + 3n + 2$.

16. Cousin primes are primes that differ by 4. Find two pairs of cousin primes.
17. Goldbach's conjecture states that every even number greater than 2 is a sum of two primes:

   (a)   Show that the conjecture holds true for 26 and for 40.
   (b)   Although Goldbach's conjecture only specifies that an even number can be written as the sum of two primes in one way, often there is more than one way. Find all the ways that 60 can be written as the sum of two primes.
   (c)   Show that 11 cannot be written as the sum of two primes. Explain why this is not a counterexample for Goldbach's conjecture.

4.6   Summary and Review Exercises

4.6.1   Vocabulary and Symbols

prime
composite
Primality Test
Sieve of Eratosthenes
Fundamental Theorem of Arithmetic
prime factorization
prime power factorization
$2\mathbb{Z}$
divides in $2\mathbb{Z}$
prime in $2\mathbb{Z}$
twin primes
near-square primes
Mersenne primes
Fermat primes

4.6.2   Suggested Readings

Devlin, Keith. *World's Largest Prime*. **Focus** (The newsletter of the Mathematical
Association of America) Vol. 17, (December, 1997) p 1.

Doxiadis, Apostolos. *Uncle Petros and Goldbach's Conjecture: A Novel of Math-
ematical Obsession*. Bloomsbury USA. 2001.

Granville, Andrew. *Prime Number Patterns*. **The American Mathematical
Monthly.** Vol. 115 (April, 2008) pp. 279–296.

Schwartz, Richard Evan. *You Can Count on Monsters*. Natick: A. K. Peters,
Ltd. 2010.

4.6.3   Review Exercises

1. When using the Primality Test to see if 377 is prime, what primes must be
   tested to see if they are divisors of 377? Is 377 prime or composite?
2. Determine which of the following integers are prime: 113, 201, 213, 221, 259.

Exercises 3–12. Find the prime power factorization.

3. 3465
4. 40320
5. 7865
6. 36465
7. 34890
8. 16281
9. 14641
10. 12342
11. 13392
12. 6795

13. Determine if 1111111111 is prime, and find its prime factorization.
14. Determine if 13579 is prime. If it is not, factor it completely into the product of
    primes.
15. Determine if 123456789 is prime. If it is not, find its prime factorization.
16. Determine if 987654321 is prime. If it is not, find its prime factorization.
17. Given two integers m and n, the prime factorization of these is
    $m = 2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11$ and $n = 2 \cdot 3 \cdot 11$.

    (a) Find $\gcd(m, n)$.
    (b) Find $lcm(m, n)$.

18. True or false. If false, give a counterexample:

    (a) There are infinitely many primes of the type $n^2 - 49$.
    (b) If p is prime, then $2^p - 1$ is prime.
    (c) There is an infinite number of primes.

19. Twin primes:

    (a) Find the first 8 twin prime pairs $(p, p+2)$.
    (b)   Using (a), find the values you obtain when you add 1 to the product of each pair of twin primes.
    (c) Use (b) to make a conjecture/generalization about twin primes p and $p+2$.

20. Prove or disprove: If p, q, and r are odd primes, then $pqr+1$ is composite.
21. If p and q are distinct primes, find all positive divisors of pq.
22. Find all integers with exactly five positive factors. Provide some examples and a general formula.
23. Consider the following three integers in prime factorization form:

$$a = 2^2 \cdot 3^2 \cdot 5^2 \cdot 11; \qquad b = 2 \cdot 5^3 \cdot 11 \cdot 17; \qquad c = 2^2 \cdot 3^2 \cdot 11^2 \cdot 17$$

    (a) Use the above prime factorizations to determine $\gcd(a, b, c)$.
    (b) Use the above prime factorization to determine $lcm(a, b, c)$.

Exercises 24–29. Use prime power factorization to find the greatest common divisor.
24. gcd(756, 2205)
25. gcd(4725, 17460)
26. gcd(465, 3861)
27. gcd(4600, 2116)
28. gcd(630, 990)
29. gcd(96, 144)

Exercises 30–35. Use prime power factorization to find the least common multiple.
30. lcm(756, 2205)
31. lcm(4725, 17460)
32. lcm(465, 3861)
33. lcm(4600, 2116)
34. lcm(630, 990)
35. lcm(96, 144)

Chapter 5
The Euclidean Algorithm

"An algorithm must be seen to be believed."

—Donald Knuth, 1938–Present

5.1   The Division Algorithm

In Section 2.8, the definition of the greatest common divisor of two (or more) integers was introduced, and this concept was used in Chap. 3 in order to determine whether or not a particular right triangle was primitive. In Exercise 34 of Section 3.2, you were asked to determine whether or not $100 - 621 - 629$ was a primitive Pythagorean triple. Larger numbers made it more difficult to find the greatest common divisor by trial and error, but this problem came up again as Example 4.9, where prime factorizations were used to make it easier to find the greatest common divisor of these three numbers.

Using prime factorizations allows us to find the greatest common divisor of a set of integers quickly, as long as the prime factors of the original integers can be found. However, even with the Primality Test developed in Section 4.1, as numbers get larger, it becomes very labor intensive and eventually impractical to find their prime factorizations, even using super computers. This fact is the basis of one of the encryption techniques discussed in Chap. 8.

The next section introduces an algorithm called the Euclidean Algorithm, developed by Euclid, which is a step-by-step process to calculate the value of the greatest common divisor of any two integers, no matter how large. Each step of the Euclidean Algorithm is based on division of whole numbers: what happens when one integer is divided by another. If an integer c is divided by another positive integer d, there are two possible outcomes:

1. c is a multiple of d, which means d divides c evenly, OR

2. c falls between two consecutive multiples of d, that is, c leaves a remainder when divided by d. Consecutive multiples are numbers that differ by d. For example, if $d = 7$, then the pair 14, 21 or the pair 28, 35 are examples of consecutive multiples of 7 (In general, if m is a multiple of d, then m and $m + d$ are consecutive multiples. Another way to say this is that if $m = kd$, then $(k + 1)d$ is a consecutive multiple).

Let us look at a specific example. Suppose that $d = 4$. Then, if $m = 20$, m is a multiple of 4 since $20 = 5(4)$. If $c = 17$, then c is not a multiple of 4, but c falls between the two multiples $16 = 4(4)$ and $20 = 5(4)$. And, if $c = 3$, then c falls between the multiples $0 = 0(4)$ and $4 = 1(4)$. To see this clearly, list out the integers, with the multiples of 4 in bold:

$\ldots, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \ldots$

Notice that if you start on a multiple of 4, you will get to another multiple of 4 by adding 4: $0 + 4 = 4$ and $-8 + 4 = -4$, for example. Also, if you choose a number that is not a multiple of 4, it will be between two consecutive multiples. This means that it must be within 3 of a multiple. For example, $13 = \mathbf{12} + 1$, $14 = \mathbf{12} + 2$, and $15 = \mathbf{12} + 3$. This will be true for larger numbers as well. The integer 133 is not a multiple of 4, but it lies between $132 = 33(4)$ and $136 = 34(4)$, and $133 = 132 + 1$. More generally, any integer c can be written as $c = q \cdot 4 + r$, where q is an integer and r is 0, 1, 2, or 3.

The pattern for the integer 4 illustrated above will work for any positive integer. So, if d is any positive integer and c is any integer, then either c is divisible by d (in which case $c = qd$ for some integer q) or c is between consecutive multiples qd and $(q + 1)d$ for some integer q. Combining these two possibilities we get the following equation:

$c = qd + r$ where r is one of the numbers 0, 1, 2, $\ldots$, $d - 1$.

This relationship is called the division algorithm and is stated here:

Division Algorithm
Let d be a positive integer. Then for any integer c, $c = qd + r$ where $q \in \mathbb{Z}$ and $0 \leq r < d$. In this equation, q is called the **quotient**, d is called the **divisor**, r is called the **remainder**, and c is called the **dividend**.

The division algorithm is another way to write the process you perform when doing long division. For example, suppose that you are dividing 34 by 4. Then $c = 34$ and $d = 4$.

$$\begin{array}{r} 8 \\ 4\overline{)34} \\ 32 \\ \hline 2 \end{array}$$

Since 34 is not a multiple of 4, 34 falls *between* two consecutive multiples of 4: 8 (4) = 32 and 9(4) = 36. Since 34 = 8(4) + 2, the remainder is 2 when 34 is divided by 8, as shown in the division above.

Here are some examples using the division algorithm.

Example 5.1 In each example, divide c by d and then use the division algorithm to express the result:
(a) $d=5$, $c=9$ (b) $d=256$, $c=1024$

Solution
(a) $d=5$ and $c=9$

$$9 = 1(5) + 4.$$

The quotient, q, is 1 and the remainder, r, is 4.
(b) $d=256$ and $c=1024$

$$1024 = 4(256) + 0$$

The quotient is $q=4$, and since 1024 is a multiple of 256, the remainder is 0.

◈

Example 5.2 In each example, divide c by d and then use the division algorithm to express the result:
(a) $d=7$, $c=555$ (b) $d=8$, $c=6$ (c) $d=4$, $c=-22$

Solution
(a) $d=7$ and $c=555$
$$555 = 79(7) + 2$$

Note: To find the quotient, in this case 79, you are looking for the largest multiple of 7 that is still less than 555. If you divide 555 by 7 on the calculator, the whole number part of the answer (not the decimal) will be the quotient. Then to find the remainder, subtract $555 - 79(7)$ which is equal to 2.

(b) $d=8$ and $c=6$
Here, 6 is being divided by 8, but since 8 is bigger than 6, 8 does not divide 6 a whole number of times. Notice that 6 is between the multiples 0 (8) = 0 and 1 (8) = 8, so the quotient is 0 and the remainder is 6.

$$6 = 0(8) + 6$$

(c) $d = 4$ and $c = -22$

Since 4 does not divide -22 evenly, to find the quotient and remainder, we need the largest multiple of 4 that is less than -22. In this case, this will be -24 (not -20, since -20 is larger than -22). So,

$$-22 = -6(4) + 2$$

Often when performing division, we are most interested in the quotient: how many times one number divided another number evenly. The division algorithm also displays the remainder, which is also useful. There are many applications for grouping numbers together that have the same remainder when divided by a particular integer. Some examples of this using the division algorithm follow. Then, in Chap. 6, arithmetic with remainders and some of its applications will be covered in more detail.

Suppose that we are dividing integers by the number 4. Because the multiples of 4 are spaced 4 apart, the possible remainders when dividing by 4 are 0, 1, 2, or 3. Every integer has to have one of these remainders when divided by 4. Table 5.1 contains a few examples.

Table 5.1 Result of dividing n by 4

n	Division Algorithm	Remainder
4	$4 = 4(1) + 0$	0
7	$7 = 4(1) + 3$	3
45	$45 = 4(11) + 1$	1
10	$10 = 4(2) + 2$	2
17	$17 = 4(4) + 1$	1

Notice that each possible remainder shows up at least once in the table above, and 45 and 17 both have a remainder of 1 when divided by 4. What other numbers have a remainder of 1? From the division algorithm, if n is going to have a remainder of 1 when divided by 4, then n must fit the equation $n = 4q + 1$. This equation provides a way to find a list of all integers that have a remainder of 1 since the quotient q can be any integer. Choosing the values 1, 2, 3, and -3 for q, shows that 5, 9, 13, and -11 all have a remainder of 1 when divided by 4. (Check these and confirm that their remainder is 1.)

Example 5.3 Write a formula to represent all integers n that have a remainder of 3 when divided by 7. Then, find two negative integers and two positive integers that have a remainder of 3 when divided by 7.

Solution
From the division algorithm, if n has a remainder of 3 when divided by 7, then n can be written as $n = 7q + 3$, where q is an integer. Picking different values for q shows that there are both positive and negative values for n. Also notice that when we increase q by 1, n increases by 7.

q	n
-2	$7(-2)+3=-11$
-1	$7(-1)+3=-4$
0	$7(0)+3=7$
1	$7(1)+3=10$
2	$7(2)+3=17$
3	$7(3)+3=24$

From the table above, two negative values with a remainder of 3 when divided by 7 are -11 and -4 and two positive values are 10 and 17.

◆

Exercise Set 5.1

Exercises 1–14. For each value of d and c, find the quotient when dividing c by d, and then write the result in the form $c = qd + r$ from the division algorithm.

1. d = 4, c = 160
2. d = 7, c = 47
3. d = 7, c = 28
4. d = 11, c = 567
5. d = 18, c = 9
6. $d = 15$, $c = 7$
7. $d = 8$, $c = 6$
8. d = 6, c = -26
9. d = 12, c = -34
10. d = 14, c = 1567
11. d = 4, c = 8k
12. d = 3, c = 21k
13. d = 6, c = 6k + 15
14. d = 5, c = 5k + 32

15. Why might one want to know the remainder when a number is divided by 7? What about 12? Think of an example of how each of these could be used.
16. Explain what is wrong with the following if the division algorithm is being applied, and correct it:
    Suppose you want to divide 37 by 7. Since $4(7) = 28$, we can say 7 evenly divides 37 four times, with a remainder of 9, or $37 = 4(7) + 9$.
17. List each possible remainder when dividing an integer by 3. Find several different integers that have each remainder. What patterns do you notice?
18. List each possible remainder when dividing an integer by 6. Find several different integers that have each remainder. What patterns do you notice?
19. Write a formula to represent all integers that have a remainder of 4 when divided by 5.

20. Write a formula to represent all integers that have a remainder of 3 when divided by 8.
21. Suppose that you are dividing integers by 2.

    (a)   Fill in the missing values in the following table. What patterns do you see?

a	Quotient when a is divided by 2	Remainder when a is divided by 2
0	0	0
1	0	1
2		
3		
4		
5		
6		
7		
8		
9		
14		
31		

    (b)   Find an example of a number bigger than 200 with a remainder of 0 when divided by 2.
    (c)   Find an example of a number bigger than 200 with a remainder of 1 when divided by 2.

22. Prove the following conjecture true or false (First, test the conjecture on several examples).
    Conjecture: Two consecutive odd integers can never both be divisible by 3.
23. Prove that if $n \in \mathbb{Z}$, then n^2 is divisible by 4 or has a remainder of 1 when divided by 4. (Hint: Look at the cases when n is even and when n is odd separately.)

5.2   The Euclidean Algorithm

An *algorithm* is a step-by-step process that concludes with the answer to the question it is meant to solve in a finite number of steps (if applied correctly).[1]

The *Euclidean Algorithm* is a method for finding the greatest common divisor of any two integers. In contrast to the methods we have already developed to find the greatest common divisor of two integers, the Euclidean Algorithm does not become more labor intensive as the numbers involved get larger. Each step of the Euclidean

---

[1] The "division algorithm" is technically not an algorithm under this definition, but this name has become standard.

Algorithm is an application of the division algorithm. It is not complicated, but it requires careful algebra and some patience. We begin with a few specific examples to see *how* the Euclidean Algorithm works. Then, after stating the general form for the Euclidean Algorithm, we will analyze *why* it works.

Example 5.4 Find gcd(146, 60) using the Euclidean Algorithm.

Solution
We will illustrate the steps of the Euclidean Algorithm for this example.

Step 1 Use the division algorithm to write the result of dividing the larger of the two numbers (in this case, 146) by the smaller number.

$$146 = 2(\mathbf{60}) + 26$$

Step 2 Apply the division algorithm again, to divide the divisor from Step 1 (in this case, 60) by the remainder from Step 1 (in this case 26).

$$\mathbf{60} = 2(26) + 8$$

Step 3 Apply the division algorithm to divide the divisor from Step 2 (26, in this example) by the remainder in Step 2 (8, in this example).

$$26 = 3(8) + 2$$

Continue to repeat this process until the remainder is 0.

Step 4 Since the remainder is nonzero, divide the divisor from Step 3 (8, in this example) from remainder in Step 3 (2, in this example).

$$8 = 4(2) + 0$$

This 0 remainder means that the Euclidean Algorithm is complete. The last nonzero remainder is the greatest common divisor of the original two numbers, so gcd(146, 60) = 2. (Prime factorization can be used to confirm that this is correct.)

◈

The next example illustrates the usefulness of the Euclidean Algorithm. It is possible to find the greatest common divisor of 2059 and 2581 by listing all of their factors or finding their prime factorizations, but you probably would not want to.

Example 5.5 Find gcd(2059, 2581) using the Euclidean Algorithm.

Solution
The first step of the Euclidean Algorithm is again to find the quotient and remainder when the larger of the two numbers is divided by the smaller number, and then write the result using the division algorithm.

$$2581 = 1(2059) + \mathbf{522}$$

Repeat the same process, dividing the divisor by the remainder.

$$2059 = 3(\mathbf{522}) + \mathit{493}$$

Repeat until the remainder is zero.

$$\mathbf{522} = 1(\mathit{493}) + \mathbf{29}$$
$$\mathit{493} = 17(\mathbf{29}) + 0$$

Therefore, according to the Euclidean Algorithm, gcd(2059, 2581) = 29.

◆

To describe the process used in the Euclidean Algorithm in general, we will use letters to represent the steps. In order to make it easier to follow, the remainders will be designated by r_1, r_2, …. The number of remainders will depend on how many lines are needed to get to a zero remainder. This will always happen since the remainders must get smaller each time, but they can never be negative.

The quotients in each step will be designated by q_1, q_2, … and so on, depending on how many steps are needed. Here is a general statement of the algorithm. When you look at the general steps, notice that both the divisor and the remainder from the previous line carry down to the next line.

The Euclidean Algorithm

Let a and b be two positive integers, with b the bigger of the two integers. To find the greatest common divisor of a and b, apply the division algorithm repeatedly as shown. The last nonzero remainder, r_n, is the greatest common divisor of a and b.

$$b = q_1 a + r_1 \qquad 0 \le r_1 < a,$$
$$a = q_2 r_1 + r_2 \qquad 0 \le r_2 < r_1,$$
$$r_1 = q_3 r_2 + r_3 \qquad 0 \le r_3 < r_2,$$
$$r_2 = q_4 r_3 + r_4 \qquad 0 \le r_4 < r_3,$$
$$\vdots \qquad\qquad \vdots$$
$$r_{n-2} = q_n r_{n-1} + \mathbf{r_n} \quad 0 \le \mathbf{r_n} < r_{n-1},$$
$$r_{n-1} = q_{n+1} \mathbf{r_n} + 0$$

Then, gcd(a, b) = r_n.

Another example of applying the Euclidean Algorithm follows.

Example 5.6 Use the Euclidean Algorithm to find gcd(3829, 561).

Solution

$$3829 = 6(561) + 463$$
$$561 = 1(463) + 98$$
$$463 = 4(98) + 71$$
$$98 = 1(71) + 27$$
$$71 = 2(27) + 17$$
$$27 = 1(17) + 10$$
$$17 = 1(10) + 7$$
$$10 = 1(7) + 3$$
$$7 = 2(3) + 1$$
$$3 = 3(1) + 0$$

Therefore, according to the Euclidean Algorithm, gcd(3829, 561) = 1.

◆

It may seem surprising that not only does the last nonzero remainder divide both a and b, but that it is also the greatest common divisor of a and b. Let us see why this is true.

Suppose the Euclidean Algorithm is being used to find gcd(a, b), where b is the larger number. Then, the first step of the Euclidean Algorithm is

$$b = q_1 a + r_1$$

We are interested in how common divisors of a and b are related to the remainder r_1, so suppose that d is a common divisor of a and b. Then, $d|a$ and $d|b$. From the definition of divides, $a = dm$ for some $m \in \mathbb{Z}$ and $b = dk$ for some $k \in \mathbb{Z}$. Substituting these expressions into the first step of the Euclidean Algorithm, we find that

$$dk = q_1(dm) + r_1$$

Solving for r_1,

$$r_1 = dk - q_1 dm$$

Notice that both terms on the right have a factor of d, so

$$r_1 = d(k - q_1 m)$$

Since $\mathbb{Z}$ is closed under multiplication and subtraction, $k - q_1 m \in \mathbb{Z}$. Therefore, $d|r_1$.

This argument proves the following theorem about the relationship between the common divisors of two numbers and the remainder when one number is divided by the other.

Theorem 5.1
If a and b are integers and r is the remainder when b is divided by a, then any common divisor of a and b will also divide r.

Since we are interested in finding the greatest common divisor of a and b, the following corollary will be useful. (Corollaries are statements that are very closely related to theorems. They are often a special case or example of a theorem, but are used often enough that it makes sense to clearly state them, rather than reproving the result each time it is used.)

Corollary 5.1
If a and b are integers, and r is the remainder when b is divided by a, then gcd $(a, b) = \gcd(a, r)$.

Proof. Let a and b be integers and let r be the remainder when b is divided by a. From the division algorithm, $b = qa + r$. Also, by Theorem 5.1, any common divisor of a and b also divides r. Now, suppose that m is a common divisor of a and r. Since $m | a$ and $m | r$, there are integers k and l such that $a = mk$ and $r = ml$. Substituting these values into the division algorithm equation produces the following equation:

$$b = q(mk) + ml$$
$$b = m(qk + l)$$

Since $qk + l \in \mathbb{Z}$, this tells us that $m | b$. Therefore, any common divisor of a and r is also a common divisor of a and b. Since the two pairs of integers share exactly the same common divisors, the greatest common divisor must be the same. Therefore, $\gcd(a, b) = \gcd(a, r)$.

∎

Now we can use Corollary 5.1 to show that the Euclidean Algorithm produces the correct result for the greatest common divisor of a and b.

	Performing the Euclidean Algorithm	Applying Corollary 5.1
Step 1	$b = q_1 a + r_1$	$\gcd(a, b) = \gcd(a, r_1)$.
Step 2	$a = q_2 r_1 + r_2$	$\gcd(r_1, a) = \gcd(r_1, r_2)$.
Step 3	$r_1 = q_3 r_2 + r_3$	$\gcd(r_2, r_1) = \gcd(r_2, r_3)$.
Step 4	$r_2 = q_4 r_3 + r_4$	$\gcd(r_3, r_2) = \gcd(r_3, r_4)$.
⋮	⋮	⋮
Step n	$r_{n-2} = q_n r_{n-1} + r_n$	$\gcd(r_{n-1}, r_{n-2}) = \gcd(r_{n-1}, r_n)$.
Step $n+1$	$r_{n-1} = q_{n+1} r_n + 0$	$\gcd(r_n, r_{n-1}) = \gcd(r_n, 0) = r_n$.

Looking at the steps above, notice the pattern in the results from Corollary 5.1. Through these equations, we see that

$$\gcd(a, b) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \gcd(r_3, r_4) = \cdots = \gcd(r_{n-1}, r_n)$$
$$= \gcd(r_n, 0) = r_n$$

Because of the "..." that remains in the steps above, this is not a completely formal proof, but it shows that the algorithm does work in general.

If you still are not convinced of the usefulness of the Euclidean Algorithm, try finding the answer to the next example using another method before applying the Euclidean Algorithm.

Example 5.7 Find gcd(54516, 25830).

Solution
Step 1 Use the division algorithm to write the result of dividing 54516 by 25830. Since 25830 divides 54516 evenly twice, the remainder will be

$$\text{remainder} = 54516 - 2(25830) = 2856$$

Therefore, the first step of the Euclidean Algorithm is

$$54516 = 2(25830) + 2856$$

Step 2 Since the remainder is not zero, repeat the process, dividing 25830 by 2856.

$$25830 = 9(2856) + 126$$

Step 3 Continue dividing the divisor by the remainder, until you reach a remainder of zero.

$$2856 = 22(126) + 84$$

Since the last remainder is not zero, repeat:

$$126 = 1(84) + 42$$

Repeat again:

$$84 = 2(42) + 0$$

The last nonzero remainder is 42.

Hence, $42 = \text{gcd}(54516, 25830)$. (Check to see that 42 really does divide both of these numbers.)

◈

Before finishing this section, here is one more example.

Example 5.8 Find gcd(24, 192) using the Euclidean Algorithm.

Solution
Applying the division algorithm produces the equation $192 = 8(24) + 0$ for the first step of the Euclidean Algorithm. There is no line with a nonzero remainder since

24 divides 192 evenly. This means that 24 must be the greatest common divisor of these two numbers since 24 is the largest number that can divide itself, and 24 also divides 192.

◈

Theorem 5.2 states that the result from Example 5.8 is true in general.

Theorem 5.2
If a is a positive integer and $a|b$, then $\gcd(a, b) = a$.

The proof of Theorem 5.2 is left as Exercise 17.

Exercise Set 5.2

Exercises 1–11. Use the Euclidean Algorithm to find the greatest common divisor.

1. gcd(693, 231)
2. gcd(294, 588)
3. gcd(1045, 1265)
4. gcd(693, 165)
5. gcd(2145, 345)
6. gcd(266, 644)
7. gcd(595, 1463)
8. gcd(2059, 581)
9. gcd(8898, 72720)
10. gcd(12, 1812705)
11. gcd(543, 123456)
12. Think of another algorithm you have learned either inside or outside of a mathematics class. Carefully write down the steps of the algorithm.
13. (a) By testing several values for m, develop a conjecture about $\gcd(m, m+1)$.
     (b) Either prove that your conjecture is true or find a counterexample to show it is false. If the conjecture is false, revise it so that it is true. (Hint: try the Euclidean Algorithm to prove the conjecture true.)
14. Form a conjecture about the greatest common divisor of two consecutive even integers. Then either prove that your conjecture is true or find a counterexample to show it is false. If the conjecture is false, revise it so that it is true, and prove it.
15. Form a conjecture about the greatest common divisor of two consecutive odd integers. Then either prove that your conjecture is true or find a counterexample to show it is false. If the conjecture is false, revise it so that it is true, and prove it.
16. Prove **Theorem 5.1.**
17. Prove **Theorem 5.2.**

5.3   Solving Linear Equations in Two Variables and the Euclidean Algorithm Backwards

The Euclidean Algorithm can be used to find the greatest common divisor of any two integers. Once the greatest common divisor is found, it can be useful to find relationships between the integers a and b and their greatest common divisor in addition to the definition of greatest common divisor. For example, are there always integers x and y such that $ax + by = \gcd(a, b)$, and if so, is there a method to find them? The expression $ax + by$ is called a *linear combination of a and b*. Notice that another way to ask this question is "Is it always possible to find integers x and y that solve the linear equation $ax + by = \gcd(a, b)$?"

Equations of the form $ax + by = c$ are called *linear equations* because their graph is a straight line. Solving the equation $ax + by = c$ for y, we obtain the familiar slope-intercept form of a line.

$$ax + by = c$$
$$by = -ax + c$$
$$y = \frac{-a}{b}x + \frac{c}{b}$$

The last equation above shows that $ax + by = c$ represents a line with slope $\frac{-a}{b}$ and y-intercept $\frac{c}{b}$.

To graph the line represented by the equation $ax + by = c$, choose a value for x, and then solve for y to see what value makes the equation true. This pair of values (x, y) represents both a solution to the equation as well as a point on the graph of the line.

For example, consider the equation $3x + 4y = 1$. Choosing $x = 1$, and then solving for y, we obtain $y = \frac{-1}{2}$. This means that $x = 1$, $y = \frac{-1}{2}$ is a solution to the equation $3x + 4y = 1$, and that the point $\left(1, \frac{-1}{2}\right)$ is on the graph of the equation, shown in Fig. 5.1. Similarly, if $x = -1$, solving for y shows that $y = 1$, so $x = -1$, $y = 1$ is a solution of the equation, and $(-1, 1)$ is a point on the graph. Notice that in the first case, the value for y that solved the equation is not an integer, but in the second case, both x and y have integer values. When both x and y are integers, we call them an *integer solution* of the equation. Every linear equation of the form $ax + by = c$ will have infinitely many solutions, since each point on the line represents a solution. The question we want to answer is when linear equations $ax + by = c$ will have *integer* solutions.

Example 5.9 Find an integer solution to the linear equation $12x + 20y = \gcd(12, 20)$.

Solution
First, $\gcd(12, 20) = 4$, so we are looking for an integer solution to the equation $12x + 20y = 4$. In algebra, you may have learned techniques for solving linear equations in one variable and systems of two linear equations in two variables,
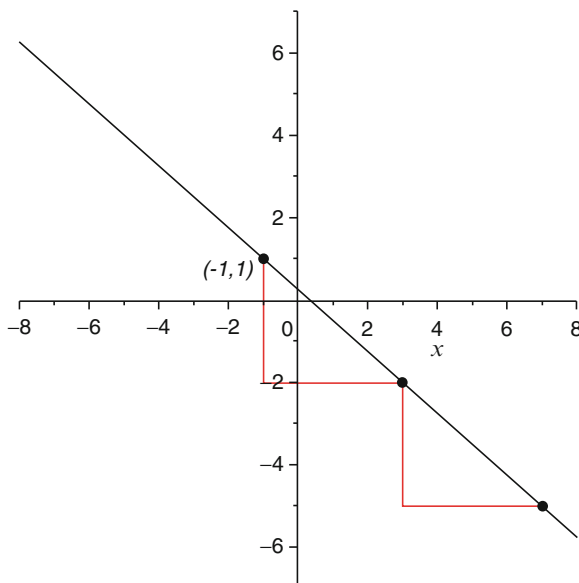
Fig. 5.1 Graph of $3x + 4y = 1$

but right now we do not have a systematic way to solve this equation. Before continuing, see if you can find a solution on your own.

To start looking for an integer solution, first notice that since 4 is less than both 12 and 20, either x or y will be negative. Since $12(2) = 24$ which is four more than 20, $x = 2$, $y = -1$ is a solution to the equation. Notice that $x = -3$, $y = 2$ is also a solution (Since this is a linear equation with two variables, the solution is not unique). To test other possible solutions, substitute the values for x and y into the original equation to see if they make it true.

◈

In Example 5.9, we guessed some solutions to the equation, and you can probably find some more, but finding solutions by trial and error will be harder with larger numbers. However, the question of which equations of this type have integer solutions and how to find them is related to the Euclidean Algorithm. By working backwards through the steps of the Euclidean Algorithm, we can find integer values for x and y that solve the equation $ax + by = \gcd(a, b)$. Since the Euclidean algorithm can always be used to find the greatest common divisor of a and b for any integers a and b, this also means that the equation $ax + by = \gcd(a, b)$ always has at least one integer solution. This method of using the Euclidean Algorithm backwards is demonstrated in the next example.

Example 5.10 Find an integer solution to the equation $345x + 285y = \gcd(345, 285)$.

Solution

First, use the Euclidean Algorithm to find $\gcd(345, 285)$.

$$345 = 1(285) + 60$$
$$285 = 4(60) + 45$$
$$60 = 1(45) + 15$$
$$45 = 3(15) + 0$$

Therefore, $\gcd(345, 285) = 15$. The first step in working backwards through the Euclidean Algorithm is to solve each step with a nonzero remainder for its remainder. These steps are shown here, with the original Euclidean Algorithm on the left and the equation solved for its remainder on the right.

Euclidean Algorithm Steps	Step Solved for the Remainder
$345 = 1(285) + 60$	$60 = 345 - 1(285)$
$285 = 4(60) + 45$	$45 = 285 - 4(60)$
$60 = 1(45) + 15$	$15 = 60 - 1(45)$
$45 = 3(15) + 0$	---------

Notice that the last line in the "Solved for the Remainder" column has the greatest common divisor on the left side. Starting at the bottom with this line, substitute the equation from the line before it, until we work our way up to the top equation.

Step 1 Begin with the last equation, set equal to the greatest common divisor of the original two numbers.

$$15 = 60 - 1(45)$$

Step 2 (Substitution) Move up one equation, and use it to substitute for the remainder from the previous line (in this case 45).

$$15 = 60 - 1(285 - 4(60))$$

Step 3 (Algebra–distribute and combine like terms) This algebraic step makes the rest of the substitutions simpler. Looking up to the next equation on the list, we see that it is solved for the remainder 60. Notice that in the equation in Step 2, the value 60 appears twice. Before carrying out the next substitution, it is useful to distribute through the parentheses and combine like terms. Note that we do not multiply through by the coefficients, in order to keep track of the remainders from the Euclidean Algorithm.

$$15 = 60 - 1(285) + 4(60)$$
$$15 = 60 + 4(60) - 1(285)$$
$$15 = 5(60) - 1(285)$$

Step 4 (Substitution) Move up one more equation, and use it to substitute for the remainder from the previous line (in this case, 60).

$$15 = 5(345 - 1(285)) - 1(285)$$

Step 5 (Algebra–distribute and combine like terms) Now that all of the equations have been used, the greatest common divisor should be in terms of the original two numbers now. Simplify and combine like terms to find the values of x and y.

$$15 = 5(345) - 5(285) - 1(285)$$
$$15 = 5(345) - 6(285)$$

The original equation to solve was $345x + 285y = 15$, so a solution is $x = 5, y = -6$.

◈

Example 5.11 Find an integer solution to the equation $1236x + 240y = \gcd(1236, 240)$.

Solution
First, work through the Euclidean Algorithm to find $\gcd(1236, 240)$. Those steps, as well as each line solved for the remainder, are shown below.

Euclidean Algorithm Steps	Step Solved for the Remainder
$1236 = 5(240) + 36$	$36 = 1236 - 5(240)$
$240 = 6(36) + 24$	$24 = 240 - 6(36)$
$36 = 1(24) + 12$	$12 = 36 - 1(24)$
$24 = 2(12) + 0$	---------

The goal is to have the greatest common divisor (in this example, 12) in terms of 1236 and 240. To do this, start with the bottom line on the right, and substitute for the remainder from the previous line.

Step 1 $12 = 36 - 1(24)$

Step 2 Substitute using the previous equation.

$$12 = 36 - 1(240 - 6(36))$$

Step 3 Algebra: distribute and combine like terms

$$12 = 36 - 1(240) + 6(36)$$
$$12 = 7(36) - 1(240)$$

Step 4 Substitute using the previous equation

$$12 = 7(1236 - 5(240)) - 1(240)$$

Step 5 Algebra: distribute and combine like terms

$$12 = 7(1236) - 35(240) - 1(240)$$
$$12 = 7(1236) - 36(240)$$

The problem was: Find values of x and y so that $1236x + 240\,y = 12$.
Comparing this equation with the last line of Step 5 shows that $x = 7$ and $y = -36$ is a solution.

◆

The steps used in this example to express $\gcd(a, b)$ as a linear combination of a and b will work for any problem and are summarized here.

Step 1 Solve each line in the Euclidean Algorithm for the remainder.

Step 2 Begin with the last nonzero remainder and substitute the expression from the previous line for the remainder from the previous line.

Step 3 Combine like terms.

Step 4 Replace the next remainder above the current one.

Step 5 Combine like terms.
Repeat until all the equations have been used, and the greatest common divisor is expressed in terms of the original a and b.

Example 5.12 Find integer values of x and y so that $1457x + 1891y = \gcd(1457, 1891)$.

Solution
To answer this question, first use the Euclidean Algorithm to find $\gcd(1457, 1891)$, and then work backwards to find values for x and y that solve the equation.
The Euclidean Algorithm and each step solved for its remainder are shown.

Euclidean Algorithm Steps	Step Solved for the Remainder
$1891 = 1(1457) + 434$	$434 = 1891 - 1(1457)$
$1457 = 3(434) + 155$	$155 = 1457 - 3(434)$
$434 = 2(155) + 124$	$124 = 434 - 2(155)$
$155 = 1(124) + 31$	$31 = 155 - 1(124)$
$124 = 4(31) + 0$	----

Start with the last equation on the right, solved for 31, the greatest common divisor of 1457 and 1891. Then, we will work our way up, substituting and then simplifying, until all the equations have been used, and we have an expression for 31 in terms of 1457 and 1891.

$$31 = 155 - 1(124)$$
$$= 155 - 1(434 - 2(155))$$
$$= 3(155) - 1(434)$$
$$= 3(1457 - 3(434)) - 1(434)$$
$$= 3(1457) - 10(434)$$
$$= 3(1457) - 10(1891 - 1(1457))$$
$$= 13(1457) - 10(1891)$$

This shows that a solution to the equation $1457x + 1891y = 31$ is $x = 13$, $y = -10$. Remember that you can always check the solution by substituting these values for x and y into the original equation.

◈

The fact that the greatest common divisor of a and b can always be written as a linear combination of a and b is used to prove the next result, called Euclid's Lemma.

This highlights an interesting divisibility property of prime numbers. This result was originally proved by Euclid in book VII of *Euclid's Elements*.

Theorem 5.3. Euclid's Lemma
If p is prime and $p|ab$, then $p|a$ or $p|b$.

Proof. Let p be prime.
Suppose $p \mid ab$, and $p \nmid a$. Then, in order to show that the original statement is true, we must show that $p \mid b$, since an "or" statement is true whenever at least one part is true. Now, since $p \nmid a$ and p is prime, the only divisor a and p can have in common is 1. Therefore, a and p are relatively prime, and $\gcd(a, p) = 1$. This means that there exist $r, s \in \mathbb{Z}$ such that $ra + sp = 1$. Multiplying both sides of this equation by b gives $rab + spb = b$. Now, since $p|ab$, there is an $m \in \mathbb{Z}$ such that $ab = pm$. Replacing ab in the equation above gives $rpm + spb = b$, or $p(rm + sb) = b$. Since $rm + sb \in \mathbb{Z}$, we have that $p \mid b$.   ∎

An important thing to notice about this theorem is that it would not be true if p were composite instead of prime. (Make sure that you can come up with a counterexample to show this: find three integers a, b, and c such that $a \mid bc$, but $a \nmid b$ and $a \nmid c$. Once you find an example, can you explain a method to get more examples quickly?)

Exercise Set 5.3

Exercises 1–11. Exercise 1–11 of Section 5.2 asked you to find the greatest common divisor of each pair of integers given here. Now, use the Euclidean Algorithm backwards to express the greatest common divisor of the two integers as a linear combination of the two integers.

1. gcd(693, 231)
2. gcd(294, 588)
3. gcd(1045, 1265)
4. gcd(693, 165)
5. gcd(2145, 345)
6. gcd(266, 644)
7. gcd(595, 1463)
8. gcd(2059, 581)
9. gcd(8898, 72720)
10. gcd(12, 1812705)
11. gcd(543, 123456)

12. The greatest common divisor of 256 and 140 was found using the Euclidean Algorithm, and the steps are shown below. Use the Euclidean Algorithm backwards to find a solution of the equation $256x + 140y = 4$.

$$256 = 1(140) + 116$$
$$140 = 1(116) + 24$$
$$116 = 4(24) + 20$$
$$24 = 1(20) + 4$$
$$20 = 5(4) + 0$$

13. The greatest common divisor of 1234 and 24 was found using the Euclidean Algorithm, and the steps are shown below. Use the Euclidean Algorithm backwards to find a solution of the equation $1234x + 24y = 2$.

$$1234 = 51(24) + 10$$
$$24 = 2(10) + 4$$
$$10 = 2(4) + 2$$
$$4 = 2(2) + 0$$

14. Find a solution to the equation $156x + 40y = \gcd(156, 40)$.
15. Find a solution to the equation $8x + 120\,y = \gcd(8, 120)$.
16. Prove that if $\gcd(a, b) = 1$ then there exist integers r and s such that $ra + sb = 1$.
17. Prove that any integer can be expressed as a linear combination of 7 and 9.
18. Prove that if $\gcd(a, b) = 1$ and $a|bc$, then $a|c$. Hint: Since $\gcd(a, b) = 1$, there is a solution to $ax + by = 1$. This means that there are integers m and n such that $am + bn = 1$.

19. Prove that if $\gcd(a, b) = 1$, $a|c$ and $b|c$, then $ab|c$. (This fact is used in Section 6.5 in the proof of Theorem 6.11: The Chinese Remainder Theorem.)
20. The following statement is FALSE: If $a|bc$, then $a|b$ or $a|c$. Find a counterexample and explain your example.
21. Find a counterexample to the following statement: If $a|c$ and $b|c$, then $ab|c$. Explain your example.

