More on Proofs – Part III of Hammack

Dr. Doreen De Leon
Math 111, Fall 2014

7 Proving Non-Conditional Statements

Although most theorems either have a conditional form or may be written in conditional form, some theorems and propositions cannot. For example, some theorems have the biconditional form, i.e., "*P if and only if Q*." We will also look at two other types of theorems.

7.1 If-and-Only-If Proof

Some propositions have the form

$$P \text{ if and only if } Q.$$

Recall from Section 2.4, that this statment means that the following conditional statements are true.

If P, then Q.

If Q, then P.

So, to prove "P if and only if Q," we must prove two conditional statements, $P \implies Q$ and its converse ($Q \implies P$). Since both statements are conditional statements, we may prove them with direct, contrapositive, or contradiction proof. Below is an outline reflecting this.

Outline for If-and-Only-If Proof

Proposition. P if and only if Q.

Proof.
[Prove $P \implies Q$ using direct, contrapositive, or contradiction proof.]
[Prove $Q \implies P$ using direct, contrapositive, or contradiction proof.] □

We will now proceed to do a few examples.

Proposition 1. Let $x \in \mathbb{Z}$. Then $11x - 7$ is even if and only if x is odd.

Proof.

$\underline{\Longrightarrow}$ First, we prove that if $11x - 7$ is an even integer, then x is odd.

We will use a proof by contrapositive for this. Assume that x is even. Then $x = 2b$, where $b \in \mathbb{Z}$. Therefore,

$$\begin{aligned} 11x - 7 &= 11(2b) - 7 \\ &= 22b - 7 \\ &= 2(11b - 4) + 1, \end{aligned}$$

which is odd.

$\underline{\Longleftarrow}$ Next, we prove the coverse, that if x is an odd integer, then $11x - 7$ is even. We will use a direct proof for this.

Let x be an odd integer. Then $x = 2a + 1$ for some integer a. So,

$$\begin{aligned} 11x - 7 &= 11(2a + 1) - 7 \\ &= 22a + 4 \\ &= 2(11a + 2), \end{aligned}$$

which is even.

□

Proposition 2. Let $x, y \in \mathbb{Z}$. Then $4 \mid (x^2 - y^2)$ if and only if x and y are of the same parity.

Proof.

$\underline{\Longrightarrow}$ We will do a proof by contrapositive. Assume that x and y have opposite parity. Without loss of generality, assume that x is even and y is odd. Then $x = 2k$ and $y = 2l + 1$ for some integers k and l. Then, we have

$$\begin{aligned} x^2 - y^2 &= (2k)^2 - (2l + 1)^2 \\ &= 4k^2 - (4l^2 + 4l + 1) \\ &= 4k^2 - 4l^2 - 4l - 1 \\ &= 4k^2 - 4l^2 - 4l - 4 + 3 \\ &= 4(k^2 - l^2 - l - 1) + 3. \end{aligned}$$

Since $k^2 - l^2 - l - 1$ is an integer, it follows that there is a remainder of 3 when $x^2 - y^2$ is divided by 4. Therefore, $4 \nmid (x^2 - y^2)$.

$\underline{\Longleftarrow}$ Assume that x and y have the same parity. We want to show that $4 \mid (x^2 - y^2)$. There are two cases.

Case 1: Both x and y are even. Then $x = 2a$ and $y = 2b$ for some integers a and b. Then,

$$x^2 - y^2 = (2a)^2 - (2b)^2 = 4a^2 - 4b^2 = 4(a^2 - b^2).$$

Since $a^2 - b^2$ is an integer, $4 \mid (x^2 - y^2)$.

Case 2: Both x and y are odd. Then, $x = 2m + 1$ and $y = 2n + 1$ for some integers m and n. So,

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

Since $m^2 + m - n^2 - n$ is an integer, $4 \mid (x^2 - y^2)$.

□

Exercise: Suppose $a \in \mathbb{Z}$. Prove that $a^3 + a^2 + a$ is even if and only if a is even.

Proof.

$\underline{\Longrightarrow|}$ Suppose that a is an odd integer. Then $a = 2m + 1$ for some integer m. So,

$$\begin{aligned} a^3 + a^2 + a &= (2m+1)^3 + (2m+1)^2 + (2m+1) \\ &= 8m^3 + 3(4m^2) + 3(2m) + 1 + 4m^2 + 4m + 1 + 2m + 1 \\ &= 8m^3 + 16m^2 + 12m + 3 \\ &= 2(4m^3 + 8m^2 + 6m + 1) + 1, \end{aligned}$$

an odd integer.

$\underline{\Longleftarrow|}$ Assume that a is an even integer. Then $a = 2n$ for some integer n. So,

$$a^3 + a^2 + a = (2n)^3 + (2n)^2 + 2n = 8n^3 + 4n^2 + 2n = 2(4n^3 + 2n^2 + n),$$

an even integer.

□

7.2 Equivalent Statements

There are some theorems that are neither conditional nor biconditional. Instead, the theorem will state that a list of statements is "*equivalent.*"

A example of such a theorem is

Theorem 1. Suppose f is a continuous function on a domain D. The following statements are equivalent.

(a) $f(z)$ has an antiderivative $F(z)$ throughout D.

(b) The integrals of $f(z)$ along contours lying entirely in D and extending from any fixed point z_1 to any fixed point z_2 all have the same value, namely,

$$\int_{z_1}^{z_2} f(z)\,dz = F(z_2) - F(z_1).$$

(c) The integrals of $f(z)$ around closed contours lying entirely in D have value 0.

Saying that the statements are equivalent is the same as saying that if one statement is true, than all are true. Simlarly, if one statement is false, then all are false.

Typically, the best way to solve such a theorem is to prove $(a) \implies (b) \implies (c) \implies (a)$.

7.3 Exisence Proofs; Existence and Uniqueness Proofs

"Simple" Existence Proofs

In this section, we will discuss how to prove two types of statements. The first type contains statements that are existentially quantified, i.e., $\exists x, R(x)$. Such statements are called **existence statements**, and theorems that have this form are called **existence theorems**. Note that an example may be sufficient to prove an existence statement, but not to prove a conditional statement.

Proposition 3. There exist integers a and b such that $(a+b)^2 = a^2 + b^2$.

Proof. Let $a = 1$ and $b = 0$. Then

$$(a+b)^2 = (1+0)^2 = 1^2 = 1^2 + 0^2 = a^2 + b^2.$$

□

Proposition 4. There exist a rational number a and a rational number b such that a^b is irrational.

Proof. Let $a = 2$ and $b = \dfrac{1}{2}$. Then, $a^b = 2^{\frac{1}{2}} = \sqrt{2}$, which is irrational. □

Existence Statements as Part of Conditional Statements

Often, an existence statement will be embedded inside of a conditional statement.

