How to Prove Conditional Statements – Part II of Hammack

Dr. Doreen De Leon
Math 111, Fall 2014

4 Direct Proof

Now, we will begin the proving of some theorems, a skill which you will need in the upper division courses for which Math 111 is a prerequisite. For clarity, we will define theorem, proof, and definition. A **theorem** is a mathematical statement that is true and can be (and has been) verified as true. A **proof** of a theorem is a written verification that shows that the theorem is true. A **definition** is an exact, unambiguous explanation of the meaning of a mathematical word or phrase. Proofs typically utilize definitions and theorems, as well as mathematical operations.

4.1 Theorems

As stated above, a **theorem** is a statement that is true and has been proven to be true. You have already encountered theorems in your Calculus text. A couple of examples are

Theorem 1 (Mean Value Theorem)**.** If a function f is continuous on the closed interval $[a, b]$, where $a < b$, and differentiable on the open interval (a, b), then there exists a point $c \in (a, b)$ such that

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$

Theorem 2 (Intermediate Value Theorem)**.** If a function f is continuous on the closed interval $[a, b]$ and if u is a number between $f(a)$ and $f(b)$, then there exists a point $c \in (a, b)$ such that $f(c) = u$.

The above theorems are stated in a conditional form. Many theorems are either stated in a conditional form or may be put into a conditional form. There are exceptions to this, however. For example, we have the following theorem.

Theorem 3. The real number $\sqrt{2}$ is irrational.

There are other words in mathematics that mean roughly the same thing as theorem. Typically, the word "theorem" is used for a statement that is considered important or significant. A statement that is true but not as significant is sometimes called a **proposition**. A **lemma** is a theorem whose main purpose is to help prove another thoerem. A **corollary** is a mathematical result that can be deduced from, and is thereby a consequence of, a theorem or proposition.

Our main goal in this class is to learn how to prove theorems. Since most theorems are stated in conditional form (or can be easily restated in conditional form), our work in Chapter 2 wshould be helpful.

4.2 Definitions

A proof of a theorem must be absolutely convincing mathematically, avoiding any ambiguity. The exact meaning of each mathematical term must be agreed on by everyone. For example, the following are commonly used definitions.

Definition. An integer n is **even** if $n = 2a$ for some integer a.

Definition. An integer n is **odd** if $n = 2k + 1$ for some integer k.

So, we know that 12 is even, since $12 = 2 \cdot 6$, and 15 is odd, since $15 = 2 \cdot 7 + 1$.

A related definition:

Definition. Two integers have the **same parity** if they are both even or they are both odd. Otherwise, they have **opposite parity**.

Notes:

1. In these typed notes, the word or term being defined is typically in boldfaced type. In the in-class notes written on the board, the term being defined is underlined.
2. Defintiions really are biconditional statements, even though they are typically not stated in that form. So, for example, the definition of an odd integer really means: "*An integer n is odd if and only if $n = 2k + 1$ for some $k \in \mathbb{Z}$.*"

Let's look at a few more definitions before we begin working on proofs.

Definition. Suppose a and b are integers. We say that a **divides** b, written $a \mid b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case, we also say that a is a **divisor** of b, and that b is a **multiple** of a.

For example, 6 divides 12 because $12 = 6 \cdot 2$. We write this as $6 \mid 12$. However, 5 does not divide 12 since there is no integer c for which $12 = 5c$. This is written as $5 \nmid 12$. Every integer has a set of integers that divides it. For example, the set of divisors of 12 is $\{1, 2, 3, 6, 12\}$. The ser of divisors of 0 is $\mathbb{Z}$.

Definition. A natural number n greater than 1 is **prime** if it has exactly two positive divsors, 1 and n. A natural number n is a **composite number** if it can be written as $n = ab$, where $1 < a < n$ and $1 < b < n$.

For example, the first few prime numbers are 2, 3, 5, and 7. The number 4 is not a prime number because it is divisible by 2.

