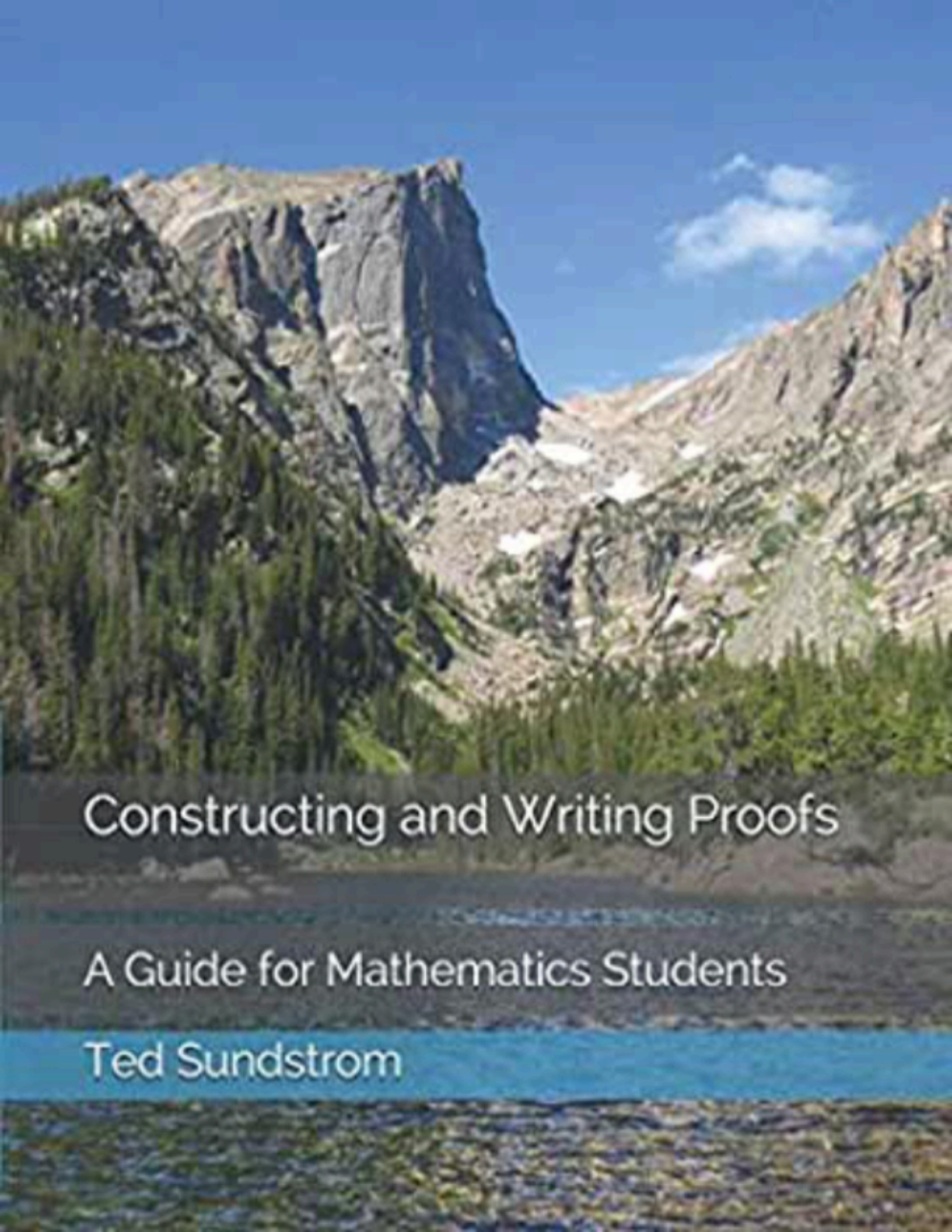
Constructing and Writing Proofs
A Guide for Mathematics Students
Ted Sundstrom

Constructing and Writing Mathematical Proofs

A Guide for Mathematics Students

November 22, 2022

Ted Sundstrom

Professor Emeritus
Grand Valley State University

Ted Sundstrom
Professor Emeritus, Grand Valley State University
Allendale, MI

Constructing and Writing Mathematical Proofs: A Guide for Mathematics Majors

License

Contents

Note to Students

This little book is not intended to be a textbook for a course dealing with an introduction to constructing and writing mathematical proofs. It is intended to be a reference book for students who need to construct and write proofs in their upper division mathematics courses. So it is assumed that students who use this as a reference have already taken an "introduction to proofs" course.

With the exception of Chapter 1, each chapter in the book has a description of a proof technique along with some justification as to why it is a valid proof method. There are then one or two completed proofs written according to the writing guidelines for mathematical proofs in Appendix A. The intent is to illustrate a well-written proof for that particular proof method. Each chapter then ends with three to five practice problems, most of which deal with mathematical proofs. Completed proofs (or solutions) for the practice problems are contained in Appendix B. So students can check their work or see other examples of well-written proofs. Chapter 1 contains most of the definitions used in the first six chapters of this book and a short summary of some logic that is pertinent to constructing mathematical proofs.

The proofs in this book primarily use the concepts of even and odd integers, the concept of one integer dividing another, and the concept of congruence in the integers. Most of this book is based on material in chapter 3 of the book *Mathematical Reasoning: Writing and Proof, Version 3* by Ted Sundstrom, which is a textbook for an "introduction to proofs" course. It is free to download as a pdf file at

https://scholarworks.gvsu.edu/books/24/.

A printed version of this book is also available on amazon.com for $22 at

http://gvsu.edu/s/1qt.

Finally, there is a website for *Mathematical Reasoning: Writing and Proof, Version 3*. Please visit

www.tedsundstrom.com

and click on the TEXTBOOKS button in the upper right corner. This website contains useful resources for an introduction to mathematical proofs course, and some of these resources could be useful for students in upper division mathematics courses.

Chapter 1

Preliminaries

This chapter is meant primarily for review and to clearly state the definitions that will be used in proofs throughout the text. For those who are familiar with this material, it is not necessary to read this chapter. It is included primarily for reference for the discussion of proofs in the other chapters.

1.1 Definitions

Definitions play a very important role in mathematics. A direct proof of a proposition in mathematics is often a demonstration that the proposition follows logically from certain definitions and previously proven propositions. A **definition** is an agreement that a particular word or phrase will stand for some object, property, or other concept that we expect to refer to often. In many elementary proofs, the answer to the question, "How do we prove a certain proposition?", is often answered by means of a definition. For mathematical proofs, we need very precise and carefully worded definitions.

Definitions Involving the Natural Numbers and the Integers

Definition.

- The set of **natural numbers**, denoted by $\mathbb{N}$, consists of the counting numbers (1, 2, 3, and so on). That is

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

- The set of **whole numbers**, denoted by $\mathbb{W}$, consists of the counting numbers and zero. That is

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

- The set of **integers**, denoted by $\mathbb{Z}$, consists of the whole numbers and their corresponding negatives. That is,

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

Definition. An integer a is an **even integer** provided that there exists an integer n such that $a = 2n$. An integer a is an **odd integer** provided there exists an integer n such that $a = 2n + 1$.

Definition. A nonzero integer m **divides** an integer n provided that there is an integer q such that $n = m \cdot q$. We also say that m is a **divisor** of n, m is a **factor** of n, and n is a **multiple** of m.

Notes

- If a and b are integers and $a \neq 0$, we frequently use the notation $a \mid b$ as a shorthand for "a divides b."
- The integer 0 is not a divisor of any integer but is a multiple of every integer.

Definition. A natural number p is a **prime number** provided that it is greater than 1 and the only natural numbers that are factors of p are 1 and p. A natural number other than 1 that is not a prime number is a **composite number**. The number 1 is neither prime nor composite.

Definition. Let $n \in \mathbb{N}$. If a and b are integers, then we say that ***a* is congruent to *b* modulo *n*** provided that n divides $a - b$. A standard notation for this is $a \equiv b \pmod{n}$. This is read as "a is congruent to b modulo n" or "a is congruent to b mod n."

Definitions Involving Sets

Definition. Two sets, A and B, are **equal** when they have precisely the same elements.

The set A is a **subset** of a set B provided that each element of A is an element of B.

Notation

- When two sets A and B are equal, we write $A = B$. When they are not equal, we write $A \neq B$.
- When the set A is a subset of the set B, we write $A \subseteq B$ and also say that A is **contained** in B. When A is not a subset of B, we write $A \nsubseteq B$.

Definition. Let A and B be two sets contained in some universal set U. The set A is a **proper subset** of B provided that $A \subseteq B$ and $A \neq B$.

Notation: When the set A is a proper subset of the set B, we write $A \subset B$.

Definition. Let A and B be subsets of some universal set U. The **intersection** of A and B, written $A \cap B$ and read "A intersect B," is the set of all elements that are in both A and B. That is,

$$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}.$$

The **union** of A and B, written $A \cup B$ and read "A union B," is the set of all elements that are in A or in B. That is,

$$A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}!.$$

Definition. Let A and B be subsets of some universal set U. The **set difference** of A and B, or **relative complement** of B with respect to A, written $A - B$ and read "A minus B" or "the complement of B with respect to A," is the set of all elements in A that are not in B. That is,

$$A - B = \{x \in U \mid x \in A \text{ and } x \notin B\}.$$

The **complement** of the set A, written A^c and read "the complement of A," is the set of all elements of U that are not in A. That is,

$$A^c = \{x \in U \mid x \notin A\}.$$

1.2 Useful Logic for Constructing Proofs

A **statement** is a declarative sentence that is either true or false but not both. A **compound statement** is a statement that contains one or more operators. Because some operators are used so frequently in logic and mathematics, we give them names and use special symbols to represent them.

- The **conjunction** of the statements P and Q is the statement "P **and** Q" and is denoted by $P \wedge Q$. The statement $P \wedge Q$ is true only when both P and Q are true.
- The **disjunction** of the statements P and Q is the statement "P **or** Q" and is denoted by $P \vee Q$. The statement $P \vee Q$ is true only when at least one of P or Q is true.
- The **negation (of a statement)** of the statement P is the statement "**not** P" and is denoted by $\neg P$. The negation of P is true only when P is false, and $\neg P$ is false only when P is true.
- The **implication** or **conditional** is the statement "**If** P **then** Q" and is denoted by $P \rightarrow Q$. The statement $P \rightarrow Q$ is often read as "P **implies** Q. The statement $P \rightarrow Q$ is false only when P is true and Q is false.
- The **biconditional statement** is the statement "***P* if and only if *Q***" and is denoted by $P \leftrightarrow Q$. The statement $P \leftrightarrow Q$ is true only when both P and Q have the same truth values.

Definition. Two expressions X and Y are **logically equivalent** provided that they have the same truth value for all possible combinations of truth values for all variables appearing in the two expressions. In this case, we write $X \equiv Y$ and say that X and Y are logically equivalent.

Theorem 1.1 states some of the most frequently used logical equivalencies used when writing mathematical proofs.

Theorem 1.1 (**Important Logical Equivalencies**)
For statements P, Q, and R,

De Morgan's Laws	$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$
	$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$
Conditional Statements	$P \to Q \equiv \neg Q \to \neg P$ *(contrapositive)*
	$P \to Q \equiv \neg P \vee Q$
	$\neg(P \to Q) \equiv P \wedge \neg Q$
Biconditional Statement	$(P \leftrightarrow Q) \equiv (P \to Q) \wedge (Q \to P)$
Double Negation	$\neg(\neg P) \equiv P$
Distributive Laws	$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
	$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
Conditionals with Disjunctions	$P \to (Q \vee R) \equiv (P \wedge \neg Q) \to R$
	$(P \vee Q) \to R \equiv (P \to R) \wedge (Q \to R)$

Definition. The phrase "for every" (or its equivalents) is called a **universal quantifier**. The phrase "there exists" (or its equivalents) is called an **existential quantifier**. The symbol $\forall$ is used to denote a universal quantifier, and the symbol $\exists$ is used to denote an existential quantifier.

Theorem 1.2 (**Negations of Quantified Statements**)
For any open sentence $P(x)$,

$$\neg(\forall x \in U)[P(x)] \equiv (\exists x \in U)[\neg P(x)], \text{ and}$$
$$\neg(\exists x \in U)[P(x)] \equiv (\forall x \in U)[\neg P(x)].$$

Chapter 2

Direct Proofs

In order to prove that a conditional statement $P \rightarrow Q$ is true, we only need to prove that Q is true whenever P is true. This is because the conditional statement is true whenever the hypothesis is false. So in a direct proof of $P \rightarrow Q$, we assume that P is true, and using this assumption, we proceed through a logical sequence of steps to arrive at the conclusion that Q is true. Unfortunately, it is often not easy to discover how to start this logical sequence of steps or how to get to the conclusion that Q is true. We will describe a method of exploration that often can help in discovering the steps of a proof. This method will involve working forward from the hypothesis, P, and backward from the conclusion, Q. We will illustrate this "forward-backward" method with the following proposition.

2.1 Using the Definitions of Congruence and Divides

We will consider the following proposition and try to determine if it is true or false.

Proposition 2.1. *For all integers a and b, if $a \equiv 5 \pmod 8$ and $b \equiv 6 \pmod 8$, then $(a + b) \equiv 3 \pmod 8$.*

Before we try to prove a proposition, it is a good idea to try some examples for which the hypothesis is true and then determine whether or not the conclusion is true for these examples. The idea is to convince ourselves that this proposition at least appears to be true. On the other hand, if we find an example where the hypothesis is true and the conclusion is false, then we have found a **counterexample** for the proposition and we would have prove the proposition to be false. The

following table summarizes four examples that suggest this proposition is true.

a	b	$a+b$	Is $(a+b) \equiv 2 \pmod 8$?
5	6	11	Yes, since $11 \equiv 3 \pmod 8$
13	22	35	Yes, since $35 \equiv 3 \pmod 8$
-3	14	11	Yes, since $11 \equiv 3 \pmod 8$
-11	-2	-13	Yes, since $-13 \equiv 3 \pmod 8$

We will not attempt to construct a proof of this proposition. We will start with the backwards process. Please keep in mind that it is a good idea to write all of this down on paper. We should not try to construct a proof in our heads. Writing helps.

