Method of Proving Theorems

A proof is a logically sound argument that demonstrates the truth of a mathematical statement. The proof techniques covered are significant not only for establishing mathematical theorems but also for their numerous applications in computer science.

1 Direct Proofs

A direct proof of a conditional statement $p \to q$ begins by assuming that p is true. Using rules of inference, we then proceed through subsequent steps to show that q must also be true. By demonstrating combination that q follows necessarily from p, a direct proof ensures that the combination of p being true and q being false is impossible. In a direct proof, we assume p is true and employ axioms, definitions, and previously proven theorems, along with rules of inference, to establish the truth of q. Direct proofs are often quite straightforward, as the path from hypothesis to conclusion is guided by the available premises.

Note:
The integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k such that $n = 2k + 1$.

$n = 2k$, k Intger

$n = 2k+1$

$2, 4, 6, 8 - - - .$

$3, 5, 7, . -$

Example 1:
Prove the theorem 'If n is an odd integer, then n^2 is odd'. By direct proof method. *

$1, 3, 5, 7, - - -$

$1^2 = 1 \quad 3^2 = 9 \quad 5^2 = 25$

$7^2 = 49 - -$

Solution:
we assume that n is odd. ~~By the definition of an odd integer, it follows~~ that $n = 2k + 1$, where k is some integer. We want to show that n^2 is also odd.
Squaring both sides of the equation $n = 2k + 1$, we get

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

By the definition of an odd integer, we can conclude that n^2 is an odd integer, since $2(2k^2 + 2k)$ is even and an even integer plus 1 is an odd integer, Therefore, it is an odd integer.
Consequently, we have proved that if n is an odd integer, then n^2 is an odd integer.

$1^2 = 1$
$2^2 = 4$
$3^2 = 9$
$4^2 = 16$
$5^2 = 25$

$36 = 6^2$

Example 2:
Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square.

Solution:
An integer a is a perfect square if there is an integer b such that $a = b^2$
we assume that m and n are both perfect squares.
By the definition of a perfect square, it follows that there are integers a and b such that $m = a^2$ and $n = b^2$.
We must show that mn must also be a perfect square.
By substituting $m = a^2$ and $n = b^2$, we get $mn = a^2b^2$.

$mn = a^2b^2$
$= (aa)(bb)$
$= (ab)(ab) = (ab)^2$

Hence, $mn = a^2b^2 = (aa)(bb) = (ab)(ab) = (ab)^2$, using commutativity and asssociativity of multiplication.
By the definition of perfect square, mn is also a perfect square.

Example 3:
Use a direct proof to show that 'the sum of two odd integers is even'.

1, 3 $\quad$ $1+3=4$

$2s+1+2t+1$
$2s+2t+2$
$2(s+t+1)$

Solution:
Suppose that a and b are two odd integers.
Then there exist integers s and t such that

$$a = 2s + 1 \text{ and } b = 2t + 1.$$

Adding, we obtain $a + b = (2s + 1) + (2t + 1) = 2(s + t + 1)$.
Since this represents $a + b$ as 2 times the integer $s + t + 1$, we conclude that $a + b$ is even.

Example 4:
Show that the square of an even number is an even number using a direct proof.

$2^2 = 4$
$4^2 = 16$
$6^2 = 36$

Solution:
We must show that 'If n is even, then n^2 is even'.
Suppose that n is even, $n = 2k$ for some integer k.
Squaring, $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.
Since we have written n^2 as 2 times an integer, we conclude that n^2 is even.

Example 5:
Show that the additive inverse, or negative, of an even number is an even number using a direct proof.

2

-2

$a = 2s$

$-a = -(2s)$

$= 2(-s)$

Solution:
We must show that whenever we have an even integer, its negative is even. Suppose that a is an even integer. Then there exists an integer s such that $a = 2s$.
Its additive inverse is $-2s = 2(-s)$. Since this is 2 times the integer s it is even.