Definition. The **greatest common divisor** of two integers a and b, not both 0, denoted $\gcd(a, b)$, is the largest positive integer that divides both a and b. The **least common multiple** of two non-zero integers a and b, denoted $\text{lcm}(a, b)$, is the smallest positive integer that is a multiple of both a and b.

For example, $\gcd(4, 12) = 4$ and $\text{lcm}(4, 12) = 24$. What about $\gcd(0, 5)$? Since every number divides 0, we know that 5 divides 0, so $\gcd(0, 5) = 5$. Why do we require that both integers cannot be zero in the definition of the greatest common divisor? If we tried to find $\gcd(0, 0)$, since every integer divides 0, there is no greatest common divisor.

We will accept the following without proof.

Fact. Suppose a and b are integers. then:

- $a + b \in \mathbb{Z}$
- $a - b \in \mathbb{Z}$
- $ab \in \mathbb{Z}$

Note that the second statement is a consequence of the first and third statements (since $a - b = a + (-1)b$). Also, these three statements may be combined. So, we can say that if $a, b, c \in \mathbb{Z}$, then $a^2 + b^2 + c^2 - 2abc \in \mathbb{Z}$.

Two other useful theorems follow.

Theorem 4. Every natural number greater than 1 has a unique factorization into primes.

Theorem 5 (The Division Algorithm)**.** Given integers a and b with $b > 0$, there exist unique integers q and r for which $a = qb + r$ and $0 \leq r < b$.

Example: Suppose that $a = -78$ and $b = 17$. Then, we know that $-78 = (17)(-5) + 7$, so from the theorem $q = -5$ and $r = 7$.

4.3 Direct Proof

We will now start discussing the technique of direct proof. First, consider that we have a proposition (or theorem, etc.) to be proved that takes the following form.

Proposition. If P, then Q.

So, the proposition is a conditional statement of the form $P \implies Q$. Our goal is to show that this statement is true. To see what we need to do, recall that the truth table for $P \implies Q$ looks like

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

We see that if P is false, the statement $P \implies Q$ is automatically true. This means that if we want to show that $P \implies Q$ is true, we don't need to worry about the situations where P is false; we need only focus on the situations when P is true. We must show that P being true forces Q to be true, as well, because this means that the second line of the table cannot happen.

So, the outline for a direct proof is as follows.

Outline for Direct Proof

Proposition. If P, then Q.

Proof. Suppose P.
⋮
Therefore Q. □

We will now do some examples.

Examples

Proposition 1. If n is an odd integer, then $3n + 7$ is an even integer.

Proof. Suppose n is an odd integer.
Then $n = 2a + 1$ for some $a \in \mathbb{Z}$ by definition of an odd number.
Then

$$3n + 7 = 3(2a + 1) + 7 = 6a + 3 + 7 = 6a + 10 = 2(3a + 5).$$

Since $3a + 5 \in \mathbb{Z}$, $3n + 7$ is even. Therefore, $3n + 7$ is an even integer if n is an odd integer. □

Proposition 2. If n is an even integer, then $3n^5$ is an even integer.

Proof. Suppose n is an even integer.
Then, $n = 2a$ for some $a \in \mathbb{Z}$.
Then,

$$3n^5 = 3(2a)^5 = 3(32a^5) = 96a^5 = 2(48a^5).$$

Since $48a^5 \in \mathbb{Z}$, $3n^5$ is an even integer. □

Proposition 3. If x and y are real numbers, then $2xy \leq x^2 + y^2$

Scratch work: We need to show that $2xy \leq x^2 + y^2$, or $0 \leq x^2 - 2xy + y^2$. But, the right-hand side is actually $(x - y)^2$, which is nonnegative, so the statement is true.

Proof. Suppose that x and y are real numbers.
Then,

$$0 \leq (x - y)^2, \text{ i.e., } 0 \leq x^2 - 2xy + y^2.$$

Add $2xy$ to both sides to obtain

$$2xy \leq x^2 + y^2.$$

□

Proposition 4. Let $S = \{1, 2, 3\}$ and let $n \in S$. If $\dfrac{n(n+3)}{2}$ is even, then $\dfrac{(n+2)(n-5)}{2}$ is even.

