Islamic University of Science and Technology

Submitted By : Nusrat Jan.

Roll no : MCA-21-05.

Class : MCA (1st Sem).

Reg No : IUST0121014346.

Subject : Discrete Mathematics.

Topic : Methods of Proofs : Direct proof, Indirect proof, Mathematical Induction for proving algorithms.

Submitted To :

Dr. Muzaffar Rasool Bhat

Date of Submission :
04/04/22

Proofs:

A proof is a logical argument that tries to show that a statement is true. In math, and computer Science, a proof has to be well thought out and tested before being accepted. But even then, a proof can be discovered to have been wrong. There are many different ways to go about proving something.

A theorem is a mathematical statement which is proven to be true.

A statement that has been proven true in order to further help in proving another statement is called a lemma.

Proof may be what best distinguishes mathematics from other disciplines, even the sciences, which are

logical, rigorous and to a greater or lesser degree. The idea of proof is central to all branches of mathematics.

Direct Proof :

A direct proof of a conditional statement $P \rightarrow q$ is constructed when the first step is the assumption that p is true; subsequent steps are constructed using rules of inference, with the final step showing that q must also be true, then q must also be true, so that the combination P true and q false never occurs. In a direct proof, we assume that p is true and use axioms, definitions, and previously proven theorems, together with rules of inference, to show that q must also be true. Direct proofs sometimes require particular insights and

can be quite tricky.

Definition 1 :

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 $n = 2k + 1$.

* Every integer is either even or odd, and no integer is both even and odd and no integer is both even and odd.

Two integer's have the same parity when both are even or both are odd; they have opposite parity when one is even and other is odd.

Example :

The sum of two even integers equals an even integer :

Consider two even integers x and y. Since they are even, they can be written as

$$x = 2a$$
$$y = 2b$$

respectively for integers a and b. Then the

Sum can be written as:

$$x+y = 2a+2b = 2(a+b) = 2P$$

where $P = a+b$, a and b are all integers.

It follows that $x+y$ has 2 as a factor and therefore is even, so the sum of any two even integer is even.

Example 2:

Proof Square Even Integer Even

Proof:

Assume n is an even integer.
By definition of even integers, $n = 2a$ for some integers a. This follows that

$$n^2 = (2a)^2$$
$$= 4a^2$$
$$= 2(2a^2)$$
$$= 2K, \text{ where } K = 2a^2 \text{ is an integer.}$$

Since $2K$ is the definition of an even integer, $n^2 = 2K$ is an even integer. Therefore we can conclude that square of an even integer is also even.

Indirect Proof : (Proof by Contraposition)

Direct proofs lead from the premises of a theorem to the conclusion. They begin with the premises, continue with a sequence of deductions, and end with the conclusions. We need other methods of proving theorems of the form $\forall x\,(P(x) \to Q(x))$. Proofs of theorems of this type that are not direct proofs, that is, that do not start with the premises and end with the conclusion, are called indirect proofs. A extremely useful type of indirect proof is known as proof by contraposition. Proofs by contraposition make use of the fact that the conditional statement $p \to q$ is equivalent to its contrapositive, $\neg q \to \neg p$. The means that the conditional statement $p \to q$ can be proved by showing

that its contrapositive, $\neg q \rightarrow \neg p$, is true.

In a proof by contraposition of $p \rightarrow q$, we take $\neg q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference.

Example 1:

Prove that there are an infinitely many prime numbers:

Proof: Suppose that the statement is false; that is, suppose there are finitely many primes.

Then we can number the primes $p_1, p_2, \ldots p_n$, where p_n is the largest prime.

Consider the number

$q = p_1 \cdot p_2 \ldots p_n + 1$ formed by multiplying all these primes and then adding 1.

We claim that q is a prime. It cannot be divided evenly by any prime p_i with $i < n$; this

will always result in a remainder of 1. And if it could be divided the that evenly by a composite number c, then it could also be a divided by some prime factor of c.. but this again results in a remainder of 1. So the only factors of q are 1 and itself.

This means that q is a prime number larger than p_n, But we assumed p_n was the largest prime, so this a contradiction.

Therefore, there are infinitely many primes.

Example 2:
Show that these statements about the integer n are equivalent:

P_1 : n is even.
P_2 : n - 1 is odd.
P_3 : n^2 is even.

Solution:

We will show that these three statements are equivalent by showing the conditional statements

$P_1 \to P_2$, $P_2 \to P_3$ and $P_3 \to P_1$ are true.

we use a direct proof to show that $P_1 \to P_2$. Suppose that n is even. The $n = 2k$ for some integer k. Consequently,

$n - 1 = 2k - 1 = 2(k-1) + 1$. This means that $n-1$ is odd because it is of the form $2m+1$, wher m is the integer $k-1$.

we also use a direct proof to show that $P_2 \to P_3$. Now suppose $n-1$ is odd. Then,

$n - 1 = 2k + 1$ for some integer k.

Hence,

$n = 2k + 2$, so that

$n^2 = (2k+2)^2 = 4k^2 + 8k + 4 = 2(2k^2 + 4k + 2)$.

This means that n^2 is twice the integer $2k^2 + 4k + 2$, and hence is even.

To Prove $P_3 \to P_1$, we use a proof by contraposition. That is, we prove that if n is not even, then n^2 is not even. This is same proving that if n is odd, then n^2 is odd,

Mathematical Induction

Mathematical Induction is a Mathematical proof technique. It is essentially used to prove that

a statement $P(n)$ holds for every natural number $n = 0, 1, 2, 3, \ldots$ that is the overall statement is a sequence of infinitely many cases ($P(0)$, $P(1)$, $P(2)$, $P(3)$, ...

Mathematical induction proves that we can climb as high as we like on a ladder,

A proof by induction consists of two cases. The first, the base case (or basis), proves the statement for $n = 0$ without assuming any knowledge of other cases. The second case, the induction step, proves that if the statement holds for any given case $n = k$, then it must also hold for the next case $n = k + 1$.

These two steps establish that the statement holds for every natural number n.

Example:
Prove by induction that $11^n - 6$ is divisible by 5 for every positive integer n.

Solution:

Let $P(n)$ be the mathematical statement
$11^n - 6$ is divisible by 5.

Base case: when $n = 1$ we have $11^1 - 6 = 5$ which is divisible by 5. So $P(1)$ is correct.

Induction hypothesis: Assume that $P(k)$ is correct for some positive integer k. That means $11^k - 6$ is divisible by 5 and hence $11^k - 6 = 5m$ for some integer m.
So $11^k = 5m + 6$.

Induction step: we will now show that $P(k+1)$ is correct. In this case we want to show that $11^{k+1} - 6$ can be expressed as a multiple of 5, so we will start with the formula $11^{k+1} - 6$ and we will rearrange it into something involving multiples of 5. At some point we will also want to use the assumption that

$11^k = 5m + 6$.

$11^{k+1} - 6 = (11 \times 11^k) - 6$ by the laws of powers

$= 11(5m + 6) - 6$ by the induction hypothesis.

$= 11(5m) + 66 - 6$ by expanding the bracket

$= 5(11m) + 60$.

$= 5(11m + 12)$ since both parts of the formula have a common factor of 5.

As $11m + 12$ is an integer we have that $11^{k+1} - 6$ is divisible by 5, so $P(k+1)$ is correct.

Hence by mathematical induction $P(n)$ is correct for all positive integers n.