22. In this problem, we will look at a more general version of **Theorem 5.3: Euclid's Lemma**.

    (a) Prove that if p is prime and $p|abc$, then $p|a$ or $p|b$ or $p|c$. (Hint: you can write abc as $(ab)c$, a product of two numbers instead of three.)
    (b) Prove that if p is prime and $p|abcd$, then either $p|a$ or $p|b$ or $p|c$ or $p|d$.
    (c) **Theorem 5.3** can be generalized to a prime p dividing the product of any number of integers. The result is still that the prime p must divide one term from the product. This general statement is given below. If $n = 2$, you will get **Theorem 5.3**. Explain how you could generalize the technique from parts (a) and (b) to prove the general statement.

    General form of Euclid's Lemma: If p is prime and $p|a_1 \cdot a_2 \cdot \cdots \cdot a_n$, then $p|a_i$ for a value of i with $1 \leq i \leq n$.

5.4   More About More Solutions to $ax + by = \gcd(a, b)$

In Section 5.3, we showed that the greatest common divisor of a and b can be written as a linear combination of a and b. Another way to say this is that there is always an integer solution to the equation $ax + by = \gcd(a, b)$. Working through the steps of the Euclidean Algorithm backwards led to a method that will always produce exactly one solution to this type of equation. However, in Example 5.9, two solutions to this type of linear equation were found by trial and error. In this section we will look for a systematic method of finding all integer solutions to linear equations of this type.

We will begin with the example of a simple equation from Section 5.3: $3x + 4y = \gcd(3, 4)$, or $3x + 4y = 1$. By testing values for x and y, one solution is $x = -1$, $y = 1$. Now, the graph of the equation $3x + 4y = 1$ is made up of all the points that are solutions to the equation, so $(-1, 1)$ is a point on the graph. Also, remember that the graph of $3x + 4y = 1$ will be a straight line.

Solving $3x + 4y = 1$ for y shows that the slope-intercept form of the line is $y = \frac{-3}{4}x + \frac{1}{4}$, so the slope of this line is $\frac{-3}{4}$. The slope of a line represents the *rise* over the *run*. Once you know a point on the line, the slope provides instructions to get to another point on the line. Remember that the rise is measured in the vertical or y direction, so the rise indicates how far up or down to move to get to another point on the line. The run is measured in the horizontal or x direction, so the run indicates how far to move to the right or left to get to another point on the line.

In this example, since the rise is -3 and the run is 4, starting at a point on the line, moving down 3 units and to the right 4 units, will take us to another point on the line. This is true for any point on the line, but if we start at a point with integer coordinates, we will reach another point with integer coordinates. Since $(-1, 1)$ is an integer solution to the equation, we can find another integer solution by moving down 3 units in the vertical direction and 4 units to the right in the horizontal direction. This takes us to the point $(3, -2)$, so $x = 3, y = -2$ is another integer solution to $3x + 4y = 1$. Repeating this procedure produces the point $(7, -5)$, so $x = 7, y = -5$ is yet another integer solution to the equation. This process of using the slope to move from one point on the line to the next is illustrated on the graph in Fig. 5.2.
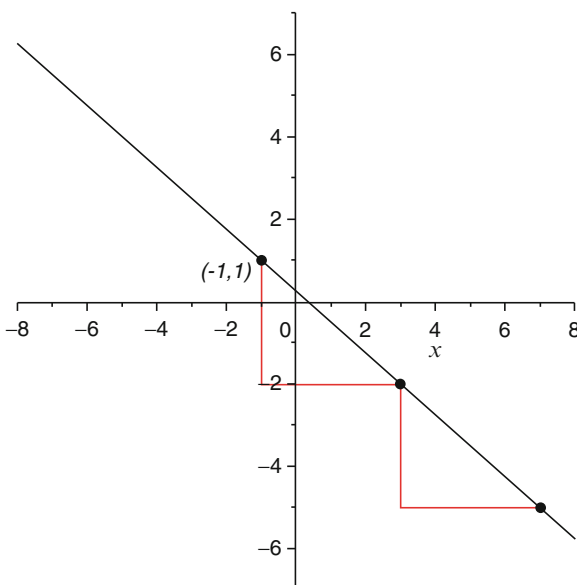
Fig. 5.2 Finding Integer Solutions of $3x + 4y = 1$

Repeating this process will produce more and more integer solutions to the equation $3x + 4y = 1$. In fact, using this method we can write general formulas for integer solutions. Starting at the first integer solution, we found $(-1, 1)$, repeatedly moving down three units and then to the right 4 units will produce another point on the line. Therefore, points with coordinates

$x = -1 + 4n$, for $n \in \mathbb{Z}$
$y = 1 - 3n$, for $n \in \mathbb{Z}$

are on the line and are therefore also integer solutions to $3x + 4y = 1$.

In general, when solving an equation of the form $ax + by = \gcd(a, b)$, the Euclidean Algorithm can always be used to find one solution. Solving the equation for y shows that $y = \frac{-a}{b}x + \frac{\gcd(a,b)}{b}$. Therefore, the slope is $\frac{-a}{b}$. Theorem 5.4 shows a general formula for solutions to $ax + by = \gcd(a, b)$.

Theorem 5.4
Let $ax + by = \gcd(a, b)$. If $x = x_0$, $y = y_0$ is one solution to this equation, then

$$x = x_0 + bn, \; y = y_0 - an$$

is also a solution, for any integer n.

Proof. Let $x = x_0$, $y = y_0$ be a solution of the equation $ax + by = \gcd(a, b)$. This means that $ax_0 + by_0 = \gcd(a, b)$. Now, to show that the new values for x and y given in Theorem 5.4 also form a solution to this equation, show that when these values are substituted into $ax + by$, the result is equal to $\gcd(a, b)$.

Substituting and simplifying,

$$\begin{aligned} a(x_0 + bn) + b(y_0 - an) &= ax_0 + abn + by_0 - abn \\ &= ax_0 + by_0 \\ &= \gcd(a, b), \end{aligned}$$

since (x_0, y_0) is a solution to the equation. Therefore, the new pair of values for x and y also gives a solution to the equation. ∎

Example 5.13 One solution to the equation $9x + 15y = 3$ is $x = -3$, $y = 2$. Find four more solutions.

Solution
According to Theorem 5.4, we can find more solutions using the formulas

$$x = -3 + 15n,$$
$$y = 2 - 9n.$$

Notice that if $n = 0$, $x = -3$ and $y = 2$, the first solution we found. The next table shows some solutions for different values of n. Remember you can always check a solution by substituting the values of x and y back into the equation.

n	$x = -3 + 15n$	$y = 2 - 9n$
-2	-33	20
-1	-18	11
1	12	-7
2	27	-16

The formulas in Theorem 5.4 produce infinitely many solutions to $ax + by = \gcd(a, b)$, but one question is whether or not they produce all possible solutions. The answer is, not always. For example, $x = 2$, $y = -1$ is a solution to the equation $9x + 15y = 3$ from Example 5.13, since $9(2) + 15(-1) = 3$, but there is no integer value of n that will produce this solution using the equations from Theorem 5.4. (Use the equations in Example 5.13 for x and y to convince yourself this is true.)

The following theorem presents the formulas to produce all solutions to equations of the form $ax + by = \gcd(a, b)$.

Theorem 5.5
Suppose that $x = x_0$, $y = y_0$ is a solution of the equation $ax + by = \gcd(a, b)$. Then, if $d = \gcd(a, b)$, all solutions have the form

$$x = x_0 + \frac{b}{d}n, \qquad y = y_0 - \frac{a}{d}n$$

where n is an integer.

We will show that if x and y have the form specified in this theorem, they do form a solution of the equation $ax + by = \gcd(a, b)$. The proof that all solutions have this form is beyond the scope of this course and is not included.

Partial Proof.
Let $x = x_0$, $y = y_0$ be a solution to the equation $ax + by = \gcd(a, b)$, and let gcd $(a, b) = d$. Then $ax_0 + by_0 = d$. Now, to show the x and y given in the theorem do form a solution, substitute into the equation and simplify to verify that the result is $d = \gcd(a, b)$.

$$
\begin{aligned}
ax + by &= a\left(x_0 + \frac{b}{d}n\right) + b\left(y_0 - \frac{a}{d}n\right) \\
&= ax_0 + \frac{ab}{d}n + by_0 - \frac{ab}{d}n \\
&= ax_0 + by_0 \\
&= d,
\end{aligned}
$$

since (x_0, y_0) was a solution to the equation. Therefore, the forms given for x and y do specify a solution to $ax + by = \gcd(a, b)$. ∎

Example 5.14 Find all solutions to the equation $12x + 20y = \gcd(12,20)$ from Example 5.9.

Solution
From Example 5.9, one of the solutions to this equation is $x = 2$, $y = -1$. By Theorem 5.5, since $\gcd(12,20) = 4$, all solutions will have the form:

$$x = 2 + \frac{20}{4}n = 2 + 5n$$

$$y = -1 - \frac{12}{4}n = -1 - 3n,$$

where n is any integer. Notice that $n = -1$, gives the solution $x = -3$, $y = 2$ which is the second solution found in Example 5.9.

◈

Exercise Set 5.4

1. When will the equations for x and y in **Theorem 5.4** produce all possible solutions to the linear equation $ax + by = \gcd(a, b)$? (Hint: Use **Theorem 5.5**.)

Exercises 2–10. Find one solution for the equation.

2. $416x + 614y = \gcd(416, 614)$
3. $12x + 510y = \gcd(12, 510)$
4. $45x + 46y = \gcd(45, 46)$
5. $14x - 42y = \gcd(14, 42)$
6. $147x + 258y = \gcd(147, 258)$
7. $10x + 17y = \gcd(10, 17)$
8. $99x - 49y = \gcd(99, 49)$
9. $14x + 42y = \gcd(14, 42)$
10. $16x + 31y = \gcd(16, 31)$

Exercises 11–19. Find all solutions to each equation from Exercises 2–10.

5.5   What If $ax + by \neq \gcd(a, b)$?

A natural question to ask now is what happens if $ax + by = c$ and c can be any integer? If c happens to be equal to $\gcd(a, b)$, then the question is already answered: There are infinitely many solutions, and after finding one solution, there are formulas to find them all. But what if $c \neq \gcd(a, b)$? Some questions that come up are:

1. Will there still always be integer solutions to the equation?
2. If there are any integer solutions, will there be infinitely many?
3. If there are integer solutions, are there formulas to find all of them?

Note that the equation $ax + by = c$ will always have infinitely many solutions, since the coordinates of each point on the graph form a solution to the equation. We are interested in *integer* solutions in particular. One way to rephrase the first question stated above is "Must every line contain at least one point with integer coordinates?" In terms of the graph, the second question can then be stated as: "If the line does contain a point with integer coordinates, will there be infinitely many such points?"

So, consider the equation $ax + by = c$ and let $d = \gcd(a, b)$. Then by Theorem 2.3, since $d|a$ and $d|b$, $d|(ax + by)$. Therefore, if the equation has an integer solution, $d|c$ as well. Forming the contrapositive of this statement gives us an answer to the first question: if $d \nmid c$, then the equation $ax + by = c$ cannot have any integer solutions.

Example 5.15 Explain why the equation $2x + 4y = 3$ cannot have any integer solutions.

Solution

Since $\gcd(2, 4) = 2$, the left-hand side can be written as $2(x + 2y)$. If x and y are integers, this represents an even integer. Since 3 is an odd integer, there are no integer solutions.

However, this equation does have (non-integer) solutions. Since every point on the line represents a solution, the values $x = \frac{1}{2}$, $y = \frac{1}{2}$ as well as $x = 1$, $y = \frac{1}{4}$ represent examples of non-integer solutions to the equation.

$\diamondsuit$

Theorem 5.6 formally states the explanation above.

> **Theorem 5.6**
> Let $d = \gcd(a, b)$. If $d \nmid c$, then there is no integer solution to $ax + by = c$.

The proof of this theorem is left as Exercise 35.

Now, suppose that $d = \gcd(a, b)$, and d divides c. Does $ax + by = c$ have integer solutions in this case?

If $d|c$, then by the definition of divides, $c = dk$ for an integer k. Therefore, we can write the equation as $ax + by = dk$.

In Section 5.3, we saw that a solution to $ax + by = d$ can always be found using the Euclidean Algorithm backwards. Let $x = x_0$, $y = y_0$ be the solution found with this method. Then,

$$ax_0 + by_0 = d.$$

Multiplying both sides of this equation by k:

$$k(ax_0 + by_0) = kd$$
$$a(kx_0) + b(ky_0) = c.$$

This shows that $x = kx_0$, $y = ky_0$ is an integer solution to $ax + by = c$ in this case. This result is summarized in the next theorem.

> **Theorem 5.7**
> Consider the equation $ax + by = c$. Let $d = \gcd(a, b)$. If $d|c$, then this equation has at least one integer solution. If (x_0, y_0) is a solution to $ax + by = \gcd(a, b)$ and $c = dk$, then a solution is given by $x = kx_0$, $y = ky_0$.

The proof of this theorem is left as Exercise 36.

Example 5.16 Find an integer solution to the equation $345x + 285y = 60$.

Solution
In Example 5.10, we found that $x = 5$, $y = -6$ is a solution to the equation $345x + 285y = 15$ where $15 = \gcd(345, 285)$. Since $60 = 4 \cdot 15$, by Theorem 5.7 we have that $x = 4 \cdot 5$, $y = 4(-6)$, or $x = 20$, $y = -24$ is a solution to $345x + 285y = 60$.

◆

> **Theorem 5.8. When $ax + bc = c$ has integer solutions**
> Let $d = \gcd(a, b)$.
>
> 1. If $d|c$, then $ax + by = c$ will have at least one integer solution.
> 2. If $d \nmid c$, then $ax + by = c$ has no integer solutions.

Now we will consider the remaining questions: (1) if there is one integer solution, are there infinitely many, and (2) is there a formula to find them?

Suppose that $d|c$ so that there is at least one integer solution to $ax + by = c$. If one solution is $x = x_0$, $y = y_0$, then the same technique used in Section 5.4 will work to find more. Solving $ax + by = c$ for y, we see that $y = \frac{-a}{b}x + \frac{c}{b}$, so the slope is $\frac{-a}{b}$. Notice that changing the right side of the equation did not affect the slope. Therefore, just as before, $x = x_0 + bn$ and $y = y_0 - an$ will be a solution to the equation for any integer n. The next theorem shows the most general form that gives all integer solutions to $ax + by = c$.

> **Theorem 5.9**
> Let $ax + by = c$, where $d = \gcd(a, b)$ and $d|c$. Then if $x = x_0$, $y = y_0$ is one solution of this equation, all solutions have the form
>
> $$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n$$
>
> where n is an integer.

Exercise 37 asks you to prove that if x and y have this form, then they will be a solution to the equation $ax + by = c$.

Example 5.17 Find all integer solutions to the equation $345x + 285y = 60$.

Solution
In Example 5.16, we found that one solution to this equation is $x = 20$, $y = -24$. Using the formulas in Theorem 5.9, all solutions are

$$x = 20 + \frac{285}{15}n = 20 + 19n,$$

$$y = -24 - \frac{345}{15}n = -24 - 23n$$

where any integer can be substituted for n. So, for example, if $n = 2$, we obtain the solution $x = 20 + 19(2) = 58$ and $y = -24 - 23(2) = -70$.

◆

Exercise Set 5.5

Exercises 1–8. Does the linear equation in two variables have an integer solution? Explain why or why not.

1. $15x + 21y = 3$
2. $4x + 6y = 35$
3. $28x - 21y = 100$
4. $12x + 18y = 50$
5. $315x + 513y = 6$
6. $235x + 5665y = 30$
7. $40x + 63y = 521$
8. $147x + 258y = 369$

Exercises 9–16. Find an integer solution of the equation.

9. $154x + 91y = 42$
10. $8x + 23y = 4$
11. $97x + 98y = 13$
12. $12x + 18y = 48$
13. $4x + 6y = 72$
14. $9x - 5y = 2$
15. $15x - 21y = 12$
16. $15x + 91y = 42$

Exercises 17–24. Find all integer solutions to the equation in Exercises 9–16.

25. Find all solutions to the linear equation $8x + 64y = 16$. Do you notice a shortcut for finding the first solution?
26. Find all solutions to the linear equation $9x + 54y = 27$. Do you notice a shortcut for finding the first solution?
27. Consider the equation $ax + 12y = 21$.

   (a) Find a value for a so that this equation will have no solutions. Explain your choice.
   (b) Find a value for a so that this equation will have a solution. Explain your choice.

28. What condition on a and b will guarantee that the equation $ax+by=c$ has a solution for any value of c?

29. Form the equation $ax+by=c$ with the values given, and then find a value for the missing number so that the equation will have a solution. Explain your choice.

   (a) $a=4$, $b=\,?$, $c=-37$
   (b) $a=\,?$, $b=-9$, $c=54$
   (c) $a=-16$, $b=48$, $c=\,?$

30. Find a value for c so that the equation $ax+8y=c$ will have integer solutions for any value of a.

31. Find a value for c so that the equation $6x+by=c$ will have integer solutions for any value of b.

32. The following statement is FALSE. Find a counterexample to the statement and explain the example: If $3|a$, $3|b$, and $3|c$, then the equation $ax+by=c$ has an integer solution.

33. You bought a new 49 gallon aquarium and some exotic fish to go with it. On your way up to the counter, the saleswoman mentions that your fish cannot survive in regular tap water, and you need to fill the tank with special fish-tropic artesian water, sold in 5 gallon and 8 gallon containers. How many containers of each size do you need to fill the tank exactly?

34. Due to various postage increases, you have a small collection of 6 cent and 15 cent stamps. If you have a letter to mail that costs 85 cents, is it possible to use your stamps to get the exact postage?

35. Prove **Theorem 5.6**. (Hint: try a proof by contradiction.)

36. Prove that if x and y are as specified in **Theorem 5.7**, they are a solution of the equation $ax+by=c$.

37. Prove that if x and y are as specified in **Theorem 5.9**, they form a solution of the equation $ax+by=c$.

38. Prove that the number 6 cannot be written as a linear combination of the integers 4 and 12 (Hint: A linear combination of 4 and 12 has the form $4x+12y$ where x and y are integers).

5.6   (Optional) Return to Primitive Pythagorean Triples

In this section, the details of the proof of the claims about the primitive Pythagorean triple formulas that were made in Section 3.2 are given. For reference, the formulas are now repeated.

Formulas for primitive Pythagorean triples
Choose integers s and t using the following rules:

(i) s and t are odd.
(ii) $s > t \geq 1$.
(iii) $\gcd(s, t) = 1$ (In other words, s and t are relatively prime.)

Then, if

$$a = st, \qquad b = \frac{s^2 - t^2}{2}, \qquad c = \frac{s^2 + t^2}{2}$$

$a - b - c$ is a primitive Pythagorean triple.

In Section 3.2, it was verified that these formulas produce Pythagorean triples, and in Section 3.3 the proof that the formulas produce all primitive Pythagorean triples was outlined.

The first result we must prove is Theorem 3.4, restated here.

Theorem 3.4
If s and t are odd positive integers such that $\gcd(s, t) = 1$, $s > t$, and $a = st$, $b = \frac{s^2 - t^2}{2}$, and $c = \frac{s^2 + t^2}{2}$, then $a-b-c$ is a primitive Pythagorean triple.

Proof (by contradiction). Since we showed in Section 3.2 that a, b, and c computed as above form a Pythagorean triple, it remains to show that gcd $(a, b, c) = 1$. Suppose instead that $\gcd(a, b, c) = d$ where $d > 1$. Now $d|a$, $d|b$, and $d|c$, so it is also true that $d|(b + c)$ and $d|(b - c)$.

Since $b + c = \frac{s^2 - t^2}{2} + \frac{s^2 + t^2}{2} = \frac{2s^2}{2} = s^2$, it must be true that $d|s^2$.

Since $b - c = \frac{s^2 - t^2}{2} - \frac{s^2 + t^2}{2} = \frac{-2t^2}{2} = -t^2$, it must be true that $d| - t^2$, and therefore also $d|t^2$.

By Theorem 4.4, since $\gcd(s, t) = 1$, $\gcd(s^2, t^2) = 1$ as well. This means that $d = 1$, which is a contradiction. Therefore, it must be true that $\gcd(a, b, c) = 1$. ∎

Now we are ready to prove the second claim from Section 3.3: if we start with a PPT $a - b - c$, then there are integers s and t, $s > t$, with s and t both odd and gcd $(s, t) = 1$ such that $a = st$, $b = \frac{s^2 - t^2}{2}$, and $c = \frac{s^2 + t^2}{2}$.

Two properties of primitive Pythagorean triples will be proved. The first is Lemma 3.1, and the second is Lemma 3.4.

Lemma 3.1
If $a - b - c$ is a primitive Pythagorean triple, then the greatest common divisor of any two sides is 1.

Proof (by contradiction). There are two possible ways to contradict this statement. Either:

1. The two legs of the Pythagorean triangle share a common divisor larger than 1.
2. One of the legs and the hypotenuse of the Pythagorean triangle share a common divisor larger than 1.

To complete the proof, we will show that both of these assumptions lead to a contradiction of the premise that we began with a *primitive* Pythagorean triple.

1. Suppose there is a number $d > 1$ that divides a and b, the two legs of the Pythagorean triangle. Then, $a = de$ and $b = df$ for integers e and f. Substituting in the Pythagorean theorem,

$$c^2 = a^2 + b^2 = (de)^2 + (df)^2 = d^2e^2 + d^2f^2 = d^2\left(e^2 + f^2\right)$$

This equation shows that d^2 divides c^2, or $d^2|c^2$. Therefore, by Theorem 4.3, $d|c$.

Hence, all three sides share a factor of d. Since $d > 1$, this contradicts the fact that $a - b - c$ forms a primitive Pythagorean triple.

2. Now suppose there is a number $d > 1$ such that $d|a$, one of the legs, and $d|c$, the hypotenuse.

Then for integers k and m, $a = kd$ and $c = dm$. Substituting into the Pythagorean theorem,

$$\begin{aligned}
c^2 &= a^2 + b^2 \\
(dm)^2 &= (kd)^2 + b^2 \\
d^2m^2 &= k^2d^2 + b^2 \\
b^2 &= d^2m^2 - k^2d^2 \\
b^2 &= d^2\left(m^2 - k^2\right).
\end{aligned}$$

Therefore, $d^2|b^2$, So by Theorem 4.3, $d|b$. This means that d is a common factor of a, b, and c which contradicts the fact that $a - b - c$ forms a primitive Pythagorean triple since $d > 1$. ∎

Lemma 3.5
If $a - b - c$ is a primitive Pythagorean triple, then $(c + b)$ and $(c - b)$ are relatively prime.

Proof. Let $a - b - c$ be a PPT. To show that $(c + b)$ and $(c - b)$ are relatively prime, we must show that their greatest common divisor is 1. Suppose that d is a common divisor, so $d|(c + b)$ and $d|(c - b)$. Then there exist integers x and y such that $dx = (c + b)$ and $dy = (c - b)$.

Adding these two equations, we obtain

$$dx + dy = (c + b) + (c - b)$$
$$d(x + y) = 2c$$

Since $x + y \in \mathbb{Z}$ this means that $d|2c$.

Subtracting these two equations we obtain

$$dx - dy = (c + b) - (c - b)$$
$$d(x - y) = 2b$$

Since $x + y \in \mathbb{Z}$ this means that $d|2b$.

Now, since $(c + b)$ and $(c - b)$ are both odd by Lemma 3.4, $d \neq 2$. Therefore, $d|b$ and $d|c$. By Lemma 3.1, $\gcd(b, c) = 1$ so d must be 1, and therefore $(c + b)$ and $(c - b)$ are relatively prime. ∎

Lemma 3.6

If $a - b - c$ is a primitive Pythagorean triple, then $(c + b)$ and $(c - b)$ are both perfect squares.

Proof. There are two cases to consider: $(c - b) = 1$ or $(c - b) \geq 2$. (Why?)

Case 1 $(c - b) = 1$. Then $a^2 = c + b$, so $c + b$ is a perfect square.

Case 2 $(c - b) \geq 2$. Factor both $(c - b)$ and $(c + b)$ as much as possible. No factor in the list of $(c - b)$ is also in the list of $(c + b)$ by Lemma 3.5. But since a^2 has two copies of each factor ($a^2 = s^2 t^2$), we must have the list of factors in $(c - b)$ consist of all squares, and the list of factors in $(c + b)$ must all appear twice. Hence, both are perfect squares. ∎

Let $s^2 = c + b$ and $t^2 = c - b$. We can find b and c in terms of s and t as follows.

$$s^2 + t^2 = 2c \text{ and } s^2 - t^2 = 2b$$

which gives us

$$c = (s^2 + t^2)/2 \text{ and } b = (s^2 - t^2)/2$$

Using these values for b and c, $a^2 = s^2 t^2$, so $a = st$.

Summarizing the above results, we have arrived at the following theorem from Section 3.3, which we can now prove.

Theorem 3.6

If $a - b - c$ is a PPT, then there exist integers $s > t \geq 1$ with s and t odd and $\gcd(s, t) = 1$ such that $a = st$, $b = \frac{s^2 - t^2}{2}$, $c = \frac{s^2 + t^2}{2}$.

Proof. Let $a - b - c$ be a PPT. Then $a^2 + b^2 = c^2$, and $a^2 = c^2 - b^2 = (c+b)(c-b)$.

By Lemma 3.4, $(c+b)$ and $(c-b)$ are both odd.

By Lemma 3.5, $(c+b)$ and $(c-b)$ are relatively prime.

By Lemma 3.6, $(c+b)$ and $(c-b)$ are both squares.

Therefore, we can write $(c+b) = s^2$ and $(c-b) = t^2$, for integers s and t. Since $(c+b)$ and $(c-b)$ are both odd, s^2 and t^2 must be odd, which means s and t are each odd.

Also, since $(c+b) = s^2$ and $(c-b) = t^2$ are relatively prime, this means that s and t are also relatively prime, so $\gcd(s, t) = 1$ by Exercise 34 in Section 4.2.

Since $a^2 = (c+b)(c-b) = s^2 t^2$, we have that $a = st$.

Now, we can write b and c in terms of s and t as follows:

$$s^2 + t^2 = (c+b) + (c-b) = 2c$$
$$s^2 - t^2 = (c+b) - (c-b) = 2b$$

Solving the first equation for c yields $c = \frac{s^2 + t^2}{2}$.

Solving the second equation for b yields $b = \frac{s^2 - t^2}{2}$.

Therefore, the PPT $a - b - c$ can be expressed in terms of s and t satisfying the conditions given in the PPT formulas. ∎

Combining Theorems 3.5 and 3.6 we obtain the final result, restated here.

Theorem 3.7

The triple of integers a, b, c forms a PPT if and only if $a = st$, $b = \frac{s^2 - t^2}{2}$, and $c = \frac{s^2 + t^2}{2}$ where s and t are odd integers such that $s > t \geq l$ and $\gcd(s, t) = 1$.

Proof. The proof of Theorem 3.6 proves the forward direction of this if and only if statement.

The proof of Theorem 3.5 proves the reverse direction of this if and only if statement. ∎

5.7   Summary and Review Exercises

5.7.1   Vocabulary and Symbols

division algorithm
quotient
divisor
remainder
dividend

Euclidean Algorithm
linear combination of a and b
Euclid's Lemma

5.7.2 Suggested Readings

Bell, Eric Temple. **Men of Mathematics**. New York: Simon and Schuster, 1986.
Osen, Lynn M. **Women in Mathematics**. Cambridge: MIT Press, 1975.
Guy, Richard K. *Nothing's New in Number Theory?* **The American Mathematical Monthly.** 105 (Dec., 1998): 951–054.

5.7.3 Review Exercises

Exercises 1–7. Find each greatest common divisor. Use the method you prefer.
 1. gcd(3487, 898989)
 2. gcd(12098, 78943)
 3. gcd(235490, 789685)
 4. gcd(156, 12705)
 5. gcd(2345, 12346)
 6. gcd(1050, 12705)
 7. gcd(165, 12750)

 8. Is it possible to have the greatest common divisor of two integers be zero? Explain.
 9. Find the least common multiple of each pair of numbers.

   (a) 22 and 33
   (b) 127 and 81
   (c) 12750 and 165

10. Consider the equation $ax + 15y = 18$. Find a value for a so that the equation has no solutions and a value for a so that the equation does have solutions.
11. Determine whether each equation has solutions. If so, find the general form of the solution. If not, explain why not.

   (a) $16x + 31y = 1$
   (b) $25x + 15y = 9$
   (c) $22x + 33y = 44$

12. How many ways can change be made for one dollar using only dimes and quarters?

13. The steps in the Euclidean Algorithm to find the GCD of 92 and 49 are given. Use this result to work backwards and find the values of x and y so that $92x + 49y = 1$.

$$92 = 1(49) + 43$$
$$49 = 1(43) + 6$$
$$43 = 7(6) + 1$$
$$7 = 1(7) + 0$$

14. In Chap. 3, there is a table of PPTs. We looked for patterns in the numbers and made many conjectures. Some of these are actually theorems, but we were unable to prove them before getting to this chapter. The following problems refer to primitive Pythagorean triples.

   (a) Show that one of numbers, *a, b*, or *c*, is divisible by 3.
   (b) Show that *b* is divisible by 4.
   (c) Show that one of *a, b*, or *c* is divisible by 5.

Chapter 6
Congruences

"Mathematics is the queen of the sciences, and the theory of numbers is the queen of Mathematics."

—Carl Friedrich Gauss, 1777–1855

6.1 Introduction to Congruences

If it is Monday today, what day of the week will it be 23 days from now? What about 49 days from now? If you stopped to answer these questions, you probably did it without having to count out 23 or 49 days. Both have to do with division and remainders. Since every seven days, the day of the week repeats, to figure out the day of the week, we just need to know how many extra days over a full week there are. In other words, if we are interested in what day of the week it is some number of days from now, we only need to know the remainder when that number of days is divided by seven—it doesn't matter how many full weeks have gone by. When 23 is divided by 7, the remainder is 2 because $23 = 3(7) + 2$. So, if today is Monday, it will be Wednesday in 23 days. And, since dividing 49 by 7 leaves a remainder of 0 (because $49 = 7(7) + 0$), it will be Monday again in 49 days.

The mathematical theory of congruences uses this idea of looking at remainders when integers are divided by a certain number. For example, since 23 has a remainder of 2 when divided by 7, we will think of 23 and 2 as "congruent with respect to" 7. Notice that 30 also has a remainder of 2 when divided by 7, so 30 is congruent to both 23 and 2, with respect to 7. In fact, there are infinitely many numbers that have this property: for example, 37, 44, 51, and 58 all have a remainder of 2 when divided by 7, so they are all congruent with respect to 7. Can you come up with more examples?

The theory of congruences was introduced by the German mathematician Carl Friedrich Gauss (1777–1855) and was published when he was 24 years old. Congruences are a generalization of equations, and Gauss chose to use the

symbol $\equiv$ in his congruence notation to emphasize this relationship. The formal definition appears in Definition 6.1. In Theorem 6.2, it will become clear how the congruences defined here relate to remainders.

Definition 6.1: congruent modulo *m*

Let *m* be a fixed positive integer. Two integers *a* and *b* are **_congruent modulo m_** if and only if $m|(a - b)$. If *a* and *b* are congruent modulo *m*, we write that as $a \equiv b \bmod m$. The expression $a \equiv b \bmod m$ is called a **_congruence_**, and the number *m* is called the **_modulus_** of the congruence.

Notice that *m* must be a positive integer, but *a* and *b* can be any integers. The statement $a \equiv b \bmod m$ is read as "*a* is congruent to *b* modulo *m*," or, often the slightly shorter form "*a* is congruent to *b* mod *m*." Showing that *a* is congruent to *b* modulo *m* is equivalent to showing that the congruence $23 \equiv 2 \bmod 7$ is true. Therefore, the definition could be written in symbols as

$$a \equiv b \bmod m \text{ if and only if } m\big|(a - b)$$

From the example above, we said that 23 and 2 are congruent with respect to 7. We can now write this as $23 \equiv 2 \bmod 7$. Applying the definition, we get $7|(23 - 2)$, or $7|21$, a true statement.

Here are some examples to practice working with congruences.

Example 6.1 Use the definition of congruent modulo *m* to determine whether each congruence is true or false.

(a) $12 \equiv 10 \bmod 3$
(b) $3 \equiv 7 \bmod 2$
(c) $-6 \equiv 2 \bmod 4$
(d) $2 \equiv -6 \bmod 4$

Solution
(a)   This congruence is false because $12 - 10 = 2$ and $3 \nmid 2$.
(b)   This congruence is true because $3 - 7 = -4$ and $2|-4$.
(c)   This congruence is true because $-6 - 2 = -8$ and $4|-8$.
(d)   This congruence is true because $2 - (-6) = 8$ and $4|8$.

Notice that the only difference between the congruence in part (c) and the one in part (d) is that 2 and -6 have changed sides of the congruence. In Exercise 36, you are asked to prove that if $a \equiv b \bmod m$, then $b \equiv a \bmod m$.

◈

Notice that if *m* divides $(a - b)$, then *m* also divides $(b - a)$, so it does not matter in which order we subtract *a* and *b*. A proof of this fact is left as Exercise 37. Because of this, from now on we will use the convention of subtracting in the order that produces a positive result. Therefore, if *a* is the larger of the two numbers, we will use $a - b$. If *b* is larger, we will use $b - a$.

Example 6.2 Find all positive integers m such that $6 \equiv 12 \ mod \ m$.

Solution
You can probably guess some numbers that work for m; for example, if $m = 2$, then $2|(12 - 6)$. To make sure that we get all of the possibilities, we will apply the definition to the congruence.

For the congruence $6 \equiv 12 \ mod \ m$ to be true, it must be true that $m|(12 - 6)$, or $m|6$. Therefore, the choices are $m = 1, 2, 3,$ or 6.

◈

Since 1 divides every integer, it will always appear on the list of possible values for the modulus that make a congruence true. In fact, every pair of integers a and b will be congruent modulo 1, because 1 always divides $a - b$. For this reason, the number 1 is not usually used as a modulus.

In addition to the definition of congruent modulo m, there are two other ways to think of congruences that can be very useful. The first one comes from writing out the definition and then rearranging the resulting equation.

> **Theorem 6.1**
> If $m > 1$, then $a \equiv b \ mod \ m$ if and only if $a = b + mk$ for some $k \in \mathbb{Z}$.

Since this theorem contains an "if and only if" statement, the proof will have two parts: $p \Rightarrow q$ and $q \Rightarrow p$ must both be proven. The beginning of the proof of $p \Rightarrow q$ is often indicated with the symbol "$(\Rightarrow)$". The beginning of the proof of $q \Rightarrow p$ is often indicated by "$(\Leftarrow)$".

Proof. $(\Rightarrow)$ Let $a \equiv b \ mod \ m$. Then, by the definition of congruence, $m|(a - b)$. Using the definition of divides, this means that $(a - b) = mk$ for an integer k. Adding b to both sides shows that $a = b + mk$.

$(\Leftarrow)$ Let $a = b + mk$. Then $a - b = mk$. By the definition of divides, this means that $m|(a - b)$. Therefore $a \equiv b \ mod \ m$ by the definition of congruence.

■

Here is an example to show how Theorem 6.1 can be used.

Example 6.3 Find four numbers that are congruent to 3 modulo 8: two negative numbers and two positive numbers.

Solution
From Theorem 6.1, we know that $a \equiv 3 \ mod \ 8$ if and only if $a = 3 + 8k$, with $k \in \mathbb{Z}$. This formula shows that to get more examples of numbers congruent to 3 modulo 8, we can add or subtract multiples of 8. Substituting different values of k, four examples are:

If	$k = -1,$	then $a = 3 + 8(-1) = -5.$
If	$k = -2,$	then $a = 3 + 8(-2) = -13.$
If	$k = 1,$	then $a = 3 + 8(1) = 11.$
If	$k = 10,$	then $a = 3 + 8(10) = 83.$

Therefore, $-5, -13, 11$, and 83 are all congruent to 3 modulo 8 (Note that you can always check these answers using the definition of congruent modulo 8. For example, $-13 \equiv 3 \bmod 8$ is true since $3 - -13 = 16$ and $8|16$.)

$\blacklozenge$

Another useful way to think of congruences is in terms of remainders. For example, when 18 is divided by 7, the remainder is 4. Using the Division Algorithm, this can be written as $18 = 7(2) + 4$. Subtracting 4 from both sides gives $18 - 4 = 7$ (2), which means that $7 \mid (18 - 4)$. By the definition of congruence, this means that $18 \equiv 4 \bmod 7$. So, 18 is congruent modulo 7 to its remainder when divided by 7.

There is nothing special about 18 in this example; in fact, every integer will be congruent modulo m to its remainder when divided by m. In other words, when 18 is divided by 7 the remainder is 4, so $18 \equiv 4 \bmod 7$. When 25 is divided by 7, the remainder is also 4, so $25 \equiv 4 \bmod 7$. Therefore, $18 \equiv 25 \bmod 7$, and in general, if two integers have the same remainder when divided by m, they must be congruent modulo m. These two results are stated in Theorems 6.2 and 6.3, followed by some examples of how they can be used.

> **Theorem 6.2**
> Let $m > 0$. Then, $a \equiv r \bmod m$, where $0 \le r \le m - 1$, and r is the remainder when a is divided by m.

The proof of this theorem is left as Exercise 34.

> **Theorem 6.3**
> Let $m > 0$. Then, $a \equiv b \bmod m$ if and only if a and b have the same remainder when divided by m.

Proof. ($\Rightarrow$) Let $a \equiv b \bmod m$. Then we must show that a and b have the same remainder when divided by m.

By Theorem 6.1, $a = b + mk$.

Now, using the division algorithm and dividing b by m, we obtain the equation $b = qm + r$ for an integer q, and the remainder r satisfies $0 \le r < m$. (Note that now we must show that r is also the remainder when a is divided by m.)

Substituting this formula for b into the equation for $a = b + mk$ produces the following:

$$a = (qm + r) + mk$$
$$a = qm + mk + r$$
$$a = m(q + k) + r$$

Since $0 \le r < m$, and $(q + k) \in \mathbb{Z}$, by the division algorithm, r is the remainder when a is divided by m as well.

($\Leftarrow$) Suppose that a and b both have the remainder r when divided by m. Now we must show that $a \equiv b \bmod m$. Then from the division algorithm, there are integers q_1 and q_2 such that

$$a = q_1m + r \text{ and } b = q_2m + r$$

Then,

$$\begin{aligned} a - b &= q_1m + r - (q_2m + r) \\ &= q_1m - q_2m + r - r \\ &= m(q_1 - q_2) \end{aligned}$$

Since $(q_1 - q_2) \in \mathbb{Z}$, this means that $m|(a - b)$. Therefore, by the definition of congruent modulo m, $a \equiv b \bmod m$.

∎

These two theorems are very useful to simplify arithmetic and algebra in congruences. Theorem 6.2 tells us that in a given modulus, each integer is congruent to its remainder when divided by the modulus, and Theorem 6.3 says that two integers with the same remainder when divided by m will always be congruent modulo m.

For example, if we are using the modulus 6, every integer (positive or negative) will be congruent to one of 0, 1, 2, 3, 4, or 5. And, the integers 16 and 28 are congruent modulo 6, because both 16 and 28 have a remainder of 4 when divided by 6. In the modulus 10, every integer will be congruent to one of the integers from 0 to 9. This value between 0 and one less than the modulus is called the ***least residue*** and is defined here.

Definition 6.2: least residue of b modulo m
The number r is the ***least residue of b modulo m*** if and only if $0 \le r \le m - 1$ and $b \equiv r \bmod m$.

In some books, the least residue, r, is called the ***least non-negative residue of b modulo m*** to emphasize that r cannot be negative. Replacing an integer with its least residue modulo m is called ***reducing the integer modulo m***.

The collection of integers 0, 1, 2,..., $m - 1$ is called the ***set of least residues modulo m***. This collection of numbers has the useful property that every integer is congruent to exactly one of the integers on this list, modulo m. The definition follows.

Definition 6.3: set of least residues modulo m
The collection of integers 0, 1, 2, ..., $m - 1$ is called the ***set of least residues modulo m***.

Example 6.4 Find the set of least residues modulo 7. How many integers are in the set of least residues modulo 7?

Solution
The set of least residues modulo 7 is 0, 1, 2, 3, 4, 5, 6. There are seven integers in the set.