Example 6:
Prove that if n is a perfect square, then $n + 2$ is not a perfect square.

$n+2 = m^2$

$k^2+2 = m^2$

$m^2-k^2 = 2$

Solution:
Let $n = k^2$ is a perfect square.
Assume that $n + 2$ is also a perfect square.
Then we can write $n + 2 = m^2$ for some integer m.

$\therefore \quad k^2 + 2 = m^2 \Rightarrow m^2 - k^2 = 2 \Rightarrow (m + k)(m - k) = 2.$

Let $(m + k) = 2,\ (m - k) = 1$. Adding these two, we get $2m = 3 \Rightarrow m = \frac{3}{2}$, which is not possible since m is an integer.
Let $(m + k) = -2,\ (m - k) = -1$. Adding these two, we get $2m = -3 \Rightarrow m = -\frac{3}{2}$, which is not possible since m is an integer.
Since both the cases leads to a contradiction, our assumption $n + 2$ is a perfect square is wrong.
Therefore $n + 2$ cannot be a perfect square.

$\frac{1}{2 \times 1} \times \frac{2}{1} = 2 \qquad -2 \times -1$

3, 5
3×5=15

Example 7:
Use a direct proof to show that the product of two odd numbers is odd.

Solution:
An odd number is one of the forms $2n+1$, where n is an integer. Let, $2a+1$ and $2b+1$ be two odd numbers where a, b are integers.
Their product is

$$(2a+1)(2b+1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1.$$

which shows that the product is odd, since it is of the form $2n+1$, with $n = 2ab + a + b$.

Proof by Contraposition (Indirect Method)

$p \to q$ $\neg q \to \neg p$.

Proof by contraposition is a method used to prove a conditional statement $p \to q$ by demonstrating the contrapositive statement $\neg q \to \neg p$. The contrapositive of a statement is logically equivalent to the original statement, which means that if we can show that $\neg q \to \neg p$ is true then the original statement $p \to q$ is also true. This approach often simplifies the proof process, especially when proving the contrapositive is easier than directly proving the original statement. In a proof by contraposition of $p \to q$, we take $\neg q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that $\neg p$ must follow.

Example 8:
Prove that if n is an integer and $5n+2$ is odd, then n is odd. *

$\neg q \to \neg p$

Solution:
Let $p : 5n+2$ is odd and $q;$ n is odd, the given statement is $p \to q$.
Assume that $\neg q$ is true. i.e., $q = n$ is odd is false. i.e., $q = n$ is even.
Then, by the definition of an even integer, $n = 2k$ for some integer k.
Substituting $2k$ for n, we find that

$$5n + 2 = 5(2k) + 2 = 10k + 2 = 2(5k + 1).$$

which shows that $5n+2$ is even because it is a multiple of 2, and therefore not odd. This is the $\neg p$ is true. Because of $\neg q \to \neg p$ is true the original statement $p \to q$ is true.
So, we have proved the theorem 'If $3n+2$ is odd, then n is odd.'

Example 9:
Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

$15 = n = 3 \times 5$

$3 \leq \sqrt{15}$ / $5 \leq \sqrt{15}$

Solution:
Let $p : n = ab$ and $q;\ a \leq \sqrt{n}$ or $b \leq \sqrt{n}$,
the given statement is $p \to q$.   > and >
Assume that $\neg q$ is true. i.e., $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$, is false. i.e., This implies that $a > \sqrt{n}$ and $b > \sqrt{n}$.

$a > \sqrt{n}$ and $b > \sqrt{n}$ $ab > \sqrt{n}.\sqrt{n} = n$

Multiplying these inequalities we get, $ab > \sqrt{n}\cdot\sqrt{n} = n$ which shows that $ab \neq n$. This is the $\neg p$ is true. Because of $\neg q \to \neg p$ is true the original conditional statement $p \to q$ is true.
Thus if $n = ab$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ is true.

