the Art of Problem Solving

Introduction to Number Theory

Mathew Crawford

2nd Edition

the Art of Problem Solving

Introduction to Number Theory

The Art of Problem Solving Introduction Series constitutes a complete curriculum for outstanding math students in grades 6-10. The books in the series are:

Introduction to Algebra by Richard Rusczyk
Introduction to Counting & Probability by David Patrick
Introduction to Geometry by Richard Rusczyk
Introduction to Number Theory by Mathew Crawford

Together these books give students a solid background in basic problem-solving mathematics and prepare them for prestigious competitions such as MATHCOUNTS and the American Mathematics Competitions.

Praise for **Introduction to Number Theory**

"Thank you so much for Introduction to Number Theory. I have thoroughly enjoyed this book. It has introduced me to math that I would never have discovered on my own...I have learned to not only do problems I thought were impossible, but I have learned to enjoy them."
10th grade student, Alabama

Mathew Crawford is the founder and CEO of MIST Academy, a school for gifted students, in Birmingham, Alabama. He is a former instructor and curriculum developer for the Art of Problem Solving online school. He is co-author of Art of Problem Solving's Intermediate Algebra textbook, and served on the Board of Directors of the Art of Problem Solving Foundation. Crawford was a perfect scorer at the national MATHCOUNTS competition in 1990, and a member of the national championship team (Alabama) in 1991. He was a 3-time invitee to the Math Olympiad Summer Program, a perfect scorer on the AIME, and a 2-time USA Math Olympiad honorable mention.

ISBN 978-1-934124-12-3
90000 >
9 781934 124123

Introduction to Number Theory

2nd Edition

Mathew Crawford
Art of Problem Solving

Number Theory

What are integers? Which integers are interesting? What can we do with them? How do we use them? How do they relate to mathematics? How do we use them to count more easily? What numbers can we *make* with them? How do we use them to write secret messages? How do we use them to read secret messages? How do we use them to run computers? How do we use them to run computers *more efficiently*? How do they help us with physics? What do they have to do with biology? How do we use them to talk with our spacecrafts?

These are questions about the subject of **number theory**. **Number theory** is the study of integers. As ancient as number theory is, humans are still uncovering mysteries behind integers and learning to use them in powerful new ways.

Integers:	$\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots$
Natural Numbers:	$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots$
Prime Numbers:	$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$
Composite Numbers:	$4, 6, 8, 9, 10, 12, 14, 15, 16, \ldots$
Even Numbers:	$\ldots, -6, -4, -2, 0, 2, 4, 6, 8, 10, 12, \ldots$
Odd Numbers:	$\ldots, -7, -5, -3, -1, 1, 3, 5, 7, 9, 11, \ldots$
Perfect Squares:	$0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, \ldots$
Negative Cubes:	$-1, -8, -27, -64, -125, -216, -343, \ldots$
Powers of 2:	$1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, \ldots$
Abundant Numbers:	$12, 18, 20, 24, 30, 36, 40, 42, 48, 54, \ldots$
Palindromes:	$11, 313, 838, 3443, 7447, 57875, 10000001, \ldots$
Fibonacci Numbers:	$1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$
Base Numbers:	$1_9, 44_5, 154_6, 10110_2, 2A41_{12}, \ldots$
Modulo 8 Residues:	$0, 1, 2, 3, 4, 5, 6, 7$

Each of these types of integers has stories—some that go back thousands of years. Since we use integers to describe so many things, knowing these stories helps us understand the world around us.

NOTATION—WRITING IN THE LANGUAGE OF MATHEMATICS

Notations are the symbols we use when expressing an idea in writing. Mathematical notation is rich, complex, and highly useful—though often frustrating to students with less experience reading it or using it to write mathematics. Hopefully this book conveys mathematical ideas as simply as possible, and introduces new notations clearly and in a timely manner. However, we list here a number of the more common notations used throughout this book to give students a basic guide to understanding the language of mathematics as we use it for the next 300-something pages.

$$a \mid b$$

The vertical line is a symbol that denotes a relationship of divisibility. Instead of writing "a divides b," or "a is a divisor of b," we write "$a \mid b$." For example, "$6 \mid 24$," means "6 divides 24."

$$a \Rightarrow b$$

This double-right arrow means "implies." For instance, instead of writing "$x + 1 = 4$ implies that $x = 3$," we write "$x + 1 = 4 \Rightarrow x = 3$."

$$n!$$

When immediately following a positive integer, this "factorial" symbol lets us know to multiply the positive integer by all the positive integers less than it: $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$.

$$\gcd(a, b)$$

When we write $\gcd(a, b)$, we mean the greatest common divisor of the integers a and b. For instance, $\gcd(8, 12) = 4$.

$$\text{lcm}[a, b]$$

We write $\text{lcm}[a, b]$ to mean the least common multiple of the integers a and b. For instance, $\text{lcm}[8, 12] = 24$.

$$\max(a, b)$$

When the term "max" precedes a group of real numbers, it refers to the maximum of that group of real numbers. For instance, $\max(1, 2, 3, 5, 8) = 8$.

$$\min(a, b)$$

When the term "min" precedes a group of real numbers, it refers to the minimum of that group of real numbers. For example, $\min(1, 2, 3, 5, 8) = 1$.

$$a \equiv b \pmod{m}$$

When we write "$a \equiv b \pmod{m}$," we mean that a and b are congruent modulo m. In other words, the difference between a and b is a multiple of m. For instance, since $13 - 1 = 12$ and $6 \mid 12$, we say that $13 \equiv 1 \pmod{6}$. (Note: We begin discussing modular arithmetic in Chapter 12.)

How to Use This Book

Learn by Solving Problems

This book is probably very different from most of the math books that you have read before. We believe that the best way to learn mathematics is by solving problems. Lots and lots of problems. In fact, we believe that the best way to learn mathematics is to try to solve problems that you don't know how to do. When you discover something on your own, you'll understand it much better than if someone just tells it to you.

Most of the sections of this book begin with several problems. The solutions to these problems will be covered in the text, but try to solve the problems *before* reading the section. If you can't solve some of the problems, that's OK, because they will all be fully solved as you read the section. Even if you solve all of the problems, it's still important to read the section, both to make sure that your solution is correct, and also because you may find that the book's solution is simpler or easier to understand than your own.

If you find that the problems are too easy, this means that you should try harder problems. Nobody learns very much by solving problems that are too easy for them.

Explanation of Icons

Throughout the book, you will see various shaded boxes and icons.

Concept:	This will be a general problem-solving technique or strategy. These are the "keys" to becoming a better problem solver!

Important:	This will be something important that you should learn. It might be a formula, a solution technique, or a caution.

WARNING!!	Beware if you see this box! This will point out a common mistake or pitfall.

Game: Remember, math is fun! This box will contain a game to think about.

Sidenote: This box will contain material which, although interesting, is not part of the main material of the text. It's OK to skip over these boxes, but if you read them, you might learn something interesting!

Bogus Solution: Just like the impossible cube shown to the left, there's something wrong with any "solution" that appears in this box.

Exercises, Review Problems, and Challenge Problems

Most sections end with several **Exercises**. These will test your understanding of the material that was covered in the section that you just finished. You should try to solve *all* of the exercises. Exercises marked with a ★ are more difficult.

All chapters contain **Review Problems**. These are problems which test your basic understanding of the material covered in the chapter. Your goal should be to solve most or all of the Review Problems for every chapter—if you're unable to do this, it means that you haven't yet mastered the material, and you should probably go back and read the chapter again.

Most of the chapters end with **Challenge Problems**. These problems are generally more difficult than the other problems in the book, and will really test your mastery of the material. Some of them are very, very hard—the hardest ones are marked with a ★. Don't necessarily expect to be able to solve all of the Challenge Problems on your first try—these are difficult problems even for experienced problem solvers. If you are able to solve a large number of Challenge Problems, then congratulations, you are on your way to becoming an expert problem solver!

Hints

Many problems come with one or more hints. You can look up the hints in the Hints section in the back of the book. The hints are numbered in random order, so that when you're looking up a hint to a problem you don't accidentally glance at the hint to the next problem at the same time.

It is very important that you first try to solve the problem without resorting to the hints. Only after you've seriously thought about a problem and are stuck should you seek a hint. Also, for problems which have multiple hints, use the hints one at a time; don't go to the second hint until you've thought about the first one.

Solutions

The solutions to all of the Exercises, Review Problems, and Challenge Problems are in the separate solution book. If you are using this textbook in a regular school class, then your teacher may decide not to make this solution book available to you, and instead present the solutions him/herself. However, if you are using this book on your own to learn independently, then you probably have a copy of the solution book, in which case there are some very important things to keep in mind:

1. Make sure that you make a serious attempt at the problem before looking at the solution. Don't use the solution book as a crutch to avoid really thinking about a problem first. You should think *hard* about a problem before deciding to give up and look at the solution.

2. After you solve a problem, it's usually a good idea to read the solution, even if you think you know how to solve the problem. The solution that's in the solution book might show you a quicker or more concise way to solve the problem, or it might have a completely different solution method that you might not have thought of.

3. If you have to look at the solution in order to solve a problem, make sure that you make a note of that problem. Come back to it in a week or two to make sure that you are able to solve it on your own, without resorting to the solution.

Resources

Here are some other good resources for you to further pursue your study of mathematics:

- The other books in the *Art of Problem Solving* Introduction series of textbooks:
  - *Introduction to Algebra* by Richard Rusczyk
  - *Introduction to Counting & Probability* by David Patrick
  - *Introduction to Geometry* by Richard Rusczyk
- *The Art of Problem Solving* books, by Sandor Lehoczky and Richard Rusczyk. Whereas the book that you're reading right now will go into great detail of one specific subject area—number theory—*the Art of Problem Solving* books cover a wide range of problem solving topics across many different areas of mathematics.
- The `www.artofproblemsolving.com` website, which contains many resources for students:
  - a discussion forum
  - online classes
  - resource lists of books, contests, and other websites
  - a LaTeX tutorial
  - and much more!

- *Alcumus*, our new free online learning system at `artofproblemsolving.com`. Alcumus offers students a customized learning experience, adjusting to student performance to deliver appropriate problems and lessons. Alcumus contains (as of May 2011) over 3,500 problems with solutions, and complements this textbook along with our *Introduction to Algebra* and *Introduction to Counting & Probability* textbooks. It offers detailed progress reports and tools for teachers to monitor students' progress.

- You can hone your problem solving skills (and perhaps win prizes!) by participating in various math contests. For middle school students in the United States, the major contests are MATHCOUNTS, MOEMS, and the AMC 8. For U.S. high school students, some of the best-known contests are the AMC/AIME/USA(J)MO series of contests (which choose the U.S. team for the International Mathematics Olympiad), the American Regions Math League (ARML), the Mandelbrot Competition, the Harvard-MIT Mathematics Tournament, and the USA Mathematical Talent Search. More details about these contests are on page ix, and links to these and many other contests are available on the Art of Problem Solving website.

A Note to Teachers

We believe that students learn best when they are challenged with hard problems that at first they may not know how to do. This is the motivating philosophy behind this book.

Rather than first introducing new material and then giving students exercises, we present problems at the start of each section that students should try to solve *before* the new material is presented. The goal is to get students to discover the new material on their own. Often, complicated problems are broken into smaller parts, so that students can discover new techniques one piece at a time. Then the new material is formally presented in the text, and full solutions to each problem are explained, along with problem-solving strategies.

We hope that teachers will find that their stronger students will discover most of the material in this book on their own by working through the problems. Other students may learn better from a more traditional approach of first seeing the new material, then working the problems. Teachers have the flexibility to use either approach when teaching from this book.

The book is linear in coverage. Generally, students and teachers should progress straight through the book in order, without skipping chapters. Sections denoted with a ★ contain supplementary material that may be safely skipped. In general, chapters are not equal in length, so different chapters may take different amounts of classroom time.

Extra! Occasionally, you'll see a box like this at the bottom of a page. This is an "Extra!" and might be a quote, some biographical or historical background, or perhaps an interesting idea to think about.

Acknowledgements

Contests

We would like to thank the following contests for allowing us to use a selection of their problems in this book:

- The **American Mathematics Competitions**, a series of contests for U.S. middle and high school students. The **AMC 8**, **AMC 10**, and **AMC 12** contests are multiple-choice tests that are taken by over 350,000 students every year. Top scorers on the AMC 10 and AMC 12 are invited to take the **American Invitational Mathematics Examination (AIME)**, which is a more difficult, short-answer contest. Approximately 10,000 students every year participate in the AIME. Then, based on the results of the AMC and AIME contests, about 500 students are invited to participate in the **USA Mathematical Olympiad (USAMO)** or the **USA Junior Mathematical Olympiad (USAJMO)**, each of which is a 2-day, 9-hour examination in which each student must show all of his or her work. Results from the USAMO and USAJMO are used to invite a number of students to the Math Olympiad Summer Program, at which the U.S. team for the International Mathematical Olympiad (IMO) is chosen. More information about the AMC contests can be found on the AMC website at `amc.maa.org`.

- **MATHCOUNTS®**, the premier contest for U.S. middle school students. MATHCOUNTS is a national enrichment, coaching, and competition program that promotes middle school mathematics achievement through grassroots involvement in every U.S. state and territory. President Barack Obama and former Presidents George W. Bush, Bill Clinton, George H. W. Bush and Ronald Reagan have all recognized MATHCOUNTS in White House ceremonies. The MATHCOUNTS program has also received two White House citations as an outstanding private sector initiative. MATHCOUNTS includes both a competition program and a free club program for schools; in 2009-10 over 7,000 schools and 250,000 students participated in MATHCOUNTS. More information is available at `www.mathcounts.org`.

- The **Mandelbrot Competition**, which was founded in 1990 by Sandor Lehoczky, Richard Rusczyk, and Sam Vandervelde. The aim of the Mandelbrot Competition is to provide a challenging, engaging mathematical experience which is both competitive and educational. Students compete both as individuals and in teams. The Mandelbrot Competition is offered at the national level for more advanced students and the regional level for less experienced problem solvers. More information can be found at `www.mandelbrot.org`.

- The **USA Mathematical Talent Search (USAMTS)**, which was founded in 1989 by Professor George Berzsenyi. The USAMTS is a free mathematics competition open to all United States middle and high school students. As opposed to most mathematics competitions, the USAMTS allows students a full month to work out their solutions. Carefully written justifications are required for each problem. More information is available at `www.usamts.org`.

- The **American Regions Math League (ARML)**, which was founded in 1976. The annual ARML competition brings together nearly 2,000 of the nation's finest students. They meet, compete against, and socialize with one another, forming friendships and sharpening their mathematical skills. The contest is written for high school students, although some exceptional junior high students attend each year. The competition consists of several events, which include a team round, a power question (in which a team solves proof-oriented questions), an individual round, and two relay rounds. More information is available at `www.arml.com`.

- The **Harvard-MIT Mathematics Tournament**, which is an annual math tournament for high school students, held at MIT and at Harvard in alternating years. It is run exclusively by MIT and Harvard students, most of whom themselves participated in math contests in high school. More information is available at `web.mit.edu/hmmt/`.

How We Wrote This Book

This book was written using the LaTeX document processing system. We must thank the authors of the various LaTeX packages that we used while preparing this book, and also the brilliant authors of *The LaTeX Companion* for writing a reference book that is not only thorough but also very readable. The diagrams were prepared using METAPOST, a powerful graphics language which is based on Knuth's METAFONT.

About Us

This book is a collaborative effort of the staff of the Art of Problem Solving. Mathew Crawford was the lead author for this book, and wrote most of the text. Several drafts of this book were read by Richard Rusczyk, Dr. David Patrick, Naoki Sato, Tim Lambert, and Amanda Jones—all of whom made many helpful suggestions. Solutions were written by Mathew Crawford with help from Will Nygard and Ruozhou (Joe) Jia. Many of the diagrams were created by Richard Rusczyk and Brian Rice. Amanda Jones designed the cover and also the Egyptian hieroglyphics. Special thanks to Meena Boppana, Ravi Boppana, Gordon Dilger, Larry Evans, and several anonymous students for alerting us to errors in the first edition.

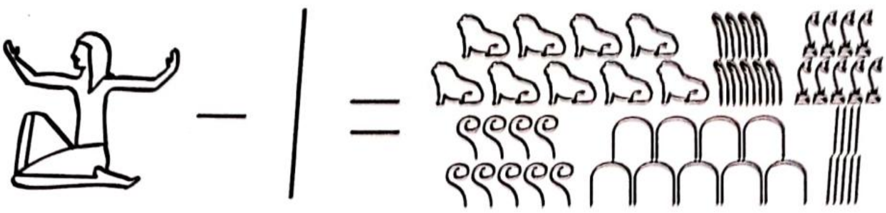
Websites

Information about source material, some problems, and errata are provided at

`http://www.artofproblemsolving.com/BookLinks/IntroNumberTheory/links.php`

Contents

For **Cindy Wright** and **Kay Tipton**, two math teachers who gave me problems to solve. Their tireless dedication to their students has always been extraordinary.



No more fiction, for now we calculate; but that we may calculate, we had to make fiction first.

– Friedrich Nietzsche

CHAPTER 9 Base Number Arithmetic

9.1 Introduction

It should come as no surprise that we can perform arithmetic operations on base numbers. After all, base numbers are just the regular numbers we always use, but written using different sets of digits.

9.2 Base Number Addition

Addition of integers is simply a way to count up from other integers. When we add 3 to 5, we count 3 integers past 5 to get to 8. Ultimately, addition is just quick counting and since we know how to count with base numbers, we can learn to add them.

Problems

Problem 9.1:

(a) Convert 21_6 to base 10.

(b) Convert 14_6 to base 10.

(c) If you count 14_6 integers past 21_6, what is the last integer you count expressed in base 10?

(d) If you count 14_6 integers past 21_6, what is the last integer you count expressed in base 6?

Problem 9.2:

(a) Express 331_7 as a sum of base 7 digit bundles.

(b) Express 213_7 as a sum of base 7 digit bundles.

(c) Add your answers from (a) and (b) and express the result as a sum of base 7 digit bundles.

(d) Express your answer from (c) as a base 7 integer.

Problem 9.3:
(a) Express 164_8 as a sum of base 8 digit bundles.
(b) Express 623_8 as a sum of base 8 digit bundles.
(c) Add your answers from (a) and (b). Carry as necessary to express your result as a sum of base 8 digit bundles.
(d) Express $164_8 + 623_8$ as a base 8 integer.

Problem 9.1: Express the sum $21_6 + 14_6$ in base 6.

Solution for Problem 9.1:

Since we are more familiar with the decimal system, we first convert the base 6 integers to decimal numerals. We add the decimal numbers and convert the sum back to base 6.

$$\begin{array}{rccr} 21_6 & \rightarrow & \rightarrow & 13 \\ +\ 14_6 & \rightarrow & \rightarrow & +\ 10 \\ \hline 35_6 & \leftarrow & \leftarrow & 23 \end{array}$$

Adding $13 + 10$ means counting 10 integers past 13 and the result is 23. We count to the *same integer* going 14_6 integers past 21_6. Thus, the sums $13 + 10$ and $21_6 + 14_6$ are the same. This allows us to add $21_6 + 14_6$:

$$21_6 + 14_6 = 13 + 10 = 23 = 35_6.$$

□

Concept: Addition, subtraction, multiplication, and exponentiation are just methods of fast counting. Since base number systems provide us with ways to write counting and arithmetic results, we can use arithmetic in all base number systems.

Problem 9.2: Express the sum $213_7 + 331_7$ in base 7.

Solution for Problem 9.2: In order to make the addition process easier, we begin by expressing these base 7 integers as sums of base 7 digit bundles:

$$\begin{aligned} 213_7 &= \mathbf{2} \cdot 7^2 + \mathbf{1} \cdot 7^1 + \mathbf{3} \cdot 7^0 \\ 331_7 &= \mathbf{3} \cdot 7^2 + \mathbf{3} \cdot 7^1 + \mathbf{1} \cdot 7^0 \end{aligned}$$

Adding these sums of digit bundles together by like terms, we get

$$(\mathbf{2}+\mathbf{3}) \cdot 7^2 + (\mathbf{1}+\mathbf{3}) \cdot 7^1 + (\mathbf{3}+\mathbf{1}) \cdot 7^0 = 5 \cdot 7^2 + 4 \cdot 7^1 + 4 \cdot 7^0 = 544_7.$$

□

Problem 9.3: Express the sum $623_8 + 164_8$ in base 8.

Solution for Problem 9.3:

$$\begin{aligned} 623_8 &= 6 \cdot 8^2 + 2 \cdot 8^1 + 3 \cdot 8^0 \\ 164_8 &= 1 \cdot 8^2 + 6 \cdot 8^1 + 4 \cdot 8^0 \end{aligned}$$

Adding these two base 8 expansions together by like terms, we get

$$(6+1)\cdot 8^2 + (2+6)\cdot 8^1 + (3+4)\cdot 8^0 = 7\cdot 8^2 + 8\cdot 8^1 + 7\cdot 8^0.$$

Unfortunately, the coefficient of the 8^1 term is not a base 8 digit. we'll have to carry:

$$(7+1)\cdot 8^2 + 0\cdot 8^1 + 7\cdot 8^0 = 8\cdot 8^2 + 0\cdot 8^1 + 7\cdot 8^0.$$

We'll have to carry one more time:

$$8\cdot 8^2 + 0\cdot 8^1 + 7\cdot 8^0 = 1\cdot 8^3 + 0\cdot 8^2 + 0\cdot 8^1 + 7\cdot 8^0 = 1007_8.$$

□

In order to solve the last two problems, we viewed base number addition in terms of digit bundles. However, just as in decimal arithmetic, we can simply add according to the digits:

$$\begin{array}{r} {\scriptstyle 1\,1} \\ 623_8 \\ +\ 164_8 \\ \hline 1007_8 \end{array}$$

Here are a few more examples of base number addition. Walk through these examples on your own and pay attention to where carrying occurs to be sure you understand the process of base number addition.

$$\begin{array}{r} 31_9 \\ +\ 52_9 \\ \hline 83_9 \end{array} \qquad \begin{array}{r} 212_3 \\ +\ 102_3 \\ \hline 1021_3 \end{array} \qquad \begin{array}{r} 43_5 \\ +\ 124_5 \\ \hline 222_5 \end{array} \qquad \begin{array}{r} 4262_7 \\ +\ 1542_7 \\ \hline 6134_7 \end{array} \qquad \begin{array}{r} 1A7_{16} \\ +\ 2B7A_{16} \\ \hline 2D21_{16} \end{array}$$

Some students might be wondering if adding between two different bases can be done easily. Adding between two bases (without first converting numbers to a single base) doesn't really make sense. Not only is there no clear way to express the answer to such an addition problem (which base would we use?), but there is no easy way to add integers in different bases without first converting both integers to the same base. The same is true for other arithmetic operations on base numbers.

Exercises

9.2.1 Add within the base indicated:

(a) $1_6 + 5_6$
(b) $15_9 + 23_9$
(c) $4_6 + 14_6$
(d) $54_7 + 126_7$
(e) $2303_5 + 131_5$
(f) $39A_{12} + 488_{12}$
(g) $6543_8 + 7426_8$
(h) $2102_3 + 1211021_3$
(i) $12_9 + 13_9 + 122_9$
(j) $101_2 + 11_2 + 1100_2 + 11101_2$
(k) $211_3 + 1002_3 + 2121_3$
(l) $A1B2_{16} + 12D94_{16}$

Extra! *The methods of theoretical physics should be applicable to all those branches of thought in which the essential features are expressible with numbers.* – Paul Dirac

9.3 Base Number Subtraction

Just as addition of natural numbers is a matter of counting upwards, subtraction of natural numbers is a matter of counting downwards.

Problems

Problem 9.4:
(a) Convert 12_7 and 25_7 to base 10.
(b) If you count downward 12_7 integers from 25_7, what is the last integer you count expressed in base 10?
(c) Express your answer from (b) in base 7?

Problem 9.5:
(a) Express 537_9 as a sum of base 9 digit bundles.
(b) Express 216_9 as a sum of base 9 digit bundles.
(c) Subtract your answer for (b) from your answer for (a) and express the result as a sum of base 9 digit bundles.
(d) Express your answer from (c) as a base 9 integer.
(e) If you count downward 216_9 integers from 537_9, what is the last integer you count expressed in base 9?

Problem 9.6:
(a) Express 514_6 as a sum of base 6 digit bundles.
(b) Express 433_6 as a sum of base 6 digit bundles.
(c) Subtract your answer for (b) from your answer for (a). What must be done with the result in order to express it as a sum of base 6 digit bundles?
(d) Express $514_6 - 433_6$ as a base 6 integer.

Problem 9.4: Express the difference $25_7 - 12_7$ in base 7.

Solution for Problem 9.4: First we note that $25_7 = 19$ and $12_7 = 9$. Subtracting $19 - 9$ means counting 9 integers back from 19 and the result is 10. The backwards counting is the same when we count 12_7 back from 25_7, so the differences $19 - 9$ and $25_7 - 12_7$ are the same. Since $10 = 13_7$, we see that the following statements of subtraction are equivalent:

$$\begin{array}{r} 25_7 \\ -\ 12_7 \\ \hline 13_7 \end{array} \qquad \begin{array}{r} 19 \\ -\ 9 \\ \hline 10 \end{array}$$

□

Problem 9.5: Express $537_9 - 216_9$ in base 9.

Solution for Problem 9.5: For larger integers, we need to organize the way in which we count backwards so that subtraction is not a heavy chore. Just as for addition, we expand the base numbers into sums of digit bundles:

$$\begin{aligned} 537_9 &= 5\cdot 9^2 + 3\cdot 9^1 + 7\cdot 9^0 \\ 216_9 &= 2\cdot 9^2 + 1\cdot 9^1 + 6\cdot 9^0 \end{aligned}$$

Subtracting the second base 9 expansion from the first by digit bundles we get

$$(\mathbf{5}-\mathbf{2})\cdot 9^2 + (\mathbf{3}-\mathbf{1})\cdot 9^1 + (\mathbf{7}-\mathbf{6})\cdot 9^0 = 3\cdot 9^2 + 2\cdot 9^1 + 1\cdot 9^0 = 321_9.$$

□

Problem 9.6: What is $514_6 - 433_6$?

Solution for Problem 9.6:

$$\begin{aligned} 514_6 &= 5\cdot 6^2 + 1\cdot 6^1 + 4\cdot 6^0 \\ 433_6 &= 4\cdot 6^2 + 3\cdot 6^1 + 3\cdot 6^0 \end{aligned}$$

Subtracting the second of these base 6 expansions from the first by like terms we get

$$(5-4)\cdot 6^2 + (1-3)\cdot 6^1 + (4-3)\cdot 6^0 = 1\cdot 6^2 + (\mathbf{-2})\cdot 6^1 + 1\cdot 6^0.$$

Unfortunately -2 is not a base 6 digit. We need to borrow 6 from the next higher valued digit bundle:

$$\begin{aligned} \mathbf{1}\cdot 6^2 + (\mathbf{-2})\cdot 6^1 + 1\cdot 6^0 &= \mathbf{6}\cdot 6^1 + (\mathbf{-2})\cdot 6^1 + 1\cdot 6^0 \\ &= (\mathbf{6}-\mathbf{2})\cdot 6^1 + 1\cdot 6^0 \\ &= 4\cdot 6^1 + 1\cdot 6^0 = 41_6. \end{aligned}$$

□

As we see in Problem 9.6, subtracting base numbers often requires borrowing from higher valued digits in a similar way as we borrow in decimal subtraction. The only difference is that instead of borrowing 10 from a digit, we borrow the value of the base. In the case of Problem 9.6, we borrowed 6 because each larger base 6 bundle is 6 times as large as the previous one.

While the last few problems highlight the fact that subtraction of integers is a matter of counting backward in all number bases, we have built our way up to viewing subtraction in terms of the digits themselves:

$$\begin{array}{r} {\scriptstyle 4\,11} \\ \cancel{5}\cancel{1}4_6 \\ -\ 433_6 \\ \hline 41_6 \end{array}$$

Here are a few more examples of base number subtraction. Walk through these examples on your own and pay attention to where borrowing occurs to be sure you understand the process of base number subtraction.

$$\begin{array}{r} 25_8 \\ -\ 11_8 \\ \hline 14_8 \end{array} \qquad \begin{array}{r} 123_4 \\ -\ 31_4 \\ \hline 32_4 \end{array} \qquad \begin{array}{r} 1001_2 \\ -\ 110_2 \\ \hline 11_2 \end{array} \qquad \begin{array}{r} 5842_9 \\ -\ 3868_9 \\ \hline 1863_9 \end{array} \qquad \begin{array}{r} 4A35_{12} \\ -\ 1B1B_{12} \\ \hline 2B16_{12} \end{array}$$

Exercises

9.3.1 Perform the arithmetic within the base indicated:

(a) $11_7 - 2_7$
(b) $58_9 - 18_9$
(c) $41_6 - 14_6$
(d) $126_7 - 54_7$
(e) $132_8 - 75_8$
(f) $13A9_{12} - 48B_{12}$
(g) $3434_5 - 1441_5$
(h) $2102102_3 - 1200212_3$
(i) $817_9 - 145_9 - 266_9$
(j) $1011_2 + 101_2 - 1100_2 + 1101_2$
(k) $A0A1_{11} - 3087_{11} - 2AA7_{11}$
(l) $3CD77_{16} - 19E8E_{16}$

9.4 Base Number Multiplication

When we multiply $3 \cdot 7$, we are really adding 7 together 3 times:

$$3 \cdot 7 = 7 + 7 + 7 = 21.$$

Multiplication is just repeated addition, so now that you know how to add base numbers, you can multiply them as well. In this section we explore the connection between base number addition and multiplication, and practice multiplying base numbers.

Problems

Problem 9.7:

(a) Evaluate $2_4 + 2_4 + 2_4$.

(b) Express $3_4 \cdot 2_4$ in base 4.

Problem 9.8:

(a) Express 34_6 as a sum of base 6 digit bundles.

(b) Express 241_6 as a sum of base 6 digit bundles.

(c) Find the product of each base 6 digit bundle from (a) with each base 6 digit bundle from (b). You should have six products when you are done.

(d) Express the sum of your answers from (c) as a sum of base 6 digit bundles.

(e) Express your answer from (d) as a base 6 integer.

Extra! *Through the years I've never stopped doing things, thinking about things, and I still think young.* – Doyle Brunson

Problem 9.7: Find the product of 3_4 and 2_4.

Solution for Problem 9.7: 3_4 and 2_4 represent the same integers as the decimal numerals 3 and 2. When we multiply $3 \cdot 2$ we really just add 2 together 3 times:

$$3 \cdot 2 = 2 + 2 + 2 = 6.$$

This product is equal to 12_4, so $3_4 \cdot 2_4 = 12_4$. We can also perform repeated addition in base 4 to get the same answer:

$$3_4 \cdot 2_4 = 2_4 + 2_4 + 2_4 = 12_4.$$

□

Problem 9.8: Calculate the product $34_6 \cdot 241_6$ and leave your answer in base 6.

Solution for Problem 9.8: Instead of adding 241_6 together 34_6 times, we organize our work by expressing the multiplicands as sums of base 6 digit bundles:

$$\begin{aligned} 34_6 &= 3 \cdot 6^1 + 4 \cdot 6^0 \\ 241_6 &= 2 \cdot 6^2 + 4 \cdot 6^1 + 1 \cdot 6^0 \end{aligned}$$

We multiply these sums of base 6 digit bundles in order to find the product:

$$\begin{aligned} 34_6 \cdot 241_6 &= \left(3 \cdot 6^1 + 4 \cdot 6^0\right)\left(2 \cdot 6^2 + 4 \cdot 6^1 + 1 \cdot 6^0\right) \\ &= 3 \cdot 6^1 \left(2 \cdot 6^2 + 4 \cdot 6^1 + 1 \cdot 6^0\right) + 4 \cdot 6^0 \left(2 \cdot 6^2 + 4 \cdot 6^1 + 1 \cdot 6^0\right) \end{aligned}$$

As we distribute the terms of this product, we end up with the six base 6 digit bundle products corresponding to each pair of digits of 34_6 and 241_6—one digit from each integer at a time:

$$\begin{aligned} \left(3 \cdot 6^1\right)\left(2 \cdot 6^2\right) &= (3 \cdot 2) \cdot 6^3 &= 1 \cdot 6^4 \\ \left(3 \cdot 6^1\right)\left(4 \cdot 6^1\right) &= (3 \cdot 4) \cdot 6^2 &= 2 \cdot 6^3 \\ \left(3 \cdot 6^1\right)\left(1 \cdot 6^0\right) &= (3 \cdot 1) \cdot 6^1 &= 3 \cdot 6^1 \\ \left(4 \cdot 6^0\right)\left(2 \cdot 6^2\right) &= (4 \cdot 2) \cdot 6^2 &= 1 \cdot 6^3 + 2 \cdot 6^2 \\ \left(4 \cdot 6^0\right)\left(4 \cdot 6^1\right) &= (4 \cdot 4) \cdot 6^1 &= 2 \cdot 6^2 + 4 \cdot 6^1 \\ \left(4 \cdot 6^0\right)\left(1 \cdot 6^0\right) &= (4 \cdot 1) \cdot 6^0 &= 4 \cdot 6^0 \end{aligned}$$

We now add these products together to determine the whole base 6 product:

$$\begin{aligned} 34_6 \cdot 241_6 &= 3 \cdot 6^1 \left(2 \cdot 6^2 + 4 \cdot 6^1 + 1 \cdot 6^0\right) + 4 \cdot 6^0 \left(2 \cdot 6^2 + 4 \cdot 6^1 + 1 \cdot 6^0\right) \\ &= 1 \cdot 6^4 + 2 \cdot 6^3 + 3 \cdot 6^1 + 1 \cdot 6^3 + 2 \cdot 6^2 + 2 \cdot 6^2 + 4 \cdot 6^1 + 4 \cdot 6^0 \\ &= 1 \cdot 6^4 + 3 \cdot 6^3 + 4 \cdot 6^2 + 7 \cdot 6^1 + 4 \cdot 6^0 \\ &= 1 \cdot 6^4 + 3 \cdot 6^3 + 5 \cdot 6^2 + 1 \cdot 6^1 + 4 \cdot 6^0 = 13514_6. \end{aligned}$$

□

Just as we do when we multiply decimal numerals, we can multiply base numbers simply using the digits themselves. The position of each digit tells us how many powers of the base we use. We must also be sure to carry according to the base in which we multiply.

$$
\begin{array}{r}
{\scriptstyle 1\,2} \\
{\scriptstyle 1\,2} \\
241_6 \\
\times \quad 34_6 \\
\hline
1444_6 \\
+\ 12030_6 \\
\hline
13514_6
\end{array}
$$

Here are a few more examples of base number multiplication. Walk through these examples on your own to be sure you understand the process of base number multiplication.

$$
\begin{array}{r}
23_4 \\
\times\ 11_4 \\
\hline
313_4
\end{array}
\qquad
\begin{array}{r}
67_9 \\
\times\ 18_9 \\
\hline
1372_9
\end{array}
\qquad
\begin{array}{r}
134_5 \\
\times\ 43_5 \\
\hline
13022_5
\end{array}
\qquad
\begin{array}{r}
6A9_{14} \\
\times\ 32B_{14} \\
\hline
178A91_{14}
\end{array}
$$

Exercises

9.4.1 Find each product within the indicated number base.

(a) $6_8 \cdot 7_8$

(b) $12_3 \cdot 201_3$

(c) $76_8 \cdot 57_8$

(d) $11_5 \cdot 3113_5$

(e) $192_{11} \cdot 3AA_{11}$

(f) $4213_6 \cdot 1215_6$

9.5 Base Number Division and Divisibility

Problems

Problem 9.9:

(a) Find the quotient and remainder when 5_7 is divided into 4 parts.

(b) Find the quotient and remainder when 13_7 is divided into 4 parts.

(c) Find the quotient and remainder when 26_7 is divided into 4 parts.

(d) When 536_7 is divided into 4 equal parts, what is the value of each part?

Problem 9.10: Determine which of the following base numbers are multiples of 6.

(a) 11110_2

(b) 313_4

(c) $1AC_{20}$

(d) 5241_7

Problem 9.9: Find the value of $536_7 \div 4_7$.

Solution for Problem 9.9:

Long division uses the division theorem, addition, subtraction, and multiplication to make the process of division easier. There is no reason that we can't use long division with base numbers. We must just keep in mind the ways in which addition, subtraction, and multiplication differ in base number arithmetic. In the example to the right, we divide 536_7 into 4_7 equal parts to find that each has the value 125_7.

$$\begin{array}{rl} & 125_7 \\ 4_7 & \overline{)\,536_7} \\ & 4 \\ & \overline{13} \\ & 11 \\ & \overline{26} \\ & 26 \\ & \overline{0} \end{array}$$

□

Let's take a look at a few more examples of base number division, including remainders. Walk through these examples on your own to be sure you understand the process of base number division.

$$\begin{array}{rl} & 347_8 \text{ R } 2_8 \\ 3_8 & \overline{)\,1267_8} \end{array} \qquad \begin{array}{rl} & 301_5 \text{ R } 11_5 \\ 12_5 & \overline{)\,4123_5} \end{array} \qquad \begin{array}{rl} & 2B6_{13} \text{ R } 46_{13} \\ 1A7_{13} & \overline{)\,52B19_{13}} \end{array}$$

Problem 9.10: Determine which of the following base numbers are multiples of 6.

(a) 11110_2

(b) 313_4

(c) $1AC_{20}$

(d) 5241_7

Solution for Problem 9.10: We can take a number of approaches to problems like these.

(a) We use long division to see if 11110_2 leaves a remainder when divided by $6 = 110_2$:

$$\begin{array}{rl} & 101_2 \\ 110_2 & \overline{)\,11110_2} \\ & 110 \\ & \overline{110} \\ & 110 \\ & \overline{0} \end{array}$$

So, 11110_2 is a multiple of 6.

(b) All multiples of 6 are even numbers. However, we can tell from the units digit of 313_4 that it is odd since each of the other digits represents bundling of even values:

$$313_4 = 3 \cdot 4^2 + 1 \cdot 4^1 + 3 \cdot 4^0 = 2(6 \cdot 4^1 + 2 \cdot 4^0) + 3.$$

Therefore, 313_4 is odd, so it is not a multiple of 6.

(c) We convert $1AC_{20}$ to decimal form to see if it is a multiple of 6:

$$1AC_{20} = 1 \cdot 20^2 + 10 \cdot 20^1 + 12 \cdot 20^0 = 400 + 200 + 12 = 612.$$

Since $612 \div 6 = 102$ without a remainder, we know $1AC_{20}$ is a multiple of 6.

(d) We subtract multiples of 6 out of each base 7 digit bundle fairly easily since $7 - 1 = 6$. If we get to 0 by subtracting multiples of 6, then 5241_7 is a multiple of 6.

$$\begin{aligned}
5241_7 &= 5 \cdot 7^3 + 2 \cdot 7^2 + 4 \cdot 7^1 + 1 \cdot 7^0 \\
&= 5 \cdot 7 \cdot 7^2 + 2 \cdot 7^2 + 4 \cdot 7^1 + 1 \cdot 7^0 \\
&= 5(6+1)7^2 + 2 \cdot 7^2 + 4 \cdot 7^1 + 1 \cdot 7^0 \\
&= 5 \cdot 6 \cdot 7^2 + 5 \cdot 7^2 + 2 \cdot 7^2 + 4 \cdot 7^1 + 1 \cdot 7^0
\end{aligned}$$

Since $5 \cdot 6 \cdot 7^2$ is a multiple of 6, we subtract it out from the total and continue since the new total will leave the exact same remainder as 5241_7 has when divided by 6:

$$\begin{aligned}
5 \cdot 7^2 + 2 \cdot 7^2 + 4 \cdot 7^1 + 1 \cdot 7^0 &= 7 \cdot 7^2 + 4 \cdot 7^1 + 1 \cdot 7^0 \\
&= 7 \cdot 7 \cdot 7^1 + 4 \cdot 7^1 + 1 \cdot 7^0 \\
&= 7(6+1)7^1 + 4 \cdot 7^1 + 1 \cdot 7^0 \\
&= 7 \cdot 6 \cdot 7^1 + 7 \cdot 7^1 + 4 \cdot 7^1 + 1 \cdot 7^0
\end{aligned}$$

Again, we subtract a multiple of 6 from the total: $7 \cdot 6 \cdot 7^1$. We continue to see if the remaining integer is a multiple of 6:

$$\begin{aligned}
7 \cdot 7^1 + 4 \cdot 7^1 + 1 \cdot 7^0 &= 11 \cdot 7^1 + 1 \cdot 7^0 \\
&= 11 \cdot 7 \cdot 7^0 + 1 \cdot 7^0 \\
&= 11(6+1)7^0 + 1 \cdot 7^0 \\
&= 11 \cdot 6 \cdot 7^0 + 11 \cdot 7^0 + 1 \cdot 7^0
\end{aligned}$$

Now when we subtract out $11 \cdot 6 \cdot 7^0$, the only thing left is $11 \cdot 7^0 + 1 \cdot 7^0 = 11 + 1 = 12$, which is a multiple of 6, so 5241_7 is a multiple of 6.

Note that over the course of subtraction above, we add each leftmost digit to the next leftmost digit. The result is the sum of the digits: $5 + 2 + 4 + 1 = 12$. This means that a base 7 integer is a multiple of 6 if and only if the sum of its digits is a multiple of 6. We explore this kind of "divisibility rule" in more detail later in this book.

