INTRODUCTION TO PROOFS

Chapter 1

INTRODUCTION

- A proof is a valid argument that establishes the truth of a mathematical statement.

- The methods we will study for building proofs are also used throughout computer science.

- Many theorems in mathematics are implications, $p \to q$. The techniques of proving implications give rise to different methods of proofs.

SOME TERMINOLOGY

- A theorem is a statement that can be shown as true.
- Less important theorems sometimes are called propositions (facts or results).
- A theorem may be universal quantification of a conditional statement with one or more premises and a conclusion.
- A proof is a valid argument that establishes the truth of a theorem.

- The statements used in proof can include axioms (or postulates)
- A less important theorem that is helpful in the proof of other results is called a lemma
- A corollary is a theorem that can be established directly from a theorem that has been proved.
- A conjecture is a statement that is being proposed to be true statement.

METHODS OF PROOF

- **DIRECT PROOF**

  $p \to q$

- **INDIRECT PROOF**
  - **PROOF BY CONTRAPOSITION**

    $p \to q \equiv \sim q \to \sim p$

  - **PROOF BY CONTRADICTION**

    $p \to q \equiv (p \wedge \sim q) \to c$

DIRECT PROOF

- The implication $p \rightarrow q$ can be proved by showing that if p is true, the q must also be true.
- This shows that the combination p true and q false never occurs.
- A proof of this kind is called a direct proof.

SOME BASICS

- An integer n is even if, and only if, $n = 2k$ for some integer k.
- An integer n is odd if, and only if, $n = 2k + 1$ for some integer k.
- An integer n is prime if, and only if, $n > 1$ and for all positive integers r and s, if $n = r.s$, then $r = 1$ or $s = 1$.
- An integer $n > 1$ is composite if, and only if, $n = r.s$ for some positive integers r and s with $r \neq 1$ and $s \neq 1$.

- A real number r is rational if, and only if, $r = \frac{a}{b}$ for some integers a and b with $b \neq 0$.

- If n and d are integers and $d \neq 0$, then d divides n, written $d|n$ if, and only if, $n = d.k$ for some integers k.

- An integer n is called a perfect square, if and only if, $n = k^2$ for some integer k.

EXERCISE

- Prove that the sum of two odd integers is even.

- **PROOF:**

Let m and n be two odd integers.

Then by definition of odd numbers

$$m = 2k + 1 \quad \text{for some } k \in Z$$

$$n = 2l + 1 \quad \text{for some } l \in Z$$

Now,

$$m + n = (2k + 1) + (2l + 1)$$

$= 2k + 2l + 2$

$= 2\ (k + l + 1)$

$= 2r$

where,

$$r = (k + l + 1) \in Z$$

Hence m + n is even.

EXERCISE

- Prove that if n is any even integer, then $(-1)^n = 1$

- **PROOF:**

  Suppose n is an even integer.

  Then $n = 2k$ for some integer k.

  Now

$$
\begin{aligned}
(-1)^n &= (-1)^{2k} \\
&= [(-1)^2]^k \\
&= (1)^k \\
&= 1 \qquad \text{(proved)}
\end{aligned}
$$

EXERCISE

- Prove that the product of an even integer and an odd integer is even.

- **PROOF:**

Suppose m is an even integer and n is an odd integer. Then,

$m = 2k$ for some integer k

and $n = 2l + 1$ for some integer l

Now

$$m.n = 2k\,.\,(2l + 1)$$
$$= 2.k\,(2l + 1)$$
$$= 2.r \qquad \text{where } r = k(2l + 1) \text{ is an integer}$$

Hence m.n is even. (Proved)

EXERCISE

- Prove that the square of an even integer is even.

- **PROOF:**

Suppose n is an even integer.