Proposition 5. If x is an irrational number, then there exists a number $y \in \mathbb{Q}$ such that $x+y$ is irrational.

Proof. Let x be an irrational number. Let $y = 0$. Then $x+y = x+0 = x$, which is irrational. □

Existence and Uniqueness Proofs

Many theorems are stated in the form of "There is a unique $x \in S$ for which $P(x)$." This statement means that (a) there is an example $x \in S$ for which $P(x)$ is true, and (2) this x is the only such example. Typically to prove such a theorem, we first prove the existence of an example, say a, and then do one of the following:

(1) Assume that a and b are elements of S possessing property P and show that $a = b$.

(2) We assume that a and b are distinct elements of S possessing property P and show by contradiction that $a = b$.

Proposition 6. Let r be an irrational number, and define $S = \{sr + t : s, t \in \mathbb{Q}\}$. For every $x \in S$, there exist unique rational numbers a and b such that $x = ar + b$.

Proof. Let $x \in S$ and suppose that $x = ar + b$ and $x = cr + d$, where $a, b, c, d \in \mathbb{Q}$. Then, $ar + b = cr + d$. If $a \neq c$, then $(a - c)r = d - b$, and so

$$r = \frac{d-b}{a-c}.$$

Since $r = \dfrac{d-b}{a-c}$ is a rational number, this is impossible. So $a = c$. Subtracting ar and cr from both sides of $ar + b = cr + d$ gives $b = d$. □

Theorem 2 (The Division Algorithm)**.** For positive integers a and b, there exist unique integers q and r such that $b = aq + r$ and $0 \leq r < a$.

Proof. First, we show that there exist integers q and r such that $b = aq + r$ with $0 \leq r < a$. We then prove that these q and r are unique.

Consider the set

$$S = \{b - ax : x \in \mathbb{Z} \text{ and } b - ax \geq 0\} \subseteq \{0, 1, 2, 3, \dots\}.$$

Note that if $x = 0$, then $b \in S$, so S is not empty. Therefore, by the well-ordering principle, S has a smallest element r, and by definition of S, $r \geq 0$. Also, since $r \in S$, there is some

integer q such that $r = b - aq$. Thus, $b = ar + q$, with $r \geq 0$. We next need to show that $r < a$. Assume to the contrary, that $r \geq a$. Let $t = r - a$. Then $t \geq 0$. Since $a > 0$, it follows that $t < r$. Moreover,

$$t = r - a = (b - aq) - a = b - (aq + a) = b - a(q + 1),$$

which implies $t \in S$, contradicting the fact that r is the smallest element of S. Therefore, $r < a$.

Next, we must show that q and r are the only integers for which $b = aq + r$ and $0 \leq r < a$. To do this, assume that there are integers q' and r' such that $b = aq' + r'$, where $0 \leq r' < a$. Assume, without loss of generality, that $r' \geq r$, so $r' - r \geq 0$. Since $aq + r = aq' + r'$, it follows that

$$a(q - q') = r' - r.$$

Since $q - q' \in \mathbb{Z}$, we have $a \mid (r' - r)$. Since $0 \leq r' - r < a$, we must have that $r' - r = 0$ and so, $r' = r$. Since $a(q - q') = r' - r = 0$ and $a \neq 0$, $q - q' = 0$ and so, $q = q'$. □

Exercise: Prove that the equation $x^5 + 2x - 5 = 0$ has a unique real solution between $x = 1$ and $x = 2$.

Proof. Note that $p(x) = x^5 + 2x - 5$ is continuous on $[1, 2]$. Also, note that $p(1) = -2 < 0$ and $p(2) = 31 > 0$. Therefore, by the Intermediate Value Theorem, there exists a point $1 < c < 2$ such that $p(c) = 0$. Now, assume that there is another, distinct point $1 < d < 2$ such that $p(d) = 0$. Assume, without loss of generality, that $c < d$. Since $1 < c < d < 2$, it follows that

$$c^5 + 2c - 5 < d^5 + 2d - 5.$$

However, we have that $c^5 + 2c - 5 = 0$ and $d^5 + 2d - 5 = 0$. Therefore,

$$0 = c^5 + 2c - 5 < d^5 + 2d - 5 = 0,$$

a contradiction. □

8 Proofs Involving Sets

You will see when you take other upper division courses that sets play an important role in mathematics. In this chapter, we will discuss how to show that an object is an element of a set, how to prove one set is a subset of another, and how to prove two sets are equal.

Recall:

$$\begin{aligned} A \times B &= \{(x, y) : x \in A, y \in B\} \\ A \cup B &= \{x : (x \in A) \vee (x \in B)\} \\ A \cap B &= \{x : (x \in A) \wedge (x \in B)\} \\ A - B &= \{x : (x \in A) \wedge (x \notin B)\} \\ \overline{A} &= U - A \end{aligned}$$

8.1 How to Prove $a \in A$

For example, if we wish to prove that $a \in \{x : P(x)\}$ is true, we should show that $P(a)$ is true. If we wish to show that $a \in \{x \in S : P(x)\}$, we first must show that $a \in S$ and then verify that $P(a)$ is true.

Examples:

(1) Consider the set $A = \{x \in \mathbb{Z} : x^2 = x\}$. Then $1 \in A$, since $1 \in \mathbb{Z}$ and $1^2 = 1$. In addition, $0 \in A$, since $0 \in \mathbb{Z}$ and $0^2 = 0$. But, $2 \notin A$ since $2 \in \mathbb{Z}$ but $2^2 = 4 \neq 2$.

(2) Consider the set $B = \{X \in \mathcal{P}(\mathbb{N}) : |X| = 4\}$. Then $\{1, 2, 3, 4\} \in B$, since $\{1, 2, 3, 4\} \in \mathcal{P}(\mathbb{N})$ and $|\{1, 2, 3, 4\}| = 4$. However, the set $\{1, 2, 3\} \notin B$ since although $\{1, 2, 3\} \in \mathcal{P}(\mathbb{N})$, $|\{1, 2, 3\}| = 3$. Also, the set $\{\{1, 2, 3\}\} \notin B$ since $\{\{1, 2, 3\}\} \notin \mathcal{P}(\mathbb{N})$ and $|\{\{1, 2, 3\}\}| = 1$.

8.2 How to Prove $A \subseteq B$

Recall that $A \subseteq B$ if every element of A is also an element of B. Therefore, to prove that $A \subseteq B$, we are actually proving that the conditional statement

If $a \in A$, then $a \in B$

is true. This can be proved directly or using proof by contrapositive.

Examples:

(1) Prove that $\{12n : n \in \mathbb{Z}\} \subseteq \{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\}$.