◈

Other sets of integers can share the properties of the set of least residues modulo *m*; in other words, there are other possible sets of integers such that none of the integers in the set are congruent modulo *m* and every integer is congruent modulo *m* to something in the set. A collection satisfying these two properties is called a **complete system of residues modulo m**.

> **Definition 6.4: complete system of residues modulo m**
> A **complete system of residues modulo m** is a set of *m* integers with the following two properties:
>
> 1. None of the integers in the set are congruent modulo *m*.
> 2. Every integer is congruent modulo *m* to one of the integers in the set.

The set of least residues modulo *m* is always one example of a complete system of residues modulo *m*, but there are other possibilities as well.

Example 6.5 Find two different complete residue systems modulo 5.

Solution
One example is 0, 1, 2, 3, and 4, the collection of least residues modulo 5. We can find another example by adding multiples of 5 to each of these numbers. One possibility is 5, 6, 7, 8, and 9. Another possibility is 5, 11, 17, 23, and 29. Notice that in the second example, a different multiple of 5 was added to each value. By continuing to add or subtract different multiples of 5, we will come up with more sets of integers that meet these two requirements. In each case, the given set will reduce to the set of least residues modulo 5, none of which are congruent to each other, and every integer is congruent to one of them.

◈

Example 6.6 For each integer given below, find its least residue modulo 9.
(a) 44   (b) -25 (c) 5

Solution
(a)   When 44 is divided by 9, the remainder is 8 so 8 is the least residue of 44 modulo 9, and $44 \equiv 8 \ mod \ 9$.
(b)   Since $-25 = -3(9) + 2$, 2 is the least residue of -25 modulo 9, and $-25 \equiv 2 \ mod \ 9$.
(c)   Here, 5 is its own least residue modulo 9, since 9 is too big to divide 5 at all, so $5 = 0(9) + 5$, and $5 \equiv 5 \ mod \ 9$.

◈

Example 6.7 Find the least residue of 13 in the given modulus. (Alternatively, we could state the instructions as, "Reduce 13 in the given modulus.")

(a) $13 \equiv$ _____ $mod\ 12$
(b) $13 \equiv$ _____ $mod\ 9$
(c) $13 \equiv$ _____ $mod\ 15$
(d) $13 \equiv$ _____ $mod\ 26$

Solution
(a) $13 \equiv 1\ mod\ 12$, since 13 has a remainder of 1 when divided by 12.
(b) $13 \equiv 4\ mod\ 9$, since $13 = 1(9) + 4$, so 4 is the least residue of 13 modulo 9.
(c) $13 \equiv 13\ mod\ 15$, since 13 is less than 15 and is already a least residue. Using the division algorithm, $13 = 0(15) + 13$.
(d) Again, $13 \equiv 13\ mod\ 26$ because 13 is less than 26, so it is already a least residue. (Notice that $26 \equiv 0\ mod\ 13$ since $26 = 2(13)$.)

◆

Example 6.8 Find the least residue of each integer in the given modulus.

(a) 141 *modulo* 6
(b) -20 *modulo* 11
(c) -56 *modulo* 5

Solution
(a) 141 *modulo* 6
     $141 \equiv 3\ mod\ 6$, since $141 = 23(6) + 3$, so 3 is the least residue of 141 *mod* 6.
     Alternatively, using Theorem 6.1, if $a \equiv 141\ mod\ 6$, then $a = 141 + 6k$. Since we are looking for the least residue, we need to choose k so that $0 \le 141 + 6k < 6$. If $k = -23$, then $a = 141 + 6(-23) = 141 - 138 = 3$. Therefore, $3 \equiv 141\ mod\ 6$.
(b) -20 *modulo* 11
     $-20 \equiv 2\ mod\ 11$, since $-20 = -2(11) + 2$.
     We can also use Theorem 6.1 when working with negative values. From Theorem 6.1, if $-20 \equiv a\ mod\ 11$, then $a = -20 + 11k$. To find the least residue, find the smallest value of k that makes the right side positive. In this case, that is $k = 2$, so $a = -20 + 11(2) = 2$. Therefore, $2 \equiv -20\ mod\ 11$, and we see again that 2 is the least residue of -20 modulo 11.
(c) -56 *modulo* 5
     Using Theorem 6.1 again, if $a \equiv -56\ mod\ 5$, then $a = -56 + 5k$. If $k = 12$, then $a = -56 + 5(12) = -56 + 60 = 4$. Therefore, $-56 \equiv 4\ mod\ 5$ and 4 is the least residue of -56 modulo 5.

   Notice that using Theorem 6.1 amounts to adding or subtracting the modulus, m, until a value from 0 to $m - 1$ is reached.

◆

Example 6.9 If *a* is an odd integer, what are the possible least residues of *a* modulo 4?

Solution
First, there are four possible least residues modulo 4. Either

$$a \equiv 0 \ mod \ 4, \ or$$
$$a \equiv 1 \ mod \ 4, \ or$$
$$a \equiv 2 \ mod \ 4, \ or$$
$$a \equiv 3 \ mod \ 4.$$

Now, which of these represent odd integers? Rewriting each of these congruences as an equation, either

$$a = 0 + 4k, \ or$$
$$a = 1 + 4k, \ or$$
$$a = 2 + 4k, \ or$$
$$a = 3 + 4k,$$
$$\text{with } k \ \in \ \mathbb{Z} \text{ in each case.}$$

Since 4 is even, $0 + 4k$ and $2 + 4k$ are even numbers. On the other hand, an even number added to an odd number is odd. Therefore, if *a* is odd, either $a = 1 + 4k$ or $a = 3 + 4k$. Then $a \equiv 1 \ mod \ 4$ or $a \equiv 3 \ mod \ 4$ and the possible least residues modulo 4 of an odd integer are 1 or 3.

◈

Notice that we usually classify even and odd integers by whether or not they are divisible by 2; in that case, if an integer is odd, the only possible remainder is 1, and so "*a* is odd" is equivalent to "$a \equiv 1$ mod 2." However, listing the values of *a* that satisfy $a \equiv 1$ mod 4, we get $\ldots, -7, -3, 1, 5, 9, 13, 17, \ldots$. All the odds aren't covered by this congruence, so two congruences modulo 4 are necessary to describe the set of odd integers, as shown in Example 6.9.

Exercise Set 6.1

Exercises 1–6. Use the definition of congruent modulo *m* to determine whether the congruence is true or false.
  1. $0 \equiv 6 \ mod \ 3$
  2. $35 \equiv 55 \ mod \ 9$
  3. $-23 \equiv 20 \ mod \ 7$
  4. $-3 \equiv 3 \ mod \ 6$
  5. $-2 \equiv 2 \ mod \ 3$
  6. $16 \equiv 185 \ mod \ 11$

7. Find all positive integers m such that $9 \equiv 15 \ mod \ m$.
8. Find all positive integers m such that $10 \equiv 12 \ mod \ m$.
9. Find all positive integers m such that $-5 \equiv 7 \ mod \ m$.
10. For any two integers a and b, is it always possible to find a positive integer m such that $a \equiv b \ mod \ m$? Either show that it is possible or find a counterexample to show that it is not.

Exercises 11–19. Rewrite the statement using a congruence or congruences.

Example: "a is even" can be written as $a \equiv 0 \ mod \ 2$

11. b is odd.
12. c is divisible by 3.
13. k has a remainder of 7 when divided by 11.
14. a has a remainder of 5 when divided by 8.
15. a is even, using the modulus 4.
16. a is even, using the modulus 6.
17. 4 divides a.
18. a is odd, using the modulus 8.
19. m is not divisible by 5.

20. Is it possible to rewrite the statement "a is odd" using the modulus 5? Explain why or why not.
21. Find 3 negative and 3 positive integers that are congruent to 5 modulo 9.
22. Find 3 negative and 3 positive integers that are congruent to 11 modulo 25.
23. Find an integer greater than 200 that is congruent to 8 modulo 9.
24. Find all values of a such that $0 \leq a \leq 25$, and $a \equiv 42 \ mod \ 11$.
25. Find the least residue of each of the integers below in the given modulus.

   (a) $10 \equiv$ _____ $mod \ 3$
   (b) $14 \equiv$ _____ $mod \ 28$
   (c) $-8 \equiv$ _____ $mod \ 7$
   (d) $124 \equiv$ _____ $mod \ 4$

26. Find the least residue of each of the integers below in the given modulus.

   (a) $42 \equiv$ _____ $mod \ 11$
   (b) $-15 \equiv$ _____ $mod \ 9$
   (c) $135 \equiv$ _____ $mod \ 8$
   (d) $254 \equiv$ _____ $mod \ 10$

27. Find the set of least residues modulo 8. How many integers are in the set of least residues modulo 8?
28. Find the set of least residues modulo 6.
29. Find the set of least residues modulo 11.
30. Explain why the set of least residues modulo m is also always a complete system of residues modulo m.

31. Is the following set of numbers a complete system of residues modulo 8? Explain your answer.

$$16, \ 23, \ 26, \ -15, \ 14, \ -5, \ 44, \ 45$$

32. Complete the if and only if ($\Leftrightarrow$) statement below to make a true statement. Then, prove the statement.

$$a \equiv 0 \bmod m \Leftrightarrow \underline{\hspace{5cm}}$$

33. Rewrite the proof of **Theorem 6.1** in the column form given in Section 2.5.
34. Prove **Theorem 6.2**. (Hint: Use the division algorithm.)
35. Rewrite the proof of **Theorem 6.3** in the column form given in Section 2.5.
36. Prove that if $a \equiv b \bmod m$, then $b \equiv a \bmod m$.
37. Prove that if $m \mid (a - b)$, then $m \mid (b - a)$. Then, explain how this is related to congruences.
38. Prove that $a \equiv a \bmod m$ for any integer $m > 0$.
39. Prove that if $a \equiv b \bmod m$ and c is an integer, then $a + c \equiv b + c \bmod m$.
40. If $a \equiv b \bmod m$ and c is an integer, prove that $ac \equiv bc \bmod m$.

6.2 Congruences Versus Equations

This section explores some ways in which congruences are similar to and different from equations. One well-known rule used when solving equations is that they must stay balanced: whatever operation you perform on one side of the equation must also be performed on the other side. In other words, you can add, subtract, multiply, or divide both sides of an equation by the same number, and if the original equation was true, then it will remain true. (The only exception is that you cannot divide by 0.)

In addition, when working with integers or real numbers, if $a \cdot b = 0$, then either $a = 0$ or $b = 0$.

We will go through these rules one by one to see which ones hold for congruences and which ones do not.

6.2.1 Adding to Both Sides of an Equation or Congruence

Rule #1 for Equations: Adding the same number to both sides of a true equation results in a true equation. Since subtraction can be written as adding a negative number, subtracting the same number from both sides of a true equation also results in a true equation. In symbols,

$$\text{if } a \;=\; b, \text{ then}$$
$$a + c \;=\; b + c, \text{ and } a - c \;=\; b - c$$

This is used when solving equations such as $x - 4 = 8$. Adding 4 to both sides gives $x = 12$, the solution to the equation.

Is this rule true for congruences? Luckily for us, the answer is yes. Exercise 39 of Section 6.1 asked about adding the same integer to both sides of a congruence. In fact, as long as numbers that are congruent in the given modulus (not necessarily even equal) are added to both sides, a true congruence will remain true. This result is stated in Theorem 6.4.

Theorem 6.4
If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ for $m > 0$, then:

1. $a + c \equiv b + d \bmod m$
2. $a - c \equiv b - d \bmod m$

Proof. This proof will have two parts.

Proof of (1) Let $m > 0$. Suppose that $a \equiv b \bmod m$ and $c \equiv d \bmod m$. Then, by the definition of congruence, we know that $m|(a - b)$ and $m|(c - d)$. From the definition of divides, there are integers k and n so that

$$a - b = mk \text{ and } c - d = mn.$$

We would like to show that $m|((a + c) - (b + d))$.
Adding the two equations above,

$$mk + mn \;=\; (a - b) + (c - d) \;=\; a + c - b - d = (a + c) - (b + d)$$

Therefore $m(k + n) = (a + c) - (b + d)$.
Hence, $m|((a + c) - (b + d))$, since $(k + n) \in \mathbb{Z}$.
By the definition of congruence, $a + c \equiv b + d \bmod m$.

Proof of (2) The proof of part (2) is left as Exercise 17.

∎

Note that the rules for congruences given in Theorem 6.4 are actually a little more general than the rules stated for equations. As long as two numbers are *congruent*, adding one to each side of a true congruence produces a true congruence.

For example, $5 \equiv 15 \bmod 10$ is a true congruence. Also, $7 \equiv 27 \bmod 10$. Therefore, it is true that $5 + 7 \equiv 15 + 27 \bmod 10$, or $12 \equiv 42 \bmod 10$. You can check this by applying the definition of congruence or by finding the least residue of each side. This makes arithmetic easier, because numbers can always be replaced by their least residue in the modulus of the congruence, as shown here in Example 6.10.

Example 6.10 Find the least residue modulo 6 of the sum $15 + 7 + 4 + 36$.

Solution
We could add up all these numbers and then find the remainder when the total is divided by 6. But, we can also replace each number by any number that is congruent modulo 6. To make the arithmetic easier, we will replace each number by its least residue, modulo 6. Calculating the least residues modulo 6,

$$15 \equiv 3 \ mod \ 6$$
$$7 \equiv 1 \ mod \ 6$$
$$4 \equiv 4 \ mod \ 6$$
$$36 \equiv 0 \ mod \ 6$$

Therefore, the sum reduces to

$$15 + 7 + 4 + 36 \equiv 3 + 1 + 4 + 0 \ mod \ 6$$
$$\equiv 8 \ mod \ 6$$
$$\equiv 2 \ mod \ 6$$

◈

Certain values of the modulus make finding the least residues especially easy, as in the next example. An application of this type of calculation to verifying ID numbers is included in Section 6.4.

Example 6.11 Find the least residue of each of the following without using a calculator.

(a) $14 + 35 + 2000 + 113 + 94 + 601$ modulo 5
(b) $4 + 20 + 38 + 576 + 19 + 1402 + 763$ modulo 10

Solution
(a) By Theorem 6.4, each integer can be replaced with another congruent to it modulo 5. In order to make arithmetic easier, replace each integer with its least residue modulo 5:

$$14 + 35 + 2000 + 113 + 94 + 601 \equiv 4 + 0 + 0 + 3 + 4 + 1 \ mod \ 5$$

Now, since each least residue is less than 5, we can combine terms on the right side until we get something greater than 5 which can be reduced again.

$$14 + 35 + 2000 + 113 + 94 + 601 \equiv 7 + 5 \ mod \ 5$$

Reducing modulo 5 once more gives

$$14 + 35 + 2000 + 113 + 94 + 601 \equiv 2 + 0 \ mod \ 5$$

Therefore,

$$14 + 35 + 2000 + 113 + 94 + 601 \equiv 2 \ mod \ 5$$

(b)   To reduce this sum modulo 10, replace each integer with its least residue modulo 10:

$$4 + 20 + 38 + 576 + 19 + 1402 + 763 \equiv 4 + 0 + 8 + 6 + 9 + 2 + 3 \bmod 10$$
$$\equiv 12 + 15 + 5 \bmod 10$$
$$\equiv 2 + 5 + 5 \bmod 10$$
$$\equiv 2 \bmod 10$$

◈

6.2.2   Multiplying on Both Sides of an Equation or Congruence

Rule #2 for Equations: Multiplying both sides of an equation by the same number results in another true equation. In symbols,

$$\text{if } a \,=\, b, \text{ then } a \cdot c = b \cdot c$$

This is used when solving linear equations such as $\frac{x}{3} = 5$. Multiplying both sides by 3 gives the solution $x = 15$. This rule also follows for congruences but again in a more general form. (A less general statement was included as Exercise 40 in Section 6.1.) You can multiply both sides of a congruence by different numbers as long as they are congruent in the modulus of the congruence.

> **Theorem 6.5**
> If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ for $m > 0$, then $a \cdot c \equiv b \cdot d \bmod m$.

Proof.
Let $a \equiv b \bmod m$.
Let $c \equiv d \bmod m$.

By the definition of congruence, $m|(a - b)$ and $m|(c - d)$.
Applying the definition of divides, there exist $k, l \in \mathbb{Z}$ such that $a - b = mk$ and $c - d = ml$. Here is where the proof gets creative. We want to end with $m|(ac - bd)$, which can be rewritten as $ac - bd = mx$ for $x \in \mathbb{Z}$. Start by multiplying $a - b = mk$ by c on both sides.

$$(a - b)c = mkc$$

Then multiply the second equation $c - d = ml$ by b on both sides.

$$b(c - d) = bml$$

Distributing on the left-hand side of each equation results in the following two equations:

$$ac - bc = mkc \ \text{and} \ bc - bd = bml$$

Adding these two equations and simplifying,

$$ac - bc + bc - bd = mkc + bml$$
$$ac - bd = mkc + bml$$
$$ac - bd = m(kc + bl)$$

Therefore, $m|(ac - bd)$, since $kc + bl \in \mathbb{Z}$. Finally, by the definition of congruence, $a \cdot c \equiv b \cdot d \ mod \ m$.

∎

   The rule in Theorem 6.5 allows us to simplify multiplication, and its usefulness is shown in the next four examples.

Example 6.12 Find the least residue of $19 \cdot 38$ *modulo* 4, without using a calculator.

Solution
Since $19 \equiv 3 \ mod \ 4$ and $38 \equiv 2 \ mod \ 4$, by Theorem 6.5,

$$19 \cdot 38 \equiv 3 \cdot 2 \ mod \ 4$$
$$\equiv 6 \ mod \ 4$$
$$\equiv 2 \ mod \ 4$$

Therefore, 2 is the least residue of $19 \cdot 38$ modulo 4.   ◈

Example 6.13 Find the least residue of 13^3 modulo 10 without using a calculator.

Solution
Again applying Theorem 6.5,

$$13^3 \equiv 13 \cdot 13 \cdot 13 \ mod \ 10$$
$$\equiv 3 \cdot 3 \cdot 3 \ mod \ 10$$
$$\equiv 27 \ mod \ 10$$
$$\equiv 7 \ mod \ 10$$

◈

Example 6.14 Find the remainder when 2^{50} is divided by 15, without using a calculator.

Solution
First, notice that this is a multiplication problem, where 2 is multiplied by itself 50 times. In terms of congruences, we are asked to find the least residue of 2^{50} modulo 15. A computer can calculate 2^{50}, but eventually exponents can become too large to calculate, so we will use properties of congruences to find another

approach. Since 2 does not reduce modulo 15, begin by raising 2 to powers to see if a power of 2 will reduce to a value that is easier to work with:

$$2 \equiv 2 \; mod \; 15$$
$$2^2 \equiv 4 \; mod \; 15$$
$$2^3 \equiv 8 \; mod \; 15$$
$$2^4 \equiv 16 \equiv 1 \; mod \; 15$$

Now, using Theorem 6.5, if the number 2^4 occurs in a product in a congruence modulo 15, it can be replaced with 1. This means that $2^8 \equiv 2^4 \cdot 2^4 \equiv 1 \cdot 1 \equiv 1 \; mod \; 15$, and similarly $2^{12} \equiv 2^4 \cdot 2^4 \cdot 2^4 \equiv 1 \cdot 1 \cdot 1 \equiv 1 \; mod \; 15$. Since 2^{50} is $2 \cdot 2 \cdot 2 \cdots 2$ fifty times, we can group these 2s into 12 groups of 4 and one group of 2 giving us that $2^{50} = (2^4)^{12} \cdot 2^2$. Reducing modulo 15,

$$2^{50} \equiv \left(2^4\right)^{12} \cdot 2^2 \; mod \; 15 \equiv (1)^{12} \cdot 2^2 \; mod \; 15 \equiv 4 \; mod \; 15$$

(The rules for exponents used here are included in Exercise 1 at the end of this section.)

◆

Example 6.15 Find the least residue of $10(4) + 19(8) + 27(14) + 6(3) + 5(7)$ modulo 10, without a calculator.

Solution
To reduce this expression, we will combine the rules from Theorems 6.4 and 6.5 which allow us to replace integers with congruent integers in sums and products. Start by replacing each integer greater than or equal to 10 with its least residue modulo 10. Then, multiply and replace with the least residue of each term again, and continue to simplify until the value is less than 10.

$$
\begin{aligned}
10(4) + 19(8) + 27(14) + 6(3) + 5(7) &\equiv 0 + 9(8) + 7(4) + 6(3) + 5(7) \; mod \; 10 \\
&\equiv 72 + 28 + 18 + 35 \; mod \; 10 \\
&\equiv 2 + 8 + 8 + 5 \; mod \; 10 \\
&\equiv 10 + 13 \; mod \; 10 \\
&\equiv 3 \; mod \; 10
\end{aligned}
$$

◆

6.2.3   Dividing Both Sides of an Equation, but not a Congruence

Rule #3 for Equations: Both sides of an equation can always be divided by the same nonzero number. In symbols,

if $a = b$, then $\frac{a}{c} = \frac{b}{c}$, as long as $c \neq 0$.

This property is used when solving equations such as $6x = 42$. Dividing both sides by 6 gives the solution $x = 7$.

Caution: This Is Not a Rule for Congruences!

The statement, "If $a \equiv b \bmod m$, then $\frac{a}{c} \equiv \frac{b}{c} \bmod m$ when $c \neq 0$," is not true for congruences, even if the number c evenly divides both sides of the congruence.

Example 6.16 Provide a counterexample to show that the following statement is *false*: If $a \equiv b \bmod m$, then $\frac{a}{c} \equiv \frac{b}{c} \bmod m$ when $c \neq 0$. Explain your reasoning.

Solution

A counterexample will consist of values of a, b, $c \neq 0$, and m such that the condition $a \equiv b \bmod m$ is true, but the conclusion, $\frac{a}{c} \equiv \frac{b}{c} \bmod m$, is false.

One possible choice is $a = 7$, $b = 11$, $c = 3$, and $m = 4$. Then $7 \equiv 11 \bmod 4$ is true, but $\frac{7}{3} \equiv \frac{11}{3} \bmod 4$ does not make sense since $\frac{7}{3}$ and $\frac{11}{3}$ are not integers; therefore dividing by 3 does not produce a true congruence.

◈

This example is quite unsatisfying. On the one hand, it does show that you cannot always divide both sides of a congruence by a nonzero number, but it does not actually produce a false congruence.

Now, what if you divide both sides of a congruence by a value that does evenly divide both sides? Will the result always be a true congruence in this case? The answer, again, is "No," which the next example shows.

Example 6.17 Find a counterexample to the statement in Example 6.16, but this time choose a value for c such that c does evenly divide both a and b.

Solution

Keeping in mind that c must divide both a and b, choose $a = 4$, $b = 12$, and $m = 8$. Then $4 \equiv 12 \bmod 8$ is true (because $12 - 4 = 8$ and $8 | 8$). But then if $c = 2$, dividing both sides of the congruence by 2 gives $2 \equiv 6 \bmod 8$ which is false because $6 - 2 = 4$ and $8 \nmid 4$.

◈

6.2.4 $a \cdot b = 0$ versus $a \cdot b \equiv 0 \bmod m$

Rule #4 for Equations: If the product of two numbers is equal to zero, then one of the numbers must be zero. In symbols,

if $a \cdot b = 0$, then either $a = 0$ or $b = 0$.

This is used when solving quadratic equations by factoring. For example, to solve $x^2 - x - 6 = 0$, factor the left-hand side to obtain the equation $(x - 3)(x + 2) = 0$. Then, since this means that either $(x - 3) = 0$, or $(x + 2) = 0$, the solution is $x = 3, -2$.

Caution: This Is Not a Rule for Congruences!
The statement, "If $a \cdot b \equiv 0 \bmod m$, then $a \equiv 0 \bmod m$ or $b \equiv 0 \bmod m$" is false for congruences. For a counterexample, let $m = 12$, $a = 3$ and $b = 4$. Then $3 \cdot 4 \equiv 0 \bmod 12$, even though $3 \not\equiv 0 \bmod 12$ and $4 \not\equiv 0 \bmod 12$.

6.2.5   Summary of Rules for Congruences

Here are the results that are true for congruences, summarized in one theorem.

> **Theorem 6.6**
> If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ for $m > 0$, then:
>
> 1. $a + c \equiv b + d \bmod m$
> 2. $a - c \equiv b - d \bmod m$
> 3. $ac \equiv bd \bmod m$

Example 6.18   Without a calculator, find the least residue of $20(5) + 4(32) - 6(12) + 25^2$ modulo 10.

Solution
Using the results in Theorem 6.6, first replace each integer in the expression with its least residue modulo 10, and then continue to simplify until you arrive at a value less than 10.

$$
\begin{aligned}
20(5) + 4(32) - 6(12) + 25^2 &\equiv 0 + 4(2) - 6(2) + 5^2 \bmod 10 \\
&\equiv 8 - 12 + 25 \bmod 10 \\
&\equiv 8 - 2 + 5 \bmod 10 \\
&\equiv 1 \bmod 10
\end{aligned}
$$

◈

The next example shows how congruences can be used to explain why the divisibility test for 3 from Section 2.9 works. Exercises 18–20 ask you to check several other divisibility tests.

Example 6.19   Prove that the divisibility test for 3 included in Section 2.9 works: Prove that 3 divides an integer a if and only if 3 divides the sum of the digits of a.

Solution
Because the divisibility test is an "if and only if" statement, there are two parts to proving it is true. First show that if 3 divides a, then 3 divides the sum of the digits of a. Second, prove that if 3 divides the sum of the digits of a, then 3 divides a.

Before starting the proof, one question is the following: How will we represent the sum of the digits of the number a? For example, if $a = 816$, then the ones digit is

6, the tens digit is 1, and the hundreds digit is 8. Adding up the digits shows that 816 is divisible by 3 since $8 + 1 + 6 = 15$. To work with this idea in general, a way to write an integer in terms of its digits would be helpful. To do this, we will use *expanded notation*. In expanded notation, $816 = 6 + 1(10) + 8(100)$, so each digit is multiplied by its place value. Therefore, if the integer a has ones digit a_0, tens digit a_1, and so on, then in expanded notation, $a = a_0 + a_1 \cdot 10 + a_2 \cdot 100 + \cdots + a_n \cdot 10^n$.

Now, let us proceed with the proof.

Proof.

($\Rightarrow$) Let a be an integer. Let $3 | a$. Then, in expanded notation,

$a = a_0 + a_1 \cdot 10 + a_2 \cdot 100 + \cdots + a_n \cdot 10^n$. Since $3 | a$, $a \equiv 0 \bmod 3$. Therefore,

$$a_0 + a_1 \cdot 10 + a_2 \cdot 100 + \cdots + a_n \cdot 10^n \equiv 0 \bmod 3$$

Now, since $10 \equiv 1 \bmod 3$, using Theorem 6.6, part (3) each 10 can be replaced by 1 in the congruence modulo 3. Therefore,

$$0 \equiv a_0 + a_1 \cdot 10 + a_2 \cdot 100 + \cdots + a_n \cdot 10^n$$
$$\equiv a_0 + a_1 + a_2 + \cdots + a_n \bmod 3$$

Therefore, $3 | (a_0 + a_1 + a_2 + \cdots + a_n)$, so 3 divides the sum of the digits of a.

($\Leftarrow$) Let 3 divide the sum of the digits of a. In symbols,

$$3 \,\big|\, (a_0 + a_1 + a_2 + \cdots + a_n)$$

This also means that $a_0 + a_1 + a_2 + \cdots + a_n \equiv 0 \bmod 3$. Now, since $10 \equiv 1 \bmod 3$, we can multiply any term by 1 or 10 as many times as we wish and maintain a true congruence modulo 3. Therefore,

$$0 \equiv a_0 + a_1 \cdot 1 + a_2 \cdot 1 + \cdots + a_n \cdot 1 \bmod 3$$
$$0 \equiv a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n \bmod 3$$

The right-hand side of the congruence is the integer a written in expanded notation. Therefore, we can conclude that $0 \equiv a \bmod 3$ which means that $3 \mid a$.

■

◈

Exercise Set 6.2

---

1. ***Exponent Review.*** Use the rules for exponents reviewed here to simplify the expressions.
   Rules for Exponents
   Rule 1. $m^a \cdot m^b = m^{a+b}$
   Rule 2. $(m^a)^b = m^{ab}$

   (a) $2^6 2^{10}$

   (b) $\left(4^8\right)^3$

   (c) $3^5 9^3$ (Hint: Remember that $9 = 3^2$.)

   (d) $\left(5^3\right)^4 \cdot 5^{10}$

   (e) $3^5 \cdot \left(3^4\right)^7$

2. Rewrite 5^{46} in terms of 5^4 and then find the least residue of 5^{46} modulo 12.
3. Rewrite 7^{151} in terms of 7^4 and then find the least residue of 7^{151} modulo 10.
4. Rewrite 5^{137} in terms of 5^2 and then find the least residue modulo 11.
5. Rewrite 3^{207} in terms of 3^4 and then find the least residue of 3^{207} modulo 7.
6. Find the remainder when 3^{152} is divided by 13.

Exercises 7–11. Write the integer in expanded notation.

  7. 47
  8. 589
  9. 1234
10. 1000
11. 67890

Exercises 12–15. Find the least residue in the given modulus, without using a calculator. (Use Theorem 6.6 to make the calculations easier.)

12. $6^2 + (5 \cdot 46)$ *modulo* 35
13. 5^{256} *modulo* 5
14. $25^2(31)$ *modulo* 4
15. $70 + 36 + 48 + 35 + 20 + 18$ *modulo* 11

16. Consider the congruence $ab \equiv 0 \bmod m$.

   (a) Choose some different values for m, and then find some values for a and b that make the congruence true. Some questions to think about when you are picking examples are:

      • For every value of m, can you always make the congruence true without letting a or b be 0?
      • Can you always find values for a and b that are smaller than m? Bigger than m?

   (b) Write a conjecture about when you can find a and b such that $a \neq 0$, $b \neq 0$, and $ab \equiv 0 \bmod m$.

17. Prove **Theorem 6.4, part (2)**.
18. Use congruences to prove that the divisibility test for 9 works.
19. Use congruences to prove that the divisibility test for 5 works.
20. Use congruences to prove that the divisibility test for 4 works.

6.3   Solving Linear Congruences

In Section 6.2, we compared rules for solving linear equations to rules for congruences. This section discusses how these rules relate to solving linear congruences. First, we will summarize what you already know about solving linear equations.

A linear equation (in one variable) is any equation of the form $ax + b = c$, where a, b, and c are constants and $a \neq 0$. Solving the equation means finding all values of x that make the equation true. A number x_0 is a solution of $ax + b = c$ if $ax_0 + b = c$ is true. Equations of this type all have exactly one solution; to find it, add, subtract, multiply, or divide each side of the equation by the same quantity until x is by itself. In the case of the equation above, subtracting b from both sides and then dividing by a gives $x = \frac{c-b}{a}$. Here are two examples of solving linear equations for review.

Example 6.20   Solve the linear equation $3x + 7 = 14$.

Solution

$$3x + 7 = 14$$
$$3x + 7 - 7 = 14 - 7$$
$$3x = 7$$
$$x = \frac{7}{3}$$

◆

Example 6.21   Solve the linear equation $4x - 9 = 7$.

Solution

$$4x - 9 = 7$$
$$4x - 9 + 9 = 7 + 9$$
$$4x = 16$$
$$x = 4$$

◆

Note that the first equation did not have an integer solution, but the second equation did. Now, transitioning from equations to congruences, here is the definition of a linear congruence.

> **Definition 6.5: linear congruence**
> A *linear congruence* is a congruence of the form $ax \equiv b \bmod m$.

As with equations, an integer x_0 is a solution of the linear congruence $ax \equiv b \bmod m$ if $ax_0 \equiv b \bmod m$ is true. So, solving a linear congruence means

finding all values for x that make the congruence true. Some questions to think about are:

1. Do all linear congruences have solutions?
2. Can linear congruences have more than one solution?
3. Can linear congruences be solved using the same methods used for equations?

We will look at some examples to start answering these questions.

Example 6.22 Solve the linear congruences. Give the final answer in reduced form.
(a) $3x \equiv 4 \ mod \ 7$
(b) $2x \equiv 3 \ mod \ 4$
(c) $2x \equiv 4 \ mod \ 6$

Solution
(a) $3x \equiv 4 \ mod \ 7$

Since we cannot divide both sides of a congruence by a nonzero number, we need a different solution technique.

Since 7 is the modulus of the congruence, any solution will have to be congruent to one of the least residues modulo 7. Therefore, unlike for linear equations, we can actually test all the possibilities to see what makes the congruence true.

Choice for x	Substitute x into congruence	Solution?
0	$3(0) \equiv 0 \ mod \ 7$	No
1	$3(1) \equiv 3 \ mod \ 7$	No
2	$3(2) \equiv 6 \ mod \ 7$	No
3	$3(3) \equiv 2 \ mod \ 7$	No
4	$3(4) \equiv 5 \ mod \ 7$	No
5	$3(5) \equiv 1 \ mod \ 7$	No
6	$3(6) \equiv 4 \ mod \ 7$	Yes ☺

Therefore, if $x \equiv 6 \ mod \ 7$, then x is a solution to this congruence. Notice this is slightly different from solutions to equations. While only one of the least residues solved the congruence, any integer congruent to 6 modulo 7 will make this congruence true. Therefore, 13, 20, 27, -1, or -8 will all make the congruence true. Since all these solutions are congruent modulo 7, they are called ***congruent solutions***.

(b) $2x \equiv 3 \ mod \ 4$

Again, since we cannot divide both sides of a congruence by the same number, we will use the set of least residues modulo 4 to find out what solutions there are. If there is a solution, it must be congruent to either 0, 1, 2, or 3 modulo 4.

Choice for x	Substitute x into congruence	Solution?
0	$2(0) \equiv 0 \ mod \ 4$	No
1	$2(1) \equiv 2 \ mod \ 4$	No
2	$2(2) \equiv 0 \ mod \ 4$	No
3	$2(3) \equiv 2 \ mod \ 4$	No

None of the possibilities work, so this congruence has no solutions! This is an important difference from linear equations: all linear equations have a solution, but we have found at least one linear congruence that does not.

(c) $2x \equiv 4 \; mod \; 6$

We can again test all least residues modulo 6 to see if we get any solutions:

Choice for x	Substitute x into congruence	Solution?
0	$2(0) \equiv 0 \; mod \; 6$	No
1	$2(1) \equiv 2 \; mod \; 6$	No
2	$2(2) \equiv 4 \; mod \; 6$	Yes ☺
3	$2(3) \equiv 0 \; mod \; 6$	No
4	$2(4) \equiv 2 \; mod \; 6$	No
5	$2(5) \equiv 4 \; mod \; 6$	Yes ☺

There are two least residues that solve the congruence: $x = 2$ and $x = 5$.

◈

Part (c) in Example 6.22 illustrates another new development. The values $x = 2$ and $x = 5$ both satisfy the congruence $2x \equiv 4 \; mod \; 6$. These solutions are called **incongruent solutions**, since they are not congruent to each other modulo 6. When we talk about different solutions, we are actually counting the number of incongruent solutions, so this congruence has incongruent solutions, $x = 2$ and $x = 5$. Since any integer that is congruent to these values modulo 6 will also be a solution, the complete solution to $2x \equiv 4 \; mod \; 6$ is

$$x \equiv 2 \; mod \; 6 \text{ or } x \equiv 5 \; mod \; 6$$

Another way to think of incongruent solutions is that they are all less than the modulus, in reduced form. (If you find the least residue of two congruent solutions, what will happen?)

Example 6.23   Solve the linear congruence $x + 4 \equiv 2 \; mod \; 7$. Give the least residue of the solution.

Solution
Notice that the form of this congruence is slightly different than the form given in the definition of linear congruence. However, from Theorem 6.6, we can subtract congruent values from each side of a congruence. Therefore, to isolate x, subtract 4 from both sides of the congruence.

$$
\begin{aligned}
x + 4 - 4 &\equiv 2 - 4 \; mod \; 7 \\
x &\equiv -2 \; mod \; 7 \\
x &\equiv 5 \; mod \; 7
\end{aligned}
$$

Notice that the first solution was negative, so adding 7 gave the least residue of the solution. The solutions -2 and 5 are another example of *congruent solutions*. This congruence has one incongruent solution, $x = 5$. The complete solution is $x \equiv 5 \; mod \; 7$.

◈

Example 6.24 Show that $x = 25$, $x = -13$, and $x = 63$ are all solutions of the congruence $5x \equiv 11 \bmod 19$. Then find the least residue modulo 19 of each of the solutions and compare.

Solution

First, show each given value of x solves the congruence, using Theorem 6.6, part (3).

If $x = 25$, then $5 \cdot 25 \equiv 5 \cdot 6 \equiv 11 \bmod 19$.

If $x = -13$, then $5(-13) \equiv 5 \cdot 6 \equiv 11 \bmod 19$.

Finally, if $x = 63$, then $5 \cdot 63 \equiv 5 \cdot 6 \equiv 11 \bmod 19$.

Therefore, all three of these values for x are solutions to $5x \equiv 11 \bmod 19$. Their least residues are

$$25 \equiv 6 \bmod 19$$
$$-13 \equiv 6 \bmod 19$$
$$63 \equiv 6 \bmod 19$$

Therefore, these are congruent solutions. ◈

It would be useful to know whether a congruence has any solutions and, if so how many, before trying to solve it. In addition, right now trying all possible least residues is our only method to solve congruences. But when solving a congruence such as $57x \equiv 7 \bmod 121$, checking all the possible least residues modulo 121 is not very appealing. It turns out that not only can we tell how many solutions a congruence has before we solve it, but we can also find the solutions using something you already know. The next example illustrates how this works.

Example 6.25 Solve the linear congruence $57x \equiv 7 \bmod 121$.

Solution

Checking all the possibilities to see if there are solutions would mean checking the integers 0 through 120, something we prefer to avoid. Instead, we will look for a different approach.

Using the definition of congruence, rewrite the congruence $57x \equiv 7 \bmod 121$ as

$$121 \mid (57x - 7),$$

which is equivalent to $57x - 7 = 121y$, for some $y \in \mathbb{Z}$. Rearranging this equation produces $57x - 121y = 7$, which is a familiar form: one of the linear equations in two variables from Chap. 5! From Chap. 5, we know that this equation will have a solution, since $\gcd(57, 121) = 1$, and $1|7$. Remember that to find the solution, first apply the Euclidean Algorithm to find $\gcd(57, 121)$, and then follow the process in reverse to solve $57x - 121y = 1$. Finally, multiply both sides by 7 to get back to our original equation.

Euclidean Algorithm	Solve for Remainder
$121 = 2(57) + 7$	$7 = 121 - 2(57)$
$57 = 8(7) + 1$	$1 = 57 - 8(7)$
$7 = 7(1) + 0$	-------

Now, working in reverse from the last equation solved for its remainder:

$$\begin{aligned} 1 &= 57 - 8(7) \\ &= 57 - 8(121 - 2(57)) \\ 1 &= 17(57) - 8(121) \end{aligned}$$

Rewriting the equation in the order of the original problem,

$$57(17) - 121(8) = 1.$$

Finally, multiplying by 7 gives

$$\begin{aligned} 57(7 \cdot 17) - 121(7 \cdot 8) &= 7 \cdot 1 \\ 57(119) - 121(56) &= 7 \end{aligned}$$

Since, the linear equation being solved is $57x - 121y = 7$, $x = 119$ is a solution to the congruence. (To verify that $x = 119$ is a solution, substitute $x = 119$ into the original congruence to make sure it is true.) In fact, any x such that $x \equiv 119 \ mod \ 121$ will also work. Notice that the value of y is extra information in the problem, and is not needed as part of the solution.

◈

The next theorem applies Theorem 5.8 (about solutions of linear equations) to congruences.

Theorem 6.7

Let m be a positive integer and let $\gcd(a, m) = d$. Consider the linear congruence $ax \equiv c \ mod \ m$.

1. If $d \mid c$, then the congruence $ax \equiv c \ mod \ m$ has at least one solution.
2. If $d \nmid c$, then the congruence $ax \equiv c \ mod \ m$ has no solutions.