Then $n = 2k$

Now,

$$
\begin{aligned}
\text{square of } n = n^2 &= (2.k)^2 \\
&= 4k^2 \\
&= 2.(2k^2) \\
&= 2.p \qquad \text{where, } p = 2k^2 \in Z
\end{aligned}
$$

Hence, n^2 is even. (proved)

EXERCISE

- Prove that if n is an odd integer, then $n^3 + n$ is even.

- **PROOF:**

Let n be an odd integer,

then

$$n = 2k + 1 \text{ for some } k \in Z$$

Now,

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

$$= (2k + 1)\,(4k^2 + 4k + 2)$$

$$= (2k + 1)\,2.(2k^2 + 2k + 1)$$

$$= 2.(2k + 1)\,(2k^2 + 2k + 1) \quad k \in Z$$

= an even integer

EXERCISE

- Prove that, if the sum of any two integers is even, then so is their difference.

- **PROOF:**

  Suppose m and n are integers

  So that $m + n$ is even.

  Then by definition of even numbers

$$m + n = 2k \qquad \text{for some integer } k$$

$$\Rightarrow \quad m = 2k - n \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Now,

$$\begin{aligned} m - n &= (2k - n) - n \qquad \text{using (1)} \\ &= 2k - 2n \\ &= 2(k - n) = 2r \end{aligned}$$

where,

$r = k - n$ is an integer

Hence $m - n$ is even.

EXERCISE

- Prove that the sum of any two rational numbers is rational.

- **PROOF:**

  Suppose r and s are rational numbers.

  Then by definition of rational

$$r = \frac{a}{b} \quad \text{and} \quad s = \frac{c}{d}$$

  for some integers a, b, c, d with $b \neq 0$ and $d \neq 0$

- Now,

$$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{p}{q}$$

where,

$p = ad + bc \in Z$ and $q = bd \in Z$ and $q \neq 0$

Hence r + s is rational.

EXERCISE

- Given any two distinct rational numbers r and s with $r < s$. Prove that there is a rational number x such that $r < x < s$.

PROOF:

Given two distinct rational numbers r and s such that

$$r < s \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Adding r to both sides of (1), we get

$$r + r < r + s$$

$$2r < r + s$$

$$\Rightarrow \quad r < \frac{r+s}{2} \quad \ldots\ldots\ldots\ldots (2)$$

- Next adding s to both sides of (1), we get

$$r + s < s + s$$

$$\Rightarrow \quad r + s < 2s$$

$$\Rightarrow \quad \frac{r+s}{2} < s \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

Combining (2) and (3), we may write

$$r < \frac{r+s}{2} < s \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(4)$$

Since the sum of two rational is rational,

Therefore r + s is rational.

Also the quotient of a rational by a non-zero rational, is rational, Therefore $\dfrac{r+s}{2}$ is rational and by (4) it lies between r & s.

Hence, we have found a rational number

such that $r < x < s$. (proved)

EXERCISE

- Prove that for all integers a, b and c, if $a|b$ and $b|c$ then $a|c$.

PROOF:

Suppose $a|b$ and $b|c$

where a, b, c $\in Z$.

Then by definition of divisibility

$b=a.r$ and $c=b.s$ for some integers r and s.

Now, $c = b.s$

$= (a.r).s$ (substituting value of b)

$= a.(r.s)$ (associative law)

$= a.k$

where,

$k = r.s \in Z$

$\Rightarrow$ $a|c$ by definition of divisibility

EXERCISE

- Prove that for all integers a, b and c if $a|b$ and $a|c$ then $a|(b+c)$

- **PROOF:**

Suppose $a|b$ and $a|c$ where a, b, c $\in Z$

By definition of divides

$b = a.r$ and $c = a.s$ for some r, s $\in Z$

Now

$$b + c = a.r + a.s \qquad \text{(substituting values)}$$
$$= a.(r+s) \qquad \text{(by distributive law)}$$
$$= a.k$$

where $k = (r + s) \in Z$

Hence $a|(b + c)$ by definition of divides.