We used four different methods to solve the four parts of this problem. Sometimes we cleverly applied relationships between integers. However, standard division always works with these kinds of problems. □

Exercises

9.5.1 Perform the indicated division within the given base. Include any remainders.

(a) $134_9 \div 7_9$
(b) $11111_2 \div 101_2$
(c) $1444_6 \div 31_6$
(d) $4516_8 \div 43_8$
(e) $81818_{11} \div 81_{11}$
(f) $9A71B_{16} \div 3E9_{16}$

9.5.2 Is 2246_8 divisible by 16_8?

9.5.3 Is 4554_7 divisible by 11_7?

9.5.4 Determine which of the following base numbers are multiples of 3.

(a) 1221_3
(b) 334_5
(c) 4113_6
(d) 7881_9

9.6 Summary

Concept: Addition, subtraction, multiplication, and exponentiation are just methods of fast counting. Since base number systems provide us with ways to write counting and arithmetic results, we can use arithmetic in all base number systems.

The secret to base number arithmetic is that there is no secret. We just need to be careful and pay attention to the base of the number system in which we work. Since we bundle value into digits according to the base we are working in, we carry and borrow according to the value of the base.

REVIEW PROBLEMS

9.11 Perform the indicated addition.

(a) $12_9 + 42_9$

(b) $34_5 + 411_5$

(c) $101110_2 + 1001_2 + 11011_2$

9.12 Perform the indicated subtraction.

(a) $5144_6 - 1023_6$

(b) $713_{12} - A9_{12}$

9.13 Perform the indicated multiplication.

(a) $21_7 \cdot 54_7$

(b) $2102_3 \cdot 121_3$

9.14 Perform the indicated division.

(a) $205_6 \div 15_6$

(b) $1510_8/52_8$

9.15 Determine which of the following are multiples of 5.

(a) 117_9

(b) 111101_2

(c) 111101_4

(d) 4105_6

(e) $A1BA_{15}$

9.16 Determine which of the following are multiples of 12.

(a) 717_8

(b) 212021_3

(c) 14202_5

(d) 6234_7

(e) $C10B_{13}$

Challenge Problems

9.17 Find the value of the base b such that the following addition problem is correct:

$$\begin{array}{r} 6651_b \\ +\quad 115_b \\ \hline 10066_b \end{array}$$

9.18 Compute: $(10101_2 + 1011_2) \cdot (110011_2 + 1101_2) \div (1000_2 + 100_2 + 10_2 + 1_2 + 1_2)$. **Hints:** 82

9.19 Find the positive base b in which the equation $4 \cdot 12 = 103$ is valid. **Hints:** 141

9.20 Is there any base b for which 3443_b is prime? If so, provide an example. If not, explain why not. **Hints:** 35

9.21 Find the largest prime number (in decimal form) that divides the sum,

$$1_2 + 10_2 + 100_2 + \cdots + 100000000_2.$$

Hints: 125

9.22 A binary number consists of 17 digits, all of which are 1. Triple the number.

(a) How many digits does the new binary number have?

(b) How many of those digits are 1's?

Hints: 153, 78

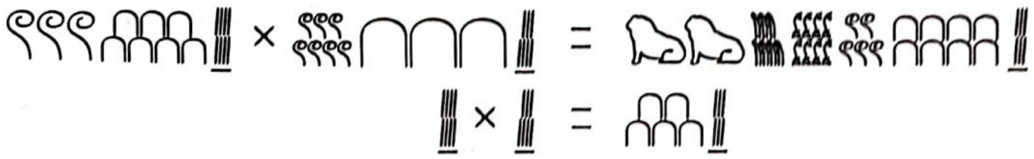
9.23 Let the product (12)(15)(16), each factor written in base b, equal 3146 in base b. Let $s = 12+15+16$, each term expressed in base b. Find the value of s in base b. *(Source: AHSME)* **Hints:** 51

9.24 Cleo needs to determine if a 71777-digit base 12 integer is a multiple of 3. The last five digits of the integer are 71777. Find a method that helps Cleo quickly determine whether or not the enormous integer is a multiple of 3. **Hints:** 27

9.25 The evil villain Harris Pilton wrote three secret two-digit numbers, x, y, and z on a napkin. Berris Fueler must name three numbers, A, B, and C, after which Harris will announce the value of $Ax+By+Cz$. If Berris can then name Harris' three secret numbers, Harris will let Berris go. Save Berris! Come up with a way to choose A, B, and C such that Berris is sure to escape Harris' evil clutches. **Hints:** 96

9.26 Find the sum of all the natural numbers that are three-digit palindromes when expressed in base 5. Express your answer in base 5. **Hints:** 149

Extra! *A stupid man's report of what a clever man says is never accurate because he unconsciously translates what he hears into something he can understand.* – Bertrand Russell



God created the integers; all else is the work of man. – Leopold Kronecker

CHAPTER 10 Units Digits

10.1 Introduction

Units digits store an enormous amount of useful information about integers. In this chapter we explore the ways in which units digits behave within arithmetic. After exploring units digits in the decimal number system, we explore the ways in which units digits behave in other number base systems. Once you are familiar and comfortable with all of the lessons in this chapter you will be ready to explore a much deeper realm of number theory using a tool known as *modular arithmetic*.

10.2 Units Digits in Arithmetic

In this section we take a look at the ways in which units digits of integers relate to the units digits of sums, differences, and products of those integers. We also explore some problems that are solved most easily with an understanding of these relationships.

Problems

Problem 10.1: Find the units digit of each of the following and explain any pattern.

(a) $8+9$
(b) $8+19$
(c) $8+29$
(d) $8+39$
(e) $8+1049$
(f) $438+31459$

Problem 10.2: Find the units digit of each of the following.

(a) $13+16$
(b) $132+299$
(c) $4576+982$
(d) $14+67+78+142+71777$

Problem 10.3: Find the units digit of each of the following and explain any pattern.

(a) $243 - 6$
(b) $243 - 16$
(c) $243 - 26$
(d) $243 - 36$
(e) $243 - 166$
(f) $5613 - 3926$

Problem 10.4: Find the units digit of each of the following.

(a) $37 - 22$
(b) $431 - 286$
(c) $5418 - 4379$
(d) $931 - 413 - 79$

Problem 10.5: Find the units digit of each of the following and explain any pattern.

(a) $4 \cdot 3$
(b) $4 \cdot 13$
(c) $4 \cdot 23$
(d) $4 \cdot 33$
(e) $4 \cdot 783$
(f) $214 \cdot 573$

Problem 10.6: Find the units digit of each of the following.

(a) $53 \cdot 79$
(b) $44 \cdot 88$
(c) $103 \cdot 107$
(d) $710 \cdot 319$
(e) $492 \cdot 5137$
(f) $9127 \cdot 4286$

Problem 10.7: Find the units digit of each of the following and explain any pattern.

(a) 4^3
(b) 24^3
(c) 4^4
(d) 24^4
(e) 4^5
(f) 24^5
(g) 4^6
(h) 24^6
(i) 4^{100}
(j) 24^{100}

Problem 10.8: The product of two positive integers has a units digit of 3. One of the integers has a units digit of 7. What is the units digit of the other integer?

Problem 10.9: Karen is a teenager and the square of her age is equal to the number on her street address. If her age and the number on her street address have the same units digit, but do not add up to a multiple of 10, how old is Karen?

Problem 10.1: Find the units digit of each of the following and explain any pattern.

(a) $8 + 9$
(b) $8 + 19$
(c) $8 + 29$
(d) $8 + 39$
(e) $8 + 1049$
(f) $438 + 31459$

Solution for Problem 10.1:

$$\begin{aligned} 8 + 9 &= 17 \\ 8 + 19 &= 27 \\ 8 + 29 &= 37 \\ 8 + 39 &= 47 \\ 8 + 1049 &= 1057 \\ 438 + 31459 &= 31897 \end{aligned}$$

We might conjecture that the sum of any two positive integers with units digits of 8 and 9 has a units digit of 7. Exploring this possible relationship between units digits leads us to expand integers into sums of decimal digit bundles. This helps us "visualize" relationships between the digits.

Extra! *Never tell people how to do things. Tell them what to do and they will surprise you with their ingenuity.* – General George Patton Jr.

The values of the digit bundles with powers of 10 from 10^1 on up never affect the units digit because increasing those digits never affects the units digit values (the coefficient of 10^0). This means that we need only consider the units digits of integers when determining the units digit of their sum.

$$\begin{aligned}
\mathbf{9} &= \mathbf{9} \cdot 10^0 \\
1\mathbf{9} &= 1 \cdot 10^1 + \mathbf{9} \cdot 10^0 \\
2\mathbf{9} &= 2 \cdot 10^1 + \mathbf{9} \cdot 10^0 \\
3\mathbf{9} &= 3 \cdot 10^1 + \mathbf{9} \cdot 10^0 \\
104\mathbf{9} &= 1 \cdot 10^3 + 0 \cdot 10^2 + 4 \cdot 10^1 + \mathbf{9} \cdot 10^0
\end{aligned}$$

$$\begin{aligned}
438 + 31459 &= \left(4 \cdot 10^2 + 3 \cdot 10^1 + \mathbf{8} \cdot 10^0\right) + \left(3 \cdot 10^4 + 1 \cdot 10^3 + 4 \cdot 10^2 + 5 \cdot 10^1 + \mathbf{9} \cdot 10^0\right) \\
&= 3 \cdot 10^4 + 1 \cdot 10^3 + (4+4) \cdot 10^2 + (3+5) \cdot 10^1 + (\mathbf{8} + \mathbf{9}) \cdot 10^0 \\
&= 3 \cdot 10^4 + 1 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10^1 + \mathbf{17} \cdot 10^0 \\
&= 3 \cdot 10^4 + 1 \cdot 10^3 + 8 \cdot 10^2 + 9 \cdot 10^1 + \mathbf{7} \cdot 10^0 = 31897.
\end{aligned}$$

Only units digits of the integers being summed affect the units digit of the final sum.

$$\begin{array}{r} 438 \\ +\ 31459 \\ \hline 31897 \end{array}$$

□

Important: The units digit of the sum of two positive integers is the same as the units digit of the sum of just their units digits. Repeating this process, the units digit of the sum of a group of positive integers is the same as the units digit of the sum of just the units digits of those positive integers.

This fact helps us most when the integers are large or numerous.

Problem 10.2: Find the units digit of each of the following.

(a) $13 + 16$

(b) $132 + 299$

(c) $4576 + 982$

(d) $14 + 67 + 78 + 142 + 71777$

Solution for Problem 10.2: We simply sum the units digits to get our answers.

(a) $3 + 6 = 9$, so 9 is the units digit of $13 + 16$.

(b) $2 + 9 = 11$, so 1 is the units digit of $132 + 299$.

(c) $6 + 2 = 8$, so 8 is the units digit of $4576 + 982$.

(d) $4 + 7 + 8 + 2 + 7 = 28$, so 8 is the units digit of $14 + 67 + 78 + 142 + 71777$.

□

Extra! *Tomorrow is the most important thing in life. Comes into us at midnight very clean. It's perfect when it arrives and it puts itself in our hands. It hopes we've learned something from yesterday.*
– John Wayne

Problem 10.3: Find the units digit of each of the following and explain any pattern.

(a) $243 - 6$ (c) $243 - 26$ (e) $243 - 166$

(b) $243 - 16$ (d) $243 - 36$ (f) $5613 - 3926$

Solution for Problem 10.3:

$$\begin{aligned} 243 - \mathbf{6} &= 237 \\ 243 - \mathbf{16} &= 227 \\ 243 - \mathbf{26} &= 217 \\ 243 - \mathbf{36} &= 207 \\ 243 - \mathbf{166} &= 77 \\ 5613 - \mathbf{3926} &= 1687 \end{aligned}$$

These examples make us think that subtracting a positive integer with a units digit of 6 from a larger integer with a units digit of 3 results in a difference with units digit 7. As in Problem 10.1, we expand integers into sums of decimal digit bundles to better view relationships between the digits.

The values bundled into powers of 10 from 10^1 on up never affect the units digit. Even though we must unbundle and borrow from a tens digit bundle, the rest of the bundles never affect the units digit as we count backwards (subtract). We borrow from the tens digit exactly once in each case. This affects the units digits of the differences (the coefficient of 10^0) in the same way.

$$\begin{aligned} \mathbf{6} &= \mathbf{6 \cdot 10^0} \\ \mathbf{16} &= 1 \cdot 10^1 + \mathbf{6 \cdot 10^0} \\ \mathbf{26} &= 2 \cdot 10^1 + \mathbf{6 \cdot 10^0} \\ \mathbf{36} &= 3 \cdot 10^1 + \mathbf{6 \cdot 10^0} \\ \mathbf{166} &= 1 \cdot 10^2 + 6 \cdot 10^1 + \mathbf{6 \cdot 10^0} \end{aligned}$$

$$\begin{aligned} 5613 - \mathbf{3926} &= \left(5 \cdot 10^3 + 6 \cdot 10^2 + 1 \cdot 10^1 + \mathbf{3} \cdot 10^0\right) - \left(3 \cdot 10^3 + 9 \cdot 10^2 + 2 \cdot 10^1 + \mathbf{6} \cdot 10^0\right) \\ &= (5-3) \cdot 10^3 + (6-9) \cdot 10^2 + (1-2) \cdot 10^1 + (\mathbf{3} - \mathbf{6}) \cdot 10^0 \\ &= 2 \cdot 10^3 + (-3) \cdot 10^2 + (-1) \cdot 10^1 + (\mathbf{-3}) \cdot 10^0 \\ &= 1 \cdot 10^3 + 7 \cdot 10^2 + (-1) \cdot 10^1 + (\mathbf{-3}) \cdot 10^0 \\ &= 1 \cdot 10^3 + 6 \cdot 10^2 + 9 \cdot 10^1 + (\mathbf{-3}) \cdot 10^0 \\ &= 1 \cdot 10^3 + 6 \cdot 10^2 + 8 \cdot 10^1 + \mathbf{7} \cdot 10^0 = 1687 \end{aligned}$$

The values of digits other than the units digit do not affect the fact that we borrow from the tens digit in the same way in each of the examples.

$$\begin{array}{r} {\scriptstyle \,15\,10} \\ {\scriptstyle 4\,\cancel{5}\,\cancel{0}\,13} \\ \cancel{5}\cancel{6}\cancel{1}\cancel{3} \\ -\,3926 \\ \hline 1687 \end{array}$$

□

Important: When we subtract a positive integer from a larger integer, the units digit of the result equals the result of subtracting the units digit of the smaller integer from the units digit of the larger (carrying if necessary). This result can be extended to subtraction of several integers at a time.

Problem 10.4: Find the units digit of each of the following.

(a) $37 - 22$
(b) $431 - 286$
(c) $5418 - 4379$
(d) $931 - 413 - 79$

Solution for Problem 10.4: In order to find the units digit of each difference, we subtract the units digits in the appropriate order. In cases where the result is negative, we add 10 repeatedly until the result is positive, just as we would while "borrowing" in regular subtraction.

(a) $7 - 2 = 5$, so 5 is the units digit of $37 - 22$.

(b) $1 - 6 = -5$, but adding 10 back we get $-5 + 10 = 5$. So, 5 is the units digit of $431 - 286$.

(c) $8 - 9 = -1$, but adding 10 back we get $-1 + 10 = 9$. So, 9 is the units digit of $5418 - 4379$.

(d) $1 - 3 - 9 = -11$, but adding 20 back we get $-11 + 20 = 9$. So, 9 is the units digit of $931 - 413 - 79$.

□

Problem 10.5: Find the units digit of each of the following and explain any pattern.

(a) $4 \cdot 3$
(b) $4 \cdot 13$
(c) $4 \cdot 23$
(d) $4 \cdot 33$
(e) $4 \cdot 783$
(f) $214 \cdot 573$

Solution for Problem 10.5:

$$\begin{aligned}
\mathbf{4 \cdot 3} &= 12 \\
\mathbf{4} \cdot 1\mathbf{3} &= 52 \\
\mathbf{4} \cdot 2\mathbf{3} &= 92 \\
\mathbf{4} \cdot 3\mathbf{3} &= 132 \\
\mathbf{4} \cdot 78\mathbf{3} &= 3132 \\
214 \cdot 573 &= 122622
\end{aligned}$$

These products suggest that multiplying an integer with a units digit of 4 by an integer with a units digit of 3 results in a product with units digit 2. Once again we expand integers into sums of decimal digit bundles in order to get a grip on the relationships between the digits.

The values bundled into powers of 10 from 10^1 on up will never affect the units digit. Each time such a bundle is multiplied by an integer, the result has a units digit of 0.

$$\begin{aligned}
3 &= \mathbf{3} \cdot 10^0 \\
13 &= 1 \cdot 10^1 + \mathbf{3} \cdot 10^0 \\
23 &= 2 \cdot 10^1 + \mathbf{3} \cdot 10^0 \\
33 &= 3 \cdot 10^1 + \mathbf{3} \cdot 10^0 \\
783 &= 7 \cdot 10^2 + 8 \cdot 10^1 + \mathbf{3} \cdot 10^0
\end{aligned}$$

$$\begin{aligned}
214 \cdot 573 &= (21 \cdot 10 + \mathbf{4})(57 \cdot 10 + \mathbf{3}) \\
&= 21 \cdot 57 \cdot 10^2 + (21 + 57)10 + \mathbf{4 \cdot 3} \\
&= 119700 + 780 + \mathbf{12} \\
&= 122622
\end{aligned}$$

No digits besides the units digits of the multiplicands 214 and 573 affect the units digit of the product. □

Important: The units digit of the product of two positive integers is the same as the units digit of the product of their units digits. Repeating this process, the units digit of the product of a group of positive integers is the same as the units digit of the product of their units digits.

Problem 10.6: Find the units digit of each of the following.

(a) $53 \cdot 79$ (c) $103 \cdot 107$ (e) $492 \cdot 5137$
(b) $44 \cdot 88$ (d) $710 \cdot 319$ (f) $9127 \cdot 4286$

Solution for Problem 10.6: In order to find the units digit of each product, we simply multiply the units digits of each pair of integers.

(a) $3 \cdot 9 = 27$, so 7 is the units digit of $53 \cdot 79$.

(b) $4 \cdot 8 = 32$, so 2 is the units digit of $44 \cdot 88$.

(c) $3 \cdot 7 = 21$, so 1 is the units digit of $103 \cdot 107$.

(d) $0 \cdot 9 = 0$, so 0 is the units digit of $710 \cdot 319$.

(e) $2 \cdot 7 = 14$, so 4 is the units digit of $492 \cdot 5137$.

(f) $7 \cdot 6 = 42$, so 2 is the units digit of $9127 \cdot 4286$.

□

Problem 10.7: Find the units digit of 24^{100}.

Solution for Problem 10.7:

The 100^{th} power of 24 is the product of 100 24's. Since only the units digits of the 24's affect the units digit of the product, the units digit of 24^{100} is the units digit of 4^{100}.

Now that we've simplified the problem a bit, we search for a way to determine the units digit of 4^{100}. In order to do that we test a few smaller powers of 4 as shown on the right.

$$\begin{aligned} 4^1 &= 4 \\ 4^2 &= 16 \\ 4^3 &= 64 \\ 4^4 &= 256 \\ 4^5 &= 1024 \\ 4^6 &= 4096 \end{aligned}$$

It appears that the units digits of powers of 4 alternate between 4 and 6. We don't want to take this for granted, so we set out to determine why this pattern seems to continue. Since we are computing units digits of products, we examine the result of each step in the chain of multiplication that makes up the powers of 4:

$$\begin{aligned} 4 \cdot 4 &= 16 \\ 4 \cdot 6 &= 24 \end{aligned}$$

Any time we multiply an integer with a units digit of 4 by the integer 4, the result must have a units digit of 6. Any time we multiply an integer with a units digit of 6 by the integer 4, the result must have a units digit of 4. Now we know for certain that the units digits of the powers of 4 alternate, with each even power having a units digit of 6. Therefore, 6 is the units digit of 24^{100}. □

Concept: Hunting for patterns can be very helpful when solving problems or learning more about mathematics. Play around with numbers and test simple cases. See if you can establish a pattern. Then try to determine why the pattern you discovered works.

Problem 10.8: The product of two positive integers has a units digit of 3. One of the integers has a units digit of 7. What is the units digit of the other integer?

Solution for Problem 10.8:

$$\begin{aligned} 1 \cdot 7 &= 7 \\ 3 \cdot 7 &= 21 \\ 5 \cdot 7 &= 35 \\ 7 \cdot 7 &= 49 \\ 9 \cdot 7 &= 63 \end{aligned}$$

When a product of integer multiplicands is odd, each of the multiplicands is odd. Since the product of the two positive integers in this problem is odd, we need only test to see which of the odd digits multiply by 7 to produce a units digit of 3. We find that the units digit of the other positive integer must be 9.

□

Concept: The possible number of units digits in a problem is usually very limited. We can solve such problems involving units digits by simply computing the possible outcomes.

Problem 10.9: Karen is a teenager and the square of her age is equal to the number on her street address. If her age and the number on her street address have the same units digit, but do not add up to a multiple of 10, how old is Karen?

Solution for Problem 10.9: Solving word problems often becomes easier when we assign variables to represent unknown quantities in the problem. Let's call Karen's age K. We know that the street address is equal to K^2 and has the same units digit as K. We know that Karen is a teenager, so we test values of K from 13 to 19 to see which has a units digit equal to K^2:

$$\begin{array}{lll} K = 13 & K^2 = 169 & 3 \neq 9 \\ K = 14 & K^2 = 196 & 4 \neq 6 \\ K = 15 & K^2 = 225 & 5 = 5 \\ K = 16 & K^2 = 256 & 6 = 6 \\ K = 17 & K^2 = 289 & 7 \neq 9 \\ K = 18 & K^2 = 324 & 8 \neq 4 \\ K = 19 & K^2 = 361 & 9 \neq 1 \end{array}$$

Since the square of Karen's age has the same units digit as her age, she must be either 15 or 16 years old. Now we check to see whether or not the sum of each of these with its square is a multiple of 10:

$$\begin{array}{ll} 15 + 225 = 240 & 10 \mid 240 \\ 16 + 256 = 272 & 10 \nmid 272 \end{array}$$

Karen is 16 years old. □

Concept: Translate word problems into the language of mathematics so that you can solve them mathematically.

Exercises

10.2.1 Find the units digit of each of the following.

(a) $14 + 33$
(b) $724 + 888$
(c) $8233 + 9129$
(d) $36 + 37 + 38 + 39$
(e) $87 - 14$
(f) $741 - 423$
(g) $9215 - 8767$
(h) $837 - 412 - 279$
(i) $537 + 812 - 55 + 9412 - 3148$
(j) $1 + 2 + 3 + \cdots + 100$
(k) $13 \cdot 41$
(l) $75 \cdot 123$
(m) $29 \cdot 79 + 31 \cdot 81$
(n) $19^3 \cdot 167^5$
(o) 7^3
(p) 7^{12}
(q) $7 \cdot 17 \cdot 1977 - 7^3$
(r) 18^6
(s) 312^8
(t) $13^{19} \cdot 19^{13}$

10.2.2 What digit is in the units place of $(3^3)^5$? *(Source: MATHCOUNTS)*

10.2.3 Find the units digit of the following:

$$(972 - 268)(973 - 267)(974 - 266) + (968 - 272)(967 - 273)(966 - 274) - (999 - 222)^3$$

10.2.4 Tim is three times as old as Jeff, who is a teenager. If their ages have the same units digits, how old is Jeff?

10.2.5 The product of two natural numbers has a units digit of 1. If one of the integers has a units digit of 3, what is the units digit of the sum of the two integers?

10.2.6 Gary says to Gerry, "I'm thinking of an integer that is the product of 5 consecutive odd integers. It's units digit is 3." Gary was about to explain more about this integer, when Gerry interrupted, "You've made a mistake!" How does Gerry know?

10.3 Base Number Units Digits

Base number arithmetic works the same way as decimal arithmetic. For this reason, nearly everything that we have learned about the ways in which units digits behave in decimal arithmetic applies to base number arithmetic as well. The only differences relate to the bases of the number systems.

Problems

Problem 10.10: Using digit bundles of each number base, find the units digit of each of the following (within the indicated number base).

(a) $34_8 + 71_8$
(b) $131_4 + 2323_4$
(c) $5234_6 - 2155_6$
(d) $121_3 \cdot 202_3$

Try to explain any relationships you see in the results.

Problem 10.11: A natural number n has a units digit of 5 when expressed in base 8. What is the remainder when n is divided by 8?

Problem 10.12: Find the base 7 units digit of $(416_7)^{416}$.

Problem 10.13: Lindsay does all her arithmetic in base 11. When multiplying two positive integers, she notes that their product has a units digit of 3. If one of the two base 11 integers has a units digit of 7, find the base 11 units digit of the other one.

Problem 10.10: Using digit bundles of each number base, find the units digit of each of the following (within the indicated number base).

(a) $34_8 + 71_8$ (c) $5234_6 - 2155_6$

(b) $131_4 + 2323_4$ (d) $121_3 \cdot 202_3$

Try to explain any relationships you see in the results.

Solution for Problem 10.10: Expanding integers into sums of digit bundles helped us understand relationships between units digits in decimal arithmetic, so we try the same thing with base numbers. The only differences are the bases of the digit bundles.

(a)

$$\begin{aligned} 34_8 + 71_8 &= (3\cdot 8^1 + 4\cdot 8^0) + (7\cdot 8^1 + 1\cdot 8^0) \\ &= 10\cdot 8^1 + 5\cdot 8^0 \\ &= (8+2)\cdot 8^1 + 5\cdot 8^0 \\ &= 1\cdot 8^2 + 2\cdot 8^1 + 5\cdot 8^0 \\ &= 125_8 \end{aligned}$$

The units digit is $4 + 1 = 5$, which is just the units digit from the sum of the units digits of 34_8 and 71_8.

Expanding base numbers into sums of digit bundles makes clear that we need only to work with the units digits to find the units digit of the final sum. This helps not only with addition, but also with subtraction, multiplication, and exponentiation in the same ways it did for decimal integers! (Make sure you see why.)

Now we can find the answers to the rest of the problems without much effort.

(b) The units digit of $131_4 + 2323_4$ is the units digit of $1_4 + 3_4 = 10_4$, which is **0**.

(c) The units digit of $5234_6 - 2155_6$ is the units digit of $14_6 - 5_6 = 5_6$, which is **5**.

Notice that in (c) we subtracted $14_6 - 5_6$ instead of $4_6 - 5_6$ because we needed to carry from the sixes digit. However, the actual sixes digit in the original subtraction problem did not affect the answer.

(d) The units digit of $121_3 \cdot 202_3$ is the units digit of $1_3 \cdot 2_3 = 2_3$, which is **2**.

□

Problem 10.11: A natural number n has a units digit of 5 when expressed in base 8. What is the remainder when n is divided by 8?

Solution for Problem 10.11: Let's take a look at a few examples:

$$\begin{array}{rclcl c rcl}
5_8 & = & 5\cdot 8^0 & = & 5_{10} & \longrightarrow & 5\div 8 & = & 0\,\mathrm{R}\,5\\
15_8 & = & 1\cdot 8^1+5\cdot 8^0 & = & 13_{10} & \longrightarrow & 13\div 8 & = & 1\,\mathrm{R}\,5\\
25_8 & = & 2\cdot 8^1+5\cdot 8^0 & = & 21_{10} & \longrightarrow & 21\div 8 & = & 2\,\mathrm{R}\,5\\
35_8 & = & 3\cdot 8^1+5\cdot 8^0 & = & 29_{10} & \longrightarrow & 29\div 8 & = & 3\,\mathrm{R}\,5\\
45_8 & = & 4\cdot 8^1+5\cdot 8^0 & = & 37_{10} & \longrightarrow & 37\div 8 & = & 4\,\mathrm{R}\,5
\end{array}$$

The remainders when each of these base 8 natural numbers gets divided by 8 are all 5, which is the base 8 units digit of each of them. The rest of the base 8 digits represent values that are multiples of 8, so they don't contribute to the remainders when we divide by 8. □

Problem 10.12: Find the base 7 units digit of $(416_7)^{416}$.

Solution for Problem 10.12: Since $(416_7)^{416}$ is just a product of base 7 integers, we find its units digit by evaluating $(6_7)^{416}$. Now we look for a pattern in the units digits of successive powers of 6_7:

The units digit of $(6_7)^2 = 51_7$ is 1.

The units digit of $(6_7)^3 = 51_7\cdot 6_7$ is the same as in $1_7\cdot 6_7 = 6_7$, which is 6.

The units digit of $(6_7)^4 = (6_7)^3\cdot 6_7$ is the same as in $6_7\cdot 6_7 = 51_7$, which is 1.

We already see repetition. When 6_7 gets multiplied by a base 7 natural number with a units digit of 6, the product has a units digit of 1. When 6_7 gets multiplied by a base 7 natural number with a units digit of 1, the product has a units digit of 6. Since these facts never change, the units digits of powers of 6_7 alternate between 1 and 6.

Since the even exponents lead to units digits of 1, we know $(6_7)^{416}$ has units digit 1. Therefore, $(416_7)^{416}$ also has a units digit of 1 (in base 7). □

Problem 10.13: Lindsay does all her arithmetic in base 11. When multiplying two positive integers, she notes that their product has a units digit of 3. If one of the two base 11 integers has a units digit of 7, find the base 11 units digit of the other one.

Solution for Problem 10.13:

$$\begin{array}{rcl rcl}
1_{11}\cdot 7_{11} & = & 7_{11} & 6_{11}\cdot 7_{11} & = & 39_{11}\\
2_{11}\cdot 7_{11} & = & 13_{11} & 7_{11}\cdot 7_{11} & = & 45_{11}\\
3_{11}\cdot 7_{11} & = & 1A_{11} & 8_{11}\cdot 7_{11} & = & 51_{11}\\
4_{11}\cdot 7_{11} & = & 26_{11} & 9_{11}\cdot 7_{11} & = & 58_{11}\\
5_{11}\cdot 7_{11} & = & 32_{11} & A_{11}\cdot 7_{11} & = & 64_{11}
\end{array}$$

Similarly to how we approached Problem 10.8, we examine a table of possible products of 7 and each possible base 11 units digit. The only possible base 11 units digit of Lindsay's other positive integer is 2. Make sure you see why we can leave 0 off the table.

□

Exercises

10.3.1 Find the units digit of each of the following within the indicated number base.

(a) $52_7 + 62_7$
(b) $913_{11} + 825_{11}$
(c) $14_5 + 323_5$
(d) $413_6 - 215_6$
(e) $1001101_2 \cdot 100101101_2$
(f) $15_{18} \cdot 928_{18}$
(g) $(14_8)^2$
(h) $(515_7)^3$
(i) $(437_9)^{313}$

10.3.2 Two positive integers each have a units digit of 2 when expressed in base b.

(a) Find the units digit of their product when $b = 3$.
(b) Find the units digit of their product when $b = 4$.
(c) Find the units digit of their product when $b = 5$.
(d) Find the units digit of their product when $b = 6$.

10.3.3 The product of two consecutive integers have a units digit other than 0 when expressed in base 6. Find the units digit of their sum when expressed in base 6.

10.4 Unit Digits Everywhere!

Problems

Problem 10.14: What are the possible units digits of perfect squares?

Problem 10.15: What are the possible units digits of perfect squares written in base 4?

Problem 10.16: What are the possible units digit of $n!$, where n is a positive integer?

Problem 10.17: Sylvester tells Tweety that he's thinking of four consecutive odd integers that are positive and whose product has a units digit of 1. Tweety tells Sylvester that this isn't possible. Is Tweety right?

Problem 10.18:

(a) If m is a whole number, what are the possible units digits of $2 \cdot 3^m$?
(b) If m is a whole number, what are the possible units digits of $4 \cdot 3^m$?
(c) If m is a whole number, what are the possible units digits of $6 \cdot 3^m$?
(d) If m is a whole number, what are the possible units digits of $8 \cdot 3^m$?
(e) How many of the positive divisors of 6^{2006} have a units digit of 6?

Extra! *Mystery creates wonder and wonder is the basis of man's desire to understand.* – Neil Armstrong

Problem 10.14: What are the possible units digits of perfect squares?

Solution for Problem 10.14:

$$\begin{aligned} 0^2 &= 0 \\ 1^2 &= 1 \\ 2^2 &= 4 \\ 3^2 &= 9 \\ 4^2 &= 16 \\ 5^2 &= 25 \\ 6^2 &= 36 \\ 7^2 &= 49 \\ 8^2 &= 64 \\ 9^2 &= 81 \end{aligned}$$

Since the units digit of the product of any two integers is the units digit of the product of their units digits, we only need to find the units digits of the squares of all the (decimal) digits. As we see, the only possible units digits of squares are 0, 1, 4, 5, 6, and 9. The digits 2, 3, 7, and 8 are not the units digits of any perfect squares.

□

Concept: Part of the power of focusing on units digits is that they can simplify problems involving many integers into just a few cases that can be easily calculated.

Problem 10.15: What are the possible units digits of perfect squares written in base 4?

Solution for Problem 10.15:

$$\begin{aligned} 0^2 &= 0_4 \\ 1^2 &= 1_4 \\ 2^2 &= 10_4 \\ 3^2 &= 21_4 \end{aligned}$$

In base 4, there are only 4 digits, so we need test only 4 cases corresponding to the squares of each of these digits. As we see, the only possible units digits of perfect squares when written in base 4 are 0 and 1.

□

Notice that a consequence of Problem 10.15 is that any even perfect square is a multiple of 4, while any odd perfect square is 1 more than a multiple of 4. This fact helps us quickly see some integers like 1026 and 4579 are not perfect squares—without computing any squares or square roots!

Problem 10.16: What are the possible units digit of $n!$, where n is a positive integer?

Solution for Problem 10.16: Examining a few factorials helps shed light on this problem:

$$\begin{aligned} 1! &= 1 & 5! &= 120 \\ 2! &= 2 & 6! &= 720 \\ 3! &= 6 & 7! &= 5040 \\ 4! &= 24 & 8! &= 40320 \end{aligned}$$

All the factorials from 5! on up have units digits of 0 because each is a multiple of 10. So, the only possible units digits of factorials of positive integers are 0, 1, 2, 4, and 6.□

Problem 10.17: Sylvester tells Tweety that he's thinking of four consecutive odd integers that are positive and whose product has a units digit of 1. Tweety tells Sylvester that this isn't possible. Is Tweety right?

Solution for Problem 10.17:

First, note that if any one of the integers has a units digit of 5, then their product will have a units digit of 5. We know this because 5 times any odd digit results in a units digit of 5.

$$\begin{aligned} 1\cdot 5 &= 5\\ 3\cdot 5 &= 15\\ 5\cdot 5 &= 25\\ 7\cdot 5 &= 35\\ 9\cdot 5 &= 45 \end{aligned}$$

If none of the integers has a units digit of 5, then they must have all four other odd digits as their units digits. This is because the greatest of the integers is only 6 more than the least—not enough more for a units digit to be repeated. Taking the product of these four odd digits we get $1\cdot 3\cdot 7\cdot 9 = 189$. This means that the product of these four consecutive odd integers is either 5 or 9. Tweety was correct. □

Problem 10.18: How many of the positive divisors of 6^{2006} have a units digit of 6?

Solution for Problem 10.18:

$$6^{2006} = 2^{2006}\cdot 3^{2006}$$

Positive divisors of 6^{2006} have the form $2^a\cdot 3^b$ where a and b are whole numbers no greater than 2006. Since we are looking for divisors with units digits of 6, we need only search the even divisors.

Let's start with the divisors in the form $2^1\cdot 3^b$. Once the units digits begin repeating, the pattern is determined: $2, 6, 8, 4, 2, 6, 8, 4, 2, \ldots$. We see that the units digits of these divisors are 6 when b is 1 more than a multiple of 4.

$$\begin{aligned} 2^1\cdot 3^0 &= 2\\ 2^1\cdot 3^1 &= 6\\ 2^1\cdot 3^2 &= 18\\ 2^1\cdot 3^3 &= 54\\ 2^1\cdot 3^4 &= 162\\ &\vdots \end{aligned}$$

Now we look at the units digits of the divisors in the form $2^2\cdot 3^b$. They also repeat in a pattern. In fact, the pattern in the same, it just starts with 4 instead of 2: $4, 2, 6, 8, 4, 2, 6, 8, 4, \ldots$. The units digits of these divisors are 6 when b is 2 more than a multiple of 4.

$$\begin{aligned} 2^2\cdot 3^0 &= 4\\ 2^2\cdot 3^1 &= 12\\ 2^2\cdot 3^2 &= 36\\ 2^2\cdot 3^3 &= 108\\ 2^2\cdot 3^4 &= 324\\ &\vdots \end{aligned}$$

Similar reasoning shows us that divisors in the form $2^3\cdot 3^b$ have units digits of 6 when b is 3 more than a multiple of 4 and divisors in the form $2^4\cdot 3^b$ have units digit of 6 when b is a multiple of 4.

When we get to divisors in the form $2^5\cdot 3^b, 2^6\cdot 3^b, \ldots$, we find that these follow the same patterns of the previous cases because the units digits of 2^1 and 2^5 are the same, the units digits of 2^2 and 2^6 are the same, etc.

The result is that a and b must have the same remainder when divided by 4 in order for $2^a \cdot 3^b$ to have a units digit of 6. Now we must count all the possibilities, keeping in mind that $a > 0$:

	Possible values of a	Possible values of b	Possible values of $2^a \cdot 3^b$
Remainder of 0:	501	502	$501 \cdot 502 = 251502$
Remainder of 1:	502	502	$502 \cdot 502 = 252004$
Remainder of 2:	502	502	$502 \cdot 502 = 252004$
Remainder of 3:	501	501	$501 \cdot 501 = 251001$

The total number of positive divisors of 6^{2006} that have a units digit of 6 is

$$251502 + 252004 + 252004 + 251001 = 1006511.$$

□

Exercises

10.4.1 If the square of a positive integer has a units digit of 4, what are the possible units digits of the integer itself?

10.4.2 The product of two positive integers has a units digit of 6. If one of the integers has a units digit of 8, what are the possible values of the units digit of the other one?

10.4.3 Find the possible units digits of a perfect square in base 8.

10.4.4

(a) Find the units digit of the sum,

$$1! + 2! + 3! + \cdots + 2006!.$$

(b) Find the units digit of that sum when it is expressed in base 7.

10.5 Summary

Though it took some work to demonstrate all we learned about units digits, we can summarize most of it in a single, simple statement:

> **Important:** When we add, subtract, and multiply positive integers (to get positive integers), the units digit of the result is determined solely by the units digits of all the integers involved. This is true even for base numbers.

Along the way, we saw more examples of one of the most important concepts in all of problem solving—particularly in number theory:

Concept: Hunting for patterns can be very helpful when solving problems or learning more about mathematics. Play around with numbers and test simple cases. See if you can establish a pattern. Then try to determine why the pattern you discovered works.

Having a few simple rules for dealing with units digits in arithmetic gave us simpler approaches for tackling some word problems and some challenging problems involving different types of integers like squares and factorials. Even though we can list all squares and factorials, we can learn a lot of useful facts about them from their units digits alone.

Concept: Part of the power of focusing on units digits is that they can simplify problems involving many integers into just a few cases that can be easily calculated.

REVIEW PROBLEMS

10.19 Find the units digit of each of the following.

(a) $724 + 4317$
(b) $10412 - 7895$
(c) $41 \cdot 99$
(d) $16 \cdot 17 \cdot 18$
(e) 2^{23}
(f) $24!$
(g) 7^{1777}
(h) $14^{92} - 1776$
(i) $3^{10} \cdot 5^6$
(j) $(9^9 - 8^8)(7^7 - 6^6)$
(k) $24^{129} \cdot 37^{441}$
(l) $8^{99} \cdot 9^{88}$

10.20 Find the units digit of $3^{1986} - 2^{1986}$. *(Source: MATHCOUNTS)*

10.21 Jenny has 8 stamp books that each contain 42 pages. Each page in her books contains 6 stamps. Jenny decides to reorganize her stamp books such that each page contains 10 stamps. This will give her more space to collect stamps without having to buy new books. Under her new system, Jenny fills up 4 complete books, still with 42 pages per book. Her fifth book now contains 33 pages filled with 10 stamps per page and 1 last page with the remaining stamps. How many stamps are on that last page?

10.22 The product of two positive integers has a units digit of 9. If one of the integers has a units digit of 7, what is the units digit of the other?

10.23 The product of two primes has a units digit of 3. What are the possible units digits of their sum?

10.24 Find the units digit of each of the following within the indicated number base.

(a) $83_9 + 171_9$
(b) $314_5 + 2423_5$
(c) $516_8 - 224_8$
(d) $517_8 - 433_8 + 114_8$
(e) $15_7 \cdot 42_7$
(f) $513_9 \cdot 7121_9$
(g) $A1B_{13} \cdot 41A_{13}$
(h) $1202_3 \cdot 212_3$
(i) $412_5 \cdot 11204_5 \cdot 311132_5$
(j) $(17_{12})^6$

10.25 Two positive integers have units digits of 2 and 3 respectively when expressed in base b. Find the units digit of their product when b equals

(a) 4
(b) 5
(c) 6
(d) 7171977

10.26 What are the possible units digits of a perfect square written in base 5?

10.27 What are the possible units digits of a perfect fourth power (in base 10)?

10.28 If n is a positive integer, what are the possible values of the units digit of $\frac{(n+2)!}{n!}$?

10.29 When the product of two consecutive positive integers is written in base 7, the units digit is 5. Find the units digit of their base 7 sum.

Challenge Problems

10.30 What are the possible units digit of a perfect fourth power written in base 5?

10.31

(a) Find all the possible units digits of perfect squares written in base 3.
(b) Find all the possible units digits of perfect squares written in base 6.
(c) Find all the possible units digits of perfect squares written in base 7.
(d) Find all the possible units digits of perfect squares written in base 9.

