1 Introduction

A **theorem** is a mathematical statement that is true and can be verified as true.

A **proof** of a theorem is a written verification that shows that the theorem is definitely and unequivocally true.

A **definition** is an exact, unambiguous explanation of the meaning of a mathematical word or phrase.

2 Theorems

Example Theorems:

Theorem Let f be differentiable on an open interval I and let $c \in I$. If $f(c)$ is the maximum or minimum value of f on I, then $f'(c) = 0$.

Theorem If $\sum_{k=1}^{\infty} a_k$ converges, then $\lim_{k\to\infty} a_k = 0$.

Theorem Suppose f is continuous on the interval $[a, b]$. Then f is integrate-able on $[a, b]$.

Theorem Every absolutely convergent series converges.

Theorem If n is a non-negative integer, then $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$

Theorem The harmonic series $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + ...$ diverges.

A theorem of the form “If P, then Q,” can be regarded as a device that produces new information from P.

In general the word “theorem” is reserved 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 theorem.

A **corollary** is a result that is an immediate consequence of a theorem or proposition.

3 Definitions

Definition 4.1 An integer n is **even** if $n = 2a$ for some integer $a \in \mathbb{Z}$.

Definition 4.2 An integer n is **odd** if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.

Definition 4.3 Two integers have the **same parity** if they are both even or they are both odd. Otherwise, they have **opposite parity**.

It is common to express definitions as conditional statements even though the bi-conditional would more appropriately convey the meaning.

Definition 4.4 Suppose a and b are integers. We say that a **divides** b, written $a|b$, 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

Note that if a does not divide b, then $a|b$ is false. Otherwise, if a does divide b, then $a|b$ is true.

Each number has a set of integers that can be divided called the set of divisors.

Example: The set of divisors of 6 and 0

$$\{a \in \mathbb{Z} : a|6\} = \{-6, -3, -2, -1, 1, 2, 3, 6\} \tag{1}$$

$$\{a \in \mathbb{Z} : a|0\} = \mathbb{Z} \tag{2}$$

Definition 4.5 A number $n \in \mathbb{N}$ is **prime** if it has exactly two positive divisors, 1 and n. If n has more than two positive divisors, it is called **composite**. (Thus n is composite if and only if $n = ab$ for $1 < a, b < n$.)

Definition 4.6 The **greatest common divisor** of integers a and b, denoted $gcd(a, b)$, is the largest integer that divides both a and b. The **least common multiple** of non-zero integers a and b, denoted $lcm(a, b)$, is the smallest integer in $\mathbb{N}$ that is a multiple of both a and b.

We usually only consider a and b when $a, b \neq 0$ because $gcd(0, 0) = \infty$

$gcd()$ can be used for factoring and $lcd()$ can be used for simplifying fractions

Statements that use facts do not need to justify anything that uses the facts, we accept them as true.

Fact 4.1 If a and b are integers, then so are their sum, product, and difference. That is, if $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}, a - b \in Z$ and $ab \in \mathbb{Z}$.

Fact 4.2 Every natural number greater than 1 has a unique factorization into primes.

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

q is the quotient and r is the remainder

4 Direct Proof

direct proof - a simple way to prove theorems or propositions that have the form of conditional statements.

Conditional truth table review (if p then q):

P	Q	$p \implies q$
T	F	T
T	F	F
F	T	T
F	F	T

Proof outline for a direct proof:

Proposition If P, then Q.

Proof. Suppose P.
...
...
...
Therefore Q.

□

Example proofs:

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.
Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by definition of an odd number.
Thus $x^2 = (2a + 1)2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$.
So $x^2 = 2b + 1$ where b is the integer $b = 2a^2 + 2a$.
Thus $x^2 = 2b + 1$ for an integer b.
Therefore x^2 is odd, by definition of an odd number. □

Proposition Let a, b and c be integers. If $a|b$ and $b|c$, then $a|c$

Proof. Suppose $a|b$ and $b|c$.
By Definition 4.4, we know $a|b$ means $b = ad$ for some $d \in \mathbb{Z}$.
Likewise, $b|c$ means $c = be$ for some $e \in \mathbb{Z}$.
Thus $c = be = (ad)e = a(de)$, so $c = ax$ for the integer $x = de$.
Therefore $a|c$.
□

Proposition If x is an even integer, then $x^2 - 6x + 5$ is odd.

Proof. Suppose x is an even integer.
Then $x = 2a$ for some $a \in \mathbb{Z}$, by definition of an even integer.
So $x^2-6x+5 = (2a)^2-6(2a)+5 = 4a^2-12a+5 = 4a^2-12a+4+1 = 2(2a^2-6a+2)+1$.
Therefore we have $x^2 - 6x + 5 = 2b + 1$, where $b = 2a^2 - 6a + 2 \in \mathbb{Z}$.
Consequently, $x^2 - 6x + 5$ is odd, by definition of an odd number.
□

Proposition If $a, b, c \in \mathbb{N}$, then $lcm(ca, cb) = c * lcm(a, b)$.