$\mathbb{IR} + \mathbb{Q} =$ Irrational

Example 10:
Prove that the sum of an irrational number and a rational number is irrational.
Solution:
Let $p : x$ irrational number and y rational number
$q;\ x + y$ is irrational.
The given statement is $p \to q$.
Assume that $\neg q$ is true. i.e., $x + y$ is rational
Since $x + y$ is a rational number and y is a rational number, then $x + y + (-y)$ is a rational number because the sum of the rational numbers $x + y$ and $-y$ must be rational. Which shows that x is rational. This contradicts our hypothesis that x is irrational. Therefore, the assumption that $x + y$ is rational is incorrect, and we conclude, that $x + y$ is irrational.

$p \to q$ $\frac{1}{x} = \frac{p}{q}$ $q \neq 0$ $p \neq 0$. $q \neq 0$ $p \neq 0$ $p = 0$ $\frac{1}{x} = \frac{0}{q} = 0$ //

$\neg q$ True

$\neg p$ True

Example 11:
Prove that if x is irratonal, then $1/x$ is irrational, $\boxed{x \neq 0.}$ *

Solution:
Let p : x is irrational, ~~then~~ q: $1/x$ is irrational, the given statement is $p \to q$.
Assume that $\neg q$ is true. i.e., ~~$1/x$ is irrational~~. i.e., $\frac{1}{x}$ is rational, ~~then x is rational~~. Then by definition $\frac{1}{x} = \frac{p}{q}$ for some integers p and q with $q \neq 0$. Since $\frac{1}{x}$ cannot be 0, we know that $p \neq 0$.

Now $x = \frac{1}{\frac{1}{x}} = \frac{1}{\frac{p}{q}} = \frac{q}{p}$ by the usual rules of algebra and arithmetic.

Hence x can be written as the quotient of two integers with the denominator non zero. Thus, by definition, x is rational.

That is, $\neg p$ is true. Because of $\neg q \rightarrow \neg p$ is true the original conditional statement $p \rightarrow q$ is true.

Example 12:

Show that if n is an integer and $n^3 + 5$ is odd, then n is even using a proof by contraposition.

$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

$(2k+1)^3 = 8k^3 + 3.4k^2 + 3.2k + 1$

$8k^3 + 12k^2 + 6k + 1$

Solution:

Let p : $n^3 + 5$ is odd and q; n is even, the given statement is $p \longrightarrow q$. Assume that $\neg q$ is true. i.e., $q = n$ is even false. i.e. $q = n$ is odd.

Then, ~~by the definition of an even integer~~, $n = 2k + 1$ for some integer k.

Then $n^3 + 5 = (2k+1)^3 + 5 = 8k^3 + 12k^2 + 6k + 6$
$= 2(4k^3 + 6k^2 + 3k + 3)$.

Thus $n^3 + 5$ is two times some integer, so it is even.

Which shows $\neg p$ is true. Because of $\neg q \longrightarrow \neg p$ is true the original conditional statement $p \longrightarrow q$ is true.

So, we have proved the theorem '$n^3 + 5$ is odd, then n is even.

Example 13:

Prove that if x, y, and z are integers and $x + y + z$ is odd, then atleast one of x, y, and z is odd.

Assume $\neg q$

Solution:

Let $p : x + y + z$ is odd, q; at least one of x, y, and z is odd, the given statement is $p \rightarrow q$

Assume to the contrary that x, y, and z are all even. Then there exist integers a, b, and c such that $x = 2a$, $y = 2b$, and $z = 2c$.

Then $x + y + z = 2a + 2b + 2c = 2(a + b + c)$ is even. This contradicts the hypothesis that $x + y + z$ is odd. Therefore, the assumption was wrong, and atleast one of x, y, and z is odd.

Proof by Contradiction

3

Proof by contradiction is a method where to prove a statement p, one assumes the opposite, $\neg p$, and then demonstrates that this assumption leads to a logical contradiction. By showing that assuming $\neg p$ results in an inconsistency with known facts, definitions, or previously established results, one can conclude that the assumption $\neg p$ must be false. Therefore, the original statement p must be true. This technique is particularly useful when direct proof is difficult or when the truth of p can be easily established by disproving its negation.