10.32 What is the units digit of $(133^{13})^3$? *(Source: MATHCOUNTS)*

10.33 Brannon is reading the book *Flatland* and notices that the product of the numbers of the two pages his book is open to has a units digit of 6. What is the units digit of the sum of the two page numbers? **Hints:** 101

10.34 How many of the following integers have a units digit of 6?

$$2^1, 2^2, 2^3, 2^4, \ldots, 2^{99}, 2^{100}$$

10.35 Find the units digit of n given that $mn = 21^6$ and m has a units digit of 7.

10.36 Given that m and n are positive integers such that $m^2n = 39^{39}$ and n has units digit 1, find the possible values of the units digit of m. **Hints:** 90

10.37 The product of two numbers has been accidentally erased by a student. All that remains is shown here.

```
   _8
 × __
 ----
  3__
 _12
 ----
 ----
```

The student only remembers that the product was larger than 4000. Name the larger factor. *(Source: MATHCOUNTS)* **Hints:** 53

10.38 How many three-digit integers are multiples of both 4 and 6 and have a units digit of 2? **Hints:** 31

10.39 Let S be the sum of ten consecutive positive integers and let P be their product. Explain why the units digit of $P - S$ must be 5. **Hints:** 169

10.40 Find the units digit of 3^{2006} when expressed in each of the following bases:

(a) 4

(b) 5

(c) 7

(d) 8

(e) 9

10.41 The cube of the three-digit natural number $A7B$ is 108531333. What is $A + B$? *(Source: MATHCOUNTS)* **Hints:** 4, 108

10.42

(a) Find the units digit of 2! when expressed in base 3.

(b) Find the units digit of 4! when expressed in base 5.

(c) Find the units digit of 6! when expressed in base 7.

(d) Find the units digit of 10! when expressed in base 11.

10.43 Margaret and her younger sister Wylia are both between 10 and 20 years old. The sum of their ages has a units digit of 6 and the difference between their ages is 2. If Wylia's age is an even number, how old is Margaret?

10.44 Find the smallest integer greater than 2 that has a units digit of 2 when written in base 3, base 4, base 5, and base 6. (You can leave your answer as a decimal integer.) **Hints:** 40

10.45 In how many number bases, b, does

$$32_b + 32_b + 32_b + 32_b + 32_b + 32_b + 32_b$$

have a units digit of 2? **Hints:** 13

10.46 How many Mersenne primes have units digit 3? **Hints:** 163

10.47

(a) Convert 1599 to base 16.

(b) Find all possible units digits of perfect fourth powers when written in base 16.

(c) Determine all non-negative integral solutions $(n_1, n_2, \ldots, n_{14})$ if any, of the Diophantine equation

$$n_1^4 + n_2^4 + \cdots + n_{14}^4 = 1599.$$

(Source: USAMO) **Hints:** 115

Sidenote: **Benford's Law**

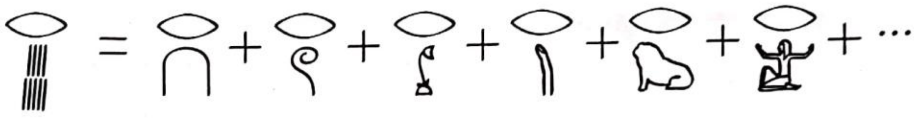
While units digits can be quite useful, a curious relationship exists between the first digit of many numbers. In 1938, physicist Frank Benford of the General Electric Company was looking through pages of logarithm values. He noticed that the pages corresponding to numbers beginning with the numeral 1 were more worn than other pages. He conjectured that numbers starting off with the digit 1 simply occur more frequently. Today this is known as "**Benford's Law**" and can be used for a variety of statistical purposes such as catching tax cheaters and testing for the presence of falsified experimental data.

Benford's Law seems at first counterintuitive. For each number that begins with 1, we can change the first digit to any other digit. It would stand to reason that all these numbers have the same chance of "happening." However, in reality, most numbers used in business, science, and other areas of life are exponential in nature. This makes a difference! Consider the following table of powers of 2:

2^0	1	2^{10}	1024	2^{20}	1048576
2^1	2	2^{11}	2048	2^{21}	2097152
2^2	4	2^{12}	4096	2^{22}	4194304
2^3	8	2^{13}	8192	2^{23}	8388608
2^4	16	2^{14}	16384	2^{24}	16777216
2^5	32	2^{15}	32768	2^{25}	33554432
2^6	64	2^{16}	65536	2^{26}	67108864
2^7	128	2^{17}	131072	2^{27}	134217728
2^8	256	2^{18}	262144	2^{28}	268435456
2^9	512	2^{19}	524288	2^{29}	536870912

Of the first thirty positive integers that are powers of 2, nine of them have 1 as their first digit. That's 30% of the total, where intuition suggests only 10%. If you carry the experiment further—to hundreds or thousands of powers of 2—the result is almost exactly the same! Around 30% of the powers of 2 in your list will begin with the digit 1.

This is not unique to the number 2. Try it with any positive integer that isn't a power of 10. You'll find that if you compute enough powers, the proportion of the results whose first nonzero digit is 1 is a little over 30%. The basic reasoning is that when we go from 1 to 2, we increase 100%, but when we go from 2 to 3, or 3 to 4, etc., we increase by smaller percentages. This means that an exponentially increasing set of numbers "spends more time" in ranges between $1 \cdot 10^n$ and $2 \cdot 10^n$ (for integer values of n). The 30% approximation comes from the fact that $10^{0.3} \approx 2 = 2/1$. Do you see why this relates to exponentially increasing sets of numbers?



If people do not believe that mathematics is simple, it is only because they do not realize how complicated life is.
– John Louis von Neumann

CHAPTER 11

Decimals and Fractions

11.1 Introduction

Numbers are sometimes written as decimals and sometimes as fractions (and sometimes in other ways, like a symbol for the number π). In this chapter we explore important and useful relationships between decimals and fractions. Not only do the methods we discuss help us convert between decimals and fractions, a highly useful skill on its own, but they also build our understanding of numbers in a way that helps us solve different types of problems.

11.2 Terminating Decimals

Some numbers can be exactly written in decimal notation using a whole number of digits. For instance, 4.3, −1.72, 612.199, and 0.0355 can be written this way. These numerals each have a *last* digit, so we call them **terminating decimals**. In this section we discuss ways in which we write some fractions as terminating decimals:

$$\frac{43}{10} = 4.3 \qquad -\frac{43}{25} = -1.72 \qquad \frac{612199}{1000} = 612.199 \qquad \frac{71}{2000} = 0.0355$$

Definition: A number whose decimal representation ends after a finite number of digits has a **terminating decimal** expansion. We call these numbers **terminating decimals**.

Extra! *There are three ways you can get to the top of a tree: 1) sit on an acorn; 2) make friends with a bird; 3) climb it.*
–Anonymous

Problems

Problem 11.1: Let n be a positive integer.

(a) When we divide a decimal number by 10, how are the numeral and the quotient related?

(b) When we divide a decimal number by 10^n, how are the numeral and the quotient related?

Problem 11.2: Let x be a number with a decimal expansion that terminates m digits after the decimal point. Find the smallest power of 10 that we can multiply by x to get an integer product.

Problem 11.3: For these problems, n represents a natural number.

(a) Write $\frac{1}{2^n}$ as a decimal for each of $n = 1, 2, 3$, and 4.

(b) How many digits past the decimal point do we need to express $\frac{1}{2^n}$ as a decimal?

Problem 11.4: For a given natural number n, how many digits past the decimal point do we need to express $\frac{1}{5^n}$ as a decimal?

Problem 11.5: Let $\frac{n}{d}$ be a reduced fraction where $d = 2^a \cdot 5^b$ for whole numbers a and b.

(a) Find the smallest power of 10 that we can multiply by $\frac{n}{d}$ to get an integer product.

(b) How many digits to the right of the decimal point are required in order to express $\frac{n}{d}$ as a decimal numeral?

Problem 11.1: Let n be a positive integer. When we divide a decimal number by 10^n, how are the numeral and the quotient related?

Solution for Problem 11.1: Let's take a look at a few examples of what happens when we divide numbers by 10:

$$\begin{array}{r} 0.1 \\ 10\,\overline{)\,1.0} \\ \underline{1.0} \\ 0 \end{array} \qquad \begin{array}{r} 0.3 \\ 10\,\overline{)\,3.0} \\ \underline{3.0} \\ 0 \end{array} \qquad \begin{array}{r} 1.7 \\ 10\,\overline{)\,17.0} \\ \underline{10} \\ 7.0 \\ \underline{7.0} \\ 0 \end{array} \qquad \begin{array}{r} 2.93 \\ 10\,\overline{)\,29.30} \\ \underline{20} \\ 9.3 \\ \underline{9.0} \\ 0.30 \\ \underline{0.30} \\ 0 \end{array}$$

Dividing a number by 10 seems to cause the decimal point to shift one digit to the left in the quotient. This makes sense as 10 *is* the number base in which we are working.

Extra! *I don't believe it. Prove it to me and I still won't believe it.* – Douglas Adams

Now we rewrite each dividend as a sum of decimal digit bundles before multiplying each by 10^{-1}. This makes the process of dividing these numbers by 10 more clear:

$$\begin{aligned}
1 \div 10 &= (1\cdot 10^0)\cdot 10^{-1} &&= 1\cdot 10^{-1} &&= 0.1\\
3 \div 10 &= (3\cdot 10^0)\cdot 10^{-1} &&= 3\cdot 10^{-1} &&= 0.3\\
17 \div 10 &= (1\cdot 10^1 + 7\cdot 10^0)\cdot 10^{-1} &&= 1\cdot 10^0 + 7\cdot 10^{-1} &&= 1.7\\
29.3 \div 10 &= (2\cdot 10^1 + 9\cdot 10^0 + 3\cdot 10^{-1})\cdot 10^{-1} &&= 2\cdot 10^0 + 9\cdot 10^{-1} + 3\cdot 10^{-2} &&= 2.93
\end{aligned}$$

Dividing by 10 reduces the power of 10 in each decimal digit bundle by 1. This means all the digits remain the same and in the same order, but the decimal point shifts one digit to the left.

Dividing by 10^n is the same thing as dividing by 10 a total of n times. This means that when we divide by 10^n, we move the decimal point n places to the left. Here are a few examples:

$$\begin{array}{lll}
\dfrac{1}{100} = 0.01 & \dfrac{17}{100} = 0.17 & \dfrac{600}{10} = 60\\[2ex]
\dfrac{30}{1000} = 0.03 & \dfrac{17}{1000} = 0.017 & \dfrac{600}{100} = 6\\[2ex]
\dfrac{217}{10000} = 0.0217 & \dfrac{17}{10000} = 0.0017 & \dfrac{600}{1000} = 0.6\\[2ex]
\dfrac{19}{100000} = 0.00019 & \dfrac{17}{100000} = 0.00017 & \dfrac{600}{10000} = 0.06
\end{array}$$

In the cases where 600 is divided by powers of 10, the decimal point doesn't "appear" until after we've divided by more than one power of 10. We can think of the decimal point as invisible after the units digit until we need to see it, but it still moves over one digit when we divide a number by 10. □

Important: For a positive integer n, when we divide a decimal number by 10^n, we move the decimal point n places to the left.

Concept: When faced with a problem involving the properties of numbers or principles of arithmetic, consider whether it's more illuminating to view the numbers in terms of decimals or fractions. The fact that either one of these forms might shed more light on a particular idea than the other is another example of how we use convenient mathematical forms to solve problems.

Problem 11.2: Let x be a number with a decimal expansion that terminates m digits after the decimal point. Find the smallest power of 10 that we can multiply by x to get an integer product.

Solution for Problem 11.2: The number x has m digits to the right of the decimal, so $10x$ has $m-1$ digits to the right of the decimal point. Multiplying by 10 again, 10^2x has $m-2$ digits to the right of the decimal point. Each time we multiply by 10, we reduce the number of digits to the right of the decimal point by 1. In order to get rid of all the digits to the right of the decimal point, we multiply x by 10^m to get an integer, $10^m x$. □

Problem 11.3: For a given natural number n, how many digits past the decimal point do we need to express $\frac{1}{2^n}$ as a decimal?

Solution for Problem 11.3: We first take a look at a few examples to help us establish what happens to decimals when we divide them by powers of 2:

$$
\begin{array}{llllllll}
n=1: & \frac{1}{2^n} & = & \frac{1}{2^1} & = & \frac{1}{2} & = 0.5 & \textbf{1 digit} \\
n=2: & \frac{1}{2^n} & = & \frac{1}{2^2} & = & \frac{1}{4} & = 0.25 & \textbf{2 digits} \\
n=3: & \frac{1}{2^n} & = & \frac{1}{2^3} & = & \frac{1}{8} & = 0.125 & \textbf{3 digits} \\
n=4: & \frac{1}{2^n} & = & \frac{1}{2^4} & = & \frac{1}{16} & = 0.0625 & \textbf{4 digits}
\end{array}
$$

It appears that we need another digit past the decimal point for each power of 2 by which we divide. To try to confirm this observation, we take a look at the process of dividing by 2 in decimal form. Dividing by 2 means multiplying by $0.5 = 5 \cdot 0.1$. Let's take a look at this same process of multiplication in decimal form:

$$
\begin{array}{llllllll}
n=1: & \frac{1}{2^n} & = & \frac{5^1}{10^1} & = & 5 \cdot (0.1)^1 & = 0.5 & \textbf{1 digit} \\
n=2: & \frac{1}{2^n} & = & \frac{5^2}{10^2} & = & 25 \cdot (0.1)^2 & = 0.25 & \textbf{2 digits} \\
n=3: & \frac{1}{2^n} & = & \frac{5^3}{10^3} & = & 125 \cdot (0.1)^3 & = 0.125 & \textbf{3 digits} \\
n=4: & \frac{1}{2^n} & = & \frac{5^4}{10^4} & = & 625 \cdot (0.1)^4 & = 0.0625 & \textbf{4 digits}
\end{array}
$$

We already know that multiplying a number by 0.1 (which is the same as dividing it by 10) causes the decimal point to shift one digit to the left. Multiplying an odd number by 5 results in an odd number, so multiplying by 5 in these cases will not result in a new 0 digit. The decimal point still shifts one digit to the left. The result is that for any natural number n, the fraction $\frac{1}{2^n}$ has exactly n digits after the decimal point. □

Sidenote: $2^{20} = 1048576$ has 7 digits. $2^{20} \cdot 5^{20} = 10^{20}$, which has 21 digits. Try to see why the number of digits of 5^{20} is $21 - 7 = 14$ without computing any powers of 5. There is a similar Challenge Problem at the end of this chapter.

Note also that the decimal point shifts one digit to the left any time we divide an odd number by 2:

$$
\begin{array}{llllllll}
n=1: & \frac{3}{2^n} & = & \frac{3}{2^1} & = & \frac{3}{2} & = & 1.5 & \textbf{1 digit} \\[2ex]
n=2: & \frac{3}{2^n} & = & \frac{3}{2^2} & = & \frac{3}{4} & = & 0.75 & \textbf{2 digits} \\[2ex]
n=3: & \frac{3}{2^n} & = & \frac{3}{2^3} & = & \frac{3}{8} & = & 0.375 & \textbf{3 digits} \\[2ex]
n=4: & \frac{3}{2^n} & = & \frac{3}{2^4} & = & \frac{3}{16} & = & 0.1875 & \textbf{4 digits}
\end{array}
$$

Make sure you see why this works.

Problem 11.4: For a given natural number n, how many digits past the decimal point do we need to express $\frac{1}{5^n}$ as a decimal?

Solution for Problem 11.4: We use the same method as we did in Problem 11.3, but reversing the roles of 2 and 5:

$$
\begin{array}{llllllllll}
n=1: & \frac{1}{5^n} & = & \frac{1}{5^1} & = & \frac{2^1}{10^1} & = & 2^1\cdot(0.1)^1 & = & 0.2 & \textbf{1 digit} \\[2ex]
n=2: & \frac{1}{5^n} & = & \frac{1}{5^2} & = & \frac{2^2}{10^2} & = & 2^2\cdot(0.1)^2 & = & 0.04 & \textbf{2 digits} \\[2ex]
n=3: & \frac{1}{5^n} & = & \frac{1}{5^3} & = & \frac{2^3}{10^3} & = & 2^3\cdot(0.1)^3 & = & 0.008 & \textbf{3 digits} \\[2ex]
n=4: & \frac{1}{5^n} & = & \frac{1}{5^4} & = & \frac{2^4}{10^4} & = & 2^4\cdot(0.1)^4 & = & 0.0016 & \textbf{4 digits}
\end{array}
$$

Dividing by 5 means multiplying by 0.2, moving the decimal point one place over unless the integer we are dividing has at least one power of 5 in its prime factorization. This means that $\frac{1}{5^n}$ has exactly n digits to the right of the decimal point. □

We extend the method from Problem 11.4. For an integer m that is not divisible by 5, the decimal expansion of $\frac{m}{5^n}$ also has exactly n digits to the right of its decimal point. For instance, when $m = 7$ we have

$$
\begin{array}{llllllllll}
n=1: & \frac{7}{5^n} & = & \frac{7}{5^1} & = & 7\cdot\frac{2^1}{10^1} & = & 7\cdot 2^1\cdot(0.1)^1 & = & 1.4 & \textbf{1 digit} \\[2ex]
n=2: & \frac{7}{5^n} & = & \frac{7}{5^2} & = & 7\cdot\frac{2^2}{10^2} & = & 7\cdot 2^2\cdot(0.1)^2 & = & 0.28 & \textbf{2 digits} \\[2ex]
n=3: & \frac{7}{5^n} & = & \frac{7}{5^3} & = & 7\cdot\frac{2^3}{10^3} & = & 7\cdot 2^3\cdot(0.1)^3 & = & 0.056 & \textbf{3 digits}
\end{array}
$$

Problem 11.5: Let $\frac{n}{d}$ be a reduced fraction where $d = 2^a \cdot 5^b$ for whole numbers a and b. How many digits to the right of the decimal point are required in order to express $\frac{n}{d}$ as a decimal numeral?

Solution for Problem 11.5: We already know that for a terminating decimal, the number of digits past the decimal point is the exponent of the smallest power of 10 that, when multiplied by the decimal number, results in an integer product. This seems like a good starting point. In order to get an idea as to where it might lead us, let's take a look at a few examples:

$$\begin{array}{lllllll}
a=2 & b=1 & \frac{1}{20} & = & \frac{1}{2^2 \cdot 5^1} & = & 0.05 & \text{2 digits} \\
a=2 & b=1 & \frac{33}{20} & = & \frac{33}{2^2 \cdot 5^1} & = & 1.65 & \text{2 digits} \\
a=1 & b=2 & \frac{1}{50} & = & \frac{1}{2^1 \cdot 5^2} & = & 0.02 & \text{2 digits} \\
a=4 & b=2 & \frac{17}{400} & = & \frac{17}{2^4 \cdot 5^2} & = & 0.0425 & \text{4 digits} \\
a=3 & b=5 & \frac{1}{25000} & = & \frac{1}{2^3 \cdot 5^5} & = & 0.00004 & \text{5 digits}
\end{array}$$

It appears that the number of digits past the decimal point needed to write each fraction as a decimal is the larger of a and b. Indeed this is true! We need to multiply each fraction by at least that many powers of 10 to cancel out all of the powers of 2 and 5 in the denominator of each fraction in order to produce an integer:

$$\frac{1}{25000} \cdot 10^5 = \frac{10^5}{2^3 \cdot 5^5} = \frac{2^5 \cdot 5^5}{2^3 \cdot 5^5} = 2^2 = 4.$$

□

Exercises

11.2.1 Find the number of digits past the decimal point needed to express each of the following.

(a) $\frac{83}{4}$

(b) $\frac{83}{25}$

(c) $\frac{11}{20}$

(d) $\frac{11}{50}$

(e) $\frac{16}{125}$

(f) $\frac{917}{500}$

(g) $\frac{1}{2000}$

(h) $\frac{19}{1600}$

11.2.2 Find quick ways to convert each of the following to decimals.

(a) $\frac{14}{25}$

(b) $\frac{83}{125}$

(c) $\frac{3}{8}$

(d) $\frac{91}{200}$

11.3 Repeating Decimals

Some rational numbers cannot be written as terminating decimals.

Definition: A number whose decimal representation becomes an endlessly repeating sequence of digits has a **repeating decimal** expansion. We simply call these numbers **repeating decimals**.

An example of a repeating decimal is $\frac{1}{13} = 0.076923076923076923\ldots$, in which the block of six digits 0-7-6-9-2-3 repeats endlessly.

Problems

Problem 11.6:

(a) Find the first three digits after the decimal point in the decimal expansion of 1/3.

(b) How do we know that the decimal expansion of 1/3 repeats endlessly?

(c) Find the repeating decimal expansions of the fractions 1/3, 2/3, and 10/3.

Problem 11.7:

(a) Find the first 9 digits after the decimal point in the decimal expansion of 2/7.

(b) How do we know that the decimal expansion of 2/7 repeats endlessly?

(c) Find the repeating decimal expansions of the fractions 1/7, 2/7, 3/7, and 10/7.

Problem 11.8: Let a and b be relatively prime natural numbers.

(a) Show that if b is divisible by a prime other than 2 or 5, then $\frac{a}{b}$ is not a terminating decimal.

(b) Show that $\frac{a}{b}$ is either a repeating decimal or a terminating decimal.

Problem 11.9:

(a) Find the smallest integer n such that $\frac{10^n}{12}$ reduces to a fraction with a denominator that is divisible by neither 2 nor 5. Write the resulting fraction in reduced form, then convert it to a decimal.

(b) Divide your decimal from part (b) by 10^n. (This will be the decimal expansion for 1/12.)

Problem 11.6: What is the decimal expansion for $\frac{1}{3}$? How can we be sure it repeats endlessly?

Solution for Problem 11.6:

We begin dividing 1 by 3 and see that the decimal expansion does not terminate one, two, or even three digits past the decimal point. In fact, at each step in the division process, we find ourselves dividing 3 into 10. The quotient is 3, which becomes a new digit of the decimal of 1/3. The remainder is 1, to which we append a 0 and continue the long division. Since this process never changes, the decimal representation of 1/3 repeats endlessly. Follow the division yourself and make sure you understand the repetition of division.

$$\begin{array}{r|l}
 & 0.333\ldots \\ \hline
3 & 1.000\ldots \\
 & \underline{0.9} \\
 & 0.10 \\
 & \underline{0.09} \\
 & 0.01 \\
 & \underline{0.009} \\
 & 0.001
\end{array}$$

□

Problem 11.7: What is the decimal expansion for $\frac{2}{7}$? How can we be sure it repeats endlessly?

Solution for Problem 11.7:

Dividing 7 into 2 results in 6 digits before 2 is left as a remainder. Continuing the division process, dividing 7 into 2 again looks exactly as it does for the first 6 digits. This means those first 6 digits repeat endlessly, always leaving a remainder of 2 to restart the pattern.

$$\begin{array}{r|l}
 & 0.285714\ldots \\ \hline
7 & 2.000000\ldots \\
 & \underline{1.4} \\
 & 0.60 \\
 & \underline{0.56} \\
 & 0.040 \\
 & \underline{0.035} \\
 & 0.0050 \\
 & \underline{0.0049} \\
 & 0.00010 \\
 & \underline{0.00007} \\
 & 0.000030 \\
 & \underline{0.000028} \\
 & 0.000002
\end{array}$$

We can also determine the decimal forms of other fractions with a denominator of 7. Here we show a few with the first two blocks of their repeating digits:

$$\begin{aligned}
\frac{1}{7} &= 0.142857142857\ldots \\
\frac{3}{7} &= 0.428571428571\ldots \\
\frac{10}{7} &= 1.428571428571\ldots
\end{aligned}$$

□

There is a way for writing repeating decimals that is a little easier than writing out the entire block of repeating digits two or three times to be certain that the repeating block is understood. We draw a line over the entire repeating block of digits to show that those digits repeat:

$$\frac{1}{3} = 0.\overline{3} \qquad \frac{1}{7} = 0.\overline{142857}$$

$$\frac{2}{3} = 0.\overline{6} \qquad \frac{2}{7} = 0.\overline{285714}$$

This convention helps us to more easily write repeating decimals within mathematical statements:

$$0.\overline{285714} + 0.\overline{142857} = 0.\overline{428571}.$$

Note also that some repeating decimals have non-repeating digits before their repeating blocks of decimals. Here are a couple of examples in which we do not write the bar over the non-repeating decimals:

$$\frac{1}{6} = 0.1\overline{6} \qquad\qquad \frac{31}{14} = 2.2\overline{142857}.$$

Problem 11.8: Let $\frac{a}{b}$ be a fraction in lowest terms. For which values of b is $\frac{a}{b}$ a terminating decimal and for which values of b is $\frac{a}{b}$ a repeating decimal?

Solution for Problem 11.8: We begin by looking back at what we've learned about terminating decimals. We know that we can multiply a terminating decimal by a large enough power of 10 to produce an integer. This means that for some natural number m,

$$\frac{a \cdot 10^m}{b} = \frac{a \cdot 2^m \cdot 5^m}{b}$$

is an integer. This means that all the prime factors of b must be present in the numerator. However, none of those prime factors are in the prime factorization of a because $\gcd(a, b) = 1$. This means that if b has any prime divisors other than 2 or 5, then the decimal expansion of $\frac{a}{b}$ does not terminate.

Important: For relatively prime natural numbers a and b, the decimal expansion of $\frac{a}{b}$ terminates if and only if b has no prime divisors other than 2 or 5.

On the other hand, if $\frac{a \cdot 10^m}{b}$ is never an integer, then there is a remainder at every step in the process of long division when b is divided into a.

$$\begin{array}{r|l}
 & 0.153846\ldots \\ \hline
13 & 2.000000\ldots \\
 & \underline{1.3} \\
 & 0.70 \\
 & \underline{0.65} \\
 & 0.050 \\
 & \underline{0.039} \\
 & 0.0110 \\
 & \underline{0.0104} \\
 & 0.00060 \\
 & \underline{0.00052} \\
 & 0.000080 \\
 & \underline{0.000078} \\
 & 0.000002
\end{array}$$

Consider the process of long division used to find the repeating decimal of 2/13. We multiply each new remainder by 10 and continue the division process. However, each remainder must be between 1 and 12 inclusive (0 would mean the fraction terminates, but 13 is a prime other than 2 or 5). Eventually, one of those remainders must repeat itself. From that point, the division process continues exactly as it did from the point at which that remainder showed up the first time. This means that 2/13 is a repeating decimal. In fact, we needed only note that 2/13 never leaves a remainder of 0 in the division process to know that 2/13 is a repeating decimal.

Likewise, so long as b has a prime divisor other than 2 or 5, the process of long division used to expand $\frac{a}{b}$ into decimal form repeats, so $\frac{a}{b}$ is a repeating decimal. □

Important: All rational numbers have either terminating decimal expansions or repeating decimal expansions.

Sidenote: While all rational numbers are either terminating or repeating decimals, irrational numbers have decimal expansions that neither terminate nor repeat. **Irrational numbers** are numbers that cannot be expressed as the ratio between two integers. Here are some familiar examples:

$$\begin{aligned} \sqrt{2} &= 1.41421\ldots \\ \pi &= 3.14159\ldots \\ e &= 2.71828\ldots \end{aligned}$$

These decimals are approximations and as we said before, these blocks of digits do not repeat regularly.

Problem 11.9: Find the decimal expansion of $\frac{1}{12}$.

Solution for Problem 11.9:

$$\begin{array}{r} 0.083\ldots \\ 12\,\overline{)\,1.000\ldots} \\ \underline{0.96} \\ 0.040 \\ \underline{0.036} \\ 0.004 \end{array}$$

We can find the decimal expansion through long division as we do at left. This involves a process of multiplying each remainder by 10 and dividing again. However, multiplying a fraction by powers of 10 can help us convert fractions to decimals more easily. In particular, it helps us in cases where the fraction repeats *and* the denominator contains factors of 2 or 5.

Let's take a look at this second possible method in action. First, we multiply 1/12 by powers of 10 until there are no factors of 2 or 5 left in the denominator:

$$\begin{aligned} \frac{10^1}{12} &= \frac{5}{6} = \frac{5^1}{2^1 \cdot 3^1} \\ \frac{10^2}{12} &= \frac{25}{3} = \frac{5^2}{3^1} \end{aligned}$$

Next, we convert the product of 100 and 1/12 to decimal form. This should be easy at this point as you should know the fraction to decimal conversion of 1/3 quite well:

$$100 \cdot \frac{1}{12} = \frac{25}{3} = 8\frac{1}{3} = 8.\overline{3}.$$

Finally, we divide 100 back out to get 1/12 again, which results in shifting the decimal point two places to the left:

$$\frac{1}{12} = \frac{100 \cdot \frac{1}{12}}{100} = \frac{8.\overline{3}}{100} = 0.08\overline{3}.$$

□

The method outlined in Problem 11.9 usually works best when we can divide factors of 2 or 5 out of the denominator to produce a denominator whose decimal we know well. Here's one more example:

$$\frac{13}{14} = \frac{13}{2 \cdot 7} = \frac{1}{10} \cdot \frac{10 \cdot 13}{2 \cdot 7} = \frac{1}{10} \cdot \frac{65}{7} = (0.1)(9.\overline{285714}) = 0.9\overline{285714}.$$

Exercises

11.3.1 Convert each of the following fractions into decimal numerals.

(a) $\frac{1}{9}$

(b) $\frac{1}{11}$

(c) $\frac{1}{15}$

(d) $\frac{4}{15}$

(e) $\frac{1}{24}$

(f) $\frac{29}{24}$

(g) $\frac{1}{90}$

(h) $\frac{223}{90}$

(i) $\frac{1}{18}$

(j) $\frac{1}{27}$

(k) $\frac{1}{108}$

(l) $\frac{1}{1080}$

11.3.2 Find the 1314^{th} digit past the decimal point in the decimal expansion of $\frac{5}{14}$.

11.4 Converting Decimals to Fractions

We can convert fractions involving integers into their decimal forms using long division, but the problem of converting repeating decimals to fractions is a bit more difficult. In this section we use the repetition process to convert repeating decimals into fractions.

Problems

Problem 11.10: Notice the similarity between the repeating decimals $0.\overline{4}$ and $10 \cdot 0.\overline{4} = 4.\overline{4}$.

(a) Find the difference between $4.\overline{4}$ and $0.\overline{4}$.

(b) Find the ratio between your answer from (a) and $0.\overline{4}$.

(c) Express $0.\overline{4}$ as a fraction in reduced form.

Problem 11.11:
(a) Find the smallest natural number m such that $2.\overline{09}$ and $10^m \cdot 2.\overline{09}$ have the same repeating decimal.
(b) Express $2.\overline{09}$ as a fraction in reduced form.
(c) Express $0.2\overline{09}$ as a fraction in reduced form.

Problem 11.12:
(a) Express $0.\overline{027}$ as a fraction in reduced form.
(b) Express $0.0\overline{027}$ as a fraction in reduced form.

Problem 11.13: What's the difference between 1 and $0.\overline{9}$?

Problem 11.10: Express $0.\overline{4}$ as a fraction in reduced form.

Solution for Problem 11.10: It is at first difficult to grasp how we might convert numbers with repeating decimals into fractions. Focusing on the repeating decimal part gives us a clue. Moving the decimal point over a digit allows us to examine $0.\overline{4}$ in relation to another number with the same repeating decimal part:

$$\begin{aligned} & 0.\overline{4} \\ 10 \cdot 0.\overline{4} &= 4.\overline{4} \end{aligned}$$

We can now create a terminating decimal by subtracting these numbers to rid ourselves of the repeating decimal part:

$$4.\overline{4} - 0.\overline{4} = 4.$$

Motivated by this decimal similarity, we apply algebra to this problem by using a variable to represent $0.\overline{4}$:

$$\begin{aligned} x &= 0.\overline{4} \\ 10x &= 4.\overline{4} \end{aligned}$$

thus,

$$10x - x = 9x = 4.$$

After dividing by 9 we see that $x = 4/9$, so $0.\overline{4} = \dfrac{4}{9}$. □

Concept: Algebraic methods are useful in developing techniques to solve some arithmetic problems. In Problem 11.10 we used algebra to take advantage of the self-similarity of a repeating decimal. We assigned a variable to represent the repeating decimal and found a way to express the variable as a fraction, thereby giving us a way to convert a repeating decimal to a fraction.

Problem 11.11:
(a) Express $2.\overline{09}$ as a fraction in reduced form.
(b) Express $0.2\overline{09}$ as a fraction in reduced form.

Solution for Problem 11.11: Once again we focus on the self-similarity of repeating decimals.

(a) First, we let $x = 2.\overline{09}$. Since there are 2 digits in x's repeating block, we compare x to 10^2x:

$$\begin{aligned} x &= 2.\overline{09} \\ 100x &= 209.\overline{09} \end{aligned}$$

We subtract these numbers to get rid of the repeating decimal:

$$100x - x = 99x = 209.\overline{09} - 2.\overline{09} = 207.$$

Solving for x we have

$$2.\overline{09} = x = \frac{207}{99} = \frac{23}{11}.$$

(b) Note that $2.\overline{09} = 10 \cdot 0.2\overline{09}$. This 10 to 1 ratio allows us to divide our answer from part (a) by 10 to get our answer:

$$0.2\overline{09} = \frac{2.\overline{09}}{10} = \frac{\frac{23}{11}}{10} = \frac{23}{110}.$$

□

Problem 11.12: Express $0.0\overline{027}$ as a fraction in reduced form.

Solution for Problem 11.12: We use the conversion method from Problem 11.11 part (b). Since there are 3 repeating digits, we set $x = 0.0\overline{027}$ and compare it to 10^3x:

$$1000x - x = 999x = 2.\overline{702} - 0.0\overline{027} = 2.7 = \frac{27}{10},$$

thus

$$x = \frac{\frac{27}{10}}{999} = \frac{27}{9990} = \frac{1}{370}.$$

□

Sidenote: Another method for converting repeating decimals to fractions involves summing an infinite geometric series. We rework Problem 11.12 this way:

$$0.0\overline{027} = \frac{27}{10 \cdot 1000^1} + \frac{27}{10 \cdot 1000^2} + \frac{27}{10 \cdot 1000^3} + \cdots = \frac{\frac{27}{10 \cdot 1000}}{1 - \frac{1}{1000}} = \frac{27}{9990} = \frac{1}{370}.$$

After all, decimal digits all have fractional forms and their repetition represents an infinite series.

Problem 11.13: What's the difference between 1 and $0.\overline{9}$?

Solution for Problem 11.13: The number $0.\overline{9}$ presents difficulties for many students of mathematics. Hopefully, the following methods will convince you that the only difference between 1 and $0.\overline{9}$ is the way in which we chose to write them. They are in fact equal.

First, notice that $0.\overline{9} = 3 \cdot 0.\overline{3} = 3 \cdot \frac{1}{3} = 1$. Multiplying integers and fractions makes evaluation of $0.\overline{9}$ easier.

Next, we find the value of $0.\overline{9}$ using algebra. Let $x = 0.\overline{9}$, so

$$\begin{aligned} x &= 0.\overline{9} \\ 10x &= 9.\overline{9} \end{aligned}$$

Subtracting the first equation from the second we see that

$$10x - x = 9.\overline{9} - 0.\overline{9} = 9.$$

Solving $9x = 9$, we get $x = 1$, so $0.\overline{9} = 1$.

If you're still not convinced, try subtracting $0.\overline{9}$ from 1, one step at a time:

$$\begin{aligned} 1 - 0 &= 1 \\ 1 - 0.9 &= 0.1 \\ 1 - 0.99 &= 0.01 \\ 1 - 0.999 &= 0.001 \\ 1 - 0.9999 &= 0.0001 \end{aligned}$$

As we subtract out more and more of the decimal expansion of $0.\overline{9}$ from 1, we find that the difference between 1 and $0.\overline{9}$ gets continually closer to 0. This process never ends and the difference diminishes to a number smaller than any positive number you can think of, so it must be 0. Think about it this way: if there is no number between 1 and $0.\overline{9}$, then they must be the same number!

Finally, we write $0.\overline{9}$ as an infinite geometric series and find its sum:

$$0.\overline{9} = \frac{9}{10^1} + \frac{9}{10^2} + \frac{9}{10^3} + \cdots = \frac{\frac{9}{10}}{1 - \frac{1}{10}} = 1.$$

Think about each of these arguments until you are convinced that $0.\overline{9} = 1$. □

Exercises

11.4.1 Express each of the following as a fraction in lowest terms.

(a) $0.\overline{5}$

(b) $0.00\overline{5}$

(c) $1.\overline{27}$

(d) $0.1\overline{27}$

(e) $4.\overline{054}$

(f) $0.\overline{405}$

(g) $0.\overline{76}$

(h) $0.2\overline{76}$

11.5★ Base Numbers and Decimal Equivalents

Not all numbers are integers—whether we write them as decimals or in other number bases. We now explore how some of these numbers look in bases other than 10. Here are some examples of base numbers that are not integers (far left) along with their decimal equivalents.

$$
\begin{aligned}
0.5_7 &= 5\cdot 7^{-1} &&= \frac{5_7}{10_7} = \frac{5}{7} = 0.\overline{714285}\\
0.101_2 &= 1\cdot 2^{-1}+1\cdot 2^{-3} &&= \frac{101_2}{1000_2} = \frac{5}{8} = 0.625\\
1.32_4 &= 1\cdot 4^{0}+3\cdot 4^{-1}+2\cdot 4^{-2} &&= \frac{132_4}{100_4} = \frac{15}{8} = 1.875\\
88.8_9 &= 8\cdot 9^{1}+8\cdot 9^{0}+8\cdot 9^{-1} &&= \frac{888_9}{10_9} = \frac{728}{9} = 80.\overline{8}
\end{aligned}
$$

For decimals, we call the dot that separates the integral part from the fractional part of the number the "decimal point." For non-decimal base number systems, we need another name:

> **Definition:** In base number systems, the dot used to separate the integral part of a number from the fractional part is called the **radix point**. (**Radix** is just another name for the **base** of a number system.)

Problems

Problem 11.14:
(a) Convert the decimal $0.19\overline{4}$ to a fraction.
(b) Rewrite your fraction from (a) in the form $\frac{a}{6^1}+\frac{b}{6^2}$ where $0 \le a < 6$ and $0 \le b < 6$.
(c) Rewrite your fraction from (b) as a base 6 numeral.

Problem 11.15:
(a) Rewrite 0.24_7 as a fraction in the form $\frac{a}{7^1}+\frac{b}{7^2}$ where $0 \le a < 7$ and $0 \le b < 7$.
(b) Rewrite your fraction from (a) as a single fraction.
(c) Find the first four digits past the decimal point of your fraction from (b).

Problem 11.16: Convert $\frac{717}{343}$ to a base 7 numeral.

Problem 11.17:
(a) Express $\frac{1}{8}$ as a geometric series in which all terms have denominators that are powers of 9 and all of whose numerators are base 9 digits (0-8).
(b) Rewrite your answer from (a) as a base 9 numeral with repeating digits.

Problem 11.14: Convert the decimal $0.19\overline{4}$ to base 6.

Solution for Problem 11.14: In order to convert $0.19\overline{4}$ to base 6, we express it as a sum of base 6 digit bundles using negative powers of 6.

$$6^{-1} = \frac{1}{6^1}, \qquad 6^{-2} = \frac{1}{6^2}, \qquad 6^{-3} = \frac{1}{6^3}, \qquad \cdots$$

It might take a very long time to perform these calculations in decimal form, so we first convert $0.19\overline{4}$ into fractional form:

$$0.19\overline{4} = \frac{175}{900} = \frac{7}{36}.$$

We now begin the process of subtracting out digit bundles of the highest powers of 6 possible:

$$\frac{1}{6} < \frac{7}{36} < \frac{2}{6},$$

so we can subtract 6^{-1} out once:

$$\frac{7}{36} - \frac{1}{6} = \frac{1}{36}.$$

We now rewrite 7/36 as a sum of base 6 digit bundles, thereby converting the decimal numeral $0.19\overline{4}$ to base 6:

$$0.19\overline{4} = \frac{7}{36} = \frac{\mathbf{1}}{\mathbf{6^1}} + \frac{\mathbf{1}}{\mathbf{6^2}} = 1 \cdot 6^{-1} + 1 \cdot 6^{-2} = \mathbf{0.11_6}.$$

□

Problem 11.15: Find the first four digits after the decimal point when 0.24_7 is rewritten as a decimal numeral.

Solution for Problem 11.15: In order to convert 0.24_7 into decimal form, we first find the value of each of its base 7 digits. We begin by expressing 0.24_7 as a sum of base 7 digit bundles:

$$0.24_7 = 2 \cdot 7^{-1} + 4 \cdot 7^{-2} = \frac{\mathbf{2}}{\mathbf{7^1}} + \frac{\mathbf{4}}{\mathbf{7^2}} = \frac{\mathbf{18}}{\mathbf{49}}.$$

Using long division or another method, we find that $\frac{18}{49} = 0.3673\ldots$. □

Sidenote: We can also use a cleverly chosen geometric series to help with Problem 11.15:

$$\frac{18}{49} = \frac{36}{98} = \frac{\frac{36}{100}}{1 - \frac{2}{100}}$$

$$= \frac{36}{100^1} + \frac{72}{100^2} + \frac{144}{100^3} + \cdots = 0.36 + 0.0072 + 0.000144 + \cdots = 0.3673\ldots.$$

Extra! *What would I do if I had only six months to live? I'd type faster.* – Isaac Asimov

Problem 11.16: Convert $\frac{717}{343}$ to a base 7 numeral.