Proof. Let $n \in S$ such that $\dfrac{n(n+3)}{2}$ is even.
Since $\dfrac{n(n+3)}{2} = 2$ when $n = 1$, $\dfrac{n(n+3)}{2} = 5$ when $n = 2$, and $\dfrac{n(n+3)}{2} = 9$ when $n = 3$, it follows that $n = 1$.
When $n = 1$,

$$\frac{(n+2)(n-5)}{2} = -6.$$

Therefore, $\dfrac{(n+2)(n-5)}{2}$ is even. □

4.4 Using Cases

When proving a statement is true, we sometimes need to consider two or more cases to show that the statement is true in all possible scenarios. This method of proof is called **proof by cases**.

Examples:

Proposition 5. If $n \in \mathbb{Z}$, then $n^2 + 3n + 5$ is an odd integer.

There are two relevant possibilities for n: either n is odd or n is even. We must determine the truth of this statement for both cases.

Proof.

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

$$\begin{aligned} n^2 + 3n + 5 &= (2a)^2 + 3(2a) + 5 \\ &= 4a^2 + 6a + 5 \\ &= 2(2a^2 + 3a + 2) + 1. \end{aligned}$$

Since $2a^2 + 3a + 2 \in \mathbb{Z}$, $n^2 + 3n + 5$ is odd.

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

$$\begin{aligned} n^2 + 3n + 5 &= (2b + 1)^2 + 3(2b + 1) + 5 \\ &= 4b^2 + 10b + 9 \\ &= 2(2b^2 + 5b + 4) + 1. \end{aligned}$$

Since $2b^2 + 5b + 4 \in \mathbb{Z}$, $n^2 + 3n + 5$ is odd.

These cases show that $n^2 + 3n + 5$ is odd for all integers n. □

Proposition 6. Let $x, y \in \mathbb{Z}$. Then if x and y are of the same parity, then $x + y$ is even.

Proof. Assume that x and y are of the same parity. There are two cases to consider.

Case 1: x and y are even. Then $x = 2a$ and $y = 2b$ for some integers a and b. So, $x + y = 2a + 2b = 2(a + b)$. Since $a + b \in \mathbb{Z}$, $x + y$ is even.

Case 2: x and y are odd. Then $x = 2a + 1$ and $y = 2b + 1$ for some $a, b \in \mathbb{Z}$. So, $x + y = 2(a + 1) + 2(b + 1) = 2a + 2 + 2b + 2 = 2(a + b + 2)$. Since $a + b + 2 \in \mathbb{Z}$, $x + y$ is even.

The above cases show that $x + y$ is even if x and y are of the same parity. □

Exercise: Let $a, b \in \mathbb{Z}$. Prove that if ab is odd, then $a^2 + b^2$ is even.

4.5 Treating Similar Cases

Sometimes, two or more cases in a proof will be so similar that writing them separately is unnecessary. A nice example is in the textbook.

Proposition 7. If two integers have opposite parity, then their sum is odd.

Proof. Suppose m and n are two integers of opposite parity. We want to show that $m + n$ is odd. This is done in two cases, as follows.

Case 1: Suppose m is even and n is odd. Then $m = 2a$ and $n = 2b + 1$ for some integers a and b. Therefore,

$$m + n = 2a + 2b + 1 = 2(a + b) + 1,$$

which is odd since $a + b \in \mathbb{Z}$.

Case 2: Suppose m is odd and n is even. Then $m = 2a + 1$ and $n = 2b$ for some integers a and b. Therefore,

$$m + n = 2a + 1 + 2b = 2(a + b) + 1,$$

which is odd since $a + b \in \mathbb{Z}$.

