Journey into Discrete Mathematics

Owen Byer, Deirdre L. Smeltzer, Kenneth Wantz

Contents

Preface

What is Discrete Mathematics?

The word *discrete* in mathematics is in contrast to the word *continuous*. For example, the set of integers is discrete, while the set of real numbers is continuous. Thus, *discrete mathematics* describes a collection of branches of mathematics with the common characteristic that they focus on the study of things consisting of separate, irreducible, often finite parts. Although largely neglected in typical pre-college mathematics curricula, discrete mathematics is essential for developing logic and problem-solving abilities. Questions located within the realm of discrete mathematics naturally invite creativity and innovative thinking that go beyond formulas. Furthermore, the cultivation of logical thinking forms a necessary foundation for proof-writing. For these reasons, discrete mathematics is crucial (*do we like this word?*) for undergraduate study of both mathematics and computer science.

Goals of the Book

Simply stated, the goal of *Journey into Discrete Mathematics* is to nurture the development of skills needed to learn and do mathematics. These skills include the ability to read, write, and appreciate a good mathematical proof, as well as a basic fluency with core mathematical topics such as sets, relations and functions, graph theory, and number theory. The content and the corresponding requisite mathematical thinking are appropriate for students in computer science and other problem-solving disciplines, but the content presentation and the nature of the problem sets reinforce the primary goal of training mathematicians. Throughout the book, we emphasize the language of mathematics and the essentials of proof-writing, and we underscore that the process is very important in mathematics.

Entry-level discrete mathematics serves as an excellent gateway to upper-level mathematics by priming students' minds for upper-level concepts. *Journey into Discrete Mathematics* is designed for use in the

first non-calculus course of a mathematics major, employing a writing style that models a high degree of mathematical accuracy while maintaining accessibility for early college students. For example, the treatment of inclusion-exclusion provides both informal and technically precise explanations. Ultimately, the goal behind this approach is communication: we want to model and teach students to communicate both accurately and clearly.

Journey into Discrete Mathematics utilizes problems and examples to lay the foundation for concepts to be encountered in future mathematics courses. For example, the chapter on relations and functions introduces students to definitions such as one-to-one and onto; several problems in Chapter 4 guide students through definitions of continuity using nested quantifiers; the treatment of greatest common divisor foreshadows finding the GCD of polynomial functions; the binomial and multinomial theorems are presented as tools for combinatorial counting; and Euler's totient function and Fermat's Little Theorem are important number theoretic concepts that students will see again in an Abstract Algebra course. The homework questions are divided into sections according to difficulty, spanning the gamut from routine to quite challenging. The first section generally includes exercises that are more routine or computational, meant to give students a chance to practice given techniques, while the latter sections generally consist of problems that require creativity, synthesis of multiple concepts, or proofs.

This book takes the time to describe the origins of important discrete math topics as well as connections between concepts. The treatment of matrices references Arthur Cayley's first use of matrices; the introduction of Fibonacci numbers is placed within historical context; the work on inductive thinking and proof by induction exhibits care for making connections with deductive thinking, the Well-ordering Principle, and other mathematical concepts. Inspirational quotes throughout the book and the incorporation of the first names of mathematicians in examples and exercises (with a corresponding summary page providing a brief biography for each one mentioned) contribute to familiarizing students with the names of key figures within discrete mathematics.

Features of the Book

Convince Me Chapter. This opening chapter contains a selection of interesting, non-standard problems of varying degrees of difficulty. Readers are invited to think creatively and argue persuasively as they work to find solutions. This process cultivates an understanding of the importance of making a good mathematical argument, while setting the tone for the problem-solving nature of the book. Moreover, many of the solutions in this chapter foreshadow the mathematical techniques and theorems that will be encountered later in the book.

Hook Problems. In the manner of the *Convince Me* problems, each chapter begins with an intriguing and challenging problem intended to capture the reader's interest. Each hook problem can be solved using techniques to be developed in the chapter and usually reappears later in the chapter, either as an example or as a homework problem.

Presentation of Logic. Chapters 3 and 4 of the book combine the topics of sets, logic, and proof-writing in a distinctive way. This approach helps to highlight the high level of congruity between concepts such as DeMorgan's Laws for sets and logic, membership tables and truth tables, logical operators and set operators. The chapter on logic and proof-writing appears early in the book to help students bridge the gap between intuitive thinking and the formal presentation of an argument, both of which are necessary in mathematics.

First Thoughts and Further Thoughts. Solutions to many examples in the book are preceded by "First Thoughts," describing the initial thought-process that one might engage in when first considering a new problem. This is intended to be both helpful and reassuring to students who might be intimidated by seeing final polished proofs and assuming that "real" mathematicians can produce these immediately, without any intermediary struggles or failed attempts. First Thoughts help train students in the ways that mathematicians actually operate. Similarly, "Further Thoughts" often follow a solution in order to provide additional insight about, alternative approaches to, or extensions of the given solution; once again, the goal is to cultivate a spirit of *doing mathematics.*

Advanced Topic Chapters. Several core topics (counting, number theory, and graph theory) are addressed twice in this book: first in an introductory chapter covering standard content, and later in a chapter

with extended optional (often, but not always, more advanced) material. This provides instructors with flexibility to customize the course, depending on their particular goals, or expand beyond a typical first course in discrete mathematics.

Course Outline

This book is designed to be used as a stand-alone text for a three-credit or four-credit discrete mathematics course for average to above average math majors who are learning to write proofs; however, since there is more material in this book than can be covered in a single semester, instructors will have to make some choices. For students who have already had an introduction-to-proofs course, select portions of the first six chapters of the book can be covered rather quickly, and the last half of the book can serve as a main text for a junior-level course in combinatorics. If this book is supplemented with a few extra topics (such as probability, solving recurrence relations, or finite-state machines), then there is enough material for a two-semester sequence in discrete mathematics.

With that goal in mind, we suggest one design for such a three-credit course. The second column in Table 1 lists the core sections we believe should be covered. We estimate that the core sections can be covered in about thirty-four 50-minute lectures. The remaining class periods could be used for review days, testing days, and optional sections from the third column. The first column of the table lists sections containing material that is essential for students to know before covering corresponding sections of the middle two columns. The middle columns contain material that is used in sections listed in the fourth column, though they may not be absolute prerequisites. For example, although matrices (first addressed in Section 2.3) also appear in Chapter 9 (Graph Theory), one need not study Section 2.3 in order to be able to understand the essential components of Chapter 9.

TABLE 1. Section priorities and interdependencies

Prerequisites sections for →	Core Sections	Optional Sections	→ Material used
	1.1 – 1.2		
	2.1		
	2.2		Chapters 4, 5, 6, 7,
		2.3	5.1, 5.2, Chapter
	3.1 – 3.6		Chapter 4
		3.7	
2.2, 3.1–3.6	4.1 – 4.2		proofs throughout b
4.2		4.3	
2.2, 3.1–3.6	4.4 – 4.5		proofs throughout b
2.2	5.1		5.2, 5.3, 9.1
2.2	5.2		7.4, 9.1
2.2	5.3		
		5.4	6.1, 6.2 Chapter 1
		6.1, 6.2	
4.2, 5.3	6.3 – 6.4		proofs throughout later
		6.5	
2.2, 6.3	7.1		12.1
2.2, 6.3	7.2		Chapter 12
2.2		7.3	12.4
2.2, 6.3	7.4		
2.2		7.5 – 7.6	12.4
	8.1 – 8.3		Chapters 9 and 11,
	8.4		11.3, 11.4
		8.5	
8.3	9.1		Chapter 10, 13.4
	9.2		
		9.3	13.1, 13.2
	9.4		13.1, 13.2
6.4		9.5	
Chapter 4		10.1 – 10.2	
3.2, 3.4, 3.6, 8.3	11.1		
2.2	11.2		
		11.3	11.5
Chapter 8		11.4	
Chapter 8, 11.3		11.5	
7.1		12.1	
2.2		12.2	
7.4		12.3	
7.3, 12.3		12.4	
7.4, 12.3		12.5	
9.1, 9.4		13.1	
6.4, 9.1, 9.3, 9.4		13.2	
9.1, 9.4		13.3	
9.1, 9.4		13.4	

CHAPTER 1

Convince Me!

Obvious is the most dangerous word in mathematics.
– E.T. Bell (1883–1960)

How did you learn how to ride a bicycle? If you learned as a child, you may have first ridden a tricycle and then a bicycle with training wheels before attempting to balance on a two-wheeler. Although you probably first understood how a bicycle works by watching someone else use one, and perhaps an adult ran along behind with a hand on the back of the bike during your first tentative rides, the primary way in which one becomes an expert bicyclist is through practice.

The same is true of mathematics. You cannot learn to do mathematics simply by watching someone else do mathematics. To become adept, you must be willing to practice, sometimes failing and sometimes succeeding, even if only partially. In this chapter, we encourage you to "dive in" to mathematics by presenting you with problems that are easy to understand and of variable difficulty to solve.

You may already have an idea of what mathematical problems are, but we hope to expand your view. Some of the challenges that we pose in the next section may not even seem like math! A "mathematical problem" isn't necessarily the same as an "exercise"; an exercise is for practicing a known procedure, whereas a problem is something to be solved when the approach may not be obvious.

Improving skill in problem-solving may require learning to recognize patterns, developing theoretical notions, and determining how best to use a variety of mathematical tools and techniques. The particular focus of this book is on solving problems in discrete mathematics — which has some differences from solving problems in, say, calculus. Understanding the language of discrete mathematics, including symbols and definitions, will be necessary for understanding the concepts; just as familiarity with common abbreviations (e.g., "BRB") allows for quick

everyday communication, so the language and symbolism of mathematics will allow for quicker communication of mathematical ideas. In discrete mathematics, this will be the language of sets, logic, functions, enumeration, and graphs, and it will be introduced systematically as needed.