Solution for Problem 11.16: Since we want to rewrite 717/343 in base 7, we begin by rewriting the fraction as a sum of base 7 digit bundles:

$$\frac{717}{343} = 2 + \frac{0}{7^1} + \frac{4}{7^2} + \frac{3}{7^3} = \mathbf{2} \cdot 7^0 + \mathbf{0} \cdot 7^{-1} + \mathbf{4} \cdot 7^{-2} + \mathbf{3} \cdot 7^{-3} = \mathbf{2.043}_7.$$

□

Problem 11.17: Express $\frac{1}{8}$ as a base 9 numeral.

Solution for Problem 11.17: In order to convert 1/8 to base 9, we will have to rewrite it as a sum of base 9 digit bundles. As we begin subtracting out base 9 digit bundles we notice a pattern:

$$\begin{aligned}
\frac{1}{8} - \frac{1}{9^1} &= \frac{1}{8 \cdot 9^1} \\
\frac{1}{8 \cdot 9^1} - \frac{1}{9^2} &= \frac{1}{8 \cdot 9^2} \\
\frac{1}{8 \cdot 9^2} - \frac{1}{9^3} &= \frac{1}{8 \cdot 9^3} \\
\frac{1}{8 \cdot 9^3} - \frac{1}{9^4} &= \frac{1}{8 \cdot 9^4} \\
&\vdots
\end{aligned}$$

We now realize that 1/8 is the sum of a geometric series with first term 1/9 and common ratio 1/9:

$$\frac{1}{8} = \frac{\mathbf{1}}{9^1} + \frac{\mathbf{1}}{9^2} + \frac{\mathbf{1}}{9^3} + \cdots.$$

Now we can use the geometric series to express 1/8 as a sum of base 9 digit bundles which allows us to convert 1/8 to base 9:

$$\frac{1}{8} = \mathbf{1} \cdot 9^{-1} + \mathbf{1} \cdot 9^{-2} + \mathbf{1} \cdot 9^{-3} + \cdots = \mathbf{0.\overline{1}_9}.$$

It might at first surprise some students to learn that there are numbers with repeating digits after the radix point in base numbers. However, they are only strange because we usually write numbers as decimals. □

Extra! **Two Bits, Four Bits, Six Bits, a Dollar!**

For over two centuries, stock prices have been quoted in fractions based on a Spanish money system in which dollar coins were physically broken into "pieces of eight" worth 12.5 cents each.

Exercises

11.5.1 Convert the following fractions to the indicated number bases.

(a) $\frac{19}{64}$ to base 4

(b) $\frac{729}{1331}$ to base 11

(c) $\left(\frac{6}{5}\right)^3$ to base 5

(d) $\frac{1}{12}$ to binary

(e) $\frac{1}{12}$ to base 3

(f) $\frac{1}{7}$ to base 8

(g) $\frac{1}{3}$ to base 7

(h) $\frac{1}{12}$ to base 11

11.5.2 Convert the following base numbers to decimal numerals.

(a) 0.10101_2

(b) $2.\overline{5}_7$

(c) $0.\overline{21}_3$

(d) $3.\overline{4}_{13}$

11.6 Summary

Definitions:

- A number whose decimal representation ends after a finite number of digits has a **terminating decimal** expansion. We simply call these numbers **terminating decimals**.
- A number whose decimal representation becomes an endlessly repeating sequence of digits has a **repeating decimal** expansion. We simply call these numbers **repeating decimals**.
- In base number systems, the dot used to separate the integral part of a number from the fractional part is called the **radix point**. (**Radix** is just another name for the **base** of a number system.)

Concept: Algebraic methods are useful in developing techniques to solve some arithmetic problems.

We combined our understanding of number theory with algebra to determine many useful relationships between decimals and fractions. An understanding of these relationships helps us convert numbers between decimal and fraction forms. We even extended these concepts to other base number systems.

Important: Facts about the relationships between fractions and decimals:

- For a positive integer n, when we divide a decimal number by 10^n, we move the decimal point n places to the left.
- All rational numbers have either terminating decimal expansions or repeating decimal expansions. A fraction in lowest terms whose numerator and denominator are both integers has a repeating decimal expansion if the denominator is divisible by a prime other than 2 or 5. Otherwise, the decimal expansion terminates.
- For a rational number in lowest terms $\frac{a}{b}$, the number of digits past the decimal point needed to write its decimal expansion is the larger of the powers of 2 and 5 in the prime factorization of b.

Concept: When faced with a problem involving the properties of numbers or principles of arithmetic, consider whether it's more illuminating to view the numbers in terms of decimals or fractions. The fact that either one of these forms might shed more light on a particular idea than the other is another example of how we use convenient mathematical forms to solve problems.

REVIEW PROBLEMS

11.18 Express each of the following fractions as decimal numerals.

(a) $\frac{7}{4}$	(f) $\frac{713}{80}$	(k) $\frac{1}{14}$
(b) $-\frac{13}{40}$	(g) $\frac{1}{32}$	(l) $\frac{23}{12}$
(c) $\frac{17}{50}$	(h) $\frac{20}{3}$	(m) $\frac{73}{99}$
(d) $\frac{871}{50}$	(i) $-\frac{7}{9}$	(n) $\frac{89}{990}$
(e) $\frac{513}{250}$	(j) $\frac{62}{7}$	(o) $\frac{3112}{999}$

11.19 How many of the first 10 positive integers have reciprocals that are repeating decimals? *(Source: MATHCOUNTS)*

11.20 Compute: $\dfrac{4!+3!}{3!+2!}$. Express your answer as a decimal to the nearest hundredth.

(Source: MATHCOUNTS)

11.21 Find the 291^{st} digit past the decimal point in the expansion of $\frac{1}{37}$.

11.22 Express each of the following decimal numerals as a fraction in reduced form.

(a) 4.2
(b) 0.08
(c) −1.25
(d) 2.912
(e) $7.\overline{6}$
(f) $0.\overline{4}$
(g) $5.\overline{90}$
(h) $0.5\overline{90}$
(i) $-3.\overline{428571}$
(j) $2.\overline{837}$
(k) $0.2\overline{837}$
(l) $0.1\overline{27}$

Challenge Problems

11.23 Convert the following fractions to the indicated number bases.

(a) 1/25 to base 5.

(b) 130/49 to base 7.

(c) 1/10 to base 8.

11.24 Convert each of the following to base 10.

(a) 11.011_2

(b) $3.\overline{2}_4$

(c) $-0.\overline{41}_6$

11.25 Find the decimal equivalents for each of the following fractions.

(a) $\frac{1}{37}$
(b) $\frac{27}{37}$
(c) $\frac{1}{41}$
(d) $\frac{1}{101}$
(e) $\frac{1000}{101}$
(f) $\frac{1}{17}$
(g) $\frac{1}{85}$
(h) $\frac{1}{95}$
(i) $\frac{1}{21}$

11.26 What is the 4037th digit following the decimal point in the expansion of $\frac{1}{17}$? *(Source: MATHCOUNTS)* **Hints:** 152

11.27 Evaluate the infinite geometric series,

$$\frac{7^0}{100^1}+\frac{7^1}{100^2}+\frac{7^2}{100^3}+\cdots$$

as a fraction and find the first 6 digits in its decimal expansion.

11.28 Let p be a prime number other than 2 or 5. What is the maximum possible number of digits in the repeating block of digits in $1/p$? **Hints:** 70

11.29

(a) How many digits are in the decimal expansion of 10^{30}?

(b) How many digits are in the decimal expansion of 2^{30}? **Hints:** 114

(c) How many digits are in the decimal expansion of 5^{30}? **Hints:** 30

11.30 What are the first 18 digits in the decimal expansion of $\frac{1}{998}$? **Hints:** 45, 89

11.31 Suppose that a and b are digits, not both nine and not both zero, and the repeating decimal $.\overline{ab}$ is expressed as a fraction in lowest terms. How many different denominators are possible? *(Source: AHSME)* **Hints:** 5

11.32 We noted that when $\gcd(m, n) = 1$, the fraction m/n has a terminating decimal representation if and only if the prime factorization of n contains no primes other than 2 or 5. Suppose we look at the expansion (past the radix point) of m/n in base 8—for what values of n will the radix expansion of m/n terminate and for what values of n will it repeat? Can you generalize to other number bases? **Hints:** 18

Extra! Here are a few interesting, but more difficult number theory problems whose solutions can be found in the forums at www.artofproblemsolving.com:

- Let $N = .136051865568150631001360 51\ldots$ be the decimal whose digits past the decimal point are the units digits of all triangular numbers (increasing from $1, 3, 6, 10, \ldots$). Determine with proof whether N is rational or irrational.

- Prove that every odd square in the octonary system (base 8) has a units digit of 1. Prove also that if this units digit 1 is snipped off, the remaining part is always a triangular number:

$$\begin{array}{lcl} & \vdots & \\ 11_8^2 = 121_8 & \rightarrow & 12_8 = 10 = 1+2+3+4 \\ 13_8^2 = 171_8 & \rightarrow & 17_8 = 15 = 1+2+3+4+5 \\ 15_8^2 = 251_8 & \rightarrow & 25_8 = 21 = 1+2+3+4+5+6 \\ & \vdots & \end{array}$$

- Prove that every positive integer that can be written using only 1 as each digit in base 9 is a triangular number:

$$\begin{array}{rcrcl} 1_9 & = & 1 & = & 1 \\ 11_9 & = & 10 & = & 1+2+3+4 \\ 111_9 & = & 91 & = & 1+2+\cdots+13 \\ 1111_9 & = & 820 & = & 1+2+\cdots+40 \\ & \vdots & & \vdots & \end{array}$$

- Find all natural numbers n such that it is possible to construct a sequence in which each number $1, 2, 3, \ldots, n$ appears twice, the second of the appearances of each integer r being r places beyond the first appearance. For instance, for $n = 4$, a possible sequence is
$$4, 2, 3, 2, 4, 3, 1, 1.$$
Also, for $n = 5$, a possible sequence is
$$3, 5, 2, 3, 2, 4, 5, 1, 1, 4.$$

- Prove that infinitely many triangular numbers are perfect squares.

- Prove that the product of 8 consecutive integers cannot be the square of a perfect square (a perfect fourth power).

Versions of these problems are collected in *Mathematical Morsels* by Ross Honsberger.

"Can you do addition?" the White Queen asked. "What's one and one and one and one and one and one and one and one and one and one?" "I don't know," said Alice. "I lost count." – Lewis Carroll

CHAPTER 12 Introduction to Modular Arithmetic

12.1 Introduction

We sometimes think of numbers as they appear on a number line—stretching out infinitely in each direction. We base our normal system of arithmetic on the ways numbers relate to each other on the number line. At other times, we think of numbers as repeating in cycles. We think of 7 P.M. as being the same time every evening, even though we never experience the same moment in time more than once. In this chapter we develop a system of arithmetic around this kind of cyclical number system.

In the grid below, times since the beginning of New Year's Day, are compared with times as we see them on clocks. See how many patterns you can find in the numbers:

Hours Since New Year:	1	2	3	4	5	6	7	8	9	10	11	12
Time:	1 A.M.	2 A.M.	3 A.M.	4 A.M.	5 A.M.	6 A.M.	7 A.M.	8 A.M.	9 A.M.	10 A.M.	11 A.M.	12 P.M.
Hours Since New Year:	13	14	15	16	17	18	19	20	21	22	23	24
Time:	1 P.M.	2 P.M.	3 P.M.	4 P.M.	5 P.M.	6 P.M.	7 P.M.	8 P.M.	9 P.M.	10 P.M.	11 P.M.	12 A.M.
Hours Since New Year:	25	26	27	28	29	30	31	32	33	34	35	36
Time:	1 A.M.	2 A.M.	3 A.M.	4 A.M.	5 A.M.	6 A.M.	7 A.M.	8 A.M.	9 A.M.	10 A.M.	11 A.M.	12 P.M.
Hours Since New Year:	37	38	39	40	41	42	43	44	45	46	47	48
Time:	1 P.M.	2 P.M.	3 P.M.	4 P.M.	5 P.M.	6 P.M.	7 P.M.	8 P.M.	9 P.M.	10 P.M.	11 P.M.	12 A.M.
⋮												
Hours Since New Year:	133	134	135	136	137	138	139	140	141	142	143	144
Time:	1 P.M.	2 P.M.	3 P.M.	4 P.M.	5 P.M.	6 P.M.	7 P.M.	8 P.M.	9 P.M.	10 P.M.	11 P.M.	12 A.M.
Hours Since New Year:	145	146	147	148	149	150	151	152	153	154	155	156
Time:	1 A.M.	2 A.M.	3 A.M.	4 A.M.	5 A.M.	6 A.M.	7 A.M.	8 A.M.	9 A.M.	10 A.M.	11 A.M.	12 P.M.
Hours Since New Year:	157	158	159	160	161	162	163	164	165	166	167	168
Time:	1 P.M.	2 P.M.	3 P.M.	4 P.M.	5 P.M.	6 P.M.	7 P.M.	8 P.M.	9 P.M.	10 P.M.	11 P.M.	12 A.M.

12.2 Congruence

Problems

Problem 12.1: The clock below has only five numbers on its face: 0, 1, 2, 3 and 4. The clock has only one hand which moves around the circular face from 0 to 1 to 2 to 3 to 4 and back to 0 in that order. We set the clock to 0 and let it begin ticking clockwise. The first 12 numbers it hits are 1, 2, 3, 4, 0, 1, 2, 3, 4, 0, 1, and 2.

(a) To what number does the clock point after 20 ticks?
(b) To what number does the clock point after 21 ticks?
(c) To what number does the clock point after 22 ticks?
(d) To what number does the clock point after 25 ticks?
(e) To what number does the clock point after 29 ticks?
(f) To what number does the clock point after 30 ticks?
(g) To what number does the clock point after 36 ticks?
(h) To what number does the clock point after 41 ticks?
(i) To what number does the clock point after 593 ticks?

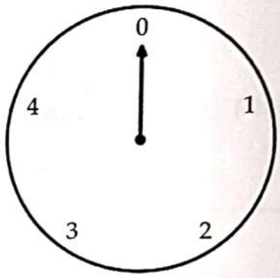


Figure 12.1

Problem 12.2: Build a 10 row grid of integers according to the following rules:

(i) Place 4 integers in each row.
(ii) Let 0 be the leftmost integer in the top row.
(iii) For any pair of consecutive integers in a row, make the integer on the right 1 more than the integer on its left.
(iv) Make the first integer in each row after the first row 1 more than the last integer in the previous row.

Your first two rows should look like this:

0	1	2	3
4	5	6	7

(a) Which integers in the grid are in the same column as 0?
(b) Which integers in the grid are in the same column as 1?
(c) Which integers in the grid are in the same column as 2?
(d) Which integers in the grid are in the same column as 3?
(e) If you extended your grid to include a thousand rows, would the integer 3713 be in the same column as 0, 1, 2, or 3?

Extra! *Convictions are more dangerous enemies of truth than lies.* – Friedrich Nietzsche

Problem 12.3: Imagine a grid built like the one in the previous problem (starting at 0 and counting up) that has 7 columns instead of 4.

(a) How many of the 100 smallest natural numbers will be in the same column as 0?

(b) How many of the 100 smallest natural numbers will be in the same column as 1?

(c) How many of the 100 smallest natural numbers will be in the same column as 2?

(d) How many of the 100 smallest natural numbers will be in the same column as 3?

(e) How many of the 100 smallest natural numbers will be in the same column as 4?

(f) How many of the 100 smallest natural numbers will be in the same column as 5?

(g) How many of the 100 smallest natural numbers will be in the same column as 6?

Problem 12.1: Consider a list of integers starting with 1, 2, 3, 4, 0, 1, 2, 3, 4, and 0. After each 0 is a 1, after each 1 is a 2, after each 2 is a 3, after each 3 is a 4, and after each 4 is a 0.

(a) What integer is the 20^{th} number on the list?

(b) What integer is the 21^{st} number on the list?

(c) What integer is the 22^{nd} number on the list?

(d) What integer is the 25^{th} number on the list?

(e) What integer is the 29^{th} number on the list?

(f) What integer is the 30^{th} number on the list?

(g) What integer is the 36^{th} number on the list?

(h) What integer is the 41^{st} number on the list?

(i) What integer is the 593^{rd} number on the list?

Solution for Problem 12.1: The clock in Figure 12.1 helps represent the process of counting using only the 5 integers 0, 1, 2, 3, and 4. Let's take a look at the first 50 numbers in the list and also the first 50 counting numbers side-by-side:

1	2	3	4	0
1	2	3	4	0
1	2	3	4	0
1	2	3	4	**0**
1	**2**	3	4	**0**
1	2	3	**4**	**0**
1	2	3	4	0
1	2	3	4	0
1	2	3	4	0
1	2	3	4	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**
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

The answers to the first 8 problem parts are in bold and we see their positions matched in the two grids. Together, the grids match where each positive integer falls on the 5-numbered clock. In fact, each clock position, represented in the grid on the left, is just the remainder when each integer in the right grid is divided by 5. If we added enough rows, the 593rd integer in the grid on the left would be the remainder of $593 \div 5$, which is 3. Likewise, the clock points to 3 after 593 ticks. □

In Problem 12.1 we counted using only the 5 integers 0, 1, 2, 3, and 4. We call this system for counting **modulo** 5.

> **Definition:** A **modulus** is a system for counting using only the fixed set of integers $0, 1, 2, \ldots, m-1$. When working in this modulus of m integers, we say that we are working with the integers **modulo** m.

We can also count in modulo 2, modulo 3, modulo 4, or in any other modulus. We can even count backwards. Take a look at the values of some integers along side their values in modulo 6:

1	**2**	3	4	5	0		−11	**−10**	−9	−8	−7	−6
1	2	3	4	5	**0**		−5	−4	−3	−2	−1	**0**
1	2	3	4	5	0		1	2	3	4	5	6
1	2	3	**4**	5	0		7	8	9	**10**	11	12
1	2	3	4	5	0		13	14	15	16	17	18
1	2	3	4	5	0		19	20	21	22	23	24
1	2	3	4	5	0		25	26	27	28	29	30

Consider a one-handed clock with 6 numbers in order: 0, 1, 2, 3, 4, and 5. When we count counterclockwise 10 ticks from 0 (like counting down from 0 to **−10**), we end up at **2**. When we count clockwise **10** ticks from 0, the clock points to **4**. An integer and its additive inverse don't necessarily end up in the same place on the clock!

Problem 12.2: Build a 10 row grid with 4 integers in each row. Make the leftmost integer in the top row 0 and count upwards. Your first two rows should look like this:

$$\begin{matrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \end{matrix}$$

(a) Which integers in the grid are in the same column as 0?

(b) Which integers in the grid are in the same column as 1?

(c) Which integers in the grid are in the same column as 2?

(d) Which integers in the grid are in the same column as 3?

(e) If you extended your grid to include a thousand rows, would the integer 3713 be in the same column as 0, 1, 2, or 3?

Sidenote: Carl Friedrich Gauss first introduced modular arithmetic to the mathematical world in his landmark book *Disquisitiones Arithmeticae* published in 1801. His motto, "few, but ripe," understates a description of his work. While not as prolific in publication as many mathematicians, Gauss made extremely important contributions to numerous areas of mathematics and physics. Many mathematicians consider Gauss the greatest mathematician of all time.

Solution for Problem 12.2:

In the grid on the right, each column counts up by 4's starting at 0, 1, 2, or 3. In essence, the grid groups all the multiples of 4 in the first column, integers that are 1 more than multiples of 4 in the next column, integers that are 2 more than multiples of 4 in the third column, and integers that are 3 more than multiples of 4 in the last column.

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	26	27
28	29	30	31
32	33	34	35
36	37	38	39

In order to determine which column 3713 would be in, we divide it by 4. Since the remainder is 1, 3713 is 1 more than a multiple of 4 and will fall into the second column along with $1, 5, 9, \ldots$. □

Since there are only 4 values in modulo 4, many of our regular integers share the same modulo 4 values. For instance, in Problem 12.2 we noted that 3713 has the same value as 1 in modulo 4.

> **Definition:** We say that two integers are **congruent** or **equivalent** modulo m when their difference is a multiple of m. Otherwise, they are **incongruent** in modulo m.

Two integers are congruent in a modulus when they share the same value. For instance, 3713 and 1 are congruent in modulo 4. From the counting grid in Problem 12.2, we see that 8 and 28 are congruent in modulo 4 and so are 17 and 33. We use the symbol "≡" to express congruence and shorten "modulus" to "mod":

$$8 \equiv 28 \pmod{4} \quad \text{and} \quad 17 \equiv 33 \pmod{4}.$$

Since 25 and 38 do not share the same column, we see that they are incongruent in modulo 4. We write

$$25 \not\equiv 38 \pmod{4} \quad \text{and} \quad 12 \not\equiv 7 \pmod{4}.$$

Now, for positive integers a and b, we have $a \equiv b \pmod{m}$ if and only if the difference between a and b is a multiple of m. This means that for some integer k, that $a - b = km$. Dividing by m to isolate k, we get

$$k = \frac{a-b}{m}.$$

The fraction on the right-hand side is an integer if and only if a and b are congruent modulo m.

> **Important:** For integers a and b, we say that $a \equiv b \pmod{m}$ if and only if $\frac{a-b}{m}$ is an integer. Otherwise, $a \not\equiv b \pmod{m}$.

> **Extra!** *A moment comes, which comes but rarely in history, when we step out from the old to the new, when an age ends, and when the sound of a nation, long suppressed, finds utterance.*
>
> – Jawaharial Nehru

Problem 12.3: Of the 100 smallest natural numbers, how many are congruent to each of the following?

(a) 0 (mod 7)
(b) 1 (mod 7)
(c) 2 (mod 7)
(d) 3 (mod 7)
(e) 4 (mod 7)
(f) 5 (mod 7)
(g) 6 (mod 7)

Solution for Problem 12.3: We solve this problem by building a counting grid and simply counting how many of the 100 smallest natural numbers are in each row. However, we use a bit of algebra to improve on our use of counting grids. We write each number in the same column as 0 as $7n$, for integers n. We write each number in the same column as 1 as $7n+1$, for integers n. Similar parametric expressions relate the integers in each of the other columns:

Column 0	Column 1	Column 2	Column 3	Column 4	Column 5	Column 6
$7n$	$7n+1$	$7n+2$	$7n+3$	$7n+4$	$7n+5$	$7n+6$

Each integer n corresponds to a row in our grid:

	$7n$	$7n+1$	$7n+2$	$7n+3$	$7n+4$	$7n+5$	$7n+6$
$n=0$	0	1	2	3	4	5	6
$n=1$	7	8	9	10	11	12	13
$n=2$	14	15	16	17	18	19	20
$n=3$	21	22	23	24	25	26	27
$n=4$	28	29	30	31	32	33	34
$n=5$	35	36	37	38	39	40	41
$n=6$	42	43	44	45	46	47	48
$n=7$	49	50	51	52	53	54	55
$n=8$	56	57	58	59	60	61	62
$n=9$	63	64	65	66	67	68	69
$n=10$	70	71	72	73	74	75	76
$n=11$	77	78	79	80	81	82	83
$n=12$	84	85	86	87	88	89	90
$n=13$	91	92	93	94	95	96	97
$n=14$	98	99	100				

The positive integers up to 100 that are congruent to 0 (mod 7) correspond to values of $7n$ for $n=1$ up to $n=14$. Now it's easy to see that there are 14 of them. The positive integers up to 100 that are congruent to 1 (mod 7) correspond to the values of $7n+1$ for $n=0$ to $n=14$, so there are 15 of them. Similarly, 15 of the positive integers above are congruent to 2 (mod 7) and 14 of them are congruent to each of 3, 4, 5, and 6 (mod 7). □

We generate the integers in each column of the counting grid in Problem 12.3 above by plugging integers into a particular parametric expression.

Extra! *Intellectuals are people who believe that ideas are of more importance than values. That is to say, their own ideas and other people's values.* – Gerald Brenan

Important: Parametric expressions give us another way to tell when two integers are congruent in a given modulus:

For two integers a and b, $a \equiv b \pmod{m}$ if and only if

$$\begin{aligned} a &= q_1 m + r \\ b &= q_2 m + r \end{aligned}$$

where q_1, q_2, and r are integers and $0 \le r < m$.

This helps us apply modular arithmetic to counting and algebra problems.

Exercises

12.2.1

$$1, 2, 3, 4, 5, 6, 7, 8, 0, 1, 2, 3, 4, 5, 6, 7, 8, 0, 1, \ldots$$

Here we count up in modulo 9 (starting at 1) where the only integers are 0, 1, 2, 3, 4, 5, 6, 7, and 8. Counting up from 8 we go back to 0 and start over.

(a) What is the 22^{nd} number in the list?
(b) What is the 25^{th} number in the list?
(c) What is the 26^{th} number in the list?
(d) What is the 27^{th} number in the list?
(e) What is the 28^{th} number in the list?
(f) What is the 37^{th} number in the list?
(g) What is the 84^{th} number in the list?
(h) What is the 99^{th} number in the list?
(i) What is the 2023^{rd} number in the list?
(j) If some member of the list is 3, how many members later will the next 3 appear?
(k) If some member of the list is 7, how many members later will the next 3 appear?
(l) If some member of the list is 5, how many members later will the next 4 appear?

12.2.2 Which of the following integers are congruent to 6 (mod 8)?

(a) -18
(b) 27
(c) 54
(d) 254
(e) 754
(f) 1036
(g) 6310
(h) 13254

12.2.3 Which of the following integers are congruent to 3 (mod 11)?

(a) -311
(b) -8
(c) 8
(d) 33
(e) 410
(f) 2379

12.2.4 Which of the following integers are congruent to 0 (mod 15)?

(a) -415
(b) -75
(c) 25
(d) 155
(e) 555
(f) 7275

12.2.5 Which of the following statements of modular congruence are true and which are false?

(a) $118 \equiv 25 \pmod{13}$
(b) $2401 \equiv 147 \pmod{49}$
(c) $183 \equiv 291 \pmod{6}$
(d) $2701 \equiv 14393 \pmod{8}$
(e) $493 \equiv 873 \pmod{10}$
(f) $4113 \equiv 396 \pmod{9}$

12.2.6 How many of the 200 smallest natural numbers are congruent to 1 (mod 9)?

12.3 Residues

Problems

Problem 12.4:
(a) Find the greatest multiple of 12 less than or equal to each of the following integers:

137 97 68 −97 177 −46 124 43 238 72 102 39

(b) Write each of those integers in the form $12n + r$ where n and r are integers and $0 \le r < 12$.
(c) Arrange the following integers in pairs that are congruent in modulo 12.

0	1	2	3	4	5	6	7	8	9	10	11
137	97	68	−97	177	−46	124	43	238	72	102	39

Problem 12.5: List all integers between −100 and 100 that are congruent to 5 (mod 9).

Problem 12.6: Note that $207 \equiv 25 \pmod{7}$, $25 \equiv 4 \pmod{7}$, and $207 \equiv 4 \pmod{7}$. Is it always true that when $a \equiv b \pmod{7}$ and $b \equiv c \pmod{7}$, then $a \equiv c \pmod{7}$?

Problem 12.4: Arrange the following integers in pairs that are congruent in modulo 12.

0	1	2	3	4	5	6	7	8	9	10	11
137	97	68	−97	177	−46	124	43	238	72	102	39

Extra! *Better make it six, I can't eat eight.* – Dan Osinski, baseball pitcher, when a waitress asked if he wanted his pizza cut into six or eight slices.

Solution for Problem 12.4:

$$\begin{array}{rcrcrl}
72 &=& 6\cdot 12+\mathbf{0} &\equiv& 0 & \pmod{12}\\
97 &=& 8\cdot 12+\mathbf{1} &\equiv& 1 & \pmod{12}\\
-46 &=& -4\cdot 12+\mathbf{2} &\equiv& 2 & \pmod{12}\\
39 &=& 3\cdot 12+\mathbf{3} &\equiv& 3 & \pmod{12}\\
124 &=& 10\cdot 12+\mathbf{4} &\equiv& 4 & \pmod{12}\\
137 &=& 11\cdot 12+\mathbf{5} &\equiv& 5 & \pmod{12}\\
102 &=& 8\cdot 12+\mathbf{6} &\equiv& 6 & \pmod{12}\\
43 &=& 3\cdot 12+\mathbf{7} &\equiv& 7 & \pmod{12}\\
68 &=& 5\cdot 12+\mathbf{8} &\equiv& 8 & \pmod{12}\\
177 &=& 14\cdot 12+\mathbf{9} &\equiv& 9 & \pmod{12}\\
238 &=& 19\cdot 12+\mathbf{10} &\equiv& 10 & \pmod{12}\\
-97 &=& -9\cdot 12+\mathbf{11} &\equiv& 11 & \pmod{12}
\end{array}$$

We divide each of the integers in the second row by 12 to find a quotient and remainder. For instance, $137 \div 12 = 11$ R 5. We then rewrite 137 in terms of 12, 11, and 5:

$$137 = 11 \cdot 12 + 5.$$

Subtracting 5 from both sides, we see that $137-5$ is a multiple of 12:

$$137 - 5 = 11 \cdot 12.$$

This means $137 \equiv 5 \pmod{12}$.

□

Definition: We say that r is the modulo m **residue** of n when $n \equiv r \pmod{m}$ and $0 \le r < m$.

In Problem 12.4 we found the modulo 12 residues of each of a dozen integers.

Problem 12.5: List all integers between -100 and 100 whose modulo 9 residues are 5.

Solution for Problem 12.5: An integer has a modulo 9 residue of 5 when it can be written as $9n+5$ for some integer n. This means we can identify the integers we are looking for by identifying possible values of n such that

$$-100 < 9n + 5 < 100.$$

Subtracting 5 from all parts of the inequality we get

$$-105 < 9n < 95.$$

Dividing everything by 9 we see that $-11\frac{2}{3} < n < 10\frac{5}{9}$. Since n is an integer, we know that $-11 \le n \le 10$. We generate the 22 integers between -100 and 100 using these values of n:

$$\begin{array}{rcrrcr}
n &=& -11: & 9(-11)+5 &=& -94\\
n &=& -10: & 9(-10)+5 &=& -85\\
n &=& -9: & 9(-9)+5 &=& -76\\
n &=& -8: & 9(-8)+5 &=& -67\\
n &=& -7: & 9(-7)+5 &=& -58\\
n &=& -6: & 9(-6)+5 &=& -49\\
n &=& -5: & 9(-5)+5 &=& -40\\
n &=& -4: & 9(-4)+5 &=& -31\\
n &=& -3: & 9(-3)+5 &=& -22\\
n &=& -2: & 9(-2)+5 &=& -13\\
n &=& -1: & 9(-1)+5 &=& -4
\end{array}
\qquad
\begin{array}{rcrrcr}
n &=& 0: & 9(0)+5 &=& 5\\
n &=& 1: & 9(1)+5 &=& 14\\
n &=& 2: & 9(2)+5 &=& 23\\
n &=& 3: & 9(3)+5 &=& 32\\
n &=& 4: & 9(4)+5 &=& 41\\
n &=& 5: & 9(5)+5 &=& 50\\
n &=& 6: & 9(6)+5 &=& 59\\
n &=& 7: & 9(7)+5 &=& 68\\
n &=& 8: & 9(8)+5 &=& 77\\
n &=& 9: & 9(9)+5 &=& 86\\
n &=& 10: & 9(10)+5 &=& 95
\end{array}$$

These are the integers between -100 and 100 that are congruent to 5 (mod 9). □

Definition: The integers congruent to r modulo m make up a **residue class**. Residue classes are also known as **congruence classes** or **equivalence classes**.

For instance, the integers $-94, -85, -76, \ldots, 86, 95$, and all other integers congruent to 5 (mod 9) make up a modulo 9 residue class. Going back to Problem 12.3, we see that 5, 12, 19, etc., are part of a modulo 7 residue class. We can think of a residue class as the group of integers that share the same column in a counting grid (as we have constructed them in this chapter).

Problem 12.6: Is it always true that when $a \equiv b \pmod 7$ and $b \equiv c \pmod 7$, then $a \equiv c \pmod 7$?

Solution for Problem 12.6: Let's first take a look at an algebraic solution, then one that rests on the intuition we have developed thus far.

Solution 1: Since $a \equiv b \pmod 7$, we have $a - b = 7j$ for some integer j. Since $b \equiv c \pmod 7$, we have $b - c = 7k$ for some integer k. Adding our two equations, we get

$$(a - b) + (b - c) = 7j + 7k.$$

Simplifying the left-hand side and factoring the right-hand side, we get

$$a - c = 7(j + k).$$

Since $j + k$ is an integer, $a - c$ is a multiple of 7. Thus $a \equiv c \pmod 7$.

Solution 2: Since $a \equiv b \pmod 7$, a and b share the same column of a 7-column counting grid (a and b have the same residue). Likewise, $b \equiv c \pmod 7$, so b and c share the same column. This column contains a, b, and c, so $a \equiv c \pmod 7$. □

There was nothing special about modulo 7 that helped us solve Problem 12.6, so we declare a more general result. Make sure you understand why it's true:

Important: If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$.

Exercises

12.3.1 List all the modulo 3 residues.

12.3.2 Write each of the following integers in the form $8n + r$ where n and r are integers and $0 \le r < 8$.

(a) 11
(b) 23
(c) 54
(d) 99
(e) 434
(f) 812

12.3.3 Determine the residue of each of the following within the given modulus.

(a) 71 (mod 3)
(b) −14 (mod 8)
(c) 14 (mod 8)
(d) 194 (mod 11)
(e) 3944 (mod 9)
(f) 471 (mod 21)

12.3.4 Find the modulo 6 residue of each of the following.

(a) 11
(b) 23
(c) 37
(d) 54
(e) 99
(f) 219
(g) 434
(h) 812
(i) 1529

12.3.5 Prove that if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$. (Try first without looking back through the section!)

12.4 Addition and Subtraction

We know how counting works in a modulus. Now we'll do what we did in Chapter 1 with our regular system of numbers—we'll construct a useful system of arithmetic. We begin with addition and subtraction.

Problems

Problem 12.7:

	Column 0 $8n$	Column 1 $8n+1$	Column 2 $8n+2$	Column 3 $8n+3$	Column 4 $8n+4$	Column 5 $8n+5$	Column 6 $8n+6$	Column 7 $8n+7$
$n=0$	0	1	2	3	4	5	6	7
$n=1$	8	9	10	11	12	13	14	15
$n=2$	16	17	18	19	20	21	22	23
$n=3$	24	25	26	27	28	29	30	31

Notice that $1 \equiv 9 \equiv 17 \equiv 25 \pmod{8}$. Notice also that if we count up 1 from each of those integers, that the results are congruent modulo 8:

$$1+1 \equiv 9+1 \equiv 17+1 \equiv 25+1 \pmod{8}.$$

Let a_1 and a_2 be integers such that $a_1 \equiv a_2 \pmod{8}$.

(a) Show that $a_1 + 1 \equiv a_2 + 1 \pmod{8}$.

(b) Show that $a_1 - 1 \equiv a_2 - 1 \pmod{8}$.

(c) Show that $a_1 + b \equiv a_2 + b \pmod{8}$ for any integer b.

Problem 12.8: Let a_1, a_2, b_1, and b_2 be integers such that

$$\begin{aligned} a_1 &\equiv a_2 \pmod{m} \\ b_1 &\equiv b_2 \pmod{m} \end{aligned}$$

(a) Explain why $a_1 + b_1 \equiv a_1 + b_2 \pmod{m}$.

(b) Explain why $a_1 + b_2 \equiv a_2 + b_2 \pmod{m}$.

(c) Explain why $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$.

Problem 12.9: Note each of the following:

$$\begin{aligned} 6004 &= 1000 \cdot 6 + 4 \\ 603 &= 100 \cdot 6 + 3 \\ 65 &= 10 \cdot 6 + 5 \end{aligned}$$

Explain a way to quickly find the remainder when $6004 + 603 - 65 - 6$ is divided by 6.

Problem 12.10: The remainders when two natural numbers are divided by 16 are 11 and 14 respectively.

(a) Find the remainder when their sum is divided by 16.

(b) Find the remainder when their sum is divided by 8.

Problem 12.11: Eric's teacher asked him to find the remainder when the sum of the following 201-term arithmetic series is divided by 5:

$$2 + 7 + 12 + \cdots + 1002.$$

At first, Eric began to apply his knowledge of algebra to sum the series. Then Eric realized that each of the terms in the arithmetic progression is congruent to 2 (mod 5). This allowed him to find the answer more quickly. How did he do it?

Problem 12.7: Let a_1 and a_2 be integers such that $a_1 \equiv a_2 \pmod 8$.

(a) Show that $a_1 + 1 \equiv a_2 + 1 \pmod 8$.

(b) Show that $a_1 - 1 \equiv a_2 - 1 \pmod 8$.

(c) Show that $a_1 + b \equiv a_2 + b \pmod 8$ for any integer b.

Solution for Problem 12.7:

	Column 0 $8n$	Column 1 $8n+1$	Column 2 $8n+2$	Column 3 $8n+3$	Column 4 $8n+4$	Column 5 $8n+5$	Column 6 $8n+6$	Column 7 $8n+7$
$n=0$	0	1	2	3	4	5	6	7
$n=1$	8	9	10	11	12	13	14	15
$n=2$	16	17	18	19	20	21	22	23
$n=3$	24	25	26	27	28	29	30	31

(a) The 8-column counting grid helps us compare integers in modulo 8. Integers a_1 and a_2 are congruent modulo 8 when they're in the same column. Counting up 1 from a_1 and a_2 brings us to $a_1 + 1$ and $a_2 + 1$. Intuitively, we see that $a_1 + 1$ and $a_2 + 1$ share the same column. This means that when $a_1 \equiv a_2 \pmod 8$, then also $a_1 + 1 \equiv a_2 + 1 \pmod 8$.

A more rigorous algebra proof follows from the fact that two integers are congruent modulo 8 when their difference is a multiple of 8. Since $a_1 \equiv a_2 \pmod 8$, we know that

$$\frac{a_1 - a_2}{8}$$

is an integer. However, this fraction equals

$$\frac{a_1 + 1 - a_2 - 1}{8} = \frac{(a_1 + 1) - (a_2 + 1)}{8}.$$

Since the last fraction is an integer, $a_1 + 1 \equiv a_2 + 1 \pmod 8$.

(b) We can count backwards just as easily as we can count upwards. Again, a_1 and a_2 are in the same column. Counting down 1 from each bring us to $a_1 - 1$ and $a_2 - 1$, which also share a column. This means that when $a_1 \equiv a_2 \pmod 8$, then also $a_1 - 1 \equiv a_2 - 1 \pmod 8$.

Again, we provide an algebraic proof. Since $a_1 \equiv a_2 \pmod 8$, we know that

$$\frac{a_1 - a_2}{8}$$

is an integer. This fraction equals

$$\frac{a_1 - 1 - a_2 + 1}{8} = \frac{(a_1 - 1) - (a_2 - 1)}{8}.$$

Since the last fraction is an integer, $a_1 - 1 \equiv a_2 - 1 \pmod 8$.

(c) Recall that addition and subtraction of integers is just a fast way of counting. Counting up or down 1 (in modulo 8) from each of a pair of congruent integers results in another pair of congruent integers. Repeating this process $|b|$ times, we count up or down from a_1 and a_2 to a pair of integers that are congruent modulo 8: $a_1 + b \equiv a_2 + b \pmod 8$.

Now we provide an algebraic proof: Since $a_1 \equiv a_2 \pmod 8$, we know that

$$\frac{a_1 - a_2}{8}$$

is an integer. This fraction equals

$$\frac{a_1 + b - a_2 - b}{8} = \frac{(a_1 + b) - (a_2 + b)}{8}.$$

This last fraction is an integer, so $a_1 + b \equiv a_2 + b \pmod 8$.

□

Problem 12.8: Let a_1, a_2, b_1, and b_2 be integers such that

$$a_1 \equiv a_2 \pmod m$$
$$b_1 \equiv b_2 \pmod m$$

Show that $a_1 + b_1 \equiv a_2 + b_2 \pmod m$.

Solution for Problem 12.8: Nothing we did along the way of solving Problem 12.7 depended on the value of the modulus. We follow the same algebraic approach to any modulus m. From the definition of congruence, we know that

$$\frac{a_1 - a_2}{m} \quad \text{and} \quad \frac{b_1 - b_2}{m}$$

are integers. We manipulate each of these integers into different forms:

$$\begin{aligned}\frac{b_1 - b_2}{m} &= \frac{a_1 + b_1 - a_1 - b_2}{m} = \frac{(a_1 + b_1) - (a_1 + b_2)}{m}\\ \frac{a_1 - a_2}{m} &= \frac{a_1 + b_2 - a_2 - b_2}{m} = \frac{(a_1 + b_2) - (a_2 + b_2)}{m}\end{aligned}$$

Since each of the quantities on the right is an integer, we have

$$\begin{aligned}a_1 + b_1 &\equiv a_1 + b_2 \pmod{m}\\ a_1 + b_2 &\equiv a_2 + b_2 \pmod{m}\end{aligned}$$

Putting these two congruences together, we have

$$a_1 + b_1 \equiv a_1 + b_2 \equiv a_2 + b_2 \pmod{m}.$$

Most importantly, we see that $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$. □

Important: Let a_1, a_2, b_1, and b_2 satisfy

$$\begin{aligned}a_1 &\equiv a_2 \pmod{m}\\ b_1 &\equiv b_2 \pmod{m}\end{aligned}$$

Addition of these integers holds as follows:

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{m}.$$

Notice that when we add units digits to find units digits of sums, we are doing the same thing as if we added modulo 10 residues:

$$137 + 592 \equiv 7 + 2 \equiv 9 \pmod{10},$$

which is the units digit of $137 + 592 = 729$.

Problem 12.9: Note each of the following:

$$\begin{aligned}6004 &= 1000 \cdot 6 + 4\\ 603 &= 100 \cdot 6 + 3\\ 65 &= 10 \cdot 6 + 5\end{aligned}$$

Explain a way to quickly find the remainder when $6004 + 603 - 65 - 6$ is divided by 6.