We know that the goal is to prove that $(a+b) \equiv 3 \pmod 8$. (We label this as statement Q.) We then ask a "backwards question" such as, "How do we prove $(a+b) \equiv 3 \pmod 8$?" We may be able to answer this question in different ways depending on whether or not we have some previously proven results, but we can always use the definition. An answer to this question is, "We can prove that 8 divides $(a+b)-3$." (We label this as statement $Q1$). We now ask, "How can we prove that 8 divides $(a+b)-3$?" Again, we can use the definition and answer that we can prove that there exists an integer k such that $(a+b)-3 = 8k$. (This is statement $Q2$.) Here is what we should have written down.

- Q: $(a+b) \equiv 3 \pmod 8$.
- $Q1$: 8 divides $(a+b)-3$.
- $Q2$: There exists an integer k such that $(a+b)-3 = 8k$.

The idea is that if we can prove that $Q2$ is true, then we can conclude that $Q1$ is true, and then we can conclude that Q is true. $Q2$ is a good place to stop the backwards process since it involves proving that something exists and we have an equation with which to work. So we start the forward process. We start by writing down the assumptions stated in the hypothesis of the proposition and label it statement P. We then make conclusions based on these assumptions. While doing this, we look at the items in the backward process and try to find ways to connect the conclusions in the forward process to the backward process. From statement P, we conclude that 8 divides $a-5$ and 8 divides $b-6$. (This becomes statement $P1$.) We make a conclusion based on statement $P1$, which becomes statement $P2$. The forward process can be summarized as follows:

- P: a and b are integers and $a \equiv 5 \pmod 8$ and $b \equiv 6 \pmod 8$.
- $P1$: 8 divides $a-5$ and 8 divides $b-6$.

- $P2$: There exists an integer m such that $a - 5 = 8m$ and there exists an integer n such that $b - 6 = 8n$.

It now seems that there is a way to connect the forward part ($P2$) to the backward part ($Q2$) using the existence of m and n (which have been proven to exist) and the equations in $P2$ and $Q2$.

Solving the two equations in $P2$ for a and b, we obtain $a = 8m + 5$ and $b = 8n + 6$. We can now use these in $Q2$.

Important Note: In the proof, we cannot use the integer k in $Q2$ since we have not proven that such an integer exists. This is why we used the letter m in statement $P2$. The goal is to prove that the integer k exists.

We can now proceed as followings:

$$\begin{aligned}(a + b) - 3 &= (8m + 5) + (8n + 6) - 3\\ &= 8m + 8n + 8\\ &= 8(m + n + 3)\end{aligned}$$

Since the integers are closed under addition, we conclude that $(m + n + 3)$ is an integer and so the last equation implies that 8 divides $(a + b) - 3$. We can now write a proof. The following proof is written according to the writing guidelines in Appendix A.

Proposition 2.1. *For all integers a and b, if $a \equiv 5 \pmod 8$ and $b \equiv 6 \pmod 8$, then $(a + b) \equiv 3 \pmod 8$.*

Proof. We assume that a and b are integers and that $a \equiv 5 \pmod 8$ and $b \equiv 6 \pmod 8$. We will prove that $(a + b) \equiv 3 \pmod 8$. From the assumptions, we conclude that

$$8 \text{ divides } (a - 5) \text{ and } 8 \text{ divides } (b - 6).$$

So there exist integers m and n such that

$$a - 5 = 8m \text{ and } b - 6 = 8n.$$

Solving these equations for a and b, we obtain $a = 8m + 5$ and $b = 8n + 6$. We can now substitute for a and b in the expression $(a + b) - 3$. This gives

$$\begin{aligned}(a + b) - 3 &= (8m + 5) + (8n + 6) - 3\\ &= 8m + 8n + 8\\ &= 8(m + n + 3)\end{aligned}$$

Since the integers are closed under addition, we conclude that $(m + n + 3)$ is an integer and so the last equation implies that 8 divides $(a + b) - 3$. So by the definition of congruence, we can conclude that $(a + b) \equiv 3 \pmod 8$. This proves that for all integers a and b, if $a \equiv 5 \pmod 8$ and $b \equiv 6 \pmod 8$, then $(a + b) \equiv 3 \pmod 8$. ■

Note: This shows a typical way to construct and write a direct proof of a proposition or theorem. We will not be going into this much detail on the construction process in all of the results proved in this book. In fact, most textbooks do not do this. What they most often show is only the final product as shown in the preceding proof. Do not be fooled that this is the way that proofs are constructed. Constructing a proof often requires trial and error and because of this, it is always a good idea to write down what is being assumed and what it is we are trying to prove. Then be willing to work backwards from what it is to be proved and work forwards from the assumptions. The hard part is often connecting the forward process to the backward process. This becomes extremely difficult if we do not write things down and try to work only in our heads.

We sometimes think that a proposition is true and attempt to write a proof. If we get stuck, we need to consider that a possible reason for this is that the proposition is actually false. Consider the following proposition.

Proposition 2.2. *For each integer n, if 7 divides $\left(n^2 - 4\right)$, then 7 divides $(n - 2)$.*

If we think about starting a a proof, we would let n be an integer, assume that 7 divides $\left(n^2 - 4\right)$ and from this assumption, try to prove that 7 divides $(n-2)$. That is, we would assume that there exists an integer k such that $n^2 - 4 = 7k$ and try to prove that there exists an integer m such that $n - 2 = 7m$. From the assumption, we can using factoring and conclude that

$$(n - 2)(n + 2) = 7k.$$

There does not seem to be a direct way to prove that there is an integer m such that $n - 2 = 7m$. So we start looking for examples of integers n such that 7 divides $\left(n^2 - 4\right)$ and see if 7 divides $(n-2)$ for these examples. After trying a few examples, we find that for $n = 0$ and $n = 5$, 7 divides $\left(n^2 - 4\right)$. (There are many other such values for n.) For $n = 5$, we see that

$$n^2 - 4 = 21 = 7 \cdot 3 \quad \text{and} \quad n - 2 = 3.$$

However, 7 does not divide 3. This shows that for $n = 5$, the hypothesis of Proposition 2.2 is true and the conclusion is false. This is a counterexample for the proposition and proves that Proposition 2.2 is false.

Note: This is the standard way to prove a conditional statement is false. Find an example (called a counterexample) in which the hypothesis is true and the conclusion is false. Sometimes, even though a proposition is false, we can modify the statement of the proposition and create a new true proposition. We can do this for Proposition 2.2 once we have studied more number theory. There is a theorem from number theory that states:

> For each prime number p and all integers a and b, if p divides ab, then p divides a or p divides b.

This result is known as **Euclid's Lemma**. Using this result, when we get to the part where we conclude that $(n-2)(n+2) = 7k$, we can conclude that 7 divides $(n-2)(n+2)$ and hence, 7 divides $n-2)$ or 7 divides $(n+2)$. So we would have the following true proposition.

Proposition. For each integer n, if 7 divides $\left(n^2-4\right)$, then 7 divides $(n-2)$ or 7 divides $(n+2)$.

2.2 Direct Proofs Involving Sets

One of the most basic types of proofs involving sets is to prove that one set is a subset of another set. If S and T are both subsets of some universal set U, to prove that S is a subset of T, we need to prove that

$$\text{For each element } x \text{ in } U, \text{ if } x \in S, \text{ then } x \in T.$$

When we have to prove something that involves a universal quantifier, we frequently use a method that can be called the **choose-an-element method.** The key is that we have to prove something about all elements in $\mathbb{Z}$. We can then add something to the forward process by choosing an arbitrary element from the set S. This does not mean that we can choose a specific element of S. Rather, we must give the arbitrary element a name and use only the properties it has by being a member of the set S.

The truth of the next proposition may be clear, but it is included to illustrate the process of proving one set is a subset of another set. In this proposition, the set S is the set of all integers that are a multiple of 6. So when we "choose" an element from S, we are not selecting a specific element in S (such as 12 or 24), but rather we are selecting an arbitrary element of S and so the only thing we can assume is that the element is a multiple of 6.

Proposition 2.3. *Let S be the set of all integers that are multiples of 6, and let T be the set of all even integers. Then S is a subset of T.*

Proof. Let S be the set of all integers that are multiples of 6, and let T be the set of all even integers. We will show that S is a subset of T by showing that if an integer x is an element of S, then it is also an element of T.

Let $x \in S$. (**Note**: The use of the word "let" is often an indication that the we are choosing an arbitrary element.) This means that x is a multiple of 6. Therefore, there exists an integer m such that

$$x = 6m.$$

Since $6 = 2 \cdot 3$, this equation can be written in the form

$$x = 2(3m).$$

By closure properties of the integers, $3m$ is an integer. Hence, this last equation proves that x must be even. Therefore, we have shown that if x is an element of S, then x is an element of T, and hence that $S \subseteq T$. ■

One way to prove that two sets are equal is to prove that each one is a subset of the other one. This is illustrated in the next proposition.

Proposition 2.4. *Let A and B be subsets of some universal sets. Then $A - B = A \cap B^c$.*

Proof. Let A and B be subsets of some universal set. We will prove that $A - B = A \cap B^c$ by proving that each set is a subset of the other set. We will first prove that $A - B \subseteq A \cap B^c$. Let $x \in A - B$. We then know that $x \in A$ and $x \notin B$. However, $x \notin B$ implies that $x \in B^c$. Hence, $x \in A$ and $x \in B^c$, which means that $x \in A \cap B^c$. This proves that $A - B \subseteq A \cap B^c$.

To prove that $A \cap B^c \subseteq A - B$, we let $y \in A \cap B^c$. This means that $y \in A$ and $y \in B^c$, and hence, $y \in A$ and $y \notin B$. Therefore, $y \in A - B$ and this proves that $A \cap B^c \subseteq A - B$. Since we have proved that each set is a subset of the other set, we have proved that $A - B = A \cap B^c$. ■

2.3 Practice Problems for Chapter 2

1. Use a counterexample to prove the following statement is false.

For all integers a and b, if 5 divides a or 5 divides b, then 5 divides $(5a + b)$.

2. Construct a table of values for $\left(3m^2 + 4m + 6\right)$ using at least six different integers for m. Make one-half of the values for m even integers and the other half odd integers. Is the following proposition true or false?

If m is an odd integer, then $\left(3m^2 + 4m + 6\right)$ is an odd integer.

Justify your conclusion. (If the proposition is true, then write a proof of the proposition. If the proposition is false, provide an example of an odd integer for which $\left(3m^2 + 4m + 6\right)$ is an even integer.)

3. The **Pythagorean Theorem** for right triangles states that if a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse, then $a^2 + b^2 = c^2$. For example, if $a = 5$ and $b = 12$ are the lengths of the two sides of a right triangle and if c is the length of the hypotenuse, then the $c^2 = 5^2 + 12^2$ and so $c^2 = 169$. Since c is a length and must be positive, we conclude that $c = 13$.

Construct and provide a well-written proof for the following proposition.

Proposition. If m is a real number and m, $m + 1$, and $m + 2$ are the lengths of the three sides of a right triangle, then $m = 3$.

4. Let n be a natural number and let a, b, c, and d be integers. Prove each of the following.

(**a**) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $(a + c) \equiv (b + d) \pmod{n}$.

(**b**) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

5. One way to prove that two sets are equal is to prove that each one is a subset of the other one. Consider the following proposition:

Proposition. *Let A and B be subsets of some universal set. Then $A - (A - B) = A \cap B$.*

Prove this proposition is true or give a counterexample to prove it is false.

Chapter 3

Using Logical Equivalencies in Proofs

It is sometimes difficult to construct a direct proof of a conditional statement. Fortunately, there are certain logical equivalencies in Theorem 1.1 on page 5 that can be used to justify some other methods of proof of a conditional statement. Knowing that two expressions are logically equivalent tells us that if we prove one, then we have also proven the other. In fact, once we know the truth value of a statement, then we know the truth value of any other statement that is logically equivalent to it.

3.1 Using the Contrapositive

One of the most useful logical equivalencies to prove a conditional statement is that a conditional statement $P \rightarrow Q$ is logically equivalent to its contrapositive, $\neg Q \rightarrow \neg P$. This means that if we prove the contrapositive of the conditional statement, then we have proven the conditional statement. The following are some important points to remember.

- A conditional statement is logically equivalent to its contrapositive.
- Use a direct proof to prove that $\neg Q \rightarrow \neg P$ is true.
- Caution: One difficulty with this type of proof is in the formation of correct negations. (We need to be very careful doing this.)

- We might consider using a proof by contrapositive when the statements P and Q are stated as negations.

We will use the following proposition to illustrate how the contrapositive of a conditional statement can be used in a proof.

Proposition 3.1. *For each integer n, if n^2 is an even integer, then n is an even integer.*

Proof. We will prove this result by proving the contrapositive of the statement, which is

For each integer n, if n is an odd integer, then n^2 is an odd integer.

So we assume that n is an odd integer and prove that n^2 is an odd integer. Since n is odd, there exists an integer k such that $n = 2k + 1$. Hence,

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2\left(2k^2 + 2k\right) + 1 \end{aligned}$$

Since the integers are closed under addition and multiplication, $\left(2k^2 + 2k\right)$ is an integer and so the last equation proves that n^2 is an odd integer. This proves that for all integers n, if n is an odd integer, then n^2 is a n odd integer. Since this is the contrapositive of the proposition, we have completed a proof of the proposition. ■

3.2 Using Other Logical Equivalencies

There are many logical equivalencies, but fortunately, only a small number are frequently used when trying to construct and write proofs. Most of these are listed in Theorem 1.1 on page 5. We will illustrate the use of one of these logical equivalencies with the following proposition:

For all real numbers a and b, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.

First, notice that the hypothesis and the conclusion of the conditional statement are stated in the form of negations. This suggests that we consider the contrapositive. Care must be taken when we negate the hypothesis since it is a conjunction. We use one of De Morgan's Laws as follows:

$$\neg\left(a \neq 0 \ \wedge \ b \neq 0\right) \equiv (a = 0) \vee (b = 0)\,.$$

So the contrapositive is:

For all real numbers a and b, if $ab = 0$, then $a = 0$ or $b = 0$.

The contrapositive is a conditional statement in the form $X \to (Y \vee Z)$. The difficulty is that there is not much we can do with the hypothesis ($ab = 0$) since we know nothing else about the real numbers a and b. However, if we knew that a was not equal to zero, then we could multiply both sides of the equation $ab = 0$ by $\frac{1}{a}$. This suggests that we consider using the following logical equivalency based on a result in Theorem 1.1 on page 5:

$$X \to (Y \vee Z) \equiv (X \wedge \neg Y) \to Z.$$

Proposition 3.2. *For all real numbers a and b, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.*

Proof. We will prove the contrapositive of this proposition, which is

For all real numbers a and b, if $ab = 0$, then $a = 0$ or $b = 0$.