$\frac{1}{2}$ $\frac{\cancel{2}}{\cancel{4}} = \frac{1}{2}$ ×

Example 15:
Prove that $\sqrt{2}$ is irrational by proof by contradiction.

Solution:
Let p be the proposition $\sqrt{2}$ is irrational. We assume that $\sqrt{2}$ is rational. If $\sqrt{2}$ is rational, there exist integers p and q with $\sqrt{2} = \dfrac{p}{q}$, where $q \neq 0$ and p and q have no common factors so that the fraction $\dfrac{p}{q}$ is in lowest terms. *

$\sqrt{2} = \frac{p}{q}$

$2 = \frac{p^2}{q^2}$ $p^2 = 2q^2$

Squaring both sides, $2 = \dfrac{p^2}{q^2}$. Hence, $2q^2 = p^2$ which is even.
If p^2 is even, p must also be even. Let $p = 2a$ for some integer a.
Thus, $2q^2 = 4a^2$, $q^2 = 2a^2$ which is even.

$2q^2 = p^2$

$p = 2a$

$2q^2 = 4a^2$

Again, using the fact that if the square of an integer is even, then the integer itself must be even, we conclude that q must be even.
We have now shown $\sqrt{2} = \dfrac{p}{q}$, where p and q are even, that is, 2 divides both p and q which is contradiction that $\dfrac{p}{q}$ is in lowest terms. Our assumption is wrong. Therefore, by contradiction, $\sqrt{2}$ is irrational.

Example 16:
Prove that, if $5n + 6$ is odd, then n is odd.

Solution:
Assume the contradiction of the given statement.
i.e., if $5n + 6$ is odd, then n is even.
Because n is even, there is an integer k such that $n = 2k$.
Substituting $n = 2k$ in $5n + 6$ we get,
$5n+6 = 5(2k)+6 = 10k+6 = 2(5k+3)$ which is even which shows that the statement is false, we arrive at a contradiction. This completes the proof by contradiction that if $5n + 6$ is odd, then n is odd.

Example 17:
Show that if n is an integer and 'If $3n + 2$ is even, then n is even'.

Solution:
Assume the contraadiction of the given statement.
i.e., if $3n + 2$ is even, then n is odd.
Because n is odd, there is an integer k such that $n = 2k + 1$.

Substituting $n = 2k + 1$ in $3n + 6$ we get,
$3n + 2 = 3(2k + 1) + 2 = 6k + 5 = 6k + 4 + 1 = 2(3k + 2) + 1$. which is odd which shows that the statement is false. we arrive at a contradiction. This completes the proof by contradiction that if $3n + 2$ is even, then n is even.

Proof by Counter examples

$\_ = (\ )^2 + (\ )^2$

$3 = (0)^2 + (1)^2$

$0 = 0$

$1^2 = 1 < 3$

$2^2 = 4$

Example 19:
Show that the statement, 'Every positive integer is the sum of the squares of two integers' is false by finding a counter example.

Solution:
Consider the positive integer 3. It cannot be written as the sum of the squares of two integers. To show this, the only perfect squares less than 3 are $0^2 = 0$ and $1^2 = 1$. Furthermore, there is no way to get 3 as the sum of two terms each of which is 0 or 1. Consequently, we have shown that "Every positive integer is the sum of the squares of two integers" is false.

Example 20:
Show that the statement is false by finding a counter example 'Every positive integer is the sum of squares of three integers'

$\_ = (\ )^2 + (\ )^2 + (\ )^2$

Solution:
Consider the positive integer 7.
Only perfect squares less than 7 are $\mathbf{0^2 = 0}$ and $\mathbf{1^2 = 1}$ and $\mathbf{2^2 = 4}$. But $\mathbf{0^2 + 1^2 + 2^2 = 5 \neq 7}$. i.e., we cannot write 7 as the sum of squares of three integers'. Consequently, we have shown that "Every positive integer is the sum of the squares of three integers" is false.
So, the statement is false.