Solution for Problem 12.9: We could just perform the arithmetic first, then find the remainder. However, each integer is congruent to its modulo 6 residue, so we can set ourselves up to solve a simpler problem:

$$\begin{aligned}6004 + 603 - 65 - 6 &\equiv 4 + 603 - 65 - 6\\ &\equiv 4 + 3 - 65 - 6\\ &\equiv 4 + 3 - 5 - 6\\ &\equiv 4 + 3 - 5 - 0\\ &\equiv 2 \pmod{6}\end{aligned}$$

Using modulo 6 residues made the arithmetic simpler. The remainder is 2. □

Problem 12.10: The remainders when two natural numbers are divided by 16 are 11 and 14 respectively.

(a) Find the remainder when their sum is divided by 16.

(b) Find the remainder when their sum is divided by 8.

Solution for Problem 12.10: Let's begin by naming the integers in this problem. Let a and b be natural numbers such that

$$\begin{aligned} a &\equiv 11 \pmod{16} \\ b &\equiv 14 \pmod{16} \end{aligned}$$

(a) Adding the above congruences, we get

$$a + b \equiv 11 + 14 \equiv 25 \equiv 9 \pmod{16}.$$

The remainder when $a + b$ is divided by 16 is 9.

(b) Since 8 is a divisor of 16, we rewrite a and b in a way that helps us determine their modulo 8 residues:

$$\begin{aligned} a &= 16k_1 + 11 &= 2k_1(8) + 8 + 3 &= (2k_1 + 1)8 + 3 \\ b &= 16k_2 + 14 &= 2k_2(8) + 8 + 6 &= (2k_2 + 1)8 + 6 \end{aligned}$$

for some integers k_1 and k_2. Thus $a \equiv 3 \pmod 8$ and $b \equiv 6 \pmod 8$. Adding these congruences, we get

$$a + b \equiv 3 + 6 \equiv 9 \equiv 1 \pmod 8.$$

The remainder when $a + b$ is divided by 8 is 1.

□

Concept: Modular arithmetic helps us solve problems about unknown integers by giving us a way to work with their incomplete descriptions.

Problem 12.11: Eric's teacher asked him to find the remainder when the sum of the following 201-term arithmetic series is divided by 5:

$$2 + 7 + 12 + \cdots + 1002.$$

At first, Eric began to apply his knowledge of algebra to sum the series. Then Eric realized that each of the terms in the arithmetic progression is congruent to 2 (mod 5). This allowed him to find the answer more quickly. How did he do it?

Solution for Problem 12.11: Eric noticed that the sum of the arithmetic progression is congruent in modulo 5 to the sum of the modulo 5 residues of the terms:

$$\begin{aligned} 2 + 7 + 12 + \cdots + 1002 &\equiv 2 + 2 + 2 + \cdots + 2 \\ &\equiv 201(2) \\ &= 402 \\ &\equiv 2 \pmod 5 \end{aligned}$$

So Eric knew, without knowing the value of the gigantic sum, that its remainder when divided by 5 is 2. □

Exercises

12.4.1 State whether each of the following is true or false.

(a) $73 + 89 \equiv 3 + 9 \pmod{10}$

(b) $93 - 47 \equiv 3 - 2 \pmod{9}$

(c) $403 + 397 \equiv 3 + 7 \pmod{8}$

(d) $1214 + 1591 \equiv 3 + 2 \pmod{7}$

(e) $134 + 453 - 217 \equiv 2 + 3 - 1 \pmod{12}$

(f) $2372 + 971 - 1549 \equiv 7 + 3 - 9 \pmod{11}$

12.4.2 Determine the modulo 4 residue of the following sum:

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 + 11 + 12.$$

12.4.3 Sally, Wei-Hwa, and Zoe are playing a game of marbles involving first arranging as many piles of 10 marbles as possible. Sally brought 239 marbles, Wei-Hwa brought 174 marbles, and Zoe brought 83 marbles. If all their marbles are grouped together, how many must be removed in order to start the game?

12.4.4 Let a, b, and c be natural numbers whose remainders when divided by 13 are 4, 7, and 9. Find the remainder when their sum is divided by 13.

12.4.5 A roll of quarters contains 40 quarters and a roll of dimes contains 50 dimes. James has a jar that contains 83 quarters and 159 dimes. Lindsay has a jar that contains 129 quarters and 266 dimes. James and Lindsay pool these quarters and dimes and make complete rolls with as many of the coins as possible. How much are the leftover quarters and dimes worth?

12.5 Multiplication and Exponentiation

Problems

Problem 12.12: Let a_1, a_2 be integers such that $a_1 \equiv a_2 \pmod{6}$ and let b be an integer.

(a) Show that $2a_1 \equiv 2a_2 \pmod{6}$.

(b) Show that $a_1b - a_2b$ is a multiple of 6.

(c) Show that $a_1b \equiv a_2b \pmod{6}$.

Problem 12.13: Let a_1, a_2, b_1, and b_2 be integers such that

$$\begin{aligned} a_1 &\equiv a_2 \pmod{m} \\ b_1 &\equiv b_2 \pmod{m} \end{aligned}$$

(a) Show that $a_1b_1 \equiv a_2b_1 \pmod{m}$.

(b) Show that $a_2b_1 \equiv a_2b_2 \pmod{m}$.

(c) Show that $a_1b_1 \equiv a_2b_2 \pmod{m}$.

Problem 12.14: The remainders when two natural numbers are divided by 12 are 5 and 9.

(a) Find the remainder when their product is divided by 12.

(b) Find the remainder when their product is divided by 4.

Problem 12.15:

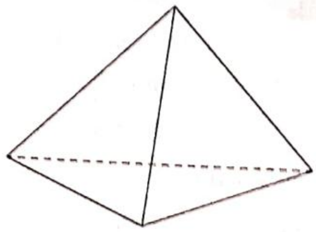


Figure 12.2: 6 toothpicks constructing a tetrahedron.

Jenny buys 15 boxes each containing 625 toothpicks. She arranges 6 toothpicks at a time into tetrahedra until there are not enough toothpicks to make any more full tetrahedra. How many toothpicks does Jenny have left?

Problem 12.16: In Section 12.4, we related the tale of Eric whose teacher asked him to find the remainder when the sum of the 201-term arithmetic series,

$$2 + 7 + 12 + \cdots + 1002$$

is divided by 5. Eric cleverly used the modulo 5 residues of each term to find the remainder without computing the sum. Later that day, Eric realized that he could also solve the problem quickly by applying modular arithmetic on a formula for the sum of an arithmetic progression:

$$a_1 + a_2 + \cdots + a_n = \frac{n(a_1 + a_n)}{2}.$$

How did Eric do it?

Problem 12.17: Let $a_1 \equiv a_2 \pmod{m}$ and n be a natural number.

(a) Show that $a_1^2 \equiv a_2^2 \pmod{m}$.

(b) Show that $a_1^n \equiv a_2^n \pmod{m}$.

Problem 12.18: Note that $12 \equiv 1 \pmod{11}$ and $21 \equiv -1 \pmod{11}$.

(a) Find the remainder when 12^{100} is divided by 11.

(b) Find the remainder when 21^{100} is divided by 11.

(c) Is $21^{100} - 12^{100}$ a multiple of 11?

Extra! *I have never let my schooling interfere with my education.* – Mark Twain

Problem 12.12: Let a_1, a_2 be integers such that $a_1 \equiv a_2 \pmod{6}$ and let b be an integer. Show that

$$a_1 b \equiv a_2 b \pmod{6}.$$

Solution for Problem 12.12: Let's start with an example. Let $b = 2$. Since $a_1 \equiv a_2 \pmod{6}$, the difference $a_1 - a_2$ is a multiple of 6. In other words,

$$a_1 - a_2 = 6k$$

for some integer k. Multiplying this equation by 2, we get

$$2a_1 - 2a_2 = 12k,$$

which is also a multiple of 6, so $2a_1 \equiv 2a_2 \pmod{6}$.

Similarly, we multiply $a_1 - a_2 = 6k$ by any integer b to get

$$a_1 b - a_2 b = 6bk,$$

which is a multiple of 6. Thus $a_1 b \equiv a_2 b \pmod{6}$. □

Problem 12.13: Let a_1, a_2, b_1, and b_2 be integers such that

$$\begin{aligned} a_1 &\equiv a_2 \pmod{m} \\ b_1 &\equiv b_2 \pmod{m} \end{aligned}$$

Show that $a_1 b_1 \equiv a_2 b_2 \pmod{m}$.

Solution for Problem 12.13: We explore a couple of solutions to this problem.

Solution 1: First, note that

$$\begin{aligned} a_1 - a_2 &= k_1 m \\ b_1 - b_2 &= k_2 m \end{aligned}$$

for some integers k_1 and k_2. Now, note each of the following:

$$\begin{aligned} a_1 b_1 - a_2 b_1 &= b_1(a_1 - a_2)m &= b_1 k_1 m \\ a_2 b_1 - a_2 b_2 &= a_2(b_1 - b_2)m &= a_2 k_2 m \end{aligned}$$

Adding the far left and far right parts of these equation chains, we get

$$a_1 b_1 - a_2 b_1 + a_2 b_1 - a_2 b_2 = b_1 k_1 m + a_2 k_2 m.$$

Simplifying the left-hand side and factoring m out of the right-hand side, we get

$$a_1 b_1 - a_2 b_2 = (b_1 k_1 + a_2 k_2)m.$$

Since $a_1 b_1 - a_2 b_2$ is a multiple of m, $a_1 b_1 \equiv a_2 b_2 \pmod{m}$.

Solution 2: Since the differences $a_1 - a_2$ and $b_1 - b_2$ are multiples of m, we have

$$\begin{aligned} a_1 &= a_2 + t_1 m \\ b_1 &= b_2 + t_2 m \end{aligned}$$

for some integers t_1 and t_2. Now, we expand the product a_1b_1:

$$\begin{aligned} a_1b_1 &= (a_2+t_1m)(b_2+t_2m) \\ &= a_2b_2 + a_2t_2m + b_2t_1m + t_1t_2m \\ &= a_2b_2 + (a_2t_2 + b_2t_1 + t_2t_2)m \end{aligned}$$

Now, we note that $a_1b_1 - a_2b_2$ is a multiple of m:

$$\begin{aligned} a_1b_1 - a_2b_2 &= a_2b_2 + (a_2t_2 + b_2t_1 + t_2t_2)m - a_2b_2 \\ &= (a_2t_2 + b_2t_1 + t_2t_2)m \end{aligned}$$

Thus $a_1b_1 \equiv a_2b_2 \pmod{m}$. □

Important: Let a_1, a_2, b_1, and b_2 satisfy

$$\begin{aligned} a_1 &\equiv a_2 \pmod{m} \\ b_1 &\equiv b_2 \pmod{m} \end{aligned}$$

Multiplication of these integers holds as follows:

$$a_1b_1 \equiv a_2b_2 \pmod{m}.$$

Problem 12.14: The remainders when two natural numbers are divided by 12 are 5 and 9.

(a) Find the remainder when their product is divided by 12.

(b) Find the remainder when their product is divided by 4.

Solution for Problem 12.14: Let the integers be a and b where

$$\begin{aligned} a &\equiv 5 \pmod{12} \\ b &\equiv 9 \pmod{12} \end{aligned}$$

(a) Multiplying the above congruences, we get

$$ab \equiv 5 \cdot 9 \equiv 45 \equiv 9 \pmod{12}.$$

The remainder when ab is divided by 12 is 9.

(b) We don't yet know anything about a and b modulo 4, so we start with what we do know:

$$\begin{aligned} a &= 12n_1 + 5 \\ b &= 12n_2 + 9 \end{aligned}$$

for some integers n_1 and n_2. Now we find the remainder when each of a and b is divided by 4:

$$\begin{aligned} a &= 4(3n_1 + 1) + 1 \\ b &= 4(3n_2 + 2) + 1 \end{aligned}$$

This means that $a \equiv b \equiv 1 \pmod{4}$, so $ab \equiv 1 \cdot 1 \equiv 1 \pmod{4}$ and the remainder is 1.

□

Problem 12.15: Jenny buys 15 boxes each containing 625 toothpicks. She arranges 6 toothpicks at a time into tetrahedra until there are not enough toothpicks to make any more full tetrahedra. How many toothpicks does Jenny have left?

Solution for Problem 12.15: We could multiply 15 times 625 and find the remainder when that product is divided by 6. However, it saves time to find the product of the modulo 6 residues of 15 and 625:

$$\begin{aligned} 15 &\equiv 3 \pmod 6 \\ 625 &\equiv 1 \pmod 6 \end{aligned}$$

$$15 \cdot 625 \equiv 3 \cdot 1 \equiv \mathbf{3} \pmod 6,$$

so there are **3** leftover toothpicks. □

Problem 12.16: In Section 12.4, we related the tale of Eric whose teacher asked him to find the remainder when the sum of the 201-term arithmetic series,

$$2 + 7 + 12 + \cdots + 1002$$

is divided by 5. Eric cleverly used the modulo 5 residues of each term to find the remainder without computing the sum. Later that day, Eric realized that he could also solve the problem quickly by applying modular arithmetic on a formula for the sum of an arithmetic progression:

$$a_1 + a_2 + \cdots + a_n = \frac{n(a_1 + a_n)}{2}.$$

How did Eric do it?

Solution for Problem 12.16: First, Eric noted the average of the first and last terms in the arithmetic series:

$$\frac{a_1 + a_{201}}{2} = \frac{2 + 1002}{2} = 502.$$

Eric then found the modulo 5 residues of this average as well as the number of terms:

$$\begin{aligned} 502 &\equiv 2 \pmod 5 \\ 201 &\equiv 1 \pmod 5 \end{aligned}$$

Then Eric quickly found the modulo 5 residue of the series sum using the formula:

$$\begin{aligned} 2 + 7 + 12 + \cdots + 1002 &= 201\left(\frac{2 + 1002}{2}\right) \\ &= 201 \cdot 502 \\ &\equiv 1 \cdot 2 \\ &\equiv 2 \pmod 5) \end{aligned}$$

Once again Eric found that the remainder is 2. □

Concept: Modular arithmetic becomes a powerful tool when combined with an understanding of algebra.

Problem 12.17: Let $a_1 \equiv a_2 \pmod{m}$ and n be a natural number. Show that $a_1^n \equiv a_2^n \pmod{m}$.

Solution for Problem 12.17: We begin with a simple example:

$$a_1 \cdot a_1 \equiv a_2 \cdot a_2 \pmod{m} \;\Rightarrow\; a_1^2 \equiv a_2^2 \pmod{m}.$$

We can continually multiply in factors of a_1 and a_2 to congruent powers of a_1 and a_2 to show that the next highest powers of a_1 and a_2 are also congruent:

$$\begin{aligned}
a_1 \cdot a_1^2 \equiv a_2 \cdot a_2^2 \pmod{m} \quad &\Rightarrow \quad a_1^3 \equiv a_2^3 \pmod{m}\\
a_1 \cdot a_1^3 \equiv a_2 \cdot a_2^3 \pmod{m} \quad &\Rightarrow \quad a_1^4 \equiv a_2^4 \pmod{m}\\
a_1 \cdot a_1^4 \equiv a_2 \cdot a_2^4 \pmod{m} \quad &\Rightarrow \quad a_1^5 \equiv a_2^5 \pmod{m}\\
&\;\;\vdots\\
a_1 \cdot a_1^{n-1} \equiv a_2 \cdot a_2^{n-1} \pmod{m} \quad &\Rightarrow \quad a_1^n \equiv a_2^n \pmod{m}
\end{aligned}$$

From this process we see that for any natural number n, $a_1^n \equiv a_2^n \pmod{m}$. □

Concept: In the solution to Problem 12.17, we used a process called **induction** to build on a simple result to establish a more general result. The idea is that each step along the way is essentially the same. Each new congruence is a direct result of the previous congruence and the process continues endlessly.

Important: For any natural number n and integers a_1 and a_2, where $a_1 \equiv a_2 \pmod{m}$,

$$a_1^n \equiv a_2^n \pmod{m}.$$

Problem 12.18: Is $21^{100} - 12^{100}$ a multiple of 11?

Solution for Problem 12.18: We certainly don't want to multiply out these huge exponentials, so we attempt to apply modular arithmetic. First, we note the residues of 12 and 21:

$$\begin{aligned}
21 &\equiv 10 \pmod{11}\\
12 &\equiv 1 \pmod{11}
\end{aligned}$$

With these residues, we simplify the problem ... a bit. We want to find the modulo 11 residue of

$$21^{100} - 12^{100} \equiv 10^{100} - 1^{100} \equiv 10^{100} - 1 \pmod{11}.$$

This result is not as simple as we would like it to be, so we hunt for a nicer way to work with 21^{100} in modulo 11. Noting that $21 \equiv -1 \pmod{11}$, we establish a much nicer result:

$$21^{100} - 12^{100} \equiv (-1)^{100} - 1^{100} = 1 - 1 \equiv 0 \pmod{11}.$$

Now we see that indeed $21^{100} - 12^{100}$ is a multiple of 11. □

Concept: In modular arithmetic, we usually work with residues because they typically make the arithmetic easiest. However, negative integers are easier to work with in some cases. It's always good to keep an open mind to the possibility of simpler solutions.

Exercises

12.5.1 Find the modulo 4 residues of each of the following.

(a) $17 \cdot 18$
(b) $523 \cdot 421$
(c) 15^{15}
(d) $121 \cdot 122 \cdot 123$
(e) $100!$
(f) $1 \cdot 3 \cdot 5 \cdot 7 \cdot 9$

12.5.2 Find the remainder when $514 \cdot 891$ is divided by 11.

12.5.3 The remainders when three positive integers are divided by 5 are 1, 2, and 3. Find the remainder when their product is divided by 5.

12.5.4 Find the remainder when $317 \cdot 5^{51}$ is divided by 6.

12.5.5 John has 73 bags each of which contains a quarter, a dime, a nickel, and a penny. He takes these bags to the bank and exchanges all the money for some number of dollar bills, dimes, and pennies. If the number of pennies John gets after exchanging the money with the bank is less than 10, how many pennies does he have?

12.5.6 Find the remainder when $24^{50} - 15^{50}$ is divided by 13.

12.6 Patterns and Exploration

Problems

Problem 12.19:
(a) Find the remainder when 5^2 is divided by 7.
(b) Find the remainder when 5^3 is divided by 7.
(c) Find the remainder when 5^4 is divided by 7.
(d) Find the remainder when 5^5 is divided by 7.
(e) Find the remainder when 5^6 is divided by 7.
(f) Find the remainder when 5^7 is divided by 7.
(g) Find the remainder when 5^8 is divided by 7.
(h) Find the remainder when 5^{2005} is divided by 7.

Problem 12.20:
(a) Find the remainder when 4^{18} is divided by 9.
(b) Find the remainder when 19^{80} is divided by 9.
(c) Find the remainder when $4^{18} \cdot 19^{80}$ is divided by 9.

Problem 12.21: The square of a positive integer leaves a remainder of 1 when divided by 5. What are the possible remainders when the integer itself is divided by 5?

Problem 12.22:
(a) Let n be a positive integer. Find the modulo 4 residue of n given that

$$7^n \equiv 1 \pmod{10}.$$

(b) Find the units digit of 7^{7^7}.

Extra! While many great mathematicians were fostered in their studies, Parisian **Marie-Sophie Germain** (1776–1831) faced unfortunate bias while making important contributions to number theory. As a teenager, Germain read works of Archimedes and taught herself Latin and Greek in order to read the words of other great mathematicians. Resisting her studies as the domain of young men, her parents took away her candles so she could not read at night. Still, Germain studied in the dark or by stolen candles. Eventually her parents submitted and, as they were a moderately wealthy family, supported her pursuits financially.

Germain corresponded closely with the great mathematicians of her time including **Adrien-Marie Legendre** and Carl Gauss, sometimes hiding her true identity for fear of being rejected by great teachers because she was a woman. She signed letters to mathematicians using the pseudonym "M. LeBlanc" until her reputation was well-established. Germain won the friendship of Gauss by contacting a friend of her family's, a French commander who saw to Gauss's safety during the French occupation of his hometown, Brunswick, in 1806. Gauss never retracted his praise of Germain's work, even though she revealed to him that she was a woman. Years later, Gauss convinced his university employers to grant Germain an honorary doctorate.

Germain's works include a proof relating to Fermat's Last Theorem which is regarded as the most productive approach to the theorem for several decades after. She also helped develop much of the mathematics behind the field of solid mechanics, a branch of physics that was only beginning to develop in the early nineteenth century.

A class of primes are named in honor of Germain. A **Sophie Germain prime** p is a prime such that $2p + 1$ is also prime. Sophie Germain primes are still investigated by number theorists.

Problem 12.19: Find the remainder when 5^{2005} is divided by 7.

Solution for Problem 12.19: We begin by finding the modulo 7 residues of some smaller powers of 5.

$$\begin{aligned}
5^0 &\equiv 1 \pmod 7\\
5^1 &\equiv 5 \pmod 7\\
5^2 &\equiv 4 \pmod 7\\
5^3 &\equiv 6 \pmod 7\\
5^4 &\equiv 2 \pmod 7\\
5^5 &\equiv 3 \pmod 7\\
5^6 &\equiv 1 \pmod 7\\
5^7 &\equiv 5 \pmod 7\\
5^8 &\equiv 4 \pmod 7\\
&\vdots
\end{aligned}$$

There are only 6 nonzero modulo 7 residues. Eventually, one of them repeats. The product of 5 times any specific modulo 7 residue never changes. So, when one residue repeats, all subsequent residues repeat as well, forming a pattern.

Solution 1: Our pattern above includes all 6 nonzero modulo 7 residues, so we must determine where 5^{2005} lies along this repeating chain of remainders. We do this by noting that $2005 \equiv 1 \pmod 6$. This tells us that 2005 is 1 more than a multiple of 6. Thus,

$$5^{2005} \equiv 5^1 \equiv \mathbf{5} \pmod 7,$$

so 5 is the remainder.

Solution 2: Since $5^6 \equiv 1 \pmod 7$, we break 5^{2005} into as many powers of 5^6 as possible:

$$5^{2005} = 5^1 \cdot 5^{2004} = 5^1 \cdot (5^6)^{334} \equiv 5 \cdot 1^{334} \equiv 5 \cdot 1 \equiv \mathbf{5} \pmod 7.$$

The remainder is 5. □

Concept: When faced with a problem that requires a difficult or impossible calculation, hunting for patterns often helps. This is especially true in modular arithmetic problems. The limited number of residues within a modulus sometimes make it easy to spot useful patterns.

Problem 12.20: Find the remainder when $4^{18} \cdot 19^{80}$ is divided by 9.

Solution for Problem 12.20: We note that

$$4^{18} \equiv (4^3)^6 \equiv 64^6 \equiv 1^6 \equiv 1 \pmod 9$$

and

$$19^{80} \equiv 1^{80} \equiv 1 \pmod 9.$$

Multiplying these together, we get $4^{18} \cdot 19^{80} \equiv 1 \cdot 1 \equiv 1 \pmod 9$. So, 1 is the remainder. □

Problem 12.21: The square of a positive integer leaves a remainder of 1 when divided by 5. What are the possible remainders when the integer itself is divided by 5?

Solution for Problem 12.21: There are only 5 residues in modulo 5, so we square each one:

$$\begin{aligned} 0^2 &\equiv 0 \pmod 5 \\ 1^2 &\equiv 1 \pmod 5 \\ 2^2 &\equiv 4 \pmod 5 \\ 3^2 &\equiv 4 \pmod 5 \\ 4^2 &\equiv 1 \pmod 5 \end{aligned}$$

The square of a positive integer leaves a remainder of 1 when divided by 5 when the positive integer itself leaves a remainder of either 1 or 4 when divided by 5. □

Problem 12.22: Find the units digit of 7^{7^7}.

Solution for Problem 12.22: We begin by establishing a relationship between the exponents and units digits of powers of 7. For a nonnegative integer n,

$$\begin{array}{lcl} n \equiv 0 \pmod 4 & \Rightarrow & 7^n \equiv 1 \pmod{10} \\ n \equiv 1 \pmod 4 & \Rightarrow & 7^n \equiv 7 \pmod{10} \\ n \equiv 2 \pmod 4 & \Rightarrow & 7^n \equiv 9 \pmod{10} \\ n \equiv 3 \pmod 4 & \Rightarrow & 7^n \equiv 3 \pmod{10} \end{array}$$

If we can determine the modulo 4 residue of the exponent 7^7 in 7^{7^7}, then we can determine the units digit of 7^{7^7}. Now we note that

$$7^7 \equiv (-1)^7 \equiv -1 \equiv 3 \pmod 4.$$

This tells us that

$$7^{7^7} \equiv 7^3 \equiv 3 \pmod{10},$$

so 7^{7^7} has a units digit of 3. □

Exercises

12.6.1 Find the remainder when each of the following is divided by 5.

(a) 2^8
(b) 3^{19}
(c) 4^{55}
(d) 7^{17}
(e) 19^{77}
(f) $14^{92} \cdot 17^{76}$

12.6.2

(a) Find all possible modulo 4 residues of a perfect square.

(b) Show that there are no solutions in integers to the equation $a^2 + b^2 = 10511$.

12.6.3 Find the units digit of 9^{8^7}.

12.6.4 Find the tens and units digit of 7^{2006}.

12.6.5 Find the remainder when

$$1^2 + 2^2 + 3^2 + \cdots + 99^2$$

is divided by 9.

12.6.6 Prove that if $a \equiv b \pmod{m_1}$ and $m_2 \mid m_1$, then $a \equiv b \pmod{m_2}$.

12.7 Summary

Modular arithmetic is an extraordinarily useful tool for solving mathematical problems. This chapter serves as a primer for performing the most fundamentally important modular arithmetic calculations.

Definitions:

- A **modulus** is a system for counting using only the fixed set of integers $0, 1, 2, \ldots, m-1$. When working in this modulus of m integers, we say that we are working with the integers **modulo** m.
- We say that two integers a and b are **congruent** or **equivalent** modulo m when their difference is a multiple of m. We write this as

  $$a \equiv b \pmod{m}.$$

  Otherwise, a and b are **incongruent** in modulo m and write this as

  $$a \not\equiv b \pmod{m}.$$

- We say that r is the modulo m **residue** of n when $n \equiv r \pmod{m}$ and $0 \le r < m$.
- The integers congruent to r modulo m make up a **residue class**. Residue classes are also known as **congruence classes** or **equivalence classes**.

Concept: Congruence works in modular arithmetic much the same way that equality works with regular integers (or any numbers in the regular system of real numbers). However, instead of meaning that two integers are the same, congruence means that the integers occupy the same column in a counting grid in which the number of columns is the modulus of the system.

Extra! *Don't be too timid and squeamish about your actions. All life is an experiment. The more experiments you make the better.* – Ralph Waldo Emerson

Important: Let a_1, a_2, b_1, and b_2 be integers such that

$$\begin{aligned} a_1 &\equiv a_2 \pmod{m} \\ b_1 &\equiv b_2 \pmod{m} \end{aligned}$$

Each of the following must also be true:

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{m} \end{aligned}$$

Also, for any positive integer n,

$$a_1^n \equiv a_2^n \pmod{m}.$$

Concept: Part of what makes modular arithmetic useful is that we can usually simplify calculations by working with the residues of integers. However, be aware of exceptions. It's often easiest to work with -1 or other integers with convenient properties relating to a particular problem.

Concept: When faced with a problem that requires a difficult or impossible calculation, hunting for patterns often helps. This is especially true in modular arithmetic problems. The limited number of residues within a modulus sometimes make it easy to spot useful patterns.

REVIEW PROBLEMS

12.23 Find the modulo 6 residues of each of the following.

(a) 13
(b) 53
(c) 84
(d) 184
(e) $63 + 91$
(f) $141 - 78$
(g) $519 - 444 + 37$
(h) $12 - 11 + 10 - 9 + 8 - 7$
(i) $43 \cdot 32$
(j) $59 \cdot 159$
(k) 14^6
(l) 101^{99}

12.24 Which of the following statements of congruence are true and which are false?

(a) $177 \equiv 17 \pmod{8}$

(b) $871 \equiv 713 \pmod{29}$

(c) $1322 \equiv 5294 \pmod{12}$

(d) $5141 \equiv 8353 \pmod{11}$

(e) $13944 \equiv 8919 \pmod{13}$

(f) $67 \cdot 73 \equiv 1 \cdot 3 \pmod{5}$

(g) $17 \cdot 18 \cdot 19 \cdot 20 \equiv 4! \pmod{8}$

(h) $83^{144} \equiv 15^{144} \pmod{17}$

12.25 How many integers between 1000 and 3000 inclusive are congruent to 5 (mod 7)?

12.26 For how many values of n, where $40 \le n \le 80$ is $n \equiv -n \pmod{12}$?

12.27 Four jars of jelly beans are individually repackaged into packs of 12 jelly beans. After the maximum number of packs are filled from each of these jars, the numbers of remaining jelly beans in the jars are 3, 5, 7, and 11. If the four jars had been combined before repackaging and the maximum number of packs were filled, how many jelly beans would have been left out of the 12 packs?

12.28 Two positive integers leave remainders of 6 and 13 when divided by 14.

(a) Find the remainder when their sum is divided by 14.

(b) Find the remainder when their difference is divided by 14.

(c) Find the remainder when their product is divided by 14.

(d) Find the remainder when their product is divided by 7.

12.29 Prove that if $a \equiv 19 \pmod{30}$, then $3a \equiv 7 \pmod{10}$.

12.30 Find the remainder when 7^{255} is divided by 11.

12.31 Find the remainder when $9^{42} - 5^{42}$ is divided by 7.

12.32 John tells Susie that he's thinking of an integer that leaves a remainder of 2 when divided by 6. Susie correctly informs John that the number is not a perfect square. How does she know?

Challenge Problems

12.33

(a) Find the last two digits of 99^{2005}. **Hints:** 139

(b) Find the last two digits of 7^{603}. **Hints:** 95

12.34 Find the modulo 200 residue of the sum

$$1 + 2 + 3 + 4 + \cdots + 199 + 200.$$

Hints: 158

12.35 Find the smallest natural number n such that

$$617n \equiv 943n \pmod{18}.$$

Hints: 92

12.36 Find the remainder when

$$17 + 177 + 1777 + 17777 + \cdots + 177777777777777777777$$

is divided by 8. Note that the last summand is 21 digits long (one 1 and twenty 7's). **Hints:** 133

12.37 Suppose a and b are positive integers, neither of which is a multiple of 3. Find all possible remainders when $a^2 + b^2$ is divided by 3. *(Source: UNCC)* **Hints:** 2

12.38 Ryun and Zhenya play a game with a pile of 82 toothpicks. The players take turns removing 1, 2, 3, or 4 toothpicks from the pile on each turn. The player that removes the last toothpick loses. Zhenya goes first. Help her formulate a winning strategy. **Hints:** 37, 71

12.39 A natural number, n, has a units digit of A when expressed in base 12. Find the remainder when n^2 is divided by 6. **Hints:** 124

12.40 For each integer $N > 1$, there is a mathematical system in which two or more integers are defined to be congruent if they leave the same non-negative remainder when divided by N. If 69, 90, and 125 are congruent in one such system, then what is the residue of 81 in that system? *(Source: AMC)* **Hints:** 77

12.41 A certain natural number is congruent to 4 (mod 9), congruent to 1 (mod 5), and congruent to 5 (mod 8).

(a) Show that the number is congruent to 1 (mod 3). **Hints:** 130

(b) Show that the number is congruent to 1 (mod 4). **Hints:** 76

(c) Show that the number is congruent to 1 (mod 60). **Hints:** 166

12.42 Find the remainder when

$$10^{10} + 10^{100} + 10^{1000} + \cdots + 10^{10000000000}$$

is divided by 7. *(Source: Mathematical Circles)* **Hints:** 121

12.43 A group of 25 Chicago Cubs fans got together for a party to discuss how *this is the year*. At the end of the party, many of the Cubs fans shake hands with one another. Let n be the number of the Cubs fans who shook hands with an odd number of other Cubs fans.

(a) Prove that n is even. **Hints:** 117

(b) Prove that n would still be even had there been 100 Cubs fans at the party.

12.44 What is the size of the largest subset, S, of $\{1, 2, 3, \ldots, 50\}$ such that no pair of distinct elements of S has a sum divisible by 7? *(Source: AMC)* **Hints:** 81, 50

12.45 The Fibonacci sequence is defined by $F_1 = F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$. Find the remainder when F_{2006} is divided by 5. **Hints:** 147

12.46 Find all prime numbers p for which $p^2 - 1$ is not a multiple of 24. **Hints:** 105

12.47 Prove that among any 51 integers, there are two whose squares have the same remainder when divided by 100. **Hints:** 151

12.48 Denote by p_k the k^{th} prime number. Show that, for any positive integer n, the number $p_1p_2p_3\cdots p_n+1$ cannot be the perfect square of an integer. *(Source: M&IQ 1992)* **Hints:** 88, 155

Extra! *In theory there is no difference between theory and practice. In practice there is.* – Yogi Berra

Extra! **Prime-Generating Polynomials**

Prolific Swiss mathematician **Leonhard Euler** (1707-1783) noticed that the polynomial $f(n) = n^2 + n + 41$ generates values that are prime for $n = 0, 1, 2, \ldots, 39$. However,

$$f(40) = 40^2 + 40 + 41 = 40(40 + 1) + 41 = 40(41) + 41 = 41^2$$

is composite. Still, this interesting polynomial sparked a vast amount of interest in polynomials with integer coefficients that generate only prime numbers for the smallest several nonnegative integer inputs.

Mathematician **Adrien-Marie Legendre** (1752-1833) proved that there are no polynomials with rational coefficients that give primes for every integer input. However, mathematicians and math enthusiasts have found many polynomials that generate only primes for the smallest several nonnegative integer inputs. Here are a few of them:

Polynomial	Prime from 0 to n for $n =$
$n^2 + n + 17$	15
$n^2 - n + 41$	40
$n^2 - 79n + 1601$	80
$2n^2 + 11$	10
$2n^2 + 29$	28
$4n^2 + 4n + 59$	13
$6n^2 - 342n + 4903$	57
$7n^2 - 371n + 4871$	23
$8n^2 - 488n + 7243$	61
$36n^2 - 810n + 2753$	44
$43n^2 - 537n + 2971$	34
$103n^2 - 4707n + 50383$	42
$n^3 + n^2 + 17$	10
$3n^3 - 183n^2 + 3318n - 18757$	46
$n^4 + 29n^2 + 101$	19

The essence of mathematics is not to make simple things complicated, but to make complicated things simple.
– S. Gudder

CHAPTER 13 Divisibility Rules

13.1 Introduction

In this chapter we explore **divisibility rules**—rules that help us determine when any given integer is divisible by particular natural numbers. We use modular arithmetic to derive a number of these rules. Some will be harder to discover than others and along the way they will challenge us to put modular arithmetic into practice as a problem solving tool. As we will see, modular arithmetic reveals useful features of integers beyond what simple rules tell us.

Focus on the methods we use to determine different rules. Understanding how to build these rules means understanding how to explore and establish a wide variety of relationships between integers.

13.2 Divisibility Rules

Throughout this section, assume that all integers are expressed as decimal numerals (base 10) unless otherwise stated.

Problems

Problem 13.1: Demonstrate each of the following:

(a) $632 \equiv 2 \pmod{2}$

(b) $632 \equiv 2 \pmod{5}$

(c) $632 \equiv 2 \pmod{10}$

(d) A natural number is always congruent to its units digit modulo 2, 5, or 10.

Problem 13.2: Demonstrate each of the following:

(a) $593 \equiv 93 \pmod{100}$

(b) $727 \equiv 27 \pmod{100}$

(c) Any natural number is congruent in modulo 100 to the integer formed by its last two digits.

(d) $52141 \equiv 141 \pmod{10^m}$, where $m = 3$.

(e) $91238328 \equiv 38328 \pmod{10^m}$, where $m = 5$.

(f) For any positive integer m, a natural number is congruent in modulo 10^m to the integer formed by its last m digits.

Problem 13.3: Let m be any positive integer. Demonstrate each of the following.

(a) A natural number is congruent in modulo 2^m to the integer formed by its last m digits.

(b) A natural number is congruent in modulo 5^m to the integer formed by its last m digits.

Problem 13.4: Demonstrate each of the following:

(a) $40 \equiv 4 \pmod 3$

(b) $700 \equiv 7 \pmod 3$

(c) $2000 \equiv 2 \pmod 3$

(d) $d \cdot 10^n \equiv d \pmod 3$ for natural numbers d and n.

(e) $2740 \equiv 2 + 7 + 4 \pmod 3$

(f) A natural number is congruent modulo 3 to the sum of its digits.

Problem 13.5: Demonstrate each of the following:

(a) $40 \equiv 4 \pmod 9$

(b) $700 \equiv 7 \pmod 9$

(c) $2000 \equiv 2 \pmod 9$

(d) $d \cdot 10^n \equiv d \pmod 9$ for natural numbers d and n.

(e) $2740 \equiv 2 + 7 + 4 \pmod 9$

(f) A natural number is congruent modulo 9 to the sum of its digits.

Problem 13.6: Demonstrate each of the following:

(a) $40 \equiv -4 \pmod{11}$

(b) $700 \equiv 7 \pmod{11}$

(c) $2000 \equiv -2 \pmod{11}$

(d) $d \cdot 10^n \equiv d(-1)^n \pmod{11}$ for natural numbers d and n.

(e) $2740 \equiv -2 + 7 - 4 \pmod{11}$

(f) Find a rule that relates the digits of a natural number to its modulo 11 residue.

Problem 13.7: For each of the following integers, determine whether or not they are a multiple of each of 2, 3, 4, 5, 8, 9, 10, 11, 12, and 25.

(a) 540 (c) 1554

(b) 814 (d) 138780

Problem 13.1: Demonstrate that any natural number is congruent to its units digit in each of modulo 2, modulo 5, and modulo 10.

Solution for Problem 13.1: We begin with an example:

$$\frac{632-2}{10} = \frac{630}{10} = 63,$$

which is an integer. This tells us that $632 \equiv 2 \pmod{10}$. Since $632 - 2$ is divisible by 10, we know that it is also divisible by every divisor of 10, including 2 and 5:

$$632 \equiv 2 \pmod{2} \qquad \text{and} \qquad 632 \equiv 2 \pmod{5}.$$

Now we consider whether or not we can make more general statements mathematically. We can express a natural number n in terms of a sum of decimal digit bundles,

$$n = d_k \cdot 10^k + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0,$$

where d_0 is the units digit. Now, we note that $n - d_0$ is a multiple of 10 since all the remaining nonzero digit bundles (if there are any) are multiples of 10:

$$\frac{n-d_0}{10} = \frac{d_k \cdot 10^k + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10^1}{10} = d_k \cdot 10^{k-1} + \cdots + d_2 \cdot 10^1 + d_1 \cdot 10^0,$$

which is an integer. Thus $n \equiv d_0 \pmod{10}$. In turn, that implies that a natural number and its units digit are also congruent modulo 2 and 5. □

In Problem 13.1 we showed that a natural number is equivalent to its units digit in modulo 2, 5, and 10. Not only can we now find the residue of a natural number in modulo 2, 5, and 10 more quickly, but we can now also identify several divisibility rules. Since a natural number is a multiple of 2 if and only if its units digit is congruent to 0 modulo 2, we know that an integer is even if and only if its units digit is even. Similarly, we have divisibility rules for 5 and 10:

Important:

- A natural number is a multiple of 2 if and only if its units digit is even.
- A natural number is a multiple of 5 if and only if its units digit is 0 or 5.
- A natural number is a multiple of 10 if and only if its units digit is 0.

Problem 13.2: Let m be any positive integer. Prove that every natural number is congruent in modulo 10^m to the integer formed by its last m digits.

Solution for Problem 13.2: We first take a look at a few examples:

$$\begin{aligned}
\frac{593-93}{10^2} &= \frac{500}{10^2} = 5 &\Rightarrow\ & 593 \equiv 93 \pmod{10^2} \\
\frac{727-27}{10^2} &= \frac{700}{10^2} = 7 &\Rightarrow\ & 727 \equiv 27 \pmod{10^2} \\
\frac{52141-141}{10^3} &= \frac{52000}{10^3} = 52 &\Rightarrow\ & 52141 \equiv 141 \pmod{10^3} \\
\frac{91238328-38328}{10^5} &= \frac{91200000}{10^5} = 912 &\Rightarrow\ & 91238328 \equiv 38328 \pmod{10^5}
\end{aligned}$$

When we subtract the integer formed by the last m digits of any natural number from the natural number itself, the result is an integer with at least m terminating 0's. An integer with at least m terminating 0's is a multiple of 10^m. So, the difference between any natural number and the integer formed by its last m digits is a multiple of 10^m. Therefore, every natural number is congruent in modulo 10^m to the integer formed by its last m digits. □

Problem 13.3: Let m be any positive integer. Demonstrate each of the following:

(a) A natural number is congruent in modulo 2^m to the integer formed by its last m digits.

(b) A natural number is congruent in modulo 5^m to the integer formed by its last m digits.

Solution for Problem 13.3: In Problem 13.1, we used the fact that the equivalence of two integers in modulo 10 implies that the two integers are also equivalent in modulos 2 and 5 because 2 and 5 are divisors of 10. We apply this fact to both parts of this problem.

(a) In Problem 13.2, we showed that any natural number is equivalent in modulo 10^m to the integer formed by its last m digits. This means that any natural number is equivalent to the integer formed by its last m digits in any modulus that is a divisor of 10^m. Since 2^m is a divisor of 10^m, we know that every natural number is congruent in modulo 2^m to the integer formed by its last m digits.