In mathematics, simply knowing how to solve a problem is rarely satisfying. A second important step is to persuade others that your solution is correct. Thus, another invaluable purpose of this book is to develop skills in constructing mathematical proofs. We will demonstrate and discuss a variety of types of proof, illustrating sound methods for convincing others of a correct solution. As with problem-solving, though, the development of proof-writing expertise requires practice, practice, and more practice. Without further ado, let us begin!

1.1. Opening Problems

Although the problems below are quite varied in nature, each one has a solution that does not require high-level mathematics. We urge you to select several of interest to solve. Try to give a convincing argument as to why your solution is correct.

(1) In a game for two players, seventeen coins lie on a table. The players take turns, at each turn removing between one and four coins from the table. The player who takes the last coin loses. If you are going to play this game, ask yourself if you prefer to go first or if you should ask your friend to go first — or does it matter?

As an example, suppose you go first and take four coins (leaving thirteen coins on the table), your friend goes second and takes four coins (leaving nine coins), you then take two coins (leaving seven coins), your friend takes one coin (leaving six coins). Now things look bad for you: you take two coins and your friend wisely removes three more, forcing you to take the last coin and lose the game.

Could you have done something different so that you would have won the game? It might be hard to find a solution immediately. Some may have insight and see the strategy right away, but for most people, finding the solution requires previous experience or lots of experimenting; this is what most mathematicians would

do when faced with this problem.

Additional experimentation should lead you to conjecture that the player who goes first can always win; that is, no matter how the second player plays the game, if the first player follows the proper strategy, she can always win. Give a convincing argument of this conjecture.

(2) Must there be two people in Los Angeles who have the same number of hairs on their heads? You may say that the answer is clearly "yes" since there are surely at least two completely bald people in L.A. Let's agree to disregard the people who are completely bald. Now, what is your answer?

(3) What is the last digit of 3^{1776}? We believe most of you can answer this question by finding a pattern for the last digit of 3^1, 3^2, 3^3, and so on, looking for a pattern. Having done that, what about finding the last *two* digits of 3^{1776}?

(4) Consider a single-elimination tournament, which starts with $n \geq 1$ teams. In the first round, all teams are divided into pairs if n is even, and the winner in each pair passes to the next round (no ties). If n is odd, then one random (lucky) team passes to the next round without playing. The second round proceeds similarly. At the end, only one team is left — the winner. Find a *simple* formula for the total number of games played in the tournament.

(5) Suppose you have access to an unlimited supply of 3-cent and 5-cent stamps. If you need to send an envelope that requires 47 cents, can you create the exact postage using these stamps? What other postage amounts can you pay by using combinations of these stamps? Describe as many as possible.

(6) Can you create a 3×3 rectangular array of numbers (repeat numbers permitted) such that the sum of numbers in every row is 10 and the sum of numbers in every column is 10? Can you do the same for a 3×4 array of numbers?

(7) Which is larger, 3^{400} or 4^{300}?

(8) You are a participant in a game show in which there are three doors to choose between. Behind each door is an amount of money. You

choose a door and are shown the amount behind it. If you wish, you may take the money and the game ends. If you decline, you may choose another door, and see the amount behind that door, but you forfeit the opportunity to accept the amount behind the previous door. You may accept the prize behind the second door; if you decline, then you must take the amount behind the third door, sight unseen. If you play this game optimally, what is the probability that you will win the largest amount of money possible?

(9) Consider a simple game for two players in which the players take turns placing coins on a round table. The coins may not overlap and may not be moved once they are placed. The loser is the first person to be unable to place a coin on the table. Is there a winning strategy? If so, which player has the advantage, the one going first or the one going second?

(10) There are seven cups on a table — all standing upside down. You are allowed to turn over any four of them in one move. Is it possible to eventually have all of the cups right-side-up by repeating this move?

(11) A large chocolate bar is composed of 40 smaller squares in a 5 by 8 grid. How many cuts will it take to cut it into those 40 squares if one must always slice along grid lines and the knife may pass through only one chunk of chocolate per cut (i.e., one cannot line up several previously sliced chunks and cut them simultaneously).

(12) Represent the number 1492 as a sum of two positive integers whose product is the greatest. Next try to maximize the product if you are permitted to use three positive integers. Finally, maximize the product if any number of positive integers is permitted. (It may be helpful to experiment with a much smaller number than 1492.)

(13) A group of persons sits in a circle, each holding an even number of pieces of candy. Each person simultaneously gives half of his or her candy to the person on the right. Any person who ends up with an odd number of pieces of candy selects one piece from a large bowl of candy in the center of the circle, so that once again all persons have an even number of pieces. Show that after enough iterations of this procedure all persons will have the same number of pieces of candy. Is this statement also true if at each iteration each person

gives half of his or her candy to each person to the left and right?

(14) Students in an elementary school classroom are seated in five rows, with each row having six desks. From each row, a tallest student is chosen; then, a shortest of these five students is chosen (call this student A). Now, from each column, a shortest student is chosen; then, a tallest of these six students is chosen (call this student B). Who is taller, A or B? Can they be the same height? Can A and B be the same person?

(15) Given a group of 21 people, show that there are as many ways to select an odd number of them as there are ways to select an even number of them. (Each "way" is determined by the people chosen, not by the number of people chosen. So, choosing Al and Sal counts as a different selection than choosing Hal and Cal.)

(16) Two bright math students, Terence and Srinivasa, each have a number on their forehead. Each can see the number on the other person's forehead, but not the number on his own. They are told that the two numbers are consecutive positive integers. They start the conversion with Terence saying, "I don't know my number." Srinivasa thinks for a moment and replies, "I don't know my number either." They then repeat this exact same conversation, for a total of 53 times, at which point Terence exclaims, "Hey, I just figured out my number!" Srinivasa immediately follows, "Yeah? Me too!" What is the number on Terence's forehead?

(17) Consider a group of 100 prisoners. They are told they will be given a collective chance at a pardon if they can work together to solve the following problem.

At the appointed time all 100 prisoners will come into a large room to gather in a circle. Each prisoner will have a hat placed on his head as he enters, and it will be one of seven colors (Red, Orange, Yellow, Green, Blue, Indigo, or Violet). Each prisoner will be able to see all hats except his own. One at a time, each prisoner will guess out loud the color of his or her own hat. If at most one of the 100 prisoners is incorrect, they will all go free; otherwise they will all be executed. The prisoners can plan a strategy ahead of time, but once they are brought into the room, there will be no communication, other than that each prisoner can hear all of the other guesses. No clues can be given based on eye contact, positioning of the prisoners, timing of responses, etc. What strategy

could the prisoners adopt to best guarantee survival? Under this strategy, what is the probability of survival?

1.2. Solutions

(1) According to the rules of the game, whichever player is faced with only one coin on the table will lose. In fact, once there were only six coins left, and it was your turn, you were bound to lose: if you took n (with $1 \leq n \leq 4$) coins your friend would take $5 - n$ of them, leaving just one coin. Therefore, each player's goal should be to leave his opponent with six coins on his turn.

Arguing backwards from there, if you can leave your opponent with eleven coins, if he takes n of them ($1 \leq n \leq 4$), then you can always take $5 - n$ of them, which will be a number between 1 and 4, as required. Then it will be his turn with six coins remaining. Similarly, whoever's turn it is with sixteen coins remaining will lose if the other player always selects $5-n$ coins immediately after n coins are taken.

In general, if a player is, at any turn, faced with $5k+1$ coins (for any integer k), he will lose if his opponent plays strategically. Therefore, no matter how many coins are initially on the table, the first player can always win if it is possible to use the first turn to remove an appropriate number of coins so that $5k + 1$ coins remain for his opponent for some integer k. If both players follow the proper strategy, the first player will lose only when there there are $5k + 1$ coins on the table at the start of the game for some integer k.

Can you generalize the strategy to the case where initially m coins are placed on the table, and each player may remove between 1 and t coins on his turn?

(2) The population of Los Angeles is about 4 million people. It is possible for them all to have a different number of hairs on their heads only if the human head could have 4 million hairs on it. How many hairs could fit on a human head? Suppose that half of a typical human head is covered with hair. If the

radius of the head is 6 inches, and it is assumed to be spherical, half of the surface area would be $(1/2)4\pi 6^2 = 72\pi < 250$ square inches. How many hairs are there per square inch? Assuming the follicles are 20 per linear inch would give 400 per square inch, and about 100,000 hairs on a human head.[1] This is nowhere near 4 million, so we can safely conclude that it must be the case that two residents of Los Angeles have the same number of hairs on their heads.

(3) The consecutive powers of 3 are 3, 9, 27, 81, 243, 729, etc., so the last digits seem to follow the pattern 3, 9, 7, 1, and then the cycle repeats. Indeed, multiplying each digit in that sequence by 3 gives the next one in the sequence, wrapping around. Every fourth power of 3, therefore, has 1 as its last digit, and since 1776 is divisible by 4, 3^{1776} has 1 as its last digit.

Now, can you figure out what the last two digits of 3^{1776} would be? While the above method works, we will find a faster solution in Chapter 7 that uses properties of modular arithmetic.

(4) As is often the case, this is best approached by way of small cases. Suppose there are only four teams (call them A, B, C, and D) participating in the tournament. In round 1, A competes against B and C competes against D. Assume that A and C are the winners of their respective games; these teams then compete against each other. Regardless of whether A or C wins, the total number of games played will be 3.

Can you easily see how this generalizes? If not, try diagramming the situation for some other values of n. You should see that if there are n teams competing, the number of games played is always $n - 1$. In fact, this is sensible: in each game, exactly one team is eliminated, and all teams but one (the tournament winner) will be eliminated at some point.

(5) There are many ways to obtain 47 cents, including nine 3-cent stamps and four 5-cent stamps. One cannot obtain a total of 7 cents, as can readily be checked. However, $8 = 2(4)$, $9 =$

[1] A quick internet search confirms that this is a reasonable approximation.