Therefore, $m + n$ is odd for any two integers m and n of opposite parity. □

Note that the two cases in this proof are identical, except for the order in which the even and odd terms occur. In this situation, we need only do one case and indicate that the other case is nearly identical by using the phrase "Without loss of generality, ..." So, without further ado, the concise proof of the proposition follows.

Proof. Suppose m and n are two integers of opposite parity. We want to show that $m + n$ is odd. Without loss of generality, suppose that m is even and n is odd. Then $m = 2a$ and $n = 2b + 1$ for some integers a and b. Therefore,

$$m + n = 2a + 2b + 1 = 2(a + b) + 1,$$

which is odd by definition. □

Let's look at another example.

Proposition 8. Let a and b be integers. Then if a is even or b is even, ab is even.

Proof. Suppose that a and b are integers. Without loss of generality, suppose that a is even. Then $a = 2k$ for some integer k. So

$$ab = 2k(b) = 2(kb),$$

which is even by definition since kb is an integer. □

Exercises: Evaluate the following proofs.

Proposition 9. If x and y are integers of the same parity, then $x - y$ is even.

Proof. Let x and y be two integers of the same parity. We consider two cases, when x and y are both even and when they are both odd.

Case 1: x and y are both even. Let $x = 6$ and $y = 2$, which are both even. Then $x - y = 4$, which is even.

Case 2: x and y are both odd. Let $x = 7$ and $y = 1$, which are both odd. Then $x - y = 6$, which is even.

□

Evaluation:

Proposition 10. If m is an even integer and n is an odd integer, then $3m + 5n$ is odd.

Proof. Let m be an even integer and n be an odd integer. Then $m = 2a$ and $n = 2a + 1$ for some $a \in \mathbb{Z}$. Therefore,

$$\begin{aligned} 3m + 5n &= 3(2a) + 5(2a + 1) = 6a + 10a + 5 \\ &= 16a + 5 \\ &= 2(8a + 2) + 1. \end{aligned}$$

Since $8a + 2$ is an integer, $3m + 5n$ is odd. □

Evaluation:

5 Contrapositive Proof

One alternative to a direct proof is a **contrapositive proof**. Contrapositive proofs are also used to prove conditional statements of the form "If P, then Q."

5.1 Contrapositive Proof

Suppose that we wish to solve a proposition of the form **Proposition.** If P, then Q.

This is a conditional statement of the form $P \implies Q$, and our goal is to show that this statement is true. In Section 2.6, we showed that this is logically equivalent to showing $\sim Q \implies \sim P$, known as the **contrapositive form** of $P \implies Q$. Since the two statements are logically equivalent, it follows that to prove that $P \implies Q$, it is sufficient to prove that $\sim Q \implies \sim P$. Using direct proof to show that $\sim Q \implies \sim P$ we would assume that $\sim Q$ is true and use this to deduce that $\sim P$ is true. This is known as a **contrapositive proof**.

So, the outline for a contrapositive proof is as follows.

Outline for Contrapositive Proof

Proposition. If P, then Q.

Proof. Suppose $\sim Q$.

$\vdots$

Therefore $\sim P$. $\square$

Let's look at some examples.

Proposition 11. If $11x - 7$ is even, then x is odd.

This proposition is easier to prove using contrapositive proof. What is the contrapositive of the statement? Let

P: $11x - 7$ is even;

Q: x is odd.

Then $\sim Q$ is x is not odd, or x is even; and $\sim P$ is $11x - 7$ is not even, or $11x - 7$ is odd.

Proof. (Contrapositive) Assume that x is even. Then $x = 2a$ for some $a \in \mathbb{Z}$. Therefore,

$$11x - 7 = 11(2a) - 7 = 22a - 7 = 22a - 8 + 1 = 2(11a - 4) + 1.$$

Since $11a - 4 \in \mathbb{Z}$, $11x - 7$ is odd. $\square$

Proposition 12. Let $A = \{0, 1, 2\}$ and $B = \{4, 5, 6\}$ be subsets of $S = \{0, 1, 2, 3, 4, 5, 6\}$. Let $n \in S$. Prove that if $\dfrac{n(n-1)(n-2)}{6}$ is even, then $n \in A \cup B$.