Theorem 6.8 tells us how to find out how many incongruent solutions a linear congruence will have.

Theorem 6.8

If $\gcd(a, m) = d$ and $d|c$, then $ax \equiv c \ mod \ m$ has exactly d incongruent solutions.

To find the solutions of $ax \equiv c \ mod \ m$, first find one solution using the Euclidean Algorithm method illustrated in Example 6.25. Then, the rest of the solutions will be spaced a distance of $\frac{m}{d}$ from each other, where $d = \gcd(a, m)$.

Therefore, the general form for the incongruent solutions to $ax \equiv c \ mod \ m$ given that x_0 is one solution is

$$x = x_0 + k \cdot \frac{m}{d} \ mod \ m, \ k = 0, \ 1, \ 2, \ \ldots, \ d - 1.$$

The form for all incongruent solutions to $ax \equiv c \ mod \ m$ given that x_0 is one solution is given in Theorem 6.9. (Any value that is congruent modulo m to one of the solutions listed above will be a solution to the congruence.)

> **Theorem 6.9**
> If x_0 is one solution to the linear congruence $ax \equiv c \ mod \ m$, and $d = \gcd(a, m)$, then the incongruent solutions have the form $x = x_0 + k \cdot \frac{m}{d} \ mod \ m$, $k = 0, \ 1, \ 2, \ldots, (d - 1)$.

Example 6.26 Solve $9x \equiv 6 \ mod \ 15$.

Solution
First, since $\gcd(9, 15) = 3$ and $3|6$, there will be three incongruent solutions to this congruence. To find the first solution, use the definitions of congruence and divides to rewrite the congruence as an equation.

$$15|(9x - 6)$$
$$9x - 6 = 15y$$
$$9x - 15y = 6$$

Now, use the Euclidean Algorithm to find $\gcd(9, 15)$ to find a solution of $9x - 15y = \gcd(9, 15)$.

Euclidean Algorithm	Solve for Remainder
$15 = 1(9) + 6$	$6 = 15 - 1(9)$
$9 = 1(6) + 3$	$3 = 9 - 1(6)$
$6 = 2(3) + 0$	---

Beginning with the last equation solved for the remainder:

$$3 = 9 - 1(6)$$
$$= 9 - 1(15 - 1(9))$$
$$= 9 - 15 + 9$$
$$3 = 9(2) - 15(1)$$

This equation gives a solution to $9x - 15y = 3$. To find the solution to the equation we started with, multiply both sides by 2:

$$3 \cdot 2 = 9(2 \cdot 2) - 15(1 \cdot 2)$$
$$6 = 9(4) - 15(2)$$

From this equation, one solution to the congruence is $x_0 = 4$, and there are a total of three incongruent solutions, $\frac{15}{3} = 5$ units apart. Therefore the incongruent solutions are $x_0 = 4, x_1 = 9, \ x_2 = 14$, and the complete solution is

$$x_0 \equiv 4 \ mod \ 15$$
$$x_1 \equiv 9 \ mod \ 15$$
$$x_2 \equiv 14 \ mod \ 15.$$

Notice that adding 5 again onto the last solution of 14 produces 19 which reduces to 4 modulo 15, so this produces a solution but it is congruent to one that has already been found.

◈

Solving a congruence of the form $ax \equiv 1 \ mod \ m$ is often useful. For this congruence to have a solution, $\gcd(a, m)$ must divide 1. Therefore, $ax \equiv 1 \ mod \ m$ only has a solution when $\gcd(a, m) = 1$, or when a and m are relatively prime. In this case, there will be only one solution. For example, if the modulus is 6, $x \equiv 1 \ mod \ 6$ and $5x \equiv 1 \ mod \ 6$ will have solutions, but $2x \equiv 1 \ mod \ 6$, $3x \equiv 1 \ mod \ 6$ and $4x \equiv 1 \ mod \ 6$ will not. (Can you see why?)

Now, think for a minute about the real numbers, and not just the integers. In the real numbers, the equation $ax = 1$ has a solution as long as $a \neq 0$ since $a \cdot \frac{1}{a} = 1$. The values a and $\frac{1}{a}$ are called *inverses* (or, sometimes, *multiplicative inverses*). Following this definition, if there is an integer b such that $ab \equiv 1 \ mod \ m$, then a and b are called ***inverses modulo m***. The formal definition is given in Definition 6.6.

> **Definition 6.6: inverse modulo *m***
> An integer a is the ***inverse of b modulo m*** if and only if $ab \equiv 1 \ mod \ m$. Note that b is also the ***inverse of a modulo m***.

Note that an integer can be its own inverse modulo m. For example, for any m, $1 \cdot 1 \equiv 1 \ mod \ m$, so 1 is always its own inverse modulo m.

Example 6.27 Find the inverse of 7 modulo 10.

Solution
The inverse of 7 modulo 10 is an integer b such that $7b \equiv 1 \ mod \ 10$. Since gcd $(7, 10) = 1$ and $1|1$, there is one solution. The Euclidean Algorithm can be used to solve the problem, but in this case, since the numbers are relatively small, we will

use trial and error. Substituting values for b shows that $7 \cdot 3 \equiv 1 \bmod 10$, so 7 and 3 are inverses of each other modulo 10.

◆

Example 6.28 Find the least residue of each integer that has an inverse modulo 10 and then find the inverse of each one.

Solution
In order to find the inverse of an integer a modulo 10, find a solution to the congruence $ax \equiv 1 \bmod 10$. From Theorem 6.7, we see that for this congruence to have a solution, $\gcd(a, 10)$ must divide 1. This can only happen if $\gcd(a, 10) = 1$. Therefore, least residues with inverses modulo 10 are 1, 3, 7, and 9.

As stated above, $1 \cdot 1 \equiv 1 \bmod 10$, so 1 is its own inverse.

To find the inverse of 3, check values on the list above since they are the only ones with inverses. Since $3 \cdot 7 \equiv 1 \bmod 10$, 3 and 7 are inverses modulo 10, as we saw in Example 6.27.

We still haven't found an inverse for 9, but since $9 \cdot 9 \equiv 1 \bmod 10$, 9 is its own inverse modulo 10.

◆

The next theorem generalizes the result from Example 6.28 about when integers will have an inverse in a particular modulus.

Theorem 6.10
The integer a has an inverse modulo m if and only if $\gcd(a, m) = 1$.

The proof of this theorem is left as Exercise 32.

Example 6.29 Find the least residue of each integer that has an inverse modulo 11 and then find the inverse of each one.

Solution
From Theorem 6.10, if $\gcd(a, 11) = 1$, then a has an inverse modulo 11. Since 11 is prime, $\gcd(11, a) = 1$ for every nonzero least residue modulo 11, so 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10 all have inverses modulo 11 (Note that 0 will never be included on the list of integers with inverses. Exercise 31 asks you to explain why). Now, match up the integers with their inverses:

$$
\begin{aligned}
1 \cdot 1 &\equiv 1 \bmod 11 \\
2 \cdot 6 &\equiv 1 \bmod 11 \\
3 \cdot 4 &\equiv 1 \bmod 11 \\
5 \cdot 9 &\equiv 1 \bmod 11 \\
7 \cdot 8 &\equiv 1 \bmod 11 \\
10 \cdot 10 &\equiv 1 \bmod 11
\end{aligned}
$$

◆

Sometimes calculating an inverse can give you a shortcut for solving a linear congruence, as illustrated in Example 6.30.

Example 6.30   Solve the congruence $7x \equiv 1 \ mod \ 9$.

Solution
The Euclidean Algorithm could be used to solve this congruence which will have one solution, since $\gcd(7, 9) = 1$. But, if we find the inverse of 7 modulo 9, we could also multiply both sides of the congruence by it. Since $7 \cdot 4 \equiv 1 \ mod \ 9$, multiply both sides of the original congruence by 4:

$$4 \cdot 7x \equiv 4 \cdot 1 \ mod \ 9$$
$$28x \equiv 4 \ mod \ 9$$
$$1 \cdot x \equiv 4 \ mod \ 9$$

Therefore, the solution to the congruence $7x \equiv 1 \ mod \ 9$ is $x \equiv 4 \ mod \ 9$.

◆

Exercise Set 6.3

Exercises 1–3.   Solve the linear congruence. Give the least residue of the solution.
  1. $x + 12 \equiv 5 \ mod \ 8$
  2. $x - 5 \equiv 40 \ mod \ 11$
  3. $2x + 11 \equiv x + 4 \ mod \ 13$

  4. Is $x = 14$ a solution to the congruence $6x \equiv 4 \ mod \ 20$
  5. Is $x = 11$ a solution to the congruence $12x \equiv 2 \ mod \ 15$

Exercises 6–15.   Determine whether or not the congruence has any solutions and, if so, how many (incongruent) solutions it has.
  6. $4x \equiv 6 \ mod \ 13$
  7. $2x \equiv 5 \ mod \ 7$
  8. $3x \equiv 6 \ mod \ 9$
  9. $103x \equiv 444 \ mod \ 999$
 10. $15x \equiv 9 \ mod \ 25$
 11. $40x \equiv 3 \ mod \ 20$
 12. $7x \equiv 1 \ mod \ 11$
 13. $8x \equiv 20 \ mod \ 36$
 14. $16x \equiv 32 \ mod \ 20$
 15. $19x \equiv 17 \ mod \ 31$

 16. One solution to the congruence $ax \equiv b \ mod \ 23$ is $x = 4$. Find two more values for x that make the congruence true.
 17. One solution to the congruence $ax \equiv b \ mod \ 16$ is $x = -3$. Find two more values for x that make the congruence true.

Exercises 18–21. Determine whether or not the congruence has any solutions. If so, find the incongruent solutions.

18. $19x \equiv 30 \; mod \; 40$
19. $6x \equiv 4 \; mod \; 8$
20. $14x + 14 \equiv 6 \; mod \; 26$
21. $2x - 8 \equiv 8 \; mod \; 5$

22. In Example 6.25, we found that if $x \equiv 119 \; mod \; 121$, then x is a solution of the congruence $57x \equiv 7 \; mod \; 121$. Find two more (not necessarily incongruent) solutions—one positive and one negative—and show they are solutions of the congruence.

23. For which integers, $0 \leq c < 30$, does the congruence $12x \equiv c \; mod \; 30$ have solutions? When there are solutions, also determine how many incongruent solutions there are.

24. State the contrapositive of part (1) of **Theorem 6.7**.

25. Write an example of a linear congruence with exactly one integer solution.

26. Write an example of a linear congruence with exactly two integer solutions.

27. Write an example of a linear congruence with exactly five integer solutions.

28. If the congruence $ax \equiv b \; mod \; m$ has exactly one integer solution, what can you say about a, b, and m? Explain.

29. Find the inverse of 3 modulo 8. Does every integer have an inverse modulo 8? If not, which integers do?

30. Find the inverse of 3 modulo 5. Does every integer have an inverse modulo 5? If not, which integers do?

31. Explain why 0 will not have an inverse modulo m if $m > 1$.

32. Prove **Theorem 6.10**.

6.4 An Application of Congruences: Identification Numbers and Check Digits

In 1997, a woman started receiving unexpected wire transfers into her bank account which ended up totaling about $700,000. It turned out that she had not won an international lottery as she initially claimed; instead, 13 different foreign governments had been attempting to wire donations into the UN Environment Program's account. Instead, they ended up in her personal bank account; the two account numbers differed by only one digit.

Since so much information is now stored on and processed by computers, things from bank accounts to books, and even individual people, are assigned identification numbers (ID numbers) to help clearly identify them. You probably have a school ID number, so that your bill and your grades are not accidentally sent to another student with the same name. Books have ID numbers called International Standard Book Numbers (ISBNs) for cataloging and to differentiate between different editions of the same book or two completely different books that happen

to have the same title. Products in the grocery store also have ID numbers called Universal Product Codes (UPCs) that are represented by a bar code on the product packaging so that the cashier can quickly scan in the product. Your credit card number is an ID number that allows you (and hopefully no one else) to purchase products in stores or online.

When these numbers are read, typed, or scanned into a computer, what happens if they are not transferred correctly? Could you order the wrong book if you type in one digit of the ISBN incorrectly? Could you be charged for lobster when you are trying to buy ramen noodles if the grocery store scanner misreads the bar code on your purchase? Could your credit card be charged if someone else accidentally reverses two digits when typing his credit card number into amazon.com?

To avoid potential mix-ups like these, as well as to prevent forgeries of things like money orders or airline tickets, most identification numbers are equipped with a digit called a ***check digit***. This check digit is included somewhere in the ID number (often, but not always, at the end) and is calculated using a formula called a ***check digit scheme***. The formulas used to calculate check digits vary in complexity and many incorporate congruences. The check digit schemes are determined by the institution that formulates the ID numbers, so there are different schemes for different types of identification numbers. Here are some examples.

6.4.1 US Postal Service Money Orders

In order to keep track of the money orders issued and prevent fraud, each US Postal Service money order has an 11-digit serial number. The last digit is the check digit and the check digit scheme is described below.

Check Digit Scheme for US Postal Money Orders

USPS money orders have serial numbers with 11 digits which are represented as:

$$a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11}$$

The check digit, a_{11}, is chosen so that

$$a_{11} \equiv a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} \; mod \; 9$$

Example 6.31 Verify that the serial number on the US Postal Service money order below satisfies the check digit scheme.

United States Postal Service Money Order

Solution

The serial number on this money order is 69943964084. The check digit, 4, must be congruent modulo 9 to the sum of the rest of the digits in the serial number.

$$
\begin{aligned}
6 + 9 + 9 + 4 + 3 + 9 + 6 + 4 + 0 + 8 &\equiv 6 + 4 + 3 + 6 + 4 + 8 \bmod 9 \\
&\equiv 10 + 9 + 12 \bmod 9 \\
&\equiv 1 + 0 + 3 \bmod 9 \\
&\equiv 4 \bmod 9
\end{aligned}
$$

The serial number does satisfy the check digit scheme.

◆

6.4.2   Universal Product Codes

The Universal Product Code is a 12-digit identification number that is used by stores and manufacturers to keep track of the items they sell. The digits of the ID number are encoded in the bar code symbol that is scanned by the cashier when you check out. Computerized cash registers are programmed with a check digit scheme. If the number does not satisfy the scheme, then the cashier will have to re-scan the item. The check digit scheme for UPC codes works as follows.

Check Digit Scheme for UPC Symbols

UPC numbers have 12 digits which we will represent as:

$$a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11} a_{12}.$$

The check digit, a_{12}, is chosen so that

$$3a_1 + a_2 + 3a_3 + a_4 + 3a_5 + a_6 + 3a_7 + a_8 + 3a_9 + a_{10} + 3a_{11} + a_{12}$$
$$\equiv 0 \bmod 10$$

Example 6.32 The UPC on a box of peppermints is 817335042120 (Notice the placement of the digits of the UPC on the package). Verify that this ID number satisfies the check digit scheme for UPC symbols.

Photo of VerMint®s, made by VerMints Inc.

Solution

In this case, 0 is the check digit, and it should have been chosen to make the sum in the check digit scheme congruent to 0 modulo 10. To simplify the congruence, use the rules listed in Theorem 6.6, which allow us to replace integers in a congruence with their least residue. Substituting the given UPC into the left side of the check digit scheme, we will then reduce each value modulo 10. Once all the terms are less than 10, group numbers so that the sum is larger than 10 and reduce again:

$$(3 \cdot 8) + 1 + (3 \cdot 7) + 3 + (3 \cdot 3) + 5 + (3 \cdot 0) + 4 + (3 \cdot 2) + 1 + (3 \cdot 2) + 0$$
$$\equiv 24 + 1 + 21 + 3 + 9 + 5 + 4 + 6 + 1 + 6 \ mod \ 10$$
$$\equiv 4 + 1 + 1 + 3 + 9 + 5 + 4 + 6 + 1 + 6 \ mod \ 10$$
$$\equiv (4 + 1 + 1 + 3 + 9) + (5 + 4 + 6) + (1 + 6) \ mod \ 10$$
$$\equiv 18 + 15 + 7 \ mod \ 10$$
$$\equiv 8 + 5 + 7 \ mod \ 10$$
$$\equiv 13 + 7 \ mod \ 10$$
$$\equiv 0 \ mod \ 10$$

The UPC ID number checks out!

◈

Example 6.33 In the summer of 2013, "rainbow looms" became very popular for making colorful bracelets and necklaces out of small rubber bands. Almost immediately, several other companies began making similar products with similar names and offered them for sale. One way to make sure you get the product you want is to identify it with the UPC code. The first eleven digits of the UPC for the

original rainbow loom are 67054116018___. Verify that the check digit for this product is 3.

Solution
Apply the check digit scheme for UPCs to make sure that it works for this code with 3 as the check digit:

$$3(6) + 7 + 3(0) + 5 + 3(4) + 1 + 3(1) + 6 + 3(0) + 1 + 3(8) + 3$$
$$\equiv 18 + 7 + 5 + 12 + 1 + 3 + 6 + 1 + 24 + 3 \; mod \; 10$$
$$\equiv 8 + 7 + 5 + 2 + 1 + 3 + 6 + 1 + 4 + 3 \; mod \; 10$$
$$\equiv (8 + 7) + (5 + 2 + 1 + 3) + (6 + 1 + 4) + 3 \; mod \; 10$$
$$\equiv 15 + 11 + 11 + 3 \; mod \; 10$$
$$\equiv 5 + 1 + 1 + 3 \; mod \; 10$$
$$\equiv 0 \; mod \; 10$$

The UPC checks out!

◈

6.4.3   International Standard Book Number

The International Standard Book Number, or ISBN, is an ID number assigned to each book to clearly identify the book. Different editions of a book and different books of the same title will have different ISBNs.

In 2007, the book industry changed from 10-digit-long ISBNs to 13-digit-long ISBNs. Books published prior to 2007 were issued a new 13-digit ISBN in addition to their original 10-digit ISBN. In each case, the last digit of the ID number is the check digit, but there is a separate check digit scheme for each type of ISBN.

Check Digit Scheme for 10-Digit ISBNs

ISBNs with 10 digits are represented as:

$$a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10}$$

The check digit a_{10} is chosen so that

$$10 \cdot a_1 + 9 \cdot a_2 + 8 \cdot a_3 + 7 \cdot a_4 + 6 \cdot a_5 + 5 \cdot a_6 + 4 \cdot a_7 + 3 \cdot a_8 + 2 \cdot a_9 + a_{10}$$
$$\equiv 0 \; mod \; 11$$

Note that since this scheme is computed modulo 11, it is possible that the check digit could be 10. Since the check digit can only be one character long, a check digit of 10 is replaced by an X in the ten-digit ISBN.

> **Check Digit Scheme for 13-Digit ISBNs**
>
> ISBNs with 13 digits are represented as:
>
> $$a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}a_{13}$$
>
> The check digit a_{13} is chosen so that
>
> $a_1 + 3a_2 + a_3 + 3a_4 + a_5 + 3a_6 + a_7 + 3a_8 + a_9 + 3a_{10} + a_{11} + 3a_{12}$
> $\quad + a_{13}$
> $\quad \equiv 0 \ mod \ 10$

Example 6.34 Over 900 different editions of the classic Shakespeare play *Romeo and Juliet* have been published, so using the ISBN to order a copy will allow you to be certain that you get the right one. The ISBN for an edition by Dover is 0486275574. Verify that it satisfies the appropriate check digit scheme.

Solution
Since this is a 10-digit ISBN, we will confirm that the check digit, 4, satisfies the scheme given for 10-digit ISBNs. Substituting into the left-hand side of the check digit scheme:

$(10 \cdot 0) + (9 \cdot 4) + (8 \cdot 8) + (7 \cdot 6) + (6 \cdot 2) + (5 \cdot 7) + (4 \cdot 5) + (3 \cdot 5) + (2 \cdot 7) + 4$
$\equiv 0 + 36 + 64 + 42 + 12 + 35 + 20 + 15 + 14 + 4 \ mod \ 11$
$\equiv 0 + 3 + 9 + 9 + 1 \ + 2 + 9 + 4 + 3 + 4 \ mod \ 11$
$\equiv 12 + 12 + 13 + 7 \ mod \ 11$
$\equiv 1 + 1 + 2 + 7 \ mod \ 11$
$\equiv 11 \ mod \ 11$
$\equiv 0 \ mod \ 11$

Therefore, the check digit scheme is satisfied by this ISBN.

◈

Exercise Set 6.4

1. The 10-digit ISBN for the children's book *The Math Curse* by Jon Scieszka and Lane Smith has the first 9 digits 0-670-86194-__. Show that the check digit is 4.
2. If a customer wants to cash a postal money order with the serial number 75435899213, should the cashier give him the money, or call the police?
3. Determine whether or not the check digit scheme for USPS money orders would catch each of the following errors. Explain why or why not.

   (a)   A 9 in the serial number is accidentally replaced with a 0.

    (b)   An 8 in the serial number is accidentally replaced with a 0.
    (c)   The order of the first and second digits is accidentally reversed.
    (d)   The order of the tenth and eleventh digits is accidentally reversed.

4. The book *Harry Potter and the Prisoner of Azkaban* by J.K. Rowling has been published in about 70 different languages and about 200 different editions. The first twelve digits of the 13-digit ISBN for a German edition published in 1999 are 978355155169__. Confirm that the check digit is 6.

5. An ID number for *The Hunger Games* written by Suzanne Collins is 9780439023481. Determine whether this is the UPC for the movie DVD or the ISBN for the book and then use the appropriate check digit scheme to make sure the ID is valid.

6. Find a product with a 12-digit UPC code and test it to make sure that the check digit scheme works for the UPC code you find.

7. Apply the appropriate ISBN check digit scheme to the ISBN of your favorite book.

8. Use the UPC check digit scheme to verify the UPC code on your favorite snack.

9. There are other check digit schemes in addition to those listed here. Look up the check digit scheme for a bank's Routing Transit Number and confirm that it works on your number. (Note: the routing transit number is not your account number. It is the nine-digit bank code that is printed on the bottom of checks.)

6.5   The Chinese Remainder Theorem

Suppose that a farmer with cows and chickens has 72 legs among the 20 animals on his farm. (The farmer is not included in either count.) How many chickens and how many cows are on this farm? This type of question is common in algebra classes. One way to solve it is to set up some equations that model the information given. For example, if $x = $ *number of cows* and $y = $ *number of chickens*, then we obtain two equations:

$$x + y = 20$$
$$4x + 2y = 72$$

Notice that this is a different situation than in Chap. 5, when we were solving a single linear equation in two variables. Here there is a system of linear equations, because the additional piece of information (the number of animals) allows us to write a second equation. One way to answer the question is to solve the first equation for one variable and then substitute into the second. Solving the first equation for x gives $x = 20 - y$. Substituting into the second equation, we get

$$4(20 - y) + 2y = 72$$
$$80 - 4y + 2y = 72$$
$$-2y + 80 = 72$$
$$-2y = -8$$
$$y = 4$$

which means there are 4 chickens on the farm. Using the equation $x = 20 - y$, we find there are 16 cows.

Just as we were able to generalize linear equations to linear congruences, systems of linear equations can be generalized to systems of linear congruences. This type of problem has been around for an extremely long time. One of the first known problems involving a system of linear congruences was recorded by ancient Chinese mathematician Sun Zi, who lived sometime between the third and fifth century. Little is known about him, except that he wrote a three chapter mathematical work which included instructions, problems, and the earliest known example of a problem involving a system of congruences. Here is the question he asked:

> *Suppose we have an unknown number of objects. When counted in threes, 2 are left over, when counted in fives, 3 are left over, and when counted in sevens, 2 are left over. How many objects are there?*

Notice that this question is all about remainders, so we can write it in terms of congruences. If x represents the unknown number of objects, then when x is divided by 3, the remainder is 2; when x is divided by 5, the remainder is 3; and when x is divided by 7, the remainder is 2. Rewriting each of these in terms of a congruence, we get the following:

$$x \equiv 2 \ mod \ 3$$
$$x \equiv 3 \ mod \ 5$$
$$x \equiv 2 \ mod \ 7$$

Therefore, to find x, we must solve this system of congruences. In other words, find an integer x that makes all three congruences true. It turns out that we can use a technique very similar to the method for solving systems of linear equations. We will start with an example with just two congruences to see how it works.

Example 6.35 Solve the system of congruences

$$x \equiv 1 \ mod \ 3$$
$$x \equiv 5 \ mod \ 7.$$

Solution
Start by rewriting the first congruence as an equation, using the definition of congruence and the definition of divides.

$$x \equiv 1 \bmod 3$$
$$3 \mid (x - 1)$$
$$x - 1 = 3k$$
$$x = 3k + 1$$

Now, substitute this formula for x that satisfies the first congruence into the second congruence.

$$3k + 1 \equiv 5 \bmod 7$$

The goal now is to find a formula for k that can be substituted back into the equation for x. To do this, solve the congruence for k. Start by subtracting 1 from both sides of the congruence to get:

$$3k \equiv 4 \bmod 7.$$

Unfortunately, we cannot simply divide by 3 to solve for k; however, we can multiply both sides of the congruence by the *inverse* of 3 modulo 7. Checking a few values shows that $5 \cdot 3 \equiv 1 \bmod 7$. Therefore, multiply both sides of the congruence by 5:

$$5 \cdot 3k \equiv 5 \cdot 4 \bmod 7$$
$$1 \cdot k \equiv 20 \bmod 7$$
$$k \equiv 6 \bmod 7$$

Using the definition of congruence again, we can rewrite this congruence as an equation for k:

$$7 \mid (k - 6)$$
$$k - 6 = 7t$$
$$k = 6 + 7t$$

Substituting for k in $x = 3k + 1$,

$$x = 3(6 + 7t) + 1$$
$$= 18 + 21t + 1$$
$$x = 19 + 21t$$

This might not be quite the form you would expect for x, because there is still a variable of t in the formula. But, remember that x came from a congruence, so there will always be more than one possible integer to satisfy the congruence. We can work backwards from the formula for x to see what congruence it gives us:

$$x = 19 + 21t$$
$$x - 19 = 21t$$
$$21 \mid (x - 19)$$

Therefore, the solution is $x \equiv 19 \bmod 21$. Checking the original system, we see that $19 \equiv 1 \bmod 3$ and $19 \equiv 5 \bmod 7$ are both true.

◆

Returning to the question proposed by the ancient Chinese mathematician Sun Zi, we will see if it can be solved using the same idea as in Example 6.35.

Example 6.36 Find a solution to the system of congruences

$$x \equiv 2 \bmod 3$$
$$x \equiv 3 \bmod 5$$
$$x \equiv 2 \bmod 7$$

Solution
Start with the first congruence, and rewrite it as an equation:

$$x \equiv 2 \bmod 3$$
$$3 \mid (x - 2)$$
$$x - 2 = 3k$$
$$x = 2 + 3k$$

Substitute the formula obtained for x into the second congruence, $x \equiv 3 \bmod 5$, and solve for k:

$$2 + 3k \equiv 3 \bmod 5$$
$$3k \equiv 1 \bmod 5$$
$$2 \cdot 3k \equiv 2 \cdot 1 \bmod 5$$
$$6k \equiv 2 \bmod 5$$
$$k \equiv 2 \bmod 5$$

Rewrite the congruence for k as an equation:

$$k \equiv 2 \bmod 5$$
$$5 \mid (k - 2)$$
$$k - 2 = 5t$$
$$k = 2 + 5t$$

Use this formula for k to rewrite x:

$$x = 2 + 3k = 2 + 3(2 + 5t) = 2 + 6 + 15t = 8 + 15t$$

Now substitute this equation for x into the third congruence in the system.

$$x \equiv 2 \bmod 7$$
$$8 + 15t \equiv 2 \bmod 7$$
$$15t \equiv -6 \bmod 7$$
$$t \equiv 1 \bmod 7$$

Finally, use the congruence $t \equiv 1 \bmod 7$ to write an equation for t which we will substitute into the equation for x to find the solution.

$$t \equiv 1 \bmod 7$$
$$7 \,|\, (t-1)$$
$$t - 1 = 7m$$
$$t = 1 + 7m$$

Then,

$$\begin{aligned} x &= 8 + 15t \\ &= 8 + 15(1 + 7m) \\ &= 8 + 15 + 105m \\ &= 23 + 105m \end{aligned}$$

Since $x = 23 + 105m$, we can also write that $x \equiv 23 \bmod 105$. A quick check shows that this value does satisfy all three of the congruences given in the problem. ◈

One question to ask at this point is if all systems of linear congruences will have a solution. The answer is no. The Chinese Remainder Theorem gives an example of a particular type of system of linear congruences that is guaranteed to have solutions. The Chinese Remainder Theorem is called an *existence* theorem; in other words, it tells you when a solution exists, but it does not tell you what the solution is. This is only somewhat useful, but in order to prove the theorem, we will actually construct a general solution and show that it works (This is called a *constructive* proof). Therefore, the theorem together with the solution constructed in the proof will allow us to solve linear systems of congruences that fit the form required in the Chinese Remainder Theorem. The Chinese Remainder Theorem can be stated for a system with any number of linear congruences. We will start with two congruences and then look at the general case.

Theorem 6.11 Chinese Remainder Theorem (for Two Congruences)
Let m_1 and m_2 be positive integers with $\gcd(m_1, m_2) = 1$. Then the system of linear congruences

$$z \equiv a \bmod m_1$$
$$z \equiv b \bmod m_2$$

has a unique solution modulo $m_1 m_2$. (This means that it has one solution z with $0 \le z < m_1 m_2$.)

Proof. There are two parts to this proof. The first is to construct a solution and show that it satisfies both of the congruences. Second, we must show that there is only one incongruent solution modulo $m_1 m_2$. To do this we will assume that there are two solutions and show that they are congruent modulo $m_1 m_2$.

Part I: Constructing a Solution
To find a solution, find a value for z so that both congruences are satisfied: in other words, it must be true that $z \equiv a \bmod m_1$ and $z \equiv b \bmod m_2$. Suppose we begin with $z = a + b$. If we could find a way to cancel out the b when we substitute into the first congruence and cancel out the a for the second congruence, we would have it. One way to do this is to multiply each by a factor that will be zero in the modulus of the congruence. For example, in the first congruence, we want the term with b to be zero. So, we can multiply b by m_1 to get $z = a + bm_1$. Then, in the second congruence we want the term with a to disappear, so we can multiply a by m_2 so that $z = am_2 + bm_1$. Now, substitute $z = am_2 + bm_1$ into each of the original congruences to see if we have a solution.

Substituting into $z \equiv a \bmod m_1$:	**Substituting into $z \equiv b \bmod m_2$:**
$z \equiv am_2 + bm_1 \equiv am_2 + 0 \bmod m_1$	$z \equiv am_2 + bm_1 \equiv 0 + bm_1 \bmod m_2$
$z \equiv am_2 \bmod m_1$	$z \equiv bm_1 \bmod m_2$

Neither of these is quite what we want–in each case, there is an extra factor left in the congruence. Since $\gcd(m_1, m_2) = 1$, we know that m_2 has an inverse modulo m_1: call it x_1. Similarly, m_1 has an inverse modulo m_2: call it x_2. Therefore, the following two congruences are true:

$$m_2 x_1 \equiv 1 \bmod m_1$$
$$m_1 x_2 \equiv 1 \bmod m_2$$

Now, adjust the formula for z to include these inverses: $z = am_2 x_1 + bm_1 x_2$.

Testing $z = am_2 x_1 + bm_1 x_2$ in both original congruences again, we get:

Substituting into $z \equiv a \bmod m_1$:	**Substituting into $z \equiv b \bmod m_2$:**
$z \equiv am_2 x_1 + bm_1 x_2 \bmod m_1$	$z \equiv am_2 x_1 + bm_1 x_2 \bmod m_2$
$z \equiv am_2 x_1 \bmod m_1$	$z \equiv bm_1 x_2 \bmod m_2$
$z \equiv a \bmod m_1$	$z \equiv b \bmod m_2$

This time the original congruence is returned in each case. Finally, this shows $z = am_2 x_1 + bm_1 x_2$ is a general form for the solution of a system of two congruences, when the moduli are relatively prime.

Part II: Show There Is Only One Solution Modulo $m_1 m_2$:
To show z is unique modulo $m_1 m_2$, show that any other solution is congruent to z modulo $m_1 m_2$. Suppose that z' is another solution of the two congruences. Then

$$z' \equiv a \bmod m_1$$
$$z' \equiv b \bmod m_2$$

are also true, so that

$$z \equiv z' \bmod m_1$$
$$z \equiv z' \bmod m_2.$$

From the definition of congruence, we have that $m_1|(z - z')$ and $m_2|(z - z')$. Since $\gcd(m_1, m_2) = 1$, it is also true that $m_1 m_2|(z - z')$. (This fact is proved in Exercise 19 of Section 5.3). By the definition of congruence, this means that $z \equiv z' \bmod m_1 m_2$. ∎

Example 6.37 Find the solution to the system of linear congruences. Give the least residue of the solution.

$$z \equiv 4 \bmod 10$$
$$z \equiv 3 \bmod 7$$

Solution
According to the Chinese Remainder Theorem, since $gcd(10, 7) = 1$, this system of congruences will have one solution between 1 and $10(7) = 70$.

From the constructive proof of Theorem 6.11, we know that the solution will have the form $z = 4 \cdot 7x_1 + 3 \cdot 10x_2$, where x_1 and x_2 are chosen so that

$$7x_1 \equiv 1 \bmod 10$$
$$10x_2 \equiv 1 \bmod 7$$

To solve $7x_1 \equiv 1 \bmod 10$, we can use trial and error to find that $7 \cdot 3 \equiv 21 \equiv 1 \bmod 10$, so $x_1 = 3$.
To solve $10x_2 \equiv 1 \bmod 7$, we can make things easier by first reducing 10 modulo 7. This results in the congruence $3x_2 \equiv 1 \bmod 7$. Again by trial and error, $3 \cdot 5 \equiv 15 \equiv 1 \bmod 7$. Therefore, $x_2 = 5$.
Substituting into the equation for z, we find that the solution is

$$z = 4 \cdot 7x_1 + 3 \cdot 10x_2 = 4 \cdot 7 \cdot 3 + 3 \cdot 10 \cdot 5 = 234$$

Since there is one solution between 1 and 70, the least residue of z is $z \equiv 24 \bmod 70$.
Checking the solution by substituting into the original two congruences, we see that each is true for the value $z = 24$.

◆

Example 6.38 Show that $x = 10$ and $x = 22$ are both solutions to the system of congruences

$$x \equiv 2 \ mod \ 4$$
$$x \equiv 4 \ mod \ 6$$

and explain why this does not contradict the Chinese Remainder Theorem.

Solution

To show that $x = 10$ is a solution, substitute 10 into each of the congruences.

$$10 \equiv 2 \ mod \ 4 \text{ is true since } 10 - 2 = 8 \text{ and } 4 | 8.$$
$$10 \equiv 4 \ mod \ 6 \text{ is true since } 10 - 6 = 4 \text{ and } 4 | 4.$$

Also, $x = 22$ is a solution.

$$22 \equiv 2 \ mod \ 4 \text{ is true since } 22 - 2 = 20 \text{ and } 4 | 20.$$
$$22 \equiv 4 \ mod \ 6 \text{ is true since } 22 - 6 = 16 \text{ and } 4 | 16.$$

Therefore, in this example there are two incongruent solutions less than 24, the product of the two moduli. The Chinese Remainder Theorem is not contradicted, because its condition is not true here; it only tells us what will happen when we are working with a system of congruences with relatively prime moduli. Here, the congruences do not have relatively prime moduli since $\gcd(4, 6) = 2$, so the Chinese Remainder Theorem tells us nothing at all.

◈

When the conditions of the Chinese Remainder Theorem are not met, the conclusion of the theorem does not apply. If there are solutions, they might not be unique, as in Example 6.38. In other cases, there may be no solutions at all, as Example 6.39 shows.

Example 6.39 Show that this system of linear congruences below has no solutions.

$$x \equiv 2 \ mod \ 4$$
$$x \equiv 3 \ mod \ 6$$

Solution

First, rewrite each of these congruences as an equation. If $x \equiv 2 \ mod \ 4$, then $4 | (x - 2)$, so $x - 2 = 4k$. Solving for x, $x = 4k + 2$.

Using the second congruence, if $x \equiv 3 \ mod \ 6$, then $6 | (x - 3)$, so $x - 3 = 6m$. Solving for x in this case, $x = 6m + 3$.

Now, setting the two formulas for x equal to each other, we obtain the following:

$$4k + 2 = 6m + 3$$
$$4k = 6m + 1$$

This is impossible, because it is saying that $4k$ is an odd number. To see this more clearly, we can factor a 2 out of each even term:

$$2(2k) = 2(3m) + 1$$

The form on the left satisfies the definition of even, and the formula on the right satisfies the definition of odd. Since this is impossible, there is no solution to the system of congruences above. Even though each individual congruence has solutions, there is no number that will make both true at the same time.

◈

The Chinese Remainder Theorem can be extended to any number of linear congruences, as long as the moduli of any two of the congruences are relatively prime. Here is a more general version.

Theorem 6.12 General Chinese Remainder Theorem
Let $m_1, m_2, \ldots, m_n$ be positive integers such that $\gcd(m_i, m_j) = 1$ when m_i and m_j are two different integers from the list. Then the system of linear congruences

$$z \equiv a_1 \bmod m_1$$
$$z \equiv a_2 \bmod m_2$$
$$\vdots$$
$$z \equiv a_n \bmod m_n$$

has a unique solution modulo $m_1 \cdot m_2 \cdots \cdots m_n$.
    (This means that there is only one value for z with $0 \leq z < m_1 \cdot m_2 \cdots \cdots m_n$ that satisfies all of the congruences in the system.)

Sketch of the Proof.
The proof of the more general version follows the same pattern as the case for two congruences but is slightly more complicated and beyond this course, so we will not include it here. However, we will construct the general solution for three congruences.

$$z \equiv a_1 \bmod m_1$$
$$z \equiv a_2 \bmod m_2$$
$$z \equiv a_3 \bmod m_3$$

Starting with $z = a_1 + a_2 + a_3$, we need to cancel out two of the three terms in each congruence. For example, a_1 appears in the first congruence but not the second or third. Therefore, multiply a_1 by m_2 and m_3. Using similar reasoning for the other two terms, we obtain

$$z = a_1 m_2 m_3 + a_2 m_1 m_3 + a_3 m_1 m_2$$

Now, the extra factors can be canceled out by computing inverses of $m_2 m_3$, $m_1 m_3$, and $m_1 m_2$. The congruences that need to be solved to find these inverses are

$$m_2 m_3 x \equiv 1 \ mod \ m_1$$
$$m_1 m_3 x \equiv 1 \ mod \ m_2$$
$$m_1 m_2 x \equiv 1 \ mod \ m_3$$

Since one of the premises of the theorem is that none of the moduli have any common factors, in each case above the congruence will have a solution. Therefore, if the solutions are x_1, x_2, and x_3, we have the following congruences:

$$m_2 m_3 x_1 \equiv 1 \ mod \ m_1$$
$$m_1 m_3 x_2 \equiv 1 \ mod \ m_2$$
$$m_1 m_2 x_3 \equiv 1 \ mod \ m_3$$

Finally this allows us to find the general form for the solution when the system has three congruences:

$$z = a_1 m_2 m_3 x_1 + a_2 m_1 m_3 x_2 + a_3 m_1 m_2 x_3$$

In Exercise 9, you are asked to check to see that this is indeed a solution of all congruences in the system.

∎

Example 6.40 Solve the congruence $11x \equiv 3 \ mod \ 40$.

Solution
From Section 6.4, since $\gcd(11, 40) = 1$, this congruence has one incongruent solution modulo 40. We can find it using the Euclidean Algorithm method of Section 6.4, but sometimes it is also possible to use the Chinese Remainder Theorem to break up a congruence with a large modulus into several smaller more manageable congruences (with relatively prime moduli).

The prime factorization of the modulus 40 is $40 = 2^3 \cdot 5$, so use 8 and 5 for the moduli, since they are relatively prime.