Proof. Suppose that $x \in \{12n : n \in \mathbb{Z}\}$. Then $x = 12n$ for some integer n. Therefore, we have that $x = 2(6n)$, so $x \in \{2n : n \in \mathbb{Z}\}$, and $x = 3(4n)$ so $x \in \{3n : n \in \mathbb{Z}\}$. Therefore, $\{12n : n \in \mathbb{Z}\} \subseteq \{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\}$. □

(2) Prove that if $k \in \mathbb{Z}$, then $\{n \in \mathbb{Z} : n \mid k\} \subseteq \{n \in \mathbb{Z} : n \mid k^2\}$.

Proof. Suppose that $k \in \mathbb{Z}$. Next, suppose that $l \in \{n \in \mathbb{Z} : n \mid k\}$. Then $l \mid k$, so there is an integer m for which $k = lm$. Then, squaring both sides gives

$$k^2 = (lm)^2 = l^2m^2.$$

Therefore, we may write $k^2 = l(lm^2)$, and since lm^2 is an integer, we obtain $l \mid k^2$. Thus, $l \in \{n \in \mathbb{Z} : n \mid k^2\}$ and $\{n \in \mathbb{Z} : n \mid k\} \subseteq \{n \in \mathbb{Z} : n \mid k^2\}$. □

Exercise: Prove that if $m, n \in \mathbb{Z}$, then $\{x \in \mathbb{Z} : mn \mid x\} \subseteq \{x \in \mathbb{Z} : m \mid x\} \cap \{x \in \mathbb{Z} : n \mid x\}$.

Proof. Suppose that $m, n \in \mathbb{Z}$. Let $r \in \{x \in \mathbb{Z} : mn \mid x\}$. Then there exists a constant c such that $r = (mn)c$. Since $r = (mn)c$, we have that $r = m(nc)$, which means that $m \mid r$, so $r \in \{x \in \mathbb{Z} : m \mid x\}$. We also have that $r = n(mc)$, so $n \mid r$ and $r \in \{x \in \mathbb{Z} : n \mid x\}$. Therefore, $r \in \{x \in \mathbb{Z} : m \mid x\} \cap \{x \in \mathbb{Z} : n \mid x\}$, and $\{x \in \mathbb{Z} : mn \mid x\} \subseteq \{x \in \mathbb{Z} : m \mid x\} \cap \{x \in \mathbb{Z} : n \mid x\}$. □

8.3 How to Prove $A = B$

In proofs, it is often necessary to show that two sets are equal. There is a standard way to do this. Suppose that we want to show that $A = B$. If we show that $A \subseteq B$, then every element of A is also in B, but B could have elements that are not in A, so we can't conclude that $A = B$. If we *also* show that $B \subseteq A$, then B can't contain anything that is not in A, so $A = B$. So, to summarize, the standard procedure for proving $A = B$ is to prove both $A \subseteq B$ and $B \subseteq A$.

Outline for Proving $A = B$

Proposition. $A = B$.

Proof.
[Prove $A \subseteq B$.]
[Prove $B \subseteq A$.]
Therefore, since $A \subseteq B$ and $B \subseteq A$,
it follows that $A = B$. □

Example: Let $A, B,$ and C be nonempty sets. If $A \times C = B \times C$, then $A = B$.

Proof. Assume that $A \times C = B \times C$. Since $C \neq \varnothing$, then set C contains some element c. Let $x \in A$. Then $(x, c) \in A \times C$. Since $A \times C = B \times C$, it follows that $(x, c) \in B \times C$. Therefore, $x \in B$ and $A \subseteq B$.

Similarly, let $y \in B$ and $c \in C$. Then $(y, c) \in B \times C$. Since $A \times C = B \times C$, we have that $(y, c) \in A \times C$. Therefore, $y \in A$ and $B \subseteq A$.

Since $A \subseteq B$ and $B \subseteq A$, $A = B$. □

Example: If $A, B,$ and C are nonempty sets, then $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof. Suppose that $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$, which means that $x \in B$ or $x \in C$. Therefore, we have that $x \in A$ and $x \in B$ or $x \in A$ and $x \in C$, or $x \in A \cap B$ or $x \in A \cap C$, which means that $x \in (A \cap B) \cup (A \cap C)$. Therefore, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Next suppose that $r \in (A \cap B) \cup (A \cap C)$. This means that $r \in A \cap B$ or $r \in A \cap C$. If $r \in A \cap B$, then $r \in A$ and $r \in B$. If $r \in A \cap C$, then $r \in A$ and $r \in C$. Therefore, we have that $r \in A$ and either $r \in B$ or $r \in C$, so $r \in A \cap (B \cup C)$ and $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

Since $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ and $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$, it must be true that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. □

There is another proof of this example using the definitions we introduced at the beginning of this chapter, as well as properties of the logical operators. For this proof, we do not need to show that $A \cap (B \cup c) \subseteq (A \cap B) \cup (A \cap C)$ and $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$, because the properties give equality.

Proof.

$$\begin{aligned}
A \cap (B \cup C) &= \{x : (x \in A) \wedge (x \in B \cup C)\} && \text{(definition of intersection)} \\
&= \{x : (x \in A) \wedge ((x \in B) \vee (x \in C))\} && \text{(definition of union)} \\
&= \{x : ((x \in A) \wedge (x \in B)) \vee ((x \in A) \wedge (x \in C))\} && \text{(distributive law)} \\
&= \{x : (x \in A \cap B) \vee (x \in A \cap C)\} && \text{(definition of intersection)} \\
&= (A \cap B) \cup (A \cap C) && \text{(definition of union)}
\end{aligned}$$

□

Exercise: Let A and B be sets in the universal set U. Prove that $A - B = A \cap \overline{B}$.

Proof. Suppose $x \in A - B$. Then, $x \in A$ and $x \notin B$. Since $x \notin B$, we have that $x \in U - B$, or $x \in \overline{B}$. Thus, we have $x \in A$ and $x \in \overline{B}$, so $x \in A \cap \overline{B}$.

Now, suppose that $y \in A \cap \overline{B}$. Then $y \in A$ and $y \in \overline{B}$. Since $y \in \overline{B}$, we know that $y \in U - B$, or $y \notin B$. So, we have $y \in A$ and $y \notin B$, or $y \in A - B$. Therefore, $A \cap \overline{B} \subseteq A - B$.

Since $A - B \subseteq A \cap \overline{B}$ and $A \cap \overline{B} \subseteq A - B$, $A - B = A \cap \overline{B}$. □

9 Disproof

From Chapter 4 until the present time, we have dealt with proving that a given statement is true. Now, we will discuss what we should do if we are given a statement that is false. In order to prove that a statement is false, we carry out a procedure called **disproof**. This chapter, then, is concerned with **disproving** statements.