Proof. (Contrapositive) Suppose that $n \notin A \cup B$. Then $n \in S - (A \cup B)$. Since $A \cup B = \{0, 1, 2, 4, 5, 6\}$, this means that $n \in \{3\}$, or $n = 3$. Therefore,

$$\frac{n(n-1)(n-2)}{6} = \frac{3(3-1)(3-2)}{6} = 1,$$

which is odd. Therefore, $\dfrac{n(n-1)(n-2)}{6}$ is odd. □

Proving "If P, then Q," using proof by contrapositive requires us to determine the negated statements $\sim P$ and $\sim Q$. In working with these, we may need to use the techniques for negating statements that we discussed in Section 2.10.

Proposition 13. Let a and b be integers. If ab is even, then a is even or b is even.

In this case,

P: ab is even;

Q: a is even or b is even.

So, $\sim P$ is simply ab is not even, or ab is odd. However, $\sim Q$ is that it is not true that a is even or b is even. Using DeMorgan's law, this is equivalent to it is not true that a is even and it is not true that b is even, or a is odd and b is odd. Now, we are ready to prove the statement.

Proof. Suppose that a and b are integers and that a and b are both odd. Then $a = 2m + 1$ for some $m \in \mathbb{Z}$ and $b = 2n + 1$ for some $n \in \mathbb{Z}$. Therefore,

$$ab = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1.$$

Since $2(2mn + m + n)$ is an integer, ab is odd. □

5.2 Congruence of Integers

Definition. Given integers a and b and an $n \in \mathbb{N}$, we say that a and b are **congruent modulo** n if $n \mid (a - b)$. We express this as $a \equiv b \pmod{n}$. If a and b are not congruent modulo n, we write this as $a \not\equiv b \pmod{n}$.

Examples.

1. $9 \equiv 1 \pmod 4$ because $4 \mid (9-1)$.
2. $25 \equiv 4 \pmod 3$ because $3 \mid (25-4)$.
3. $10 \equiv -3 \pmod{13}$ because $13 \mid (10-(-3))$.
4. $3 \equiv 11 \pmod 4$ because $4 \mid (3-11)$.

The idea here is that $a \equiv b \pmod n$ means that a and b have the same remainder when divided by n. For example, $3 \equiv 11 \pmod 4$, and we see that both 3 and 11 have the same remainder when divided by 4. In general, note that if a and b both have the same remainder r when divided by n, then it follows that $a = kn + r$ and $b = ln + r$, for some $k, l \in \mathbb{Z}$. Then, $a - b = (kn + r) - (ln + r) = n(k - l)$. But, $a - b = n(k - l)$ means that $n \mid (a - b)$, so $a \equiv b \pmod n$. Conversely, we can show that if $a \equiv b \pmod n$, then a and b have the same remainder when divided by n.

Let's do some examples of proofs involving congruence of integers.

Proposition 14. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod n$ and $a \equiv c \pmod n$, then $c \equiv b \pmod n$.

Proof. Suppose that $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, and that $a \equiv b \pmod n$ and $a \equiv c \pmod n$. This means that $n \mid (a - b)$ and $n \mid (a - c)$. Thus, there are integers k and l such that $a - b = nk$ and $a - c = nl$. Subtracting the second equation from the first gives $c - b = nk - nl = n(k - l)$. Therefore, $n \mid (c - b)$ and $c \equiv b \pmod n$ by definition of congruence modulo n. □

Proposition 15. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod n$, then $a^3 \equiv b^3 \pmod n$.