Now, consider the system of congruences:

$$11x \equiv 3 \ mod \ 5$$
$$11x \equiv 3 \ mod \ 8$$

These are not quite in the form given in the Chinese Remainder Theorem, but notice the 11 in front of the x can be reduced in both cases:

$$x \equiv 3 \ mod \ 5$$
$$3x \equiv 3 \ mod \ 8$$

Then, multiplying both sides of the second congruence by 3, we obtain $9x \equiv 9 \ mod \ 8$, or $x \equiv 1 \ mod \ 8$.

Now the system is:

$$x \equiv 3 \ mod \ 5$$
$$x \equiv 1 \ mod \ 8$$

This does fit the form given in the Chinese Remainder Theorem, and since the moduli are relatively prime, we know that this system has a unique solution modulo 40. The solution to this system will also be the solution to the original congruence. The solution of the system will have the form $x = 3 \cdot 8 \cdot x_1 + 1 \cdot 5 \cdot x_2$, where $8x_1 \equiv 1 \ mod \ 5$ and $5 \cdot x_2 \equiv 1 \ mod \ 8$. Therefore, $x_1 = 2$ and $x_2 = 5$. Thus, the solution becomes $x = 3 \cdot 8 \cdot 2 + 1 \cdot 5 \cdot 5 = 73$. Since the solution is unique modulo 40, the least residue is $x \equiv 33 \ mod \ 40$. Substituting this value into the original congruence, $11x \equiv 3 \ mod \ 40$, gives $11(33) \equiv 363 \equiv 3 \ mod \ 40$.

◆

Example 6.41 A professor feeds his pet python every four days and bathes it once a week. This week he fed it on Tuesday and bathed it on Wednesday. When, if ever, will he feed and wash the python on the same day?

Solution

Let us denote this Tuesday when the python was fed as day 1. Then, since the python is fed every four days, he will eat on day 1, day 5, day 9, ... or when the day number, x, satisfies $x \equiv 1 \ mod \ 4$. Also, since the python is bathed on Wednesday, day 2, and he bathes every 7 days, he will have a bath on day x if $x \equiv 2 \ mod \ 7$.

Then, the question we would like to answer is if there is a day that satisfies both congruences. In other words, is there a solution to the following system of congruences?

$$x \equiv 1 \ mod \ 4$$
$$x \equiv 2 \ mod \ 7$$

According to the Theorem 6.11, the Chinese Remainder Theorem, since gcd $(4, 7) = 1$ there is a unique solution to this system of congruences modulo 28. In order to find the solution, we can use the formula from the constructive proof of Theorem 6.11.

Using this formula, we obtain that $x = 1 \cdot 7x_1 + 2 \cdot 4x_2 = 7x_1 + 8x_2$, where x_1 and x_2 are chosen so that $7x_1 \equiv 1 \ mod \ 4$ and $4x_2 \equiv 1 \ mod \ 7$. Substituting values into these congruences, we find that $x_1 = 3$ and $x_2 = 2$. Therefore, $x = 7(3) + 8(2) = 37$ is a solution to the system of congruences. The solution is unique modulo 28, so if $x \equiv 37 \ mod \ 28$, then the snake will eat and bathe on day x. Since the least residue of 37 modulo 28 is 9, the first day the snake will bathe and eat is the ninth day, and if $x \equiv 9 \ mod \ 28$, the python will eat and bathe on that day.

◆

Example 6.42 Solve the system of congruences.

$$x \equiv 2 \ mod \ 3$$
$$x \equiv 5 \ mod \ 4$$
$$x \equiv -3 \ mod \ 7$$

Solution
This is solvable since any two of the moduli are relatively prime, and the Chinese Remainder Theorem applies. From the general form for the solution of a system with three congruences,

$$z \equiv 2 \cdot 4 \cdot 7 \cdot x_1 + 5 \cdot 3 \cdot 7 \cdot x_2 + (-3) \cdot 3 \cdot 4 \cdot x_3 \ mod \ 84$$

where

$$4 \cdot 7 \cdot x_1 \equiv 1 \ mod \ 3$$
$$3 \cdot 7 \cdot x_2 \equiv 1 \ mod \ 4$$
$$3 \cdot 4 \cdot x_3 \equiv 1 \ mod \ 7$$

Reducing the coefficients of x in each modulus, we can simplify each of these congruences into the following:

$$x_1 \equiv 1 \ mod \ 3$$
$$x_2 \equiv 1 \ mod \ 4$$
$$5x_3 \equiv 1 \ mod \ 7$$

In the last case, since $5 \cdot 3 \equiv 1 \ mod \ 7$, multiplying both sides by 3 yields

$$x_3 \equiv 3 \ mod \ 7$$

Finally substituting these values into the formula for z, and simplifying, we obtain the solution to the original system of congruences.

$$z \equiv 2 \cdot 4 \cdot 7 \cdot 1 + 5 \cdot 3 \cdot 7 \cdot 1 + (-3) \cdot 3 \cdot 4 \cdot 3 \ mod \ 84$$
$$z \equiv 53 \ mod \ 84$$

◈

From these examples, one can see that a major issue in computing solutions using the Chinese Remainder Theorem is solving the congruences needed to find the inverses that are part of the solution. In the examples in this section, the numbers were small enough so that these inverses could be found by trial and error. However, if the numbers were larger, we could use the techniques of Section 6.4 to solve these congruences. For large numbers or large systems of congruences, these solutions will become too long computationally to be done by hand. The Chinese Remainder Theorem is still useful for determining whether systems of equations have solutions, and it has applications in computing. For example,

because it allows you to break up larger moduli into relatively prime components, it can be used to compute with numbers larger than the "word" capacity of a computer.

Exercise Set 6.5

Exercises 1–5. Determine whether the given value of x is a solution of the system of congruences.

1. $x = 31$
    $x \equiv 4 \bmod 9$
    $x \equiv 9 \bmod 20$

2. $x = 28$
    $x \equiv 2 \bmod 3$
    $x \equiv 4 \bmod 8$

3. $x = 8$
    $4x \equiv 2 \bmod 5$
    $2x \equiv 1 \bmod 3$

4. $x = 34$
    $x \equiv 4 \bmod 10$
    $x \equiv 5 \bmod 7$

5. $x = 5$
    $3x \equiv 5 \bmod 10$
    $5x \equiv 1 \bmod 6$

Exercises 6–8. Find the least non-negative solution to each system of congruences below.

6. $x \equiv 3 \bmod 4$
    $x \equiv 2 \bmod 5$

7. $x \equiv 2 \bmod 3$
    $x \equiv 1 \bmod 8$

8. $x \equiv 1 \bmod 7$
    $x \equiv 4 \bmod 6$

9. Verify that the general solution constructed in the proof sketch of Theorem 6.12 satisfies the system of three linear congruences.

10. Find the general form of the solution to a system of four linear congruences when their moduli do not have any common factors and show that it satisfies each congruence in the system (Hint: Look for a pattern in the solution for two congruences and the solution for three congruences).

Exercises 11–16. Solve the system of linear congruences. Give the least residue of the solution.

11. $z \equiv 3 \bmod 5$
    $z \equiv 3 \bmod 8$

12. $z \equiv 3 \bmod 5$
    $z \equiv 2 \bmod 8$

13. $z \equiv -5 \bmod 6$
    $z \equiv -5 \bmod 7$

14. $z \equiv 4 \bmod 5$
    $z \equiv 5 \bmod 7$

15. $z \equiv 4 \bmod 6$
    $z \equiv 5 \bmod 7$

16. $z \equiv 20 \bmod 9$
    $z \equiv -3 \bmod 10$

Exercises 17–19. Find a value of z that solves the system of congruences.

17. $z \equiv 1 \bmod 3$, $z \equiv 1 \bmod 5$, $z \equiv 1 \bmod 7$
18. $z \equiv 5 \bmod 7$, $z \equiv 2 \bmod 12$, $z \equiv 8 \bmod 13$
19. $z \equiv 2 \bmod 3$, $z \equiv 3 \bmod 5$, $z \equiv 2 \bmod 7$

20. Professor Merck buys a new car every three years; he bought his first car in 1981. He gets a sabbatical leave every seven years, starting in 1992. When does he first get both during the same year?

6.6   Summary and Review Exercises

6.6.1   Vocabulary and Symbols

congruence $a \equiv b \bmod m$
congruent modulo m
modulus
least residue of b modulo m
reducing an integer modulo m
set of least residues modulo m
complete system of residues modulo m
linear congruence
congruent solutions
incongruent solutions
inverse modulo m
check digit
check digit scheme

Universal Product Code (UPC)
International Standard Book Number (ISBN)
system of linear congruences
Chinese Remainder Theorem

6.6.2   Suggested Readings

Gallian, J. S. *The Mathematics of Identification Numbers*. **The College Mathematics Journal**. Vol 22, (1991) pp 194–202.
Khovanova, Tanya *A Story of Storytelling Numbers*. **Math Horizons**. (Sept. 2009): 14–17. Also at www.maa.org/mathhorizons
Plummer, Phil. *Divisibility tests for primes greater than 5*. **Pi Mu Epsilon Journal.** Vol. 10 (Spring, 1995) pp 96–98.
Snapp, Bart and Chris Snapp. *Automotive Number Theory*. **Math Horizons**. (Sept. 2009): 26–27. also at www.maa.org/mathhorizons

6.6.3   Review Exercises

Exercises 1–7. How many incongruent solutions does the congruence have?
  1. $20x \equiv 4 \bmod 30$
  2. $20x \equiv 30 \bmod 4$
  3. $353x \equiv 254 \bmod 4$
  4. $57x \equiv 76 \bmod 95$
  5. $64x \equiv 83 \bmod 106$
  6. $57x \equiv 87 \bmod 405$
  7. $49x \equiv 5000 \bmod 999$

  8. For each of the problems in #1 that has solutions, find the solutions.
  9. If a and b are integers of the form $7k+1$, is ab expressible in the same form? Prove your answer. (Hint: If $a = 7k+1$ and $b = 7m+1$, does $ab = 7x+1$ for an $x \in \mathbb{Z}$?)
 10. Find all solutions of the congruence: $15x \equiv 3 \bmod 16$.
 11. Find all solutions of the congruence $11x \equiv 9 \bmod 16$.
 12. How many incongruent solutions does the congruence $9x \equiv 27 \bmod 54$ have? Find them.
 13. The first 11 digits of a Universal Product Code (UPC) for a carton of frozen sweet potatoes are 31233100597. Find the 12th digit (the check digit).
 14. Prove that if $a \equiv b \bmod m$ and c is an integer, then $ac \equiv bc \bmod m$.
 15. Prove that if $a \equiv b \bmod m$ and c is an integer, then $a+c \equiv b+c \bmod m$.
 16. Prove that if a is an odd integer, then $a^2 \equiv 1 \bmod 8$.
 17. Solve the system of congruences. Find the least residue of the solution.

$$x \equiv 4 \bmod 7$$
$$x \equiv 5 \bmod 8$$

18. When I wrote down the UPC code from the book "Mathematics and Common Sense" I think that I may have switched two digits in the code 7851688127009. Did I make this mistake? Explain your answer.

19. I can read all but one digit of the UPC code on my one-pound box of Domino Dark Brown Sugar. They are 0 4 9 2 0 0 0 5 x 0 0 4, where x represents the digit I cannot read. What is the missing digit?

20. A UPC for a product is 0 51000 02526 5
    Explain why the errors in the following misread versions of this UPC would not be detected as errors:
        0 51000 02625 5
        0 50000 05526 5

Exercises 21–28. Compute the least residue of the expression in the given modulus.

21. $7^3 + 5^2$ *modulo* 8
22. $36(6) - 2(15)$ *modulo* 25
23. $43 - 5(9)$ *modulo* 31
24. $21^2 - 11$ *modulo* 20
25. $9 + 18 + 27 + 36$ *modulo* 9
26. $33^2 \cdot 35^2$ *modulo* 31
27. 12^{35} *modulo* 29
28. 58^{49} *modulo* 19

6.6.4   Activities

Activity 1: Modular Arithmetic Quilts
Tables for modular arithmetic have many uses. They provide us with a way to visualize addition and multiplication of least residues modulo m. For example, $(4 + 3) \equiv 2 \bmod 5$, so in the table go down to "4" and over to "3" and the sum "2" is shown. The same type of table can be constructed for multiplication. Table 6.1 shows addition, and Table 6.2 shows multiplication of least residues modulo 5.

Notice that multiplication by zero always results in zero, so this least residue is often omitted from the multiplication table.

We will use these arithmetic tables to illustrate a method of designing a quilt. Here are instructions for the addition table.

1. Using the table for addition modulo 5, replace each number with a symbol. For example, replace "0" with polka dots, "1" with horizontal stripes, "2" with vertical stripes, "3" with diagonal lines upper left to lower right, and four

Table 6.1 Addition of least residues modulo 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Table 6.2 Multiplication of least residues modulo 5

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

with diagonal lines from upper right to lower left. You will have an interesting pattern.

2. More creative designs can be found. You can use any pattern you would like and choose completely different patterns or choose one and rotate it into different positions. For this example, two squares were cut from this photograph of Mt. McKinley, and then rotated to make 5 different figures.

Here is the original photo of Mount McKinley, taken by Agnes M. Rash.
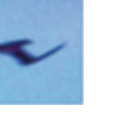
The squares cut out of the photograph are the bird and part of the mountain, shown here.
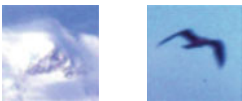
To make the five different figures used to represent the five least residues modulo 5, the bird was rotated. Here is how the figures were matched up with the least residues. (There is no method for doing this; different assignments will just make different patterns.)

0	1	2	3	4

3. This pattern comes from substituting the figures into the addition table modulo 5. Notice the different patterns in the table, forming addition modulo 5 quilt.

Form your own patterns and create a modulo 5 picture table or quilt using your own design. (For example, try the six sides of a die as your patterns with a modulo 7 addition or multiplication table).

4. Here are some suggestions that you can try to create new designs. Try to pay attention to how the designs change with each of these options.

   a. Use a multiplication table instead of addition
   b. Use a different prime number for the modulus.
   c. Use a composite modulus.

Activity 2. Modular Sudoku
In Modular Sudoku, the numbers in each row/column are congruent to the integers 1 through 9 mod 10. In this version of Sudoku, find the least residue mod 10 and then continue as for a regular Sudoku puzzle. Solve the Modular Sudoku puzzle given here. Then see if you can make up one of your own.

	15		27	49				44
	11	54	55	22	33	8		
	77	2	11	78	54	55	23	
								89
				25	29	57		12
22	19			67		66	18	33
14	12		23			49		65
	28	39		16	57			
		66			45			98

This game can be combined with Multi-Sudoku. For example, use large numbers and reduce those mod 100, resulting in two digit numbers and then find the greatest common divisor and proceed as above.

Chapter 7
Numerical Functions and Special Congruences

If only I had the theorems! Then I should find the proofs easily enough.

—Bernard Riemann, 1826–1866

7.1 Introduction

In this chapter the topic of congruences is expanded to look at three particularly useful theorems on congruences, named after the people who introduced them. The first, Wilson's Theorem, was originally stated by John Wilson, but the first published proof was by another mathematician, Joseph Lagrange. The second, Fermat's Little Theorem, was stated by Pierre de Fermat, although it was first proved by Leonhard Euler. The third congruence, known as Euler's Theorem, was actually stated and proved by Euler himself. Wilson's Theorem is about factorials. Fermat's Little Theorem and Euler's Theorem both provide methods of finding powers of integers that will have a least residue of one in a particular modulus. Both Fermat's Little Theorem and Wilson's Theorem require that the modulus is prime, but Euler was able to generalize Fermat's Little Theorem so that a prime modulus is not required.

In addition to these congruences, we will introduce some examples of how functions are defined and used in number theory, because one of these functions, called the Euler ϕ-function (read "Euler phi function"), is part of the congruence Euler discovered. Finally, some applications of these congruences are included. For example, they can sometimes be used as an alternate method to solve linear congruences. In Chap. 8, Euler's Theorem is used to develop a secure code.

7.2   Wilson's Theorem

John Wilson discovered a theorem involving factorials in congruences. Remember that the factorial of an integer n, written $n!$, is the product of n and all positive integers less than n. So $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ and $8! = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$. Now, what happens to factorials in a congruence? If we choose a modulus, say $m = 6$, then $6!$, $7!$, and any larger factorial will all be congruent to 0 modulo 6, since each of these factorials will contain a factor of 6. This means that the largest factorial modulo m that is not always zero is $(m - 1)!$. The next two examples are of congruences with factorials. See if you notice any similarities or differences between them.

Example 7.1 For each value of m, find the least residue of $(m - 1)!$ modulo m.
(a) $m = 4$ (b) $m = 8$ (c) $m = 9$

Solution
(a) $m = 4$
      $(4 - 1)! \equiv 3! \equiv 6 \equiv 2 \, mod \, 4$
(b) $m = 8$
      $(8 - 1)! \equiv 7! \equiv 0 \, mod \, 8$
(c) $m = 9$
      $(9 - 1)! \equiv 8! \equiv 0 \, mod \, 9$

◈

Example 7.2 For each value of m, find the least residue of $(m - 1)!$ modulo m.
(a) $m = 3$ (b) $m = 5$ (c) $m = 11$

Solution
(a) $m = 3$
      $(3 - 1)! \equiv 2 \, mod \, 3$
(b) $m = 5$
      $(5 - 1)! \equiv 4! \equiv 24 \equiv 4 \, mod \, 5$
(c) $m = 11$
      $(11 - 1)! \equiv 10! \, mod \, 11$
      $$\equiv (10 \cdot 9) \cdot (8 \cdot 7) \cdot (6 \cdot 5) \cdot (4 \cdot 3) \cdot (2 \cdot 1) \, mod \, 11$$
      $$\equiv 2 \cdot 1 \cdot 8 \cdot 2 \, mod \, 11$$
      $$\equiv 10 \, mod \, 11$$

◈

In Example 7.1, the three values chosen for m are composite, but in Example 7.2, the choices for m are prime. Notice the difference in the results. In the examples when the modulus m is composite, $(m - 1)!$ reduces to 0, except in the case when $m = 4$. In fact, if m is a composite integer other than 4, $(m - 1)!$ will always be congruent to 0 modulo m. (Can you see why?) The proof of this fact is left as Exercise 17.

However, when m is prime, as in Example 7.2, there is a different pattern. In each case, $(m-1)!$ is congruent to $(m-1)$ modulo m. This is the relationship that Wilson noticed. This conjecture can be stated more formally as follows:

Conjecture 7.1:   If p is prime, then $(p-1)! \equiv p-1 \bmod p$.

This conjecture turns out to be true, and it is known as Wilson's Theorem, although it is often written in a slightly different form. Remember that when adding and subtracting in a congruence, integers can be replaced with other integers congruent in the modulus. Since $p \equiv 0 \bmod p$, subtracting 1 from each side shows that $p-1 \equiv 0-1 \equiv -1 \bmod p$. Therefore, the congruence in the conjecture can be rewritten as $(p-1)! \equiv -1 \bmod p$. This is the congruence known as Wilson's Theorem.

Theorem 7.1 Wilson's Theorem
If p is prime, then $(p-1)! \equiv -1 \bmod p$.

Before proving Wilson's Theorem, here is another example. Suppose that $p=7$. Then, by Wilson's Theorem, $6! \equiv -1 \bmod 7$. Writing out the terms of 6! in the congruence,

$$6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \equiv -1 \bmod 7.$$

From Theorem 6.10, each of 6, 5, 4, 3, 2, and 1 have an inverse modulo 7, since all are relatively prime to 7. Also, notice that 6 and 1 are each their own inverse since $1^2 \equiv 1 \bmod 7$ and $6^2 \equiv 36 \equiv 1 \bmod 7$. Therefore, since there are four terms left, we should be able to match them up as inverses of each other. We see that $5 \cdot 3 \equiv 1 \bmod 7$ and $2 \cdot 4 \equiv 1 \bmod 7$. Therefore, rearranging the terms of 6!, to put inverses next to each other,

$$\begin{aligned} 6 \cdot (5 \cdot 3) \cdot (4 \cdot 2) \cdot 1 &\equiv 6 \bmod 7 \\ &\equiv (6-7) \bmod 7 \\ &\equiv -1 \bmod 7 \end{aligned}$$

Notice that 6 is its own inverse modulo 7 because $6 \cdot 6 \equiv 36 \equiv 1 \bmod 7$. In fact, for any modulus m, the value $m-1$ is always its own inverse modulo m. This fact is stated in Lemma 7.1.

Lemma 7.1
If $m > 0$, then $m-1$ is its own inverse modulo m. In other words, $(m-1)^2 \equiv 1 \bmod m$.

Proof. Let m be a positive integer. Then to show that $m - 1$ is its own inverse modulo m, show that the congruence $(m - 1)^2 \equiv 1 \ mod \ m$ is true. Starting on the left side,

$$(m - 1)^2 \equiv m^2 - 2m + 1 \ mod \ m$$
$$\equiv 0 - 0 + 1 \ mod \ m$$
$$\equiv 1 \ mod \ m$$

Therefore, $(m - 1)$ is its own inverse modulo m.

■

If a congruence has a prime modulus, p, we can say more: not only is $p - 1$ its own inverse modulo p, but any integer that is its own inverse must be congruent to either 1 or $p - 1$ modulo p.

Lemma 7.2
If p is prime, then b is its own inverse modulo p if and only if $b \equiv 1 \ mod \ p$ or $b \equiv p - 1 \ mod \ p$.

Proof. ($\Rightarrow$) *Show that if p is prime and b is its own inverse modulo p, then $b \equiv 1 \ mod \ p$ or $b \equiv p - 1 \ mod \ p$.*

Let p be prime and suppose b is its own inverse modulo p. From the definition of inverse, this means that $b^2 \equiv 1 \ mod \ p$. Subtracting 1 from both sides of this congruence, $b^2 - 1 \equiv 0 \ mod \ p$. Factoring the left side of the congruence, $(b - 1)(b + 1) \equiv 0 \ mod \ p$. From the definition of congruence, $p|(b - 1)(b + 1)$. Now by Euclid's Lemma (Theorem 5.3) either $p|(b - 1)$ or $p|(b + 1)$. If $p|(b - 1)$, then by the definition of congruence, $b \equiv 1 \ mod \ p$. If $p|(b + 1)$, then $b \equiv -1 \ mod \ p$, and since $p \equiv 0 \ mod \ p$, we have that $b \equiv p - 1 \ mod \ p$.

Therefore, in a prime modulus, if b is its own inverse, then $b \equiv 1 \ mod \ p$ or $b \equiv p - 1 \ mod \ p$.

($\Leftarrow$) *Show that if $b \equiv 1 \ mod \ p$ or $b \equiv p - 1 \ mod \ p$, then b is its own inverse modulo p.*

If $b \equiv 1 \ mod \ p$, then $b^2 \equiv 1^2 \equiv 1 \ mod \ p$, and b is its own inverse.

If $b \equiv p - 1 \ mod \ p$, then Lemma 7.1 shows that b is its own inverse modulo p.

■

Here is one more example to illustrate why Wilson's Theorem works.

Example 7.3 Verify Wilson's Theorem for $p = 11$.

Solution
For $p = 11$, Wilson's Theorem states that $(11 - 1)! \equiv -1 \ mod \ 11$. Applying the definition of congruence, this says that $11|(10! + 1)$. By Lemma 7.2, only 1 and

10 are their own inverse modulo 11, so each of the other terms in 10! can be matched up with its inverse:

$$\begin{aligned} 10! &= 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \\ &\equiv 10 \cdot (9 \cdot 5) \cdot (8 \cdot 7) \cdot (6 \cdot 2) \cdot (4 \cdot 3) \cdot 1 \; mod \; 11 \\ &\equiv 10 \; mod \; 11 \end{aligned}$$

Therefore, $10! + 1 \equiv 10 + 1 \equiv 0 \; mod \; 11$, which shows that $11 | (10! + 1)$, or $(11 - 1)! \equiv - 1 \; mod \; 11$.

◈

Now we are ready for the proof of Wilson's Theorem.

Proof of Wilson's Theorem. Let p be a prime integer. We will show that $(p - 1)! \equiv - 1 \; mod \; p$. Writing out the terms in the factorial,

$$(p - 1)! = (p - 1)(p - 2) \cdots 3 \cdot 2 \cdot 1$$

Now, p does not share any common factors with the integers in this product since each one is less than p, and p is prime. Therefore, by Theorem 6.10, each integer in the product has an inverse modulo p.

By Lemma 7.2, only $(p - 1)$ and 1 are their own inverses. Therefore, each of the remaining terms can be paired with its inverse, so that their product is 1 modulo p. Therefore, all of the terms result in a 1 in the product, except for $(p - 1)$. Then,

$$\begin{aligned} (p - 1)! &\equiv (p - 1) \cdot (p - 2) \cdots 3 \cdot 2 \cdot 1 \; mod \; p \\ &\equiv (p - 1) \cdot 1 \cdot 1 \cdot \; \cdots \; \cdot 1 \equiv p - 1 \; mod \; p \end{aligned}$$

Finally, since $p \equiv 0 \; mod \; p$

$$(p - 1)! \equiv -1 \; mod \; p$$

■

The next example illustrates the use of Wilson's Theorem.

Example 7.4 Find the least residue of each of the following expressions in the given modulus.

(a) $12! \; mod \; 13$
(b) $6! \; mod \; 7$
(c) $8! \; mod \; 7$
(d) $9! \; mod \; 11$

Solution

(a) According to Wilson's Theorem (with $p = 13$), $12! \equiv -1 \bmod 13$. To find the least residue of -1, add 13 to -1 to get $12! \equiv 12 \bmod 13$.

(b) Applying Wilson's Theorem with $p = 7$ gives $6! \equiv -1 \bmod 7 \equiv 6 \bmod 7$.

(c) Since $8! \equiv 8 \cdot 7 \cdot 6 \cdots 2 \cdot 1$ contains a factor of 7, $8! \equiv 0 \bmod 7$. Notice Wilson's Theorem is not useful here.

(d) This looks similar to the form of the congruence in Wilson's Theorem, and the modulus 11 is prime, but notice that $9 = 11 - 2$, rather than $11 - 1$ as given in the theorem. Let us see if Wilson's Theorem can still be used to help solve the problem.

   Applying Wilson's Theorem to $p = 11$ produces the congruence $10! \equiv -1 \bmod 11$. To relate this to the question, rewrite $10!$ in terms of $9!$:

$$10 \cdot 9! \equiv -1 \bmod 11$$

Now, by Lemma 7.1, 10 is its own inverse modulo 11, so $10 \cdot 10 \equiv 1 \bmod 11$. By multiplying both sides of the congruence above by 10 we obtain:

$$10 \cdot 10 \cdot 9! \equiv 10 \cdot -1 \bmod 11$$
$$1 \cdot 9! \equiv -10 \bmod 11$$
$$9! \equiv 1 \bmod 11$$

◆

Example 7.5 What is the remainder when $42!$ is divided by 43?

Solution

This question can be rephrased as, "Find $42!$ modulo 43."

Since 43 is prime, by Wilson's Theorem, $42! \equiv -1 \bmod 43$. Since remainders must be positive, add 43 to the right-hand side to find the least residue of -1:

$$42! \equiv -1 + 43 \bmod 43$$
$$42! \equiv 42 \bmod 43$$

Therefore, the remainder when $42!$ is divided by 43 is 42.

◆

Theorem 7.2 provides another true congruence using factorials.

Theorem 7.2
If p is prime, then $(p - 2)! \equiv 1 \bmod p$.

The proof of Theorem 7.2 is left as Exercise 13.

Exercise Set 7.2

1. Verify that Wilson's Theorem is true for $p = 5$.
2. Verify that Wilson's Theorem is true for $p = 13$.
3. Write an equation that relates $p!$ and $(p - 1)!$.
4. Write an equation that relates $(p - 1)!$ and $(p - 3)!$.
5. Find the least residue of each expression in the given modulus without a calculator. Show your work.

   (a) $12! \equiv$ _____ $mod\ 13$
   (b) $13! \equiv$ _____ $mod\ 11$
   (c) $3! \equiv$ _____ $mod\ 5$
   (d) $7! \equiv$ _____ $mod\ 8$

6. Find the least residue of each expression in the given modulus without a calculator. Show your work.

   (e) $17! \equiv$ _____ $mod\ 18$
   (f) $11! \equiv$ _____ $mod\ 13$
   (g) $6! \equiv$ _____ $mod\ 5$
   (h) $30! \equiv$ _____ $mod\ 31$

7. What is the remainder when $22!$ is divided by 23?
8. What is the remainder when $42!$ is divided by 41?
9. What is the remainder when $15!$ is divided by 17? (Hint: Exercises 3 and 4 might be helpful.)
10. What is the remainder when $21!$ is divided by 23?
11. What is the remainder when $26!$ is divided by 29? (Hint: Exercises 3 and 4 might be helpful.)
12. (a) Show that the following statement is false:

    If m is a positive integer and b is its own inverse modulo m, then $b \equiv 1\ mod\ m$ or $b \equiv m - 1\ mod\ m$.

    (b) Explain how part (a) relates to Lemma 7.2.

13. Prove **Theorem 7.2**. (Hint: $(p - 1)! = (p - 1)(p - 2)!$.)
14. Prove that if $p > 2$ is prime, then $2(p - 2)! \equiv -1\ mod\ p$.
15. (a) Prove that if $m > 0$, then $(m - 1) \equiv -1\ mod\ m$.
    (b) Use the result from part (a) to find the least residue of 40^{82} modulo 41.
    (c) Use the results from part (a) to find the least residue of 42^{101} modulo 43.

16. Prove that if $m > 0$, then $(m - 2) \equiv -2\ mod\ m$.
17. Prove that if m is composite and $m > 4$, then $(m - 1)! \equiv 0\ mod\ m$.

18. (a) State the converse of **Wilson's Theorem**.
    (b) Prove that if $a|b$ and $b|c$, then $a|c$.
    (c) Prove that if $a|b$ and $a|c$, then $a|(b-c)$.
    (d) Prove that the converse of Wilson's Theorem is true. (Hint: the results from parts (b) and (c) may be helpful.)

7.3   Fermat's Little Theorem

In Section 6.2, we learned that arithmetic can be simplified in any modulus, by first reducing the numbers involved to their least residue. In particular, Example 6.14 asked for the least residue of 2^{50} *mod* 15. In this case, the fact that $2^4 \equiv 1$ *mod* 15 allowed us to show that $2^{50} \equiv 4$ *mod* 15. However, numbers are not always this convenient. In some cases it may be more difficult to find an exponent that makes an expression reduce to 1, and in other cases there may not be any exponent that will make the expression reduce to 1.

For example, calculating powers of 9 modulo 15 produces the following pattern:

$$9 \equiv 9 \bmod 15,$$
$$9^2 \equiv 6 \bmod 15,$$
$$9^3 \equiv 9 \bmod 15, \ldots,$$

This pattern continues, and there is no exponent that makes the expression reduce to 1. In other cases, it may just be more difficult than in Example 6.14 to find an exponent that makes an expression reduce to 1. Fermat's Little Theorem gives an example of when an integer raised to a power has a least residue of 1, with a prime modulus.

Theorem 7.3 Fermat's Little Theorem
If p is a prime number, and a is an integer such that $p \nmid a$, then

$$a^{p-1} \equiv 1 \bmod p$$

Notice that there are two conditions that must be met to apply Fermat's Little Theorem. First, the modulus must be prime. The second condition states that p does not divide a. Since p is prime, this means that a and p have no factors in common, so another way to think of this is that a and p must be relatively prime.

Proof. Let p be prime and let $a \in \mathbb{Z}$ such that $p \nmid a$. Now, consider the list of integers:

$$1 \cdot a, \ 2 \cdot a, \ 3 \cdot a, \ldots, (p-1) \cdot a$$

We will show that this list has the following properties.

1. None of the integers on this list are divisible by p, which means that none are congruent to zero modulo p.
2. None of the integers on this list are congruent to each other modulo p.

We will use a proof by contradiction to show that each of these statements is true.

For the first statement, suppose that $p | m \cdot a$ where $m \cdot a$ is one of the integers listed above. By Euclid's Lemma (Theorem 5.3), either $p|m$ or $p|a$. Since $p \nmid a$ was a premise, it must be true that $p|m$. But this is also impossible since m is less than p. Therefore, $p \nmid m \cdot a$, which means p does not divide any of the integers on the list.

To prove the second statement, suppose that $k \cdot a \equiv m \cdot a \ mod \ p$ for different integers k and m. Then from the definition of congruence, $p|(ka - ma)$ which can be rewritten as $p|a(k-m)$. By Euclid's Lemma, since $p \nmid a$, it must be true that $p|(k-m)$. Applying the definition of congruence tells us that $k \equiv m \ mod \ p$. This is impossible since k and m were chosen to be distinct integers less than p. Therefore, no integers on this list are congruent to each other modulo p.

These two facts show that $1 \cdot a, \ 2 \cdot a, \ 3 \cdot a, \ldots, (p-1) \cdot a$ is a list of $p-1$ integers, none of which are congruent to zero or congruent to each other modulo p. Therefore, they will each have a different least residue, and the least residues of the numbers on the list must be $1, 2, 3, \ldots, (p-1)$. Therefore,

$$(1 \cdot a)(2 \cdot a)(3 \cdot a) \cdots ((p-1) \cdot a) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \ mod \ p$$

Regrouping the terms produces

$$(p-1)! \cdot a^{p-1} \equiv (p-1)! \ mod \ p$$

Applying Wilson's Theorem and simplifying, we obtain the following.

$$-1 \cdot a^{p-1} \equiv -1 \ mod \ p$$
$$a^{p-1} \equiv 1 \ mod \ p$$

This proves that the congruence in Fermat's Little Theorem is true when p is prime and $p \nmid a$.

∎

Example 7.6 For each pair of integers a and p given below, determine whether or not Fermat's Little Theorem can be used. If so, verify that the congruence given in the theorem is true. If not, explain why Fermat's Little Theorem does not apply.

(a) $a = 5, p = 11$
(b) $a = 14, p = 9$
(c) $a = 22, p = 3$

Solution
(a) Fermat's Little Theorem applies to this example: 11 is prime, and 5 is not divisible by 11. Therefore, according to the theorem,

$$5^{(11-1)} \equiv 1 \bmod 11$$
$$5^{10} \equiv 1 \bmod 11$$

To verify that this congruence is true, apply the definition of congruence:

$$11 \mid \left(5^{10-1}\right)$$
$$11 \mid (9765625 - 1)$$
$$11 \mid 9765624$$

which is true since $11 \cdot 887784 = 9765624$.

(b) Fermat's Little Theorem does not apply to this case, because even though 9 does not divide 14, 9 is not prime.
(c) Fermat's Little Theorem applies to this case since 3 is prime, and $3 \nmid 22$. Then, according to Fermat's Little Theorem, $22^2 \equiv 1 \bmod 3$.

To verify this, confirm that $3 \mid (22^2 - 1)$, or $3 \mid 483$. Alternatively, $22 \equiv 1 \bmod 3$, so this also shows $22^2 \equiv 1 \bmod 3$.

◈

Example 7.7 Use Fermat's Little Theorem to find the remainder when 4^{185} is divided by 7.

Solution
The exponent here is large enough that you probably would not have much luck using a calculator. Fermat's Little Theorem can help!

First, write the question as a congruence to relate it to Fermat's Little Theorem. Asking for the remainder when dividing by 7 is the same as asking for the least residue of 4^{185} modulo 7. Since 7 is prime and 7 does not divide 4, Fermat's Little Theorem tells us that $4^6 \equiv 1 \bmod 7$.

Now, $185 = 6 \cdot 30 + 5$, so $4^{185} = 4^{6 \cdot 30 + 5} = (4^{6 \cdot 30}) \cdot (4^5) = (4^6)^{30} \cdot (4^5)$.

Then, using the congruence from Fermat's Little Theorem,

$$
\begin{aligned}
4^{185} &\equiv \left(4^6\right)^{30} \cdot \left(4^5\right) \bmod 7 \\
&\equiv (1)^{30} \cdot \left(4^5\right) \bmod 7 \\
&\equiv 4^5 \bmod 7 \\
&\equiv 4^2 \cdot 4^3 \bmod 7 \\
&\equiv 16 \cdot 64 \bmod 7 \\
&\equiv 2 \cdot 1 \bmod 7 \\
&\equiv 2 \bmod 7
\end{aligned}
$$

Therefore, 2 is the remainder when 4^{185} is divided by 7.

◈

Another way Fermat's Little Theorem can be used is to solve linear congruences. In Chap. 6, we developed a method to solve linear congruences of the form $ax \equiv b \ mod \ m$, based on the linear equations of two variables studied in Chap. 5. If the congruence satisfies the conditions of Fermat's Little Theorem—that the modulus m is prime and $m \nmid a$, then Fermat's Little Theorem provides an alternate solution technique.

Example 7.8 Use Fermat's Little Theorem to find a solution of $2x \equiv 3 \ mod \ 5$.

Solution
Since 5 is prime, and 5 does not divide 2, the conditions of Fermat's Little Theorem are met. Therefore, $2^4 \equiv 1 \ mod \ 5$. In order to use this fact, multiply both sides of the original congruence by 2^3.

$$\begin{aligned} 2^3 \cdot 2x &\equiv 2^3 \cdot 3 \ mod \ 5 \\ 2^4 \cdot x &\equiv 8 \cdot 3 \ mod \ 5 \\ 1 \cdot x &\equiv 4 \ mod \ 5 \\ x &\equiv 4 \ mod \ 5 \end{aligned}$$

Therefore, any integer congruent to 4 modulo 5 is a solution to the given congruence.

◈

Example 7.9 For each congruence, find the least residue of a solution using Fermat's Little Theorem, if possible. If Fermat's Little Theorem cannot be used, explain why not.

(a) $4x \equiv 5 \ mod \ 7$
(b) $8x \equiv 9 \ mod \ 13$
(c) $5x \equiv 2 \ mod \ 6$

Solution
(a) $4x \equiv 5 \ mod \ 7$

Since 7 is prime, and 7 does not divide 4, apply Fermat's Little Theorem to obtain the congruence $4^6 \equiv 1 \ mod \ 7$. Therefore, to get x by itself in the congruence, multiply both sides by 4^5.

$$\begin{aligned} \left(4^5 \cdot 4\right)x &\equiv 4^5 \cdot 5 \ mod \ 7 \\ 4^6 \cdot x &\equiv 4^5 \cdot 5 \ mod \ 7 \\ 1 \cdot x &\equiv \left(4^2\right)^2 \cdot 4 \cdot 5 \ mod \ 7 \\ x &\equiv (16)^2 \cdot 20 \ mod \ 7 \\ x &\equiv 2^2 \cdot 6 \ mod \ 7 \\ x &= 24 \ mod \ 7 \\ x &\equiv 3 \ mod \ 7 \end{aligned}$$

(b) $8x \equiv 9 \bmod 13$

Since 13 is prime and 13 does not divide 8, apply Fermat's Little Theorem to obtain $8^{12} \equiv 1 \bmod 13$. Therefore, to get x by itself in the congruence, we can multiply both sides of the congruence by 8^{11}.

$$8^{11} \cdot 8x \equiv 8^{11} \cdot 9 \bmod 13$$
$$8^{12}x \equiv 8^{11} \cdot 9 \bmod 13$$
$$x \equiv 8^{11} \cdot 9 \bmod 13$$

So far, so good. This is a solution for x, but to find the least residue modulo 13, we must reduce 8^{11}. Fermat's Little Theorem can help again. Rewrite $8^{12} \equiv 1 \bmod 13$ as $8 \cdot 8^{11} \equiv 1 \bmod 13$. Now, to cancel the 8 on the left-hand side, multiply both sides by the inverse of 8 modulo 13. Since $5 \cdot 8 \equiv 40 \bmod 13 \equiv 1 \bmod 13$, we multiply both sides by 5.

$$(5 \cdot 8) \cdot 8^{11} \equiv 5 \cdot 1 \bmod 13$$
$$1 \cdot 8^{11} \equiv 5 \bmod 13$$

Putting this back into the congruence for x,

$$x \equiv 8^{11} \cdot 9 \bmod 13$$
$$\equiv 5 \cdot 9 \bmod 13$$
$$x \equiv 6 \bmod 13$$

From this example, you can see that while Fermat's Little Theorem is a faster method of finding a solution to a congruence when the prime modulus is relatively small, the work to find the least residue of the solution generally increases as the size of the modulus increases.