This contrapositive, however, is logically equivalent to the following:

For all real numbers a and b, if $ab = 0$ and $a \neq 0$, then $b = 0$.

To prove this, we let a and b be real numbers and assume that $ab = 0$ and $a \neq 0$. We can then multiply both sides of the equation $ab = 0$ by $\frac{1}{a}$. This gives

$$\frac{1}{a}(ab) = \frac{1}{a} \cdot 0.$$

We now use the associative property on the left side of this equation and simplify both sides of the equation to obtain

$$\begin{aligned} \left(\frac{1}{a} \cdot a\right) b &= 0 \\ 1 \cdot b &= 0 \\ b &= 0 \end{aligned}$$

Therefore, $b = 0$ and this proves that for all real numbers a and b, if $ab = 0$ and $a \neq 0$, then $b = 0$. Since this statement is logically equivalent to the contrapositive of the proposition, we have proved the proposition. ■

3.3 Proofs of Biconditional Statements

One of the logical equivalencies in Theorem 1.1 on page 5 is the following one for biconditional statements.

$$(P \leftrightarrow Q) \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)\,.$$

This logical equivalency suggests one method for proving a biconditional statement written in the form "P if and only if Q." This method is to construct separate proofs of the two conditional statements $P \rightarrow Q$ and $Q \rightarrow P$.

We will illustrate this with a proposition about right triangles.

Recall that the **Pythagorean Theorem** for right triangles states that if a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse, then $a^2 + b^2 = c^2$. We also know that the area of any triangle is one-half the base times the altitude. So for the right triangle we have described, the area is $A = \frac{1}{2}ab$.

Proposition 3.3. *Suppose that a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse. This right triangle is an isosceles triangle if and only if the area of the right triangle is $\frac{1}{4}c^2$.*

Proof. We assume that we have a right triangle where a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse. We will prove that this right triangle is an isosceles triangle if and only if the area of the right triangle is $\frac{1}{4}c^2$ by proving the two conditional statements associated with this biconditional statement.

We first prove that if this right triangle is an isosceles triangle, then the area of the right triangle is $\frac{1}{4}c^2$. So we assume the right triangle is an isosceles triangle. This means that $a = b$, and consequently, $A = \frac{1}{2}a^2$. Using the Pythagorean Theorem, we see that

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

Hence, $a^2 = \frac{1}{2}c^2$, and we obtain $A = \frac{1}{2}a^2 = \frac{1}{4}c^2$. This proves that if this right triangle is an isosceles triangle, then the area of the right triangle is $\frac{1}{4}c^2$.

We now prove the converse of the first conditional statement. So we assume the area of this isosceles triangle is $A = \frac{1}{4}c^2$, and will prove that $a = b$. Since the

area is also $\frac{1}{2}ab$, we see that

$$\begin{aligned} \frac{1}{4}c^2 &= \frac{1}{2}ab \\ c^2 &= 2ab \end{aligned}$$

We now use the Pythagorean Theorem to conclude that $a^2 + b^2 = 2ab$. So the last equation can be rewritten as follows:

$$\begin{aligned} a^2 - 2ab + b^2 &= 0 \\ (a-b)^2 &= 0. \end{aligned}$$

The last equation implies that $a = b$ and hence the right triangle is an isosceles triangle. This proves that if the area of this right triangle is $A = \frac{1}{4}c^2$, then the right triangle is an isosceles triangle.

Since we have proven both conditional statements, we have proven that this right triangle is an isosceles triangle if and only if the area of the right triangle is $\frac{1}{4}c^2$. ■

3.4 Practice Problems for Chapter 3

1. Is the following proposition true or false?

For all integers a and b, if ab is even, then a is even or b is even.

Justify your conclusion by writing a proof if the proposition is true or by providing a counterexample if it is false.

2. Are the following statements true or false? Justify your conclusions.

(**a**) For each $a \in \mathbb{Z}$, if $a \equiv 2 \pmod 5$, then $a^2 \equiv 4 \pmod 5$.

(**b**) For each $a \in \mathbb{Z}$, if $a^2 \equiv 4 \pmod 5$, then $a \equiv 2 \pmod 5$.

(**c**) For each $a \in \mathbb{Z}$, $a \equiv 2 \pmod 5$ if and only if $a^2 \equiv 4 \pmod 5$.

3. A real number x is defined to be a **rational number** provided

$$\text{there exist integers } m \text{ and } n \text{ with } n \neq 0 \text{ such that } x = \frac{m}{n}.$$

A real number that is not a rational number is called an **irrational number.**

It is known that if x is a positive rational number, then there exist positive integers m and n with $n \neq 0$ such that $x = \frac{m}{n}$.

Is the following proposition true or false? Explain.

Proposition. For each positive real number x, if x is irrational, then $\sqrt{x}$ is irrational.

Chapter 4

Proof by Contradiction

4.1 Explanation and an Example

Another method of proof that is frequently used in mathematics is a **proof by contradiction.** This method is based on the fact that a statement X can only be true or false (and not both). The idea is to prove that the statement X is true by showing that it cannot be false. This is done by assuming that X is false and proving that this leads to a contradiction. (The contradiction often has the form $(R \wedge \neg R)$, where R is some statement.) When this happens, we can conclude that the assumption that the statement X is false is incorrect and hence X cannot be false. Since it cannot be false, then X must be true.

A logical basis for the contradiction method of proof is the tautology

$$[\neg X \to C] \to X,$$

where X is a statement and C is a contradiction. The following truth table establishes this tautology.

X	C	$\neg X$	$\neg X \to C$	$(\neg X \to C) \to X$
T	F	F	T	T
F	F	T	F	T

This tautology shows that if $\neg X$ leads to a contradiction, then X must be true. The previous truth table also shows that the statement $\neg X \to C$ is logically equivalent to X. This means that if we have proved that $\neg X$ leads to a contradiction, then we have proved statement X. So if we want to prove a statement X using a

proof by contradiction, we assume that $\neg X$ is true and show that this leads to a contradiction.

When we try to prove the conditional statement, "If P then Q" using a proof by contradiction, we must assume that $P \to Q$ is false and show that this leads to a contradiction. Since we are assuming the conditional statement is false, we are, in effect, assuming its negation is true. According to Theorem 1.1 on page 5,

$$\neg (P \to Q) \equiv P \wedge \neg Q.$$

We will illustrate the process of a proof by contradiction with the following proposition.

Proposition 4.1. *For each real number x, if $0 < x < 1$, then* $\dfrac{1}{x(1-x)} \geq 4$.

Proof. We will use a proof by contradiction. So we assume that the proposition is false, or that there exists a real number x such that $0 < x < 1$ and

$$\frac{1}{x(1-x)} < 4. \tag{1}$$

We note that since $0 < x < 1$, we can conclude that $x > 0$ and that $(1 - x) > 0$. Hence, $x(1 - x) > 0$ and if we multiply both sides of inequality (1) by $x(1 - x)$, we obtain

$$1 < 4x(1 - x).$$

We can now use algebra to rewrite the last inequality as follows:

$$\begin{aligned} 1 &< 4x - 4x^2 \\ 4x^2 - 4x + 1 &< 0 \\ (2x - 1)^2 &< 0 \end{aligned}$$

However, $(2x - 1)$ is a real number and the last inequality says that a real number squared is less than zero. This is a contradiction since the square of any real number must be greater than or equal to zero. Hence, the proposition cannot be false, and we have proved that for each real number x, if $0 < x < 1$, then $\dfrac{1}{x(1-x)} \geq 4$. ■

4.2 Proving that Something Does Not Exist

In mathematics, we sometimes need to prove that something does not exist or that something is not possible. Instead of trying to construct a direct proof, it is sometimes easier to use a proof by contradiction so that we can assume that the something exists.

We will illustrate this by proving the following proposition. Notice that the conclusion of the proposition involves trying to prove that an integer with a certain property does not exist. If we use a proof by contradiction, we can assume that such an integer z exists. This gives us more with which to work.

Proposition 4.2. *For all integers x and y, if x and y are odd integers, then there does not exist an integer z such that $x^2 + y^2 = z^2$.*

Proof. We will use a proof by contradiction. So we assume that the proposition is false or that there exist integers x and y such that x and y are odd and there exists an integer z such that $x^2 + y^2 = z^2$. Since x and y are odd, there exist integers m and n such that $x = 2m + 1$ and $y = 2n + 1$. So we get

$$\begin{aligned} x^2 + y^2 &= (2m+1)^2 + (2n+1)^2 \\ &= 4m^2 + 4m + 1 + 4n^2 + 4n + 1 \\ &= 2\left(2m^2 + 2m + 2n^2 + 2n + 1\right) \end{aligned} \tag{1}$$

Since the integers are closed under addition and multiplication, we see that $2\left(2m^2 + 2m + 2n^2 + 2n + 1\right)$ is an integer, and so the last equation shows that $x^2 + y^2$ is an even integer. Hence, z^2 is even since $z^2 = x^2 + y^2$. So using the result in Proposition 3.1 on page 14, we can conclude that z is even and that there exists an integer k such that $z = 2k$. Now, using equation (1) above, we see that

$$\begin{aligned} z^2 &= 2\left(2m^2 + 2m + 2n^2 + 2n + 1\right) \\ (2k)^2 &= 2\left(2m^2 + 2m + 2n^2 + 2n + 1\right) \\ 4k^2 &= 2\left(2m^2 + 2m + 2n^2 + 2n + 1\right) \end{aligned}$$

Dividing both sides of the last equation by 2, we obtain

$$\begin{aligned} 4k^2 &= 2\left(2m^2 + 2m + 2n^2 + 2n + 1\right) \\ 2k^2 &= 2\left(m^2 + m + n^2 + n\right) + 1 \end{aligned}$$

However, the left side of the last equation is an even integer and the right side is an odd integer. This is a contradiction, and so the proposition cannot be false. Hence,

we have proved that for all integers x and y, if x and y are odd integers, then there does not exist an integer z such that $x^2 + y^2 = z^2$. ■

4.3 Rational and Irrational Numbers

One of the most important ways to classify real numbers is as a rational number or an irrational number. Following is the definition of rational (and irrational) numbers given in Problem (3) on page 18.

Definition. A real number x is defined to be a **rational number** provided that there exist integers m and n with $n \neq 0$ such that $x = \frac{m}{n}$. A real number that is not a rational number is called an **irrational number.**

This may seem like a strange distinction because most people are quite familiar with the rational numbers (fractions) but the irrational numbers seem a bit unusual. However, there are many irrational numbers such as $\sqrt{2}$, $\sqrt{3}$, $\sqrt[3]{2}$, π, and the number e.

We use the symbol $\mathbb{Q}$ to stand for the set of rational numbers. There is no standard symbol for the set of irrational numbers. Perhaps one reason for this is because of the closure properties of the rational numbers, namely that the rational numbers $\mathbb{Q}$ are closed under addition, subtraction, multiplication, and division by nonzero rational numbers. This means that if $x, y \in \mathbb{Q}$, then

- $x + y$, $x - y$, and xy are in $\mathbb{Q}$; and
- If $y \neq 0$, then $\frac{x}{y}$ is in $\mathbb{Q}$.

The basic reasons for these facts are that if we add, subtract, multiply, or divide two fractions, the result is a fraction. One reason we do not have a symbol for the irrational numbers is that the irrational numbers are not closed under these operations. For example, $\sqrt{2}$ is irrational and we see that

$$\sqrt{2}\sqrt{2} = 2 \quad \text{and} \frac{\sqrt{2}}{\sqrt{2}} = 1.$$

This shows that the product of irrational numbers can be rational and the quotient of irrational numbers can be rational.

It is also important to realize that every integer is a rational number since any integer can be written as a fraction. For example, we can write $3 = \frac{3}{1}$. In general, if $n \in \mathbb{Z}$, then $n = \frac{n}{1}$, and hence, $n \in \mathbb{Q}$.

Because the rational numbers are closed under the standard operations and the definition of an irrational number simply says that the number is not rational, we often use a proof by contradiction to prove that a number is irrational. This is illustrated in the next proposition.

Proposition 4.3. *For all real numbers x and y, if x is rational and $x \neq 0$ and y is irrational, then $x \cdot y$ is irrational.*

Proof. We will use a proof by contradiction. So we assume that there exist real numbers x and y such that x is rational, $x \neq 0$, y is irrational, and $x \cdot y$ is rational. Since $x \neq 0$, we can divide by x, and since the rational numbers are closed under division by nonzero rational numbers, we know that $\frac{1}{x} \in \mathbb{Q}$. We now know that $x \cdot y$ and $\frac{1}{x}$ are rational numbers and since the rational numbers are closed under multiplication, we conclude that

$$\frac{1}{x} \cdot (xy) \in \mathbb{Q}.$$

However, $\frac{1}{x} \cdot (xy) = y$ and hence, y must be a rational number. Since a real number cannot be both rational and irrational, this is a contradiction to the assumption that y is irrational. We have therefore proved that for all real numbers x and y, if x is rational and $x \neq 0$ and y is irrational, then $x \cdot y$ is irrational. ■

4.4 Practice Problems for Chapter 4

1. (**a**) Determine at least five different integers that are congruent to 2 modulo 4. Are any of these integers congruent to 3 modulo 6?

(**b**) Is the following proposition true or false? Justify your conclusion with a counterexample (if it is false) or a proof (if it is true).

Propostion. For each integer n, if $n \equiv 2 \pmod 4$, then $n \not\equiv 3 \pmod 6$.

2. For the following, it may be useful to use the facts that the set of rational numbers $\mathbb{Q}$ is closed under addition, subtraction, multiplication, and division by nonzero rational numbers.

Prove the following proposition:

> **Proposition**. For all real numbers x and y, if x is rational and $x \neq 0$ and y is irrational, then $x + y$ is irrational.