Proof. Suppose that $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, and that $a \equiv b \pmod n$. This means that $n \mid (a - b)$, so there is an integer k for which $a - b = nk$. Then,

$$\begin{aligned} a - b &= nk \\ (a - b)(a^2 + ab + b^2) &= nk(a^2 + ab + b^2) \\ a^3 + a^2b + ab^2 - ba^2 - ab^2 - b^3 &= nk(a^2 + ab + b^2) \\ a^3 - b^3 &= nk(a^2 + ab + b^2). \end{aligned}$$

Since $a^2 + ab + b^2 \in \mathbb{Z}$, we have that $n \mid (a^3 - b^3)$ and so, $a^3 \equiv b^3 \pmod n$. □

5.3 Mathematical Writing

Some guidelines for good mathematical writing are

1. Never begin a sentence with a mathematical symbol. (Example: Don't say, "x is an integer, so x^2 is an integer." Instead, say "Since x is an integer, x^2 is an integer.")

2. End each sentence with a period, even if the sentence ends with a mathematical symbol or expression.

3. Separate mathematical symbols or expressions with words. (Example: Don't say, "If $x^2 - 1 = 0$, $x = 0$ or $x = 1$." Instead, say "If $x^2 - 1 = 0$, then $x = 0$ or $x = 1$.")

4. Don't use symbols in place of words, where words are more appropriate.

5. Don't use a symbol if it is not needed. (Example: Don't say, "Two matrices A and B are equal if they are the same size and corresponding entries are equal." Why? The names of the matrices are not essential, since they are not used in the remainder of the statement. Instead, simply say, "Two matrices are equal if they are the same size and corresponding entries are equal."

6. Use the first person plural; i.e., when doing mathematical writing, use "we" and "us" instead of "I," "me," or "you."

7. Use the active voice wherever possible. (Example: You could say, "The desired result is obtained by multiplying both sides by -1." However, it reads better if we say, "Multiplying both sides by -1 gives the desired result."

8. Explain each new symbol that you introduce.

9. Make sure that pronoun references are clear; e.g., don't use "it" when there are two preceding objects.

10. Be careful of the use of "since," "because," "as for," and "so." For example "Q since P" means that P is true and therefore, Q is true.

11. "Thus," "hence," "therefore," and "consequently" all precede a statement that follows logically from previous statements or clauses.

Exercise: Prove the following statement using either direct or contrapositive proof. Sometimes one approach will be much easier than the other.

(1) Suppose $x \in \mathbb{Z}$. If $x^3 - 1$ is even, then x is odd.

(2) If n is odd, then $8 \mid (n^2 - 1)$.

Solution:

(1) *Proof.* (Contrapositive) Suppose that x is not an odd integer. Then, x is an even integer. Therefore, $x = 2a$ for some integer a. So,

$$x^3 - 1 = (2a)^3 - 1 = 8a^3 - 1 = 8a^3 - 2 + 1 = 2(4a^3 - 1) + 1.$$

Since $4a^3 - 1$ is an integer, $x^3 - 1$ is odd. □

(2) *Proof.* (Direct) Suppose that n is an odd integer. Then $n = 2a + 1$ for some integer a. Then

$$n^2 - 1 = (2a + 1)^2 - 1 = 4a^2 + 4a = 4a(a + 1).$$

So far, we have that $n^2 - 1 = 4a(a + 1)$. But we need to show that $8 \mid (n^2 - 1)$. If we consider the product $a(a+1)$, one of a or $a+1$ must be even and the other odd. Therefore, $a(a+1)$ is even and $a(a+1) = 2k$ for some integer k. This means that $n^2-1 = 4(2k) = 8k$, or $8 \mid (n^2 - 1)$. □

6 Proof by Contradiction

The method of **proof by contradiction** may be used to prove any kind of statement, including conditional statements. A proof by contradiction is done as follows.

Let P be a statement that we wish to prove. We start by assuming that P is a false statement. Our goal is to arrive at or deduce a statement that contradicts some assumption that we made in the proof or some known fact (e.g., a definition, a theorem, etc.). If we denote this assumption, or known fact, by C, then what we have deduced is $\sim C$. In other words, we have shown that $\sim P \implies \sim C$ is true, where $\sim C$ is false. Therefore, $\sim P$ is false and so P is true.