3(3), and $10 = 2(5)$. Note that 11, 12, and 13 cent amounts can be obtained by adding one 3-cent stamp to each of the previous configurations, respectively. Similarly one can continue adding 3-cent stamps to these arrangements to obtain any integer amount greater than 13 cents. This idea will be explored more formally in Chapter 6 (Induction).

(6) A 3×3 grid with a 10 in each of the three positions on one of the diagonals and a 0 in all other positions will meet the requirements given.

It is not possible in a 3×4 rectangular array, however. If each column sum is 10, and there are four columns, then the total of all the entries in the array will be 120. On the other hand, if each row sum is 10, and there are three rows, the total of all of the entries in the array will be 90. This is a contradiction, so such a grid is not possible.

(7) Note that $3^{400} = (3^4)^{100}$ and $4^{300} = (4^3)^{100}$. Since $3^4 = 81$ is larger than $4^3 = 64$, we see that $3^{400} > 4^{300}$.

(8) You should pick any door, see the amount behind it, and decline it. Then select another door and compare its value to the first one. If it is higher, keep it. If it is not, take the amount behind the third door. Label the three amounts as Low, Medium, and High, and note there are six corresponding permutations of L, M, and H. You should then verify that the above strategy will enable you to select the largest amount in half of them. Two such orderings are (M, L, H) and (M, H, L). An ordering in which you will not obtain the largest amount is (H, M, L).

(9) The first person can win if she places her coin in the exact center of the table. After that point, she always takes her turn by placing a coin diametrically opposite of the coin placed by the second player. The space will always be available, so she will always be able to move.

(10) Think about the possible numbers of glasses that can be right-side-up at any given time. We will discuss a formal solution to this problem in Chapter 10.

(11) Every time a cut is made, one chunk of chocolate becomes two chunks of chocolate. Thus, no matter which order the pieces are cut, it will take 39 cuts to break the original bar into 40 squares.

(12) The maximum value of ab if $a + b = 1492$ is 746^2, when $a = b = 746$. Of course, one can try other values of a and b in a futile effort to exceed this product, but a short proof will show an improvement is impossible. If $a = 746 - x$ and $b = 746 + x$, then $ab = 746^2 - x^2$. Clearly the product will be maximum when $x = 0$, which means $a = b = 746$.

This solution will generalize to $a = b = n/2$ if 1492 is replaced by n. Of course, if n is not even, you must modify a and b appropriately since we are required to use integers. What does this generalization tell you about how to maximize the product of a set of more than two positive integers whose sum is 1492? Try with three integers whose sum is 10.

(13) Consider what happens to the difference between the greatest and fewest number of candies held by anyone as the rounds progress. A formal approach for solving problems like this will be discussed in Chapter 10.

(14) Certainly, it is possible that A and B may be the same person. For example, this will happen if the students are seated in order of height, with the shortest student in the desk that is in Row 1 and Column 1, the next shortest student in the Row 1, Column 2 spot, and so on, with the tallest student in the desk that's in Row 5, Column 6.

Let $h(A)$ and $h(B)$ be the heights of students A and B, respectively. Then, in the general case, $h(A) \geq h(B)$. To see this, for each i, define t_i to be the height of the tallest student in Row i; then $h(A) = \min\{t_i : 1 \leq i \leq 5\}$. Similarly, define s_j to be the height of the shortest student in column j; then, $h(B) = \max\{s_j : 1 \leq j \leq 6\}$. Clearly, if A and B are in the same row, $h(A) \geq h(B)$. By definition, $h(B) = s_k$ for some k, and B is a shortest student in column k. Likewise, $h(A) = t_l$ for some l, and A is a tallest student in Row l. Let $h(l, k)$ be the height of the student in Row l and Column k. It follows

that $h(A) \geq h(l,k) \geq h(B)$.

(15) If a group of n persons is chosen, then $21-n$ persons remain. Notice that n and $21-n$ have different parities (one must be even and one must be odd). Therefore, for each group with an odd number of persons, there is a corresponding group with an even number of persons, and vice-versa. These two sets of groups are therefore in one-to-one correspondence, so the sets have the same size.

(16) Try the problem with a smaller number of rounds than 53 (say, two rounds). What must Terence's number be if he immediately knew his number after seeing Srinivasa's number? What must it be if he could figure out his number as soon as Srinivasa first acknowledged that he didn't know his own number? We will see this problem again in Chapter 6 where we learn to use induction as a proof technique.

(17) Assign each color a number and have the first person add up all the "numbers" he sees. We will return to this problem when we discuss modular arithmetic in Chapter 7.

Think of an integer between 41 and 59, inclusive. Subtract 25 from your number and write down the resulting 2-digit number. Now subtract 50 from your original number and square the result to form another 2-digit number, using a zero as the first digit if necessary. Append this 2-digit number to the right side of the one you wrote down earlier, forming a 4-digit number. This 4-digit number should be the square of the original number. Why does this work? Can you amend the method to work for numbers outside of the 41-59 range?

CHAPTER 2

Mini Theories

To many, mathematics is a collection of theorems.
For me, mathematics is a collection of examples;
a theorem is a statement about a collection of
examples and the purpose of proving theorems is
to classify and explain the examples...

– John B. Conway (1937 –)

In the first chapter, *Convince Me!*, we gave many examples of convincing arguments in solving mathematical problems. In this chapter we continue our journey into mathematics in a more formal way by exploring several familiar mathematical theories, developing them from the ground up, in order to serve as a microcosm for how mathematical theories are created. By a mathematical theory, we mean a collection of undefined terms, a set of axioms (statements that are accepted as being true), definitions, theorems — all of which relate to a given mathematical topic — and numerous results which can be derived from them. The topics we undertake in this chapter, properties of real numbers, divisibility of integers, and matrices, will likely not be new to the reader. This leaves us free to focus our attention on the importance of definitions and the development of the theories.

2.1. Introduction

We begin with definitions and properties of real numbers that are commonly used in mathematics. The reader should not dismiss the importance of the "elementary" notions given here, as they will be used to build mathematical theory in later sections of the book.

The following notation for sets of numbers is commonly used, other than perhaps $[n]$ to denote the first n natural numbers.

- $\mathbb{N} = \{1, 2, 3, \ldots\}$ is the set of positive integers, also known as the set of **natural** numbers.
- $[n] = \{1, 2, 3, \ldots, n\}$.
- $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ is the set of nonnegative integers, also known as the set of **whole** numbers.
- $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is the set of **integers**.
- $\mathbb{Q}$ is the set of **rational** numbers. Its elements can be represented by fractions $\frac{m}{n}$ or m/n, where $m, n \in \mathbb{Z}$ and $n \neq 0$. Notice that such a representation is not unique:

$$3/5 = (-6)/(-10) = 60/100.$$

  Alternatively, the elements of $\mathbb{Q}$ can be represented by periodic decimals. Such a representation, again, is not unique:

$$\frac{23917}{1000} = 23\frac{917}{1000} = 23.917 = 23.917000\ldots = 23.916999\ldots\ .$$

- $\mathbb{R}$ is the set of all **real** numbers. They can be represented by decimals, both periodic (e.g., $3.\overline{45} = 3.45454545\ldots$) and non-periodic (e.g., $0.101001000100001\ldots$).

Nineteenth century German mathematician Leopold Kronecker (1823–1891) is quoted as saying, "God created the integers; all else is the work of mankind." [**16**] In fact, the above sets of numbers form nested subsets: for example, the natural numbers are contained within the integers, the integers are contained within the rational numbers, and the rational numbers are contained within the real numbers. We will not go through the rigorous process of demonstrating how one constructs the reals from the integers (though it can be done). Rather, while acknowledging that the domain of discourse of discrete mathematics is almost always the integers, we accept that the following basic "laws" apply to all real numbers.

PROPERTY 2.1. *Let $\mathbb{S}$ represent any one of $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$. The following properties hold for all a, b, and c in $\mathbb{S}$.*

1. *Closure: The sum, difference, and product of two numbers in $\mathbb{S}$ is also in $\mathbb{S}$.*
2. *Commutative laws: $a + b = b + a$ and $ab = ba$.*
3. *Associative laws: $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.*
4. *Distributive law: $a(b + c) = ab + ac$.*
5. *Additive and Multiplicative Identities: $0 + a = a$ and $1 \cdot a = a$.*
6. *Additive Inverse: There is an additive inverse in $\mathbb{S}$, denoted $-a$, such that $a + (-a) = 0$.*

(7) *Multiplicative Inverse: If* $\mathbb{S} = \mathbb{Q}$ *or* $\mathbb{S} = \mathbb{R}$ *and* $a \neq 0$*, there is a multiplicative inverse in* $\mathbb{S}$*, denoted* a^{-1}*, such that* $a \cdot a^{-1} = 1$.
(8) *Exponential laws:* $(a^n)^m = a^{nm}$, $(ab)^n = a^n b^n$, *and* $a^n a^m = a^{n+m}$ *for all real numbers* m *and* n.

Notice we did not attempt to prove the above properties. Indeed, the properties seem so basic that one could rightly ask what assumptions would even be permitted when trying to prove them. However, part of the purpose of this chapter is to demonstrate how a mathematical theory is built, and we have the opportunity to do that now. The statements in the following theorem may seem as obvious as the ones just listed, but we will see that each one is actually a consequence of one or more parts of Property 2.1.

THEOREM 2.2.