First, mathematical statements can be diided into two categories. One category consists of all statements that have been proved to be true (e.g., theorems, propositions, lemmas, corollaries). There are also some trivial statements in this category (e.g., $2 = 2$). At the other end of the spectrum is a category consisting of statements that are known to be false (e.g., $0 = 1$, all odd

numbers are prime, etc.). There is a third category, however, between these two extremees. It consists of statements whose truth or falsity has not been determined. Such statements are called **conjectures**. Examples include: the Goldbach Conjecture (Any even number greater than 2 is the sum of two primes.), the Twin Primes Conjecture (There are infinitely many primes p such that $p + 2$ is also prime.)

Many mathematicians spend much of their time and energy attempting to prove or disprove conjectures, or in creating new conjectures based on collected evidence or intuition. When a conjecture is proved (or disproved), the proof or disproof is oftne published in a paper, provided the conjecture is of suffieient interest. If it is proved, then the conjecture becomes a theorem (e.g., Fermat's Last Theorem).

In this chapter, then, we will work on deciding if statements are true or false, and then proving or disproving them.

In order to disprove a statement P, we simply need to prove $\sim P$. One way to do this is through a counterexample.

9.1 Disproving Universal Statements: Counterexamples

Suppose that we are given a universally quantified statement, such as

$$\forall x \in S, P(x).$$

To disprove this statement, we must prove its negation. Its negation is

$$\sim (\forall x \in S, P(x)) = \exists x \in S, \sim P(x).$$

The negation is an existence statement, so to prove that the negation is true, we need only find an example of an $x \in S$ that makes $\sim P(x)$ true, i.e., an $x \in S$ that makes $P(x)$ false.

Things are even simpler if we want to disprove a conditional statement $P(x) \implies Q(x)$. This statement means for every x that makes $P(x)$ true, $Q(x)$ will also be true. Therefore, to disprove $P(x) \implies Q(x)$, we just need to find an x that makes $P(x)$ true and $Q(x)$ false.

An example that disproves a statement is called a **counterexample**.

We will now look at some examples illustrating this idea.

Example: Prove or disprove. Let $A, B,$ and C be three sets. If $A \times C = B \times C$, then $A = B$.

Solution: The elements of $A \times C$ are ordered pairs of the form (x, y), where $x \in A$ and $y \in C$. Let $(x, y) \in A \times C$. If $A \times C = B \times C$, then it follows that $(x, y) \in B \times C$. This says that $x \in B$ and $y \in C$. Conversely, if $(x, y) \in B \times C$, then $(x, y) \in A \times C$, which implies that $x \in A$ also. This seems to suggest that the statement is true.

However, the above argument depends on our assumption that $A \times C$ contains at least one element (x, y). What if $A \times C = \varnothing$? If A or C is empty, this could happen. Suppose $C \neq \varnothing$

and $A \times C = \varnothing$, then A must be empty. But $B \times C = A \times C = \varnothing$ would mean that B must also be empty and so, $A = B$. If $C = \varnothing$, then $A \times C = \varnothing$ and $B \times C = \varnothing$, regardless of A and B. This suggests a different response.

Counterexample: Let $A = \{1\}$, $B = \{2\}$, and $C = \varnothing$. Then $A \times C = B \times C = \varnothing$, but $A \neq B$.

If C were required to be non-empty, then the statement would be true.

Example: Prove the following. Let $A, B,$ and C be three sets, where $C \neq \varnothing$. If $A \times C = B \times C$, then $A = B$.

Proof. Assume that $A \times C = B \times C$. Since $C \neq \varnothing$, the set C contains some element, c. Suppose that $A \neq \varnothing$. Let $x \in A$. Then $(x, c) \in A \times C$. Since $A \times C = B \times C$, it follows that $(x, c) \in B \times C$. Therefore, $x \in B$ and so $A \subseteq B$. By a similar argument, it follows that $B \subseteq A$. Therefore, $A = B$.

If $A = \varnothing$, then $A \times C = \varnothing$, and therefore, $B \times C = \varnothing$. Since $C \neq \varnothing$, this means that $B = \varnothing$ and $A = B$. □

Example: Prove or disprove. Every even integer n can be written as the sum of three distinct even integers.

First, note that this statement is saying that if we are given an even integer n, we can find three distinct even integers $a, b,$ and c such that $n = a + b + c$. Let's check a couple of examples to (hopefully) give us some intuition. Let $n = 0$. Then, we can write $0 = -2 + 0 + 2$, so the statement is true for $n = 0$. It is also true for $n = 2$, since $2 = -2 + 0 + 4$. If $n = 4$, then we can write $n = -2 + 2 + 4$. In fact, it appears that in general, we can write $n = -2 + 2 + n$. Will this always work? Yes, provided that $n \neq -2, 2$. Therefore, it appears that the statement is true, but we need to consider three cases, $n = -2$, $n = 2$, and all other n.

Proof. Let n be an even integer. We show that n is the sum of three distinct even integers by considering the following cases.

Case 1: $n = -2$. Note that we can write $-2 = -4 + 0 + 2$.

Case 3: $n = 2$. Note that we can write $2 = -2 + 0 + 4$.

Case 3: $n \neq -2, 2$. In this case, we can write $n = -2 + 2 + n$.

□

Example: Prove or disprove. For every positive integer n, $n^2 + 5n$ is an odd integer.

Let's look at $n^2 + 5n$ for a few integers. If $n = 1$, then $n^2 + 5n = 1^2 + 5(1) = 6$, which is even. So, we have found a counterexample, and our work is done.

Counterexample: The statement is false. Let $n = 1$. Then $n^2 + 5n = 1 + 5(1) = 6$, which is even. Thus, $n = 1$ is a counterexample.

Exercise: Prove or disprove the following.

(1) For every positive integer, $2^{2^n} \geq 4^{n!}$.

Solution: This statement is false.

Counterexample: Let $n = 3$. Then $2^{2^3} = 2^8 = 256$, but $4^{3!} = 4^6 = 4096$. Therefore, $2^{2^3} < 4^{3!}$ and so $n = 3$ is a counterexample.

(2) If x and y are integers of the same parity, then xy and $(x + y)^3$ are of the same parity.

Solution: This statement is false.

Counterexample: Let $x = 1$ and $y = 3$. Then $xy = 1(3) = 3$, an odd integer but $(x+y)^3 = (1 + 3)^3 = 64$, an even integer. Therefore, xy and $(x + y)^3$ have opposite parity. So, $x = 1$ and $y = 3$ produce a counterexample.