(c) $5x \equiv 2 \bmod 6$

Fermat's Little Theorem cannot be used to solve this congruence, since the modulus, 6, is not prime. Note that this does not mean there is no solution; only that we cannot find a solution by applying Fermat's Little Theorem. In fact, you can check that if $x \equiv 4 \bmod 6$, then x is a solution to the congruence.

◈

Exercise Set 7.3

1. For each pair of integers a and p, determine whether or not **Fermat's Little Theorem** can be used. If so, verify that the congruence given in the Theorem is true. If not, explain why not.

   (a) $a = 12,\ p = 5$
   (b) $a = 6,\ p = 7$

(c) $a = 4$, $p = 15$
(d) $a = 42$, $p = 3$

2. For each pair of integers a and p, determine whether or not **Fermat's Little Theorem** can be used. If so, verify that the congruence given in the theorem is true. If not, explain why not.

   (a) $a = 8$, $p = 13$
   (b) $a = 12$, $p = 33$
   (c) $a = 21$, $p = 7$
   (d) $a = 9$, $p = 5$

3. Find the remainder when 5^{204} is divided by 11.
4. Find the least residue of 2^{5000} modulo 13.
5. For each of the congruences below, first determine whether the congruence has a solution. If so, find the solution using **Fermat's Little Theorem** whenever possible. (If it is not possible, explain why not.)

   (a) $3x \equiv 10 \ mod \ 11$
   (b) $5x \equiv 2 \ mod \ 9$
   (c) $4x \equiv 3 \ mod \ 7$
   (d) $6x \equiv 8 \ mod \ 17$

7.4   A Numerical Function: Euler's Phi Function

One of the main topics studied in high school algebra is functions. For example, you may recall that functions like $f(x) = x^2$, $g(x) = 2x^2 - 6x + 4$, and $h(x) = -x^2 - 6$ all have a similar shape (called a parabola). One important property of functions is their *domain*. The *domain* of a function is the collection of numbers for which the function is defined. Many of the functions used in algebra have the entire collection of real numbers as their domain. For example, all the equations given above are defined for any real number.

Functions are also used in number theory. Just as in algebra, functions in number theory have a domain. However, since number theory is restricted to working in the integers, the domain of a function in number theory will only include integers. In fact, we are most interested in functions whose domains are the positive integers. These functions whose domains are the positive integers are sometimes called *numerical functions*, *number theoretic functions*, or *arithmetic functions*.[1]

Numerical functions are often defined by counting something. In this section, the "Euler phi function" is introduced. In the next section, we will look at two more

---

[1] Note that in this context, "arithmetic" is an adjective describing the function and not a noun describing the math you learned in elementary school. The pronunciation is also different: ar-ith-**met**-ik instead of the noun *uh*-**rith**-m*uh*-tik.

examples of numerical functions: the "number of positive divisors function" and the "sum of positive divisors function."

The "Euler phi function" is named after the mathematician Leonhard Euler. The notation for the Euler phi function is $\phi(n)$, where ϕ is the lowercase Greek letter "phi." The domain of $\phi(n)$ is the positive integers, and if n is a positive integer, then $\phi(n)$ is defined to be the number of positive integers less than or equal to n that are relatively prime to n. In other words, $\phi(n)$ counts the number of integers, k, less than or equal to n such that $\gcd(n, k) = 1$.

Definition 7.1: Euler phi function, $\phi(n)$
For an integer $n > 0$,

$$\phi(n) = \text{the number of positive integers } k \le n \text{ such that } \gcd(k, n) = 1.$$

Example 7.10 Find the value of $\phi(n)$ for each value of n.
(a) $\phi(4)$ (b) $\phi(7)$ (c) $\phi(10)$

Solution
(a) $\phi(4)$

The positive integers less than or equal to 4 are 1, 2, 3, and 4. Since 2 and 4 both share a common factor with 4, only 1 and 3 are relatively prime to 4. Therefore, $\phi(4) = 2$.

(b) $\phi(7)$

The positive integers less than or equal to 7 are 1, 2, 3, 4, 5, 6, and 7. All of these are relatively prime to 7 except for 7 itself. Therefore, $\phi(7) = 6$.

(c) $\phi(10)$

The positive integers less than or equal to 10 that are also relatively prime to 10 are 1, 3, 7, and 9. Therefore, $\phi(10) = 4$.

◈

Example 7.11 Find $\phi(40)$ and $\phi(41)$.

Solution
To find $\phi(40)$, count the number of positive integers less than 40 that are relatively prime to 40. Since all evens will share a divisor of 2 with 40, only the odd integers less than 40 have a possibility of being relatively prime to 40. If an odd integer is not relatively prime to 40, it can only share a common divisor of 5. So the integers less than 40 and relatively prime to 40 are 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, and 39. Therefore, $\phi(40) = 16$.

To find $\phi(41)$, notice that 41 is prime, so its only divisors are 1 and 41. Therefore, each integer from 1 through 40 is relatively prime to 41 and $\phi(41) = 40$.

◈

Although the definition of $\phi(n)$ is given in terms of counting, evaluating the function this way for large numbers such as 500 or 1,000 or greater could get very time-consuming. On the other hand, the example of $\phi(41)$ illustrates that the value of $\phi(n)$ is easy to find for certain integers. As another example, 733 is a large number, but it also happens to be prime, so all integers from 1 through 732 are relatively prime to 733. Therefore, $\phi(733) = 732$. This idea is generalized in Theorem 7.4.

Theorem 7.4
If p is prime, then $\phi(p) = p - 1$.

Proof. Let p be a prime number. Then the only divisors of p are 1 and p. Therefore, all positive integers less than p must be relatively prime to p. Therefore, $\phi(p) = p - 1$.

■

We will certainly want to evaluate $\phi(n)$ for values of n that are not prime, so we need to find other patterns in values of $\phi(n)$. Since primes are the building blocks for all of the integers, the formula in Theorem 7.4 may be helpful in finding formulas for the value ϕ at non-prime integers. The next example explores values of ϕ evaluated at a power of a prime.

Example 7.12 Find the value of $\phi(n)$ for each value of n and look for a pattern for ϕ at the power of a prime.
(a) $\phi(2^3)$ (b) $\phi(3^2)$ (c) $\phi(5^2)$ (d) $\phi(3^4)$

Solution
(a) $\phi(2^3)$

The value $\phi(2^3)$ counts the positive integers less than or equal to 8 and relatively prime to 8. The four positive integers less than or equal to 8 which share a common divisor with 8 are 2, 4, 6, and 8, so the rest of the integers less than 8 are relatively prime to 8. Therefore,

$$\phi(2^3) = 8 - 4 = 4$$

(b) $\phi(3^2)$

To find $\phi(3^2)$, count the number of positive integers less than or equal to 9, and relatively prime to 9. The positive integers less than or equal to 9 which do share a common divisor with 9 are 3, 6, and 9. Therefore,

$$\phi(3^2) = 9 - 3 = 6$$

(c) $\phi(5^2)$

Again, count the positive integers less than or equal to 25 that are relatively prime to 25. Notice that as in the examples above, since 25 is a power of a prime, the only

possible divisors other than 1 are powers of that prime: in this case, 5 or 25. This makes it fairly easy to list the numbers less than or equal to 25 that will share a common factor other than 1, because they all must have 5 as a factor: 5, 10, 15, 20, and 25. Note that there are five such integers, and there are 25 integers from 1 to 25, so

$$\phi(5^2) = 25 - 5 = 20$$

(d) $\phi(3^4)$

Let us see if we can calculate the value of $\phi(3^4) = \phi(81)$ without first writing out all the integers that do share a common factor with 81. Since three is prime, the integers that are not relatively prime to 81 must be multiples of 3. The question is, how many multiples of 3 are there between 1 and 81. We can start counting them: $1 \cdot 3, 2 \cdot 3, 3 \cdot 3, \ldots$, and we will stop at $81 = 3^4 = 3^3 \cdot 3$. So, there are 3^3 multiplies of 3 from 1 to 81 which means that the rest of the integers less than 81 are relatively prime to 81. Therefore,

$$\phi(3^4) = 3^4 - 3^3 = 81 - 27 = 54$$

◈

Each of the examples above fits the same pattern which is generalized in Theorem 7.5.

Theorem 7.5
If p is prime and a is a positive integer, then $\phi(p^a) = p^a - p^{a-1}$.

The proof of Theorem 7.5 is left as Exercise 8.

Example 7.13 Evaluate $\phi(64)$ and $\phi(2401)$.

Solution
Since $64 = 2^6$, by Theorem 7.5, $\phi(64) = \phi(2^6)$
$$= 2^6 - 2^5$$
$$= 64 - 32$$
$$= 32$$

In order to use Theorem 7.5 to find $\phi(2401)$, we need to know if 2401 is a power of a prime. Checking for prime divisors shows that $2401 = 7^4$. Therefore, by Theorem 7.5,

$$\phi(2401) = \phi(7^4)$$
$$= 7^4 - 7^3$$
$$= 2401 - 343$$
$$= 2058$$

◈

The next step is to determine what happens to the Euler phi function $\phi(n)$, when $n = p \cdot q$, with p and q two different primes. In the following example, we will try to establish a pattern.

Example 7.14 Find the value of $\phi(n)$ look for a pattern for ϕ at the product of two different primes.

(a) $\phi(6)$ (b) $\phi(10)$ (c) $\phi(15)$ (d) $\phi(21)$

Solution

(a) $\phi(6)$

The integers less than 6 and relatively prime to 6 are 1 and 5. Therefore, $\phi(6) = 2$. Also, notice that $6 = 2 \cdot 3$, $\phi(2) = 1$, and $\phi(3) = 2$, so $\phi(2) \cdot \phi(3) = \phi(6)$.

(b) $\phi(10)$

From Example 7.10 part c), $\phi(10) = 4$. Also, notice that $10 = 2 \cdot 5$, $\phi(2) = 1$, and $\phi(5) = 4$, so $\phi(2) \cdot \phi(5) = \phi(10)$.

(c) $\phi(15)$

The integers less than 15 and relatively prime to 15 are 1, 2, 4, 7, 8, 11, 13, and 14. Therefore, $\phi(15) = 8$. Also, notice that $15 = 3 \cdot 5$, and when making this list, the numbers left out were all those with a factor of 5 or a factor of 3. Also, $\phi(3) = 2$, and $\phi(5) = 4$, so

$$\phi(3) \cdot \phi(5) = \phi(15)$$

(d) $\phi(21)$

Let us see if we can use the ideas from the previous examples to figure out the value of $\phi(21)$ without writing out all the integers less than 21 that are relatively prime to 21. First, notice $21 = 3 \cdot 7$, so integers that are divisible by 3 or divisible by 7 will share a factor with 21. There are seven multiples of 3 less than or equal to 21: $1 \cdot 3$, $2 \cdot 3$, ..., $7 \cdot 3$. Also, there are three multiples of 7 less than or equal to 21: $1 \cdot 7$, $2 \cdot 7$, and $3 \cdot 7$. In each case, the last multiple is 21, so subtract the seven multiples of 3 less than or equal to 21 and the two multiples of 7 that are less than 21 to get that $\phi(21) = 21 - 7 - 2 = 12$. Again, notice that $\phi(3) = 2$ and $\phi(7) = 6$, so $\phi(3) \cdot \phi(7) = \phi(21)$.

◈

Did you notice a pattern in the example above? The pattern illustrated in Example 7.14 is generalized in Theorem 7.6.

Theorem 7.6
If p and q are two different primes, then
$$\phi(p \cdot q) = \phi(p) \cdot \phi(q) = (p-1)(q-1).$$

Proof. Let p and q be two different primes. To calculate the value of $\phi(p \cdot q)$, we need to count up the number of integers less than or equal to $p \cdot q$ that are relatively prime to $p \cdot q$. In order to do this, consider the number of integers that do share a common factor, and then subtract this number from $p \cdot q$, the total number of integers from 1 to $p \cdot q$.

Since p and q are both prime, an integer with a common factor must be either a multiple of p or a multiple of q. There are p multiples of q less than or equal to $p \cdot q$ which are $1 \cdot q,\ 2 \cdot q,\ 3 \cdot q, \ldots, p \cdot q$. Similarly there are q multiples of p less than or equal to $p \cdot q$ which are $1 \cdot p,\ 2 \cdot p,\ 3 \cdot p, \ldots, q \cdot p$. Therefore, the total number of integers less than or equal to $p \cdot q$ that do share a common factor with $p \cdot q$ is $q + (p-1)$. (Note that we subtract 1 from p so that $p \cdot q$ will not be counted twice.) Therefore,

$$\begin{aligned}
\phi(p \cdot q) &= p \cdot q - (q + (p-1)) \\
&= p \cdot q - q - p + 1 \\
&= (p-1)(q-1) \\
&= \phi(p) \cdot \phi(q)
\end{aligned}$$

∎

From here, you might wonder if Theorem 7.6 can be generalized from a product of primes to a product of any two integers. Unfortunately, the answer is NO. Example 7.15 illustrates a counterexample.

Example 7.15 Show that the following statement is false: If m and n are positive integers, then $\phi(mn) = \phi(m) \cdot \phi(n)$.

Solution
To show this statement is false, we need a counterexample. Suppose that $m = 2$ and $n = 10$, so $m \cdot n = 20$. Counting up the positive integers less than 20 and relatively prime to 20 shows that $\phi(20) = 8$. However, $\phi(2) = 1$ and $\phi(10) = 4$. Therefore, $\phi(20) \neq \phi(2) \cdot \phi(10)$.

◈

Although Theorem 7.6 does not generalize to the product of any two integers, there is a general formula for $\phi(n)$, based on the prime factorization of n. That formula is given in Theorem 7.7.

Theorem 7.7

If $n = p_1^{n_1} \cdot p_2^{n_2} \cdots \cdot p_k^{n_k}$ is the prime power factorization of n, then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

The proof of this theorem is beyond the scope of this course, but we can apply it to some more examples.

Note that if p_i represents one of the prime factors in the prime factorization of n, then since p_i is a divisor of n, the expression for $\phi(n)$ from Theorem 7.7 will always produce an integer:

Example 7.16 Find $\phi(100)$ and $\phi(315)$.

Solution

To use Theorem 7.7, find the prime factorizations of 100 and 315.
  $100 = 2^2 \cdot 5^2$ and $315 = 3^2 \cdot 5 \cdot 7$. Now, applying Theorem 7.7,

$$\phi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 100\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 40 \text{ and}$$

$$\phi(315) = 315\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 315\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)\left(\frac{6}{7}\right) = 3(48) = 144$$

◆

Exercise Set 7.4

1. Find all values of n for which $\phi(n) = 1$.
2. Find $\phi(n)$ for $1 \leq n \leq 12$. Describe any patterns you see in the values of ϕ.
3. Evaluate $\phi(96)$.
4. Evaluate $\phi(100)$.
5. Find a counterexample to show that the following statement is false: If $n < m$ then $\phi(n) < \phi(m)$.
6. Prove that if $n > 2$ is a power of 2, then $\phi(n)$ is an even number. (Hint: $n = 2^a$ where $a > 1$.)
7. Prove that if n is composite with two distinct odd prime factors, then $\phi(n)$ is divisible by 4.
8. Prove **Theorem 7.5**.

7.5 More Numerical Functions

Another numerical function is the ***number of positive divisors function***, $d(n)$. The letter d is used to represent the function, as a reminder that this function counts divisors. Although its name is not catchy, it does describe what this function does. Again, $d(n)$ is defined on the positive integers, and $d(n)$ counts the number of positive divisors of n.

Definition 7.2: number of positive divisors function, d(n)
For an integer $n > 0$,

$$d(n) = \text{the number of positive divisors of } n.$$

Example 7.17 Find the value of $d(n)$.
(a) $d(4)$ (b) $d(7)$ (c) $d(10)$

Solution
(a) $d(4)$

   The positive divisors of 4 are 1, 2, and 4, so $d(4) = 3$.

(b) $d(7)$

   Since 7 is prime, 1 and 7 are the only positive divisors of 7, so $d(7) = 2$.

(c) $d(10)$

   The positive divisors of 10 are 1, 2, 5, and 10, so $d(10) = 4$.

◈

   The last numerical function we will consider in this section is called the ***sum of positive divisors function*** and is written as $\sigma(n)$, using the lowercase Greek letter "sigma," σ, to represent "sum."

Definition 7.3: sum of positive divisors function, $\sigma(n)$
For an integer $n > 0$,

$$\sigma(n) = \text{the sum of the positive divisors of } n.$$

Example 7.18 Find the value of $\sigma(n)$.
(a) $\sigma(4)$ (b) $\sigma(7)$ (c) $\sigma(10)$

Solution
(a) $\sigma(4)$

   Since the positive divisors of 4 are 1, 2, and 4, $\sigma(4) = 1 + 2 + 4 = 7$.

(b) $\sigma(7)$

   Since the positive divisors of 7 are 1 and 7, $\sigma(7) = 1 + 7 = 8$.

(c) $\sigma(10)$

   Since the positive divisors of 10 are 1, 2, 5, and 10, $\sigma(10) = 1 + 2 + 5 + 10 = 18$.
◈

Example 7.19 An integer n is defined to be a *perfect number* if and only if n is equal to the sum of all of its divisors except for itself (but including 1). Make a conjecture about $\sigma(n)$ when n is perfect.

Solution
In order to make a conjecture, we will test some examples. The two smallest perfect numbers are 6 and 28 ($6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$). Start by comparing σ for these two perfect numbers, as well as two numbers which are not perfect. For variety, we'll pick an even, 12, and a prime, 7.

$$\sigma(6) = 1 + 2 + 3 + 6 = 12$$
$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$$
$$\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$$
$$\sigma(7) = 1 + 7 = 8$$

   Notice that $\sigma(6) = 2 \cdot 6 = 12$ and $\sigma(28) = 2 \cdot 28 = 56$. That is not the case in the last two examples: $\sigma(12)$ is greater than $2 \cdot 12 = 24$ and $\sigma(7)$ is less than $2 \cdot 7 = 14$. At this point, one possible conjecture is the following:

> **Conjecture 7.2:** If n is a perfect number, then $\sigma(n) = 2n$.

   This conjecture is true. The proof is left as Exercise 11.
◈

   The functions $d(n)$ and $\sigma(n)$ both also have formulas that can be used to calculate them. Although these formulas are not used in Chap. 8 for producing codes, they are included here for completeness and this section contains some exercises where they will be useful. The proofs are beyond the scope of this text and are not included.

Theorem 7.8
If $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \cdots \cdot p_k^{a_k}$, then

$$d(n) = (a_1 + 1)(a_2 + 1) \cdot \cdots \cdot (a_k + 1)$$

Theorem 7.9
If $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \cdots \cdot p_k^{a_k}$, then

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdot \cdots \cdot \frac{p_k^{a_k+1} - 1}{p_k - 1}$$

Exercise Set 7.5

1. What is the smallest possible value for $d(n)$? What are the possible choices for n that result in this value?
2. Can $d(n)$ be negative? Explain.
3. Prove or disprove the following conjecture.
   CONJECTURE: If p and q are different primes, then $d(pq) = 4$.
4. Find all values of n for which $d(n) = 1$.
5. Find all values of n for which $d(n) = 2$.
6. Find all values of n for which $d(n) = 3$.
7. Find all values of n for which $\sigma(n) = 1$.
8. Find all values of n for which $\sigma(n) = 2$.
9. Prove that if p is prime and $a > 0$, then $d(p^a) = a + 1$.
10. Prove that if p is prime, then $\sigma(p) = p + 1$.
11. Prove **Conjecture 7.2** from Example 7.19.

7.6   Euler's Theorem

Euler's Theorem is more general than Fermat's Little Theorem. The congruence in the theorem still gives an example of when the power of an integer will have a least residue of 1, but the modulus does not have to be prime. Here is a statement of the theorem.

Theorem 7.10 Euler's Theorem
If m is a positive integer and a is an integer with $\gcd(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \; mod \; m$$

In order to prove Euler's Theorem, the following Lemmas will be useful.

Lemma 7.3
If $\gcd(c, m) = 1$ and $ac \equiv bc \bmod m$, then $a \equiv b \bmod m$.

Proof. Let $\gcd(c, m) = 1$ and suppose $ac \equiv bc \bmod m$. By the definition of congruence, $m | (ac - bc)$. Therefore, by the definition of divides, $ac - bc = mk$ for an integer k. Factoring the left-hand side, $c(a - b) = mk$. Therefore $m | c(a - b)$. Now, since $\gcd(c, m) = 1$, m must divide $(a - b)$. (The proof of this fact is Exercise 18 in Section 5.3). Since $m | (a - b)$, $a \equiv b \bmod m$ by the definition of congruence.

$\blacksquare$

Lemma 7.4
If $\gcd(a, m) = 1$ and $\gcd(b, m) = 1$, then $\gcd(ab, m) = 1$.

Proof. Suppose $\gcd(a, m) = 1$ and $\gcd(b, m) = 1$. Then there are integers r and s such that $ra + sm = 1$, and integers k and l such that $kb + lm = 1$. Then, $(ra + sm)kb + lm = 1$. Simplifying the left-hand side, we obtain

$$rakb + smkb + lm = 1$$
$$rk(ab) + (skb + l)m = 1$$

This shows that a linear combination of ab and m is equal to 1. Now, call $\gcd(ab, m) = d$. Since $d | ab$ and $d | m$, it is also true that $d | (rk(ab) + (skb + l)m)$. (This is true by Theorem 2.3.) Therefore, $d | 1$. Since d must be a positive integer, this tells us that $d = 1$. Therefore, $\gcd(ab, m) = 1$.

$\blacksquare$

Lemma 7.4 can be generalized to more than two pairs of numbers. The general statement follows in Lemma 7.5. The proof is similar to that of Lemma 7.4 but is beyond the scope of this course.

Lemma 7.5
If $\gcd(b_1, m) = \gcd(b_2, m) = \cdots = \gcd(b_n, m) = 1$, then $\gcd(b_1 \cdot b_2 \cdots b_n, m) = 1$.

Now we will proceed with the proof of Theorem 7.10, Euler's Theorem.

Proof of Euler's Theorem. Let $m > 0$ and let a be an integer such that $\gcd(a, m) = 1$. Since $\phi(m)$ counts the number of integers less than m that are relatively prime to m, listing these integers will produce $\phi(m)$ numbers. Let $1 = b_1, b_2, \ldots, b_{\phi(m)}$ be the integers less than m and relatively prime to m. Now multiply each element of this

list by a. This produces a second list of integers: $a, ab_2, ab_3, \ldots, ab_{\phi(m)}$. By Lemma 7.4, since $\gcd(a, m) = 1$ and $\gcd(b_i, m) = 1$, it is also true that $\gcd(ab_i, m) = 1$ for $i = 1, 2, \ldots, \phi(m)$. Therefore, the least residues of each of the ab_i terms must be on the first list since it includes all the least residues of integers relatively prime to m. The question is, are any of the ab_i congruent to each other modulo m, or are they matched one for one with the terms on the original list? To find out, suppose that $ab_i \equiv ab_j \bmod m$. Applying the definition of congruence, we obtain the following:

$$ab_i \equiv ab_j \bmod m$$
$$m \mid (ab_i - ab_j)$$
$$m \mid a(b_i - b_j)$$

Since $\gcd(m, a) = 1$, $m \mid (b_i - b_j)$ by Exercise 18 of Section 5.3. Again applying the definition of congruence, this means that $b_i \equiv b_j \bmod m$. But this is a contradiction since the list of the b_n's contains the distinct integers less than m and relatively prime to m. Therefore, the least residues of the integers ab_i in some order are $1 = b_1, b_2, \ldots, b_{\phi(m)}$. This means that

$$a \cdot ab_2 \cdot \cdots \cdot ab_{\phi(m)} \equiv 1 \cdot b_2 \cdot b_3 \cdots \cdots b_{\phi(m)} \bmod m$$

Factoring the a out of the terms on the left,

$$a^{\phi(m)}\left(1 \cdot b_2 \cdot \cdots \cdot b_{\phi(m)}\right) \equiv 1 \cdot b_2 \cdot b_3 \cdots \cdots b_{\phi(m)} \bmod m$$

By Lemma 7.5, $\gcd(b_1 \cdot b_2 \cdot \cdots \cdot b_{\phi(m)}, m) = 1$. Therefore, by Lemma 7.3,

$$a^{\phi(m)} \equiv 1 \bmod m$$

This proves Euler's Theorem.

∎

   Euler's Theorem is useful for reducing large powers of an integer, modulo m. Here is an example of how it can be used.

Example 7.20 Find the last two digits of the number 7^{209}.

Solution
The last two digits of a number are the same as the remainder when divided by 100. Therefore, the question is asking for the least residue of 7^{209} modulo 100. Since gcd $(7, 100) = 1$, Euler's Theorem applies. By Euler's Theorem,

$$7^{\phi(100)} \equiv 1 \bmod 100$$

By Example 7.16, $\phi(100) = 40$. Therefore, $7^{40} \equiv 1 \ mod \ 100$. Since $209 = 5(40) + 9$,

$$7^{209} \equiv 7^{5(40)+9} \ mod \ 100$$
$$\equiv \left(7^{40}\right)^5 \cdot 7^9 \ mod \ 100$$
$$\equiv 1 \cdot 7^9 \ mod \ 100$$

The value 7^9 is small enough that a calculator can be used to find that $7^9 \equiv 7 \ mod \ 100$. Alternatively, since $7^3 \equiv 343 \ mod \ 100 \equiv 43 \ mod \ 100$, we have $7^9 \equiv (7^3)^3 \ mod \ 100 \equiv 43^3 \ mod \ 100 \equiv 79507 \ mod \ 100 \equiv 7 \ mod \ 100$.

Therefore, the last two digits of the number 7^{209} are 07.

◈

Euler's Theorem can also be used to find a solution to a linear congruence, as long as the conditions of the theorem are met.

Example 7.21 Find a solution to the congruence $4x \equiv 7 \ mod \ 15$.

Solution
Since $\gcd(4, 15) = 1$ and $1|7$, the congruence has a solution. Now, applying Euler's Theorem to $a = 4$ and $m = 15$,

$$4^{\phi(15)} \equiv 1 \ mod \ 15.$$

From Theorem 7.7, $\phi(15) = 15\left(\frac{2}{3}\right) \cdot \left(\frac{4}{5}\right) = 8$. Therefore, $4^8 \equiv 1 \ mod \ 15$. Notice that this means 4 and 4^7 are inverses modulo 15. Multiplying the original congruence by 4^7 on both sides produces:

$$4^7 \cdot 4x \equiv 4^7 \cdot 7 \ mod \ 15$$
$$x \equiv 4^7 \cdot 7 \ mod \ 15$$

Now, to reduce 4^7, we find that $4^2 \equiv 1 \ mod \ 15$ so $4^7 \equiv (4^2)^3 \cdot 4 \equiv 4 \ mod \ 15$.

Therefore,

$$x \equiv 4 \cdot 7 \ mod \ 15 \equiv 13 \ mod \ 15$$

◈

The most important application of Euler's Theorem covered in this textbook is cryptography. In Chap. 8, Euler's Theorem will be essential in the creation of the RSA code.

Exercise Set 7.6

1. Find the last digit of the number 3^{246}. (Hint: the last digit is the remainder when the number is divided by 10.)
2. Find the last two digits of the number 11^{244}.
3. Find the last digit of the number 7^{405}.

4. Find the remainder when 6^{341} is divided by 5.
5. Show that if $\gcd(a, m) = 1$, then the inverse of a modulo m is $a^{\phi(m) - 1}$.
6. Prove that if p is prime and $p \nmid a$, then $a^{p - 1} \equiv 1 \ mod \ p$.

7.7   Summary and Review Exercises

7.7.1   Vocabulary and Symbols

Wilson's Theorem
Fermat's Little Theorem
numerical functions
number theoretic functions
arithmetic functions
Euler phi function, $\phi(n)$
number of positive divisors function, $d(n)$
sum of positive divisors function, $\sigma(n)$
Euler's Theorem

7.7.2   Suggested Readings

Robinson, Raphael M. *Mersenne and Fermat Numbers,* **Proceedings of the American Mathematical Society,** 1954, 842–846

Burckhardt, J. J. *Leonhard Euler, 1707 – 1783*, **Mathematics Magazine, v. 56,** 262–273, 1983

Colquitt, W. M. and L. Welsh Jr. *A new Mersenne Prime*, **Mathematical Computation, v. 56** 867–870, 1991.

Crandall, R., J. Doenias, C. Norrie, and J. Young, *The Twenty-Second Fermat Number is Composite,* **Mathematical Computation, v. 64** 863–868, 1995.

7.7.3   Review Exercises

1. Find a counterexample to the following statement and explain the example.
   If a and b are positive integers, then $\phi(ab) = \phi(a)\phi(b)$.
2. Find the least residue of 2^{132} modulo 47.
3. Find the least residue of 17! modulo 18.
4. Find the least residue of 15! modulo 17.
5. List the possible least residues modulo 17.
6. Which integer(s) cannot occur as the units digit of the fifth power of an integer?

7. Which integer(s) can occur as the units digit of the fourth power of an integer?
8. Find the remainder when $36 \cdot 15 \cdot 22 \cdot 18 \cdot 39$ is divided by 7.
9. Compute $35^{21} \; mod \; 11$.
10. Compute 34^{74} modulo 57.
11. Compute the value of $37^{31} \cdot 29^2 \; mod \; 31$.
12. Compute the value of $33^{31} \cdot 26^2 \; mod \; 31$.

Exercises 13–16. Use Euler's Theorem to compute the least residue of the expression.
13. 29^{128} modulo 20
14. 79^{79} modulo 8
15. 3^{1000} modulo 14
16. 9^{13} modulo 11

Exercises 17–19. Apply Fermat's Little Theorem when appropriate to find the least residue of the expression in the given modulus. If Fermat's Little Theorem does not apply, explain why.
17. 2^{10} modulo 7
18. 3^{17} modulo 17
19. 3^{12} modulo 14

20. Use Euler's Theorem or Fermat's Little Theorem to evaluate $10^{13} \; mod \; 11$.
21. Find the least residue of 377^3 modulo 124.
22. Prove that if m is composite and $m > 4$, then $(m - 1)! \equiv 0 \; mod \; m$.

Chapter 8
Cryptology

> *The problem of distinguishing prime numbers from composites, and of resolving composite numbers into their prime factors, is one of the most important and useful in all of arithmetic.*
>
> —Carl Friedrich Gauss, 1777–1855

8.1 Introduction

For as long as there have been civilizations, people have tried to keep secrets—where the food is stored, where the treasure is hidden, who has the money, and so on. Now that so much information is transmitted over the Internet, it has become very important to develop secure methods of sending and receiving information. Security concerns are widespread because so much personal information is stored on computers; Internet accounts are protected by passwords, and many monetary transactions take place online. Eavesdroppers try to intercept online transactions, hoping to steal your credit card information or even your identity. Over the years, governments have relayed vital information to allies while attempting to keep enemies from obtaining it. Entire agencies, such as the National Security Agency, employ hundreds of mathematicians to keep their government's information a secret while trying to intercept and decode information belonging to other governments or groups.

In this chapter, there are two interesting questions that we will answer:

1. How can you give information to some individuals while keeping it a secret from others?
2. In the age of high-speed computers, how can you safely transfer information across the Internet without that information being obtained by the wrong person?

The field of *cryptology* encompasses all aspects of secret codes. The subfield of *cryptography* is concerned with developing and implementing codes, and the subfield of *cryptanalysis* focuses on how to break these codes.

The original message that is to be securely transmitted is called the *plaintext*. Once the message has been converted to a coded form, it is called the *ciphertext*. The process of turning the plaintext into ciphertext is called the *cipher* or *encryption method*. The process used by the intended receiver to convert the ciphertext back into plaintext is called the *decryption method*. The *key* describes the process or processes used to both encrypt and decrypt messages.

A *cryptosystem* consists of the encryption and decryption methods as well as the key that is needed to use them. There are two types of keys. In *private key codes*, either the same key is used for encryption and decryption or knowing one key will allow you to find the other. These systems are called private key because anyone who obtains either key will be able to decrypt messages, whether they are the intended recipient or not. Only the sender and the intended recipient can have access to the key. On the other hand, in *public key codes*, anyone can have access to the encryption key, and they still will not be able to figure out the decryption key (which is still private). Public key codes were first invented in the 1970s, and one of the most famous examples will be discussed in Section 8.4.

Although early and modern methods of cryptography vary greatly, almost every cryptosystem follows the same basic process, outlined below.

Step 1 The sender and intended receiver agree on an encryption method and exchange keys if necessary.

Step 2 The message is encrypted using the chosen encryption method and key. This converts the plaintext to ciphertext.

Step 3 The ciphertext is transmitted to the intended receiver.

Step 4 The receiver decrypts the ciphertext using the key and obtains the plaintext.

8.2 Private Key Cryptography

8.2.1 Substitution Ciphers

The simplest form of encrypting a message is a *substitution cipher*. In a substitution cipher, the ciphertext is produced by replacing each letter of the plaintext by another letter (or possibly number or symbol) according to the key. Many newspapers include a puzzle consisting of a famous quote encrypted with a substitution cipher. These types of puzzles are called *cryptograms*. The organization American Cryptogram Association has cryptograms available for fun on their web page: www.cryptogram.org.

   Although the hobby of deciphering coded messages for fun goes all the way back to the Middle Ages and was also popularized by Edgar Allen Poe in the 1800s, the ciphers now commonly used in cryptograms and other puzzles were not originally developed for entertainment. Originally, ciphers of this type were used for encrypting military or personal secrets. However, especially with the availability of computers, these encryption techniques are no longer secure. Using a combination of frequency analysis (e.g., "e" is the most common letter in English) and pattern recognition (e.g., a one letter word will be "I," "a," or possibly "o") these codes can be broken fairly quickly.

Example 8.1 Use the substitution cipher given below to encrypt the message BRAVO.

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Solution
To encrypt the message, find each letter of the message BRAVO in the plaintext row of the key and replace it with the corresponding ciphertext. This leads to the following encryption:

   B → G
   R → W
   A → F
   V → A
   O → T
   Therefore, the ciphertext is GWFAT.

◈

8.2.2   Caesar Cipher

Julius Caesar, who lived from 100 BC to 44 BC, famously used a substitution cipher to send sensitive military information. He used a simple shift method of replacing each letter with the letter three spaces away. Here is the encryption key for Caesar's cipher.

Table 8.1   Caesar cipher encryption key

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Example 8.2 Use the Caesar cipher to encrypt the message: BE PREPARED.

Solution:
Using the encryption key provided in Table 8.1, we obtain the following ciphertext.
                           EH SUHSDUHG

◈

Example 8.3 Decrypt the following message that was encrypted using the Caesar cipher.

<div align="center">

QHYHU JLYH XS

</div>

Solution

In order to decrypt this message, we could simply use the encryption key in Table 8.1, finding the letters in the encrypted message in the ciphertext row rather than the plaintext row. For example, Q in ciphertext corresponds to N in plaintext. For a long message, and especially for more complicated keys, it may be easier to rewrite the key with the ciphertext in alphabetical order, so that we can more quickly find the letters in the encrypted message. The Caesar cipher decryption key is shown in Table 8.2.

Table 8.2 Caesar cipher decryption key

Ciphertext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plaintext	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Using the decryption key to decode the message, we obtain

<div align="center">

NEVER GIVE UP

</div>

◈

While this encryption method would likely have been fairly secure in Caesar's time (partly because many people were illiterate), it is no longer a secure way to send important information.

Notice that many different shift ciphers similar to the one used by Caesar are possible. An encryption key can be generated by shifting letters by one, two, three, etc. all the way to 25 spaces, before A would match up again with A.

By replacing each letter of the alphabet with a numerical equivalent, we can represent encryption techniques of this type using modular arithmetic and congruences. There is no set way to match the letters of the alphabet up with numbers. In this section, we will use the numerical equivalents given in Table 8.3.

Table 8.3 Numerical equivalents

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Example 8.4 Represent the Caesar cipher encryption method using modular arithmetic. Then, encrypt the message: **PEANUTS**.

Solution

First, to represent the encryption key for the Caesar cipher using modular arithmetic, suppose that $\mathcal{P}$ is the numerical equivalent for one of the letters appearing in the plaintext message. So, for the plaintext letter E, $\mathcal{P} = 4$. Now, shifting to the right three letters in the alphabet is equivalent to adding 3 to the value of $\mathcal{P}$. Therefore, if $\mathcal{C}$ represents the ciphertext, $\mathcal{C} = \mathcal{P} + 3$.

This formula works, except for the plaintext letters X $= 23$, Y $= 24$, and Z $= 25$. For example, if we are encrypting an X, $\mathcal{P} = 23$, so $\mathcal{C} = 23 + 3 = 26$ which is not matched up with a letter. From the Caesar cipher encryption key in Table 8.1, we see that X should be encrypted as A, whose numerical equivalent is 0. In order to make the numerical equivalents restart at 26, we will calculate the ciphertext modulo 26. Therefore, the numerical encrypted form of plaintext $\mathcal{P}$ is $\mathcal{C} \equiv \mathcal{P} + 3 \, mod \, 26$, where $\mathcal{C}$ is the least residue of $\mathcal{P} + 3$ modulo 26. Note that this means $\mathcal{C}$ will be between 0 and 25.

Now, we will encode the message **PEANUTS**.

Encryption Process:

1. Match each letter in the plaintext with its numerical equivalent.

<div align="center">

15 4 0 13 20 19 18

</div>

2. For each number representing a letter of plaintext, use the formula $\mathcal{C} \equiv \mathcal{P} + 3 \, mod \, 26$, where $\mathcal{P}$ is a number from the plaintext and $\mathcal{C}$ is the coded ciphertext.

$$
\begin{aligned}
\mathcal{C} &\equiv 15 + 3 \equiv 18 \, mod \, 26 \\
\mathcal{C} &\equiv 4 + 3 \equiv 7 \, mod \, 26 \\
\mathcal{C} &\equiv 0 + 3 \equiv 3 \, mod \, 26 \\
\mathcal{C} &\equiv 13 + 3 \equiv 16 \, mod \, 26 \\
\mathcal{C} &\equiv 20 + 3 \equiv 23 \, mod \, 26 \\
\mathcal{C} &\equiv 19 + 3 \equiv 22 \, mod \, 26 \\
\mathcal{C} &\equiv 18 + 3 \equiv 21 \, mod \, 26
\end{aligned}
$$

This produces the list of numerical equivalents for the ciphertext:

<div align="center">

18   7   3   16   23   22   21

</div>

3. Convert to letter equivalents to form the ciphertext: **S H D Q X W V**

<div align="right">◈</div>

Congruences can also be used to decrypt messages that were encrypted with the Caesar cipher. Solving the formula $\mathcal{C} \equiv \mathcal{P} + 3 \, mod \, 26$ for the plaintext $\mathcal{P}$ by subtracting 3 from both sides of the congruence reveals the decryption key: $\mathcal{P} \equiv \mathcal{C} - 3 \, mod \, 26$.

Example 8.5 Use the decryption key $\mathcal{P} \equiv \mathcal{C} - 3 \, mod \, 26$ to decrypt the following message encrypted with the Caesar cipher.

<div align="center">

V Q R R S B

</div>

Solution
Decryption Process

1. Rewrite the ciphertext using the numerical equivalents from Table 8.3 for each letter:

<div align="center">

21 16 17 17 18 1

</div>

2. Apply the formula $\mathcal{P} \equiv \mathcal{C} - 3 \; mod \; 26$ to each number $\mathcal{C}$ in the ciphertext.

$$\mathcal{P} \equiv 21 - 3 \equiv 18 \; mod \; 26$$
$$\mathcal{P} \equiv 16 - 3 \equiv 13 \; mod \; 26$$
$$\mathcal{P} \equiv 17 - 3 \equiv 14 \; mod \; 26$$
$$\mathcal{P} \equiv 17 - 3 \equiv 14 \; mod \; 26$$
$$\mathcal{P} \equiv 18 - 3 \equiv 15 \; mod \; 26$$
$$\mathcal{P} \equiv \; 1 - 3 \equiv -2 \; mod \; 26 \equiv 24 \; mod \; 26$$

Therefore, the numerical equivalent of the plaintext is

18   13   14   14   15   24

3. Convert each number to its alphabetical equivalent to reveal the plaintext.

SNOOPY

◆

Example 8.6 Use the Caesar cipher method of Example 8.4 to encrypt the message THEORY.