(1) *For any real number* a*, the additive inverse of* a *is unique.*
(2) *The number* 0 *is the unique additive identity for* $\mathbb{R}$.
(3) *For any real number* $a \neq 0$*, the multiplicative inverse of* a *is unique.*
(4) *The number* 1 *is the unique multiplicative identity for* $\mathbb{R}$.
(5) *For any real number* a, $-(-a) = a$.
(6) *For any real numbers* a *and* b, $-(a + b) = (-a) + (-b)$.
(7) *For any real number* a, $a \cdot 0 = 0$.
(8) *For any real number* a, $-1 \cdot a = -a$.
(9) *For any real numbers* a *and* b, $(-a)(-b) = ab$.
(10) *For any real number* a*, if* $a \neq 0$ *and* $ab = ac$*, then* $b = c$.
(11) *Zero product property: For any real numbers* a *and* b*, if* $ab = 0$*, then* $a = 0$ *or* $b = 0$.

Proof. We provide a guided proof of each property. In each proof there are a series of "Why?" questions. In lieu of completing a problem set for this section, the reader should supply a reason (usually a property from Property 2.1 or from an already proven part of this theorem) that justifies each statement in the proof preceding a "Why?" query.

(1) To prove the uniqueness of the inverse, assume that b and c are both additive inverses of a. Then

$$\begin{aligned} b &= b + 0 && \text{(a. Why?)} \\ &= b + (a + c) && \text{(b. Why?)} \\ &= (b + a) + c && \text{(c. Why?)} \\ &= 0 + c && \text{(d. Why?)} \\ &= c. && \text{(e. Why?)} \end{aligned}$$

Therefore, $b = c$, and a has a unique additive inverse.

(2) To show that there is only one additive identity, we let e be an additive identity and prove $e = 0$. If e is an additive identity, then $e + a = a$ for all a (a. Why?). Then for any given a, $e + a + (-a) = 0$ (b. Why?) It follows that $e + (a + (-a)) = 0$ (c. Why?) Therefore, $e + 0 = 0$, so $e = 0$ (d. Why?). Thus, 0 is the unique additive identity.

(3) To prove uniqueness, assume that b and c are both multiplicative inverses of a. Then $ab = ac = 1$ (a. Why?) and $ab = ba$ (b. Why?). It follows that

$$\begin{aligned} b &= b(1) && \text{(c. Why?)} \\ &= b(aa^{-1}) && \text{(d. Why?)} \\ &= (ba)(a^{-1}) && \text{(e. Why?)} \\ &= (ba)(c) && \text{(f. Why?)} \\ &= 1 \cdot c = c. && \text{(g. Why?)} \end{aligned}$$

Thus, $b = c$ and the multiplicative inverse of a is unique.

(4) Assume that e is a multiplicative identity and let a be any nonzero number. Then a has a multiplicative inverse, a^{-1}. It follows that

$$\begin{aligned} e &= e \cdot 1 && \text{(a. Why?)} \\ &= e(a \cdot a^{-1}) && \text{(b. Why?)} \\ &= (e \cdot a)a^{-1} && \text{(c. Why?)} \\ &= a \cdot a^{-1} && \text{(d. Why?)} \\ &= 1. && \text{(e. Why?)} \end{aligned}$$

This proves 1 is the unique multiplicative identity.

(5) $-a$ has a unique additive inverse (a. Why?), denoted $-(-a)$, and $-(-a) + -a = 0$ (b. Why?). On the other hand $a + (-a) = 0$ (c. Why?). Therefore $-(-a)$ and a are both additive inverses of $-a$. This proves that $-(-a) = a$ (d. Why?).

(6) It suffices to show that $(-a) + (-b)$ is an additive inverse of $a + b$ (a. Why?) Indeed, $(a + b) + ((-a) + (-b)) = (a + (-a)) + (b + (-b))$ (b. Why?). This sum is 0 (c. Why?), which proves that $(-a) + (-b)$ is an inverse of $a + b$ (d. Why?).

(7) $a \cdot 0 = a(0 + 0)$ (a. Why?), which equals $a \cdot 0 + a \cdot 0$ (b. Why?). By adding $-(a \cdot 0)$ to both sides of $a \cdot 0 = a \cdot 0 + a \cdot 0$, we obtain $0 = a \cdot 0$ (c. Why?).

(8) It suffices to prove that $-1 \cdot a$ is the additive inverse of a (a. Why?). We have $a + (-1 \cdot a) = 1 \cdot a + (-1) \cdot a$ (b. Why?),

which equals $(1 + (-1)) \cdot a$ (c. Why?). This value is $0 \cdot a = 0$ (d. Why?), which proves that $-1 \cdot a$ is the additive inverse of a (e. Why?).

(9)

$$\begin{aligned}(-a)(-b) &= (-1 \cdot a)(-1 \cdot b) && \text{(a. Why?)}\\ &= (-1)(a)(-1)(b) && \text{(b. Why?)}\\ &= (-1)(-1)(a)(b) && \text{(c. Why?)}\\ &= -(-1)(ab) && \text{(d. Why?)}\\ &= 1(ab) = ab. && \text{(e. Why?)}\end{aligned}$$

(10) Since $a \neq 0$, a has a real-valued multiplicative inverse, a^{-1}. By assumption, $ab = ac$; thus, $a^{-1}(ab) = a^{-1}(ac)$, and therefore $(a^{-1}a)b = (a^{-1}a)c$ (a. Why?). It follows that $1 \cdot b = 1 \cdot c$ (b. Why?), so $b = c$ (c. Why?).

(11) If $b = 0$, we are done. If $b \neq 0$, then b has a real-valued multiplicative inverse, b^{-1}. Then

$$\begin{aligned}a &= a \cdot 1 && \text{(a. Why?)}\\ &= a(bb^{-1}) && \text{(b. Why?)}\\ &= (ab)(b^{-1}) && \text{(c. Why?)}\\ &= 0 \cdot b^{-1} = 0. && \text{(d. Why?)}\end{aligned}$$

Thus, either $a = 0$ or $b = 0$, which completes the proof. □

We close the section with discussion of two commonly used functions in discrete mathematics. For any x, the **absolute value** of x, denoted $|x|$, is defined as

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}.$$

For example, $|5| = 5$, $|0| = 0$, and $|-7| = -(-7) = 7$. Note that $|x|$ can be viewed as the distance on the real number line from the number x to the origin, 0. Clearly, for any a, $-|a| \leq |a|$, and for any real numbers a and b, $|a| \leq |b|$ if and only if $-|b| \leq a \leq |b|$. Furthermore, the distance on the real number line between a and b is $|a-b| = |b-a|$. (See Figure 1.)

This background provides us with two additional properties. Each one follows from the definition of operations on real numbers, by considering various cases for a and b.

THEOREM 2.3.

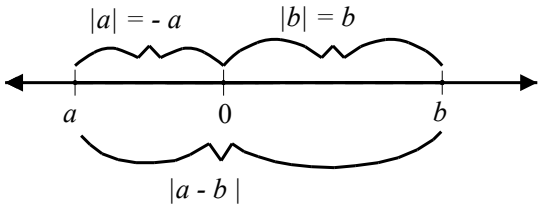

FIGURE 1

(1) Absolute Value Product: $|ab| = |a||b|$.
(2) Triangle Inequality: $|a + b| \leq |a| + |b|$.

While real numbers are the dominant domain of discourse in many areas of mathematics, most questions in discrete mathematics yield integral answers. In some cases, a real number must be rounded (up or down) to obtain an integer. The **floor function** of a real number x gives the largest integer less than or equal to x; it is denoted $\lfloor x \rfloor$. Therefore,

$$\lfloor 2.9 \rfloor = 2, \ \lfloor \pi \rfloor = 3, \ \lfloor -4.2 \rfloor = -5, \text{ and } \lfloor 6 \rfloor = 6.$$

Notice that, if $x > 0$, $\lfloor x \rfloor$ can be obtained by truncating the decimal part of x or by rounding down to the nearest integer. If $x < 0$, truncating does not produce an integer less than x; the floor of a negative non-integer is one less than the truncation of x.

As an application, consider the problem of finding the number of multiples of seven that lie between 1 and 100. One could list the successive multiples of seven and then count them, but a moment of reflection should lead to the answer of $\left\lfloor \frac{100}{7} \right\rfloor = \lfloor 14.29 \rfloor = 14$.

The "round up" counterpart to the floor function is the **ceiling function**, which will be explored in the exercises.

2.2. Divisibility of Integers

As we noted in Section 2.1, integers are featured prominently in any discrete math book. In fact, for the remainder of this book, unless otherwise stated,

letters $a, b, c, \ldots$ will be used to represent integers.

We begin our discussion about integers with a simple statement:

The sum of two even integers is an even integer.

Undoubtedly, the reader can distinguish between even and odd integers and is quite certain that this statement is true. How would one prove it though, based on a definition of even? Many people would define even integers as those ending in 0, 2, 4, 6, or 8. With this definition, proving that the sum of two even integers is even would require considering all possible pairs of numbers ending in the digits 0, 2, 4, 6, or 8 and demonstrating that in all cases, the sum also ends in 0, 2, 4, 6, or 8. While such a proof is valid, it is quite tedious and would not be the method of choice of most mathematicians.

Rather, a mathematician would prefer to define a number n to be **even** if it can be written as the product of 2 and some integer. Seeing that the integers that satisfy this definition must be those that end in 0, 2, 4, 6, or 8 is not difficult; at the same time, this definition will be far more useful in proofs. To wit, here is a proof that the sum of any two even integers is an even integer.

Proof. Let m and n be any two even integers. Then, by definition, $n = 2j$ and $m = 2k$ for some integers j and k, in which case $n + m = 2j + 2k = 2(j + k)$. Since $j + k$ is an integer (by the closure property) we have demonstrated that the sum of n and m can be written as the product of 2 and some integer. Therefore $n + m$ is even. □

Hopefully the above example underscores that a good definition must be both accurate and useful. This definition of "even" is actually a special case within the broader notion of divisibility.