6.1 Proving Statements with Contradiction

The outline for a proof by contradiction is as follows.

Outline for Proof by Contradiction

Proposition. P.

Proof. Suppose $\sim P$.
⋮
Therefore $\sim C$, which is false since C is true. □

Now, we will do some examples to illustrate this technique. To enable us to do a larger variety of proofs, we introduce the following definition.

Definition. A real number x is **rational** if $x = \dfrac{a}{b}$ for some $a, b \in \mathbb{Z}$ where $b \neq 0$. A real number x is **irrational** if it is not rational, i.e., if $x \neq \dfrac{a}{b}$ for every $a, b \in \mathbb{Z}$ with $b \neq 0$.

Proposition 16. There is no smallest positive real number.

Proof. Assume, to the contrary, that there is a smallest positive real number, say r. Since $0 < \frac{r}{2} < r$, it follows that $\frac{r}{2}$ is a positive real number that is smaller than r. This is a contradiction to our assumption that r is the smallest positive real number. □

Proposition 17. No odd integer can be expressed as the sum of three even integers.

In this case, we consider

$$P: \text{ No odd integer can be expressed as the sum of three even integers.}$$

To give a proof by contradiction, we need to determine $\sim P$. The negation $\sim P$ is

$$\sim P: \text{ There exists an odd integer that can be expressed as the sum of three even integers.}$$

Proof. Assume, to the contrary, that there exists an odd integer n which can be expressed as the sum of three even integers, x, y, and z. Then, $x = 2a$, $y = 2b$, and $z = 2c$, where $a, b, c \in \mathbb{Z}$. Therefore,

$$n = x + y + z = 2a + 2b + 2c = 2(a + b + c).$$

Since $a + b + c$ is an integer, n is even, a contradiction. □

Proposition 18. The sum of a rational number and an irrational number is irrational.

Proof. Assume, to the contrary, that there exist a rational number x and an irrational number y whose sum is a rational number z. Thus, $x + y = z$, where $x = \frac{a}{b}$ and $z = \frac{c}{d}$ for some integers a, b, c, and d where $b, d \neq 0$. This implies that

$$y = z - x = \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd}.$$

Since $bc - ad$ and bd are integers with $bd \neq 0$, it follows that y is rational, which is a contradiction. □

6.2 Proving Conditional Statements by Contradiction

In this section, we will exclusively deal with proving conditional statements. So, suppose we are given the proposition below.

Proposition. If P, then Q.

Then, the negation of $P \implies Q$ is $P \wedge \sim Q$ (or, P and $\sim Q$). So, a proof by contradiction of a conditional statement begins with the assumption P and $\sim Q$, and tries to deduce a statement that contradicts some assumption made in the proof or a known fact. Let's do an example to illustrate this.

Proposition 19. If a is an even integer and b is an odd integer, then $4 \nmid (a^2 + 2b^2)$.

First, we need to construct the negation of this statement. We have

P: a is an even integer and b is an odd integer.

Q: $4 \nmid (a^2 + 2b^2)$.

For a proof by contradiction, we need to assume that P and $\sim Q$. $\sim Q$ is simply

$$\sim Q : \ 4 \mid (a^2 + 2b^2).$$

Proof. Assume, to the contrary, that there exists an even integer a and an odd integer b such that $4 \mid (a^2 + 2b^2)$. Then $a = 2x$ and $b = 2y + 1$ for some integers x and y, and $a^2 + 2b^2 = 4z$ for some integer z. Thus, we have

$$\begin{aligned} 4z &= a^2 + 2b^2 \\ &= (2x)^2 + 2(2y + 1)^2 \\ &= 4x^2 + 8y^2 + 8y + 2 \\ \implies 2z &= 2x^2 + 4y^2 + 4y + 1 \\ &= 2(x^2 + 2y^2 + 2y) + 1. \end{aligned}$$

Since $x^2 + 2y^2 + 2y$ is an integer, the right-hand side is odd, but $2z$ is even, a contradiction. □