(b) This part is almost exactly the same as part (a). Since 5^m is also a divisor of 10^m, we know also that every natural number is congruent in modulo 5^m to the integer formed by its last m digits.

□

Extra! *In my mind's eye, I visualize how a particular ... sight and feeling will appear on a print. If it excites me, there is a good chance it will make a good photograph. It is an intuitive sense, an ability that comes from a lot of practice.* – Ansel Adams

In Problems 13.2 and 13.3 we used the fact that an integer is divisible by m powers of 10 if and only if its last m digits are 0 to derive several useful statements about the residues of integers based on their last m digits. We now restate this divisibility rule along with two more that are special cases of what we have proved:

Important: Let m be a positive integer.

- A natural number is a multiple of 2^m if and only if the integer formed by its last m digits is a multiple of 2^m.
- A natural number is a multiple of 5^m if and only if the integer formed by its last m digits is a multiple of 5^m.
- A natural number is a multiple of 10^m if and only if its last m digits are all 0.

Problem 13.4: Show that a natural number is congruent to the sum of its digits modulo 3.

Solution for Problem 13.4: Our goal is to relate integers to their digits, so we focus on the place value of each digit:

$$2740 = 2 \cdot 10^3 + 7 \cdot 10^2 + 4 \cdot 10^1 + 0 \cdot 10^0.$$

Once we find the modulo 3 values of each power of 10, we use modular arithmetic to multiply and add all the modulo 3 values together. We note that

$$10 \equiv 1 \pmod 3.$$

Taking both sides of this congruence to the power of a whole number n yields

$$10^n \equiv 1^n \equiv 1 \pmod 3.$$

This is very convenient for us as it's easy to multiply by 1:

$$\begin{array}{rcllcl} 2 \cdot 10^3 & \equiv & 2 \cdot 1^3 & \equiv 2 \cdot 1 & \equiv & 2 \pmod 3 \\ 7 \cdot 10^2 & \equiv & 7 \cdot 1^2 & \equiv 7 \cdot 1 & \equiv & 7 \pmod 3 \\ 4 \cdot 10^1 & \equiv & 4 \cdot 1^1 & \equiv 4 \cdot 1 & \equiv & 4 \pmod 3 \\ 0 \cdot 10^0 & \equiv & 0 \cdot 1^0 & \equiv 0 \cdot 1 & \equiv & 0 \pmod 3 \end{array}$$

Adding these congruences and simplifying the sum, we get

$$2740 = 2 \cdot 10^3 + 7 \cdot 10^2 + 4 \cdot 10^1 + 0 \cdot 10^0 \equiv 2 \cdot 1 + 7 \cdot 1 + 4 \cdot 1 + 0 \cdot 1 \equiv 2 + 7 + 4 + 0 \equiv 1 \pmod 3.$$

Similarly, we compare any natural number to its digits modulo 3:

$$\begin{aligned} n &= d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_1 \cdot 10^1 + d_0 \cdot 10^0 \\ &\equiv d_k \cdot 1^k + d_{k-1} \cdot 1^{k-1} + \cdots + d_1 \cdot 1^1 + d_0 \cdot 1^0 \\ &\equiv d_k \cdot 1 + d_{k-1} \cdot 1 + \cdots + d_1 \cdot 1 + d_0 \cdot 1 \\ &\equiv d_k + d_{k-1} + \cdots + d_1 + d_0 \pmod 3 \end{aligned}$$

Thus, every natural number is equivalent to the sum of its digits modulo 3. The most common application of this fact is that the sum of the digits of an integer is a multiple of 3 if and only if the integer is itself a multiple of 3. Make sure you see why! □

> **Important:** An integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

Problem 13.5: Show that a natural number is congruent to the sum of its digits modulo 9.

Solution for Problem 13.5: We use the same method we used in Problem 13.4. Since $10^n \equiv 1^n \equiv 1 \pmod 9$ for any whole number n, we have

$$\begin{aligned}
2\cdot 10^3 &\equiv 2\cdot 1^3 \equiv 2\cdot 1 \equiv 2 \pmod 9\\
7\cdot 10^2 &\equiv 7\cdot 1^2 \equiv 7\cdot 1 \equiv 7 \pmod 9\\
4\cdot 10^1 &\equiv 4\cdot 1^1 \equiv 4\cdot 1 \equiv 4 \pmod 9\\
0\cdot 10^0 &\equiv 0\cdot 1^0 \equiv 0\cdot 1 \equiv 0 \pmod 9
\end{aligned}$$

Adding these congruences, we get

$$2740 = 2\cdot 10^3 + 7\cdot 10^2 + 4\cdot 10^1 + 0\cdot 10^0 \equiv 2\cdot 1 + 7\cdot 1 + 4\cdot 1 + 0\cdot 1 \equiv 2+7+4+0 \equiv 4 \pmod 9.$$

More generally,

$$\begin{aligned}
n &= d_k\cdot 10^k + d_{k-1}\cdot 10^{k-1} + \cdots + d_1\cdot 10^1 + d_0\cdot 10^0\\
&\equiv d_k\cdot 1^k + d_{k-1}\cdot 1^{k-1} + \cdots + d_1\cdot 1^1 + d_0\cdot 1^0\\
&\equiv d_k\cdot 1 + d_{k-1}\cdot 1 + \cdots + d_1\cdot 1 + d_0\cdot 1\\
&\equiv d_k + d_{k-1} + \cdots + d_1 + d_0 \pmod 9
\end{aligned}$$

Thus, every natural number is equivalent to the sum of its digits modulo 9. The most common application of this fact is that the sum of the digits of an integer is a multiple of 9 if and only if the integer is itself a multiple of 9. □

The divisibility rule for 3 works the same as the divisibility rule for 9 because 3 is a divisor of 9. Since $10 = 9 + 1$ is the base of our decimal system, every power of 10 is congruent to 1 modulo 9. Make sure you see why this allows us to compare an integer to the sum of its digits.

> **Important:** An integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

Problem 13.6: Find a rule that relates the digits of a natural number to its modulo 11 residue.

Solution for Problem 13.6: This problem is very similar to Problems 13.4 and 13.5 in that powers of 10 can be easily determined in modulo 11. We note that

$$10 \equiv -1 \pmod{11}.$$

Now, for any whole number n,

$$10^n \equiv (-1)^n \pmod{11}.$$

This is very convenient for us as multiplication by -1 is simple:

$$\begin{aligned}
2\cdot 10^3 &\equiv 2\cdot(-1)^3 &\equiv 2\cdot(-1) &\equiv -2 \pmod{11}\\
7\cdot 10^2 &\equiv 7\cdot(-1)^2 &\equiv 7\cdot 1 &\equiv 7 \pmod{11}\\
4\cdot 10^1 &\equiv 4\cdot(-1)^1 &\equiv 4\cdot(-1) &\equiv -4 \pmod{11}\\
0\cdot 10^0 &\equiv 0\cdot(-1)^0 &\equiv 0\cdot 1 &\equiv 0 \pmod{11}
\end{aligned}$$

Adding these congruences, we get

$$2740 = 2\cdot 10^3 + 7\cdot 10^2 + 4\cdot 10^1 + 0\cdot 10^0 \equiv 2\cdot(-1) + 7\cdot 1 + 4\cdot(-1) + 0\cdot 1 \equiv -2+7-4+0 \equiv 1 \pmod{11}.$$

More generally,

$$\begin{aligned}
n &= d_k\cdot 10^k + d_{k-1}\cdot 10^{k-1} + \cdots + d_1\cdot 10^1 + d_0\cdot 10^0\\
&\equiv d_k\cdot(-1)^k + d_{k-1}\cdot(-1)^{k-1} + \cdots + d_1\cdot(-1)^1 + d_0\cdot(-1)^0\\
&\equiv d_k\cdot(-1)^k + d_{k-1}\cdot(-1)^{k-1} + \cdots - d_1 + d_0 \pmod{11}
\end{aligned}$$

Thus, every natural number is equivalent to the "alternating sum" of its digits modulo 11 (adding the units digit, subtracting the tens digit, etc.). The most common application of this fact is that the alternating sum of the digits of an integer is a multiple of 11 if and only if the integer is itself a multiple of 11. □

Important: An integer is a multiple of 11 if and only if the alternating sum of its digits is a multiple of 11.

There are divisibility rules for other integers, but most of them are not as easy to discover, remember, or apply. We can even derive divisibility rules for base numbers. See if you can discover some of them on your own using the methods we used in this section. Some of these problems are left as Challenge Problems at the end of this chapter.

Now that we have developed a number of divisibility rules, let's take a look at how much easier they make finding divisors of some integers.

Problem 13.7: For each of the following integers, determine whether or not they are a multiple of each of 2, 3, 4, 5, 8, 9, 10, 11, 12, and 25.

(a) 540
(b) 814
(c) 1554
(d) 138780

Solution for Problem 13.7: Before we tackle the problem parts, we note that since $\gcd(3,4) = 1$ and $\text{lcm}[3,4] = 12$, an integer is a multiple of 12 if and only if it is a multiple both of 3 and of 4.

(a)
- The units digit of 540 is 0, telling us that 540 is a multiple of **2**, of **5**, and of **10**.
- The sum of the digits of 540 is $5+4+0 = 9$, which is a multiple of 9, so 540 is a multiple both of **3** and of **9**.

- The last two digits of 540 are 40, which is a multiple of 4, so 540 is a multiple of **4**, but 40 is not a multiple of 25, so 540 is not a multiple of 25.
- Since 540 is a three-digit number, the divisibility test for 8 is just the same as dividing 540 by 8. We already know that 540 is a multiple of 4, so we use that as a starting point. Since $540/4 = 135$, we see that 540 has only 2 powers of 2 in its prime factorization and is therefore not a multiple of 8.
- Since 540 is a multiple of both 3 and 4, it is also a multiple of **12**.
- The alternating digit sum of 540 is $0 - 4 + 5 = 1$, which is not a multiple of 11, so 540 is not a multiple of 11.

(b)
- The units digit of 814 is 4, so 814 is a multiple of **2**, but not a multiple of 5 or 10. Since 814 is not a multiple of 5, it is not a multiple of any multiple of 5, including 25.
- The sum of the digits of 814 is $8 + 1 + 4 = 13$, which is a multiple of neither 3 nor of 9, so 814 is a multiple of neither 3 nor of 9.
- The last two digits of 814 are 14, which is not a multiple of 4, so 814 is not a multiple of 4 or any other multiple 4. Thus, it is not a multiple of 8.
- Since 814 is a multiple of neither 3 nor 4, it is not a multiple of 12.
- The alternating digit sum of 814 is $4 - 1 + 8 = 11$, which is a multiple of 11, so 814 is a multiple of **11**.

(c)
- The last digit of 1554 is 4, so 1554 is a multiple of **2**, but not of 5 or of 10. Since 1554 is not a multiple of 5, it is not a multiple of 25.
- The sum of the digits of 1554 is $1 + 5 + 5 + 4 = 15$, which is a multiple of 3, but not of 9. So, 1554 is a multiple of **3**, but not of 9.
- The last two digits of 1554 are 54, which is not a multiple of 4, so 1554 is neither a multiple of 4 nor of 8.
- Since 1554 is not a multiple of 4, it is not a multiple of 12.
- The alternating digit sum of 1554 is $4 - 5 + 5 - 1 = 3$, which is not a multiple of 11, so 1554 is not a multiple of 11.

(d)
- The last digit of 138780 is 0, so 138780 is a multiple of **2**, of **5**, and of **10**.
- The sum of the digits of 138780 is $1+3+8+7+8+0 = 27$, which is a multiple of both 3 and 9, so 138780 is a multiple both of **3** and of **9**.
- The last two digits of 138780 are 80, which is a multiple of 4, but not of 25, so 138780 is a multiple of **4**, but not of 25.
- The last three digits of 138780 are 780, which is not a multiple of 8, so 138780 is not a multiple of 8.
- Since 138780 is a multiple both of 3 and of 4, it is also a multiple of **12**.
- The alternating digit sum of 138780 is $0 - 8 + 7 - 8 + 3 - 1 = -7$, which is not a multiple of 11, so 138780 is not a multiple of 11.

□

Exercises

13.2.1 Use divisibility rules to help find prime factorizations of each of the following integers.

(a) 525
(b) 1408
(c) 22572
(d) 82200
(e) 179010
(f) 10485760

13.2.2 Find the remainder when each of the following is divided by 8.

(a) 9319
(b) 12411
(c) 65989
(d) 91827
(e) 204201
(f) 204001^{34}

13.2.3 Find the remainder when each of the following is divided by 9.

(a) 9319
(b) 12411
(c) 65989
(d) 91827
(e) 204201
(f) 204001^{34}

13.2.4 What is the least number greater than 9000 that is divisible by 11? *(Source: MATHCOUNTS)*

13.3★ Divisibility Rules With Algebra

We often use the digits of an integer to help determine some of its divisors. However, we sometimes face problems in which we know some of the divisors of an integer, but not all of its digits. In this section we discuss how to apply divisibility rules to these kinds of problems.

Problems

All integers in the following problems are written in decimal form.

Problem 13.8: A is the tens digit of the integer $3A6$. For what value(s) of A is $3A6$ a multiple of 9?

Problem 13.9: Suppose A and B represent digits of $25A9B$, which is a multiple of 36.

(a) Apply the divisibility rule for 4 to $25A9B$ to determine possible values of B.
(b) Apply the divisibility rule for 9 to $25A9B$ to determine possible values of the ordered pairs (A, B).
(c) Find all possible values of $25A9B$.

Problem 13.10: Find the ordered pair(s) of digits (A, B) that make $67A7B$ a multiple of 225.

Extra! *You can only get good at chess if you love the game.* – Bobby Fischer

Problem 13.8: For which digit(s) A is $3A6$ a multiple of 9?

Solution for Problem 13.8: In order for $3A6$ to be a multiple of 9, the sum of its digits must be a multiple of 9. We summarize this fact in a statement of congruence:

$$3 + A + 6 \equiv 0 \pmod 9.$$

This means that $A + 9 \equiv A \equiv 0 \pmod 9$. Since A is a digit from 0 to 9 inclusive, either $A = 0$ or $A = 9$. □

Concept: When number theory problems involve variables, we can examine the information in the problem using the same techniques we apply to simpler problems. Then we apply algebraic concepts to solve those problems.

Problem 13.9: Find all possible ordered pairs (A, B) of digits that make $25A9B$ a multiple of 36.

Solution for Problem 13.9: We are working with an integer that is a multiple of 36 and has two variable digits. Divisibility rules help us determine which integers have certain divisors, so we look for divisibility rules that will help us in this case. Since $36 = 2^2 \cdot 3^2$, we can apply the divisibility rules for 4 and 9.

According to the divisibility rule for 4, the two-digit integer $9B$ must be a multiple of 4, thus

$$90 + B \equiv 0 \pmod 4.$$

This means that $B + 90 \equiv B + 2 \equiv B - 2 \equiv 0 \pmod 4$, so

$$B \equiv 2 \pmod 4.$$

Since B must be a decimal digit, we know that either $B = 2$ or $B = 6$.

According to the divisibility rule for 9,

$$2 + 5 + A + 9 + B \equiv 0 \pmod 9.$$

This tells us that $A + B + 16 \equiv A + B + 7 \equiv A + B - 2 \equiv 0 \pmod 9$, so

$$A + B \equiv 2 \pmod 9.$$

Since $\gcd(4, 9) = 1$ and $\operatorname{lcm}[4, 9] = 36$, an integer is a multiple of 36 if and only if it is a multiple both of 4 and of 9 (make sure you see why). This means (A, B) must satisfy both congruences we found. We perform casework from the first congruence to get our solutions:

- When $B = 2$, we have
$$A + 2 \equiv 2 \pmod 9,$$
from which we determine that $A \equiv 0 \pmod 9$ and we have ordered pairs of digits $(0, 2)$ and $(9, 2)$.
- When $B = 6$, we have
$$A + 6 \equiv 2 \pmod 9,$$
from which we determine that $A \equiv 5 \pmod 9$ and we have ordered pair of digits $(5, 6)$.

These are all the ordered pairs (A, B) that we seek and the possible values of $25A9B$ are 25092, 25992, and 25596. □

> **Concept:** While there might be no simple rule for how to solve a particular problem, we can often use several rules together to complete the task.

Understanding divisibility of integers helped us break Problem 13.9 into two problems. After solving both problems together, we had our solution to the whole problem.

Problem 13.10: Find the ordered pair(s) of digits (A, B) that make $67A7B$ a multiple of 225.

Solution for Problem 13.10: There is no one simple divisibility rule for multiples of 225, so we consider what rules we might use. We note that $225 = 3^2 \cdot 5^2$. An integer is a multiple of 225 if and only if it is a multiple of both $3^2 = 9$ and $5^2 = 25$.

The divisibility rule for 25 tells us that $67A7B$ is a multiple of 25 when $7B$ is a multiple of 25:

$$70 + B \equiv 0 \pmod{25}.$$

We find that $B = 5$ is the only possibility.

We now apply the divisibility rule for 9 to $67A75$:

$$6 + 7 + A + 7 + 5 = A + 25 \equiv 0 \pmod{9}.$$

Solving for A we find that $A \equiv 2 \pmod{9}$, so $A = 2$.

The only possible ordered pair is $(2, 5)$ and the multiple of 225 is 67275. □

Exercises

13.3.1 For which digit(s) N is $8N5$ a multiple of 25?

13.3.2 For how many ordered pairs of digits (A, B) is the integer $5AB3$ a multiple of 9?

13.3.3 For how many ordered pairs of digits (A, B) is the integer $5AB4$ a multiple of 9?

13.3.4 If the five digit number $5DDDD$ is divisible by 6, then find the digit D. *(Source: Mandelbrot)*

13.3.5

(a) For which ordered pairs of digits (A, B) is $4AB8$ a multiple of 4?

(b) For which ordered pairs of digits (A, B) is $4AB8$ a multiple of 3?

(c) For which ordered pairs of digits (A, B) is $4AB8$ a multiple of 12?

13.3.6 Find the value of the digit D if $47D4$ leaves a remainder of 2 when divided by 33.

13.3.7 Find the ordered pair of digits (M, N) that make $52MN5$ a multiple of 1125.

13.4 Summary

Important: We used modular arithmetic to demonstrate relationships between the values of integers and their digits.

- Let m be a positive integer. Every natural number is congruent to its last m digits modulo 2^m, modulo 5^m, and modulo 10^m.
- Every natural number is congruent to the sum of its digits modulo 3 and modulo 9.
- Every natural number is congruent to the alternating sum of its digits modulo 11.

Through the mechanics of modular arithmetic we have now derived numerous useful divisibility rules:

Important: Here is a list of the most commonly used divisibility rules. When used, m represents any natural number.

- An integer is a multiple of 2 if and only if its units digit is even.
- An integer is a multiple of 2^m if and only if its last m digits themselves form an integer that is a multiple of 2^m.
- An integer is a multiple of 5 if and only if its units digit is 0 or 5.
- An integer is a multiple of 5^m if and only if its last m digits themselves form an integer that is a multiple of 5^m.
- An integer is a multiple of 10 if and only if its units digit is 0.
- An integer is a multiple of 10^m if and only if its last m digits are all 0.
- An integer is a multiple of 3 if and only if the sum of its digits is a multiple of 3.
- An integer is a multiple of 9 if and only if the sum of its digits is a multiple of 9.
- An integer is a multiple of 11 if and only if the alternating sum of its digits is a multiple of 11.

We could in fact derive a divisibility rule for any natural number. However, most such rules are overly complicated so as to provide no real computational or problem solving advantages.

While these divisibility rules are nice, don't forget how we derived them! Through modular arithmetic, we derived more powerful rules that help us find residues more quickly for each modulus for which we have a divisibility rule.

Once we established and practiced applying divisibility rules, we applied them to problems in which we needed to find the digits of integers that fit certain descriptions.

Concept: When number theory problems involve variables, we can examine the information in the problem using the same techniques we apply to simpler problems. Then we apply algebraic concepts to solve those problems.

Concept: While there might be no simple rule for how to solve a particular problem, we can often use several rules together to complete the task.

REVIEW PROBLEMS

13.11 Determine which of the following are multiples of 9.

(a) 8712
(b) 12994
(c) 52515
(d) 8192547

13.12 Determine which of the following are multiples of 11.

(a) 748
(b) 8557
(c) 39149
(d) 2492172

13.13 Determine which of the following are multiples of 8.

(a) 1444
(b) 83412
(c) 971352
(d) 2222222220

13.14 If A and B represent digits of the base ten number $60A5B$, which is a multiple of 72, what are A and B? **Hints:** 112

13.15 If A and B represent digits of the base ten number $50A11B$, which is a multiple of 45, what are the possible values of $50A11B$? **Hints:** 44

Extra! *To explain the lure of speed you would have to explain human nature; but it is easier understood than explained. All men in all ages have beggared themselves for fast horses or camels or ships or cars or bikes or aeroplanes: all men have strained themselves dry to run or walk or swim faster. Speed is the second oldest animal craving in our nature, and our generation is fortunate in being able to indulge it more cheaply and generally than our ancestors. Every natural man cultivates the speed that appeals to him. I have a motor-bike income.*

– T.E. Lawrence (Lawrence of Arabia)

Challenge Problems

13.16 A nine-digit number uses the digits 1-9 once each. What is the probability that the number is prime? *(Source: MATHCOUNTS)* **Hints:** 119

13.17 A four-digit number uses each of the digits 1, 2, 3 and 4 exactly once. What is the probability that the number is a multiple of 4? *(Source: MATHCOUNTS)* **Hints:** 63

13.18 How many four-digit palindromes are multiples of 9? **Hints:** 36

13.19★ Find a divisibility rule for 99. Show that it always works. **Hints:** 46, 137

13.20 To test a number for divisibility by 7, remove the final digit, then subtract twice this digit from whatever remains. The new number is divisible by 7 if and only if the original one is. For example, 7 divides 434 since it divides $43 - 2(4) = 35$. If instead we subtract three times the final digit from what remains, we obtain a divisibility test for a different prime. What is it? *(Source: Mandelbrot)* **Hints:** 84

13.21 How many three-digit natural numbers have digits that sum to 13 and leave a remainder of 1 when divided by 4? **Hints:** 109

13.22 Find a six-digit number whose first three digits are 523 such that the integer is divisible by each of 7, 8, and 9. **Hints:** 11

13.23★ Show that for $n \geq 2$, the number of digits in the block of repeating digits in the decimal expansion of $\frac{1}{3^n}$ is 3^{n-2}. **Hints:** 75

13.24 Show that a natural number n is a multiple of $b-1$ if and only if the sum of its digits are a multiple of $b-1$ when n is expressed in base b. **Hints:** 15

13.25 For all integer values of $n \geq 2$, k will divide $n^3 - n$. What is the greatest possible integer value of k? *(Source: MATHCOUNTS)* **Hints:** 98, 26

13.26★ What is the smallest 5-digit palindrome that is a multiple of 99? *(Source: HMMT)* **Hints:** 49

13.27 Demonstrate that for natural numbers m and n that the modulo 3^m residue of n can be determined from its last m digits alone when expressed in base 12. **Hints:** 69

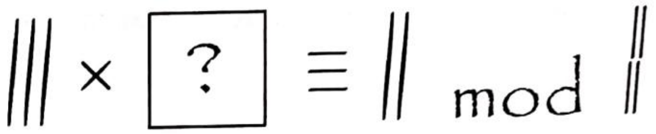
13.28 Prove that a power of 2 cannot end in four equal digits. *(Source: Mathematical Circles)* **Hints:** 161

13.29★ The integer n is the smallest positive multiple of 15 such that every digit of n is either 0 or 8. Compute $n/15$. *(Source: AIME)* **Hints:** 39

13.30★ Find the smallest natural number all of whose digits are 1 that is a multiple of:

(a) 3
(b) 33
(c) 333
(d) 3333333333

Hints: 29, 65, 6



It's not that I'm so smart, it's just that I stay with problems longer. – Albert Einstein

CHAPTER 14 Linear Congruences

14.1 Introduction

A **linear congruence equation** is a lot like an ordinary linear equation. Here is an example:

$$3x \equiv 2 \pmod{4}.$$

> **Definition:** A **linear congruence equation** is a congruence that involves a variable raised only to the first power.

For the rest of this chapter, we simply refer to **linear congruence equations** as **linear congruences.** In general, for integers a and b, a modulus m, and a single variable x, a linear congruence can be expressed in the form

$$ax \equiv b \pmod{m},$$

though expressing a linear congruence in this form sometimes requires simplification as we will see.

Here are a few examples of linear congruences with their solutions:

$$\begin{array}{lll} 3x \equiv 2 \pmod{4} & \text{is satisfied by} & x \equiv 2 \pmod{4} \\ 5y \equiv 7 \pmod{8} & \text{is satisfied by} & y \equiv 3 \pmod{8} \\ 6x \equiv 5 \pmod{11} & \text{is satisfied by} & x \equiv 10 \pmod{11} \end{array}$$

There are also linear congruences with no solutions, such as

$$2x \equiv 1 \pmod{4}.$$

This chapter explores both how to determine when linear congruences have solutions and how to find any solutions they have.

14.2 Modular Inverses and Simple Linear Congruences

Problems

Problem 14.1: Find all values of x that satisfy each of the following linear congruences.

(a) $x - 3 \equiv 0 \pmod 4$

(b) $x - 2 \equiv 0 \pmod 4$

(c) $x - 1 \equiv 0 \pmod 4$

(d) $x + 1 \equiv 0 \pmod 4$

(e) $x + 2 \equiv 0 \pmod 4$

(f) $x + 3 \equiv 0 \pmod 4$

Problem 14.2:

(a) Find the smallest positive multiple of 4 that is 1 more than a multiple of 5.

(b) Find all solutions to $4n \equiv 1 \pmod 5$.

Problem 14.3: For each of the following linear congruences, find all solutions or show that there are none.

(a)	$2x \equiv 1 \pmod{10}$	(e)	$6x \equiv 1 \pmod{10}$
(b)	$3x \equiv 1 \pmod{10}$	(f)	$7x \equiv 1 \pmod{10}$
(c)	$4x \equiv 1 \pmod{10}$	(g)	$8x \equiv 1 \pmod{10}$
(d)	$5x \equiv 1 \pmod{10}$	(h)	$9x \equiv 1 \pmod{10}$

Problem 14.4: In this problem we examine when an integer b cannot have a modulo m inverse.

(a) Show that $\gcd(b, m)$ is a divisor of $bx - tm$ for any integers x and t.

(b) Show that if there is some x such that $bx \equiv 1 \pmod m$, then $\gcd(b, m) \mid 1$.

(c) Conclude that b^{-1} does not exist in modulo m when $\gcd(b, m) > 1$.

Problem 14.5: Let r be a modulo 60 residue such that $\gcd(r, 60) = 1$.

(a) Show that if $rx \equiv ry \pmod{60}$ for integers x and y, then x and y are members of the same modulo 60 residue class.

(b) Show that when r is multiplied by each of the modulo 60 residues that no two of the products are congruent modulo 60.

(c) Show that r has *exactly one* modulo 60 inverse.

Problem 14.6: John bought n boxes of cookies containing 11 cookies each. On the way home from the store, John noticed that if he ate just one cookie, the total number of cookies remaining would be a multiple of 23. What is the smallest possible value of n?

Extra! *Nothing endures but change.* – Heraclitus

Problem 14.1: Solve each of the following linear congruences.

(a) $x - 3 \equiv 0 \pmod 4$		(d) $x + 1 \equiv 0 \pmod 4$
(b) $x - 2 \equiv 0 \pmod 4$		(e) $x + 2 \equiv 0 \pmod 4$
(c) $x - 1 \equiv 0 \pmod 4$		(f) $x + 3 \equiv 0 \pmod 4$

Solution for Problem 14.1: We could solve each linear congruence by plugging in all possible modulo 4 residues to find out which, if any of them, work. However, we know that we can add or subtract any integer to both sides of a congruence to produce another valid congruence. Adding 3 to both sides of the first congruence, we get

$$x \equiv 3 \pmod 4,$$

which describes all possible solutions for x: $\ldots, -5, -1, 3, 7, \ldots$.

We add to or subtract from each side of each congruence in order to isolate the variable:

$$\begin{aligned}
x - 2 &\equiv 0 \pmod 4 &&\Rightarrow& x &\equiv 2 \pmod 4\\
x - 1 &\equiv 0 \pmod 4 &&\Rightarrow& x &\equiv 1 \pmod 4\\
x + 1 &\equiv 0 \pmod 4 &&\Rightarrow& x &\equiv 3 \pmod 4\\
x + 2 &\equiv 0 \pmod 4 &&\Rightarrow& x &\equiv 2 \pmod 4\\
x + 3 &\equiv 0 \pmod 4 &&\Rightarrow& x &\equiv 1 \pmod 4
\end{aligned}$$

So, we have solutions to each of the simple linear congruences. □

Concept: In much the same way that we solve ordinary algebraic linear equations, we solve simple linear congruences by manipulating both sides of the congruence until the variable is isolated.

Unfortunately, not all of the same methods we use to solve algebraic equations are available in modular arithmetic. We need to develop other methods for solving more complicated linear congruences.

Problem 14.2: Find all solutions to $4n \equiv 1 \pmod 5$.

Solution for Problem 14.2:

Bogus Solution: First, we find a multiple of 4 that is congruent to 1 (mod 5):

$$4n \equiv 1 \equiv 6 \equiv 11 \equiv 16 \pmod 5.$$

Dividing both sides of $4n \equiv 16 \pmod 5$ by 4, we get $n \equiv 4 \pmod 5$.

Extra! *I have learned throughout my life as a composer chiefly through my mistakes and pursuits of false assumptions, not by my exposure to founts of wisdom and knowledge.* – Igor Stravinsky

While the answer in the bogus solution is correct, the method is not. Division is not a valid operation in modular arithmetic. However, matching 1 with a congruent multiple of 4 was a good start! We note that

$$4 \cdot 4 \equiv 1 \pmod{5}.$$

We can use this fact to solve our original linear congruence. Multiplying both sides of $4n \equiv 1 \pmod{5}$ by 4 we get

$$16n \equiv 4 \pmod{5}.$$

But $16 \equiv 1 \pmod{5}$, so the left-hand side is $16n \equiv 1n \equiv n \pmod{5}$. Finally, our congruence becomes $n \equiv 4 \pmod{5}$, which are the solutions to the congruence $4n \equiv 1 \pmod{5}$. □

WARNING!! Division is not defined in modular arithmetic!

Here's an example where division fails to find all the solutions to a linear congruence:

$$3x \equiv 3 \pmod{6}$$

Dividing both sides of this linear congruence by 3, we get $x \equiv 1 \pmod{6}$. While these solutions satisfy the original linear congruence, so do $x \equiv 3 \pmod{6}$ and $x \equiv 5 \pmod{6}$.

Without the operation of division available to us, we used multiplication to solve Problem 14.2. We multiplied 4 by a number we found (which happened also to be 4) to get 1 (mod 5). In other words, we multiplied 4 by its modulo 5 inverse in order to isolate the variable n.

Definition: A **modular inverse** of an integer b (modulo m) is an integer b^{-1} such that

$$b \cdot b^{-1} \equiv 1 \pmod{m}.$$

More simply, we refer to b^{-1} as an **inverse**.

For instance, using the modulo 5 multiplication table at right, we find inverses of some modulo 5 residues:

$$\begin{aligned} 1^{-1} &\equiv 1 \pmod{5} \\ 2^{-1} &\equiv 3 \pmod{5} \\ 3^{-1} &\equiv 2 \pmod{5} \\ 4^{-1} &\equiv 4 \pmod{5} \end{aligned}$$

	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

Note that 1 is its own inverse in any modulus because $1 \cdot 1 \equiv 1 \pmod{m}$. Also, $0 \cdot x \equiv 0 \pmod{m}$, so 0 never has an inverse in any modulus.

Extra! *The sorcery and charm of imagination, and the power it gives to the individual to transform his world into a new world of order and delight, makes it one of the most treasured of all human capacities.* – Frank Barron

Problem 14.3: Find the inverses of all modulo 10 residues that have inverses.

Solution for Problem 14.3: We write out an entire modulo 10 multiplication table to be sure we find all the inverses of modulo 10 residues (and thus all integers modulo 10):

	0	**1**	2	**3**	4	5	6	**7**	8	**9**
0	0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	**1**	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	**1**	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	**1**

From the modulo 10 multiplication table, we find that

$$\begin{aligned} 1^{-1} &\equiv 1 \pmod{10} \\ 3^{-1} &\equiv 7 \pmod{10} \\ 7^{-1} &\equiv 3 \pmod{10} \\ 9^{-1} &\equiv 9 \pmod{10} \end{aligned}$$

and that there is no modulo 10 inverse for 0, 2, 4, 5, 6, or 8.

□

Problem 14.4: Prove that b^{-1} does not exist in modulo m when $\gcd(b, m) > 1$.

Solution for Problem 14.4: When b^{-1} exists, it's the solution to the linear congruence

$$bx \equiv 1 \pmod{m}.$$

This means that for some value of x, that

$$bx - tm = 1,$$

for some integer t. Now, let $d = \gcd(b, m)$. Thus, $d \mid bx$ and $d \mid tm$. Since a divisor of two integers is a divisor of their difference,

$$d \mid (bx - tm).$$

But we know that $bx - tm = 1$, so $d \mid 1$. Hence $d = 1$. Thus, when b^{-1} exists, the GCD of b and m is 1. So, when $\gcd(b, m) > 1$, b^{-1} does not exist. □

Important: If $\gcd(b, m) > 1$, then b does not have a modulo m inverse.

In Problem 14.3, we found that each modulo 10 residue that is relatively prime with 10 has an inverse. In fact, every modulo 10 residue appears as a product in each row and column (of the modulo 10 multiplication table) started with a multiplicand that is relatively prime to 10.

Problem 14.5: Let r be a modulo 60 residue such that $\gcd(r, 60) = 1$. Show that r has a modulo 60 inverse.

Solution for Problem 14.5: Let x and y be integers such that $rx \equiv ry \pmod{60}$. Thus,

$$rx - ry = r(x - y) = 60t$$

for some integer t. This means that $60 \mid r(x-y)$. But, since $\gcd(r, 60) = 1$, we know that $60 \mid (x-y)$. Thus, $x \equiv y \pmod{60}$. This means that when $x \not\equiv y \pmod{60}$, that $rx \not\equiv ry \pmod{60}$. So, when we multiply r by each of the modulo 60 residues, none of the products are equivalent modulo 60. This means that each product is equivalent to a different modulo 60 residue, one of which is 1. Thus, *exactly one* of the modulo 60 residues is a modulo 60 inverse of r. □

Notice that in Problem 14.5, nothing in our solution depended specifically on the number 60. We can just as easily replace 60 with any modulus m and our solution shows that when r and m are relatively prime, r^{-1} exists. Combining this with the fact that residues not relatively prime with m don't have inverses, we summarize our work:

Important: A modulo m residue r has a single inverse if and only if $\gcd(m, r) = 1$. Otherwise, it has no inverse.

Note that when the modulus m is prime, every residue other than 0 is relatively prime to the modulus, thus every nonzero residue has a modulo m inverse.

Problem 14.6: John bought n boxes of cookies containing 11 cookies each. On the way home from the store, John noticed that if he ate just one cookie, the total number of cookies remaining would be a multiple of 23. What is the smallest possible value of n?

Solution for Problem 14.6: John bought $11n$ cookies where $11n \equiv 1 \pmod{23}$. Our goal is to find the smallest positive integer n that satisfies the congruence. Our answer will be the modulo 23 inverse of 11.

Solution 1: We add multiples of 23 to 1 until we reach an integer that is a multiple of 11:

$$1 \equiv 24 \equiv 47 \equiv 70 \equiv 93 \equiv 116 \equiv 139 \equiv 162 \equiv 185 \equiv 208 \equiv 231 \pmod{23}.$$

Since $11 \cdot 21 = 231 \equiv 1 \pmod{23}$, 21 is the modulo 23 inverse of 11.

Solution 2: While looking for an integer n such that $11n \equiv 1 \pmod{23}$, we find that

$$11 \cdot 2 \equiv -1 \pmod{23}.$$

Multiplying both sides of the congruence by -1 and organizing, we get

$$11 \cdot (-2) \equiv 1 \pmod{23}.$$

Since $-2 \equiv 21 \pmod{23}$, we have $11 \cdot 21 \equiv 1 \pmod{23}$. So 21 is the modulo 23 inverse of 11. □

Exercises

14.2.1 Find all solutions to each of the following linear congruences.

(a) $x - 5 \equiv 2 \pmod{3}$

(b) $x + 223 \equiv 114 \pmod{8}$

(c) $5x \equiv 1 \pmod{11}$

(d) $2x + 17 \equiv 0 \pmod{9}$

14.2.2 Find the modulo 11 inverses for the residues 1-10 inclusive.

14.2.3 Which modulo 15 residues have inverses?

14.2.4★ Prove that an integer cannot have more than one inverse in a given modulus.

14.3 Solving Linear Congruences

Problems

Problem 14.7:
(a) Find all solutions to $7a \equiv 1 \pmod{20}$.
(b) Find all solutions to $7b \equiv 2 \pmod{20}$.
(c) Find all solutions to $7c \equiv 3 \pmod{20}$.

Problem 14.8: Find all solutions to $48x - 115 \equiv 291 \pmod{13}$.

Problem 14.9: Find all solutions to $2x \equiv 3 \pmod{4}$.

Problem 14.10: Let k be a positive integer. Prove that if $ak \equiv bk \pmod{mk}$ for integers a and b, then $a \equiv b \pmod{m}$.

Problem 14.11: Find all solutions to $56x + 43 \equiv 211 \pmod{96}$.

Problem 14.12: Prove that a linear congruence $ax \equiv b \pmod{m}$ has solutions if and only if $\gcd(a, m) \mid b$.

Problem 14.13:
(a) Rewrite the following statement as a linear congruence:

The product of 5 and an integer is 3 more than a multiple of 7.

(b) Solve the linear congruence.

Problem 14.7:
(a) Find all solutions to $7a \equiv 1 \pmod{20}$.
(b) Find all solutions to $7b \equiv 2 \pmod{20}$.
(c) Find all solutions to $7c \equiv 3 \pmod{20}$.

Solution for Problem 14.7:

(a) Since 7 and 20 are relatively prime, 7 has a modulo 20 inverse. Now we hunt for a multiple of 7 that is congruent to 1 (mod 20):

$$7a \equiv 1 \equiv 21 \pmod{20}.$$

Multiplying both sides of $7a \equiv 21 \pmod{20}$ by 7^{-1}, we get

$$a \equiv 21 \cdot 7^{-1} \equiv 3 \cdot 7 \cdot 7^{-1} \equiv 3 \cdot 1 \equiv 3 \pmod{20}.$$

So, the solutions to $7a \equiv 1 \pmod{20}$ are $a \equiv 3 \pmod{20}$. This also shows that $7^{-1} \equiv 3 \pmod{20}$.

(b) In part (a) we showed that $7^{-1} \equiv 3 \pmod{20}$. Multiplying both sides of $7b \equiv 2 \pmod{20}$ by 7^{-1}, we get
$$b \equiv 2 \cdot 7^{-1} \equiv 2 \cdot 3 \equiv 6 \pmod{20}.$$
So, the solutions to $7b \equiv 2 \pmod{20}$ are $b \equiv 6 \pmod{20}$.

(c) Multiplying both sides of $7c \equiv 3 \pmod{20}$ by 7^{-1}, we get
$$c \equiv 3 \cdot 7^{-1} \equiv 3 \cdot 3 \equiv 9 \pmod{20}.$$
So, the solutions to $7c \equiv 3 \pmod{20}$ are $c \equiv 9 \pmod{20}$.

□

Important: When the coefficient of a variable in a congruence is relatively prime with the modulus, we can get rid of the coefficient by multiplying both sides of the congruence by the inverse. This helps us isolate the variable.

Problem 14.8: Find all solutions to $48x - 115 \equiv 291 \pmod{13}$.

Solution for Problem 14.8: We would like to isolate the variable, so we start by adding 115 to both sides of the congruence:
$$48x \equiv 406 \pmod{13}.$$
We simplify both sides by noting that $48 \equiv 9 \pmod{13}$ and $406 \equiv 3 \pmod{13}$:
$$9x \equiv 3 \pmod{13}.$$
Note that $9^{-1} \equiv 3 \pmod{13}$. Multiplying both sides by 9^{-1}, we get
$$x \equiv 3 \cdot 9^{-1} \equiv 3 \cdot 3 \equiv 9 \pmod{13},$$
so $x \equiv 9 \pmod{13}$ are the solutions to $48x - 115 \equiv 291 \pmod{13}$. □

Problem 14.9: Find all solutions to $2x \equiv 3 \pmod{4}$.

Solution for Problem 14.9: It would be nice if we could isolate the variable. However, 2 and 4 are not relatively prime. Thus, we cannot multiply both sides by the inverse of 2 because 2 has no modulo 4 inverse. We'll have to look for a different approach.

We go back to the basics. When $2x \equiv 3 \pmod{4}$, we know that
$$2x - 3 = 4n$$
for some integer n. Rearranging this equation, we get $2x - 4n = 3$. Factoring the left-hand side, we get
$$2(x - 2n) = 3.$$
The left-hand side of this new equation is a multiple of 2. However, the right-hand side is not. This is impossible, so there are no solutions. Thus, there are no solutions to the linear congruence. □

We showed that $2x \equiv 3 \pmod 4$ has no solutions by showing that the parametric equation we related to the congruence has no solutions. This is true because 2 and 4 share a common factor that 3 does not. In general, for the linear congruence $ax \equiv b \pmod m$, we have

$$ax - mn = b$$

for some integer n. Dividing both sides of the equation by $\gcd(a, m)$, we get

$$\frac{ax}{\gcd(a,m)} - \frac{mn}{\gcd(a,m)} = \frac{b}{\gcd(a,m)}.$$

Since the denominators in the left-hand side are divisors of the numerators, the left-hand side is an integer. The right-hand side is only an integer when $\gcd(a, m) \mid b$. Otherwise, the right-hand side is a fraction, in which case there are no solutions to the equation or to the linear congruence.