3. Is the base 2 logarithm of 3, $\log_2(3)$, a rational or irrational number? Justify your conclusion.

4. Is the real number $\sqrt{2} + \sqrt{3}$ a rational or irrational number? Justify your conclusion.

Chapter 5

Using Cases in Proofs

The method of using cases in a proof is often used when the hypothesis of a proposition is a disjunction. This is justified by the logical equivalency

$$[(P \vee Q) \to R] \equiv [(P \to R) \wedge (Q \to R)] .$$

This is one of the logical equivalencies in Theorem 1.1 on page 5. In some other situations when we are trying to prove a proposition or a theorem about an element x in some set U, we often run into the problem that there does not seem to be enough information about x to proceed. For example, consider the following proposition:

Proposition 5.1. *If n is an integer, then $\left(n^2 + n\right)$ is an even integer.*

If we were trying to write a direct proof of this proposition, the only thing we could assume is that n is an integer. This is not much help. In a situation such as this, we will sometimes construct our own cases to provide additional assumptions for the forward process of the proof. Cases are usually based on some common properties that the given element may or may not possess. The cases must be chosen so that they exhaust all possibilities for the object in the hypothesis of the proposition. For the Proposition 5.1, we know that an integer must be even or it must be odd. We can thus use the following two cases for the integer n:

- The integer n is an even integer; or
- The integer n is an odd integer.

Proposition 5.1. *If n is an integer, then $\left(n^2+n\right)$ is an even integer.*

Proof. We assume that n is an integer and will prove that $\left(n^2+n\right)$. Since we know that any integer must be even or odd, we will use two cases. The first is that n is an even integer, and the second is that n is an odd integer.

In the case where n is an even integer, there exists an integer m such that

$$n = 2m.$$

Substituting this into the expression n^2+n yields

$$\begin{aligned} n^2+n &= (2m)^2+2m \\ &= 4m^2+2m \\ &= 2(2m^2+m) \end{aligned}$$

By the closure properties of the integers, $2m^2+m$ is an integer, and hence n^2+n is even. So this proves that when n is an even integer, n^2+n is an even integer.

In the case where n is an odd integer, there exists an integer k such that

$$n = 2k+1.$$

Substituting this into the expression n^2+n yields

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

By the closure properties of the integers, $2k^2+3k+1$ is an integer, and hence n^2+n is even. So this proves that when n is an odd integer, n^2+n is an even integer.

Since we have proved that n^2+n is even when n is even and when n is odd, we have proved that if n is an integer, then $\left(n^2+n\right)$ is an even integer. ■

5.1 Some Common Situations to Use Cases

When using cases in a proof, the main rule is that the cases must be chosen so that they exhaust all possibilities for an object x in the hypothesis of the original proposition. Following are some common uses of cases in proofs.

When the hypothesis is, "n is an integer."	Case 1: n is an even integer. Case 2: n is an odd integer.		
When the hypothesis is, "m and n are integers."	Case 1: m and n are even. Case 2: m is even and n is odd. Case 3: m is odd and n is even. Case 4: m and n are both odd.		
When the hypothesis is, "x is a real number."	Case 1: x is rational. Case 2: x is irrational.		
When the hypothesis is, "x is a real number."	Case 1: $x = 0$. Case 2: $x \neq 0$.	OR	Case 1: $x > 0$. Case 2: $x = 0$. Case 3: $x < 0$.
When the hypothesis is, "a and b are real numbers."	Case 1: $a = b$. Case 2: $a \neq b$.	OR	Case 1: $a > b$. Case 2: $a = b$. Case 3: $a < b$.

5.2 Using Cases with the Division Algorithm

An important result for the set of integers is known as the Division Algorithm. This is somewhat of a misnomer since it is stated in terms of addition and multiplication. The reason for this is that the set of integers is closed under addition and multiplication but is not closed under division. However, we have known for some time that when we divide one integer by another nonzero integer, we get a quotient and a remainder. For example, when we divide 337 by 6, we often write

$$\frac{337}{6} = 56 + \frac{1}{6}.$$

When we multiply both sides of this equation by 6, we get

$$337 = 6 \cdot 56 + 1.$$

When we are working within the system of integers, the second equation is preferred over the first since the second one uses only integers and the operations of

addition and multiplication, and the integers are closed under addition and multiplication. Following is a complete statement of the Division Algorithm.

The Division Algorithm
For all integers a and b with $b > 0$, there exist unique integers q and r such that

$$a = bq + r \text{ and } 0 \leq r < b.$$

So when we speak of **the quotient** and **the remainder** when we "divide an integer a by the positive integer b," we will always mean the quotient (q) and the remainder (r) guaranteed by the Division Algorithm. So the remainder r is the least nonnegative integer such that there exists an integer (quotient) q with $a = bq + r$.

The Division Algorithm can sometimes be used to construct cases that can be used to prove a statement that is true for all integers. We have done this when we divided the integers into the even integers and the odd integers since even integers have a remainder of 0 when divided by 2 and odd integers have a remainder of 1 when divided by 2.

Sometimes it is more useful to divide the integer a by an integer other than 2. For example, if a is divided by 3, there are three possible remainders: 0, 1, and 2. If a is divided by 4, there are four possible remainders: 0, 1, 2, and 3. The remainders form the basis for the cases.

If the hypothesis of a proposition is that "n is an integer," then we can use the Division Algorithm to claim that there are unique integers q and r such that

$$n = 3q + r \text{ and } 0 \leq r < 3.$$

We can then divide the proof into the following three cases: (1) $r = 0$; (2) $r = 1$; and (3) $r = 2$. This is done in Proposition 5.2.

Proposition 5.2. *If n is an integer, then 3 divides $n^3 - n$.*

Proof. Let n be an integer. We will show that 3 divides $n^3 - n$ by examining the three cases for the remainder when n is divided by 3. By the Division Algorithm, there exist unique integers q and r such that

$$n = 3q + r, \text{ and } 0 \leq r < 3.$$

This means that we can consider the following three cases: (1) $r = 0$; (2) $r = 1$; and (3) $r = 2$.

In the case where $r = 0$, we have $n = 3q$. By substituting this into the expression $n^3 - n$, we get

$$\begin{aligned} n^3 - n &= (3q)^3 - (3q) \\ &= 27q^3 - 3q \\ &= 3\left(9q^3 - q\right). \end{aligned}$$

Since $\left(9q^3 - q\right)$ is an integer, the last equation proves that $3 \mid \left(n^3 - n\right)$.

In the second case, $r = 1$ and $n = 3q + 1$. When we substitute this into $\left(n^3 - n\right)$, we obtain

$$\begin{aligned} n^3 - n &= (3q + 1)^3 - (3q + 1) \\ &= \left(27q^3 + 27q^2 + 9q + 1\right) - (3q + 1) \\ &= 27q^3 + 27q^2 + 6q \\ &= 3\left(9q^3 + 9q^2 + 2q\right). \end{aligned}$$

Since $\left(9q^3 + 9q^2 + 2q\right)$ is an integer, the last equation proves that $3 \mid \left(n^3 - n\right)$.

The last case is when $r = 2$. The details for this case are part of Problem (2). Once this case is completed, we will have proved that 3 divides $n^3 - n$ in all three cases. Hence, we may conclude that if n is an integer, then 3 divides $n^3 - n$. ■

5.3 Practice Problems for Chapter 5

1. Consider the following proposition:

Proposition. For each integer a, if 3 divides a^2, then 3 divides a.

(**a**) Write the contrapositive of this proposition.

(**b**) Prove the proposition by proving its contrapositive. **Hint**: Consider using cases based on the Division Algorithm using the remainder for "division by 3." There will be two cases since the hypothesis of the contrapositive is, "3 does not divide a."

2. Complete the details for the proof of Case 3 of Proposition 5.2.

3. Is the following proposition true or false? Justify your conclusion with a counterexample or a proof.

Proposition. For each integer n, if n is odd, then 8 divides $n^2 - 1$.

Chapter 6

Mathematical Induction

One of the defining characteristics of the set of natural numbers $\mathbb{N}$ is the so-called Principle of Mathematical Induction.

The Principle of Mathematical Induction
If T is a subset of $\mathbb{N}$ such that

1. $1 \in T$, and

2. For every $k \in \mathbb{N}$, if $k \in T$, then $(k + 1) \in T$,

then $T = \mathbb{N}$.

In many mathematics courses, this principle is given as an axiom for the set of natural numbers. Although we will not do so here, the Principle of Mathematical Induction can be proved by using the so-called Well-Ordering Principle, which states that every non-empty subset of the natural numbers contains a least element. So in some courses, the Well-Ordering Principle is stated as an axiom of the natural numbers. It should be noted, however, that it is also possible to assume the Principle of Mathematical Induction as an axiom and use it to prove the Well-Ordering Principle. We will only use the Principle of Mathematical Induction in this book.

6.1 Using the Principle of Mathematical Induction

The primary use of the Principle of Mathematical Induction is to prove statements of the form

$$(\forall n \in \mathbb{N})\,(P\,(n))\,,$$

where $P(n)$ is some open sentence. Recall that a universally quantified statement like the preceding one is true if and only if the truth set T of the open sentence $P(n)$ is the set $\mathbb{N}$. So our goal is to prove that $T = \mathbb{N}$, which is the conclusion of the Principle of Mathematical Induction. To verify the hypothesis of the Principle of Mathematical Induction, we must

1. Prove that $1 \in T$. That is, prove that $P(1)$ is true.
2. Prove that if $k \in T$, then $(k+1) \in T$. That is, prove that if $P(k)$ is true, then $P(k+1)$ is true.

The first step is called the **basis step** or the **initial step**, and the second step is called the **inductive step**. This means that a proof by mathematical induction will have the following form:

Procedure for a Proof by Mathematical Induction
To prove: $(\forall n \in \mathbb{N})\,(P\,(n))$

Basis step:	Prove $P(1)$.
Inductive step:	Prove that for each $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true.

We can then conclude that $P(n)$ is true for all $n \in \mathbb{N}$.

Note that in the inductive step, we want to prove that the conditional statement "for each $k \in \mathbb{N}$, if $P(k)$ then $P(k+1)$" is true. So we will start the inductive step by assuming that $P(k)$ is true. This assumption is called the **inductive assumption** or the **inductive hypothesis.**

The key to constructing a proof of the inductive step is to discover how $P(k+1)$ is related to $P(k)$ for an arbitrary natural number k. This is why it is important to write down explicitly what $P(k)$ and $P(k+1)$ are within the proof. Notice how this is done in the proof of the following proposition.

Proposition 6.1. *For each natural number n,*

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Proof. We will use a proof by mathematical induction. For each natural number n, we let $P(n)$ be

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

We first prove that $P(1)$ is true. Notice that $\frac{1\,(1+1)\,(2\cdot 1+1)}{6} = 1$. This shows that

$$1^2 = \frac{1\,(1+1)\,(2\cdot 1+1)}{6},$$

which proves that $P(1)$ is true.

For the inductive step, we prove that for each $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true. So let k be a natural number and assume that $P(k)$ is true. That is, assume that

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}. \tag{1}$$

The goal now is to prove that $P\,(k+1)$ is true. That is, it must be proved that

$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= \frac{(k+1)\,[(k+1)+1]\,[2(k+1)+1]}{6} \\ &= \frac{(k+1)\,(k+2)\,(2k+3)}{6}. \end{aligned} \tag{2}$$

To do this, we add $(k+1)^2$ to both sides of equation (1) and algebraically rewrite the right side of the resulting equation. This gives

$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\ &= \frac{(k+1)\,[k(2k+1) + 6(k+1)]}{6} \\ &= \frac{(k+1)\left(2k^2 + 7k + 6\right)}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6}. \end{aligned}$$

Comparing this result to equation (2), we see that if $P(k)$ is true, then $P(k+1)$ is true. Hence, the inductive step has been established, and by the Principle of Mathematical Induction, we have proved that for each natural number n, $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$. ■

6.2 The Extended Principle of Mathematical Induction

A little exploration shows that the following proposition appears to be true.

Proposition 6.2. *For each integer n with $n \geq 4$, $n! > n^4$.*

We would like to use mathematical induction to prove this, but the proposition has the added assumption that $n \geq 4$. So to do this, we use a slight modification of the Principle of Mathematical Induction called the Extended Principle of Mathematical Induction.

The Extended Principle of Mathematical Induction
Let M be an integer. If T is a subset of $\mathbb{Z}$ such that

1. $M \in T$, and
2. For every $k \in \mathbb{Z}$ with $k \geq M$, if $k \in T$, then $(k+1) \in T$,

then T contains all integers greater than or equal to M. That is, $\{n \in \mathbb{Z} \mid n \geq M\} \subseteq T$.

The primary use of the Principle of Mathematical Induction is to prove statements of the form

$$(\forall n \in \mathbb{Z}, \text{ with } n \geq M)\,(P(n)),$$

where M is an integer and $P(n)$ is some open sentence. (In most induction proofs, we will use a value of M that is greater than or equal to zero.) So our goal is to prove that the truth set T of the predicate $P(n)$ contains all integers greater than or equal to M. So to verify the hypothesis of the Extended Principle of Mathematical Induction, we must

1. Prove that $M \in T$. That is, prove that $P(M)$ is true.
2. Prove that for every $k \in \mathbb{Z}$ with $k \geq M$, if $k \in T$, then $(k+1) \in T$. That is, prove that if $P(k)$ is true, then $P(k+1)$ is true.

As before, the first step is called the **basis step** or the **initial step**, and the second step is called the **inductive step**. This means that a proof using the Extended Principle of Mathematical Induction will have the following form:

Using the Extended Principle of Mathematical Induction
Let M be an integer. To prove: $(\forall n \in \mathbb{Z} \text{ with } n \geq M)\,(P(n))$

Basis step: Prove $P(M)$.

Inductive step: Prove that for every $k \in \mathbb{Z}$ with $k \geq M$, if $P(k)$ is true, then $P(k+1)$ is true.

We can then conclude that $P(n)$ is true for all $n \in \mathbb{Z}$ with $n \geq M$.

This is basically the same procedure as the one for using the Principle of Mathematical Induction. The only difference is that the basis step uses an integer M other than 1. For this reason, when we write a proof that uses the Extended Principle of Mathematical Induction, we often simply say we are going to use a proof by mathematical induction. We will prove Proposition 6.2 using the Extended Principle of Mathematical Induction.

Proposition 6.2. *For each integer n with $n \geq 4$, $n! > n^4$.*

Proof. We will use a proof by mathematical induction. For this proof, we let

$$P(n) \text{ be "} n! > 2^n \text{."}$$

We first prove that $P(4)$ is true. Using $n = 4$, we see that $4! = 24$ and $2^4 = 16$. This means that $4! > 2^4$ and, hence, $P(4)$ is true.