Proof. (Alternate proof) Assume, to the contrary, that there exists an even integer a and an odd integer b such that $4 \mid (a^2 + 2b^2)$. Then $a = 2x$ and $b = 2y + 1$ for some integers x and y, and $a^2 + 2b^2 = 4z$ for some integer z. Thus, we have

$$\begin{aligned} 4z &= a^2 + 2b^2 \\ &= (2x)^2 + 2(2y + 1)^2 \\ &= 4x^2 + 8y^2 + 8y + 2 \\ \implies 2 &= 4z - 4x^2 - 8y^2 - 8y \\ &= 4(z - x^2 - 2y^2 - 2y). \end{aligned}$$

Since $z - x^2 - 2y^2 - 2y$ is an integer, we have that $4 \mid 2$, which is impossible. □

6.3 Combining Techniques

Often, especially in more complicated proofs, multiple proof techniques are combined in a single proof. One example of this is proof by contradiction combined with direct proof by cases. Or, direct proof may be combined with proof by contradiction.

Proposition 20. The integer 100 cannot be written as the sum of three integers, an odd number of which are odd.

We will prove this by contradiction. So,

Proof. Assume, to the contrary, that 100 can be written as the sum of three integers a, b, and c, an odd number of which are odd. We consider two cases.

Case 1: Exactly one of a, b, and c is odd. Without loss of generality, assume that a is odd. Then, $a = 2x + 1$, $b = 2y$, and $c = 2z$ for some $x, y, z \in \mathbb{Z}$. So,

$$100 = a + b + c = (2x + 1) + 2y + 2z = 2(x + y + z) + 1.$$

Since $x + y + z$ is an integer, we conclude that 100 is odd, a contradiction.

Case 2: All of a, b, and c are odd. Then, $a = 2x + 1$, $b = 2y + 1$, and $c = 2z + 1$. So,

$$100 = a + b + c = (2x + 1) + (2y + 1) + (2z + 1) = 2(x + y + z + 1) + 1.$$

Since $x + y + z + 1$ is an integer, we conclude that 100 is odd, a contradiction.

□

6.4 Some Words of Advice

Proof by contradiction should not be your "go-to" proof. It is best to first consider a direct proof or a contrapositive proof, going to proof by contradiction if the other approaches do not work.

Exercises: Prove the following using proof by contradiction.

1. Suppose $n \in \mathbb{Z}$. If n is odd, then n^2 is odd.
2. $\sqrt[3]{2}$ is irrational.

Solutions:

1. Assume, to the contrary, that there exists an integer n such that n is odd and n^2 is even. Then $n = 2a + 1$ for some integer a. So,

$$n^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1.$$

Since $2a^2 + 2a$ is an integer, n^2 is odd, a contradiction.

2. Assume, to the contrary, that $\sqrt[3]{2}$ is rational. Then there exist integers a and b, where $b \neq 0$, for which $\sqrt[3]{2} = \dfrac{a}{b}$. Assume, without loss of generality, that this fraction is in reduced form so that a and b are not both even. Since $\sqrt[3]{2} = \dfrac{a}{b}$, we have

$$\left(\sqrt[3]{2}\right)^3 = \left(\frac{a}{b}\right)^3.$$

So,

$$\begin{aligned} 2 &= \frac{a^3}{b^3} \\ \implies a^3 &= 2b^3. \end{aligned}$$

Thus, a^3 is even, from which we deduce that a is even. (Why? This might be a lemma proved before the main proposition.) Since a is even, $a = 2d$ for some integer d. And, we have

$$(2d)^3 = 2b^3 \implies 8d^3 = 2b^3,$$

or $b^3 = 4d^3 = 2(2d^3)$. Therefore, b^3 is even, from which we deduce that b is even, a contradiction.

Note that in Exercise 1 above, it would have been just as easy, and perhaps more illuminating, to prove the statement directly. However, for Exercise 2, proof by contradiction is the best way to proceed. In the previous section, Proposition 17 could have easily been proved using direct proof.