For two integers a and b, $b \neq 0$, if there exists an integer q such that $a = bq$, then we say that b **divides** a or a is **divisible** by b, and denote this relationship by writing $b|a$. If $a = bq$, then a is called a **multiple** of b, b is called a **divisor** of a, and q is called the **quotient** of the division of a by b. For example, $5|(-15)$ since $-15 = 5 \cdot (-3)$, 2 is a divisor of 20 since $20 = 2 \cdot 10$, and 0 is a multiple of 5 since $0 = 5 \cdot 0$.

Our use of "the" when referring to "the quotient" above is justified by the fact that if such q exists, then it is unique. To see this, note that if $a = bq_1 = bq_2$ for some q_1 and q_2, then $b(q_1 - q_2) = 0$. Since we have assumed $b \neq 0$, then by the zero product property, $q_1 - q_2 = 0$. This proves that $q_1 = q_2$, so the quotient is unique.

Why do we need to restrict b from being zero when we say $b \mid a$? The reason is the following. The equality $a = 0 \cdot q$ implies $a = 0$; therefore the only number a which seems to allow division by zero is 0 itself. But $0 = 0 \cdot q$ is correct for every q, which means that the quotient of the division of 0 by 0 could be any number. This proves to be too inconvenient when properties of integers (as well as rational or real numbers) are discussed, and therefore the division by zero is not defined at all.

We defined an even integer to be an integer divisible by 2; i.e., n is even if $n = 2k$ for some integer k. In a similar manner, we define an integer n to be **odd** if $n = 2j + 1$ for some integer j. It may seem obvious that no integer can be both even and odd; in a Section 4.5 exercise, you are asked to prove this.

Though not as elementary as "even" and "odd," the concept of a prime number is also familiar, but one which we wish to define formally here. A positive integer $p \neq 1$ is called a **prime number**, or **prime**, if it is divisible only by ± 1 and $\pm p$. The first nine primes are 2, 3, 5, 7, 11, 13, 17, 19, and 23. The number 2 is the only even prime; more generally, a prime number p is the only prime divisible by p. A positive integer with more than two positive divisors is called a **composite number**, or **composite**. The integer 1 is therefore the only positive integer that is neither prime nor composite.

The first result of the following theorem has already been proven. Proofs of the remaining parts of the theorem are asked for in upcoming problem sets.

THEOREM 2.4.

(1) The sum of any two even integers is an even integer.
(2) The sum of any two odd integers is an even integer.
(3) The sum of an even integer and an odd integer is an odd integer.
(4) The product of two odd integers is an odd integer.
(5) The product of an even integer and any other integer is an even integer.

Part (1) of Theorem 2.4 is the specific case with $c = 2$ in part (3) of Theorem 2.5, which lists several important properties related to the division of integers. Though most of these properties may look familiar or seem obvious—and we are no doubt being redundant in saying this—mathematical rigor includes being able to prove such statements.

Short proofs like these are important for learning to apply definitions, and they help build mathematical understanding. The reader should study them thoroughly.

THEOREM 2.5. *For all integers a, b, c, x, and y,*

(1) if $b \mid a$, then $b \mid ca$;
(2) if $c \mid b$ and $b \mid a$, then $c \mid a$;
(3) if $c \mid a$ and $c \mid b$, then $c|(a + b)$ and $c|(a - b)$;
(4) if $c \mid a$ and $c \mid b$, then $c|(xa + yb)$;
(5) if $a \neq 0$, then a and $-a$ are divisors of a;
(6) 1 and -1 are divisors of a;
(7) if $b \mid a$ and $a \neq 0$, then $|b| \leq |a|$; and
(8) a nonzero number has a finite number of divisors, whereas zero is divisible by any nonzero number.

Remark. At this point in the book, we have not provided the reader with the tools for proving statements such as those in Theorem 2.5. Therefore, we encourage reading through the proofs below to gain as much understanding and insight as possible without undue concern for the formal structure. Proof techniques will be addressed in a formal manner in Section 4.5. ◇

Proof.

(1) We need to show that $b \mid ca$, i.e., that there exists an integer q such that $ca = bq$. If $b \mid a$, then $a = bq_1$ for some integer q_1. Then $ca = c(bq_1) = b(cq_1)$. Since cq_1 is an integer by closure, setting $q = cq_1$, we obtain that $b \mid ca$.
(2) We have to show that $c \mid a$, i.e., that there exists an integer q such that $a = cq$. If $c \mid b$ and $b \mid a$, then $b = cq_1$ and $a = bq_2$ for some integers q_1 and q_2. Then $a = bq_2 = (cq_1)q_2 = c(q_1q_2)$. Setting q equal to the integer q_1q_2, we find $a = qc$, which completes the proof.
(3) We prove the statement for $a+b$, as the proof for $a-b$ is nearly identical. We have to show that $c|(a+b)$, i.e., that there exists an integer q such that $a + b = cq$. Since $c \mid a$ and $c \mid b$, there are integers q_1 and q_2 such that $a = cq_1$ and $b = cq_2$. Then $a+b = cq_1+cq_2 = c(q_1+q_2)$. Since q_1+q_2 is an integer, setting $q = q_1 + q_2$, we obtain $a + b = cq$.
(4) Before we start our proof, we point out that this statement is a generalization of the previous one. Indeed, taking $x = y = 1$, we obtain $c|(a+b)$, and taking $x = 1, y = -1$, we get $c|(a-b)$.

We present two proofs of (4), one based on (3) and (1) and another that is independent of this theorem.

Proof 1. Since $c \mid a$ and $c \mid b$, from (1) we see that $c \mid xa$ and $c \mid yb$. It then follows from (3) that $c|(xa + yb)$.

Proof 2. We have to show that $c|(xa + yb)$, i.e., that there exists an integer q such that $xa + yb = qc$. Since $c \mid a$ and $c \mid b$, there are integers q_1, q_2 such that $a = cq_1$ and $b = cq_2$. Then $xa + yb = x(cq_1) + y(cq_2) = c(xq_1 + yq_2)$. Since $xq_1 + yq_2$ is an integer, setting $q = xq_1 + yq_2$ shows that $xa + yb = cq$.

Further Thoughts. Since (4) implies (3), and the second proof of (4) is independent of (3), one might ask why we bothered to prove (3) at all. The answer is two-fold. First, development of a mathematical theory most often follows an "inductive" path, i.e., a generalization from particular cases to a general conclusion. On the other hand, having (3) proven enabled us to construct the first proof of (4). ◇

(5) Since $a = a \cdot 1$ and $-a = a(-1)$, the statement follows. (Both 1 and -1 are integers.)
(6) Since for every integer a, $a = 1 \cdot a = (-1) \cdot (-a)$, the statement follows.
(7) By definition, $b \mid a$ implies that $a = bq$ for some integer q, and therefore $|a| = |b||q|$. Since $a \neq 0$, $q \neq 0$, and therefore $|q| \geq 1$. Hence $|a| = |b||q| \geq |b|$, giving $|b| \leq |a|$.
(8) If $b \mid a$ and $a \neq 0$, then (7) gives $|b| \leq |a|$. Thus b is an integer in the set $\{-a, -a + 1, \ldots, -1, 1, \ldots, a - 1, a\}$. Therefore a nonzero integer a has at most $2|a|$ divisors, and this proves the first statement. The second statement is obvious, since $0 = b \cdot 0$ for any b. □

Regardless of how basic the statements of Theorem 2.5 appear, in the right hands they become powerful tools, which can be used to establish many interesting and not-so-obvious facts about integers. This is not always easy and several attempts are often needed to find (and write) a valid proof. Below we give several examples of simple applications. We assume that the integers are represented in base ten, so the term "digit" refers to an integer 0 through 9.

Example 1. Take a 2-digit integer, switch the digits, and subtract the obtained number from the original one. Prove that the difference will always be divisible by 9.

First Thoughts. If your initial reaction is one of disbelief, you should experiment. Two examples include $83 - 38 = 45$ and $75 - 57 = 18$; both 45 and 18 are divisible by 9. The statement seems to be true, though the examples may not give an indication of why. We should consider a general way to represent an integer in terms of its digits. In the base-10 system, the number 83, with digits 8 and 3, can be represented as $83 = 8(10) + 3$. We can generalize this representation to any 2-digit number. ◇

Solution. Let N be an arbitrary 2-digit number. Then $N = 10a + b$ for some digits a and b. After the digits are reversed, we obtain a number $M = 10b + a$. Then $N - M = (10a + b) - (10b + a) = 9a - 9b = 9(a - b)$. Since $a - b$ is an integer, $9|(N - M)$, so the proof is complete. □

The following problem is similar to Problem 5 in Chapter 1.

EXAMPLE 2. Is it possible to pay an exact total of \$100,674 when buying only \$12 items and \$32 items?

First Thoughts. In general, if you have no idea how to begin to answer a question, it is a good idea to try either a simpler or slightly different problem, and such an approach could be helpful for here. For example, would it be possible to pay an exact total of \$100,673 when buying only \$12 items and \$32 items? Hopefully, you will recognize that if one only buys items whose individual costs are even, an odd total like \$100,673 cannot be obtained. What insight can that give to the original problem, though, since 100,674 is even? A slight rephrasing will help: if one only buys items whose costs are divisible by $k = 2$, then a total that is not divisible by $k = 2$ cannot be obtained. But the same statement is true if k is replaced by any integer! Now, can you find an appropriate value of k to help with the given problem? ◇

Solution. The answer is "No." To show this we assume the contrary, and let integers x and y represent the number of \$12 items and \$32, respectively. Then the total price is $12x + 32y = \$100,674$. Since $4|12$ and $4|32$, then $4|(12x + 32y) = \$100,674$ (according to Theorem 2.5 (4)). But 4 does not divide 100,674 (check it!). This contradiction proves that a total of \$100,674 cannot be obtained.

The following theorem, known by several names, is used by middle school students and number theorists alike. It simply says that integers can be divided to give a unique quotient and remainder.