For the inductive step, we prove that for all $k \in \mathbb{N}$ with $k \geq 4$, if $P(k)$ is true, then $P(k+1)$ is true. So let k be a natural number greater than or equal to 4, and assume that $P(k)$ is true. That is, assume that

$$k! > 2^k. \tag{1}$$

The goal is to prove that $P(k+1)$ is true or that $(k+1)! > 2^{k+1}$. Multiplying both sides of inequality (1) by $k+1$ gives

$$\begin{aligned} (k+1) \cdot k! &> (k+1) \cdot 2^k, \text{ or} \\ (k+1)! &> (k+1) \cdot 2^k. \end{aligned} \tag{2}$$

Now, $k \geq 4$. Thus, $k + 1 > 2$, and hence $(k + 1) \cdot 2^k > 2 \cdot 2^k$. This means that

$$(k + 1) \cdot 2^k > 2^{k+1}. \tag{3}$$

Inequalities (2) and (3) show that

$$(k + 1)! > 2^{k+1},$$

and this proves that if $P(k)$ is true, then $P(k + 1)$ is true. Thus, the inductive step has been established, and so by mathematical induction, we have proved that $n! > 2^n$ for each natural number n with $n \geq 4$. ■

6.3 The Second Principle of Mathematical Induction

Let $P(n)$ be

n is a prime number or n is a product of prime numbers.

Suppose we would like to use induction to prove that $P(n)$ is true for all natural numbers greater than 1. We have seen that the idea of the inductive step in a proof by induction is to prove that if one statement in an infinite list of statements is true, then the next statement must also be true. The problem here is that when we factor a composite number, we do not get to the previous case. For example, if assume that $P(39)$ is true and we want to prove that $P(40)$ is true, we could factor 40 as $40 = 2 \cdot 20$. So the assumption that $P(39)$ is true does not help us prove that $P(40)$ is true. What we would like to do is use $P(2)$ and $P(20)$.

This work is intended to show the need for another principle of induction. In the inductive step of a proof by induction, we assume one statement is true and prove the next one is true. The idea of this new principle is to assume that *all* of the previous statements are true and use this assumption to prove the next statement is true. This is stated formally in terms of subsets of natural numbers in the *Second Principle of Mathematical Induction*.

The Second Principle of Mathematical Induction
Let M be an integer. If T is a subset of $\mathbb{Z}$ such that

1. $M \in T$, and
2. For every $k \in \mathbb{Z}$ with $k \geq M$, if $\{M, M+1, \ldots, k\} \subseteq T$, then $(k+1) \in T$,

then T contains all integers greater than or equal to M. That is, $\{n \in \mathbb{Z} \mid n \geq M\} \subseteq T$.

The primary use of mathematical induction is to prove statements of the form

$$(\forall n \in \mathbb{Z}, \text{with } n \geq M)\,(P(n))\,,$$

where M is an integer and $P(n)$ is some predicate. (For most proofs, $M = 0$ or $M = 1$. So our goal is to prove that the truth set T of the predicate $P(n)$ contains all integers greater than or equal to M. To use the Second Principle of Mathematical Induction, we must

1. Prove that $M \in T$. That is, prove that $P(M)$ is true.
2. Prove that for every $k \in \mathbb{N}$, if $k \geq M$ and $\{M, M+1, \ldots, k\} \subseteq T$, then $(k+1) \in T$. That is, prove that if $P(M), P(M+1), \ldots, P(k)$ are true, then $P(k+1)$ is true.

As before, the first step is called the **basis step** or the **initial step**, and the second step is called the **inductive step**. This means that a proof using the Second Principle of Mathematical Induction will have the following form:

Using the Second Principle of Mathematical Induction
Let M be an integer. To prove: $(\forall n \in \mathbb{Z}$ with $n \geq M)\,(P(n))$

Basis step: Prove $P(M)$.

Inductive step: Let $k \in \mathbb{Z}$ with $k \geq M$. Prove that if $P(M), P(M+1), \ldots, P(k)$ are true, then $P(k+1)$ is true.

We can then conclude that $P(n)$ is true for all $n \in \mathbb{Z}$ with $n \geq M$.

We will use this procedure to prove the proposition to prove the following proposition.

Proposition 6.3. *Each natural number greater than 1 is either a prime number or is a product of prime numbers.*

Proof. We will use the Second Principle of Mathematical Induction. We let $P(n)$ be

$$n \text{ is either a prime number or } n \text{ is a product of prime numbers.}$$

For the basis step, $P(2)$ is true since 2 is a prime number.

To prove the inductive step, we let k be a natural number with $k \geq 2$. We assume that $P(2), P(3), \ldots, P(k)$ are true. That is, we assume that each of the natural numbers $2, 3, \ldots, k$ is a prime number or a product of prime numbers. The goal is to prove that $P(k+1)$ is true or that $(k+1)$ is a prime number or a product of prime numbers.

Case 1: If $(k+1)$ is a prime number, then $P(k+1)$ is true.

Case 2: If $(k+1)$ is not a prime number, then $(k+1)$ can be factored into a product of natural numbers with each one being less than $(k+1)$. That is, there exist natural numbers a and b with

$$k+1 = a \cdot b, \quad \text{and} \quad 1 < a \leq k \text{ and } 1 < b \leq k.$$

Using the inductive assumption, this means that $P(a)$ and $P(b)$ are both true. Consequently, a and b are prime numbers or are products of prime numbers. Since $k+1 = a \cdot b$, we conclude that $(k+1)$ is a product of prime numbers. That is, we conclude that $P\ (k+1)$ is true. This proves the inductive step.

Hence, by the Second Principle of Mathematical Induction, we conclude that $P(n)$ is true for all $n \in \mathbb{N}$ with $n \geq 2$, and this means that each natural number greater than 1 is either a prime number or is a product of prime numbers. ■

6.4 Practice Problems for Chapter 6

1. (**a**) Calculate $1 + 3 + 5 + \cdots + (2n-1)$ for several natural numbers n.

(**b**) Based on your work in part (a), if $n \in \mathbb{N}$, make a conjecture about the value of the sum $1 + 3 + 5 + \cdots + (2n-1) = \sum_{j=1}^{n} (2j-1)$.

(**c**) Use mathematical induction to prove your conjecture in part (b).

2. Prove the following:

Proposition. For each natural number n, 3 divides $4^n \equiv 1 \pmod 3$.

3. For which natural numbers n is 3^n greater than $5 + 2^n$? State a proposition (with an appropriate quantifier) and prove it.

4. The **Fibonacci numbers** are a sequence of natural numbers $f_1, f_2, f_3, \ldots, f_n, \ldots$ defined recursively as follows:

- $f_1 = 1$ and $f_2 = 1$, and
- For each natural number n, $f_{n+2} = f_{n+1} + f_n$.

In words, the recursion formula states that for any natural number n with $n \geq 3$, the n^{th} Fibonacci number is the sum of the two previous Fibonacci numbers. So we see that

$$\begin{aligned} f_3 &= f_2 + f_1 = 1 + 1 = 2, \\ f_4 &= f_3 + f_2 = 2 + 1 = 3, \text{ and} \\ f_5 &= f_4 + f_3 = 3 + 2 = 5. \end{aligned}$$

(**a**) Calculate f_6 through f_{20}.

(**b**) Is every third Fibonacci number even? That is it true that for each natural number n, f_{3n} is even? Justify your conclusion.

(**c**) Is it true that for each natural number n with $n \geq 2$, $f_1 + f_3 + \cdots + f_{2n-1} = f_{n+1} - 1$? Justify your conclusion.

5. Prove the following proposition using mathematical induction.

Proposition. For each $n \in \mathbb{N}$ with $n \geq 8$, there exist nonnegative integers x and y such that $n = 3x + 5y$.

Suggestion: Use the Second Principle of Induction and have the basis step be a proof that $P(8)$, $P(9)$, and $P(10)$ are true using an appropriate open sentence for $P(n)$.

Chapter 7

Injective and Surjective Functions

This chapter does not discuss a proof technique but applies some of the proof techniques from earlier in the book to propositions and problems dealing with functions, in particular, injections and surjections. These are concepts that some students struggle with when they first study them in an introduction to proofs course. So we give a few examples of such proofs in this chapter.

To understand the proofs discussed in this chapter, we need to understand functions and the definitions of an injection (one-to-one function) and a surjection (onto function). It is assumed that students have studied these concepts before, but the definitions are stated below for reference.

7.1 Definitions and Notation

Definition. A **function** from a set A to a set B is a rule that associates with each element x of the set A exactly one element of the set B. A function from A to B is also called a **mapping** from A to B.

Function Notation. When we work with a function, we usually give it a name. The name is often a single letter, such as f or g. If f is a function from the set A to be the set B, we will write $f: A \to B$. This is simply shorthand notation for the fact that f is a function from the set A to the set B. In this case, we also say that f maps A to B.

Definition. Let $f: A \to B$. (This is read, "Let f be a function from A to B.") The set A is called the **domain** of the function f, and we write $A = \text{dom}(f)$. The set B is called the **codomain** of the function f, and we write $B = \text{codom}(f)$.

If $a \in A$, then the element of B that is associated with a is denoted by $f(a)$ and is called the **image of a under f**. If $f(a) = b$, with $b \in B$, then a is called a **preimage of b under f**.

Some Function Terminology. When we have a function $f: A \to B$, we often write $y = f(x)$. In this case, we consider x to be an unspecified object that can be chosen from the set A, and we would say that x is the **independent variable** of the function f and y is the **dependent variable** of the function f.

Definition. Let $f: A \to B$. The set $\{f(x) \mid x \in A\}$ is called the **range of the function f** and is denoted by range (f). The range of f is sometimes called the **image of the function f** (or the **image of A under f**).

The range of $f: A \to B$ could equivalently be defined as follows:

$$\text{range}(f) = \{y \in B \mid y = f(x) \text{ for some } x \in A\}.$$

Notice that this means that $\text{range}(f) \subseteq \text{codom}(f)$ but does not necessarily mean that $\text{range}(f) = \text{codom}(f)$. Whether we have this set equality or not depends on the function f.

Definition. Let $f : A \to B$ be a function from the set A to the set B. The function f is called an **injection** provided that

$$\text{for all } x_1, x_2 \in A, \text{ if } x_1 \neq x_2, \text{ then } f(x_1) \neq f(x_2).$$

When f is an injection, we also say that f is a **one-to-one function**, or that f is an **injective function**.

Notice that the condition that specifies that a function f is an injection is given in the form of a conditional statement. As we shall see, in proofs, it is usually easier to use the contrapositive of this conditional statement.

Let $f: A \to B$.

"The function f is an injection" means that

- For all $x_1, x_2 \in A$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$; or
- For all $x_1, x_2 \in A$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$.

"The function f is not an injection" means that

- There exist $x_1, x_2 \in A$ such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$.

Definition. Let $f: A \to B$ be a function from the set A to the set B. The function f is called a **surjection** provided that the range of f equals the codomain of f. This means that

for every $y \in B$, there exists an $x \in A$ such that $f(x) = y$.

When f is a surjection, we also say that f is an **onto function** or that f maps A **onto** B. We also say that f is a **surjective function**.

One of the conditions that specifies that a function f is a surjection is given in the form of a universally quantified statement, which is the primary statement used in proving a function is (or is not) a surjection.

Let $f: A \to B$.

"The function f is a surjection" means that

- range(f) = codom$(f) = B$; or
- For every $y \in B$, there exists an $x \in A$ such that $f(x) = y$.

"The function f is not a surjection" means that

- range$(f) \neq$ codom(f); or
- There exists a $y \in B$ such that for all $x \in A$, $f(x) \neq y$.

One last definition.

Definition. A **bijection** is a function that is both an injection and a surjection. If the function f is a bijection, we also say that f is **one-to-one and onto** and that f is a **bijective function**.

7.2 Some Examples and Proofs

Many of us have probably heard in precalculus and calculus courses that a linear function is a bijection. We prove this in the following proposition, but notice how careful we are with stating the domain and codomain of the function.

Proposition 7.1. *Let The function $f:\mathbb{R}\to\mathbb{R}$ by $f(x)=mx+b$ for all x in $\mathbb{R}$ is a bijection.*

Proof. We let m be a nonzero real number and let b be a real number and define $f:\mathbb{R}\to\mathbb{R}$ by $f(x)=mx+b$ for all x in $\mathbb{R}$. We will prove that f is a bijection by proving it is both an injection and a surjection.

To prove that f is an injection, we let x_1 and x_2 be real numbers (hence, in the domain of f) and assume that $f(x_1)=f(x_2)$. This means that $mx_1+b=mx_2+b$. We can then subtract b from both sides of this equation and then divide both sides by m since $m\neq 0$ as follows:

$$\begin{aligned} mx_1+b &= mx_2+b \\ mx_1 &= mx_2 \\ x_1 &= x_2 \end{aligned}$$

So we have proved that for all $x_1, x_2\in\mathbb{R}$, if $f(x_1)=f(x_2)$, then $x_1=x_2$, and hence, f is an injection.

To prove that f is a surjection, we choose a real number y in the codomain of f. We need to prove that there exists an $x\in\mathbb{R}$ such that $f(x)=y$. Working backward, we see that if $mx+b=y$, then $x=\dfrac{y-b}{m}$ (since $m\neq 0$). We see that $x\in\mathbb{R}$ (the domain of f) since the real numbers are closed under subtraction and

division by nonzero real numbers. This is done as follows:

$$\begin{aligned} f(x) &= f\left(\frac{y-b}{m}\right) \\ &= m\left(\frac{y-b}{m}\right) + b \\ &= (y-b) + b \\ &= b \end{aligned}$$

This proves that for each $y \in \mathbb{R}$, there exists an $x \in \mathbb{R}$ such that $f(x) = y$, and hence, f is a surjection.

Since we have proved that f is both an injection and a surjection, we have proved that f is a bijection. ■

We will now discuss some examples of functions that will illustrate why the domain and the codomain of a function are just as important as the rule defining the outputs of a function when we need to determine if the function is an injection or a surjection.

Example 7.2 (**The Importance of the Domain and Codomain**)
Each of the following functions will have the same rule for computing the outputs corresponding to a given input. However, they will have different domains or different codomains.

1. **A Function that Is Neither an Injection nor a Surjection**
   Let $f: \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 + 1$. Notice that

   $$f(2) = 5 \text{ and } f(-2) = 5.$$

   This is enough to prove that the function f is not an injection since this shows that there exist two different inputs that produce the same output.

   Since $f(x) = x^2 + 1$, we know that $f(x) \geq 1$ for all $x \in \mathbb{R}$. This implies that the function f is not a surjection. For example, -2 is in the codomain of f and $f(x) \neq -2$ for all x in the domain of f.