9.2 Disproving Existence Statements

We have spent time disproving universally quantified statements and conditional statements. Now, we will work on disproving an existence statement, such as

$$\exists x \in S, P(x).$$

To disprove this, we need to prove its negation,

$$\sim (\exists x \in S, P(x)) = \forall x \in S, \sim P(x).$$

The negation is universally quantified, so proving it requires us to show that $\sim P(x)$ is true for all $x \in S$, and so counterexamples are not sufficient. In this case, we need to use direct, contrapositive, or contradiction proof to prove the conditional statement "If $x \in S$, then $\sim P(x)$."

Example: Prove or disprove. There is a real-valued solution of the equation

$$x^6 + 2x^2 + 1 = 0.$$

Observation: We can see that the statement is false because x^6 and x^2 are even powers of x, meaning that both are non-negative. Therefore, the left-hand side of the equation is greater than or equal to 1.

Solution: The statement is false.

Disproof. Let $x \in \mathbb{R}$. Then since $x^6 \geq 0$ and $x^2 \geq 0$, it follows that $x^6 + 2x^2 + 1 \geq 1$ and so, $x^6 + 2x^2 + 1 \neq 0$. □

Example: Prove or disprove. There exists a real number x such that $x^3 < x < x^2$.

Observations: If there is a real number x such that $x^3 < x < x^2$, then this number is not 0. Therefore, any number satisfying this property is either positive or negative. Suppose that $x > 0$. Then we can divide $x^3 < x < x^2$ by x to obtain $x^2 < 1 < x$. For all real numbers $x > 1$, however, $x^2 > x$, so there is no positive real number x for which $x^3 < x < x^2$. So, any real number satisfying this relation must be negative. Dividing $x^3 < x < x^2$ by x gives us $x^2 > 1 > x$. If $0 > x > -1$, this does not work since $x^2 < 1$. If $x = -1$, then we also get a false statement. What if $x < -1$? Then $x < 1$ and $x^2 > 1$, so the statement is true. So, we simply provide an example to prove the statement.

Proof. Let $x = -2$. Then $x^2 = 4 > -2$ and $x^3 = (-2)^3 = -8 < -2$. Therefore, $x^3 < x < x^2$. □

Exercise: Prove or disprove. There exists an integer n such that $3n^2 - 5n + 1$ is even.

Observations: If this is true, then there are two possibilities: n is an odd integer or n is an even integer. If n is odd, then $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then

$$3n^2 - 5n + 1 = 3(2k + 1)^2 - 5(2k + 1) + 1 = 12k^2 + 2k - 1 = 2(6k^2 + k - 1) + 1,$$

an odd number. If n is even, then $n = 2l$ for some $l \in \mathbb{Z}$. then,

$$3n^2 - 5n + 1 = 3(2l)^2 - 5(2l) + 1 = 12l^2 - 10l + 1 = 2(6l^2 - 5l) + 1,$$

an odd number. Therefore, the statement is false, and we need to prove the negation of this, which is "For all integers n, $3n^2 - 5n + 1$ is odd."

Solution: Let n be an integer. Then, there are two cases.

Case 1: n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. So,

$$3n^2 - 5n + 1 = 3(2k + 1)^2 - 5(2k + 1) + 1 = 12k^2 + 2k - 1 = 2(6k^2 + k - 1) + 1,$$

an odd number.

Case 2: n is even. Then $n = 2l$ for some $l \in \mathbb{Z}$. So,

$$3n^2 - 5n + 1 = 3(2l)^2 - 5(2l) + 1 = 12l^2 - 10l + 1 = 2(6l^2 - 5l) + 1,$$

an odd number.

9.3 Disproof by Contradiction

Contradiction can be a very useful way to disprove a statement. To see how this works, suppose we wish to disprove a statement P. To disprove P, we must prove $\sim P$. To prove $\sim P$ using

a proof by contradiction means that we assume that $\sim\sim P$ is true and deduct a contradiction. But, since $\sim\sim P = P$, this results in assuming that P is true and deducing a contradiction.

Example: Disprove the statement: There exists an odd integer n such that $n^2 + 2n + 3$ is odd.

Disproof. Suppose by contradiction that this statement is true. So, let n be an odd integer. Then $n = 2k + 1$ for some integer k. Thus,

$$\begin{aligned} n^2 + 2n + 3 &= (2k+1)^2 + 2(2k+1) + 3 \\ &= 4k^2 + 4k + 2 + 4k + 2 + 3 \\ &= 4k^2 + 8k + 6 \\ &= 2(2k^2 + 4k + 3). \end{aligned}$$

Since $2k^2 + 4k + 3$ is an integer, $n^2 + 2n + 3$ is even, a contradiction. Therefore, the statement is false. □

Example: Disprove the statement: There exist odd integers a and b such that $4 \mid (3a^2 + 7b^2)$.

Disproof. Suppose by contradiction that the statement is true. Then let a and b be odd integers. So, $a = 2n + 1$ and $b = 2m + 1$ for some integers m and n. We have that

$$\begin{aligned} 3a^2 + 7b^2 &= 3(2n+1)^2 + 7(2m+1)^2 \\ &= 3(4n^2 + 4n + 1) + 7(4m^2 + 4m + 1) \\ &= 12n^2 + 12n + 3 + 28m^2 + 28m + 7 \\ &= 12n^2 + 28m^2 + 12n + 28m + 10 \\ &= 12n^2 + 28m^2 + 12n + 28m + 8 + 2 \\ &= 4(3n^2 + 7m^2 + 3n + 7m + 2) + 2. \end{aligned}$$

Since $3a^2 + 7b^2 = 4q + r$, where $r = 2$ is the remainder, $4 \nmid (3a^2 + 7b^2)$, a contradiction. Therefore, the statement is false. □

Exercise: Disprove the statement: There is a real number x such that $x^6 + x^4 + 1 = 0$.

Disproof. Suppose by contradiction that this statement is true. Let x be a real number. Then

$$x^6 + x^4 + 1 \geq 1 > 0,$$

a contradiction. Therefore, the statement is false. □

10 Mathematical Induction

Mathematical induction, or **induction** for short, is a very important and useful technique for proving certain types of statements. For example, suppose that we wish to prove the following conjecture.

Conjecture. The sum of the first n natural numbers equals $\dfrac{n(n+1)}{2}$.

We could start by looking at the values for a few n to perhaps give us some intuition.