THEOREM 2.6. *(**Division Theorem** or **Division with Remainder Theorem** or **Division Algorithm**.) For any two integers a and b, $b \neq 0$, there exists a unique pair of integers q and r, $0 \leq r < |b|$, such that $a = qb + r$.*

Here, we give some examples; a proof of the theorem will be given in Section 6.5, where the method of mathematical induction is used.

(1) If $a = 20$ and $b = 6$, then $q = 3$ and $r = 2$, since $20 = 3 \cdot 6 + 2$ and $0 \leq 2 < 6$.
(2) If $a = -20$ and $b = 6$, then $q = -4$ and $r = 4$, since $-20 = (-4) \cdot 6 + 4$ and $0 \leq 4 < 6$. (Notice that $q = -3$ and $r = -2$ do not meet the conditions of the theorem, since $r < 0$.)
(3) If $a = 20$ and $b = -6$, then $q = -3$ and $r = 2$, since $20 = (-3)(-6) + 2$ and $0 \leq 2 < 6$.
(4) If $a = 0$ and $b = 7$, then $q = r = 0$, since $0 = 0 \cdot 7 + 0$ and $0 \leq 0 < 7$.

If $a = qb + r$ and $0 \leq r < |b|$, then we will continue calling q the **quotient** upon dividing a by b and will refer to r as the **remainder** upon dividing a by b. Another way of denoting the relationships between a and b is with modular arithmetic and congruences. These will be explored more fully in Chapter 7, but for now we simply write a div $b = q$ and a mod $b = r$ to denote that q is the quotient and r is the remainder in the Division Theorem when a is divided by b. This notation is commonly used when writing pseudocode for programs or algorithms. In the above examples, we have

(1) 20 div $6 = 3$ and 20 mod $6 = 2$;
(2) -20 div $6 = -4$ and -20 mod $6 = 4$; and
(3) 20 div $(-6) = -3$ and 20 mod $(-6) = 2$;
(4) 0 div $7 = 0$ and 0 mod $7 = 0$.

The quotient and remainder upon the division of a by b can be obtained from the floor function. If $b > 0$, then $q = \left\lfloor \frac{a}{b} \right\rfloor$, and solving for r yields $r = a - b \cdot \left\lfloor \frac{a}{b} \right\rfloor$. If $b < 0$, perform the division with $|b|$ and negate the resulting quotient; in symbols, $q = -\left\lfloor -\frac{a}{b} \right\rfloor$ for $b < 0$. In particular, notice that $(-a)$ div b and a div $(-b)$ need not have the same value.

EXAMPLE 3. If $a = 5k + 2$, then when a is divided by 5, k is the quotient and 2 is the remainder. However, if $a = 5k + (-2)$, then we should not conclude that the quotient is k and the remainder is -2, because the remainder must satisfy $0 \leq r < 5$. Rather, we must rewrite to obtain a non-negative remainder. We find that $a = 5(k-1) + 3$, so the

quotient is $k-1$ and the remainder is 3.

EXAMPLE 4. Every integer n can be written in one and only one of the four forms, $4k$, $4k+1$, $4k+2$, or $4k+3$, where k is an integer. This fact follows from the Division Theorem — just divide the dividend n by $b=4$ and note that only four remainders are possible.

The next two examples demonstrate less obvious applications of Theorem 2.6. In each case, we use the Division Theorem to rewrite the general variable n in terms of the given divisor and appropriate remainder.

EXAMPLE 5. Suppose that $n \bmod 8 = 5$. What is the remainder of the division of n^3+5n by 8?

Solution. By the Division Theorem, $n = 8k+5$, for some integer k. Then

$$\begin{aligned} n^3+5n &= (8k+5)^3+5(8k+5) \\ &= 8^3k^3+3(8^2k^2)5+3(8k)5^2+5^3+5(8k)+5^2 \\ &= 8(8^2k^3+3(8k^2)5+3k5^2+5k)+150 \\ &= 8(8^2k^3+3(8k^2)5+3k5^2+5k+18)+6. \end{aligned}$$

Thus (by the Division Theorem again), $n^3+5n = 8q+6$, where $q = 8^2k^3+3(8k^2)5+3k5^2+5k+18$. Therefore, the remainder when n^3+5n is divided by 8 is 6; i.e., $(n^3+5n) \bmod 8 = 6$.

EXAMPLE 6. Prove that $M = n(n+1)(2n+1)$ is divisible by 6 for all integers n.

Proof. For any n, by the Division Theorem, $n = 6k+r$, where k is an integer and r is an element of the set $\{0,1,2,3,4,5\}$. Let us evaluate M for each possible value of r.

(1) If $r=0$, then $M = 6k(6k+1)(12k+1)$.
(2) If $r=1$, then
$M = (6k+1)(6k+2)(12k+3) = 6(6k+1)(3k+1)(4k+1)$.
(3) If $r=2$, then
$M = (6k+2)(6k+3)(12k+5) = 6(3k+1)(2k+1)(12k+5)$.
(4) If $r=3$, then
$M = (6k+3)(6k+4)(12k+7) = 6(2k+1)(3k+2)(12k+7)$.
(5) If $r=4$, then
$M = (6k+4)(6k+5)(12k+9) = 6(3k+2)(6k+5)(4k+3)$.

(6) If $r = 5$, then
$M = (6k+5)(6k+6)(12k+11) = 6(6k+5)(k+1)(12k+11)$.

As we see, in each of the cases $6|M$, and the proof is complete. □

The previous example shows that by concentrating on the remainders one can reduce a problem of establishing a property of *infinitely* many integers to a problem of verifying the property for a *finite* number of cases. The importance of this idea is hard to overstate, and we will return to it when we study congruence relations in Chapter 7.

For our final example, we return to the problem given at the beginning of the chapter.

EXAMPLE 7. Think of an integer between 41 and 59, inclusive. Subtract 25 from your number and write down the resulting 2-digit number. Now subtract 50 from your original number and and square the result. Append this value to the one you wrote down earlier, forming a 4-digit number. Verify that this 4-digit number is the square of the original number, and prove that it happens in the general case as well.

First Thoughts. In problems like this, where we wish to find a general solution, it is imperative that we find a convenient way to represent the general number. In this case, if the first and second digits of our number are a and b, respectively, the form (ab) is not very helpful, because it cannot be manipulated algebraically. Before reading on, think for a moment how a (the tens digit) and b (the units digit) can be formed into an algebraic expression equalling the given 2-digit number. ◇

Solution. If a and b are the tens and ones digits, respectively, then from the Division Theorem, our 2-digit number can be expressed as $10a + b$. Then, according to the method, $10a + b - 25$ will be the first two digits of the square of the original number, while $(50 - (10a + b))^2$ will form the last two digits. Thus, if the method works, the square of our number will have $10a + b - 25$ hundreds and $(50 - (10a + b))^2$ ones. Algebraically, we have thus reduced the problem to showing that $(10a+b)^2$ and $100(10a+b-25)+(50-(10a+b))^2$ are equal. We leave it to the reader to use the algebraic rules of Property 2.1 to show this is the case. □

Exercises and Problems

(1) Compute the following floor function values

(a) $\lfloor \pi/2 \rfloor$
(b) $\lfloor -\pi/2 \rfloor$
(c) $\left\lfloor \frac{1+\sqrt{5}}{2} \right\rfloor$
(d) $\lfloor -\sqrt{10} \rfloor$
(e) $\lfloor 0 \rfloor$

(2) Suppose $n \in \mathbb{N}$. Prove that $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n}{2}$ when n is even and $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n-1}{2}$ when n is odd.

(3) The **ceiling function** of a real number x returns the smallest integer greater than or equal to x; it is denoted $\lceil x \rceil$. For instance, $\lceil 9.25 \rceil = 10$ and $\lceil -4.6 \rceil = -4$. Compute the following ceiling function values.
(a) $\lceil \pi/2 \rceil$
(b) $\lceil -\pi/2 \rceil$
(c) $\left\lceil \frac{1+\sqrt{5}}{2} \right\rceil$
(d) $\lceil -\sqrt{10} \rceil$
(e) $\lceil 0 \rceil$

(4) Use Exercise 2 as a guide for determining $\left\lceil \frac{n}{2} \right\rceil$ when n is even and $\left\lceil \frac{n}{2} \right\rceil$ when n is odd.

(5) For each given value of a and b, find the appropriate values of q and r according to the Division Theorem.
(a) $a = 30$ and $b = 7$.
(b) $a = -30$ and $b = 7$
(c) $a = -30$ and $b = -7$.
(d) $a = 120$ and $b = 8$.
(e) $a = -120$ and $b = 8$.

(6) Find a div b and a mod b for each problem below. In which cases does $b|a$?
(a) $a = 91$, $b = 7$
(b) $a = 344$, $b = 6$
(c) $a = -253$, $b = 11$
(d) $a = 162$, $b = -21$
(e) $a = 0$, $b = 10$

(7) How can one denote that an integer k is even using mod notation? Similarly, how can one denote that an integer j is odd?

(8) (a) Is 0 even, odd, or neither? Explain your answer.
(b) The hypotheses of the Division Theorem require that the divisor b is not 0. Which conclusion(s) of the Division Theorem fail to be true in the event that $b = 0$?

(9) Prove that the sum of two odd integers must be an even integer.

(10) Show that if $a|b$ and $b|a$, then $a = b$ or $a = -b$.

---

(11) Is the **converse**[1] of the statement in Problem 10 correct? Namely, if $a = b$ or $a = -b$, then must it follow that $a|b$ and $b|a$? Explain your answer.

(12) Construct the converse statements to Theorem 2.5 (1) and (7). Can you find a counterexample for each?