2. **A Function that Is Not an Injection but Is a Surjection**]
   Let $T = \{y \in \mathbb{R} \mid y \geq 1\}$, and define $F: \mathbb{R} \to T$ by $F(x) = x^2 + 1$. As in Example 1, the function F is not an injection since $F(2) = F(-2) = 5$.

   Is the function F a surjection? That is, does F map $\mathbb{R}$ onto T? As in Example 1, we do know that $F(x) \geq 1$ for all $x \in \mathbb{R}$.

To see if it is a surjection, we must determine if it is true that for every $y \in T$, there exists an $x \in \mathbb{R}$ such that $F(x) = y$. So we choose $y \in T$. The goal is to determine if there exists an $x \in \mathbb{R}$ such that

$$F(x) = y, \text{ or}$$
$$x^2 + 1 = y.$$

One way to proceed is to work backward and solve the last equation (if possible) for x. Doing so, we get

$$x^2 = y - 1$$
$$x = \sqrt{y-1} \text{ or } x = -\sqrt{y-1}.$$

Now, since $y \in T$, we know that $y \geq 1$ and hence that $y - 1 \geq 0$. This means that $\sqrt{y-1} \in \mathbb{R}$. Hence, if we use $x = \sqrt{y-1}$, then $x \in \mathbb{R}$, and

$$\begin{aligned} F(x) &= F\left(\sqrt{y-1}\right) \\ &= \left(\sqrt{y-1}\right)^2 + 1 \\ &= (y-1) + 1 \\ &= y. \end{aligned}$$

This proves that F is a surjection since we have shown that for all $y \in T$, there exists an $x \in \mathbb{R}$ such that $F(x) = y$. Notice that for each $y \in T$, this was a constructive proof of the existence of an $x \in \mathbb{R}$ such that $F(x) = y$.

An Important Lesson. In Examples 1 and 2, the same mathematical formula was used to determine the outputs for the functions. However, one function was not a surjection and the other one was a surjection. This illustrates the important fact that whether a function is surjective not only depends on the formula that defines the output of the function but also on the domain and codomain of the function.

3. A Function that Is an Injection but Is Not a Surjection]
Let $\mathbb{Z}^* = \{x \in \mathbb{Z} \mid x \geq 0\} = \mathbb{N} \cup \{0\}$. Define $g: \mathbb{Z}^* \to \mathbb{N}$ by $g(x) = x^2 + 1$. (Notice that this is the same formula used in Examples 1 and 2.) Following is a table of values for some inputs for the function g.

x	$g(x)$
0	1
1	2
2	5

x	$g(x)$
3	10
4	17
5	26

Notice that the codomain is $\mathbb{N}$, and the table of values suggests that some natural numbers are not outputs of this function. So it appears that the function g is not a surjection.

To prove that g is not a surjection, pick an element of $\mathbb{N}$ that does not appear to be in the range. We will use 3, and we will use a proof by contradiction to prove that there is no x in the domain ($\mathbb{Z}^*$) such that $g(x) = 3$. So we assume that there exists an $x \in \mathbb{Z}^*$ with $g(x) = 3$. Then

$$\begin{aligned} x^2 + 1 &= 3 \\ x^2 &= 2 \\ x &= \pm\sqrt{2}. \end{aligned}$$

But this is not possible since $\sqrt{2} \notin \mathbb{Z}^*$. Therefore, there is no $x \in \mathbb{Z}^*$ with $g(x) = 3$. This means that for every $x \in \mathbb{Z}^*$, $g(x) \neq 3$. Therefore, 3 is not in the range of g, and hence g is not a surjection.

The table of values suggests that different inputs produce different outputs, and hence that g is an injection. To prove that g is an injection, assume that $s, t \in \mathbb{Z}^*$ (the domain) with $g(s) = g(t)$. Then

$$\begin{aligned} s^2 + 1 &= t^2 + 1 \\ s^2 &= t^2. \end{aligned}$$

Since $s, t \in \mathbb{Z}^*$, we know that $s \geq 0$ and $t \geq 0$. So the preceding equation implies that $s = t$. Hence, g is an injection.

An Important Lesson. The functions in the three preceding examples all used the same formula to determine the outputs. The functions in Examples 1 and 2 are not injections but the function in Example 3 is an injection. This illustrates the important fact that whether a function is injective not only depends on the formula that defines the output of the function but also on the domain of the function.

7.3 Practice Problems for Chapter 7

1. Let $R^+ = \{y \in \mathbb{R} \mid y > 0\}$. Define

$f: \mathbb{R} \to \mathbb{R}$ by $f(x) = e^{-x}$, for each $x \in \mathbb{R}$, and

$g: \mathbb{R} \to \mathbb{R}^+$ by $g(x) = e^{-x}$, for each $x \in \mathbb{R}$.

Determine if each of these functions is an injection or a surjection. Justify your conclusions. **Note**: Before writing proofs, it might be helpful to draw the graph of $y = e^{-x}$. A reasonable graph can be obtained using $-3 \leq x \leq 3$ and $-2 \leq y \leq 10$. Please keep in mind that the graph does not prove any conclusion, but may help us arrive at the correct conclusions, which will still need proof.

2. For each of the following functions, determine if the function is an injection or a surjection (or both, and hence, a bijection). Justify all conclusions.

(**a**) $F: \mathbb{R} \to \mathbb{R}$ defined by $F(x) = 5x + 3$, for all $x \in \mathbb{R}$.

(**b**) $G: \mathbb{Z} \to \mathbb{Z}$ defined by $G(x) = 5x + 3$, for all $x \in \mathbb{Z}$.

(**c**) $f: (\mathbb{R} - \{4\}) \to \mathbb{R}$ defined by $f(x) = \dfrac{3x}{x-4}$, for all $x \in (\mathbb{R} - \{4\})$.

(**d**) $g: (\mathbb{R} - \{4\}) \to (\mathbb{R} - \{3\})$ defined by $g(x) = \dfrac{3x}{x-4}$, for all $x \in (\mathbb{R} - \{4\})$.

3. Let s be the function that associates with each natural number the sum of its distinct natural number divisors. This is called the **sum of the divisors function**. For example, the natural number divisors of 6 are 1, 2, 3, and 6, and so

$$\begin{aligned} s(6) &= 1 + 2 + 3 + 6 \\ &= 12. \end{aligned}$$

(**a**) Calculate $s(k)$ for each natural number k from 1 through 15.

(**b**) Is the sum of the divisors function an injection? Is it a surjection? Justify your conclusions.

4. Let $\mathcal{M}_2(\mathbb{R})$ represent the set of all 2 by 2 matrices over $\mathbb{R}$.

(**a**) Define $\det: \mathcal{M}_2(\mathbb{R}) \to \mathbb{R}$ by

$$\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc.$$

This is the **determinant function** on the set of 2 by 2 matrices over the real numbers. Is the determinant function an injection? Is the determinant function a surjection? Justify your conclusions.

(**b**) Define tran: $\mathcal{M}_2(\mathbb{R}) \to \mathcal{M}_2(\mathbb{R})$ by

$$\text{tran}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = A^T = \begin{bmatrix} a & c \\ b & d \end{bmatrix}.$$

This is the **transpose function** on the set of 2 by 2 matrices over the real numbers. Is the transpose function an injection? Is the transpose function a surjection? Justify your conclusions.

(**c**) Define $F: \mathcal{M}_2(\mathbb{R}) \to \mathbb{R}$ by

$$F\begin{bmatrix} a & b \\ c & d \end{bmatrix} = a^2 + d^2 - b^2 - c^2.$$

Is the function F an injection? Is the function F a surjection? Justify your conclusions.

Appendix A

Guidelines for Writing Mathematical Proofs

One of the most important forms of mathematical writing is writing mathematical proofs. The writing of mathematical proofs is an acquired skill and takes a lot of practice.

Following is a summary of all the writing guidelines introduced in the text. This summary contains some standard conventions that are usually followed when writing a mathematical proof.

1. **Know your audience**. Every writer should have a clear idea of the intended audience for a piece of writing. In that way, the writer can give the right amount of information at the proper level of sophistication to communicate effectively. This is especially true for mathematical writing. For example, if a mathematician is writing a solution to a textbook problem for a solutions manual for instructors, the writing would be brief with many details omitted. However, if the writing was for a students' solution manual, more details would be included.

2. **Begin with a carefully worded statement of the theorem or result to be proven.** The statement should be a simple declarative statement of the problem. Do not simply rewrite the problem as stated in the textbook or given on a handout. Problems often begin with phrases such as "Show that" or "Prove that." This should be reworded as a simple declarative statement of the theorem. Then skip a line and write "Proof" in italics or boldface font (when using a word processor). Begin the proof on the same line. Make sure that

all paragraphs can be easily identified. Skipping a line between paragraphs or indenting each paragraph can accomplish this.

As an example, an exercise in a text might read, "Prove that if x is an odd integer, then x^2 is an odd integer." This could be started as follows:

Theorem. If x is an odd integer, then x^2 is an odd integer.

Proof: We assume that x is an odd integer ....

3. **Begin the proof with a statement of your assumptions.** Follow the statement of your assumptions with a statement of what you will prove.

   Proof. We assume that x and y are odd integers and will prove that $x \cdot y$ is an odd integer.

4. **Use the pronoun "we."** If a pronoun is used in a proof, the usual convention is to use "we" instead of "I." The idea is to stress that you and the reader are doing the mathematics together. It will help encourage the reader to continue working through the mathematics. Notice that we started the proof of the theorem at the end of item (2) with "We assume that ...."

5. **Use italics for variables when using a word processor.** When using a word processor to write mathematics, the word processor needs to be capable of producing the appropriate mathematical symbols and equations. The mathematics that is written with a word processor should look like typeset mathematics. This means that variables need to be italicized, boldface is used for vectors, and regular font is used for mathematical terms such as the names of the trigonometric functions and logarithmic functions.

   For example, we do not write sin x or $sin\ x$. The proper way to typeset this is $\sin x$.

6. **Do not use $*$ for multiplication or ^ for exponents.** Leave this type of notation for writing computer code. The use of this notation makes it difficult for humans to read. In addition, avoid using / for division when using a complex fraction.

   For example, it is very difficult to read $\left(x^3 - 3x^2 + 1/2\right) / (2x/3 - 7)$; the fraction

   $$\frac{x^3 - 3x^2 + \dfrac{1}{2}}{\dfrac{2x}{3} - 7}$$

   is much easier to read.

7. **Use complete sentences and proper paragraph structure.** Good grammar is an important part of any writing. Therefore, conform to the accepted rules of grammar. Pay careful attention to the structure of sentences. Write proofs using **complete sentences** but avoid run-on sentences. Also, do not forget punctuation, and always use a spell checker when using a word processor.

8. **Keep the reader informed.** Sometimes a theorem is proven by proving the contrapositive or by using a proof by contradiction. If either proof method is used, this should be indicated within the first few lines of the proof. This also applies if the result is going to be proven using mathematical induction.

   Examples:

   - We will prove this result by proving the contrapositive of the statement.
   - We will prove this statement using a proof by contradiction.
   - We will assume to the contrary that ....
   - We will use mathematical induction to prove this result.

   In addition, make sure the reader knows the status of every assertion that is made. That is, make sure it is clearly stated whether an assertion is an assumption of the theorem, a previously proven result, a well-known result, or something from the reader's mathematical background.

9. **Display important equations and mathematical expressions.** Equations and manipulations are often an integral part of the exposition. Do not write equations, algebraic manipulations, or formulas in one column with reasons given in another column (as is often done in geometry texts). Important equations and manipulations should be displayed. This means that they should be centered with blank lines before and after the equation or manipulations, and if one side of an equation does not change, it should not be repeated. For example,

   Using algebra, we obtain

$$\begin{aligned} x \cdot y &= (2m+1)(2n+1) \\ &= 4mn + 2m + 2n + 1 \\ &= 2(2mn + m + n) + 1. \end{aligned}$$

   Since m and n are integers, we conclude that ....

10. **Equation numbering guidelines.** If it is necessary to refer to an equation later in a proof, that equation should be centered and displayed, and it should be given a number. The number for the equation should be written in parentheses on the same line as the equation at the right-hand margin.

    Example:

    Since x is an odd integer, there exists an integer n such that

    $$x = 2n + 1. \tag{1}$$

    Later in the proof, there may be a line such as

    Then, using the result in equation (1), we obtain . . . .

    Please note that we should only number those equations we will be referring to later in the proof. Also, note that the word "equation" is not capitalized when we are referring to an equation by number. Although it may be appropriate to use a capital "E," the usual convention in mathematics is not to capitalize.

11. **Do not use a mathematical symbol at the beginning of a sentence.** For example, we should not write, "Let n be an integer. n is an odd integer provided that . . . ." Many people find this hard to read and often have to reread it to understand it. It would be better to write, "An integer n is an odd integer provided that . . . ."

12. **Use English and minimize the use of cumbersome notation**. Do not use the special symbols for quantifiers $\forall$ (for all), $\exists$ (there exists), $\ni$ (such that), or $\therefore$ (therefore) in formal mathematical writing. It is often easier to write, and usually easier to read, if the English words are used instead of the symbols. For example, why make the reader interpret

    $$(\forall x \in \mathbb{R})\,(\exists y \in \mathbb{R})\,(x + y = 0)$$

    when it is possible to write

    For each real number x, there exists a real number y such that $x + y = 0$,

    or more succinctly (if appropriate)

    Every real number has an additive inverse.

13. **Tell the reader when the proof has been completed.** Perhaps the best way to do this is to say outright that, "This completes the proof." Although it may seem repetitive, a good alternative is to finish a proof with a sentence that states precisely what has been proven. In any case, it is usually good practice to use some "end of proof symbol" such as ■.

14. **Keep it simple.** It is often difficult to understand a mathematical argument no matter how well it is written. Do not let your writing help make it more difficult for the reader. Use simple, declarative sentences and short paragraphs, each with a simple point.

15. **Write a first draft of your proof and then revise it.** Remember that a proof is written so that readers are able to read and understand the reasoning in the proof. Be clear and concise. Include details but do not ramble. Do not be satisfied with the first draft of a proof. Read it over and refine it. Just like any worthwhile activity, learning to write mathematics well takes practice and hard work. This can be frustrating. Everyone can be sure that there will be some proofs that are difficult to construct, but remember that proofs are a very important part of mathematics. So work hard and have fun.

Appendix B

Answers and Hints for the Practice Problems

Chapter 2

1. A counterexample for this statement will be values of a and b for which 5 divides a or 5 divides b, and 5 does not divide $5a + b$. One counterexample for the statement is $a = 5$ and $b = 1$. For these values, the hypothesis is true since 5 divides a and the conclusion is false since $5a + b = 26$ and 5 does not divide 26.

