Appendix C

Methods of Proof

Preliminaries

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

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.

Definition C.1.

- The set of **natural numbers**, denoted $\mathbb{N}$, contains the counting numbers (1, 2, 3, and so on); that is,
$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$
- The set of **whole numbers**, denoted $\mathbb{W}$, contains the counting numbers and zero; that is,
$$\mathbb{W} = \{0, 1, 2, 3, \ldots\}.$$
- The set of **integers**, denoted $\mathbb{Z}$, contains the whole numbers and their opposites (or negatives); that is,
$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Definition C.2. 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 C.3. A nonzero integer m **divides** an integer n provided that there is an integer q such that $n = m \cdot q$.

- 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."

- If a and b are integers and $a \neq 0$ and a divides b, we also ay that m is a **divisor** of n, m is a **factor** of n, and n is a **multiple** of m.
- The integer 0 is not a divisor of any integer and is a multiple of every integer.

Definition C.4. 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 C.5. Let $n \in \mathbb{N}$. If a and b are integers, then we say that $\boldsymbol{a}$ **is congruent to** $\boldsymbol{b}$ **modulo** $\boldsymbol{n}$ provided that n divides $a - b$.

Note: A standard notation for "a is congruent to b modulo n 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 C.6. 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.

- When sets A and B are equal, we write $A = B$ and 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 C.7. 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 $A \neq B$.

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

Definition C.8. 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 C.9. 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,

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

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 $P \to Q$. The statement $P \to Q$ is often read as "P **implies** Q. The statement $P \to Q$ 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 C.10. 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.

The following theorem states some of the most frequently used logical equivalencies used when writing mathematical proofs.

Theorem C.11 (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	$P \to (Q \vee R) \equiv (P \wedge \neg Q) \to R$ $(P \vee Q) \to R \equiv (P \to R) \wedge (Q \to R)$

Direct Proofs

In order to prove that a conditional statement $P \to Q$ 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 $P \to Q$, 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.

Using the Definitions of Congruence and Divides

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

Proposition C.12. 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 proven the proposition to be false. The following table summarizes four examples that suggest this proposition is true.

a	b	$a+b$	Is $(a+b) \equiv 3 \pmod 8$?
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 now 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. So 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.

Proposition C.12. *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. *For each integer n, if 7 divides $\left(n^2 - 4\right)$, then 7 divides $(n - 2)$.*

If we think about starting 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 $n = 5$, 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 the proposition is true and the conclusion is false. This is a counterexample for the proposition and proves that the proposition is false.

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

For each element x in U, if $x \in S$, 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.** To prove that a set S is a subset of a set T, the key is that we have to prove something about all elements in S. 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 C.13. *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 C.14. *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 $A - B = A \cap B^c$. ■

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 C.11 on page 89 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.

Using the Contrapositive

One of the most useful logical equivalencies to prove a conditional statement is that a conditional statement $P \to Q$ is logically equivalent to its contrapositive, $\neg Q \to \neg P$. 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.
- To prove the statement $P \to Q$ we can use a direct proof to prove the equivalent statement that $\neg Q \to \neg P$ 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 C.15. *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 an odd integer. Since this is the contrapositive of the proposition, we have completed a proof of the proposition. ■

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 C.11 on page 89. 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 $\dfrac{1}{a}$. This suggests that we consider using the following logical equivalency based on a result in Theorem C.11 on page 89:

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

Proposition C.16. *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 $\dfrac{1}{a}$. 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. ■

Proofs of Biconditional Statements

One of the logical equivalencies in Theorem C.11 on page 89 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 C.17. *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 $\frac{1}{4}c^2$. ■

Proof by Contradiction

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 assuming its negation is true. According to Theorem C.11 on page 89,

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

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

Proposition C.18. *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

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

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 (C.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 $\dfrac{1}{x(1-x)} \geq 4$. ■

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.

Proposition C.19. *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

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

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 C.15 on page 94, 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

$$4k^2 = 2\left(2m^2 + 2m + 2n^2 + 2n + 1\right)$$
$$2k^2 = 2\left(m^2 + m + n^2 + n\right) + 1$$

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 $x^2+y^2 = z^2$. ■

Rational and Irrational Numbers

One of the most important ways to classify real numbers is as a rational number or an irrational number. (See the section on subsets of the real numbers in Investigation 3 of the textbook.)

Definition C.20. 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 $x = \dfrac{m}{n}$. A real number that is not a rational number is called an **irrational number.**

We use the symbol $\mathbb{Q}$ to stand for the set of rational numbers.

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 C.21. *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 $\dfrac{1}{x} \in \mathbb{Q}$. We now know that $x \cdot y$ and $\dfrac{1}{x}$ are rational numbers and since the rational numbers are closed under multiplication, we conclude that

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

However, $\dfrac{1}{x} \cdot (xy) = y$ 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. ■

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 C.11 on page 89. 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. *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 this propostion, 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 C.22. *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. ■

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: $a < b$.

Using Cases with the Division Algorithm

In Investigation 1 of the textbook, we introduced an important result for the set of integers is known as the Division Algorithm, which is stated below.

The Division Algorithm
Let a and b be integers with $a > 0$. Then there exist unique integers q and r such that

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

When we speak of **the quotient** and **the remainder** when we "divide an integer b by the positive integer a," 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 $b = aq + r$.

The Division Algorithm can sometimes be used to construct cases for a proof dealing with the integers. For example, 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 C.23.

Proposition C.23. *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 $3 \mid \left(n^3 - n\right)$.

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 $3 \mid \left(n^3 - n\right)$. We have now proved that 3 divides $(n^3 - n)$ in all 3 of the possible cases. Therefore, we have proved that for each integer n, 3 divides $(n^3 - n)$. ■

Exercises

(1) 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.)

(2) 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 $m = 3$.

(3) 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.

(4) 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 $a^2 \equiv 4 \pmod 5$.

(5) 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 $x = \dfrac{m}{n}$.

Is the following proposition true or false? Explain.

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

(6) (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 $n \not\equiv 3 \pmod 6$.

(7) 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 y is irrational, then $x + y$ is irrational.

(8) 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.

(9) Complete the details for the proof of Case 3 of Proposition C.23.

(10) 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 $n^2 - 1$.