Table 1: Table for results of summing the first n natural numbers

n	sum of the first n natural numbers	$\dfrac{n(n+1)}{2}$
1	$1 =$	1
2	$1 + 2 =$	3
3	$1 + 2 + 3 =$	6
4	$1 + 2 + 3 + 4 =$	10
5	$1 + 2 + 3 + 4 + 5 =$	15
$\vdots$	$\vdots$	$\vdots$
n	$1 + 2 + 3 + \cdots + n =$	$\dfrac{n(n+1)}{2}$
$\vdots$	$\vdots$	$\vdots$

If you look at the first few lines of Table 1, it does appear that the sum of the first n numbers does, in fact, equal $\dfrac{n(n+1)}{2}$. But, is this conjecture always true (i.e., does the sum always equal that value)? Let's consider writing the statements in the table as follows.

$$
\begin{aligned}
S_1 &: 1 = \frac{1(2)}{2} \\
S_2 &: 1 + 2 = \frac{2(3)}{2} \\
S_3 &: 1 + 2 + 3 = \frac{3(4)}{2} \\
&\vdots \\
S_n &: 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \\
&\vdots
\end{aligned}
$$

We wish to determine if all of the statements are true. The goal of induction is to determine the solution to this type of question. The method is fairly straightforward. The textbook provides

a great analogy. Consider a set of statements $S_1, S_2, \ldots, S_n, \ldots$, which we must prove hold true for all n, as an (infinite) set of dominoes, lined up in a row. Imagine that proving that S_1 is true is like knocking down the S_1 domino. Then, if you can prove that if any statement S_k is true (falling) forces S_{k+1} to also be true (to fall), then you have S_1 knocking down S_2, which knocks down S_3, and so on. So, the conclusion drawn is that all of the dominos are knocked down (i.e., all of the statements are proved true).

Outline for Proof by Induction

Proposition. The statements $S_1, S_2, S_3, \ldots$ are all true.

Proof. (Induction)
(1) Prove that the first statement S_1 is true.
(2) Given any integer $k \geq 1$, prove that the statement $S_k \implies S_{k+1}$ is true.
It follows by mathematical induction that every S_n is true. □

In this type of proof, the first step (1) is called the **base step**, or **basis step**. The second step (2) is called the **inductive step**. In the inductive step, direct proof is most often used to prove $S_k \implies S_{k+1}$, so this step is usually done by assuming that S_k is true and by showing that this forces S_{k+1} to be true. The assumption that S_k is true is called the **inductive hypothesis**.

Proposition 7. If $n \in \mathbb{N}$, then $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$.

Proof. We will prove this with mathematical induction.

(1) If $n = 1$, then this statement is $1 = \dfrac{1(1+1)}{2}$, which is true.

(2) We must now prove that $S_k \implies S_{k+1}$ for any $k \geq 1$. So, we must show that if $1 + 2 + 3 + \cdots + k = \dfrac{k(k+1)}{2}$, then $1 + 2 + 3 + \cdots + k + (k+1) = \dfrac{(k+1)(k+2)}{2}$. We use direct proof. Suppose

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}.$$

Then

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

It follows by induction that $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$ holds for for any natural number n. □

Let's do some more examples.

Proposition 8. If $n \in \mathbb{N}$, then

$$\frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(n+1)(n+2)} = \frac{n}{2n+4}.$$

Proof. We will prove this using induction.

(1) If $n = 1$, then $\dfrac{1}{2 \cdot 3} = \dfrac{1}{2 \cdot 1 + 4} = \dfrac{1}{6}$.

(2) Let $k \geq 1$. Assume that

$$\frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(k+1)(k+2)} = \frac{k}{2k+4}.$$

We wish to show that

$$\frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(k+1)(k+2)} + \frac{1}{(k+2)(k+3)} = \frac{k+1}{2(k+1)+4}.$$

We have that

$$\begin{aligned}
\frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(k+1)(k+2)} + \frac{1}{(k+2)(k+3)} &= \frac{k}{2k+4} + \frac{1}{(k+2)(k+3)} \\
&= \frac{k}{2(k+2)} + \frac{1}{(k+2)(k+3)} \\
&= \frac{k(k+3)+2}{2(k+2)(k+3)} \\
&= \frac{k^2+3k+2}{2(k+2)(k+3)} \\
&= \frac{(k+1)(k+2)}{2(k+2)(k+3)} \\
&= \frac{k+1}{2(k+3)} \\
&= \frac{k+1}{2k+6} \\
&= \frac{k+1}{2(k+1)+4}.
\end{aligned}$$

Therefore, it follows by induction that

$$\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{(n+1)(n+2)}=\frac{n}{2n+4}$$

holds for any natural number n. □

Proposition 9. For every non-negative integer n, $9 \mid (4^{3n}-1)$.

Proof. We will prove this using induction.

(1) If $n=0$, then the statement is $9 \mid (4^{3n}-1)$, or $9 \mid 0$, which is true.

(2) Let $k \geq 0$. Assume that $9 \mid (4^{3k}-1)$. We need to show that $9 \mid (4^{3(k+1)}-1)$.

Since $9 \mid (4^{3k}-1)$, there is an integer x such that $4^{3k}-1=9x$, so $4^{3k}=9x+1$. Since $4^{3(k+1)}=4^{3k}4^3$, we have that

$$\begin{aligned}
4^3 4^{3k} &= 4^3(9x+1)\\
4^{3k+3} &= 4^3(9x+1)\\
4^{3(k+1)}-1 &= 4^3(9x+1)-1\\
&= 64(9x)+64-1\\
&= 9(64x)+63\\
&= 9(64x)+9(7)\\
&= 9(64x+7).
\end{aligned}$$

Since $64x+7$ is an integer, $9 \mid (4^{3(k+1)}-1)$.

Therefore, it follows by induction that $9 \mid (4^{3n}-1)$ for every non-negative integer n. □

Proposition 10. For every positive integer n,

$$1\cdot 3\cdot 5\cdots(2n-1)=\frac{(2n)!}{2^n\cdot n!}.$$

Proof. We will prove this by induction (although it may also be proved directly – exercise).

(1) If $n=1$, then $1=\dfrac{2!}{2^1\cdot 1!}$ is true.

(2) Let $k \geq 1$. Assume that

$$1\cdot 3\cdot 5\cdots(2k-1)=\frac{(2k)!}{2^n\cdot k!}.$$

We need to show that

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

Observe that

$$\begin{aligned}\frac{(2(k+1))!}{2^{k+1}\cdot(k+1)!} &= \frac{(2k+2)!}{2^{k+1}\cdot(k+1)!}\\ &= \frac{(2k+2)(2k+1)\cdot(2k)!}{2\cdot 2^k\cdot(k+1)\cdot k!}\\ &= \frac{(2k+2)(2k+1)}{2(k+1)}\cdot\frac{(2k!)}{2^k\cdot k!}\\ &= (2k+1)[1\cdot 3\cdot 5\cdots(2k-1)]\\ &= 1\cdot 3\cdot 5\cdots(2k-1)\cdot(2(k+1)-1).\end{aligned}$$

Therefore, it follows by induction that

$$1\cdot 3\cdot 5\cdots(2n-1) = \frac{(2n)!}{2^n\cdot n!}$$

for every positive integer n. □

Exercise: Prove that for every positive integer n, $1\cdot 1! + 2\cdot 2! + \cdots + n\cdot n! = (n+1)! - 1$.

