Section 4.1 – Direct Proof and Counterexample I: Introduction

The underlying content of this chapter is number theory, and we will prove number theoretic statements, mostly involving even and odd integers, and composite and prime numbers.

Note that most quotients of integers are ***NOT*** integers. $3 \div 2 = \frac{3}{2} = 1.5$ is not an integer, and $3 \div 0 = \frac{3}{0}$ isn't even a number!

If we are going to evaluate the truth or falsity of a statement, we first need to understand what the statement is about. This means we need some carefully constructed, precise, and formally quantified definitions:

An integer n is **even** if, and only if, n equals twice some integer. An integer n is **odd** if, and only if, n equals twice some integer plus 1.

Symbolically, for any integer, n

$$\begin{aligned} n \text{ is even} &\Leftrightarrow n = 2k \text{ for some integer } k \\ n \text{ is odd} &\Leftrightarrow n = 2k+1 \text{ for some integer } k \end{aligned}$$

If each of the following integers is ***n***, give the associated ***k*** which makes it even or odd:

n = 4	***n*** = -6	***n*** = 11	***n*** = -3	***n*** = 0
even	even	odd	odd	***even***
k = 2	***k*** = -3	***k*** = 5	***k*** = -2	***k*** = 0

Note that the definition works using any variables, you aren't restricted to using just ***n*** and ***k***.

It follows from the definition that if you are doing a problem in which you know that a particular integer is even, you can deduce that it has the form $2 \cdot (\text{some integer})$. Conversely, if you know that an integer equals $2 \cdot (\text{some integer})$, then you can deduce that the integer is even.

An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols: For each integer n with $n > 1$,

$$\begin{aligned} n \text{ is prime} &\Leftrightarrow \forall \text{ positive integers } r \text{ and } s, \text{ if } n = rs \\ &\quad \text{then either } r = 1 \text{ and } s = n \text{ or } r = n \text{ and } s = 1. \\ n \text{ is composite} &\Leftrightarrow \exists \text{ positive integers } r \text{ and } s \text{ such that } n = rs \\ &\quad \text{and } 1 < r < n \text{ and } 1 < s < n. \end{aligned}$$

Partner up

a. Is 1 prime?

b. Is every integer greater than 1 either prime or composite?

c. Write the first six prime numbers.

d. Write the first six composite numbers.

==========

a. No. A prime number is required to be greater than 1.

b. Yes. Let n be any integer that is greater than 1. Consider all pairs of positive integers r and s such that $n = rs$. There exist at least two such pairs, namely, $r = n$ and $s = 1$ and $r = 1$ and $s = n$. Moreover, since $n = rs$, all such pairs satisfy the inequalities $1 \leq r \leq n$ and $1 \leq s \leq n$. If n is prime, then these two pairs are the only ways to write n as rs. Otherwise, there exists a pair of positive integers r and s such that $n = rs$ and neither r nor s equals either 1 or n. Therefore, in this case $1 < r < n$ and $1 < s < n$, and hence n is composite.

c. 2, 3, 5, 7, 11, 13

d. 4, 6, 8, 9, 10, 12

Proving Existential Statements

According to the definition given in Section 3.1, a statement in the form

$$\exists x \in D \text{ such that } Q(x)$$

is true if, and only if,

$$Q(x) \text{ is true for at least one } x \text{ in } D.$$

One way to prove this is to find an x in D that makes $Q(x)$ true. Another way is to give a set of directions for finding such an x. Both of these methods are called **constructive proofs of existence**.

Partner up

a. Prove: $\exists$ an even integer n that can be written in two ways as a sum of two prime numbers.

b. Suppose that r and s are integers. Prove: $\exists$ an integer k such that $22r + 18s = 2k$.

==========

a. Let $n = 10$. Then $10 = 5 + 5 = 3 + 7$ and 3, 5, and 7 are all prime numbers. Thus $\exists$ an even integer—namely, 10—that can be written in two ways as a sum of two prime numbers.

b. Let $k = 11r + 9s$. Then k is an integer because it is a sum of products of integers, and by substitution, and the distributive law of algebra,

$$2k = 2(11r + 9s) = 22r + 18s.$$

Thus $\exists$ an integer, namely k, such that $22r + 18s = 2k$.

Disproving Universal Statements by Counterexample

To disprove a statement means to show that it is false. Consider the question of disproving a statement of the form

$$\forall x \text{ in } D, \text{ if } P(x) \text{ then } Q(x).$$

Showing that this statement is false is equivalent to showing that its negation is true. The negation of the statement is existential:

$$\exists x \text{ in } D \text{ such that } P(x) \text{ and not } Q(x).$$

To disprove a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$," find a value of x in D for which the hypothesis $P(x)$ is true and the conclusion $Q(x)$ is false. Such an x is called a **counterexample**.

Statement: $\forall$ real numbers a and b, if $a^2 = b^2$, then $a = b$.

Counterexample: Let $a = 1$ and $b = -1$. Then $a^2 = 1^2 = 1$ and $b^2 = (-1)^2 = 1$, and so $a^2 = b^2$. But $a \neq b$ since $1 \neq -1$.

To prove Universal statements, we have two approaches:

1. The Method of Exhaustion (only if the domain is finite) → plug in ***every*** element in the finite domain
2. Method of Direct Proof

Partner up

Use the method of exhaustion to prove the following statement:

$\forall n \in \mathbf{Z}$, if n is even and $4 \leq n \leq 26$ then n can be written as a sum of two prime numbers.

==========

Solution:

$$4 = 2 + 2 \qquad 6 = 3 + 3 \qquad 8 = 3 + 5 \qquad 10 = 5 + 5$$
$$12 = 5 + 7 \qquad 14 = 11 + 3 \qquad 16 = 5 + 11 \qquad 18 = 7 + 11$$
$$20 = 7 + 13 \qquad 22 = 5 + 17 \qquad 24 = 5 + 19 \qquad 26 = 7 + 19$$

Method of Direct Proof

1. Express the statement to be proved in the form "For every $x \in D$, if $P(x)$ then $Q(x)$." (This step is often done mentally.)
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.")
3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Example 4.1.7 A Direct Proof of a Theorem

Prove that the sum of any two even integers is even.

Proof:

Let m and n be even integers.	[We will show $m + n$ is even]
$m = 2k$ for some integer k. $n = 2l$ for some integer l.	[By the definition of even]→ note that k and l ***have*** to be different otherwise m and n would be equal
$m + n = 2k + 2l = 2(k + l)$	[Substitution and algebra]
$k + l$ is an integer	[The sum of two integers is also an integer]
So, $m + n = 2 * integer$, and so it is even	[By definition of even]

This is analogous to writing a program, declaring variables, using comments, etc.