EXERCISE

- Prove that the sum of any three consecutive integers is divisible by 3.

PROOF:

Let n, $n + 1$ and $n + 2$ be three consecutive integers.

Now

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

where $k=(n+1) \in Z$

Hence, the sum of three consecutive integers is divisible by 3.

PROOF BY CONTRADICTION

- A proof by contradiction is based on the fact that either a statement is true or it is false but not both.

- Hence the supposition, that the statement to be proved is false, leads logically to a contradiction, impossibility or absurdity, then the supposition must be false.

- Accordingly, the given statement must be true.

- Thus to prove an implication $p \rightarrow q$ by contradiction method we suppose that the condition p and the negation of the conclusion q, i.e., $(p \wedge \sim q)$ is true and ultimately arrive at a contradiction.

- The method of proof by contradiction, may be summarized as follows:
  - Suppose the statement to be proved is false.
  - Show that this supposition leads logically to a contradiction.
  - Conclude that the statement to be proved is true.

THEOREM

- Give a proof by contradiction for the statement:

"If n^2 is an even integer then n is an even integer."

- **PROOF:**

Suppose n^2 is an even integer and n is not even, so that n is odd.

Hence

$$n = 2k + 1 \text{ for some integer k.}$$

Now

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

$$= 2.(2k^2 + 2k) + 1$$

$$= 2r + 1$$

where

$$r = (2k^2 + 2k) \in Z$$

This shows that n^2 is odd, which is a contradiction to our supposition that n^2 is even.

Hence the given statement is true.

EXERCISE

- Prove that if n is an integer and $n^3 + 5$ is odd, then n is even using contradiction method.
- **PROOF:**
- Suppose that $n^3 + 5$ is odd and n is not even (odd).
- Since n is odd and the product of two odd numbers is odd, it follows that n^2 is odd and $n^3 = n^2 . n$ is odd.
- Further, since the difference of two odd number is even, it follows that

$$= (n^3 + 5) - n^3$$

$$= 5 \qquad \text{is even.}$$

- But this is a contradiction.
- Therefore, the supposition that $n^3 + 5$ and n are both odd is wrong and so the given statement is true.

EXERCISE

- Prove by contradiction method, the statement: If n and m are odd integers, then $n + m$ is an even integer.

- **PROOF:**

Suppose n and m are odd and $n + m$ is not even (odd i.e by taking contradiction).

Now

$n = 2p + 1$ for some integer p

and

$m = 2q + 1$ for some integer q

Hence

$$n + m = (2p + 1) + (2q + 1)$$
$$= 2p + 2q + 2 = 2 \cdot (p + q + 1)$$

which is even, contradicting the assumption that $n + m$ is odd.

EXERCISE

- Prove that $\sqrt{2}$ is irrational.

- **PROOF:**

Suppose

$\sqrt{2}$ is rational.

Then there are integers m and n with no common factors so that

$$\sqrt{2} = \frac{m}{n}$$

Squaring both sides gives

$$2 = \frac{m^2}{n^2}$$

or $m^2 = 2n^2$ ....(1)

This implies that m^2 is even (by definition of even).

It follows that m is even. Hence

$m = 2k$ for some integer k…..(2)

Substituting (2) in (1), we get

$$(2k)^2 = 2n^2$$

$$\Rightarrow \quad 4k^2 = 2n^2$$

$$\Rightarrow \quad n^2 = 2k^2$$

- This implies that n^2 is even, and so n is even. But we also know that m is even.

- Hence both m and n have a common factor 2. But this contradicts the supposition that m and n have no common factors.

- Hence our supposition is false and so the theorem is true.

EXERCISE

- Prove by contradiction that $6 - 7\sqrt{2}$ is irrational.

- **PROOF:**

Suppose $6 - 7\sqrt{2}$ is rational.

Then by definition of rational,

$$6 - 7\sqrt{2} = \frac{a}{b}$$

for some integers a and b with $b \neq 0$.