7   7

$1^2 = 1$ $1^3 = 1$

$2^2 = 4$

$1^2 + 2^2 + 1^3$

$(6 \neq 7)$

Example 21:
Disprove the statement that every positive integer is the sum of at most two squares and a cube of nonnegative integers.

Solution:
We claim that the number 7 is not the sum of at most two squares and a cube.
The first two positive squares less than 7 are 1 and 4, and the first positive cube less than 7 is 1, and these are the only numbers that could be used in forming the sum 7. But $\mathbf{1^2 + 2^2 + 1^3 = 6 \neq 7}$
This counterexample disproves the statement.

Example 22:
Prove or disprove that the product of two irrational numbers is irrational.

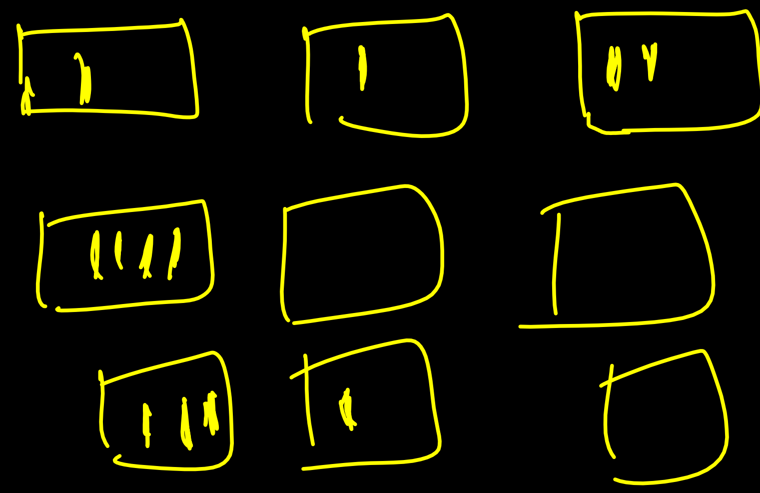
Solution:
To disprove this proposition, it is enough to find a counterexample.
We know that $\sqrt{2}$ is irrational. If we take the product of the irrational number $\sqrt{2}$ and the irrational number $\sqrt{2}$, then we obtain the rational number 2. This counterexample refutes the proposition.

$\sqrt{2} \cdot \sqrt{2} = 2$

Pigeonhole Principle

Statement

If m pigeons occupy n pigeonholes, $m > n$, then at least one pigeonhole will contain more than one pigeon.
Equivalently, if m objects are put n boxes and $m > n$, then at least one box will contain two or more objects.
For example, an office employs 13 clerks, so that at least two of them have birthday during the same month. Here, we have 13 pigeons (office clerks) and 12 pigeonhole (month of the year).



m n $m>n$

atleast $\left\lfloor \frac{(m-1)}{n} \right\rfloor + 1$ pigeon

$m = 100$

$n = 3$

Generalization of Pigeonhole principle

If m pigeons are accomodated in n pigeonholes and $m > n$, then one of the pigeonholes must contain atleast $\left\lfloor \frac{(m-1)}{n} \right\rfloor + 1$ pigeon, where $\left\lfloor \frac{(m-1)}{n} \right\rfloor$ denote the greatest integer less than or equal to $\frac{(m-1)}{n}$, which is a real number.

$m = 100$ $n = 12$

For example, Among 100 people there are atleast $\left\lfloor \frac{(100-1)}{12} \right\rfloor + 1 = 8 + 1 = 9$ who were born in the same month.

In another way, if n pigeonholes are occupied by $kn + 1$ or more pigeons, where k is a positive integer, then at least one hole is occupied by $k + 1$ or more pigeons.

n = no. of pigeon holes, no. of pigeons = $kn+1$

Example 1:
What is the minimum number of students required in a discrete mathematics class to be sure that at least six will receive the same grade, if there are five possible grades, A, B, C, D, and F?