Proof. We will prove this by induction.

(1) If $n = 1$, then $1\cdot 1! = 1 = (2!) - 1$.

(2) Let $k \geq 1$. Assume that $1\cdot 1! + 2\cdot 2! + \cdots + k\cdot k! = (k+1)! - 1$. We want to show that $1\cdot 1! + 2\cdot 2! + \cdots + k\cdot k! + (k+1)\cdot(k+1)! = (k+2)! - 1$. We have

$$\begin{aligned}1\cdot 1! + 2\cdot 2! + \cdots + k\cdot k! + (k+1)\cdot(k+1)! &= (k+1)! - 1 + (k+1)\cdot(k+1)!\\ &= (k+1+1)\cdot(k+1)! - 1\\ &= (k+2)\cdot(k+1)! - 1\\ &= (k+2)! - 1.\end{aligned}$$

Therefore, it follows by induction that $1\cdot 1! + 2\cdot 2! + \cdots + n\cdot n! = (n+1)! - 1$ for every positive integer n. □

10.1 Proof by Strong Induction

It occasionally happens in proofs that it is difficult to show that S_k forces S_{k+1} to be true. Instead, you may need the fact that some statements S_m, where $m < k$, force S_{k+1} to be treu. For such situations, there is a slight variant of induction called **strong induction**. Strong induction works just like regular induction, except that in Step (2), instead of assuming that S_k is true and showing that this forces S_{k+1} to be true, we assume that all of the statements

$S_1, S_2, \ldots, S_k$ are true and show this forces S_{k+1} to be true. The domino analogy here is that if it always happens that the first k dominos falling makes the $(k+1)$st domino fall, then all of the dominoes must fall. Below is the outline.

Outline for Proof by Strong Induction

Proposition. The statements $S_1, S_2, S_3, \ldots$ are all true.

Proof. (Strong Induction)
(1) Prove that the first statement S_1 is true.
(2) Given any integer $k \geq 1$, prove $(S_1 \wedge S_2 \wedge S_3 \wedge \cdots \wedge S_k) \implies S_{k+1}$.
It follows by strong mathematical induction that every S_n is true. □

Note that proof by strong induction does not require you to assume that $S_1, S_2, \ldots, S_{k-1}, S_k$ are true to force S_{k+1} to be true. It may be that you only need to assume that S_{k-2} and S_{k-1} are true to force S_{k+1} to be true. Strong induction says that you are allowed to use any (or all) of the statements $S_1, S_2, \ldots, S_k$ to prove that S_{k+1} is true.

Example: A sequence $\{a_n\}$ is defined recursively by

$$a_1 = 1,\ a_2 = 3,\ \text{and } a_n = 2a_{n-1} - a_{n-2} \text{ for } n \geq 3.$$

Prove that $a_n = 2n - 1$ for all $n \in \mathbb{N}$.

Proof. We will prove this using strong induction.

(1) If $n = 1$, then $a_1 = 1 = 2(1) - 1$, so the statement is true.

(2) If $n = 2$, then $a_2 = 3 = 2(2) - 1$, so the statement is true. So, we may let $k \geq 3$ and assume that $a_m = 2m - 1$ for all $1 \leq m \leq k$. We want to show that $a_{k+1} = 2(k+1) - 1 = 2k + 1$. We have

$$\begin{aligned} a_{k+1} &= 2a_k - a_{k-1} \\ &= 2(2k-1) - (2(k-1) - 1) \\ &= (4k - 2) - (2k - 3) \\ &= 2k + 1. \end{aligned}$$

Therefore, it follows by strong induction that $a_n = 2n - 1$ for all $n \in \mathbb{N}$. □

Let's do more examples.

Proposition 11. For each integer $n \geq 8$, there are nonnegative integers a and b such that $n = 3a + 5b$.

Proof. We proceed using strong induction.

(1) If $n = 8$, then we have $8 = 3(1) + 5(1)$, so the statement is true for $n = 8$.

(2) Let $k \geq 8$. Assume that the statement is true for each integer $8 \leq m \leq k$, i.e., for each integer $8 \leq m \leq k$, there exist nonnegative integers s and t such that $m = 3s + 5t$. We want to show that the statement is true for $k + 1$, i.e., we want to show that there exist nonnegative integers x and y such that $k + 1 = 3x + 5y$. We know that if $k + 1 = 9$, then since $9 = 3 \cdot 3 + 5 \cdot 0$, the statement is true, and if $k + 1 = 10$, then since $10 = 3 \cdot 0 + 5 \cdot 2$, the statement is true. Therefore, we may assume that $k + 1 \geq 11$, or $(k + 1) - 3 \geq 8$. In addition, since $(k+1)-3 < k$, we have $8 \leq (k+1)-3 < k$. By the induction hypothesis, there exist nonnegative integers p and q so that

$$(k + 1) - 3 = 3p + 5q, \text{ and so } k + 1 = 3(p + 1) + 5q.$$

So, letting $x = p + 1$ and $y = q$, we have the desired conclusion.

Therefore, it follows by strong induction that for each integer $n \geq 8$, there are nonnegative integers a and b such that $n = 3a + 5b$. □

Exercise: Prove that for any sets $A_1, A_2, \ldots, A_n$ in some universal set U, where $n \geq 2$,

$$\overline{A_1 \cap A_2 \cap \cdots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_n}.$$

Proof. We proceed using strong induction.

(1) If $n = 2$, then we have $\overline{A_1 \cap A_2} = \overline{A_1} \cup \overline{A_2}$, which we have previously proved.

(2) Let $k \geq 2$. Assume that the statment is true for each integer $1 \leq m \leq k$, i.e.,

$$\overline{A_1 \cap A_2 \cap \cdots \cap A_m} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_m}.$$

We want to show that

$$\overline{A_1 \cap A_2 \cap \cdots \cap A_{k+1}} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_{k+1}}.$$

We have

$$\begin{aligned}
\overline{A_1 \cap A_2 \cap \cdots \cap A_{k+1}} &= \overline{(A_1 \cap A_2 \cap \cdots \cap A_{k-1}) \cap (A_k \cap A_{k+1})} \\
&= (\overline{A_1 \cap A_2 \cap \cdots \cap A_{k-1}}) \cup (\overline{A_k \cap A_{k+1}}) \\
&= (\overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_{k-1}}) \cup \overline{A_k \cap A_{k+1}} \\
&= \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_{k-1}} \cup \overline{A_k} \cup \overline{A_{k+1}}.
\end{aligned}$$

Therefore, it follows by strong induction that for any sets $A_1, A_2, \ldots, A_n$ in some universal set U, where $n \geq 2$,

$$\overline{A_1 \cap A_2 \cap \cdots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_n}.$$

□

10.2 Proof by Smallest Counterexample

In this section, we discuss yet another proof technque, called **proof by smallest counterexample**. A nice feature of this method is that it leads you straight to a contradiction – so it is a hybrid of induction and proof by contradiction. An outline of this technique is followed by examples to illustrate its use.