Solution
1. Begin with the word THEORY.
2. Convert each letter in the message to its numerical equivalent: 19 7 4 14 17 24.
3. To encrypt the message, use the formula $\mathcal{C} \equiv \mathcal{P} + 3 \; mod \; 26$, where $\mathcal{P}$ is a number from the plaintext and $\mathcal{C}$ is the numerical ciphertext.

$$\mathcal{C} \equiv 19 + 3 \equiv 22 \; mod \; 26$$
$$\mathcal{C} \equiv \; 7 + 3 \equiv 10 \; mod \; 26$$
$$\mathcal{C} \equiv \; 4 + 3 \equiv 7 \; mod \; 26$$
$$\mathcal{C} \equiv 14 + 3 \equiv 17 \; mod \; 26$$
$$\mathcal{C} \equiv 17 + 3 \equiv 20 \; mod \; 26$$
$$\mathcal{C} \equiv 24 + 3 \equiv 27 \; mod \; 26 \equiv 1 \; mod \; 26$$

Therefore, the numerical ciphertext is 22 10 7 17 20 1.
4. Converting each number back to alphabetical form, we obtain the encrypted message.

WKHRUB

◆

Example 8.7 Show that decrypting the ciphertext WKHRUB from Example 8.6 does result in the original plaintext, THEORY.

Solution
Follow the decryption process on the ciphertext WKHRUB.

1. Convert the alphabetical ciphertext to numerical form: WKHRUB → 22 10 7 17 20 1.
2. Apply the formula $\mathcal{P} \equiv \mathcal{C} - 3 \; mod \; 26$ to each number $\mathcal{C}$ in the ciphertext.

$$\mathcal{P} \equiv 22 - 3 \equiv 19 \ mod \ 26$$
$$\mathcal{P} \equiv 10 - 3 \equiv 7 \ mod \ 26$$
$$\mathcal{P} \equiv \ 7 - 3 \equiv 4 \ mod \ 26$$
$$\mathcal{P} \equiv 17 - 3 \equiv 14 \ mod \ 26$$
$$\mathcal{P} \equiv 20 - 3 \equiv 17 \ mod \ 26$$
$$\mathcal{P} \equiv \ 1 - 3 \equiv -2 \ \equiv 24 \ mod \ 26$$

Therefore, the numerical form of the plaintext is

$$19 \quad 7 \quad 4 \quad 14 \quad 17 \quad 24$$

3. Converting back to letters using Table 8.3 shows that the original message THEORY is recovered.

◈

8.2.3   Vigenère Cipher

The Vigenère cipher is named after the French cryptographer Blaise de Vigenère who lived from 1523 to 1596. It is another private key code, but the encryption process is more complicated than the Caesar cipher. Instead of using the same process to encrypt each occurrence of a given letter in the plaintext, a *keyword* is used to vary the way the letter is encrypted each time it occurs. The process is illustrated in Example 8.8.

Example 8.8 Encrypt the message "DO NOT MOVE" using the Vigenère cipher with keyword SNOW.

Solution
Encryption Process for the Vigenère Cipher:

1. Match the letters of the keyword with their numerical equivalents from Table 8.3.

$$S = 18, \ N = 13, \ O = 14, \ W = 22$$

2. Rewrite the plaintext message DO NOT MOVE using the numerical equivalent of each letter from Table 8.3.

3 14 13 14 19 12 14 21 4

3. Arrange the numbers in the numerical plaintext in groups of the same length as the keyword, in this case four. You may have a block shorter than four for the last group.

$$3 \quad 14 \quad 13 \quad 14 \qquad 19 \quad 12 \quad 14 \quad 21 \qquad \qquad 4$$

4. Now, for a block of plaintext with numerical equivalents $p_1 p_2 p_3 p_4$, and keyword with numerical equivalents $k_1 k_2 k_3 k_4$, use the following formulas to produce the encrypted message or ciphertext:

$$c_1 \equiv p_1 + k_1 \ mod \ 26$$
$$c_2 \equiv p_2 + k_2 \ mod \ 26$$
$$c_3 \equiv p_3 + k_3 \ mod \ 26$$
$$c_4 \equiv p_4 + k_4 \ mod \ 26$$

Recall that the keyword numerical equivalents were obtained in Step 1. For this example, $k_1 = 18$, $k_2 = 13$, $k_3 = 14$, and $k_4 = 22$.

Repeat this process for each block, and notice that the encrypted form of the same letter is not always the same. This process is shown for each numerical block of the plaintext in the table below.

Plaintext	Plaintext (numerical)	Encryption formula	Ciphertext (numerical)	Ciphertext
D	3	$c_1 \equiv 3 + 18 \bmod 26$	21	V
O	14	$c_2 \equiv 14 + 13 \bmod 26$	1	B
N	13	$c_3 \equiv 13 + 14 \bmod 26$	1	B
O	14	$c_4 \equiv 14 + 22 \bmod 26$	10	K
T	19	$c_1 \equiv 19 + 18 \bmod 26$	11	L
M	12	$c_2 \equiv 12 + 13 \bmod 26$	25	Z
O	14	$c_3 \equiv 14 + 14 \bmod 26$	2	C
V	21	$c_4 \equiv 21 + 22 \bmod 26$	17	R
E	4	$c_1 \equiv 4 + 18 \bmod 26$	22	W

Plaintext, grouped in blocks: DONO TMOV E
Numerical plaintext: 3 14 13 14 19 12 14 21 4
Numerical ciphertext: 21 1 1 10 11 25 2 17 22
Ciphertext: VBBK LZCR W

Comparing the ciphertext to the plaintext shows that the same letter can be encrypted differently, because of the use of the keyword.

Plaintext	D	O	N	O	T	M	O	V	E
Ciphertext	V	B	B	K	L	Z	C	R	W

◈

Example 8.9 The following ciphertext was produced with a Vigenère cipher and keyword MONEY. Decrypt the message to find the original plaintext.

$$\text{P C H R R   A C G L C   D G}$$

Solution
Decryption Process for the Vigenère Cipher

1. Rewrite the keyword in terms of its numerical equivalents from Table 8.3:

$$M = 12, O = 14, N = 13, E = 4, Y = 24$$

2. Rewrite the ciphertext using the numerical equivalent of each letter from Table 8.3. Notice that since the keyword in this example has five letters, the blocks (except for the last one) have length five.

$$15 \ 2 \ 7 \ 17 \ 17 \quad 0 \ 2 \ 6 \ 11 \ 2 \quad 3 \ 6$$

3. For keyword numerical equivalents $k_1 k_2 k_3 k_4 k_5$ and ciphertext block $c_1 c_2 c_3 c_4 c_5$, solve each encryption formula in Example 8.8 for plaintext p_i to obtain the decryption formulas:

$$p_1 \equiv c_1 - k_1 \bmod 26$$
$$p_2 \equiv c_2 - k_2 \bmod 26$$
$$p_3 \equiv c_3 - k_3 \bmod 26$$
$$p_4 \equiv c_4 - k_4 \bmod 26$$
$$p_5 \equiv c_5 - k_5 \bmod 26$$

Using the numerical equivalents for the keyword values found in Step 1 ($k_1 = 12$, $k_2 = 14$, $k_3 = 13$, $k_4 = 4$, and $k_5 = 24$), apply the decryption formulas to each block of the ciphertext to recover the plaintext numerical equivalents.

This process is shown for each numerical block of the ciphertext in the table below.

Ciphertext	Ciphertext (numerical)	Decryption formula	Plaintext (numerical)	Plaintext
P	15	$p_1 \equiv \mathbf{15} - 12 \bmod 26$	3	D
C	2	$p_2 \equiv \mathbf{2} - 14 \bmod 26$	14	O
H	7	$p_3 \equiv \mathbf{7} - 13 \bmod 26$	20	U
R	17	$p_4 \equiv \mathbf{17} - 4 \bmod 26$	13	N
R	17	$p_5 \equiv \mathbf{17} - 24 \bmod 26$	19	T
A	0	$p_1 \equiv \mathbf{0} - 12 \bmod 26$	14	O
C	2	$p_2 \equiv \mathbf{2} - 14 \bmod 26$	14	O
G	6	$p_3 \equiv \mathbf{6} - 13 \bmod 26$	19	T
L	11	$p_4 \equiv \mathbf{11} - 4 \bmod 26$	7	H
C	2	$p_5 \equiv \mathbf{2} - 24 \bmod 26$	4	E
D	3	$p_1 \equiv \mathbf{3} - 12 \bmod 26$	17	R
G	6	$p_2 \equiv \mathbf{6} - 14 \bmod 26$	18	S

Ciphertext, grouped in blocks: PCHRR   ACGLC   DG
Ciphertext in numerical form: 15 2 7 17 17   0 2 6 11 2   3 6
Plaintext in numerical form: 3 14 20 13 19   14 14 19 7 4   17 18
Plaintext: D O U N T   O O T H E   R S

Therefore, the message is "DO UNTO OTHERS."

Comparing the ciphertext to the plaintext shows again that the same letter can be encrypted differently:

Ciphertext	P	C	H	R	R	A	C	G	L	C	D	G
Plaintext	D	O	U	N	T	O	O	T	H	E	R	S

◈

For many years this code was thought to be unbreakable. In 1854, however, British mathematician Charles Babbage (1791–1871) discovered a test to determine the keyword length (The publication of the method was prevented for several years by the British national security, who used the test to decode secret messages and did not want their enemies to know they had this tool). In 1920 a test was developed by US Army cryptographer William Friedman (1891–1960) to check to see if the correct key length was found. Once the key length is known, frequency analysis can again be used to break this code.

One difficulty with any private key code, no matter how complicated, is that the key must be kept between the intended sender and receiver. At some point this information must be transferred to the intended recipients of the secret messages. Section 8.4 presents an example of a public key code that does not have this issue–the encryption key can be known by anyone because it does not lead to the decryption key.

Exercise Set 8.2

When numerical equivalents are needed in this exercise section, use the values from Table 8.3.

1. The encryption key used to encrypt the message below is given here. Decrypt the message to find the plaintext.

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	Q	R	S	N	O	P	K	L	M	H	I	J	W	F	G	C	D	E	A	B	T	X	Y	Z	U	V

<div align="center">

FOXOE   MFHTEO   Q   PEMOFN   OXOF   MF   HOAB
—WQESTA   SMSOEG

</div>

2. Use the Caesar cipher to encrypt the plaintext: DO OR DO NOT DO. THERE IS NO TRY.
3. Use the Caesar cipher to decrypt the ciphertext: VDQLWB LV QRW LQ QXPEHUV.
4. Use a Vigenère cipher, with keyword GLEE, to encrypt the message: THE FINAL IS ON MONDAY.
5. Decrypt the following message, encrypted using a Vigenère cipher with keyword WHISPER: SOILXWK DLUSIVZ T.
6. We can form a slightly more complicated code than the Caesar cipher, by using a formula of the following type: $C \equiv aP + b \bmod 26$. (In the Caesar cipher, $a = 1$ and $b = 3$). The following ciphertext was encrypted using the formula $C \equiv 21P + 5 \bmod 26$: YLCLFTL OWL WNJSQT.

   (a) What is the decryption key?
   (b) Using the key from part (a), decrypt the coded message.

8.3 Encryption by Exponentiation

This section provides an example of a more complex and hence more secure method of encryption. This method of encryption, introduced in 1978 by Stephen Pohlig and Martin Hellman, is still an example of a private key code, but breaking the code without having the key is much more difficult than for the methods discussed in Section 8.2. In the Caesar cipher and Vigenère cipher, modular addition was used to encrypt the messages. To make the encryption process more difficult to reverse, this method uses exponents to encrypt the plaintext.

The general encryption process is explained below.

8.3.1 Encryption Process for Exponentiation Cipher

Steps in the Encryption Process

1. Convert the plaintext to numerical equivalents, using Table 8.3.
2. Choose a prime p. Note that p must be larger than 25 since that is the largest numerical equivalent in our numbering system. The prime p will be the modulus used in the encryption formula. In practice, p would be quite large. To make our calculations easier, we will keep p relatively small.
3. Choose a number e such that $\gcd(e, p-1) = 1$. The value e is the exponent in the encryption formula, so e is often called the *encryption exponent*.
4. To find the ciphertext, $\mathcal{C}$, raise each plaintext numerical equivalent $\mathcal{P}$ to the power e, and then reduce modulo p. The encryption formula is:

$$\mathcal{C} \equiv \mathcal{P}^e \bmod p$$

Example 8.10 Use the exponentiation method to encrypt the message "NO MORE SNOW."

Solution
Encryption Method

1. Convert each letter of the plaintext to its numerical equivalent.
   13 14 12 14 17 4 18 13 14 22
2. Choose a prime $p > 25$ and an integer e such that $\gcd(e, p-1) = 1$.
   For this example, choose $p = 29$ and $e = 3$. Then it is true that $\gcd(3, 28) = 1$.
3. Create the ciphertext by raising each of the numerical equivalents in plaintext to the exponent $e = 3$, and then find the least residue modulo 29.

Message	Plaintext $\mathcal{P}$	$\mathcal{P}^3$	Ciphertext $\mathcal{C} \equiv \mathcal{P}^3 \bmod 29$
N	13	2197	**22**
O	14	2744	**18**
M	12	1728	**17**
O	14	2744	**18**
R	17	4913	**12**
E	4	125	**9**
S	18	5832	**3**
N	13	2197	**22**
O	14	2744	**18**
W	22	10648	**5**

Therefore, the ciphertext for NO MORE SNOW is

$$22 \ 18 \ 17 \ 18 \ 12 \ 9 \ 3 \ 22 \ 18 \ 5$$

◈

8.3.2   *Decryption Process for the Exponentiation Cipher*

In order to decrypt a message encrypted with the exponentiation cipher, we must reverse the encryption process. The decryption technique is explained below, followed by an example.

Steps in the Decryption Process

Suppose that the ciphertext was encrypted with prime p and exponent e using the congruence $\mathcal{C} \equiv \mathcal{P}^e \bmod p$, where $\mathcal{P}$ is the plaintext.

1. Choose a positive integer d such that $de \equiv 1 \bmod (p-1)$. (Since gcd $(e, p-1) = 1$, this will always be possible by Theorem 6.7.) The value of d will be the exponent in the decryption formula, so d is called the *decryption exponent*.
2. Then, for each numerical ciphertext $\mathcal{C}$:

$$\mathcal{P} \equiv \mathcal{C}^d \bmod p$$

where $\mathcal{P}$ is the numerical equivalent of the plaintext.

Let us look at why this decryption method works: Why does finding the least residue of $\mathcal{C}^d$ modulo p return the numerical plaintext?

Remember that d was chosen so that $de \equiv 1 \bmod (p-1)$. Rewriting this congruence using Theorem 6.1, we obtain the expression $de = 1 + k(p-1)$ where k is an integer.

Then, beginning with the encryption formula:

$$\mathcal{C} \equiv \mathcal{P}^e \ mod \ p$$
$$\mathcal{C}^d \equiv (\mathcal{P}^e)^d \ mod \ p$$
$$\equiv \mathcal{P}^{de} \ mod \ p$$
$$\equiv \mathcal{P}^{1+k(p-1)} \ mod \ p$$
$$\equiv \mathcal{P} \cdot \mathcal{P}^{(p-1)k} \ mod \ p$$

Now, since $\mathcal{P} \le 25$ and $p > 25$ is prime, $\gcd(\mathcal{P}, \ p) = 1$. Therefore, by Fermat's Little Theorem (Theorem 7.3), $\mathcal{P}^{p-1} \equiv 1 \ mod \ p$. Then, by substituting we obtain that

$$\mathcal{C}^d \equiv \mathcal{P}\left(\mathcal{P}^{p-1}\right)^k \ mod \ p \equiv \mathcal{P} \ mod \ p.$$

Since $\mathcal{P}$ represents the numerical equivalent of the plaintext, the message has been decrypted. This fact is stated in Theorem 8.1.

> **Theorem 8.1**
> Let p be prime and let e be an integer such that $\gcd(e, p - 1) = 1$. Then there is a positive integer d such that $de \equiv 1 \ mod \ (p - 1)$, and if $\mathcal{C}$ and $\mathcal{P}$ are integers such that $\mathcal{C} \equiv \mathcal{P}^e \ mod \ p$, then $\mathcal{P} \equiv \mathcal{C}^d \ mod \ p$.

Example 8.11 Use the exponentiation cipher with $p = 29$ and $e = 3$ to encrypt the message MUSIC. Then, use the decryption process to show that correct plaintext is recovered.

Solution
Encryption

1. Replace each letter of the message MUSIC with its numerical equivalent from Table 8.3.

   12 20 18 8 2

2. Since $p = 29$ and $e = 3$, use the formula $\mathcal{C} \equiv \mathcal{P}^3 \ mod \ 29$ to obtain the numerical ciphertext $\mathcal{C}$ from each number $\mathcal{P}$ in the plaintext. The results of this process are shown in the table below.

Message	Plaintext, numerical ($\mathcal{P}$)	$\mathcal{P}^3$	Ciphertext $\mathcal{C} \equiv \mathcal{P}^3 \ mod \ 29$
M	12	1728	17
U	20	8000	25
S	18	5832	3
I	8	512	19
C	2	8	8

Thus, the ciphertext is 17 25 3 19 8.

Decryption

1. Begin with the ciphertext 17 25 3 19 8.
2. Find an integer d such that $3d \equiv 1 \ mod \ (29 - 1)$, or $3d \equiv 1 \ mod \ 28$. Notice that this congruence is asking for the inverse of 3 modulo 28, which does exist since $\gcd(3, 28) = 1$. Using the method of solving linear congruences from Section 6.3, or by trial and error, we find that $d \equiv 19 \ mod \ 28$.
3. To recover the plaintext, $\mathcal{P}$, for each ciphertext numerical equivalent, $\mathcal{C}$, use the decryption formula $\mathcal{P} \equiv \mathcal{C}^{19} \ mod \ 29$.
4. The table below shows the calculations along with the conversion from numerical plaintext to alphabetical plaintext.

Ciphertext	$\mathcal{C}^{19}$	Numerical plaintext $\mathcal{P} \equiv \mathcal{C}^{19} \ mod \ 29$	Alphabetical plaintext
17	239072435685151324847153	12	M
25	3637978807091712951660156250	20	U
3	1162261467	18	S
19	1978419655660313589123970	8	I
8	144115188075855872	2	C

◆

Exercise Set 8.3

Exercises 1–4. Find a value for the encryption exponent in the exponentiation cipher for the given value of p.

  1. $p = 17$
  2. $p = 29$
  3. $p = 43$
  4. $p = 53$

Exercises 5–8. Find the value of the decryption exponent in the exponentiation cipher for the given values of p and e.

  5. $p = 13, \ e = 5$
  6. $p = 47, \ e = 15$
  7. $p = 41, \ e = 9$
  8. $p = 71, \ e = 13$

  9. (a) Encrypt the message "SMILE" using the exponentiation cipher with encryption exponent $e = 5$ and modulus $p = 19$. (Since the largest numerical equivalent for this message is 18, a prime modulus of 19 is large enough.)

     (b) Find the decryption exponent, d, associated with $e = 5$ and $p = 19$. Use it to decrypt the ciphertext in part (a) to show the original plaintext is recovered.

10. (a) Encrypt the message "LEMON" using the exponentiation cipher with encryption exponent $e = 7$ and modulus $p = 17$. (Since the largest numerical equivalent for this message is $O = 14$, a prime modulus of 17 is large enough.)

    (b) Find the decryption exponent, d, associated with $e = 7$ and $p = 17$. Use it to decrypt the ciphertext in part (a) to show the original plaintext is recovered.

11. (a) Encrypt the message "SLY FOX" using the exponentiation cipher with encryption exponent $e = 5$ and modulus $p = 29$.

    (b) Find the decryption exponent, d, associated with $e = 5$ and $p = 29$. Use it to decrypt the ciphertext in part (a) to show the original plaintext is recovered.

12. The ciphertext **13 0 25 3 17 19 6** was created using an exponentiation cipher with $e = 7$ and $p = 31$. Verify that $d = 13$ is a valid decryption exponent and use it to decrypt the message. Use Table 8.3 to replace the numerical plaintext with letters.

8.4 Public Key Cryptography: The RSA Cryptosystem

All of the examples we have seen so far have been private key ciphers. This means that the encrypting key and the decrypting key are either the same or one can be used to find the other. Therefore, the keys must only be shared with the sender and intended recipient of the message. This creates the circular problem of somehow securely transmitting the key, so that the intended recipient will be able to decrypt the messages.

In a ***public key cryptosystem***, however, the encryption process can be publically shared, without jeopardizing the security of the codes produced using the encryption process. Public key cryptosystems were first invented in the 1970s. The most famous, called RSA, is named after its inventors Ronald **R**ivest (1948–present), Adi **S**hamir (1952–present), and Leonard **A**dleman (1945–present). Public key ciphers are vital to maintaining security, particularly in sending and receiving information over the Internet. For example, when you open a web page that asks you for a credit card number, the page's address begins with "https." The "s" indicates that you are using a secure server that encrypts your personal information. This encryption is done using the RSA encryption method. This modern application has its roots in number theory developed long before computers.

In the RSA encryption method (and other public key cryptosystems), there is both a public key and a private key. The public key is the encryption key, which contains all of the information necessary to encrypt information. The public key is completely public. It can be broadcast to both friends and enemies because it can only be used to encrypt information for the owner of the key. Even if one knows the entire RSA process for creating keys and encrypting and decrypting information, the knowledge of someone's public key does not lead to finding their private key.

The private key is the decryption key, which is kept a secret and contains all the information needed to decrypt information encrypted using the public key.

The information in the private key must be kept private, but it is not necessary to share the private key for people to encrypt information for you.

The security of the RSA encryption method is due to the surprising property that knowledge of the public (encryption) key does not lead to discovering the private (decryption key) and is based on the following fact:

> It is easy to find the product of two large numbers, but it is generally difficult to find the factors of a large number, particularly if it is the product of two large primes.

For example, if you are asked to find the product of 34141 and 28249 (two primes), with the help of a calculator, you can quickly compute that the answer is 970594489.

But, now suppose you are asked the reverse question: Can you factor the number 1321306601? Even with a calculator, it is not so simple. Even if you are told that the number is the product of two primes, it doesn't make the task much easier. We could use the Primality Test from Chap. 4 to reduce the number of factors that must be checked. Recall that only primes less than or equal to the square root of the number must be tested; however, in this case, $\sqrt{1321306601} \approx 36349.8$. This would be manageable on a computer, but if we start with primes that are hundreds of digits long, eventually even a powerful computer will not be able to test the possibilities fast enough to find the factors.

In the RSA cryptosystem, the person wishing to receive encrypted messages chooses very large values for two primes p and q which he or she keeps secret (These will be used to compute the private key). After multiplying them together, the product $m = pq$ can be revealed and is part of the public key used to encrypt information. In order to decrypt the message, the individual values of p and q are needed, but they cannot be found easily, even knowing m, when p and q are very large.

We will now proceed with the details of choosing the public and private keys for the RSA system, as well as the encryption and decryption formulas and a discussion of why the formulas work.

8.4.1   RSA Encryption and Public Keys

RSA encryption uses modular arithmetic and the fact that products of large primes are difficult to factor. The RSA public key includes two pieces of information: a number e, called the ***encryption exponent***, which is chosen by the person who knows the private key, and the modulus, m, which is the product of two very large primes, also chosen by the owner of the private key. These two numbers are frequently written as a pair, (e, m). In the RSA system, the person who wishes to receive encrypted information makes public the two numbers, e and m, so that anyone who wants to send encrypted information has access to them. This pair of values is called the ***public key***. We now explain the process of creating an RSA public key.

Creating an RSA Public (Encryption) Key

1. Choose two different large primes, p and q. (In actual practice, p and q would be primes with 150 digits or more.)
2. Let $m = p \cdot q$. (In an actual RSA key, m would have several hundred digits.)
3. Compute the value of the Euler phi function, $\phi(m)$. By Theorem 7.6,

$$\phi(m) = \phi(p \cdot q) = (p - 1)(q - 1).$$

4. Choose a positive integer e such that $\gcd(e, \phi(m)) = 1$.

Public Encryption Key: the pair of numbers (e, m) is the ***public encryption key***.

Note: the values of p, q, and $\phi(m)$ must not be revealed; they are not needed to encrypt information and knowing these values allows you to compute the private key used to decrypt coded information.

The following example illustrates the process of forming an RSA public key. To make computations possible, we are working with small primes in these examples.

Example 8.12 Create an RSA public key for the primes $p = 3$ and $q = 11$.

Solution
First, $33 = 3 \cdot 11$, so $m = 33$ in this example. Now, by Theorem 7.6 $\phi(33) = \phi(3 \cdot 11) = 2 \cdot 10 = 20$.
Then e is chosen so that $\gcd(e, 20) = 1$. There are many possibilities, each of which will result in a different public key. One choice is $e = 7$. In this case, the public key would be (7, 33).

◈

Once you have a public key, it can be used by anyone to encrypt a message using the following procedure.

RSA Encryption Method

1. Choose the public key (e, m) for the intended receiver of the message.
2. Convert the message into numerical equivalents. In the RSA method, each letter must be represented by the same number of digits, so each letter will be represented by two digits using the two-digit numerical in equivalents in Table 8.4.
3. Group the numerical plaintext into blocks of the same length so that the integer represented by each block is less than m. If the last block is not the same length as the rest, add some "dummy digits" onto the end to make all the blocks have the same length. Often, numerical equivalents of less

(continued)

(continued)

common letters such as Z or X are added to the last block if it needs to be longer.
4. Each block of plaintext, $\mathcal{B}$, is encrypted separately using the following encryption congruence:

$$\mathcal{C} \equiv \mathcal{B}^e \bmod m$$

where $\mathcal{C}$ is reduced modulo m and is the ciphertext representing $\mathcal{B}$.

Table 8.4 Numerical equivalents for RSA cryptosystem

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17

R	S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25	26

Example 8.13 Use the RSA cryptosystem with public key (3, 33) to encrypt the message GNUS.

Solution
1. Convert the message into numerical equivalents: $G = 07, N = 14, U = 21, S = 19$.
2. Since $m = 33$ in this example, each block of plaintext must be less than 33. Therefore, each block will consist of the numerical equivalent of one letter and will have length two.
3. Encrypt each block $\mathcal{B}$ using the formula

$$\mathcal{C} \equiv \mathcal{B}^3 \bmod 33$$

since $m = 33$ and $e = 3$. This will produce the numerical ciphertext. These steps are shown in the following table.

Plaintext	Plaintext ($\mathcal{B}$) (numerical)	$\mathcal{B}^3$	Ciphertext $\mathcal{C} \equiv \mathcal{B}^3 \bmod 33$
G	07	343	13
N	14	2744	5
U	21	9261	21
S	19	6859	28

Therefore, the ciphertext blocks are 13   05   21   28.

8.4.2   RSA Decryption and Private Keys

To recover the original message, we need the private or decryption key. If the public key is (e, m), here is the method for forming the private key.

Creating an RSA Private (Decryption) Key for Public Key (e, m):

1. Start with $m = p \cdot q$. (Note that m is public but p and q are not.)
2. Calculate $\phi(m) = \phi(p \cdot q) = (p-1)(q-1)$.
3. Find a positive integer d such that $d < \phi(m)$ and d is the inverse of e modulo $\phi(m)$. To do this, solve the congruence $d \cdot e \equiv 1 \bmod \phi(m)$ for d. Notice that this will always be possible since e was chosen so that gcd $(e, \phi(m)) = 1$.

Private (decryption) key: the pair of integers (d, m).

The private key is used to decrypt any messages sent to you that were encrypted using your public key.

Example 8.14 Find the private key for the public key $(3, 33)$, created using the primes $p = 3$, $q = 11$.

Solution
We must find the least residue d so that $d \cdot e \equiv 1 \bmod \phi(33)$. Substituting $e = 3$ and $\phi(33) = \phi(3 \cdot 11) = 20$ results in the congruence $3d \equiv 1 \bmod 20$. Since the modulus 20 is small, we can check values for d to find that $d = 7$. Therefore, the private key is $(7, 33)$.
◈

Now, here is the general decryption process.

RSA Decryption Method:
to decrypt a message encrypted with public key (e, m) using the private key (d, m).

1. Begin with the numerical ciphertext which needs to be decrypted.
2. Decrypt each block $\mathcal{C}$ of ciphertext separately using the following decryption formula, where $\mathcal{B}$ represents a numerical block of plaintext.

$$\mathcal{B} \equiv \mathcal{C}^d \bmod m$$

3. Once all blocks have been decrypted into numerical plaintext, replace each pair of numbers with the corresponding letter.

Example 8.15 Decrypt the ciphertext from Example 8.13, using the private key (7, 33).

Solution
The ciphertext is **13   05   21   28**. The decryption formula is

$$\mathcal{B} \equiv \mathcal{C}^7 \bmod 33$$

Where C is a block of ciphertext and $\mathcal{B}$ is a block of plaintext. The calculations are shown in the table below, using the numerical equivalents in Table 8.4 to find the plaintext.

Ciphertext, $\mathcal{C}$	$\mathcal{C}^7$	Plaintext, numerical $\mathcal{B} \equiv \mathcal{C}^7 \bmod 33$	Plaintext
13	62748517	07	G
5	78125	14	N
21	1801088541	21	U
28	13492928512	19	S

◈

Before going on to some more complicated examples, we will examine why the RSA encryption method works.

8.4.3   Why RSA Encryption Works

In this section we will examine why the decryption technique will always correctly return the original plaintext.

The RSA encryption process begins by choosing two (large) primes, p and q, and creating the public key (e, m). Then each block, $\mathcal{B}$, of plaintext is encrypted into ciphertext $\mathcal{C}$ using the relationship

$$\mathcal{C} \equiv \mathcal{B}^e \bmod m$$

To find the decryption key, the congruence below must be solved for d:

$$ed \equiv 1 \bmod \phi(m)$$

Since $\phi(m) = \phi(pq)$, applying the definition of congruence produces the following equation:

$$\phi(pq) \mid (ed - 1)$$

Therefore,

$$(ed - 1) = k\phi(pq)$$

Solving for ed,

$$ed = k\phi(pq) + 1$$

Here is where Euler's Theorem is used to verify that the decryption technique does actually reproduce the original plaintext. Recall the statement of Euler's Theorem (Theorem 7.10):

If $m > 0$ and $\gcd(m, a) = 1$, then $a^{\phi(m)} \equiv 1 \; mod \; m$.

Applying Euler's Theorem with $m = pq$ and $a = \mathcal{B}$,

$$\mathcal{C}^d \equiv (\mathcal{B}^e)^d \equiv \mathcal{B}^{k\phi(pq)+1} \equiv \mathcal{B}^{k\phi(pq)} \cdot \mathcal{B} \equiv \left(\mathcal{B}^{\phi(pq)}\right)^k \cdot \mathcal{B} \equiv 1 \cdot \mathcal{B} \equiv \mathcal{B} \; mod \; m$$

This shows that when the decrypting exponent, d, is applied to the ciphertext, we do in fact get back the plaintext $\mathcal{B}$.

This proves Theorem 8.2, stated below.

Theorem 8.2
Let p and q be different primes. Let $m = pq$, and let e be an integer such that $\gcd(e, \phi(m)) = 1$. Then, there is a positive integer d less than $\phi(m)$ such that $de \equiv 1 \; mod \; \phi(m)$, and if $\mathcal{B}$ and $\mathcal{C}$ are integers such that $\mathcal{C} \equiv \mathcal{B}^e \; mod \; m$, then $\mathcal{B} \equiv \mathcal{C}^d \; mod \; m$.

Note that Fermat's Little Theorem does not apply to this situation because we do not have a prime modulus. However, Euler's Theorem applies even when the modulus is composite. This is central to the RSA method. What would happen if we had an extremely large modulus, made up of the product of two huge primes, say 400 digits each? It is virtually impossible to find these two prime factors when we are only given their product. In fact, it is estimated that a modern computer would take longer than all of recorded history to find the two primes! Thus, we can only decrypt the message if we already know what these two primes are.

It is interesting at this point to note the importance of very large primes to modern cryptosystems. In fact, in 1994, computer programmer Roger Schlafly obtained US Patent 5,373,560 on two prime numbers that he discovered!

8.4.4   More Examples of the RSA Cryptosystem

The next two examples use a slightly larger pair of primes to illustrate how quickly the process gets complicated.

Example 8.16   Use the public key (77, 527) to encrypt the message: **W**.

Solution
1. Convert the plaintext **W** into a numerical equivalent. Using Table 8.4, **W** = 23, which is less than the modulus of 527.
2. The next task is to encrypt **W** using the encryption exponent $e = 77$. The ciphertext is

$$\mathcal{C} \equiv 23^{77} \bmod 527$$

3. Using the techniques for reducing large exponents from Chap. 6, we find that the ciphertext to be transmitted is $\mathcal{C} = 401$.   ◈

The numbers in Example 8.16 can be simplified using the techniques of Chap. 6, but for a longer message or even larger primes, this will become quite labor intensive. An online computational engine such as WolframAlpha (www.WolframAlpha.com) is very useful for longer problems of this type.

Example 8.17   The ciphertext **55   281   240   281** was created using the public key (77, 527) from Example 8.16. Decrypt the message to retrieve the original plaintext.

Solution
For the private key (d, m), the plaintext, $\mathcal{B}$, represented by a block of ciphertext, $\mathcal{C}$, can be found using the congruence

$$\mathcal{B} \equiv \mathcal{C}^d \bmod m$$

So, we just need to find d. To do this, solve the congruence $77d \equiv 1 \bmod \phi(527)$. Here, we run into trouble. We need the value of $\phi(527)$, but to compute it we need to know the prime factors of 527. According to the Primality Test from Chap. 4, we only need test primes less than or equal to $\sqrt{527} \approx 22.96$. Because the primes we are using are so small compared to those used in an actual RSA system, it is not a huge problem to check these values and find that $527 = 17 \cdot 31$. (In an actual public key, the value of m would be too large to alows us to compute p and q.) Therefore, $\phi(527) = 16 \cdot 30 = 480$, and to find d we must solve

$$77d \equiv 1 \bmod 480$$

This congruence has a solution since gcd(77, 480) = 1, and we can find it using the method of Section 6.3. Alternatively, a computational system such as WolframAlpha can be used to find the solution. After solving the congruence, we find that $d = 293$. Note that the decryption exponent, d, is large in comparison with the original prime factors of 527.

Now, the plaintext $\mathcal{B}$ for each block of ciphertext is found using the following congruence:

$$\mathcal{B} \equiv \mathcal{C}^{293} \bmod 527$$

Therefore, calculating the least residue modulo 527 of each block of the ciphertext, we obtain

$$55^{293} \equiv 21 \; mod \; 527$$
$$281^{293} \equiv 8 \; mod \; 527$$
$$240^{293} \equiv 15 \; mod \; 527$$
$$281^{293} \equiv 8 \; mod \; 527$$

(The calculations above were done using WolframAlpha.)

Therefore, the numerical plaintext is 21 08 15 08. Using Table 8.4, this corresponds to the message UH OH.

◈

Example 8.18 Given the primes 41 and 67 for an RSA encryption scheme,

(a) Find m and $\phi(m)$.
(b) Which of the following are valid encryption exponents: 7, 9, 15, 35, 49, 91?

Solution

(a) $m = 41 \cdot 67 = 2747$, and $\phi(m) = \phi(41 \cdot 67) = 40 \cdot 66 = 2640$ by Theorem 7.6.
(b) The encryption exponent e is chosen so that $\gcd(e, 2640) = 1$. To find out which of the given numbers are relatively prime to 2640, first write out the prime factorization of $2640 = 2^4 \cdot 3 \cdot 5 \cdot 11$. Therefore, the valid exponents are the numbers 7, 49, and 91. All the others share a factor with 2640 and therefore are not relatively prime to 2640.

◈

Example 8.19 Create two possible RSA public keys using the primes $p = 29$ and $q = 41$.

Solution

First, the value of m is $m = 29 \cdot 41 = 1189$. Now, the value of e is selected so that $\gcd(e, \phi(m)) = 1$. Since $\phi(m) = \phi(29 \cdot 41) = 28 \cdot 40 = 1120$, the value of e can be any integer relatively prime to 1120. The prime factorization of 1120 is $1120 = 2^5 \cdot 5 \cdot 7$, so e can be any positive integer that does not share any of these prime factors. Two possible choices for e are $e = 9$ or $e = 13$. These would produce the public keys (9, 1189) or (13, 1189).

◈

Example 8.20 After her first week of college, Penny is out of money. Her parents have provided her with their RSA public key for just this type of situation, so that there is no sibling rivalry. Help Penny by using the RSA method with public key (3, 2173) to encrypt the message SEND MONEY.

Solution

We start by using Table 8.4 to pair each letter of the message with its numerical equivalent:

19 05 14 04 13 15 14 05 25

Since $m = 2173$ in this example, blocks of length three will ensure that no block has a value larger than m. Therefore, the blocks of plaintext we will encrypt are listed below.

190 514 041 315 140 525

Now, apply the formula $\mathcal{C} \equiv \mathcal{B}^e \bmod m$ with $e = 3$ to each block to obtain the ciphertext.

$$190^3 \equiv 1012 \bmod 2173$$
$$514^3 \equiv 1628 \bmod 2173$$
$$41^3 \equiv 1558 \bmod 2173$$
$$315^3 \equiv 1616 \bmod 2173$$
$$140^3 \equiv 1674 \bmod 2173$$
$$525^3 \equiv 882 \bmod 2173$$

(These calculations were done using WolframAlpha.)
Therefore, the encrypted message to be sent out to Penny's parents is

1012 1628 1558 1616 1674 882

◈

Example 8.21   Penny's parents (of Example 8.20) have just received the encrypted message from Penny given in Example 8.20. Of course, they were not present when it was encrypted so they pull out their RSA private key (1387, 2173). Decrypt the message for them so they know what Penny needs.

Solution

Each block of the ciphertext sent by Penny can be decrypted using the congruence $\mathcal{B} \equiv \mathcal{C}^d \bmod m$, where $d = 1387$ is the decryption exponent included in the private key. Applying this to each block of Penny's ciphertext, we obtain the following results (using WolframAlpha).

$$1012^{2173} \equiv 190 \bmod 1387$$
$$1628^{2173} \equiv 514 \bmod 1387$$
$$1558^{2173} \equiv 41 \bmod 1387$$
$$1616^{2173} \equiv 315 \bmod 1387$$
$$1674^{2173} \equiv 140 \bmod 1387$$
$$882^{2173} \equiv 525 \bmod 1387$$

Therefore, the numerical blocks of plaintext are

190 514 041 315 140 525

Notice that the value 41 obtained from encrypting the third block of plaintext has a zero added in front since the blocks of plaintext all started with the same length.

Now, the numerical equivalents are two digits long, so we need to group the digits in pairs to convert back to the original plaintext message, using Table 8.4.

19	05	14	04	13	15	14	05	25
S	E	N	D	M	O	N	E	Y

This reveals Penny's message to her parents: SEND MONEY.

◆

Exercise Set 8.4

1. Does the encryption exponent e from the RSA public key have to be prime? Explain why or why not.
2. Can the encryption exponent e from the RSA public key be even? Explain why or why not.

Exercises 3–6. If the primes used for an RSA encryption scheme are $p = 31$ and $q = 97$, find the private key for each choice of the encryption exponent e given below.

3. $e = 7$
4. $e = 11$
5. $e = 13$
6. $e = 77$

Exercises 7–10. Find a public key and the corresponding private key for the primes p and q.