Solution:
The number of pigeonholes = Number of possible grades $n = 5$ at least six will receive the same grade i.e., $k + 1 = 6 \Rightarrow k = 6 - 1 = 5$

$\therefore$ No of pigeons = minimum number of students = $kn + 1$

$$= 5 \times 5 + 1 = 26$$

Thus , 26 is the minimum number of students needed to ensure that at least six students will receive the same grade.

A B C D F

Example 2:
Show that in any set of six classes, each meeting regularly once a week on a particular day of the week, there must be two that meet on the same day, assuming that no classes are held on weekends.

Solution:
Number of pigeons $= 6$ (six classes). Number of pigeonholes $= 7$ (Number of days in a week). Since each class must meet on a day, each pigeon must occupy a pigeonhole. By the pigeonhole principle at least one day must contain at least two classes.

atlby excluding weekend = 5 ( )

Example 3:
Show that if there are 30 students in a class, then at least two have last names that begin with the same letter.

Solution:
Here, the students are the items, and the 26 letters are the containers: Since there are 30 students and only 26 letters, by the pigeonhole principle, at least two students must have last names that begin with the same letter.

A B 26

Example 4:
What is the minimum number of students, each of whom comes from one of the 50 states, who must be enrolled in a university to guarantee that there are at least 100 who come from the same state?

Solution:
The number of pigeonholes = Number of states $= n = 50$ at least 100 who comes from the same state i.e., $k + 1 = 100 \Rightarrow k = 100 - 1 = 99$
$\therefore$ No of pigeons = minimum number of students $= kn + 1 = 99 \times 50 + 1 = 4951$.
Therefore, we need at least 4951 students to guarantee that at least 100 come from a single state.

Example 5:
There are six professors teaching the introductory discrete mathematics class at a univesity. The same final exam is given by all six professors. If the lowest possible score on the final is 0 and the highest possible score is 100, how many students must there be to guarantee that there are two students with the same professor who earned the same final examination score?

Solution:
There are 101 possible scores, since 0 and 100 are both included, and 6 professors, so there are $\mathbf{6} \times \mathbf{101} = \mathbf{606}$ possible professor-score pairs. Thus 607 students are sufficient to guarantee that two of them share the same professor and received the same score.

Example 6:

Show that if any four numbers 1 to 6 are chosen, then at least 2 of them will add to 7.

Solution:

Here the pigeons constitute any four numbers from $\{1, 2, 3, 4, 5, 6\}$ and the pigeonholes are the subsets $\{1, 6\}$, $\{2, 5\}$, $\{3, 4\}$. Each of the four numbers chosen from 1 to 6 must belong to one of these sets. Since pigeons are greater than pigeonhole, by the Pigeonhole principle we can conclude that the two of the selected numbers belong the same set whose sum is 7?

Example 7:

m $n = 12$

Given a group of 100 people, at minimum how many people were born in the same month?

Solution:

Here pigeons are people and pigeonholes are month of the year. So $m = 100$ and $n = 12$ then $\dfrac{(100-1)}{12} = 8$

By generalized pigeonhole principal people $8 + 1 = 9$ will born in the same month.

Example 8:

An auditorium has a seating capacity of 800. How many seats must be occupied to guarantee that at least two people seated in the auditorium have the same first and last initials? (You may use pigeonhole principle)

Solution:

Assuming each initial can be any letter from A to Z, there are 26 choices for the first initial and 26 choices for the last initial. Thus, the total number of combinations of first and last initials is $26 \times 26 = 676$ which is taken as pigeonholes. To ensure that at least two people have the same initials, we need more people than the number of combinations. In order to get at least 2 people seated in the auditorium have the same first and last initials, by pigeonhole principle, we take the pigeon as $676 + 1 = 677$.