(13) For each of the following equations, determine the subset of real numbers for which it is true.
   (a) $\lfloor x \rfloor = -\lfloor -x \rfloor$
   (b) $\lfloor x + 1 \rfloor = \lfloor x \rfloor + 1$
   (c) $\lfloor x \rfloor = \lceil x \rceil$
   (d) $\lfloor x \rfloor + 1 = \lceil x \rceil$

(14) Prove that the only common positive divisor of two consecutive integers is 1.

(15) Prove that the sum of any four consecutive integers is an even number.

(16) In each case below, determine whether or not there are integers x and y satisfying the given equation.
   (a) $16x + 10y = -22$.
   (b) $24x - 54y = 28{,}010$.

(17) Devise an efficient (as few strokes as possible) method for which you can use a calculator to determine the quotient and remainder when a is divided by b (useful when a is a large integer, but not so large that it cannot be entered in a calculator). For example, suppose $a = 23,920,534,206$ and $b = 172$.

(18) Prove that the product of
   (a) three consecutive integers is always divisible by 3;
   (b) five consecutive integers is always divisible by 5;
   (c) Generalize the statements (a) and (b). Can you prove your generalization?

(19) Suppose that $n \bmod 9 = 5$. What is $n(n^2 + 7n - 2) \bmod 9$?

(20) Prove that the difference of squares of two consecutive odd integers is always divisible by 8.

(21) Show that a square of an integer cannot give the remainder 2 when divided by 3; i.e., $n^2 \neq 3k + 2$ for any integers n, k.

(22) Modify the technique given in Example 7 to work for integers other than those in the 41 to 59 range.

---

[1] See Section 4.1 for more discussion about the converse.

(23) Explain why the following fast method of squaring integers ending with digit 5 works. Let $N = (a5)$ where a is the number formed by all the digits of N but 5. Then N^2 can be obtained by multiplying a by $a+1$ and attaching 25 at the end of the product.

For example: $35^2 = 1{,}225$ can be computed by multiplying $a = 3$ by $a+1 = 4$ and attaching 25 to 12. Similarly, $235^2 = 55{,}225$ can be found by computing the product $23 \cdot 24 = 552$ and attaching 25.

(24) Prove that in a right triangle with integer side lengths, the length of at least one leg must be divisible by 3.

(25) Under what conditions will the sum of n consecutive integers be divisible by n? (For example, the number $16+17+18+19+20+21+22 = 133$ is divisible by 7.) Can you prove your answer?

(26) Prove that in a right triangle with integer side lengths, the length of at least one side must be divisible by 5.

(27) Prove that at least one of the last two digits of a square of an integer is even.

2.3. Matrices

Since their conception in the 1840's by Arthur Cayley and James Sylvester, matrices have grown to become one of the most important tools used in all areas of mathematics and quantitative sciences. Algebra students use matrices to store and manipulate the coefficients from systems of equations. Matrices serve as the primary means of representing transformations from one geometric space to another. Computer programmers rely on matrices, referring to them as *two-dimensional arrays*. Matrices and matrix operations create crucial algebraic systems for many areas of abstract algebra. In discrete mathematics, one of the primary uses of matrices is in representing relations between elements of sets in a manner that is efficient for both storage and computation. This application of matrices will appear in Chapters 5 and 9. In this section, we define operations on matrices and compare their properties with those of real numbers given in Section 2.1.

A **matrix** is defined to be a rectangular array of numbers, meaning an arrangement of numbers in rectangular form with no empty positions. The plural form of matrix is **matrices**. The size of a matrix is determined by the number of horizontal **rows** and vertical **columns**. A matrix with m rows and n columns is said to have **size** $m \times n$, read "m by n," for positive integers m and n. When $m = n$, it is called a **square matrix**.

Each of the mn positions in an $m \times n$ matrix is assigned an "address" in a manner reminiscent of Cartesian coordinates. If the number appears at the

intersection of Row i (counting from the top down) and Column j (counting from left to right), where $1 \leq i \leq m$ and $1 \leq j \leq n$, it is called the (i, j)-**entry** of the matrix. For instance, the 2×4 matrix $\begin{bmatrix} 1 & -4 & 0 & -2 \\ 0 & 5 & 7 & -1 \end{bmatrix}$ has -4 as its $(1, 2)$-entry and 7 as its $(2, 3)$-entry.

Matrices are typically named with uppercase Latin letters, A, B, M, etc., while the entries are denoted with the corresponding lowercase letter. For instance, the (i, j)-entry of matrix A is denoted a_{ij}, giving a generic $m \times n$ matrix the form $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$.

We sometimes write $A = [a_{ij}]$ when a direct description of the entries of matrix A is needed. The **diagonal entries** of $A = [a_{ij}]$ are those for which $i = j$, namely a_{11}, a_{22}, ..., and particularly for square matrices, they are said to form the **main diagonal** of A. A square matrix for which the (i, j)-entry is 0 when $i \neq j$ is called a **diagonal matrix**.

Certain arithmetic operations can be defined on matrices of the same size as a straightforward extension of familiar operations on real numbers. If $A = [a_{ij}]$ and $B = [b_{ij}]$ are $m \times n$ matrices, the **sum** of A and B is the $m \times n$ matrix with (i, j)-entry equaling $a_{ij} + b_{ij}$; in symbols, $A + B = [a_{ij} + b_{ij}]$. Subtraction of matrices of the same size is also accomplished *componentwise*, namely $A - B = [a_{ij} - b_{ij}]$. A **scalar multiple** of a matrix A is obtained by multiplying each entry of A by a real number[2] k; that is $kA = [ka_{ij}]$.

EXAMPLE 8. Compute $B - 2C$ for $B = \begin{bmatrix} 1 & 5 \\ -2 & 6 \end{bmatrix}$ and $C = \begin{bmatrix} 3 & 0 \\ 4 & -2 \end{bmatrix}$.

Solution. As B and C are 2×2 matrices, $2C$ is 2×2, and the difference of B and $2C$ is defined:

$$\begin{aligned} B - 2C &= \begin{bmatrix} 1 & 5 \\ -2 & 6 \end{bmatrix} - 2\begin{bmatrix} 3 & 0 \\ 4 & -2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 5 \\ -2 & 6 \end{bmatrix} - \begin{bmatrix} 6 & 0 \\ 8 & -4 \end{bmatrix} \\ &= \begin{bmatrix} 1-6 & 5-0 \\ -2-8 & 6-(-4) \end{bmatrix} = \begin{bmatrix} -5 & 5 \\ -10 & 10 \end{bmatrix}. \end{aligned}$$

Matrix multiplication is defined in a very different manner from the componentwise simplicity of matrix addition. Its definition arises from Cayley's use of matrix multiplication for the composition of two transformations (functions)

[2]In the language of matrices and vectors, real numbers are often called **scalars**.

in geometric settings. We first define the **inner product** of the i-th row of A with the j-th column of B as $\begin{bmatrix} a_{i1} & a_{i2} & \cdots & a_{ip} \end{bmatrix} \cdot \begin{bmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{pj} \end{bmatrix} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ip}b_{pj}$. Notice that this requires that the number of columns of A equals the number of rows of B. The **product** of matrices A and B is defined to be the matrix AB whose (i, j)-entry is the inner product of the i-th row of A with the j-th column of B. In contrast to matrix addition, which requires that matrices have the same size, the sizes required for matrix multiplication can be characterized as follows: If A is an $m \times p$ matrix and B is a $p \times n$ matrix, then the product AB is an $m \times n$ matrix.[3]

EXAMPLE 9. Compute the product AB for matrices

$$A = \begin{bmatrix} 4 & -3 \\ 1 & 2 \\ 0 & -1 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 5 \\ -2 & 6 \end{bmatrix}.$$

Solution. First note that the number of columns of A equals the number of rows of B (namely, two), hence the product AB is defined, and its size is 3×2. Using the definition of matrix multiplication,

$$\begin{aligned} AB &= \begin{bmatrix} 4 & -3 \\ 1 & 2 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 5 \\ -2 & 6 \end{bmatrix} \\ &= \begin{bmatrix} 4(1) + (-3)(-2) & 4(5) + (-3)(6) \\ 1(1) + 2(-2) & 1(5) + 2(6) \\ 0(1) + (-1)(-2) & 0(5) + (-1)(6) \end{bmatrix} = \begin{bmatrix} 10 & 2 \\ -3 & 17 \\ 2 & -6 \end{bmatrix}. \end{aligned}$$

Notice that the product BA is not defined for matrices A and B in Example 9, since the number of columns of B (two) does not equal the number of rows of A (three). This is our first indication that matrix multiplication is not commutative: BA need not equal AB. Of course, multiplication of square matrices of the same size is always defined, but this does not resolve the issue of commutativity. Let $B = \begin{bmatrix} 1 & 5 \\ -2 & 6 \end{bmatrix}$ and $C = \begin{bmatrix} 3 & 0 \\ 4 & -2 \end{bmatrix}$. We invite the reader to gain practice multiplying matrices to confirm that $BC = \begin{bmatrix} 23 & -10 \\ 18 & -12 \end{bmatrix}$ and $CB = \begin{bmatrix} 3 & 15 \\ 0 & 8 \end{bmatrix}$.

[3]Geometrically, this indicates that AB maps n-dimensional space to m-dimensional space. It is the composition of B, mapping n-dimensional space to p-dimensional space, with A which maps p-dimensional space to m-dimensional space.

The $n \times n$ matrix with 1's on the main diagonal and 0's elsewhere is called the $n \times n$ **identity matrix**, denoted I_n. Given the advantageous arrangement of 0's and 1's, appropriately sized identity matrices fulfill the role of a multiplicative identity (see Property 2.1). As an example, let A be defined as in Example 9; then

$$AI_2 = \begin{bmatrix} 4 & -3 \\ 1 & 2 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 4(1) + -3(0) & 4(0) + -3(1) \\ 1(1) + 2(0) & 1(0) + 2(1) \\ 0(1) + (-1)(0) & 0(0) + (-1)(1) \end{bmatrix} = A$$

and similarly $I_3 A = A$. In general, for $m \times n$ matrix A, $I_m A = A$ and $AI_n = A$.