Important: A linear congruence $ax \equiv b \pmod m$ has no solutions when $\gcd(a, m) \nmid b$.

Problem 14.10: Let k be a positive integer. Prove that if $ak \equiv bk \pmod{mk}$ for integers a and b, then $a \equiv b \pmod m$.

Solution for Problem 14.10: When $ak \equiv bk \pmod{mk}$, we know that

$$ak - bk = mkn$$

for some integer n. Dividing this equation by k we get $a - b = mn$. Thus $a \equiv b \pmod m$. □

In Problem 14.10, we showed that when both sides of a congruence and the modulus share a common divisor, that we can "remove" the common divisor from all three parts.

Important: If $ak \equiv bk \pmod{mk}$ for integers a and b, a positive integer k, then

$$a \equiv b \pmod m.$$

Problem 14.11: Find all solutions to $56x + 43 \equiv 211 \pmod{96}$.

Solution for Problem 14.11: We begin by subtracting 43 from both sides of the congruence to get

$$56x \equiv 168 \pmod{96}.$$

We can also simplify the right-hand side by noting that $168 \equiv 72 \pmod{96}$:

$$56x \equiv 72 \pmod{96}.$$

Since 56, 72, and 96 share the common divisor 8, we divide it out of all three parts to get an equivalent, but simpler linear congruence:

$$7x \equiv 9 \pmod{12}.$$

Now we look for a multiple of 7 that is congruent to 9 (mod 12):

$$7x \equiv 9 \equiv 21 \pmod{12}.$$

Multiplying through by 7^{-1} yields

$$x \equiv 21 \cdot 7^{-1} \equiv 3 \cdot 7 \cdot 7^{-1} \equiv 3 \pmod{12}.$$

So, $x \equiv 3 \pmod{12}$ describes all solutions to $56x + 43 \equiv 211 \pmod{96}$. □

Problem 14.12: Prove that a linear congruence $ax \equiv b \pmod{m}$ has solutions if and only if $\gcd(a, m) \mid b$.

Solution for Problem 14.12: We already know that $ax \equiv b \pmod{m}$ has no solutions when $\gcd(a, m) \nmid b$. We only need to prove that when $\gcd(a, m) \mid b$, there are solutions.

Let $d = \gcd(a, m)$ and note that $d \mid b$. Let's rewrite a, b, and m in terms of d:

$$\begin{aligned} a &= a_1 d \\ b &= b_1 d \\ m &= m_1 d \end{aligned}$$

Note that since $\gcd(a, m) = d\gcd(a_1, m_1) = d$, we have $\gcd(a_1, m_1) = 1$. Now, we rewrite our linear congruence in a way that allows us to simplify it:

$$a_1 dx \equiv b_1 d \pmod{m_1 d} \Rightarrow a_1 x \equiv b_1 \pmod{m_1}.$$

Since a_1 is relatively prime to m_1, we know a_1 has an inverse. Multiplying both sides of our last congruence by a_1^{-1}, we get

$$x \equiv b_1 a_1^{-1} \pmod{m_1}.$$

These solutions satisfy $ax \equiv b \pmod{m}$, so our proof is complete. □

Important: A linear congruence $ax \equiv b \pmod{m}$ has solutions if and only if $\gcd(a, m) \mid b$.

Although we cannot use division in modular arithmetic, there are times when we perform simplifications on congruences that have the same effect as division, but with a catch: sometimes the modulus changes and sometimes it doesn't.

Since $\gcd(2, 3) = 1$, we solve the congruence $2x \equiv 2 \pmod{3}$ by multiplying both sides of the congruence by 2^{-1} to get $x \equiv 1 \pmod{3}$. The effect is the same as if we divided each side of the congruence by 2.

Now, consider the linear congruence $2x \equiv 2 \pmod{4}$. This means that $2x - 2 = 4a$ for some integer a. Dividing this equation by 2, we get $x - 1 = 2a$, so $x \equiv 1 \pmod{2}$ are the solutions to the original congruence. Going from the original congruence to the solution, we divided by sides of the congruence by 2, but we also divided the modulus by 2.

Lastly, we'll combine both methods above. Consider the linear congruence $12x \equiv 36 \pmod{44}$. We first divide 4 out of both sides and also the modulus to get $3x \equiv 9 \pmod{11}$. Next, we multiply both sides of the congruence by 3^{-1} to get $x \equiv 3 \pmod{11}$, which are the solutions to $12x \equiv 36 \pmod{44}$.

Now, let's take a look at the combined effect of these two types of "division." We divided both sides of the original congruence by $\gcd(12,36) = 12$. In the meantime, we divided the modulus by $\gcd(12,44) = 4$. In general, we can summarize the process as follows:

Let a, b, and c be integers such $ac \equiv bc \pmod{m}$. Then

$$a \equiv b \pmod{\frac{m}{\gcd(m,c)}}.$$

Understanding this fact helps us simplify many congruences.

Problem 14.13: Find all integers that, when multiplied by 5, are 3 more than a multiple of 7.

Solution for Problem 14.13: We seek integer values of n such that

$$5n \equiv 3 \pmod{7}.$$

We manipulate the congruence so that the right-hand side is a multiple of 5:

$$5n \equiv 10 \pmod{7}.$$

Multiplying both sides by 5^{-1} gives us the solutions we seek:

$$n \equiv 10 \cdot 5^{-1} \equiv 2 \cdot 5 \cdot 5^{-1} \equiv 2 \pmod{7},$$

so the solutions are integers n that satisfy $n \equiv 2 \pmod{7}$. □

Concept: Many remainder problems are just linear congruences.

We now summarize what we've learned about solving linear congruences. In order to do so, we use variables a little differently than we did throughout the past few problems, but you should recognize the concepts.

The General Process	**The Applied Process**
First, we can organize any linear congruence into the form $ax \equiv b \pmod{m}$, where x is the variable.	Given the linear congruence $9x + 4 \equiv 10 \pmod{12}$, we subtract 4 from both sides to get $9x \equiv 6 \pmod{12}$.
A linear congruence $ax \equiv b \pmod{m}$ has solutions if and only if $\gcd(a,m) \mid b$.	Note that $\gcd(9,12) = 3$, $3 \mid 6$, and $3 \nmid 4$. The linear congruence $9x \equiv 6 \pmod{12}$ has solutions while $9x \equiv 4 \pmod{12}$ does not.
If $\gcd(a,m) \mid b$, then we let $d = \gcd(a,m)$ and rewrite the linear congruence using $a = a_1d$, $b = b_1d$, and $m = m_1d$: $a_1dx \equiv b_1d \pmod{m_1d}$. This linear congruence has the same solutions as $a_1x \equiv b_1 \pmod{m_1}$.	Since $\gcd(9,12) = 3$, the linear congruence $9x \equiv 6 \pmod{12}$ has the same solutions as the linear congruence $\frac{9}{3}x \equiv \frac{6}{3} \pmod{\frac{12}{3}}$, which simplifies to $3x \equiv 2 \pmod{4}$.

Note that

$$\begin{aligned} d &= \gcd(a, m) \\ &= \gcd(a_1 d, m_1 d) \\ &= d \gcd(a_1, m_1) \end{aligned}$$

So, $\gcd(a_1, m_1) = 1$. This means that a_1^{-1} exists in modulo m_1. Now we multiply both sides of $a_1 x \equiv b_1 \pmod{m_1}$ by a_1^{-1} to get

$$x \equiv a_1^{-1} b_1 \pmod{m_1},$$

which are the solutions to $ax \equiv b \pmod{m}$.

Since $\gcd(3,4) = 1$, we know that 3 has a modulo 4 inverse. In fact,

$$3^{-1} \equiv 3 \pmod{4}.$$

Multiplying both sides of $3x \equiv 2 \pmod{4}$ by 3^{-1}, we get

$$\begin{aligned} x &\equiv 2 \cdot 3^{-1} \\ &\equiv 2 \cdot 3 \equiv 2 \pmod{4} \end{aligned}$$

So, $x \equiv 2 \pmod{4}$ describes all solutions to $9x \equiv 6 \pmod{12}$.

Exercises

14.3.1 Find all solutions to $3a \equiv 9 \pmod{11}$.

14.3.2 Find all solutions to $5x - 11 \equiv 7 \pmod{8}$.

14.3.3 Find all solutions to $4n \equiv 8 \pmod{10}$.

14.3.4 Find all solutions to $6a + 19 \equiv 7 \pmod{18}$.

14.4 Systems of Linear Congruences

Sometimes two or more linear congruences have solutions in common. We say that these solutions satisfy a **system of linear congruences**. Here is an example of a system of linear congruences that we explore in this section:

$$\begin{aligned} N &\equiv 1 \pmod{2} \\ N &\equiv 3 \pmod{5} \end{aligned}$$

Problems

Problem 14.14:

(a) If $2a + 1 = 5b + 3$ for some integers a and b, what is the value of b modulo 2?

(b) If $N = 2a + 1 = 5b + 3$, find the value of N modulo 10.

(c) Find all solutions to the system of linear congruences

$$\begin{aligned} N &\equiv 1 \pmod{2} \\ N &\equiv 3 \pmod{5} \end{aligned}$$

Problem 14.15: Find all solutions to the system of linear congruences

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 2 \pmod{4} \end{aligned}$$

Problem 14.16: Find all solutions to the system of linear congruences

$$\begin{aligned} a &\equiv 2 \pmod{6} \\ a &\equiv 3 \pmod{9} \end{aligned}$$

Problem 14.17: Find all solutions to the system of linear congruences

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 2 \pmod{4} \end{aligned}$$

that also satisfy

$$x \equiv 4 \pmod{5}$$

Problem 14.18:

(a) Find all positive integers that leave a remainder of 2 when divided by 5 and a remainder of 6 when divided by 7.

(b) How many three-digit positive integers leave a remainder of 2 when divided by 5 and a remainder of 6 when divided by 7?

Problem 14.19:

$$\begin{aligned} 4N &\equiv 3 \pmod{7} \\ 5N &\equiv 7 \pmod{8} \end{aligned}$$

(a) Solve each of the linear congruences above *individually*.

(b) Solve the *system* of linear congruences above.

Problem 14.14: Find all solutions to the system of linear congruences

$$\begin{aligned} N &\equiv 1 \pmod{2} \\ N &\equiv 3 \pmod{5} \end{aligned}$$

Solution for Problem 14.14: We begin by writing what we know about N in equation form:

$$\begin{aligned} N &= 2a + 1 \\ N &= 5b + 3 \end{aligned}$$

for integers a and b. Combining these equations, we get an equation relating a and b:

$$5b + 3 = 2a + 1.$$

In order to find more out about the possible values of a and b individually, we look for a way to isolate either variable. Looking at both sides of the equation in modulo 2 or modulo 5 isolates the variables for us. In order to work with smaller numbers, we choose here to examine the equation modulo 2. Simplifying both sides of the equation modulo 2, we get

$$b + 1 \equiv 1 \pmod{2} \Rightarrow b \equiv 0 \pmod{2}.$$

This means that $b = 2c$ for some integer c. Now we rewrite what we know about N in terms of c:

$$N = 5b + 3 = 5(2c) + 3 = 10c + 3.$$

This means that $N \equiv 3 \pmod{10}$.

We check the solutions to be sure they work:

$$\begin{array}{ccccccc} N & = & 10c + 3 & = & 2(5c+1)+1 & \equiv & 1 \pmod{2} \\ N & = & 10c + 3 & = & 5(2c)+3 & \equiv & 3 \pmod{5} \end{array}$$

So, the integers N such that $N \equiv 3 \pmod{10}$ are all the solutions. □

Concept: Looking at information in different mathematical forms gives us more ways to use it. When solving a system of linear congruences, we switch back and forth between using modular congruences and parametric equations.

Problem 14.15: Find all solutions to the system of linear congruences

$$\begin{array}{rcl} x & \equiv & 1 \pmod{3} \\ x & \equiv & 2 \pmod{4} \end{array}$$

Solution for Problem 14.15: From the system of congruences, we know that

$$x = 3a + 1 = 4b + 2$$

for integers a and b. Now we look at the modulo 3 values of both sides of the equation $3a + 1 = 4b + 2$:

$$1 \equiv b + 2 \pmod{3} \Rightarrow b \equiv 2 \pmod{3}.$$

This means that $b = 3c + 2$ for some integer c. Thus,

$$x = 4b + 2 = 4(3c + 2) + 2 = 12c + 10.$$

$x \equiv 10 \pmod{12}$ are the solutions to the system. □

Problem 14.16: Find all solutions to the system of linear congruences

$$\begin{array}{rcl} a & \equiv & 2 \pmod{6} \\ a & \equiv & 3 \pmod{9} \end{array}$$

Solution for Problem 14.16: According to the system of linear congruences,

$$a = 6x + 2 = 9y + 3$$

for integers x and y. Applying modulo 6 to $6x + 2 = 9y + 3$, we get

$$2 \equiv 3y + 3 \pmod{6} \Rightarrow 3y \equiv 5 \pmod{6}.$$

This means that $3y = 6z + 5$ for some integer z. Applying modulo 3 to both sides of this equation, we get

$$0 \equiv 2 \pmod{3}.$$

This congruence is clearly false, so there are no possible solutions for z. Likewise, there are no solutions for y and thus *no solutions* for a. □

We could also show that there are no solutions to Problem 14.16 using a modulus that is the GCD of the moduli in the system. The GCD of 6 and 9 is 3. From our system of linear congruences, we have

$$\begin{array}{lcl} a \equiv 2 \pmod{6} & \Rightarrow & a \equiv 2 \pmod{3} \\ a \equiv 3 \pmod{9} & \Rightarrow & a \equiv 0 \pmod{3} \end{array}$$

Since a cannot be equivalent to both 2 and 0 modulo 3, there are no solutions.

Problem 14.17: Find all solutions to the system of linear congruences

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 2 \pmod{4} \\ x &\equiv 4 \pmod{5} \end{aligned}$$

Solution for Problem 14.17: We solve the system of 3 linear congruences in steps. First we find the integers that satisfy two of them at once. Then we find we determine which of those integers also satisfy the other congruence. We already determined in Problem 14.15 that $x \equiv 10 \pmod{12}$ are the solutions to the first two congruences. From these solutions and $x \equiv 4 \pmod{5}$, we know that

$$x = 12a + 10 = 5b + 4$$

for integers a and b. Applying modulo 5 to $12a + 10 = 5b + 4$, we get

$$2a \equiv 4 \pmod{5} \Rightarrow a \equiv 2 \pmod{5}.$$

This means that $a = 5c + 2$ for some integer c. Thus,

$$x = 12a + 10 = 12(5c + 2) + 10 = 60c + 34,$$

and $x \equiv 34 \pmod{60}$ are the solutions to the system of three linear congruences. □

Concept: We can think of our process of finding a single linear congruence that satisfies two linear congruences as simplifying a system of linear congruences. We solve systems of more than two linear congruences (of the same one variable) by continual simplification. We combine two congruences into one as many times as we need to either show that there are no solutions or to express the solutions as a single linear congruence.

Problem 14.18: How many three-digit positive integers leave a remainder of 2 when divided by 5 and a remainder of 6 when divided by 7?

Solution for Problem 14.18: We want to count all three-digit integers N such that

$$N = 5a + 2 = 7b + 6,$$

where a and b are integers. Applying modulo 5 to $5a + 2 = 7b + 6$ we get

$$2 \equiv 2b + 1 \pmod 5 \Rightarrow b \equiv 3 \pmod 5.$$

This means that $b = 5c + 3$ for some integer c. Thus

$$N = 7b + 6 = 7(5c + 3) + 6 = 35c + 27.$$

Since $100 \le N < 1000$, our goal is to count the integral values of c such that

$$100 \le 35c + 27 < 1000.$$

Subtracting 27 from all parts of this inequality chain, we get

$$73 \le 35c < 973 \Rightarrow 3 \le c \le 27.$$

There are $27 - 3 + 1 = 25$ possible values of c corresponding to 25 three-digit integers N that leave a remainder of 2 when divided by 5 and a remainder of 6 when divided by 7. □

Note that the values of N in Problem 14.18 are the three-digit integers that satisfy the system of linear congruences

$$\begin{aligned} N &\equiv 2 \pmod 5 \\ N &\equiv 6 \pmod 7 \end{aligned}$$

Problem 14.19: Find all solutions to the system of linear congruences

$$\begin{aligned} 4N &\equiv 3 \pmod 7 \\ 5N &\equiv 7 \pmod 8 \end{aligned}$$

Solution for Problem 14.19: We begin by simplifying the first linear congruence:

$$4N \equiv 3 \equiv 10 \equiv 17 \equiv 24 \pmod 7,$$

so

$$N \equiv 24 \cdot 4^{-1} \equiv 6 \cdot 4 \cdot 4^{-1} \equiv 6 \pmod 7.$$

Now we simplify the second linear congruence:

$$5N \equiv 7 \equiv 15 \pmod 8,$$

so

$$N \equiv 15 \cdot 5^{-1} \equiv 3 \cdot 5 \cdot 5^{-1} \equiv 3 \pmod 8.$$

These simplifications reduce our task to solving the following system:

$$\begin{aligned} N &\equiv 6 \pmod 7 \\ N &\equiv 3 \pmod 8 \end{aligned}$$

Now we note that

$$N = 7a + 6 = 8b + 3$$

for integers a and b. Applying modulo 7 to $7a + 6 = 8b + 3$, we get

$$6 \equiv b + 3 \pmod 7 \quad \Rightarrow \quad b \equiv 3 \pmod 7.$$

This means that $b = 7c + 3$ for some integer c. Now we rewrite N in terms of c, giving us the solutions to the original system of linear congruences:

$$N = 8b + 3 = 8(7c + 3) + 3 = 56c + 27 \quad \Rightarrow \quad N \equiv 27 \pmod{56}.$$

□

Exercises

14.4.1 Solve the system of linear congruences:

$$\begin{aligned} a &\equiv 3 \pmod 8 \\ a &\equiv 5 \pmod 9 \end{aligned}$$

14.4.2 Solve the system of linear congruences:

$$\begin{aligned} 3N &\equiv 2 \pmod 4 \\ 2N &\equiv 4 \pmod 7 \end{aligned}$$

14.4.3 Find the largest integer less than 400 that leaves a remainder of 2 when divided by 3 and a remainder of 4 when divided by 7.

14.4.4 How many integers between 1 and 100 leave a remainder of 2 when divided by 4 and also a remainder of 4 when divided by 5?

14.4.5 Solve the system of linear congruences:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ 2x &\equiv 3 \pmod 5 \\ 3x &\equiv 5 \pmod 8 \end{aligned}$$

14.5 Summary

Definitions:

- A **linear congruence equation** is a congruence equation that involves a variable raised only to the first power.
- The modulo m **inverse** of an integer b is the integer b^{-1} such that

$$b \cdot b^{-1} \equiv 1 \pmod{m}.$$

Important: A modulo m residue r has a single inverse if and only if $\gcd(m, r) = 1$. Otherwise, it has no inverse.

Concept: In much the same way that we solve ordinary algebraic linear equations, we solve simple linear congruences by manipulating both sides of the congruence until the variable is isolated.

However, we must use a few different methods to get around the following fact:

WARNING!! Division is not defined in modular arithmetic.

We often multiply by inverses to reduce congruences to simpler forms. We also employ the following technique:

Important: Switching between modular and parametric forms of information about integers helps us solve systems of linear congruences.

Among other things, switching between modular and parametric forms helps us prove the following:

Important: If $ak \equiv bk \pmod{mk}$ for integers a and b, a positive integer k, then

$$a \equiv b \pmod{m}.$$

Combining the methods above, we summarized:

Important: Let a, b, and c be integers such $ac \equiv bc \pmod{m}$. Then

$$a \equiv b \pmod{\frac{m}{\gcd(m, c)}}.$$

We solved a few word problems by solving linear congruences.

> **Concept:** Many remainder problems are just linear congruences.

This includes remainder problems with more than one piece of information about remainders. Such problems become systems of linear congruences, which we also learned to solve.

> **Concept:** We can think of our process of finding a single linear congruence that satisfies two linear congruences as a simplification process. We solve systems of more than 2 linear congruences (of the same one variable) by continually simplifying. We combine two congruences into one as many times as we need to either show that there are no solutions or to express the solutions as a single linear congruence.

Let's summarize what we learned about linear congruences and how to solve them.

The General Process	The Applied Process
First, we can organize any linear congruence into the form $$ax \equiv b \pmod{m},$$ where x is the variable.	Given the linear congruence $$9x + 4 \equiv 10 \pmod{12},$$ we subtract 4 from both sides to get $$9x \equiv 6 \pmod{12}.$$
A linear congruence $ax \equiv b \pmod{m}$ has solutions if and only if $\gcd(a, m) \mid b$.	Note that $\gcd(9, 12) = 3$, $3 \mid 6$, and $3 \nmid 4$. The linear congruence $9x \equiv 6 \pmod{12}$ has solutions while $9x \equiv 4 \pmod{12}$ does not.
If $\gcd(a, m) \mid b$, then we let $d = \gcd(a, m)$ and rewrite the linear congruence using $a = a_1 d$, $b = b_1 d$, and $m = m_1 d$: $$a_1 dx \equiv b_1 d \pmod{m_1 d}.$$ This linear congruence has the same solutions as $a_1 x \equiv b_1 \pmod{m_1}$.	Since $\gcd(9, 12) = 3$, the linear congruence $$9x \equiv 6 \pmod{12}$$ has the same solutions as the linear congruence $$\frac{9}{3}x \equiv \frac{6}{3} \pmod{\frac{12}{3}},$$ which simplifies to $3x \equiv 2 \pmod{4}$.
Note that $$\begin{aligned} d &= \gcd(a, m) \\ &= \gcd(a_1 d, m_1 d) \\ &= d \gcd(a_1, m_1) \end{aligned}$$ So, $\gcd(a_1, m_1) = 1$. This means that a_1^{-1} exists in modulo m_1. Now we multiply both sides of $a_1 x \equiv b_1 \pmod{m_1}$ by a_1^{-1} to get $$x \equiv a_1^{-1} b_1 \pmod{m_1},$$ which are the solutions to $ax \equiv b \pmod{m}$.	Since $\gcd(3, 4) = 1$, we know that 3 has a modulo 4 inverse. In fact, $$3^{-1} \equiv 3 \pmod{4}.$$ Multiplying both sides of $3x \equiv 2 \pmod{4}$ by 3^{-1}, we get $$\begin{aligned} x &\equiv 2 \cdot 3^{-1} \\ &\equiv 2 \cdot 3 \equiv 2 \pmod{4} \end{aligned}$$ So, $x \equiv 2 \pmod{4}$ describes all solutions to $9x \equiv 6 \pmod{12}$.

Review Problems

14.20 Find the inverse of each of the following:

(a) 7 (mod 12)
(b) 13 (mod 14)
(c) 5 (mod 26)
(d) 16 (mod 19)

14.21 Which modulo 20 residues have no inverse?

14.22 Prove that in any modulus m that $m-1$ is its own inverse.

14.23 Solve each of the following linear congruences.

(a) $4x \equiv 3 \pmod 7$

(b) $6x - 13 \equiv 29 \pmod{72}$

(c) $26x - 473 \equiv 489 \pmod{20}$

14.24 Solve the system of linear congruences:

$$\begin{aligned} 5x &\equiv 1 \pmod 3 \\ 12x &\equiv 4 \pmod 7 \end{aligned}$$

14.25 Solve the system of linear congruences:

$$\begin{aligned} N &\equiv 2 \pmod 3 \\ N &\equiv 1 \pmod 4 \\ N &\equiv 4 \pmod 5 \end{aligned}$$

14.26 How many integers between 200 and 500 inclusive leave a remainder of 1 when divided by 7 and a remainder of 3 when divided by 4?

14.27 Find the smallest positive integer that leaves a remainder of 5 when divided by 7, a remainder of 6 when divided by 11, and a remainder of 4 when divided by 13.

Extra! *Those who dream by day are cognizant of many things which escape those who dream only by night.* – Edgar Allan Poe

Challenge Problems

14.28 A natural number leaves a remainder of 7 when divided by 11 and a remainder of 10 when divided by 12. Find the remainder when the number is divided by 66.

14.29 Let m be an integer greater than 101. Find the number of values of m such that 101 is its own inverse modulo m. **Hints:** 58

14.30 Adam and Ben start their new jobs on the same day. Adam's schedule is 3 workdays followed by 1 rest day. Ben's schedule is 7 workdays followed by 3 rest days. On how many of their first 1000 days do both have rest days on the same day? *(Source: AMC)* **Hints:** 91

14.31★ How many four-digit integers either leave a remainder of 2 when divided by 7, or a remainder of 4 when divided by 5, but not both? **Hints:** 25

14.32★ Two base 120 units digits (not necessarily different) are chosen randomly and their product is written in base 120. What is the probability that the units digit of the base 120 product is 1? **Hints:** 10

14.33★ The integer p is a 50-digit prime number. When its square is divided by 120, the remainder is not 1. What is the remainder? **Hints:** 111, 103

Extra! **Compositions of Squares**

In 1770, French mathematician **Joseph-Louis Lagrange** (1736–1813) proved that every positive integer is either a perfect square or a sum of two, three, or four perfect squares:

$$\begin{aligned}
1 &= 1^2\\
2 &= 1^2+1^2\\
3 &= 1^2+1^2+1^2\\
4 &= 2^2\\
5 &= 1^2+2^2\\
&\vdots\\
30 &= 1^2+2^2+5^2\\
31 &= 1^2+1^2+2^2+5^2\\
32 &= 4^2+4^2\\
33 &= 2^2+2^2+3^2+4^2\\
&\vdots
\end{aligned}$$

Extra! *When I am working on a problem I never think about beauty. I only think about how to solve the problem. But when I have finished, if the solution is not beautiful, I know it is wrong.*

– Buckminster Fuller

Extra! **Quadratic Forms**

In 1801, Gauss worked on an area of math that has become known as **algebraic number theory**. His explorations at that time revolved around values of expressions of the form

$$ax^2 + bxy + cy^2,$$

where a, b, and c are integer coefficients in a polynomial in which each term includes the square of a variable or the product of two variables. We call such expressions **quadratic forms**. In particular, Lagrange's theorem that every integer is either a square or a sum of two, three, or four squares is a statement about the simple quadratic form $s^2 + t^2 + u^2 + v^2$, where s, t, u, and v represent integers.

In 1916, Ramanujan discovered 53 different quadratic forms that each equal every nonnegative integer for some set of integer values of the variables. Here are a few of them:

$$\begin{array}{ccccccc} s^2 & + & t^2 & + & u^2 & + & 2v^2 \\ s^2 & + & t^2 & + & u^2 & + & 3v^2 \\ s^2 & + & t^2 & + & 2u^2 & + & 2v^2 \\ s^2 & + & t^2 & + & 3u^2 & + & 5v^2 \\ s^2 & + & 2t^2 & + & 3u^2 & + & 5v^2 \end{array}$$

More recently, Princeton University mathematician **Manjul Bhargava** proved a set of theorems that demonstrate exactly which quadratic forms generate every nonnegative integer for some set of integer inputs. Bhargava's work extended research by another famous Princetonian problem solver **John Conway** as well as Ramanujan's work. For his efforts, Bhargava was awarded the **SASTRA Ramanujan Prize**, which is awarded each year to young mathematicians for research into topics Ramanujan contributed to during his lifetime.

Extra! *Historians of a generation ago were often shocked by the violence with which scientists rejected the history of their own subject as irrelevant; they could not understand how the members of any academic profession could fail to be intrigued by the study of their own cultural heritage. What these historians did not grasp was that scientists will welcome the history of science only when it has been demonstrated that this discipline can add to our understanding of science itself and thus help to produce, in some sense, better scientists.* – I. Bernard Cohen

An idea which can be used once is a trick. If it can be used more than once it becomes a method.
– George Polya and Gabor Szego

CHAPTER 15 Number Sense

15.1 Introduction

In this chapter, we focus entirely on problem solving techniques. Just as importantly, we explore methods that help us use our familiarity with numbers to solve problems *more efficiently*. We call this useful familiarity **number sense**.

Some math students or teachers might dismiss much of this chapter as a series of tricks and gimmicks. However, many of the ideas discussed are common enough that we can make practical use of them. Others are concepts that, as they become more highly developed using more and more advanced mathematics, begin to appear more naturally related to general mathematics curriculum. Most importantly however, *exercising number sense* means *exercising your mind*.

Note that all exercises are left until the review section to test your ability to determine which problem solving methods are most appropriate for each problem.

15.2 Familiar Factors and Divisibility

Students with experience factoring integers and discovering the reasons behind various divisibility rules find themselves recognizing useful relationships between integers much more quickly. This form of number sense often leads to easier solutions and fewer mistakes. It sometimes makes the difference between solving a problem and not solving it at all.

Problems

Problem 15.1: How many digits are in the product $4^{20} \cdot 5^{36}$? *(Source: MATHCOUNTS)*

Problem 15.2: Evaluate

$$\sqrt[5]{32^2 + 16^3 + 8^4 + 4^5}.$$

(Source: MATHCOUNTS)

Problem 15.3: Find the largest 4-digit multiple of 8 that has 3, 5, and 7 among its digits. *(Source: MATHCOUNTS)*

Problem 15.4: Insert parentheses to make the following a true statement.

$$4 + 6 \times 5 - 2/6 - 2 = 12.$$

(Source: MATHCOUNTS)

Problem 15.5: Find all ordered triples of positive integers (a, b, c) such that

$$a + \frac{1}{b + \frac{1}{c}} = 9.5.$$

(Source: MATHCOUNTS)

Problem 15.6: Calculate the following product in your head:

$$163 \cdot 125.$$

Problem 15.7: John claimed to Linda that the sum of the digits of 10101^5 is 25. Linda immediately informed John that he was incorrect. How did she know so quickly?

Problem 15.1: How many digits are in the product $4^{20} \cdot 5^{36}$? *(Source: MATHCOUNTS)*

Solution for Problem 15.1: We notice many powers of 2 and 5 in this product. Many of them will combine to form powers of 10. We rewrite our product so we can view these powers of 10 separately from everything else:

$$4^{20} \cdot 5^{36} = 2^{40} \cdot 5^{36} = 2^4 \cdot \left(2^{36} \cdot 5^{36}\right) = 2^4 \cdot 10^{36} = 16 \cdot 10^{36}.$$

So, our result is 16 followed by 36 zeroes, which has $2 + 36 = 38$ digits. □

Problem 15.2: Evaluate

$$\sqrt[5]{32^2 + 16^3 + 8^4 + 4^5}.$$

(Source: MATHCOUNTS)

Solution for Problem 15.2: We could simply expand all the exponential expressions inside the radical and then evaluate the result of the radical using a prime factorization of the result. However, this would take a lot of time, so we would like to find a better method.

We notice that all of the exponential expressions are powers of 2. Common forms often help us work with quantities more easily, so we rewrite the entire expression to highlight the powers of 2:

$$\sqrt[5]{2^{10}+2^{12}+2^{12}+2^{10}}.$$

This form is nice, but we're still summing four terms. Fortunately, we can easily rewrite 2^{12} in terms of 2^{10}:

$$2^{12}=2^2\cdot 2^{10}=4\cdot 2^{10}.$$

Next, we rewrite the entire expression and group by like terms:

$$\sqrt[5]{2^{10}+2^{12}+2^{12}+2^{10}}=\sqrt[5]{2^{10}+4\cdot 2^{10}+4\cdot 2^{10}+2^{10}}=\sqrt[5]{10\cdot 2^{10}}.$$

Finally, we remove powers of 2 from the radical expression:

$$\sqrt[5]{10\cdot 2^{10}}=\sqrt[5]{2^{10}}\sqrt[5]{10}=2^2\sqrt[5]{10}=4\sqrt[5]{10}.$$

Since $\sqrt[5]{10}$ does not simplify, $4\sqrt[5]{10}$ is our answer. □

Problem 15.3: Find the largest 4-digit multiple of 8 that has 3, 5, and 7 among its digits. *(Source: MATHCOUNTS)*

Solution for Problem 15.3: By the divisibility rule for 8, we only need to look at the last 3 digits of an integer to determine whether or not an integer is a multiple of 8. We also know that any multiple of 8 is a multiple of every one of its divisors, so the number we are looking for is a multiple of 2. This means that the units digit of the number we seek must be even. This tells us that 3, 5, and 7 must be, in some order, the first three digits of the integer we seek.

We want the number to be as large as possible, so we order the digits from greatest to least to create the largest integers with all the necessary digits. If there are integer(s) in the form $753A$ that are multiples of 8 for some digit A, then these will be the largest possible 4-digit multiples of 8 with 3, 5, and 7 among their digits. Among any 8 consecutive integers, we know that the modulo 8 residue of at least 1 of those integers is 0. This means that among the 10 integers $753A$ formed by the possible values for the digit A, at least one of them is a multiple of 8.

We could now perform long division to find the possible value(s) of the digit A. However, we can quickly apply modular arithmetic (using the divisibility rule for 8) to determine A:

$$7530+A\equiv 7\cdot 10^3+530+A\equiv 530+A\equiv 480+50+A\equiv 50+A\equiv 48+2+A\equiv 2+A\equiv 0 \pmod{8}.$$

Since A is between 0 and 9 inclusive, we see that $A=6$. The largest 4-digit integer including 3, 5, and 7 among its digits is therefore 7536.

Written out, the modular arithmetic might look longer than long division, but some students comfortable with these divisibility manipulations can perform the calculations more swiftly. □

Problem 15.4: Insert parentheses to make the following a true statement.

$$4+6\times 5-2/6-2=12.$$

(Source: MATHCOUNTS)

Solution for Problem 15.4: We are working only with integers in this problem. The only part of the statement that might cause a computation to be a noninteger is the division. We notice that unless we stick parentheses around the $6-2$ that we are forced to use parentheses before the 6 to set apart an entire numerator that is a multiple of 6.

Unless we place parentheses around $(4+6)$, the 6×5 prohibits the possibility of creating a numerator that is a multiple of 6. Thus, we have the only possible way to make a numerator that is a multiple of 6:

$$((4+6)\times 5-2)/6-2=(10\times 5-2)/6-2=(50-2)/6-2=48/6-2=8-2=6\neq 12,$$

so the statement would be false. This means we must put parentheses around $6-2$.

Now we group $6-2$ with parentheses and work from there:

$$4+6\times 5-2/(6-2)=12$$

becomes

$$4+6\times 5-2/4=12.$$

Again, we'll need parentheses somewhere as we are dividing by 4 in the left-hand side of the equation. We already saw that we could produce a numerator of 48 the way we used parentheses before the division when we tried to divide by 6. This gives us our solution:

$$((4+6)\times 5-2)/(6-2)=48/4=12.$$

□

Problem 15.5: Find all ordered triples of positive integers (a,b,c) such that

$$a+\frac{1}{b+\frac{1}{c}}=9.5.$$

(Source: MATHCOUNTS)

Solution for Problem 15.5: All the variables and fractions are on the left-hand side of the equation, so we begin by focusing on that expression. We note the interesting features of the left-hand side. Since $b+\frac{1}{c}>1$, the reciprocal of this expression is less than 1: $\frac{1}{b+\frac{1}{c}}<1$. This means that the left-hand side of the equation is an integer plus some fraction that is between 0 and 1. From this we can already see that $a=9$:

$$9+\frac{1}{b+\frac{1}{c}}=9.5.$$

Subtracting 9 from both sides and expressing the result of the right-hand side as a fraction helps us compare everything that remains:

$$\frac{1}{b+\frac{1}{c}}=\frac{1}{2}.$$

Equating the reciprocals of both sides of the equation gives us an easier equation to work with:

$$b+\frac{1}{c}=2.$$

Now we see that $1/c = 2 - b$, so $1/c$ is an integer. Since c is also an integer, there is one possible value for c: $c = 1$. This means $b = 1$ as well. $(9, 1, 1)$ is the only solution. □

Problem 15.6: Calculate the following product in your head:

$$163 \cdot 125.$$

Solution for Problem 15.6: When learning about fraction to decimal conversions we saw how useful it can be to multiply a terminating decimal by the smallest power of 10 that produces an integer product. We reverse this idea to help us with multiplication.

$$125 = 1000(0.125) = 1000\left(\frac{1}{8}\right)$$

This gives us another approach to multiplication by 125:

$$163 \cdot 125 = 163 \cdot 1000 \cdot \frac{1}{8} = 1000 \cdot \frac{163}{8}$$

We now divide 8 into 163, which is not all that difficult in this case. Our product is now

$$1000 \cdot 20.375 = 20375.$$

□

Problem 15.7: John claimed to Linda that the sum of the digits of 10101^5 is 25. Linda immediately informed John that he was incorrect. How did she know so quickly?

Solution for Problem 15.7: Divisibility rules (and other facts) can often help us check our work on math problems. Linda noticed that 10101 is a multiple of 3 and that 10101^5 is therefore a multiple of 9. This means that the sum of its digits must also be a multiple of 9. Since $25 \equiv 2 + 5 \equiv 7 \pmod 9$, Linda knows that 25 is not a multiple of 9. Thus 25 cannot be the sum of the digits of 10101^5. □

Concept: Number sense is not just about solving problems. Number sense helps us connect mathematics in new and different ways. Sometimes this means finding quick ways to check our work. Sometimes it means noticing entirely new mathematical relationships.

15.3 Algebraic Methods of Arithmetic

You might be able to do some of the following problems in your head. Give it a try! Try to work the ones you can't perform in your head on paper and see if you can find a way to work them so that you don't need the paper anymore.

Problems

Problem 15.8: Evaluate:

$$200003^2 - 199997^2.$$

Problem 15.9: Find the prime factorization of $3^8 - 4$.

Problem 15.10: Find the value of

$$49^3 + 3 \cdot 49^2 + 3 \cdot 49 + 1.$$

Problem 15.11: Find the prime factorization of 205205000.

Problem 15.12: Find the third smallest natural number that leaves a remainder of 3 when divided by each of 4, 5, 6, 7, and 8.

Problem 15.8: Evaluate:

$$200003^2 - 199997^2.$$

Solution for Problem 15.8: *Solution 1:* Some clever students might recognize what we can do immediately. Students who have never seen a problem like this one should still recognize that the integers being squared are symmetrically arranged around 200000. It is the largeness of the integers that can intimidate us. For this reason we replace 200000 with a variable, x:

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

Expanding each squared binomial we find that

$$x^2 + 6x + 9 - (x^2 - 6x + 9) = 12x.$$

Substituting back for x we see that $12x = 2400000$ is our answer.

Solution 2: Factorization gives us a second solution to this problem. Clever students might factor the difference of squares:

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

When $a = 200003$ and $b = 199997$, the sum and difference of a and b are easy to calculate:

$$200003^2 - 199997^2 = (200003 + 199997)(200003 - 199997) = 400000 \cdot 6 = 2400000.$$

□

Problem 15.9: Find the prime factorization of $3^8 - 4$.

Solution for Problem 15.9: We could multiply everything out and hope for an easy time factoring primes, but that would take a lot of time. Looking for an easier method we notice that $3^8 = (3^4)^2$ and $4 = 2^2$ are both perfect squares. This allows us to make use of the difference of squares factorization:

$$3^8 - 4 = (3^4)^2 - 2^2 = (3^4+2)(3^4-2) = (81+2)(81-2) = 83 \cdot 79.$$

Since 79 and 83 are prime, the prime factorization is simply $79^1 \cdot 83^1$.

Without the difference of squares, you might be stuck hunting through primes all the way up to 79 before discovering the prime factorization of $3^8 - 4$. You might just fall asleep before you finish! □

Important: It helps to know your primes up to 100 because they are common in practical number theory problems.

While it's been mentioned before, students should be aware that 91 is not prime. In fact, we can see this from a difference of squares:

$$91 = 100 - 9 = 10^2 - 3^2 = (10 + 3)(10 - 3) = 13 \cdot 7.$$

Differences of squares can help us quickly identify many other composites as well:

$$221 = 225 - 4 = 15^2 - 2^2 = (15 + 2)(15 - 2) = 17 \cdot 13.$$

Concept: The more time you spend thinking about and solving number theory problems, the more quickly you can see useful relationships between integers. Students develop number sense more from practice than natural ability.

Problem 15.10: Find the value of

$$49^3 + 3 \cdot 49^2 + 3 \cdot 49 + 1.$$

Solution for Problem 15.10: Here we must simply cube, square, and calculate unless we are familiar with the expansion of $(x + y)^3$:

$$(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

Replacing x with 49 and y with 1 tells us that

$$(49 + 1)^3 = 49^3 + 3 \cdot 49^2 + 3 \cdot 49 + 1.$$

This algebraic substitution allows us to calculate the expression much more easily:

$$(49 + 1)^3 = 50^3 = 5^3 \cdot 10^3 = 125 \cdot 1000 = 125000.$$

□

Concept: Awareness of the ways in which algebra works together with number theory (or other subjects) adds significantly to our ability to use the tools of both algebra and number theory to solve problems.

Problem 15.11: Find the prime factorization of 205205000.