2. All examples should indicate the proposition is true. Following is a proof.

Proof. We assume that m is an odd integer and will prove that $\left(3m^2 + 4m + 6\right)$. Since m is an odd integer, there exists an integer k such that $m = 2k + 1$. Substituting this into the expression $\left(3m^2 + 4m + 6\right)$ and using algebra, we obtain

$$\begin{aligned} 3m^2 + 4m + 6 &= 3\left(2k + 1\right)^2 + 4\left(2k + 1\right) + 6 \\ &= \left(12k^2 + 12k + 3\right) + \left(8k + 4\right) + 6 \\ &= 12k^2 + 20k + 13 \\ &= 12k^2 + 20k + 12 + 1 \\ &= 2\left(6k^2 + 10k + 6\right) + 1 \end{aligned}$$

By the closure properties of the integers, $\left(6k^2 + 10k + 6\right)$ is an integer, and hence, the last equation shows that $3m^2 + 4m + 6$ is an odd integer.

This proves that if m is an odd integer, then $\left(3m^2 + 4m + 6\right)$ is an odd integer. ■

3. ***Proof.*** We let m be a real number and assume that m, $m + 1$, and $m + 2$ are the lengths of the three sides of a right triangle. We will use the Pythagorean Theorem to prove that $m = 3$. Since the hypotenuse is the longest of the three sides, the Pythagorean Theorem implies that $m^2+(m+1)^2 = (m+2)^2$. We will now use algebra to rewrite both sides of this equation as follows:

$$\begin{aligned} m^2 + \left(m^2 + 2m + 1\right) &= m^2 + 4m + 4 \\ 2m^2 + 2m + 1 &= m^2 + 4m + 4 \end{aligned}$$

The last equation is a quadratic equation. To solve for m, we rewrite the equation in standard form and then factor the left side. This gives

$$\begin{aligned} m^2 - 2m - 3 &= 0 \\ (m - 3)(m + 1) &= 0 \end{aligned}$$

The two solutions of this equation are $m = 3$ and $m = -1$. However, since m is the length of a side of a right triangle, m must be positive and we conclude that $m = 3$. This proves that if m, $m+1$, and $m+2$ are the lengths of the three sides of a right triangle, then $m = 3$. ■

4. For both parts, we assume that n is a natural number and a, b, c, and d are integers and that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. We can then conclude that n divides $a - b$ and n divides $c - d$. So there exist integers k and m such that

$$\begin{aligned} a - b &= kn \quad \text{and} \quad c - d = mn \\ a &= b + kn \quad \text{and} \quad c = d + mn \end{aligned}$$

(**a**) We then see that

$$\begin{aligned} (a + c) - (b + d) &= (a - b) + (c - d) \\ &= kn + mn \\ &= (k + m)n \end{aligned}$$

Since the integers are closed under addition, $k + m$ is an integer and the last equation proves that $a + c \equiv b + d \pmod{n}$.

(**b**) We then see that

$$\begin{aligned} ac - bd &= (b + kn)(d + mn) - bd \\ &= (bd + bmn + knd + kmn^2) - bd \\ &= (bm + kd + kmn)n \end{aligned}$$

Since the integers are closed under addition and multiplication, $(bm + kn + kmn)$ is an integer and the last equation proves that $ac \equiv bd \pmod{n}$.

5. The proposition is true. Use the choose-an-element method to prove that each set is a subset of the other set.

Proof. Let A and B be subsets of some universal set. We will prove that $A - (A - B) = A \cap B$ by proving that $A - (A - B) \subseteq A \cap B$ and that $A \cap B \subseteq A - (A - B)$.

First, let $x \in A - (A - B)$. This means that

$$x \in A \text{ and } x \notin (A - B).$$

We know that an element is in $(A - B)$ if and only if it is in A and not in B. Since $x \notin (A - B)$, we conclude that $x \notin A$ or $x \in B$. However, we also know that $x \in A$ and so we conclude that $x \in B$. This proves that

$$x \in A \text{ and } x \in B.$$

This means that $x \in A \cap B$, and hence we have proved that $A - (A - B) \subseteq A \cap B$.

Now choose $y \in A \cap B$. This means that

$$y \in A \text{ and } y \in B.$$

We note that $y \in (A - B)$ if and only if $y \in A$ and $y \notin B$ and hence, $y \notin (A - B)$ if and only if $y \notin A$ or $y \in B$. Since we have proved that $y \in B$, we conclude that $y \notin (A - B)$, and hence, we have established that $y \in A$ and $y \notin (A - B)$. So, $y \in A - (A - B)$, and this proves that if $y \in A \cap B$, then $y \in A - (A - B)$ and hence, $A \cap B \subseteq A - (A - B)$.

Since we have proved that $A - (A - B) \subseteq A \cap B$ and $A \cap B \subseteq A - (A - B)$, we conclude that $A - (A - B) = A \cap B$. ■

Chapter 3

1. ***Proof.*** We will prove that for all integers a and b, if ab is even, then a is even or b is even by proving its contrapositive, which is:

> For all integers a and b, if a is odd and b is odd, then ab is odd.

So we assume that both a and b are odd integers and will prove that ab is an odd integer. Since a and b are odd, there exist integers k and m such that $a = 2k + 1$ and $b = 2m + 1$. Using substitution and algebra, we then see that

$$\begin{aligned} ab &= (2k + 1)(2m + 1) \\ &= 4km + 2k + 2m + 1 \\ &= 2(2km + k + m) + 1 \end{aligned}$$

Since k and m are integers, the closure properties of the integers allow us to conclude that $(2km + k + m)$ is an integer. This means that ab has been written as two times an integer plus 1, and hence ab is an odd integer. This proves that for all integers a and b, if a is odd and b is odd, then ab is odd, which is the contrapositive of the proposition. So we have proved that For all integers a and b, if ab is even, then a is even or b is even. ■

2. (**a**) ***Proof.*** We assume that a is an integer and that $a \equiv 2 \pmod 5$ and will prove that $a^2 \equiv 4 \pmod 5$. Since $a \equiv 2 \pmod 5$, then there exists an integer k such that $a - 2 = 5k$ and so $a = 2 + 5k$. Then,

$$\begin{aligned} a^2 - 4 &= (2 + 5k)^2 - 4 \\ &= 20k + 25k^2 \\ &= 5\left(4k + 5k^2\right) \end{aligned}$$

Since the integers are closed under addition and multiplication, $\left(4k + 5k^2\right)$ is an integer, and so the last equation proves that 5 divides $a^2 - 4$. Hence, $a^2 \equiv 4 \pmod 5$, and this proves that for each integer a, if $a \equiv 2 \pmod 5$, then $a^2 \equiv 4 \pmod 5$. ■

(**b**) This statement is false. A counterexample is $a = 3$ since $3^2 \equiv 4 \pmod 5$ and $3 \not\equiv 2 \pmod 5$.

(**c**) This statement is false since the statement in Part (b) is false.

3. ***Proof.*** We will prove the contrapositive of this statement, which is

For each positive real number x, if $\sqrt{x}$ is rational, then x is rational.

So we assume that x is a rational number and that $\sqrt{x}$ is rational, and will prove that x is rational. Since $\sqrt{x}$ is rational, there exist positive integers m and n such that $\sqrt{x} = \frac{m}{n}$, then $x = \frac{m^2}{n^2}$. Since m and n are positive integers, m^2 and n^2 are positive integers and we can conclude that x is a rational number. This proves the contrapositive of the statement and so we have proved that for each positive real number x, if x is irrational, then $\sqrt{x}$ is irrational. ■

Chapter 4

1. (**a**) Some integers that are congruent to 2 modulo 4 are $-6, -2, 2, 6, 10$. None of these integers are congruent to 3 modulo 6. For example, $10 \not\equiv 3 \pmod 6$ since $10 - 3 = 7$ and 6 does not divide 7.

(**b**) ***Proof.*** We will use a proof by contradiction. Let $n \in \mathbb{Z}$ and assume that $n \equiv 2 \pmod 4$ and that $n \equiv 3 \pmod 6$. Since $n \equiv 2 \pmod 4$, we know that 4 divides $n-2$. Hence, there exists an integer k such that

$$n - 2 = 4k. \tag{1}$$

We can also use the assumption that $n \equiv 3 \pmod 6$ to conclude that 6 divides $n - 3$ and that there exists an integer m such that

$$n - 3 = 6m. \tag{2}$$

If we now solve equations (1) and (2) for n and set the two expressions equal to each other, we obtain

$$4k + 2 = 6m + 3.$$

However, this equation can be rewritten as

$$2(2k + 1) = 2(3m + 1) + 1.$$

Since $2k + 1$ is an integer and $3m + 1$ is an integer, this last equation is a contradiction since the left side is an even integer and the right side is an odd integer. Hence, we have proven that if $n \equiv 2 \pmod 4$, then $n \not\equiv 3 \pmod 6$. ■

2. ***Proof.*** We will use a proof by contradiction. So we assume that there exist real numbers x and y such that x is rational, y is irrational, and $x + y$ is rational. Since x is rational, we know that $-x$ is rational. Since the rational numbers are closed under addition, we know that $(-x) + (x + y$ is rational, and we see that

$$\begin{aligned}(-x) + (x + y) &= ((-x) + x) + y \\ &= 0 + y \\ &= y\end{aligned}$$

However, this shows that y must be a rational number, but we have also assumed that y is irrational. Since a real number cannot be both rational and irrational, this is a contradiction. We have therefore proved that for all real numbers x and y, if x is rational and y is irrational, then $x + y$ is irrational. ■

3. We will use a proof by contradiction to prove that $\log_2(3)$ is an irrational number.

So we assume that $\log_2(3)$ is a rational number. So, if $\log_2(3) = a$, then $2^a = 3$. This means that a is a positive rational number, and hence, there exist natural numbers m and n such that $2^{m/n} = 3$. Hence,

$$\left(2^{m/n}\right)^n = 3^n,$$

From this, we conclude that $2^m = 3^n$. However, 2^m is an even integer and 3^n is an odd integer. This is a contradiction, and so we have proved that $\log_2(3)$ is an irrational number.

4. We will use a proof by contradiction to prove that $\sqrt{2} + \sqrt{3}$ is an irrational number. So we assume that $\sqrt{2} + \sqrt{3}$ is a rational number and so we can write $\sqrt{2} + \sqrt{3} = r$, where r is a rational number and $r \neq 0$. We now rewrite this equation and then square both sides of the resulting equation to obtain

$$\begin{aligned}\sqrt{3} &= r - \sqrt{2} \\ 3 &= r^2 - 2r\sqrt{2} + 2\end{aligned}$$

We continue and rewrite this equation to isolate $\sqrt{2}$ on one side of the equation.

$$\begin{aligned}2r\sqrt{2} &= r^2 - 1 \\ \sqrt{2} &= \frac{r^2 - 1}{2r}\end{aligned}$$

Since $r \neq 0$, $2r \neq 0$, and since the rational numbers are closed under division by a nonzero rational number, the last equation shows that $\sqrt{2}$ is a rational number. This is a contradiction since it is known that $\sqrt{2}$ is irrational. This proves that $\sqrt{2} + \sqrt{3}$ is an irrational number.

Chapter 5

1. ***Proof.*** We will prove the contrapositive of this proposition, which is:

For each integer a, if 3 does not divide a, then 3 does not divide a^2.

So we let a be an integer, assume that 3 does not divide a, and will prove that 3 does not divide a^2. Since 3 does not divide a, we can use the Division Algorithm to conclude that there exists an integer q such that $a = 3q + 1$ or $a = 3q + 2$.

For the case where $a = 3q + 1$, we obtain

$$\begin{aligned} a^2 &= (3q+1)^2 \\ &= 9q^2 + 6q + 1 \\ &= 3\left(3q^2 + 2q\right) + 1 \end{aligned}$$

By the closure properties of the integers $\left(3q^2 + 2q\right)$ is an integer, and so the last equation means that a^2 has a remainder of 1 when divided by 3 and so 3 does not divide a^2.

For the case where $a = 3q + 2$, we obtain

$$\begin{aligned} a^2 &= (3q+2)^2 \\ &= 9q^2 + 12q + 4 \\ &= 3\left(3q^2 + 4q + 1\right) + 1 \end{aligned}$$

By the closure properties of the integers $\left(3q^2 + 4q + 1\right)$ is an integer, and so the last equation means that a^2 has a remainder of 1 when divided by 3 and so 3 does not divide a^2.

Since we have proved that 3 does not divide a^2 in both cases, we have proved the contrapositive of the proposition, and hence, we have proved that for each integer a, if 3 divides a^2, then 3 divides a. ■

2. For the third case, $r = 2$ and $n = 3q + 2$. When we substitute this into $\left(n^3 - n\right)$, we obtain

$$\begin{aligned} n^3 - n &= (3q+2)^3 - (3q+2) \\ &= \left(27q^3 + 54q^2 + 36q + 8\right) - (3q+2) \\ &= 27q^3 + 54q^2 + 33q + 6 \\ &= 3\left(9q^3 + 18q^2 + 11q + 2\right). \end{aligned}$$

Since $\left(9q^3 + 18q^2 + 11q + 2\right)$ is an integer, the last equation proves that $3 \mid \left(n^3 - n\right)$.

3. ***Proof.*** We let n be an integer, assume that n is odd, and will prove that 8 divides $n^2 - 1$. Since n is odd, there exists an integer k such that $n = 2k + 1$. We then see that

$$\begin{aligned} n^2 - 1 &= (2k+1)^2 - 1 \\ &= 4k^2 + 4k \\ &= 4k(k+1) \end{aligned} \tag{1}$$

We also know since k is an integer, either k or $k + 1$ is even. In either case, the product $k(k + 1)$ must be even and so there exists an integer q such that

$$k(k+1) = 2q.$$

Substituting this into the right side of equation (1), we obtain $n^2 - 1 = 8q$ and so 8 divides $n^2 - 1$. This proves that for each integer n, if n is odd, then 8 divides $n^2 - 1$. ■

Chapter 6

1. **Proposition**. For each natural number n, $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

Proof. We will use a proof by mathematical induction. For each natural number n, we let $P(n)$ be

$$1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

We first prove that $P(1)$ is true. Notice that when $n = 1$, both the left and right sides of the equation for $P(n)$ are equal to 1. This proves that $P(1)$ is true.