Proof. Assume $a, b, c \in \mathbb{N}$.
Let $m = lcm(ca, cb)$ and $n = c * lcm(a, b)$.
We will show $m = n$.
By definition, $lcm(a, b)$ is a positive multiple of both a and b.
So, $lcm(a, b) = ax = by$ for some $x, y \in \mathbb{N}$.
From this we see that $n = c * lcm(a, b) = cax = cby$.
So, n is a positive multiple of both ca and cb.
But, $m = lcm(ca, cb)$ is the smallest positive multiple of both ca and cb.
Thus $m \leq n$.
On the other hand, as $m = lcm(ca, cb)$ is a multiple of both ca and cb.
We have $m = cax = cby$ for some $x, y \in \mathbb{Z}$.
Then $\frac{1}{c}m = ax = by$ is a multiple of both a and b.
Therefore, $lcm(a, b) \leq \frac{1}{c}m$.
So $c * lcm(a, b) \leq m$, that is, $n \leq m$.
We've shown $m \leq n$ and $n \leq m$, so $m = n$.
□

Proposition Let x and y be positive numbers. If $x \leq y$, then $\sqrt{x} \leq \sqrt{y}$.

Proof. Suppose $x \leq y$. Subtracting y from both sides gives $x - y \leq 0$.
This can be written as $\sqrt{x}^2 - \sqrt{y}^2 \leq 0$.
Factor this as a difference of two squares to get $(\sqrt{x} - \sqrt{y})(\sqrt{x} + \sqrt{y}) \leq 0$.
Dividing both sides by the positive number $\sqrt{x} + \sqrt{y}$ produces $\sqrt{x} - \sqrt{y} \leq 0$.
Adding $\sqrt{y}$ to both sides gives $\sqrt{x} \leq \sqrt{y}$.

□

Proposition If x and y are positive real numbers, then $2\sqrt{xy} \leq x + y$

Proof. Suppose x and y are positive real numbers.
Observe that $0 \leq (x - y)^2$, that is, $0 \leq x^2 - 2xy + y^2$.
Adding $4xy$ to both sides gives $4xy \leq x^2 + 2xy + y^2$.
Factoring yields $4xy \leq (x + y)^2$.
Taking the square root of both sides produces $2\sqrt{xy} \leq x + y$.

□

5 Using Cases

In proving a statement is true, we sometimes have to examine multiple cases before showing the statement is true in all possible scenarios.

The following example cases are used for the next couple of proofs

n	$1 + (-1)^n(2n - 1)$
1	0
2	4
3	-4
4	8
5	-8
6	12
7	-12

Proposition If $n \in \mathbb{N}$, then $1 + (-1)^n(2n - 1)$ is a multiple of 4.

Proof. Suppose $n \in \mathbb{N}$.
Then n is either even or odd. Let's consider these two cases separately.
Case 1. Suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$, and $(-1)^n = 1$.
Thus $1 + (-1)^n(2n - 1) = 1 + (1)(2 * 2k - 1) = 4k$, which is a multiple of 4.
Case 2. Suppose n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$, and $(-1)^n = -1$.
Thus $1 + (-1)^n(2n - 1) = 1 - (2(2k + 1) - 1) = -4k$, which is a multiple of 4.
These cases show that $1 + (-1)^n(2n - 1)$ is always a multiple of 4.

□

Two cases are used above as the equation changes between positive and negative

Proposition Every multiple of 4 equals $1 + (-1)n(2n - 1)$ for some $n \in \mathbb{N}$.

Proof. In conditional form, the proposition is as follows:
If k is a multiple of 4, then there is an $n \in \mathbb{N}$ for which $1 + (-1)^n(2n - 1) = k$.
What follows is a proof of this conditional statement.
Suppose k is a multiple of 4.
This means $k = 4a$ for some integer a.
We must produce an $n \in \mathbb{N}$ for which $1 + (-1)^n(2n - 1) = k$.
This is done by cases, depending on whether a is zero, positive or negative.
Case 1. Suppose $a = 0$. Let $n = 1$. Then $1 + (-1)^n(2n - 1) = 1 + (-1)^1(2 - 1) = 0 = 4 * 0 = 4a = k$.
Case 2. Suppose $a > 0$. Let $n = 2a$, which is in $\mathbb{N}$ because a is positive.
Also, n is even, so $(-1)^n = 1$.
Thus $1 + (-1)^n(2n - 1) = 1 + (2n - 1) = 2n = 2(2a) = 4a = k$.
Case 3. Suppose $a < 0$. Let $n = 1 - 2a$, which is an element of $\mathbb{N}$ because a is negative, making $1 - 2a$ positive.
Also. n is odd, so $(-1)^n = -1$.
Thus $1 + (-1)^n(2n - 1) = 1 - (2n - 1) = 1 - (2(1 - 2a) - 1) = 4a = k$.
The above cases show that no matter whether a multiple $k = 4a$ of 4 is zero, positive or negative, $k = 1 + (-1)^n(2n - 1)$ for some $n \in \mathbb{N}$.

□

6 Treating Similar Cases

Occasionally two or more cases in a proof will be so similar that writing them separately seems tedious or unnecessary.

Observe the following proof:

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

Proof. Suppose m and n are two integers with opposite parity.
We need 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.
Thus $m = 2a$ 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 4.2).
Case 2. Suppose m is odd and n is even.
Thus $m = 2a + 1$ and $n = 2b$ for some integers a and b.
Therefore $m + n = 2a + 1 + 2b = 2(a + b) + 1$, which is odd (by Definition 4.2).
In either case, $m + n$ is odd.

□

The proof can be shortened to:

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

Proof. Suppose m and n are two integers with opposite parity.
We need to show that $m + n$ is odd.
Without loss of generality, suppose m is even and n is odd.
Thus $m = 2a$ 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 4.2).

□