- Now consider,

$$7\sqrt{2} = 6 - \frac{a}{b}$$

$$\Rightarrow \qquad 7\sqrt{2} = \frac{6b-a}{b}$$

$$\Rightarrow \qquad \sqrt{2} = \frac{6b-a}{7b}$$

Since a and b are integers, so are 6b-a and 7b and 7b≠0;

Hence is a quotient of the two integers 6b-a and 7b with 7b≠0.

Accordingly, $\sqrt{2}$ is rational (by definition of rational).

- This contradicts the fact because $\sqrt{2}$ is irrational.

  Hence our supposition is false and so $6 - 7\sqrt{2}$ is irrational.

PROOF BY CONTRAPOSITION

- A proof by contraposition is based on the logical equivalence between a statement and its contrapositive.

- Therefore, the implication $p \rightarrow q$ can be proved by showing that its contrapositive $\sim q \rightarrow \sim p$ is true.

- The contrapositive is usually proved directly.

- The method of proof by contrapositive may be summarized as:
  - Express the statement in the form if p then q.
  - Rewrite this statement in the contrapositive form if not q then not p.
  - Prove the contrapositive by a direct proof.

EXERCISE

- Prove that for all integers n, if n^2 is even then n is even.

- **PROOF:**

The contrapositive of the given statement is:

"if n is not even (odd) then n^2 is not even (odd)"

We prove this contrapositive statement directly.

Suppose n is odd.

Then

$$n = 2k + 1 \text{ for some } k \in Z$$

Now

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1$$

$$= 2.(2k^2 + 2k) + 1$$

$$= 2.r + 1$$

where,

$$r = 2k^2 + 2k \in Z$$

Hence n^2 is odd. Thus the contrapositive statement is true and so the given statement is true.

EXERCISE

- Prove that if $3n + 2$ is odd, then n is odd.

- **PROOF:**

The contrapositive of the given conditional statement is

" if n is even then $3n + 2$ is even"

Suppose n is even, then

$n = 2k$ for some $k \in Z$

Now

$$\begin{aligned} 3n + 2 &= 3\,(2k) + 2 \\ &= 2.(3k + 1) \\ &= 2.r \qquad \text{where } r = (3k + 1) \in Z \end{aligned}$$

- Hence $3n + 2$ is even.
- We conclude that the given statement is true since its contrapositive is true.

EXERCISE

- Prove that if n^2 is not divisible by 25, then n is not divisible by 5.

- **PROOF:**

The contra-positive statement is:

"if n is divisible by 5, then n^2 is divisible by 25"

Suppose n is divisible by 5.

Then by definition of divisibility

$n = 5.k$ for some integer k

- Squaring both sides

$$n^2 = 25.k^2$$

where

$$k^2 \in Z$$

So,

n^2 is divisible by 25

EXERCISE

- Prove the statement by contraposition:

  For all integers m and n, if m + n is even then m and n are both even or m and n are both odd.

- **PROOF:**

  The contrapositive statement is:

  "For all integers m and n, if m and n are not both even and m and n are not both odd, then m + n is not even."

  or more simply,

  "For all integers m and n, if one of m and n is even and the other is odd, then m + n is odd"

- Suppose m is even and n is odd.
  Then,

  $$m = 2p \qquad \text{for some integer } p$$

  and $$n = 2q + 1 \qquad \text{for some integer } q$$

  Now
  $$\begin{aligned} m + n &= (2p) + (2q + 1) \\ &= 2.(p+q) + 1 \\ &= 2.r + 1 \end{aligned}$$

  where

  $r = p+q$ is an integer

  Hence $m + n$ is odd.

- Similarly, taking m as odd and n even, we again arrive at the result that m + n is odd.

- Thus, the contrapositive statement is true.

Since an implication is logically equivalent to its contrapositive so the given implication is true.