For the inductive step, we prove that for each $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true. So let k be a natural number and assume that $P(k)$ is true. That is, assume that

$$1 + 3 + 5 + \cdots + (2k-1) = k^2. \tag{1}$$

The goal now is to prove that $P(k+1)$ is true. That is, it must be proved that

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2k-1) + (2(k+1)-1) &= (k+1)^2 \\ 1 + 3 + 5 + \cdots + (2k-1) + (2k+1) &= (k+1)^2 \end{aligned} \tag{2}$$

To do this, we add $(2k+1)$ to both sides of equation (1), which gives

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2k-1) + (2k+1) &= k^2 + 2k + 1 \\ &= (k+1)^2 \end{aligned}$$

Comparing this result to equation (2), we see that if $P(k)$ is true, then $P(k+1)$ is true. Hence, the inductive step has been established, and by the Principle of Mathematical Induction, we have proved that for each natural number n, $1 + 3 + 5 + \cdots + (2n-1) = n^2$. ■

2. ***Proof***. We will use a proof by mathematical induction. For each natural number n, we let $P(n)$ be

$$4^n \equiv 1 \pmod 3.$$

We first prove that $P(1)$ is true. Notice that when $n = 1$, $4^n = 4^1 = 4$ and $4 \equiv 1 \pmod 3$. This proves that $P(1)$ is true.

For the inductive step, we prove that for each $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true. So let k be a natural number and assume that $P(k)$ is true. That is, assume that

$$4^k \equiv 1 \pmod 3. \tag{1}$$

The goal now is to prove that $P(k+1)$ is true. That is, it must be proved that

$$4^{k+1} \equiv 1 \pmod 3. \tag{2}$$

Since we have assume that $4^k \equiv 1 \pmod 3$, we conclude that 3 divides $\left(4^k - 1\right)$ and so there exists an integer m such that

$$4^k - 1 = 3m.$$

Multiplying both sides of this equation by 4, we obtain

$$\begin{aligned} 4\left(4^k - 1\right) &= 4(3m) \\ 4^{k+1} - 4 &= 12m \\ 4^{k+1} - 3 - 1 &= 12m \\ 4^{k+1} - 1 &= 3 + 12m \\ 4^{k+1} - 1 &= 3(1 + 4m) \end{aligned}$$

So we have proved that if $P(k)$ is true, then $P(k+1)$ is true. Hence, the inductive step has been established, and by the Principle of Mathematical Induction, we have proved that for each natural number n, $4^n \equiv 1 \pmod 3$. ■

3. Proposition. For each natural number n with $n \geq 3$, $3^n > 5 + 2^n$.

Proof. We will use a proof by mathematical induction. For each natural number n, we let $P(n)$ be

$$3^n > 5 + 2^n.$$

We first prove that $P(3)$ is true. Notice that when $n = 3$, $3^n = 27$ and $5 + 2^n = 13$. Since $27 > 13$, this proves that $P(1)$ is true.

For the inductive step, we prove that for each $k \in \mathbb{N}$ with $k \geq 3$, if $P(k)$ is true, then $P(k+1)$ is true. So let k be a natural number with $k \geq 3$ and assume that $P(k)$ is true. That is, assume that

$$3^k > 5 + 2^k. \tag{1}$$

The goal now is to prove that $P(k+1)$ is true. That is, it must be proved that

$$3^{k+1} > 5 + 2^{k+1}. \tag{2}$$

So we multiply both sides of inequality (1) to obtain

$$\begin{aligned} 3 \cdot 3^k &> 3(5 + 2^k) \\ 3^{k+1} &> 15 + 3 \cdot 2^k \end{aligned} \tag{3}$$

Since $3 > 2$, $3 \cdot 2^k > 2 \cdot 2^k$ or $3 \cdot 2^k > 2^{k+1}$. In addition, $15 > 5$ and so we can co

So we have proved that if $P(k)$ is true, then $P(k+1)$ is true. Hence, the inductive step has been established, and by the Principle of Mathematical Induction, we have proved that for each natural number n, $4^n \equiv 1 \pmod 3$. ■

4. (**a**)

$f(5) = 5$	$f_9 = 34$	$f_{13} = 233$	$f(17) = 1597$
$f(6) = 8$	$f_{10} = 55$	$f_{14} = 377$	$f(18) = 2584$
$f(7) = 13$	$f_{11} = 89$	$f_{15} = 610$	$f(19) = 4181$
$f(8) = 21$	$f_{12} = 144$	$f_{16} = 987$	$f(20) = 6765$

(**b**) ***Proof.*** We will use a proof by induction. For each natural number n, we let $P(n)$ be,

$$f_{3n} \text{ is an even natural number.}$$

Since $f_3 = 2$, we see that $P(1)$ is true and this proves the basis step.

For the inductive step, we let k be a natural number and assume that $P(k)$ is true. That is, assume that f_{3k} is an even natural number. This means that there exists an integer m such that

$$f_{3k} = 2m. \tag{1}$$

We need to prove that $P(k+1)$ is true or that $f_{3(k+1)}$ is even. Notice that $3(k+1) = 3k+3$ and, hence, $f_{3(k+1)} = f_{3k+3}$. We can now use the recursion formula for the Fibonacci numbers to conclude that

$$f_{3k+3} = f_{3k+2} + f_{3k+1}.$$

Using the recursion formula again, we get $f_{3k+2} = f_{3k+1} + f_{3k}$. Putting this all together, we see that

$$\begin{aligned} f_{3(k+1)} &= f_{3k+3} \\ &= f_{3k+2} + f_{3k+1} \\ &= (f_{3k+1} + f_{3k}) + f_{3k+1} \\ &= 2f_{3k+1} + f_{3k}. \end{aligned} \tag{2}$$

We now substitute the expression for f_{3k} in equation (1) into equation (2). This gives

$$f_{3(k+1)} = 2f_{3k+1} + 2m$$
$$f_{3(k+1)} = 2\left(f_{3k+1} + m\right)$$

This preceding equation shows that $f_{3(k+1)}$ is even. Hence it has been proved that if $P(k)$ is true, then $P(k+1)$ is true and the inductive step has been established. By the Principle of Mathematical Induction, this proves that for each natural number n, the Fibonacci number f_{3n} is an even natural number. ■

(c) ***Proof.*** Let $P(n)$ be, "$f_1 + f_2 + \cdots + f_{n-1} = f_{n+1} - 1$." Since $f_1 = f_3 - 1$, $P(2)$ is true, and this proves the basis step.

For the inductive step, we let k be a natural number with $k \geq 2$ and assume that $P(k)$ is true and will prove that $P(k+1)$ is true. That is, we assume that

$$f_1 + f_2 + \cdots + f_{k-1} = f_{k+1} - 1, \tag{1}$$

and will prove that

$$f_1 + f_2 + \cdots + f_{k-1} + f_k = f_{(k+1)+1} - 1 = f_{k+2} - 1. \tag{2}$$

By adding f_k to both sides of equation (1), we see that

$$\begin{aligned}(f_1 + f_2 + \cdots + f_{k-1}) + f_k &= (f_{k+1} - 1) + f_k \\ &= (f_{k+1} + f_k) - 1 \\ &= f_{k+2} - 1.\end{aligned}$$

Comparing this to equation (2), we see that we have proved that if $P(k)$ is true, then $P(k+1)$ is true and the inductive step has been established. So by the Principle of Mathematical Induction, this proves that for each natural number n with $n \geq 2$, $f_1 + f_2 + \cdots + f_{n-1} = f_{n+1} - 1$ ■

5. ***Proof.*** We will use a proof by mathematical induction. We let $P(n)$ be, "there exist nonnegative integers x and y such that $n = 3x + 5y$."

Basis Step: For the basis step, we will show that $P(8)$, $P(9)$, and $P(10)$ are true. We see that

- $P(8)$ is true since $3 \cdot 1 + 5 \cdot 1 = 8$.

- $P(9)$ is true since $3 \cdot 3 + 5 \cdot 0 = 9$.
- $P(10)$ is true since $3 \cdot 0 + 5 \cdot 2 = 10$.

Inductive Step: Let $k \in \mathbb{N}$ with $k \geq 10$. Assume that $P(8)$, $P(9)$, ..., $P(k)$ are true. Now, notice that

$$k + 1 = 3 + (k - 2).$$

Since $k \geq 10$, we can conclude that $k - 2 \geq 8$ and hence $P(k-2)$ is true. Therefore, there exist non-negative integers u and v such that $k - 2 = (3u + 5v)$. Using this equation, we see that

$$\begin{aligned} k + 1 &= 3 + (3u + 5v) \\ &= 3(1 + u) + 5v. \end{aligned}$$

Hence, we can conclude that $P(k + 1)$ is true. This proves that if $P(8)$, $P(9)$, ..., $P(k)$are true, then $P(k + 1)$ is true. Hence, by the Second Principle of Mathematical Induction, for all natural numbers n with $n \geq 8$, there exist nonnegative integers x and y such that $n = 3x + 5y$. ■

Chapter 7

1. The function f is an injection but not a surjection. To see that it is an injection, let $a, b \in \mathbb{R}$ and assume that $f(a) = f(b)$. This implies that $e^{-a} = e^{-b}$. Now use the natural logarithm function to prove that $a = b$. Since $e^{-x} > 0$ for each real number x, there is no $x \in \mathbb{R}$ such that $f(x) = -1$. So f is not a surjection.

The function g is an injection and is a surjection. The proof that g is an injection is basically the same as the proof that f is an injection. To prove that g is a surjection, let $b \in \mathbb{R}+$. To construct the real number a such that $g(a) = b$, solve the equation $e^{-a} = b$ for a. The solution is $a = -\ln b$. It can then be verified that $g(a) = b$.

2. (**a**) Let $F : \mathbb{R} \to \mathbb{R}$ be defined by $F(x) = 5x + 3$ for all $x \in \mathbb{R}$. Let $x_1, x_2 \in \mathbb{R}$ and assume that $F(x_1) = F(x_2)$. Then,

$$\begin{aligned} 5x_1 + 3 &= 5x_2 + 3 \\ 5x_1 &= 5x_2 \\ x_1 &= x_2. \end{aligned}$$

Hence, F is an injection. Now let $y \in \mathbb{R}$. Then, $\dfrac{y-3}{5} \in \mathbb{R}$ and

$$\begin{aligned} F\left(\frac{y-3}{5}\right) &= 5\left(\frac{y-3}{5}\right) + 3 \\ &= (y-3) + 3 \\ &= y. \end{aligned}$$

Thus, F is a surjection and hence F is a bijection.

(**b**) The proof that G is an injection is similar to the proof in Part (a) that F is an injection. Now, for each $x \in \mathbb{Z}$, $5x + 3 \equiv 3 \pmod 5$, and hence $G(x) \equiv 3 \pmod 5$. This means that there is no integer x such that $G(x) = 0$. Therefore, G is not a surjection.

(**c**) Let $a, b \in \mathbb{R} - \{4\}$ and assume that $f(a) = f(b)$. Then,

$$\begin{aligned} \frac{3a}{a-4} &= \frac{3b}{b-4} \\ 3a(b-4) &= 3b(a-4) \\ 3ab - 12a &= 3ab - 12b \\ -12a &= -12b \\ a &= b. \end{aligned}$$

So f is an injection.

Use a proof by contradiction to show there is no $a \in \mathbb{R} - \{4\}$ such that $f(a) = 3$. Assume such an a exists. Then

$$\begin{aligned} \frac{3a}{a-4} &= 3 \\ 3a &= 3a - 12 \\ 0 &= -12, \end{aligned}$$

and this is a contradiction. Therefore, for all $x \in \mathbb{R} - \{4\}$, $f(x) \neq 3$ and f is not a surjection.

(**d**) The function g is a bijection. The proof that is an injection is similar to the proof that f is an injection in Part (c). To prove that it is a surjection

let $y \in \mathbb{R} - \{3\}$. Then, $\dfrac{4y}{y-3} \in \mathbb{R} - \{4\}$ and

$$\begin{aligned} g\left(\frac{4y}{y-3}\right) &= \frac{3\left(\dfrac{4y}{y-3}\right)}{\left(\dfrac{4y}{y-3}\right) - 4} \\ &= \frac{12y}{4y - 4(y-3)} \\ &= \frac{12y}{12} \\ &= y. \end{aligned}$$

This proves that g is a surjection.

3. (**a**)

$s(1) = 1$	$s(5) = 6$	$s(9) = 13$	$s(13) = 14$
$s(2) = 3$	$s(6) = 12$	$s(10) = 18$	$s(14) = 24$
$s(3) = 4$	$s(7) = 8$	$s(11) = 12$	$s(15) = 24$
$s(4) = 7$	$s(8) = 15$	$s(12) = 28$	$s(16) = 31$

(**b**) The sum of the divisors function s is not an injection. For example, $s(6) = s(11)$. This function is also not a surjection. For example, for all $x \in \mathbb{N}$, $s(x) \neq 2$ and for all $x \in \mathbb{N}$, $s(x) \neq 5$.

4. (**a**) The determinant function is not an injection. For example,

$$\det\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \det\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}.$$

The determinant function is a surjection. To prove this, let $a \in \mathbb{R}$. Then

$$\det\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} = a.$$

(**b**) The transpose function is a bijection. To prove it is an injection, let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in \mathcal{M}_2(\mathbb{R})$ and assume that

$$\operatorname{tran}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \operatorname{tran}\begin{bmatrix} p & q \\ r & s \end{bmatrix}.$$

Then, $\begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} p & r \\ q & s \end{bmatrix}$. Therefore, $a = p$, $b = q$, $c = r$, and $d = s$ and hence, $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$. To prove that the transpose function is a surjection, let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{M}_2(\mathbb{R})$. Then,

$$\text{tran} \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

(**c**) The function F is not an injection. For example

$$F \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0 \qquad \text{and} \qquad F \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = 0.$$

The function F is a surjection. To prove this, let $y \in \mathbb{R}$. Consider three cases.

- If $y = 0$, then $F \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0 = y$.
- If $y > 0$, then $\sqrt{y} \in \mathbb{R}$ and $F \begin{bmatrix} \sqrt{y} & 0 \\ 0 & 0 \end{bmatrix} = \left(\sqrt{y}\right)^2 = y$.
- If $y < 0$, then $\sqrt{-y} \in \mathbb{R}$ and $F \begin{bmatrix} 0 & \sqrt{-y} \\ 0 & 0 \end{bmatrix} = -\left(\sqrt{-y}\right)^2 = y$.

Index