Outline for Proof by Smallest Counterexample

Proposition. The statements $S_1, S_2, S_3, \ldots$ are all true.

Proof. (Smallest Counterexample)
(1) For the sake of contradiction, suppose that not every S_n is true.
(2) Check that the first statement S_1 is true.
(3) Let $k > 1$ be the smallest integer for which S_k is *false*.
(4) Then, S_{k-1} is true and S_k is false. Use this to get a contradiction. □

Example: Prove that for every positive integer n, $6|(n^3 - n)$.

Note: For this problem, we want to show that $6 \mid (k^3 - k)$ for all $k \geq 1$. We can easily see that this is true if $k = 1$. If we were doing a proof by induction, then we would next assume that $6 \mid (k^3 - k)$ and prove that this implies $6 \mid [(k+1)^3 - (k+1)]$. Since $6 \mid (k^3 - k)$, it follows that $k^3 - k = 6x$ for some integer x. Then

$$\begin{aligned}(k+1)^3 - (k+1) &= (k+1)[(k+1)^2 - 1] \\ &= (k+1)(k^2 + 2k) \\ &= k^3 + 3k^2 + 2k \\ &= k^3 - k + 3k^2 + 3k \\ &= 6x + 3k(k+1).\end{aligned}$$

If we can show that $6 \mid 3k(k+1)$, then we have a proof. To do this, we would need to show that $k(k+1)$ is even for every positive integer k. A lemma could be introduced to verify this, and the lemma could be proved by using a direct proof with cases (k is even and k is odd). Alternately, we can do a proof by smallest counterexample.

Proof. (Strongest Counterexample) Assume, to the contrary, that there are values of n such that $6 \nmid (n^3 - n)$. We see that for $n = 1$, we have $6 \mid (1^3 - 1)$, or $6 \mid 0$, which is true. Note

that the statement is also true for $n = 2$, since we obtain $6 \mid (2^3 - 2)$, or $6 \mid 6$. Therefore, the smallest positive integer m for which $6 \nmid (m^3 - m)$ is 3, so we need $m \geq 3$. Thus, we can write $m = k + 2$, where $1 \leq k < m$. We then have

$$\begin{aligned} m^3 - m &= (k+2)^3 - (k+2) \\ &= (k^3 + 6k^2 + 12k + 8) - (k+2) \\ &= (k^3 - k) + (6k^2 + 12k + 6) \end{aligned}$$

Since $k < m$, it follows that

$$\begin{aligned} m^3 - m &= 6x + (6k^2 + 12k + 6) \\ &= 6(x + k^2 + 2k + 1). \end{aligned}$$

Since $x + k^2 + 2k + 1$ is an integer, $6 \mid (m^3 - m)$, which is a contradiction to our assumption. □

Example: Prove that for every nonnegative integer n, $3 \mid (2^{2n} - 1)$.

Proof. (Strongest Counterexample) Assume, to the contrary, that there are nonnegative integers n for which $3 \nmid (2^{2n} - 1)$. Then there is a smallest nonnegative integer m such that $3 \nmid (2^{2m} - 1)$. So, we have that $3 \nmid (2^{2m} - 1)$ and $3 \mid (2^{2n} - 1)$ for all integers $0 \leq n < m$. We know that $3 \mid (2^{2n} - 1)$ for $n = 0$, so it follows that $m \geq 1$. Therefore, m can be expressed as $m = k + 1$, where $0 \leq k < m$. Thus, $3 \mid (2^{2k} - 1)$, which implies that $2^{2k} - 1 = 3x$ for some integer x, so $2^{2k} = 3x + 1$. Observe that

$$\begin{aligned} 2^{2m} - 1 &= 2^{2(k+1)} - 1 \\ &= 2^{2k+2} - 1 \\ &= 2^2 2^{2k} - 1 \\ &= 4(3x + 1) - 1 \\ &= 12x + 3 \\ &= 3(4x + 1). \end{aligned}$$

Since $4x + 1$ is an integer, $3 \mid (2^{2m} - 1)$, a contradiction. □

10.3 Fibonacci Numbers

Leonardo Pisano (now known as Fibonacci) was a mathematician who was born around 1175 in what is now Italy. He is best known today for a number sequence that he described in his book *Liber Abaci*, which is known as the **Fibonacci sequence**. The Fibonacci sequence is

$$1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21, \ldots.$$

The numbers that appear in this sequence are called **Fibonacci numbers**. We will denote the nth Fibonacci number as F_n. Then, the Fibonacci sequence is defined by

$$F_1 = 1,\ F_2 = 2,\ F_n = F_{n-1} + F_{n-2}.$$

The sequence appears uncannily often in nature, and it is also a great source of induction problems. In fact, it can be proved that

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \frac{1+\sqrt{5}}{2}.$$

Proposition 12. For all $n \in \mathbb{N}$,

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Proof. This statement can be proved using strong induction. First, we will show that the formula is valid for $n = 1$. If $n = 1$, we have

$$1 = F_1 = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^1 - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^1,$$

which is true. Now, let $k \geq 1$ and suppose that the formula is true for all $1 \leq m \leq k$. Observe that

$$\left(\frac{1\pm\sqrt{5}}{2}\right)^2 = \frac{3\pm\sqrt{5}}{2} = \frac{1\pm\sqrt{5}}{2} + 1.$$

From the definition of the Fibonacci numbers, we have

$$\begin{aligned}
F_{k+1} &= F_k + F_{k-1} \\
&= \left[\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^k\right] + \left[\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right] \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k + \left(\frac{1+\sqrt{5}}{2}\right)^{k-1} + \left(\frac{1-\sqrt{5}}{2}\right)^k + \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right] \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k-1}\left(\frac{1+\sqrt{5}}{2}+1\right) + \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\left(\frac{1-\sqrt{5}}{2}+1\right)\right] \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k-1}\left(\frac{1+\sqrt{5}}{2}\right)^2 + \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\left(\frac{1-\sqrt{5}}{2}\right)^2\right] \\
&= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k+1}.
\end{aligned}$$

Therefore, by strong induction, for all $n \in \mathbb{N}$,

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

□