Solution for Problem 15.11: We could build a factor tree while hunting for prime divisors beginning with 2. However, the integer we want to factor breaks down rather nicely:

$$205205000 = 205205 \cdot 1000.$$

Seeing that $1000 \mid 205205000$ was not particularly difficult, but there is more that we can see in the digits of 205205000. There is a repetition of the 205 block of digits. The blocks of digits are distinguished only by powers of the decimal base, 10. This allows us to write 205205 in a useful way:

$$205205 = 205 \cdot 10^3 + 205 = 205(10^3 + 1) = 205 \cdot 1001.$$

This allows us to break 205205000 down further:

$$205205000 = 205 \cdot 1001 \cdot 1000.$$

Notice that 1001 is the sum of two cubes, helping us with its factorization:

$$1001 = 10^3 + 1^3 = (10 + 1)(10^2 - 10 + 1) = 11 \cdot 91 = 7 \cdot 11 \cdot 13.$$

Now we find the prime factorizations of 205, 1001, and 1000:

$$\begin{aligned} 205 &= 5^1 \cdot 41^1 \\ 1001 &= 7^1 \cdot 11^1 \cdot 13^1 \\ 1000 &= 2^3 \cdot 5^3 \end{aligned}$$

Multiplying these prime factorizations together gives us our answer:

$$205205000 = 2^3 \cdot 5^4 \cdot 7^1 \cdot 11^1 \cdot 13^1 \cdot 41^1.$$

□

Problem 15.12: Find the third smallest natural number that leaves a remainder of 3 when divided by each of 4, 5, 6, 7, and 8.

Solution for Problem 15.12: We begin our exploration of this problem by naming the star of the show: Let N be a natural number that leaves a remainder of 3 when divided by each of 4, 5, 6, 7, and 8. We now rewrite the given information using modular congruences:

$$\begin{aligned} N &\equiv 3 \pmod 4 \\ N &\equiv 3 \pmod 5 \\ N &\equiv 3 \pmod 6 \\ N &\equiv 3 \pmod 7 \\ N &\equiv 3 \pmod 8 \end{aligned}$$

We now have a system of linear congruences, but we do not intend to solve this problem by walking through the steps for solving a system of linear congruences. We realize that it's easier to work with expressions that are multiples of integers rather than those than leave remainders. For this reason, we subtract 3 from both sides of each congruence:

$$\begin{aligned} N - 3 &\equiv 0 \pmod 4 \\ N - 3 &\equiv 0 \pmod 5 \\ N - 3 &\equiv 0 \pmod 6 \\ N - 3 &\equiv 0 \pmod 7 \\ N - 3 &\equiv 0 \pmod 8 \end{aligned}$$

Now we recognize that $N - 3$ can be any integer that is a multiple of each of 4, 5, 6, 7, and 8. Such an integer must be a multiple of the LCM of 4, 5, 6, 7, and 8. The LCM of these integers is

$$2^3 \cdot 3^1 \cdot 5^1 \cdot 7^1 = 840.$$

This means that $N - 3 = 840m$ for some integer m. Isolating N we have

$$N = 840m + 3.$$

The smallest such natural number comes from $m = 0$, the second smallest from $m = 1$, and the third smallest from $m = 2$:

$$N = 840 \cdot 2 + 3 = 1683,$$

which is our answer.

Some experienced students might recognize that the goal is to simply add 3 to each multiple of the LCM of 4, 5, 6, 7, and 8. That's fine, so long as you understand how a natural setup of this kind of problem leads to the quick solution. Failure to understand the reasoning behind quick methods keeps many problem solvers from learning to solve more difficult problems. □

Concept: Working through the long solution to a problem helps us better understand why the quick solution works and increases the range of our problem solving abilities.

Sidenote: **Squaring Integers With Units Digit 5**

There is a shortcut for squaring integers that end in 5 that might boost your mental arithmetic abilities. When squaring each of 15, 25, 35, 45, and 55, we cut off the units digit. We multiply what's left with the next highest integer. Lastly, we stick the digits 25 on the end and we have the square:

$$\begin{aligned} 1 \cdot 2 &= 2 &&\rightarrow & 15^2 &= \underline{2}25 \\ 2 \cdot 3 &= 6 &&\rightarrow & 25^2 &= \underline{6}25 \\ 3 \cdot 4 &= 12 &&\rightarrow & 35^2 &= \underline{12}25 \\ 4 \cdot 5 &= 20 &&\rightarrow & 45^2 &= \underline{20}25 \\ 5 \cdot 6 &= 30 &&\rightarrow & 55^2 &= \underline{30}25 \end{aligned}$$

This method even works for larger numbers:

$$100 \cdot 101 = 10100 \rightarrow 1005^2 = 1010025$$

Factorization lies at the heart of this arithmetic trick. When an integer has a units digit of 5, we can write it as $10n + 5$ for some integer n. Let's square this quantity:

$$(10n + 5)^2 = 100n^2 + 100n + 25 = 100(n^2 + n) + 25 = 100n(n + 1) + 25.$$

Now the method is transparent. When we cut the units digit off of $10n + 5$, we have n. Multiplying n by the next larger integer, we get $n(n + 1)$. Multiplying $n(n + 1)$ by 100 and adding 25 is like appending the digits 25 to the end of the product of n and $n + 1$.

Extra! *If you only have a hammer, you tend to see every problem as a nail.*

–Abraham Harold Maslow

15.4 Useful Forms of Numbers

Throughout this book we have seen how displaying numbers in useful forms helps us solve problems. Prime factorization helps us organize the properties of integers in ways that allow us to find divisors and multiples easily. Base numbers help us understand the ways in which integers can be grouped by powers of a single integer. In this section we work a couple of problems that test our ability to find useful forms of integers that help us solve problems—or at least solve them more quickly.

Problems

Problem 15.13: Given that a and b are natural numbers such that

$$\frac{11}{15} > \frac{a}{b} > \frac{7}{10},$$

find the smallest possible value for b. *(Source: MATHCOUNTS)*

Problem 15.14: Find the greatest common divisor of 818874 and 819. *(Source: MATHCOUNTS)*

Problem 15.13: Given that a and b are natural numbers such that

$$\frac{11}{15} > \frac{a}{b} > \frac{7}{10},$$

find the smallest possible value for b. *(Source: MATHCOUNTS)*

Solution for Problem 15.13: Careful trial and error might eventually lead you to a solution, but it would take a long time and there are obstacles to organizing your work. Many students have tripped over this problem using the following faulty logic:

Bogus Solution: We first rewrite the outside fractions using their least common denominator:

$$\frac{22}{30} > \frac{a}{b} > \frac{21}{30}.$$

If $b = 30$, there is no room for a between 21 and 22, so we double the denominators of the outside fractions to make room:

$$\frac{44}{60} > \frac{a}{b} > \frac{42}{60}.$$

Now, when $b = 60$, there is just enough room to squeeze $a = 43$ in between 42 and 44, so $b = 60$ is the answer.

This solution does not address fractions with denominators not related to the denominators of the fractions on the outside of the inequality.

Unfortunately the fractions do not seem to give way to any easy method. We could multiply through by $30b$ to clear the denominators, but that would force us to deal with a variable in each of the three parts of the chain of inequalities:

$$22b > 30a > 21b.$$

These inequalities might make trial and error easier, but not by much.

Since the fractional form in which the numbers in the problem is expressed doesn't give us much to work with, we convert the fractions to decimal form:

$$0.7\overline{3} > \frac{a}{b} > 0.7.$$

Now we have a range for the possible values of the decimal form of $\frac{a}{b}$.

Alas, we must perform a little trial and error, but it does not take us long. We focus on the possible denominators that could produce decimals in the given range. We know that b could not be 1, 2, 3, 4, 5, or 6, but

$$\frac{5}{7} = 0.\overline{714285},$$

so $b = 7$ is our answer. □

Concept: Change numbers to forms that are most useful in a given problem.

Problem 15.14: Find the greatest common divisor of 818874 and 819. *(Source: MATHCOUNTS)*

Solution for Problem 15.14: We could jump straight into prime factorization and there is even one common divisibility rule (the rule for 3) that we could successfully apply to this problem. However, we notice an interesting relationship between the two integers:

$$818874 = 1000 \cdot 819 - 126.$$

This relationship is nice enough that we try making it useful.

We typically find GCDs of pairs of integers using prime factorization. However, the Euclidean Algorithm gives us a second option:

$$\begin{aligned}\gcd(818874, 819) &= \gcd(1000 \cdot 819 - 126, 819) = \gcd(819 - 126, 819) = \gcd(693, 819)\\ &= \gcd(693, 126) = \gcd(63, 126) = \gcd(63, 0) = 63.\end{aligned}$$

Thus $\gcd(818874, 819) = 63$. Using the Euclidean Algorithm was much simpler than finding the prime factorization of a six-digit integer. □

Concept: While we may be most comfortable with a particular method of problem solving, awareness of other methods often helps us solve more difficult problems with relative ease.

While prime factorization is usually the quickest approach for finding common divisors of two natural numbers, we should keep an open mind to the use of the Euclidean algorithm in cases where we can relate the integers most easily through sums or differences.

15.5 Simplicity

While some math problems are difficult, simplicity lies at the heart of mathematics. Problem solvers seek the easiest routes to solutions. Mathematicians build models of mathematical ideas in order to evaluate and discuss them more easily. In this section we solve problems by recognizing their simplest features or by applying concepts related to them.

Problems

Problem 15.15: In how many different ways can 14 dimes be divided into three piles with an odd number of dimes in each pile?

Problem 15.16: Find the largest possible product of three positive prime numbers that sum to 30.

Problem 15.17: Find the sum of all positive numbers less than 36 that do not have any factors besides 1 in common with 36. *(Source: MATHCOUNTS)*

Problem 15.18: Find every three-digit natural number that is equal to the cube of the sum of its digits.

Problem 15.19: The five-digit number $33AB6$ is a perfect square. Find $A + B$.

Problem 15.15: In how many different ways can 14 dimes be divided into three piles with an odd number of dimes in each pile?

Solution for Problem 15.15: We begin by representing the numbers of dimes in each pile algebraically. The number of dimes in each pile is $2a + 1$, $2b + 1$, and $2c + 1$, where a, b, and c are whole numbers. We now equate the total number of dimes in each pile to the known total of all the dimes:

$$(2a + 1) + (2b + 1) + (2c + 1) = 14.$$

Subtracting 3 from each side we see that

$$2a + 2b + 2c = 11.$$

We notice that 2 is a factor of the entire left-hand side of our latest equation. However, dividing both sides by 2 gives us a fraction on the right-hand side:

$$a + b + c = \frac{11}{2}.$$

The sum of three integers cannot be a fraction, so there are 0 ways in which 14 dimes can be divided into three piles with an odd number of dimes in each pile. □

Let's take a step back and see how experienced problem solvers tackle problems such as Problem 15.15 quickly. The goal is to add three odd numbers to get an even sum. However, the sum of the first two odd numbers is even, so adding in a third odd number must produce an odd sum. Since 14 is not odd, it can't be the total number of dimes in those three piles.

Definition: The property of an integer being even or odd is known as **parity**.

Concept: Parity considerations are really just a matter of working in modulo 2. Parity arguments are common enough in problem solving to give their use special attention (in addition to their own name).

We can also work Problem 15.15 in modulo 2 in order to replicate our parity argument. Let a, b, and c be the numbers of dimes in each pile. Thus,

$$\begin{aligned} a &\equiv 1 \pmod 2 \\ b &\equiv 1 \pmod 2 \\ c &\equiv 1 \pmod 2 \end{aligned}$$

We are told that $a + b + c = 14$, but we know that

$$a + b + c \equiv 1 + 1 + 1 \equiv 1 \pmod 2.$$

However, $14 \not\equiv 1 \pmod 2$, so $a + b + c$ cannot equal 14 and there is no way to divide the dimes into three piles of odd numbers.

Problem 15.16: Find the largest possible product of three positive prime numbers that sum to 30.

Solution for Problem 15.16: The sum of three primes is 30, an even number, so either the primes are all even or exactly one of them is even. However, there is only one even prime, 2. The other two primes must therefore be odd and their sum must be $30 - 2 = 28$.

Our only options are 11 & 17, and 5 & 23. Now we must determine which has the larger product:

$$11 \cdot 17 = 187 > 115 = 5 \cdot 23.$$

We now calculate our answer:

$$11 \cdot 17 \cdot 2 = 11 \cdot 34 = 374$$

is the largest product we can form. □

Problem 15.17: Find the sum of all positive numbers less than 36 that do not have any factors besides 1 in common with 36. *(Source: MATHCOUNTS)*

Solution for Problem 15.17: We know how to identify the integers that share common divisors with 36. We begin with its prime factorization:

$$36 = 2^2 \cdot 3^2.$$

An integer will share a common divisor greater than 1 with 36 if and only if it is a multiple of 2 or 3. Modular arithmetic helps us identify the other integers between 0 and 36 (which we want to sum). We look for integers n that satisfy one of the two following systems of linear congruences:

$$\begin{aligned} n &\equiv 1 \pmod 2 \\ n &\equiv 1 \pmod 3 \end{aligned} \qquad \text{or} \qquad \begin{aligned} n &\equiv 1 \pmod 2 \\ n &\equiv 2 \pmod 3 \end{aligned}$$

Solving these systems of linear congruences, we get

$$n \equiv 1 \pmod{6} \qquad \text{or} \qquad n \equiv 5 \pmod{6}.$$

Where $0 < n < 36$, we get our list: $1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35$.

We could simply add all the integers together, but we note a simpler method. Since $\gcd(n, 36) = \gcd(36 - n, 36)$, when n is relatively prime to 36, so is $36 - n$. So, the integers between 0 and 36 that are relatively prime to 36 come in pairs that sum to 36:

$$1 + 35 = 5 + 31 = 7 + 29 = 11 + 25 = 13 + 23 = 17 + 19 = 36$$

We now sum the 12 integers by grouping them into 6 sums of 36, giving us a total sum of $6 \cdot 36 = 216$. □

Problem 15.18: Find every three-digit natural number that is equal to the cube of the sum of its digits.

Solution for Problem 15.18: We have one big piece of information that quickly helps us narrow down the possibilities: any number we seek is a positive three-digit perfect cube. There aren't many positive three-digit cubes, so we might as well list them:

$$\begin{aligned} 5^3 &= 125 \\ 6^3 &= 216 \\ 7^3 &= 343 \\ 8^3 &= 512 \\ 9^3 &= 729 \end{aligned}$$

Now we simply add the digits of each of the cubes to see which digit-sum is the root of the cube:

$$\begin{array}{rcrcl} 1+2+5 &=& 8 &\neq& 5 \\ 2+1+6 &=& 9 &\neq& 6 \\ 3+4+3 &=& 11 &\neq& 7 \\ 5+1+2 &=& 8 &=& 8 \\ 7+2+9 &=& 18 &\neq& 9 \end{array}$$

So 512 is the only three-digit integer that is equal to the cube of the sum of its digits. □

Concept: Don't make a problem harder than it needs to be. While experienced problem solvers have learned that hunting through lists is often an extremely slow way to solve a problem, there are exceptions. If you can narrow your search to a *small* list, hunting through that list might be easiest.

Problem 15.19: The five-digit number $33AB6$ is a perfect square. Find $A + B$.

Solution for Problem 15.19: If we can identify the square root of our integer, we can simply square the square root to get our integer. We hone in on the value of the square root by finding easy-to-compute perfect squares above and below the given perfect square:

$$100^2 = 10000 < 33AB6 < 40000 = 200^2.$$

This tells us that the square root is between 100 and 200. We refine this estimate even further:

$$180^2 = 32400 < 33AB6 < 36100 = 190^2.$$

The only thing left to determine is the units digit of the square root. The square of an integer has a units digit of 6 only when the integer itself has a units digit of either 4 or 6. Since $33AB6$ is closer to 32400 than 36100, we first try 184:

$$184^2 = 33856.$$

This square matches the digits given in the problem. We now know that $A = 8$, $B = 5$, and our answer is $A + B = 13$. □

Concept: We can often use clues to gather enough information to solve a problem that has no obvious or direct solution.

15.6 Summary

Experience working number theory problems helps us develop our number sense which in turn allows us to solve many problems more easily.

Concept: Number sense is not just about solving problems. Number sense helps us connect mathematics in new and different ways. Sometimes this means finding quick ways to check our work. Sometimes it means noticing entirely new mathematical relationships.

Students who develop number sense are far less likely to misunderstand or misinterpret problems or make errors involving numbers and calculations. An understanding of divisibility rules and different ways to factor integers often provides problem solvers with the confidence and insight to quickly identify and solve number theory problems.

Important: It helps to know your primes up to 100 because they are common in practical number theory problems.

Familiarity with all kinds of numbers makes problem solving easier. Primes are particularly important in the realm of number theory.

Concept: The more time you spend thinking about and solving number theory problems, the more quickly you can see useful relationships between integers. Students develop number sense more from practice than natural ability.

While some students seem to display an instantaneous ability to recognize relationships between numbers, this ability comes from *thinking about math problems*. Thinking about interesting number theory problems helps you fine-tune your number sense.

Concept: Awareness of the ways in which algebra works together with number theory (or other subjects) adds significantly to our ability to use the tools of both algebra and number theory to solve problems.

The more you learn about number theory and algebra, the more you will be able to use variables and algebraic expressions to help you solve more difficult problems. Learning to use different areas of mathematics together greatly amplifies the scope of problems you can solve.

Concept: Working through the long solution to a problem helps us better understand why a quick solution works and increases the range of our problem solving abilities.

It's nice to know how to solve problems more quickly. Problem solving efficiency often comes from thinking through the methods and techniques used to solve difficult problems. Once you understand those methods and techniques better, you can often jump straight to calculating answers.

Concept: When the forms of numbers we are working with do not seem to give way to a practical solution, changing the form in which we express those numbers to match the problem often simplifies the problem greatly.

Throughout this book we make use of forms of numbers that are most helpful in problem solving. We often use prime factorizations to help organize the properties and relationships of integers. It sometimes helps to think about fractions in terms of decimals and vice versa because one form gives us a better framework for working a particular problem. We even use some algebraic forms to help us perform integer calculations more easily.

Concept: While we may be most comfortable with a particular method of problem solving, awareness of other methods often helps us solve more difficult problems with relative ease.

While you might often be comfortable honing in on particular problem types using trusted methods, it is important to keep an open mind while problem solving. Some problems are more easily solved by one method than another and if we take the time to think about which method of attack might work best, we are more likely to solve problems quickly and accurately.

Concept: Parity considerations are really just a matter of working in modulo 2. Parity arguments are common enough in problem solving to give their use special attention (in addition to their own name).

Awareness of even and odd numbers is a handy kind of number sense. Understanding parity can help you make short work of some problems that would otherwise take considerable time to solve.

Concept: Don't make a problem harder than it needs to be. While experienced problem solvers have learned that hunting through lists is often an extremely slow way to solve a problem, there are exceptions. If you can narrow your search to a *small* list, hunting through that list might be easiest.

Practicality is a problem solver's friend. Use any method you can if it solves a problem quickly.

> **Concept:** While there may not be a direct way to compute the answers to some problems, we can often use clues to gather enough information to solve the problem.

Some problems seem to provide little useful information or no possibility for direct calculation. At these times we must consider any clues available to solve the problem. This information comes in many forms—primes, composites, perfect squares, digits, divisors, multiples, etc. It pays to have an understanding as to how different properties of integers affect possible solutions to problems.

REVIEW PROBLEMS

15.20 What number is one-half of one-tenth of one-fifth of one-half of one million? *(Source: MATHCOUNTS)*

15.21 Find the smaller of two prime numbers whose sum is also prime.

15.22 There are 24 four-digit whole numbers that use each of the four digits 2, 4, 5, and 7 exactly once. Only one of the these four-digit numbers is a multiple of another one. Which one is it? *(Source: AMC)*

15.23 Compute $55 \cdot 1212 - 15 \cdot 1212$.

15.24 If $2^5 \cdot 8^3 \cdot 16^2 = 4^m$, what is the value of m?

15.25 What is the least natural number, greater than 1, that is a factor of $11000 + 1100 + 11$? *(Source: MATHCOUNTS)*

15.26 How many digits are in the product $8^{12} \cdot 25^8$?

15.27 Find the smallest positive multiple of 1999 that ends in 2006 (last four digits).

15.28 How many ordered triples of three prime numbers exist for which the sum of the members of the triple is 24? *(Source: MATHCOUNTS)*

15.29 What is the largest 4-digit number that is equal to the cube of the sum of its digits?

15.30 Find the value of
$$61^3 - 3 \cdot 61^2 + 3 \cdot 61 - 1.$$

15.31 What is the smallest whole number such that, when divided by each of $10, 9, 8, 7, \ldots, 2$, gives a remainder of $9, 8, 7, 6, \ldots, 1$, respectively? *(Source: MATHCOUNTS)*

15.32 Find the greatest common divisor of 792 and 39654.

15.33 The positive integers A, B, $A - B$, and $A + B$ are all prime numbers. Find the sum of these four primes. *(Source: AMC)*

15.34 In how many different ways can 125 be written as the sum of 3 positive perfect squares if order does not matter and the squares do not need to be distinct?

15.35 What is the value of $\sqrt{(27)(243)}$?

15.36 Find the sum of the total number of digits in each of 2^{2006} and 5^{2006}.

15.37 Find the smallest positive integer that is one less than a multiple of each of 3, 5, 7, 9, and 11.

15.38 Use the digits 2, 4, 5 and 7 each once to create two prime numbers. What is the smallest possible product of two prime numbers created from these digits? *(Source: MATHCOUNTS)*

15.39 Evaluate

$$8008^2 - 7992^2.$$

15.40 What is the sum of all positive two-digit integers for which the sum of the digits is a multiple of 5 and the remainder is 5 when divided by 7? *(Source: MATHCOUNTS)*

15.41 If the integer $152AB1$ is a perfect square, what is the sum of the digits of its square root?

15.42 Evaluate

$$\sqrt[3]{5^{24} + 125^8 + (5^5)^5 + 25^{12}}.$$

15.43 How many positive integers less than 100 leave a remainder of 1 when divided by 2 and also when divided by 3? *(Source: Mandelbrot)*

15.44 The sum of two prime numbers is 20. What is the greatest possible product of these two primes? *(Source: MATHCOUNTS)*

15.45 What is the value of $5^2 - (10)(6) + 6^2$?

15.46 Find the smallest four-digit multiple of 5 that has 2, 4, and 8 among its digits.

15.47 Compute A divided by B where $A = 66666^4$ and $B = 22222^4$.

15.48 Find the prime factorization of $5^8 - 16$.

15.49 What is the remainder when the product of the first 25 prime numbers is divided by 4? *(Source: MATHCOUNTS)*

15.50 If $2^{20} - 2^{19} = 2^x$, what is the value of x?

15.51 There is more than one integer greater than 1 which, when divided by any integer k such that $2 \le k \le 11$, has a remainder of 1. What is the difference between the two smallest such integers? *(Source: AHSME)*

15.52 Find the greatest common divisor of 8008 and 14014.

15.53 Let $D(a, b, c)$ denote the number of multiples of a that are less than c and greater than b. For example, $D(2, 3, 8) = 2$ because there are two multiples of 2 between 3 and 8. What is $D(9^3, 9^4, 9^6)$? *(Source: UNCC)*

15.54 Evaluate

$$53^5 - 5(3)\left(53^4\right) + 10\left(3^2\right)\left(53^3\right) - 10\left(3^3\right)\left(53^2\right) + 5\left(3^4\right)(53) - 3^5.$$

15.55 Perform the following calculation entirely in your head:

$$35^4 - 25^4.$$

15.56 Find positive integers (a, b, c, d) such that

$$a + \cfrac{1}{b + \cfrac{1}{c + \frac{1}{d}}} = \frac{931}{222}.$$

15.57 Calculate

$$1005^3 - 995^3.$$

15.58 Find the value of $\dfrac{2^{2004} + 2^{2001}}{2^{2003} - 2^{2000}}$.

15.59 Perform the following calculation entirely in your head:

$$18^3 + 6 \cdot 18^2 + 12 \cdot 18 + 8.$$

15.60 Given that a and b are natural numbers such that

$$\frac{3}{5} < \frac{a}{b} < \frac{5}{8},$$

find the smallest possible value for b.

15.61 Find the least positive integer n for which $\dfrac{n - 13}{5n + 6}$ is a non-zero reducible fraction. *(Source: AHSME)*

15.62 The numbers from 1 to 2002 are listed in the following order: First all numbers that are not divisible by 3 are listed in (increasing) order. Then all numbers that are divisible by 3 but not by 3^2 are listed in order. Then all numbers that are divisible by 3^2 but not by 3^3 are listed in order, etc. What is the last number in the list? (Give the entire number, not just its last digit.)

Extra! *So comes snow after fire, and even dragons have their ending.* – J.R.R. Tolkien

Extra! **Unsolved Problems**

There are still many problems in number theory that, while they can be stated simply, remain unsolved at the time of the writing of this book. Here are a few of them:

- Are there infinitely many pairs of twin primes? The **twin prime conjecture** states that there are infinitely many pairs of twin primes. While the problem remains unsolved, many mathematicians believe that evidence strongly supports the twin prime conjecture.
- Can every even number greater than 2 be written as a sum of two primes? **Goldbach's conjecture** states that all positive even integers greater than 2 can be expressed as the sum of two primes. At one point, a million dollar prize was offered to anyone who could prove Goldbach's conjecture.
- Are there infinitely many primes that are 1 more than some perfect square?
- Is there a prime number between n^2 and $(n+1)^2$ for every integer n?
- Are there infinitely many primes p such that $2p+1$ is also prime?
- Are there infinitely many Fermat primes?
- Are there any odd perfect numbers?
- Are there infinitely many sets of three consecutive primes that form an arithmetic progression?
- Are there infinitely many primes that are 1 more than the factorial of some natural number?
- Are there infinitely many primes that are 1 less than the factorial of some natural number?

Extra! *I wanted a perfect ending. Now I've learned, the hard way, that some poems don't rhyme, and some stories don't have a clear beginning, middle, and end. Life is about not knowing, having to change, taking the moment and making the best of it, without knowing what's going to happen next. Delicious Ambiguity.* – Gilda Radner

Hints to Selected Problems

1. Don't read random hints!
2. First find the possible modulo 3 residues of squares.
3. Which of both kinds of numbers is largest and which is smallest?
4. What's the units digit of an integer whose cube has a units digit of 3?
5. First think about the general algebraic form of the fraction.
6. Think about the following equation in terms of fractions, repeating decimals, and divisibility rules:
$$\frac{1}{9}\cdot\frac{1}{33\ldots3}=\frac{1}{99\ldots9}\div 3.$$
7. Palindromes with an even number of digits can be broken down into sums of simple palindromic parts. Do these parts share any common divisors?
8. What if the skipped digit were 9 instead of 4?
9. This problem might be easiest if you notice the way in which divisors come in (not necessarily distinct) pairs: $c = ab$.
10. What relationship must the two units digits have modulo 120?
11. Do we really need all those fancy divisibility rules this time? Sometimes crude methods are best.
12. What numbers are 1 more than the numbers you want?
13. Examine the sum with an eye toward algebra.
14. In what ways can we break 9 into a product of divisors? What do those divisors represent?
15. We have worked this problem for $b = 10$ already.
16. The pattern of the coefficients suggests that we sum the equations.
17. We often look to the divisors of every part of a problem to break the problem into steps. How can we make use of the prime factorization of 12?
18. How can we "operate" on a base 8 terminating decimal to produce an integer? How does that operation relate to the fraction?

19. Make it into an algebra problem first.

20. $45^2 = 2025$.

21. It helps to first narrow down the candidates for total numbers of divisors.

22. It's easier to work with integers than fractions, so get rid of the fractions.

23. Odd + odd = even. Odd + even = odd. Even + even = even. How many of the primes are even?

24. This is the kind of problem that might be easier to solve after playing around with the way the problem works for smaller numbers.

25. When you count the number of integers that satisfy each condition, make sure you subtract the intersection from both quantities.

26. $n^3 - n = (n-1)n(n+1)$ is a product of three consecutive integers.

27. Which base 12 digit bundles are multiples of 3?

28. Make Simon proud!

29. Try long divison on strings of 1's until the first two or three parts work out. Maybe you'll see how part (d) will shape up from the simpler examples.

30. $\dfrac{10^{30}}{2^{30}} = 5^{30}$.

31. Put the information together one piece at a time. Which integers are multiples of both 4 and 6? Which of those have a units digit of 2?

32. We can write a factorial in terms of a previous factorial: $(n+1)! = (n+1) \cdot n!$. It's sometimes easier to assign a variable to the value of an integer when the variable is easier to work with.

33. Reverse-engineer the prime factorization.

34. Notice that if friend 2 is wrong, then friends 4, 6, 8, and 10 must also be wrong. Use similar relationships for all the friends to determine which two are wrong.

35. Convert 3443_5 and 3443_6 to base 10 and find their prime factorizations. Convert the factors back to the original bases. Notice anything? If not, keep trying other bases.

36. Find a divisibility rule that helps identify solutions. Compare these palindromes with integers that have half the digits to make counting easier.

37. $1 + 4 = 2 + 3 = 3 + 2 = 4 + 1$

38. Put yourself in the position of each of the students knowing that one of the integers must be 4. What might you see and what would it mean about your own number?

39. We can apply two different divisibility rules to the problem.

40. It's easier to find information about the integer that is 2 less than the answer.

41. It helps to notice that $20^3 = 8{,}000 < 10{,}000 < 27{,}000 = 30^3$.

42. Think about the relationships between the prime factorizations. Why does it matter that m and n are relatively prime?

43. Play around with small cases. If you spot a pattern, think about why it works.

44. $45 = 3^2 \cdot 5^1$.

45. Use an infinite geometric series to help evaluate the fraction.

46. $99 = 9 \cdot 11$.

47. What could the prime factorization look like?

48. What is the nature of the relationship between the number of stamps on each page and the numbers of stamps in each book?

49. Reduce the palindrome modulo 99 using $100 \equiv 1 \pmod{99}$. Which digit needs to be minimized first?

50. Divide the set into a subset for each modulo 7 residue. How does including an element from each subset affect which other numbers can be chosen to create the largest subset?

51. Set it up and solve it algebraically.

52.
$$(100 - x)^2 = 10000 - 200x + x^2.$$
Understanding perfect squares can help you understand square roots—which is the best place to start when testing for primality.

53. Try first expanding the information you have to work with by relating a couple of the known digits as units digits.

54. Relate the words to integers.

55. Relate these integers to base 3 integers.

56. Count the multiples of 5. Count the multiples of 7. How many are both?

57. Express the ratio of factorials as a product of consecutive integers. *How many* consecutive integers?

58. Write out what it means for 101 to be its own modulo m inverse algebraically. What must be true about m?

59. Count the integers you want to exclude.

60. Don't read random hints!

61. Good candidates for total divisors can be broken down into small primes. Do you see why?

62. There are two possible sets of exponents for the prime factorization of such a divisor. Work both cases.

63. How many of the digits in an arrangement of 1, 2, 3, and 4 do we need to look at in order to determine whether or not the resulting integer is a multiple of 4? Examine all those possibilities.

64. Hunt for number theory clues in the algebra.

65. Where else do we see repeating digit structures?

66. Think about the proportions of silver dollars owned by Tom, Dick, and Harry.

67. Knowing the formula for the sum of the first n natural numbers makes this one easier:

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

68. Look for a binary relationship.

69. Think about the ways in which we constructed divisibility rules for 2^m and 5^m in base 10.

70. How many possible remainders are there when you divide by p? How does this relate to the possible length of a block of digits?

71. Think about the modulo 5 residues of the remaining numbers of toothpicks after each of Zhenya's moves. Remember that she wants to leave Ryun with 1 toothpick.

72. When working a problem involving numerous pieces of information, it often helps to focus on the most restrictive piece of information. In this case, the number of divisors of the GCD helps us most.

73. First translate the problem from a word problem to an ordinary number theory problem.

74. Compare the exponents in the prime factorizations of each of the integers.

75. We are dealing with repeating digits. This allows us to apply divisibility rules to the problem. What divisibility rules deal with powers of 3?

76. Since $4 \mid 8$, use what you know about the integer modulo 8.

77. What do we know about the differences between each pair of 69, 90, and 125?

78. Express both the 17-digit number and 3 in terms of powers of 2 that are easy to multiply out.

79. Use what you know about the ways in which digits behave as you count up to determine what you can about any of the digits. Work from that starting point.

80. Compare two general terms. Using variables often helps us solve problems in which we can't simply compare specific numbers.

81. Think it through in modulo 7.

82. Do the math in the parentheses, then write values as digit bundles.

83. Examine the facts that $72 \mid 30N$ and $30 \mid 72N$ individually and combine the results.

84. When you translate the words to math, you should get two congruences, each of which implies the other. Let that be your algebraic starting point.

85. Since $12 = 2^2 \cdot 3^1$, it takes 2 powers of 2 and 1 power of 3 to make each power of 12.

86. Note that $1 + 3 = 4$ and $13 + 31 = 44 = 4(10 + 1)$. What is the sum of the digits of each of the primes you're looking for?

87. If two of the numbers are a and the other is b, their product a^2b is a perfect square. What does that tell us about the value of b?

88. In what modulus do we know specific facts about squares that we can apply to this problem?

89. Find a common ratio for the infinite geometric series by considering the value of r where

$$\frac{1}{998} = \frac{\frac{1}{1000}}{1-r}.$$

90. Don't be afraid of the squared term. If you find the units digit of m^2, you can find the possible units digits of m.

91. There are three systems of linear congruences.

92. Recall that a statement of congruence tells us about the difference between two integers.

93. Use the algebraic value of the number.

94. Translate words to math, then factor what you can. Plug in different numbers of pigs and goats if you need to.

95. Check a few powers of 7 to find a good starting point for calculations.

96. What's the smallest base in which the three two-digit numbers are necessarily distinct digits?

97. What do we know about the prime factorization based on the divisor count?

98. Plug in a few values for n and find the GCD of the results. Then see how far you can go with what you've learned.

99. The only prime divisor of 8 is 2. We already know how to count the powers of a prime in a factorial.

100. Write the number in terms of base b digit bundles. Can you factor this algebraic expression at all?

101. Test each possible product. Which consecutive units digits don't need testing at all?

102. What would Will Nygard do?

103. What do you know about squares modulo 3, 5, and 8?

104. Since the left hand side of the equation isn't particularly easy to work with, try working with the right hand side.

105. Since $\gcd(3, 8) = 1$ and $3 \cdot 8 = 24$, examine $p^2 - 1$ modulo 3 and modulo 8 first.

106. How many of them use *neither*?

107. Let m be a positive integer. What do we know about the divisors of mn that helps us compare $s(mn)$ to $s(n)$?

108. Is the three-digit number larger or smaller than 200? 300? 400? 500? 600? 700? 800? 900? How can we find out?

109. The sum of the digits leaves too many possibilities to work with. Start with the integers congruent to 1 modulo 4.

110. After noting the total divisor counting, check all ways to form the prime factorization of the integer.

111. $120 = 2^3 \cdot 3^1 \cdot 5^1$, which gives us a clue as to which moduli we might use to examine the square.

112. $72 = 2^3 \cdot 3^2$.

113. Relate the odometer to the base 9 number system.

114. Note that $2^{10} = 1024 = 10^3 + 24$. Cube that using $(x + y)^3$.

115. What are all the possible modulo 16 residues of the sum of fourth powers?

116. Assign a variable to represent the diameter. After relating the diameter to the range of areas, focus on the fact that your variable must be an integer.

117. If we ask each Cubs fan how many people they shook hands with, then added all those numbers, what must be true about the sum?

118. Even though there are three integers, we're still looking for maximum exponents.

119. Are there any divisibility rules that use all the digits of an integer regardless of order?

120. Search systematically by starting with the largest possible prime less than 25 and working your way down.

121. Work out the first term. Then work on each term using the previous term.

122. How do the numbers of terminal zeros relate to divisors?

123. Don't read random hints!

124. The base 12 units digit gives us information about n (mod 12). Use that information to determine the modulo 6 residue of n.

125. Express the sum in terms of a single power of 2.

126. Establish a pattern. Can you be sure the pattern continues?

127. What do we know about the integer that is 1 more than the integer we are looking for?

128. Think about how many digits could be selected for each place value keeping in mind that we're counting palindromes.

129. If all else fails, factor!

130. Use what you know about the number modulo 9.

131. Subtract and borrow.

132. Find a way to write both primes using the same variable. What is one more than their product?

133. Given a sequence, hunt for patterns.

134. Use the principles that helped us understand the Euclidean Algorithm.

135. How do the denominators relate?

136. Translate words to math, then factor what you can.

137. Think about the reason why the divisibility rule for 9 works in base 10. There is a number base in which integers are most easily compared to their modulo 99 residues.

138. What do these base 3 numbers look like when you write them out? How does this help you count them?

139. Modulo 100 gives the last two digits with little computation.

140. Systematic casework will help you avoid a misstep.

141. Turn the equation into a quadratic equation.

142. Jayne nearly performs the Sieve of Eratosthenes. What's the difference?

143. Remainders play a big role. Don't expand the factors after multiplying through by 7!.

144. How do powers of 3 and 9 relate? How does this affect the digits we use to write each integer in base 3 versus base 9?

145. Use what you know about perfect squares to identify one of the numbers.

146. Start with $10^3 = 1000$ and go up.

147. First go pattern hunting. How can you be sure a pattern repeats?

148. What number base seems most useful for rewriting these integers?

149. Find a nice way to pair the palindromes to make summing them easier.

150. Systematically work your way through all possible ways to form the prime factorizations.

151. How are r^2 and $(r+50)^2$ related mod 100?

152. First find the repeating block of digits—or even just the repeating remainders from long division.

153. Try smaller binary strings of 1's and look for a pattern.

154. Number the digits with base 3 integers. Which digits remain after each pass?

155. Examine the number modulo 4.

156. What happens if we multiply the given product by $114 \times 113 \times \cdots \times 2 \times 1$?

157. You're reading the wrong hint.

158. Pair the integers in the sum starting from the outside.

159. It might help to notice that $30 = 2 \cdot 3 \cdot 5$. How do these factors relate to 7?

160. After we sum the equations, we have two equal integers. What primes are divisors of either sum?

161. Think about which divisibility rule might apply that requires looking only at the last four digits of an integer.

162. Don't read random hints!

163. For which values of p is the units digit of 2^p equal to 4?

164. Test simple cases.

165. You can still pair the divisors. You just need to adjust for the special property of those divisors.

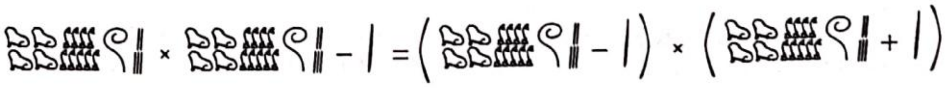
166. Subtract 1 from the number. What all do we know about the difference?

167. Consider the way each fact affects the prime factorization.

168. Examine branches of factor trees. Is the sum getting larger or smaller?

169. What are the units digits of the ten consecutive integers?

170. Start counting them side by start from least to greatest.



Index

the Art of Problem Solving
Introduction to Number Theory

The Art of Problem Solving Introduction Series constitutes a complete curriculum for outstanding math students in grades 6-10. The books in the series are:

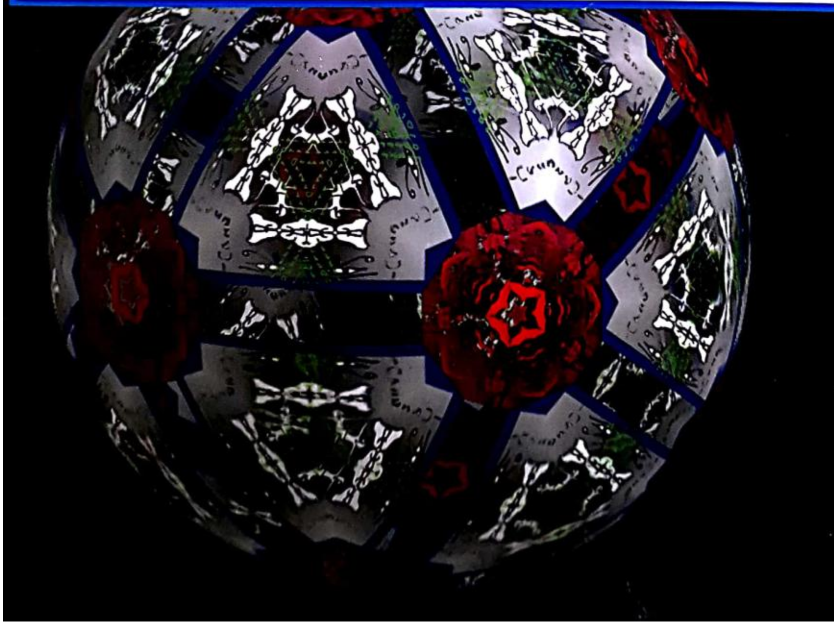
Introduction to Algebra by Richard Rusczyk
Introduction to Counting & Probability by David Patrick
Introduction to Geometry by Richard Rusczyk
Introduction to Number Theory by Mathew Crawford

Together these books give students a solid background in basic problem-solving mathematics and prepare them for prestigious competitions such as MATHCOUNTS and the American Mathematics Competitions.

Praise for **Introduction to Number Theory**

"Thank you so much for Introduction to Number Theory. I have thoroughly enjoyed this book. It has introduced me to math that I would never have discovered on my own...I have learned to not only do problems I thought were impossible, but I have learned to enjoy them."
10th grade student, Alabama

Mathew Crawford is the founder and CEO of MIST Academy, a school for gifted students, in Birmingham, Alabama. He is a former instructor and curriculum developer for the Art of Problem Solving online school. He is co-author of Art of Problem Solving's Intermediate Algebra textbook, and served on the Board of Directors of the Art of Problem Solving Foundation. Crawford was a perfect scorer at the national MATHCOUNTS competition in 1990, and a member of the national championship team (Alabama) in 1991. He was a 3-time invitee to the Math Olympiad Summer Program, a perfect scorer on the AIME, and a 2-time USA Math Olympiad honorable mention.



ISBN 978-1-934124-12-3
90000 >
9 781934 124123