7. $p = 5, \quad q = 11$
8. $p = 13, \quad q = 43$
9. $p = 19, \quad q = 31$
10. $p = 17, \quad q = 23$

11. If an RSA public key is created using the primes $p = 13$ and $q = 17$, which of the following values are possible choices for the encryption exponent, e: 8, 9, 11, 25, 35, and 36?
12. Find the numerical plaintext, using the numerical equivalents from Table 8.4, for the message: STUDY HARD.
13. Find the numerical plaintext, using the numerical equivalents from Table 8.4, for the message: HARD WORK PAYS OFF.
14. Using RSA encryption with primes 43 and 73, and encryption exponent $e = 5$, encrypt the following message: HAPPY.
15. Using the public key (77, 527) from Example 8.16, encrypt the message YES.
16. After decrypting a message, the following blocks of numerical plaintext were obtained. Use them to retrieve the original message. (Hint: Remember that the plaintext blocks all started out with the same length. See Example 8.21.)
    Plaintext: 161 518 32 116 91 405

17. You received the encrypted message **413 240**. Decrypt the message if your private key is (53, 527).
18. A person with RSA private key (103, 287) received the encrypted message **199 62 100 276**. Decrypt the message to find the original plaintext.
19. A person with RSA private key (7, 33) received the encrypted message **13 9 13 24 26 26 5**. Decrypt the message using their private key.

8.5   Summary and Review Exercises

8.5.1   Vocabulary and Symbols

cipher	encryption method
plaintext	decrypt
ciphertext	decode
cryptography	decryption method
cryptology	keyword
cryptanalysis	private key
cryptogram	public key
Caesar ciphers	private key cryptography
Vigenère ciphers	public key cryptography
encrypt	Substitution cipher
encode	RSA encryption method

8.5.2   Suggested Readings

Diffie, Whitfield and Susan Landau. *September 11th Did Not Change Cryptography Policy*. **Notices of the American Mathematical Society.** Vol. 49 (April, 2002); 448–464.

Fried, John J. *Can you keep a SECRET?* **The Philadelphia Inquirer**, tech. life section, p. F1–F2.

Kirsch, Rachel. *Cryptography: How to keep a secret*. **MAA Focus**, February/March 2011. **www.maa.org/pubs/focus.html**

Poe, Edgar Allan. "The Gold Bug." *Edgar Allan Poe: Complete Tales and Poems*. Edison, NJ: Castle Books, November, 2009. 75–99.

8.5.3   Review Exercises

1. Use the Caesar cipher to encrypt the plaintext: ATTACK AT DAWN.
2. Use the Caesar cipher to decrypt the ciphertext: WKHUH LV QRWKLQJ WR IHDU.

3. Decrypt the following message, encrypted using a Vigenère cipher with key-word SECRET: MMNVRV WMUXSD VIP.
4. Use the exponentiation cipher with $p = 41$ and $e = 9$ to encrypt the message PEACHY.
5. The ciphertext **42 26 22 21 42 48 15 7** was encrypted using the exponentiation cipher with $e = 7$ and $p = 53$. Find the decryption exponent, d, and use it to decrypt the message and recover the plaintext (Use Table 8.3 for numerical equivalents).
6. Find the numerical plaintext for the message FERMAT using the numerical equivalents in Table 8.4. Then, encrypt this message using the RSA public key (11, 29).

Exercises 7–10. Create RSA public and private keys using the primes p and q.

7. $p = 5$, $q = 11$
8. $p = 11$, $q = 23$
9. $p = 3$, $q = 41$
10. $p = 5$, $q = 37$

11. Decrypt the ciphertext **10   1   16   16   2   1   9   49   24** which was encrypted using the RSA method, if the private key is (23, 55).

Exercises 12–17. Suppose $p = 59$ and $q = 71$ are used for an RSA encryption system. Is the number a value encryption exponent, e, for the RSA public key?

12. 7
13. 9
14. 15
15. 35
16. 49
17. 91

18. Suppose $p = 47$, $q = 61$, and $e = 7$ for an RSA encryption system. Encrypt the message CODE RED with two letters represented in each block of plaintext. Use Table 8.4 for the numerical equivalents.
19. The cipher text **845 1065** was encrypted in two-letter blocks using the RSA method. Use the private key (11, 3127) to decrypt the message. Use Table 8.4 to convert the numerical plaintext to letters.
20. The RSA public key (13, 2911) was created using the primes $p = 71$ and $q = 41$.

   (a) Confirm that $e = 13$ is a valid choice for this public key.
   (b) Encrypt the message CARTWHEEL using the public key.
   (c) Find the private key for this public key.
   (d) Decrypt the message **510 2069 700 2528**. (The plaintext was grouped in blocks of two letters each before it was encrypted.) Use Table 8.4 to convert the numerical plaintext to letters.

The Whole Truth About Whole Numbers

An Elementary Introduction to Number Theory

Sylvia Forman and Agnes M. Rash

The publisher regrets the errors in the print and online versions of this book. The correct versions are given below.

p. 56, Exercise #59 should refer to Theorem 2.4 in both (a) and (b), and not Theorem 2.3.

p. 61, Exercise #21 is false as written. The question should read: Prove that the sum of any three odd integers is an odd integer.

p. 61, Exercise #15 should specify that n has exactly 6 *positive* divisors.

p. 196, Exercise #18 should say "the ISBN number" and not the UPC code.

p. 207, Exercise #14 is false, as written. The problem should read:
 Prove that if $p > 3$ is prime, then $2 (p - 3)! \equiv -1 \ mod \ p$.

p. 226, Exercise #6 should be: Use Euler's Theorem to prove Fermat's Little Theorem: If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \ mod \ p$.

p. 255, Exercise #3 has the incorrect ciphertext. The ciphertext should be:
$$\textbf{KMNVRV WMUXSE VIP}$$

p. 255, Exercise #5 has the incorrect ciphertext. The ciphertext should be:
$$\textbf{42 2 6 22 21 42 48 15 7}$$

Corrections to "Answers to Odd Exercises" beginning on p. 257

p. 257, **Section 1.2, #3**: The correct answer is: first: Leonard; second: Carl; third: Niels, fourth: Bernhard

p. 258, **Section 2.3, #25**: The correct answer is: Nine is not a prime number and two is not an even number. False.

p. 259, **Section 2.3, #43**: The correct answer is: a: two even integers are added. s: their sum is even. $a \Rightarrow s$. Alternate form: p: a is even, q: b is even, r: the sum is even. $(p \wedge q) \Rightarrow r$.

p. 261, **Section 2.8, #29**: The correct answer is 1.

p. 261, **Section 2.8, #59**: The theorem should be Theorem 2.4 and not Theorem 2.3.

p. 261, **Section 2.8, #71**: The correct answer is: undefined.

p. 262, **Section 2.10.3, #23**: The hint should read: If a and $a + 1$ are consecutive integers, look at the case when a is even and the case when a is odd.

p. 266, **Section 4.6.3, #17(b)**: The correct answer is 41580.

p. 268, **Section 5.5, #11**: The correct answer is $x = -13$, $y = 13$.

p. 270, **Section 6.5, #9**: The formulas given here are from Theorem 6.11 instead of Theorem 6.12. The correct hint is: Substitute the formula $z = a_1 m_2 m_3 x_1 + a_2 m_1 m_3 x_2 + a_3 m_1 m_2 x_3$ into each of the three congruences. Remember that $m_2 m_3 x_1 \equiv 1 \ mod \ m_1$, $m_1 m_3 x_2 \equiv 1 \ mod \ m_2$, $m_1 m_2 x_3 \equiv 1 \ mod \ m_3$.

p. 271, **Section 6.6.3, #7**: The correct answer is 1.

p. 272, **Section 6.6.3, #17**: The correct answer is $x = 53 \ mod \ 56$.

p. 271, **Section 7.2, #1**: The solution should read: $(5 - 1) \ ! = 4! = 24$, and $24 \equiv -1 \ mod \ 5$, since $24 - (-1) = 25$ and $5|25$.

p. 272, **Section 7.4, #7**: The correct theorem is Theorem 7.6, not Theorem 6.6.

p. 272, **Section 7.5, #3**: The correct theorem is Theorem 7.8, not Theorem 6.8.

p. 272, **Section 7.5, #11**: The correct Example is Example 7.19, not Example 6.19.

p. 272, **Section 8.3, #9**: The correct answer is: 18 8 12 7 17.

p. 272, **Section 8.3, #11**: The correct answer is: 15 14 7 22 19 25.

Answer to Odd Exercises

Section 1.2

 1. 135, 153, 315, 351, 513, 531
 3. first: Carl; second: Leonard; third: Niels; fourth: Bernard
 5. 92
 7. 26
 9. 71
11. 8 nickels, 24 dimes
13. 33 house numbers
15. Start both timers at the same time; when the 4 minute timer runs out there are three minutes left on the 7 minute timer.
17. in 18 years, 1999

Section 2.1

 1. 8 is even since $8/2 = 4$; 7 is not since $7/2 = 3.5$
 3. 24 is divisible by 8 since $24/8 = 3$; 12 is not divisible by 8 since $12/8 = 1.5$
 5. 14 is an integer
 7. 4/3 is not an integer
 9. $81 \in \mathbb{Z}$
11. $2/5 \notin \mathbb{Z}$
13. not prime, $63 = 7(9)$
15. prime
17. not prime, $511 = 7(73)$
19. not perfect
21. many possible answers, for example: 29, 31; 41, 43; 71, 73
23. $20 = 3 + 17$

Section 2.2

1. inductive
3. deductive
5. inductive
7. inductive
9. (a) pairs of even integers; (b) all the sums are even; (c) The sum of two even integers is even.
11. (a) each pair has one even and one odd integer; (b) all the sums are odd; (c) The sum of an even and an odd integer is odd.
13. (a) each pair has one even and one odd integer; (b) each product is even; (c) The product of an even and an odd integer is even.
15. The product of two even integers is even.
17. The product of three odd integers is odd.
19. 6, 7, 8, . . .
21. 13, 21, 34, . . .

Section 2.3

1. statement
3. not a statement
5. not a statement
7. statement
9. Original statement: true. Negation: A triangle does not have three sides: false.
11. Original statement: look out the window for truth values. Negation: Today it is not sunny outside.
13. Original statement: false. Negation: All amphibians swim: true.
15. Original statement: false. Negation: Some dogs are not friendly: true.
17. Original statement: true. Negation: Two is not a factor of six, or three is not a factor of six: false.
19. FRANKLINS
21. Two is an even number and nine is not a prime number. True.
23. Two is an even number and n is an odd number. True if n is odd, false if n is even.
25. Two is an even number and six is a multiple of 3. True.
27. Two is an even number or nine is not a prime number. True.
29. Two is an even number or n is an odd number. True (compare to #23).
31. Nine is not a prime number or two is not an even number. True.
33. (a) If the last digit of n is 0, then n is even. True. (b) If n is even, then the last digit of n is 0. False, for example 12 is even. (c) False.

35. (a) If a is divisible by 3 then a is odd. False, for example 18 is divisible by 3 and even. (b) If a is odd then a is divisible by 3. False, for example 5 is odd and not divisible by 3. (c) True.

37. False.

39. False.

41. True.

45. m: two even integers are multiplied; p: their product is an even integer; $m \Rightarrow p$.

47. The number three is not prime or there are not 12 months in a year.

49. The integer a is not odd and the integer b is not odd. (Alternatively: The integer a is even and the integer b is even.)

Section 2.4

1. must be in $\mathbb{Z}$ since $\mathbb{Z}$ is closed under addition

3. not necessarily in $\mathbb{Z}$ since $\mathbb{Z}$ is not closed under division

5. never in $\mathbb{Z}$

7. must be in $\mathbb{Z}$ since $\mathbb{Z}$ is closed under multiplication and addition

9. not necessarily in $\mathbb{Z}$ since $\mathbb{Z}$ is not closed under division

11. many possible answers

13. odd, $-25 = 2(-13) + 1$, and $-13 \in \mathbb{Z}$.

15. even, $-34 = 2(-17)$, and $-17 \in \mathbb{Z}$.

17. even, $2 = 2(1)$, and $1 \in \mathbb{Z}$.

19. could be even or odd

21. odd; $2a + 2b + 3 = 2(a + b + 1) + 1$ and $a + b + 1 \in \mathbb{Z}$ since $\mathbb{Z}$ closed under addition.

23. odd; $4b + 1 = 2(2b) + 1$, and $2b \in \mathbb{Z}$ since $\mathbb{Z}$ is closed under multiplication.

25. even; $2a + 4ab + 4 = 2(a + 2ab + 2)$, and $a + 2ab + 2 \in \mathbb{Z}$ since $\mathbb{Z}$ is closed under addition and multiplication.

Section 2.5

1. $2(m + 2k)$

3. $2(k + 1)$

5. $4k + 2$

7. $4k^2 + 4k + 1$

9. $6k = 2(3k)$ and $3k \in \mathbb{Z}$

11. $4k + 2 = 2(2k + 1)$ and $2k + 1 \in \mathbb{Z}$

13. $2m + 2n + 1 = 2(m + n) + 1$ and $m + n \in \mathbb{Z}$

15. $2k + 5 = 2(k + 2) + 1$ and $k + 2 \in \mathbb{Z}$

17. (a) John is not delivering the truck. (b) You did not get a C.

Section 2.6

1. If she does not wear it, then the shoe did not fit. False.
3. If you did not try again, then you did succeed at first. Truth value depends on your experience.
5. If 2 does divide n, then n is odd. False.
7. If p is not prime, then p is not odd. False.
9. Try an indirect proof.

Section 2.7

There are multiple possible counterexamples for most of these statements. One example is given for each question.

1. A student starting college ten years after graduating from high school will be over 22 for at least part of their college career.
3. The authors of this textbook both have college degrees; unfortunately neither is a millionaire (yet).
5. 3 and 5 are two odd numbers; however their sum is $3 + 5 = 8$, an even number
7. If $a = 3$ and $b = 5$, then the sum $3 + 5 = 8$ is even; but neither 3 nor 5 is even.
9. The numbers 2 and 5 are both prime, but their sum is $2 + 5 = 7$, which is odd, not even.
11. The numbers 2 and 11 are both prime, but their difference is $11 - 2 = 9$, which is odd, not even.
13. The integer 18 is a multiple of 6 since $6(3) = 18$; 18 is not a multiple of 12 since $12(1.5) = 18$ and $1.5 \notin \mathbb{Z}$.

Section 2.8

1. $8 | 24$
3. $5 | 70$
5. True.
7. True.
9. True.
11. False.
13. True, since $63 = 7(9)$.
15. True, since $3426 = 2(1713)$.
17. False, since $18 \neq 0 \cdot a$ for any integer a.
19. True, since $4n + 2 = 2(2n + 1)$ and $2n + 1 \in \mathbb{Z}$.
21. False.
23. True.

25. Several possible answers; $d = 4, 5, 10, 20$.

27. (a) If m is divisible by 4, then m is even.

29. 2

31. 15

33. 3

35. 18

37. 5

39. 2730

41. 167,739

43. 268

45. 17,955

47. 11,242

49. 1190

51. Many possible counterexamples; one example: $a = 6, \ b = 8$.

53. Hint: use the definition of divides to rewrite given information and the conclusion.

55. Hint: use the definition of divides to rewrite the conclusion.

57. False.

59. (b) Hint: which statement in the proof of Theorem 2.3 is false if $a = 0$?

61. If $a = b$ or $a = -b$.

63. Hint: Three consecutive even integers can be written as $2n, \ 2n + 2, \ 2n + 4$.

65. Hint: Use the definition of divides to rewrite the conclusion.

67. Hint: Use the definition of divides to rewrite the given information and the conclusion.

69. (a) conjecture: $\gcd(a, b) \cdot lcm(a, b) = ab$.

71. 0

Section 2.9

1. yes

3. yes

5. yes

7. no

9. no

11. (a) If n is divisible by 2 then n is divisible by 6. False. One counterexample is $n = 14$; (b) If n is divisible by 6 then n is divisible by 2. True; (c) False.

13. (a), (d)

15. False.

17. True.

19. False.

21. False.

23. Yes.

Section 2.10.3: Review Exercises

1. if and only if, and, or, if...then, not, integers
3. $a|b$ represents the phrase "a divides b" and is either true or false. a/b represents the number resulting from dividing a by b.
5. If 2 does divide n then n is not odd.
7. If ab is not divisible by 4 then a is not even or b is not even.
9. If n is not prime then n is not odd.
11. (a) gcd(216, 288) = 72; lcm(216, 288) = 864); (c) gcd(234, 233) = 1; lcm(234, 233) = 54522
13. $d = 20, 60, 100, 300$
15. 12
17. Hint: Show that the divisors of a also divide $-a$, and the divisors of $-a$ also divide a. Similarly for multiples.
19. Hint: Use the definition of divides to rewrite the premises and conclusion.
21. Hint: Three odd integers can be written as $2k+1$, $2l+1$, $2m+1$.
23. Hint: Two consecutive even integers can be written as $2k+2$ and $2k+4$.
25. Hint: If p and q are consecutive primes and $p+q = 2r$, how will the size of r compare to p and q?

Section 3.1

1. $a = \sqrt{95} \approx 9.7$
3. $c = \sqrt{61} \approx 7.8$
5. $b = 3$
7. If $a^2 + b^2 \neq c^2$ then a and b are not the two legs of a right triangle **or** c is not the length of the hypotenuse.
9. yes, by converse
11. yes, by converse
13. no, by contrapositive
15. (a) $27^2 + 36^2 = 2025$ and $45^2 = 2025$; (b) many possible answers; for example, $54 - 72 - 90$ and $9 - 12 - 15$.
17. (a) $27^2 + 32^2 = 1600$, and $40^2 = 1600$; (b) $12 - 16 - 20$, $6 - 8 - 10$, $3 - 4 - 5$; (c) many possible answers, for example $240 - 320 - 400$
19. many possible answers, for example, starting with $3 - 4 - 5$ and multiplying each side by 55 produces $165 - 220 - 275$.
21. 5
23. 2
25. 1
27. 3
29. 3

31. The triple $a - b - c$ is a Pythagorean triple if and only if $ka - kb - kc$ is a Pythagorean triple for positive integers k.

33. Hint: Look at the proof of Theorem 3.2.

35. Hint: Try a proof by contradiction—suppose that $\gcd(a, b, c)$ is an integer not equal to d.

Section 3.2

1. yes

3. no

5. no

7. only $9 - 40 - 41$

9. $15 - 8 - 17$

11. $21 - 20 - 29$

13. no

15. yes

17. no

19. many possible answers, for example $a = 6$, $b = 15$, $c = 10$.

21. $27 - 364 - 365$

23. $s = 11$, $t = 1$, $11 - 60 - 61$

25. $s = 63$, $t = 1$, $63 - 1984 - 1985$; $s = 9$, $t = 7$, $63 - 16 - 65$

27. $s = 45$, $t = 1$, $45 - 1012 - 1013$; $s = 9$, $t = 5$, $45 - 28 - 53$

29. $s = 9$, $t = 1$

31. Hint: Look at the relationship between side b and side c.

33. yes

35. many possible answers, for example $119 - 120 - 169$

37. $3 - 4 - 5$; $5 - 12 - 13$; $7 - 24 - 25$; $9 - 40 - 41$; $11 - 60 - 61$; $13 - 84 - 85$; $15 - 112 - 113$; $17 - 144 - 145$; $19 - 180 - 181$; $15 - 8 - 17$

39. Hint: Use the primitive Pythagorean formulas.

41. Hint: There are two things to show: first that $(s^2 - t^2)/2$ is positive and second, that it is an integer.

Section 3.4.3: Review Exercises

1. $a - b - c$ is a Pythagorean triple, where a and b represent the legs of the right triangle and c is the hypotenuse.

3. The triple represents the lengths of the three sides of the triangle.

5. (a) $s = 17$, $t = 7$; (b) $s = 23$, $t = 3$; (c) $s = 13$, $t = 1$; (d) $s = 9$, $t = 5$

7. Many possible answers, for example $780 - 1040 - 1300$.

9. Hint: If side a is an odd number, $a \geq 3$, then find s and t in the PPT formulas that produce a side of length a.

11. two; $45 - 28 - 53$; $45 - 1012 - 1013$

13. $31 - 480 - 481$

Section 4.1

1. (a) 2 (b) 3

3. 11

5. 19

7. prime

9. composite $517 = 11 \cdot 47$

11. prime

13. composite $119 = 7 \cdot 17$

15. composite $361 = 19^2$

17. composite $213 = 3 \cdot 71$

19. composite $754 = 2 \cdot 377$

21. composite $441 = 3 \cdot 147$

23. prime

25. 997 is prime using the Primality Test: no prime less than or equal to 31 divides it; $7429 = 17 \cdot 437$.

27. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67

29. dimensions are 25 rows by 10 columns; must cross off all multiples of 2, 3, 5, 7, 11 and 13.

Section 4.2

1. If 1 were a prime, then each number would have prime factorizations of many different lengths, by adding more factors of 1: $6 = 2 \cdot 3 = 2 \cdot 3 \cdot 1 = 2 \cdot 3 \cdot 1 \cdot 1 = \ldots$.

3. 1, 2, 5, 7, 4, 10, 14, 35, 20, 28, 70, 140

5. $3^2 \cdot 5 \cdot 7$

7. $17 \cdot 19 \cdot 23$

9. not prime; $3649 = 41 \cdot 89$

11. p^2, where p is prime

13. $1, p, p^2, p^3$

15. 2

17. 11

19. $2^2 \cdot 3^2 \cdot 5 \cdot 7 = 1260$

21. many possible solutions; for example $a = 14 \cdot 11^2 = 1694$, $b = 14 \cdot 17^2 = 4046$

23. many possible solutions; for example, 11 or 143

25. many possible solutions; for example, 7

27. many possible solutions; for example, 2, 5 or 10

29. Hint: Find several least common multiples using prime factorizations and look for a pattern.

31. In the proof, $c = p_1^{c_1} \cdot p_2^{c_2} \cdot \cdots \cdot p_k^{c_k}$. Squaring both sides, $c^2 = \left(p_1^{c_1} \cdot p_2^{c_2} \cdot \cdots \cdot p_k^{c_k}\right)^2$

$= \left(p_1^{c_1} \cdot p_2^{c_2} \cdot \cdots \cdot p_k^{c_k}\right) \cdot \left(p_1^{c_1} \cdot p_2^{c_2} \cdot \cdots \cdot p_k^{c_k}\right)$

$= \left(p_1^{c_1} \cdot p_1^{c_1}\right) \cdot \left(p_2^{c_2} \cdot p_2^{c_2}\right) \cdot \cdots \cdot \left(p_k^{c_k} \cdot p_k^{c_k}\right) = p_1^{2c_1} \cdot p_2^{2c_2} \cdot \cdots \cdot p_k^{2c_k}$

33. many possible answers, for example, $s = 8$, $t = 12$.

35. Conjecture is true.

Section 4.3

1. Same as proof that the difference and product of two evens is even, but the quotient of two evens need not be an even integer.

3. *Odd*$\mathbb{Z}$ is only closed under $\cdot$

5. (a) 3, 6, 12, 15, 21, 24, 30, 33, 39, 42

(b) $3\mathbb{Z}$ does not have unique factorization into primes; for example, $36 = 3 \cdot 12 = 6 \cdot 6$.

Section 4.5

1. (a) $11! + 2$, $11! + 3$, $11! + 4$, ..., $11! + 11$

(b) primes can be spaced any distance apart

3. Test the conjecture with values of n. The conjecture is false.

5. 43 when $n = 3$

7. test using examples

9. test using examples

11. can prove false

13. test using examples

15. can prove false

17. (a) $26 = 13 + 13$, $40 = 37 + 3$; (b) $60 = 7 + 53 = 13 + 47 = 17 + 43 = 19 + 41 = 23 + 37 = 29 + 31$; (c) Trying each prime less than or equal to 11, the second summand needed to produce 11 is never prime: $11 = 2 + 9 = 3 + 8 = 5 + 6 = 7 + 4 = 11 + 0$.

Section 4.6.3: Review Exercises

1. 2, 3, 5, 7, 11, 13, 17, 19

3. $3^2 \cdot 5 \cdot 7 \cdot 11$

5. $5 \cdot 11^2 \cdot 13$

7. $2 \cdot 3 \cdot 5 \cdot 1163$

9. 11^4

11. $2^4 \cdot 3^3 \cdot 31$

13. composite

15. composite

17. (a) 66; (b) 49896

19. Look for a pattern in the results in part (b)

21. $1, p, q, pq$

23. (a) 22l; (b) 9256500

25. 45

27. 92

29. 48

31. 1833300

33. 105800

35. 288

Section 5.1

1. quotient is 40; $160 = 40(4) + 0$

3. quotient is 4; $28 = 4(7) + 0$

5. quotient is 0; $9 = 0(18) + 9$

7. quotient is 0; $6 = 0(8) + 6$

9. quotient is -3; $-34 = -3(12) + 2$

11. quotient is $2k$; $8k = 2k(4) + 0$

13. quotient is $k + 2$; $6k + 15 = (k + 2)6 + 3$

15. Since 7 is the number of days in a week and 12 is the number of months in the year, the remainder of a number when divided by 7 will tell you the day of the week it will be that many days from now. The remainder of a number when divided by 12 will tell you what month it will be that many months from now.

17. possible remainders are 0, 1, 2; Remainder 0: 0, 3, 6,. . .; Remainder 1: 1, 4, 7; Remainder 2: 2, 5, 8,. . .. There are several different patterns. One example is that on each list the numbers are three apart.

19. $m = q \cdot 5 + 4$

21. (a) all evens have remainder 0 and all odds have remainder 1; (b) many possible answers, for example 202; (c) many possible answers, for example 403

23. Prove by showing one case holds true when n is even and the other holds true when n is odd.

Section 5.2

1. 231, Euclidean Algorithm 1 step
3. 55, Euclidean Algorithm 3 steps
5. 15, Euclidean Algorithm 4 steps
7. 7, Euclidean Algorithm 5 steps
9. 6, Euclidean Algorithm 7 steps
11. 3, Euclidean Algorithm 7 steps
13. (a) Conjecture: $\gcd(m, m + 1) = 1$;
　　(b) Using the Euclidean Algorithm,

$$m + 1 = 1(m) + 1$$
$$m = m(1) + 0$$

　　Therefore $\gcd(m, m + 1) = 1$.
15. Conjecture: $\gcd(2m + 1, 2m + 3) = 1$.
17. Let a be a positive integer, and $a|b$. Let $d = \gcd(a, b)$. Then, $d|a$ so $d \leq a$. Since $a|b$ and $a|a$, a is a common divisor of a and b. Since the *greatest* common divisor cannot be greater than a, it must be true that $a = \gcd(a, b)$.

Section 5.3

1. $231 = 0(693) + 1(231)$
3. $55 = 5(1265) - 6(1045)$
5. $15 = 56(345) - 9(2145)$
7. $7 = 24(1463) - 59(595)$
9. $6 = 168(72720) - 1373(8898)$
11. $3 = 39(123456) - 8867(543)$
13. $x = 5, \ y = -257$
15. $x = 1, \ y = 0$
17. Use the Euclidean Algorithm backwards to find a solution to $7x + 9y = a$, where a is any integer.
19. Use technique similar to hint given in number 18.
21. Many possible answers; one choice is $a = 4, \ b = 10, \ c = 20$.

Section 5.4

1. when $\gcd(a, b) = 1$
3. $x = -42, \ y = 1$
5. $x = 1, \ y = 0$
7. $x = -5, \ y = 3$

9. $x = 1$, $y = 0$

11. $x = 31 + 307n$, $y = -21 - 208n$, $n \in \mathbb{Z}$

13. $x = -1 + 46n$, $y = 1 - 45n$, $n \in \mathbb{Z}$

15. $x = -7 + 86n$, $y = 4 - 49n$, $n \in \mathbb{Z}$

17. $x = 1 - 49n$, $y = 2 - 99n$, $n \in \mathbb{Z}$

19. $x = 2 + 31n$, $y = -1 - 16n$, $n \in \mathbb{Z}$

Section 5.5

1. yes

3. no

5. no

7. yes

9. $x = 18$, $y = -30$

11. $x = -1$, $y = 1$

13. $x = -36$, $y = 36$

15. $x = 12$, $y = 8$

17. $x = 18 + 13n$, $y = -30 - 22n$, $n \in \mathbb{Z}$

19. $x = -1 + 98n$, $y = 1 - 97n$, $n \in \mathbb{Z}$

21. $x = -36 + 3n$, $y = 36 - 2n$, $n \in \mathbb{Z}$

23. $x = 12 - 7n$, $y = 8 - 5n$, $n \in \mathbb{Z}$

25. $x = -6 + 8n$, $y = 1 - n$; shortcut is that everything is a multiple of 8.

27. (a) choose a so that $gcd(a, 12) \nmid 21$; (b) choose a so that $gcd(a, 12)|21$

29. (a) many possible answers; one is $b = 9$; (b) many possible answers; one is $a = 12$; (c) many possible answers; one is $c = 32$

31. $c = 18$, or any integer divisible by 6.

33. 5 five gallon containers and 3 eight gallon containers

35. Suppose that $x = m$, $y = n$ is an integer solution to the equation $ax + by = c$. Since $d = gcd(a, b)$, $d|a$ and $d|b$. Therefore $a = dk$ and $b = dl$ for integers k and l, Substituting, since $am + bn = c$, we get that $dkm + dln = c$, or $d(km + ln) = c$. This is a contradiction since it was given that $d \nmid c$.

37. Substitute the equations for x and y into the equation $ax + by = c$.

Section 5.7.3: Review Exercises

1. 1

3. 5

5. 1

7. 15

9. (a) 66; (b) 10287; (c) 140250

11. (a) $x = 2 + 31n$, $y = -1 - 16n$; (b) no solution; (c) $x = -4 + 3n$, $y = 4 - 2n$

13. $x = 8$, $y = -15$

Section 6.1

1. true

3. false

5. false

7. $m = 1, 2, 3$ or 6

9. $m = 1, 2, 3, 4, 6,$ or 12

11. $b \equiv 1 \bmod 2$

13. $k \equiv 7 \bmod 11$

15. $a \equiv 0 \bmod 4$ or $a \equiv 2 \bmod 4$

17. $a \equiv 0 \bmod 4$

19. $m \not\equiv 0 \bmod 5$; alternatively $m \equiv 1 \bmod 5$ or $m \equiv 2 \bmod 5$ or $m \equiv 3 \bmod 5$ or $m \equiv 4 \bmod 5$.

21. many possible answers, for example $-4, -13, -22, 14, 23, 32$

23. many possible answers, for example 278

25. (a) 1; (b) 14; (c) 6; (d) 0

27. 0, 1, 2, 3, 4, 5, 6, 7, eight integers

29. 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

31. yes

33. Use the proof of Theorem 6.1 and the proof technique from Section 2.5

35. Use the proof of Theorem 6.3 and the proof technique from Section 2.5.

37. Hint: Use the definition of divides to rewrite the premise and conclusion.

39. Hint: Use the definition of congruence to rewrite the premise. Notice that $a - b = a + c - c - b$.

Section 6.2

1. (a) 2^{16}; (b) 4^{24}; (c) 3^{11}; (d) 5^{22}; (e) 3^{33}

3. $7^{151} \equiv 3 \bmod 10$

5. $3^{207} \equiv 6 \bmod 7$

7. $7 + 4(10)$

9. $4 + 3(10) + 2(100) + 1(1000)$

11. $9(10) + 8(100) + 7(1000) + 6(10000)$

13. 0

15. 7 *modulo* 11

17. Hint: Use the definitions of congruence and divides to rewrite the premise and conclusion.

19. Hint: Rephrase the divisibility test for 5 in terms of a congruence. Notice that $5|a$ is equivalent to $a \equiv 0 \bmod 5$.

Section 6.3

1. $x \equiv 1 \ mod \ 8$
3. $x \equiv 6 \ mod \ 13$
5. no
7. one incongruent solution
9. one incongruent solution
11. no solutions
13. four incongruent solutions
15. one incongruent solution
17. many possible answers, for example $x = 13, \ 29$
19. two incongruent solutions: $x = 2$, $x = 6$
21. one incongruent solution: $x = 3$
23. If $c = 6k$ for an integer k there are six incongruent solutions.
25. many possible answers, for example $9x \equiv 14 \ mod \ 23$.
27. many possible answers
29. 3 is its own inverse modulo 8; only integers congruent to $1, 3, 5,$ or 7 modulo 8 have inverses
31. If a is the inverse of 0 modulo m then $0 \cdot a \equiv 1 \ mod \ m$ which means that $m|1$. This is not possible since $m > 1$.

Section 6.4

1. Use the check-digit scheme for 10-digit ISBNs.
3. (a) no; (b) yes; (c) no; (d) yes
5. 13 digit ISBN, and it is valid
7. answers will vary
9. answers will vary

Section 6.5

1. no
3. yes
5. yes
7. $x \equiv 17 \ mod \ 24$
9. Substitute the formula $z = am_2x_1 + bm_1x_2$ into each congruence on the left side, and show that it simplifies to the right side. Remember that $m_2x_1 \equiv 1 \ mod \ m_1$ and $m_1x_2 \equiv 1 \ mod \ m_2$.
11. $z \equiv 3 \ mod \ 40$
13. $z \equiv 37 \ mod \ 42$

15. $z \equiv 40 \ mod \ 42$
17. $z \equiv 1 \ mod \ 105$
19. $z \equiv 23 \ mod \ 105$

Section 6.6.3: Review Exercises

1. no solutions
3. 1
5. no solutions
7. 9
9. Yes. See hint given with problem.
11. $x \equiv 11 \ mod \ 16$
13. 6
15. Hint: Use the definition of congruence to rewrite the premise and conclusion.
17. $x \equiv 53 \ mod \ 66$
19. 6
21. 0
23. 29
25. 0
27. 17

Section 7.2

1. $(5 - 1)! = 4$ and $24 \equiv -1 \ mod \ 5$ since $5|(24—1)$.
3. $p! = p(p - 1)!$
5. (a) 12; (b) 0; (c) 1; (d) 0
7. 22
9. 1
11. 14
13. Hint: Use Wilson's Theorem and Exercise 3.
15. (a) Hint: Apply the definition of congruence; (b) 1; (c) -1
17. Hint: Use the definition of composite to rewrite m.

Section 7.3

1. (a) yes; (b) yes; (c) no; (d) no
3. 9
5. (a) $x \equiv 7 \ mod \ 11$; (b) there is a solution ($x \equiv 4 \ mod \ 9$) but Fermat's Little Theorem does not apply; (c) $x \equiv 6 \ mod \ 7$; (d) $x \equiv 7 \ mod \ 17$

Section 7.4

1. $n = 1, 2$
3. 32
5. many possible answers, for example $n = 11$, $m = 12$
7. Hint: Use Theorem 6.6.

Section 7.5

1. $d(1) = 1$
3. Hint: After trying some examples, look at Theorem 6.8.
5. all prime values of n
7. $\sigma(1) = 1$
9. Hint: Theorem 6.8. (Trying some specific examples might be a helpful way to start.)
11. Hint: Review Example 6.19.

Section 7.6

1. 9
3. 7
5. Hint: Notice that $a^{\phi(m)} = a \cdot a^{\phi(m)-1}$ and use Euler's Theorem.

Section 7.7.3: Review Exercises

1. Many possible answers; for example, $a = 4$, $b = 6$.
3. 0
5. 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16
7. 0, 1, 5, 6
9. Hint: Use Fermat's Little Theorem.
11. Hint: Use Fermat's Little Theorem.
13. 1
15. 11
17. 2
19. 1
21. 1

Section 8.2

1. Hint: The first two words of the plaintext are "NEVER INJURE".
3. Hint: The last word of the plaintext is "NUMBERS".
5. Hint: The first three letters of the plaintext are "WHA".

Section 8.3

1. many possible answers; need $\gcd(e, 16) = 1$.
3. many possible answers; need $\gcd(e, 42) = 1$.
5. $d = 5$
7. $d = 9$
9. SIMHR
11. POHWTZ

Section 8.4

1. No
3. $d = 823$
5. $d = 2437$
7. answers will vary depending on public key
9. answers will vary depending on public key
11. 11, 25, 35
13. 08 01 18 04   23 15 18 11   16 01 25 19   15 06 06
15. 315 428 423
17. NO
19. Hint: The first two letters of the plaintext are "GO".

Section 8.5.3: Review Exercises

1. DWWDFN DW GDZQ
3. Hint: The first three letters of the plaintext are SIL.
5. $d = 15$. The first three letters of the plaintext are POR.
7. Many possible answers; for example, public key (17, 55) and private key (33, 55).
9. Many possible answers; for example, public key (21, 123) and private key (61, 123).

11. Hint: The first two letters of the plaintext are JA.

13. yes

15. no

17. no

19. Hint: the first block of plaintext is 0615.

Bibliography

Bell, E.T.: Men of Mathematics. Simon and Schuster, New York (1986)

Burckhardt, J.J.: Leonhard Euler, 1707–1783. Math. Mag. **56**, 262–273 (1983)

Colquitt, W.M., Welsh Jr., L.: A new Mersenne prime. Math. Comp. **56**, 867–870 (1991)

Cox, D.A.: Introduction to Fermat's last theorem. Am. Math. Mon. **101**, 3–14 (1994)

Crandall, R., Doenias, J., Norrie, C., Young, J.: The twenty-second Fermat number is composite. Math. Comp. **64**, 863–868 (1995)

Dalezman, M.: From 30 to 60 is not twice as hard. Math. Mag. **73**, 151–153 (2000)

Devlin, K.: World's largest prime. Focus (The newsletter of the Mathematical Association of America) **17**, 1 (1997)

Diffie, W., Landau, S.: September 11th did not change cryptography policy. Not. Am. Math. Soc. **49**, 448–464 (2002)

Dodge, C.W.: What is a proof? Pi Mu Epsil. J. **10**, 725–727 (1998)

Doxiadis, A.: Uncle Petros and Goldbach's Conjecture: A Novel of Mathematical Obsession. Bloomsbury, USA. 2001.

Fried, J.J.: Can you keep a SECRET? The Philadelphia Inquirer, tech. life section, F1–F2 (1998)

Gallian, J.S.: The mathematics of identification numbers. Coll. Math. J. **22**, 194–202 (1991)

Granville, A.: Prime number patterns. Am. Math. Mon. **115**, 279–296 (2008)

Guy, R.K.: Nothing's new in number theory? Am. Math. Mon. **105**, 951–954 (1998)

Irwin, Jim.: Student Finds Largest Known Prime Number. www.ucs.louisiana.edu/~ras277/methods/primenumber.htm

Kahn, D.: The Code Breakers. Macmillan, New York (1967)

Khovanova, T.: A story of storytelling numbers. Math Horizons. Also at www.maa.org/mathhorizons(2009). 14–17

Kirsch, R.: Cryptography: How to keep a secret. MAA Focus. www.maa.org/pubs/focus.html (February/March 2011)

Lamport, L.: How to write a proof. Am. Math. Mon. **102**, 600–608 (1995)

Marchall, D.C., Odell, E., Starbird, M.: Number Theory Through Inquiry. McGraw Hill, New York (2007)

Osen, L.M.: Women in Mathematics. MIT Press, Cambridge (1975)

Plummer, P.: Divisibility tests for primes greater than 5. Pi Mu Epsil. J. **10**, 96–98 (1995)

Polya, G.: How to Solve It. Pearson, New York (2009)

Pomerance, C.: The search for Primes. Sci. Am. **247**, 136–147 (1982)

Ribenboim, P.: The Little Book of Primes. Springer, New York (1991)

Robinson, R.M.: Mersenne and Fermat numbers. In: Proceedings of the American Mathematical Society, Washington, DC, pp. 842–846. (1954)

Schwartz, R.E.: You Can Count on Monsters. A. K. Peters, Natick (2010)

Silverman, J.H.: A Friendly Introduction to Number Theory, 4th edn. Pearson, New York (2013)

Snapp, B., Chris, S.: Automotive number theory. Math Horizons. Also at www.maa.org/mathhorizons (2009). 26–27

Tanton, J.: A dozen questions about the powers of two. Math Horiz. **9**, 5–10 (2001)

Vanden Eynden, C.: Introduction to Number Theory. McGraw Hill, New York (2006)

Index