While matrix division is not an acceptable operation, the topic of multiplicative inverses of square matrices is crucial. Given a matrix A, if there exists a matrix B for which $AB = I_n$ for some n, then A is said to be **invertible** and B is called the **inverse** of A. It can be proven that A and B must be square matrices of size $n \times n$, $BA = I_n$, and the inverse of A is uniquely determined. The inverse of A is denoted A^{-1}. A procedure for computing the inverse of an $n \times n$ matrix may be found in standard texts in college algebra, pre-calculus, and linear algebra and is omitted here. We will describe the simple process for computing the inverse of any invertible 2×2 matrix and use this to demonstrate that many matrices are not invertible.

If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $ad - bc \neq 0$, the inverse of A is $A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. The reader should verify that $AA^{-1} = I_2$ and $A^{-1}A = I_2$, with the suggestion that the scalar multiple $\frac{1}{ad-bc}$ be held in reserve until the matrix multiplication is complete. There are infinitely many 2×2 matrices for which $ad - bc$ is 0; this is the collection of all 2×2 matrices which are not invertible. This is in substantial contrast with the real numbers for which there is only one element that has no multiplicative inverse.

Besides the issues of commutativity of multiplication and matrix inverses, the properties of real numbers given in Property 2.1 have correspondent properties in matrix arithmetic. Considering both scalar multiplication and matrix multiplication, the list is more extensive for matrices. For ease of presentation, these properites will be described for the set of $n \times n$ matrices, for any fixed natural number n; we denote this set by M_n. Analogous properties also hold for non-square matrices with sizes appropriate for the operations.

PROPERTY 2.7. *Suppose A, B, and C are matrices in M_n and r and s are real numbers. Let $\mathbf{0}$ denote the matrix in M_n with all zero entries.*

(1) Closure: The sum, difference, and product of two matrices in M_n are also in M_n.

(2) *Commutative law:* $A + B = B + A$.
(3) *Associative laws:* $(A + B) + C = A + (B + C)$, $(AB)C = A(BC)$, $r(sA) = (rs)A$, *and* $r(AB) = (rA)B = A(rB)$.
(4) *Distributive laws:* $A(B + C) = AB + AC$, $(A + B)C = AC + BC$, $r(A + B) = rA + rB$, *and* $(r + s)A = rA + sA$.
(5) *Additive and Multiplicative Identities:* $\mathbf{0} + A = A$ *and* $AI_n = A = I_nA$.
(6) *Additive Inverse: There is an additive inverse in* M_n, *denoted* $-A$, *such that* $A + (-A) = \mathbf{0}$.
(7) *Multiplicative Inverse: If* A *is an invertible matrix, then* $AA^{-1} = I_n = A^{-1}A$.

First Thoughts. The notation $-A$ in Part (6) simply indicates that each entry of A is negated. It is equal to the scalar multiplication $(-1)A$, as a result of using Theorem 2.2(8) of Section 2.1 for each entry. In the same way, each property of matrix arithmetic not only appears to be similar to a law for real numbers found in Property 2.1, but its truth (or "proof") is based on the corresponding law for real numbers, which is applied in each entry of the matrix. ◇

Proof. Students will be asked to verify many of these claims for the special case of 2×2 matrices in the Exercises and Problems. Part (2) is shown here as a model to emulate.

Consider two arbitrary 2×2 matrices $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ and $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$.

Then

$$\begin{aligned} A + B &= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \\ &= \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{bmatrix} \\ &= \begin{bmatrix} b_{11} + a_{11} & b_{12} + a_{12} \\ b_{21} + a_{21} & b_{22} + a_{22} \end{bmatrix} \\ &= \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} + \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = B + A. \end{aligned}$$

Take notice of the use of commutativity of addition of real numbers in each entry. □

Two important properties of inverses follow directly from the discussion above. The order of the factors in the expanded form of $(AB)^{-1}$ may seem surprising at first, but the lack of commutativity of matrix multiplication dictates this order.

PROPERTY 2.8. *Suppose* A *and* B *are invertible matrices in* M_n.
(1) $\left(A^{-1}\right)^{-1} = A$

(2) $(AB)^{-1} = B^{-1}A^{-1}$

Proof. The proof of (1) will be provided as a pattern for proving the other results about inverses, which will be requested in the Problems section. The notation $\left(A^{-1}\right)^{-1}$ refers to the inverse of the matrix A^{-1}, which is the unique matrix X for which $A^{-1}X = I_n$. From Property 2.7(7), $X = A$ satisfies this matrix equation. By uniqueness, $\left(A^{-1}\right)^{-1} = A$. □

For an $m \times n$ matrix $A = a_{ij}$, the **transpose** of A, written A^T, is the $n \times m$ matrix with (i, j)-entry equaling the (j, i)-entry of A; in symbols, $A^T = [a_{ji}]$. Thus, A and A^T have rows and columns interchanged. In the event that $A^T = A$, A is said to be a **symmetric matrix**. A symmetric matrix is necessarily a square matrix with symmetry about the main diagonal. In particular, $A = [a_{ij}]$ is an $n \times n$ symmetric matrix if and only if $a_{ji} = a_{ij}$ for $1 \leq i, j \leq n$.

PROPERTY 2.9. *Suppose A, B, and C are matrices in M_n, with C invertible, and suppose r is a real number.*

(1) $\left(A^T\right)^T = A$
(2) $(A + B)^T = A^T + B^T$
(3) $(AB)^T = B^T A^T$
(4) $(rA)^T = rA^T$
(5) $\left(C^T\right)^{-1} = \left(C^{-1}\right)^T$

Parts (1)–(4) of Property 2.9 are true for all non-square matrices for which the operations are defined. The sizes of the matrices in Part (3) are noteworthy. If A is $m \times p$ and B is $p \times n$, giving AB size $m \times n$, then B^T is $n \times p$ and A^T is $p \times m$, making $B^T A^T$ size $n \times m$ as expected.

Exercises and Problems

(1) Perform the matrix operations for the matrices defined as follows:

$$A = \begin{bmatrix} 6 & -10 \\ 2 & -3 \\ 4 & 0 \end{bmatrix},\ B = \begin{bmatrix} 4 & 2 & 1 & 6 \\ -10 & 3 & 9 & 1 \\ 4 & -8 & 6 & -2 \end{bmatrix},\ C = \begin{bmatrix} 0 & -8 & 5 \\ -3 & 4 & -6 \end{bmatrix},$$

$$D = \begin{bmatrix} 5 & 10 & 5 \\ -7 & 9 & -10 \\ 0 & 4 & -2 \end{bmatrix},\ E = \begin{bmatrix} -2 & 4 & 8 \\ -7 & 6 & -1 \\ 4 & 5 & 3 \end{bmatrix}.$$

(a) $D + E$
(b) $4E - 3D$
(c) DE
(d) ED
(e) DB

(f) C^T
(g) $A + C^T$
(h) $B^T E$

(2) Positive powers of square matrices have the natural meaning. For natural number k, A^k is the product of k factors of matrix A. Refer to the matrices in Exercise 1.
(a) Compute E^2.
(b) Explain why A^2 is not defined.

(3) For A, B, C, D, and E, given in Exercise 1, determine which of the following operations are defined and perform those operations.
(a) $A + D$
(b) CB
(c) BA
(d) $B^T A$
(e) $A^T C^T$
(f) C^2
(g) D^2

---

(4) Verify each property using generic 2×2 matrices in the manner modeled in the proof of Property 2.7(2).
(a) Closure of matrix addition: if A and B are matrices in M_2, then $A + B$ is in M_2
(b) Closure of matrix multiplication: if A and B are in M_2, then AB is in M_2
(c) Associativity of matrix addition: $(A + B) + C = A + (B + C)$
(d) Left distributivity: $A(B + C) = AB + AC$
(e) Additive identity: $\mathbf{0} + A = A$
(f) Multiplicative identity: $AI_2 = A$
(g) Additive inverse: $A + (-A) = \mathbf{0}$
(h) Multiplicative inverse: $AA^{-1} = I_2$

(5) Verify each property using generic 2×2 matrices in the manner modeled in the proof of Property 2.7(2).
(a) $\left(A^T\right)^T = A$
(b) $(A + B)^T = A^T + B^T$
(c) $(AB)^T = B^T A^T$
(d) $\left(C^T\right)^{-1} = \left(C^{-1}\right)^T$

(6) Verify each property by showing that the purported inverse satisfies the necessary equation as demonstrated in the proof of Property 2.8(1).
(a) $(AB)^{-1} = B^{-1} A^{-1}$
(b) $\left(C^T\right)^{-1} = \left(C^{-1}\right)^T$

(7) Let S denote the set of all diagonal 2×2 matrices. Note that a generic element of S has the form $D = \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$. For each of the following properties, determine whether the property is true for S. For each property that holds in S, demonstrate that it is true using generic matrices from S.
   (a) Closure of matrix addition
   (b) Closure of matrix multiplication
   (c) Additive identity in S
   (d) Multiplicative identity in S
   (e) Commutativity of multiplication

(8) Let $D = \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$ be a diagonal matrix.
   (a) Under what conditions will D be invertible?
   (b) If D is invertible, determine the form of D^{-1}.
   (c) If D is invertible, must D^{-1} be diagonal?

(9) Suppose k is a natural number and $D = \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$ is a diagonal matrix.
   (a) Compute D^2.
   (b) Determine a concise formula for D^k.

(10) Suppose A is a square matrix. Using the definition of symmetric matrix and the properties in this section, explain why $A + A^T$ must be a symmetric matrix.

(11) Prove that a 2×2 matrix A is not invertible if and only if one column is a multiple of the other. Hint: Use the condition that $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible if and only if $ad - bc \neq 0$.