Proof Techniques

A proof is a sequence/series of formal statements that are either givens or deductions from givens, including deductions from previous deductions. In this section, we ar egoing to **review** direct proof, proof by contradiction, and mathematical induction.

Direct Proof

Direct proof is essentially a sequence of statements which are either givens or deductions from previous statements. These deductions may be established facts, axioms, lemmas, or theorems.

Sum of two even integers, a and b, is an even integer

Let's define the given first, even integers. An integer is said to be even if and only if it is of the form 2∗k where k $\in \mathbb{Z}$. Below are some even integers:

$$28 \text{ is even because } 2 * 14 \text{ where } 14 \in \mathbb{Z}$$
$$38 \text{ is even because } 2 * 19 \text{ where } 19 \in \mathbb{Z}$$
$$-6 \text{ is even because } 2 * (-3) \text{ where } -3 \in \mathbb{Z}$$

Proof. Since a is even, then a = 2∗k. And since b is even as well, then b = 2∗j. Therefore, the following hold.

$$a + b = 2k + 2j$$
$$a + b = 2(k + j)$$

Since $k \in \mathbb{Z}$ and $j \in \mathbb{Z}$, and $\mathbb{Z}$ is closed under addition, therefore $(k + j) \in \mathbb{Z}$ We let $m = k + j$, this gives us $a + b = 2 * m$. Therefore, the sum of two even integers, a and b, is even.

h.n.

Sum of two odd integers, a and b, is even

Let's define the given first, odd integers. An integer is said to be odd if and only if it is of the form 2∗k + 1 where k $\in \mathbb{Z}$. Below are some even integers:

$$27 \text{ is even because } 2 * 13 + 1 \text{ where } 13 \in \mathbb{Z}$$
$$39 \text{ is even because } 2 * 19 + 1 \text{ where } 19 \in \mathbb{Z}$$
$$-7 \text{ is even because } 2 * (-4) + 1 \text{ where } -4 \in \mathbb{Z}$$

Proof. Since a is odd, then a = $2*$k + 1. And since b is odd as well, then b = $2*$j + 1. Therefore, the following hold.

$$a + b = 2k + 1 + 2j + 1$$
$$a + b = 2k + 2j + 2$$
$$a + b = 2(k + j + 1)$$

Since $k \in \mathbb{Z}$, $j \in \mathbb{Z}$, $1 \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under addition, therefore $(k+j+1) \in \mathbb{Z}$. We let $m = k + j$, this gives us $a + b = 2*m + 1$. Therefore, the sum of two odd integers, a and b, is even.

h.n.

Summation - $\sum_{i=1}^{n} i = n(n+1)/2$

Let's test this first. With n being 5.

$$\sum_{i=1}^{5} i = 1 + 2 + 3 + 4 + 5$$
$$= 15$$

$$\sum_{i=1}^{5} i = \frac{5 \cdot (5+1)}{2}$$
$$= \frac{30}{2}$$
$$= 15$$

Proof. Let this sum be S.

$$S = 1 + 2 + 3 + \cdots + n - 1 + n \text{ (definition of summation)}$$
$$S = n + (n-1) + (n-2) + \cdots + 2 + 1 \text{ (addition is commutative)}$$
$$2S = (n+1) + (n+1) + ... + (n+1) \text{ (S+S, term by term addition)}$$
$$2S = n \cdot (n+1) \text{ (there are n terms of n + 1)}$$
$$S = n \cdot (n+1)/2 \text{ (simplifying the left hand side)}$$

h.n.

Proof (Disproof) by counter example

In proving a statement, it must be proven that the claim holds for all cases. But only one counterexample is needed to dispprove a claim.

∀ positive integers n, if n is prime, then n is odd

Proof. Some prime numbers $3, 5, 711, 23, 31$. But 2 is prime as well. But it is even. $2 = 2 * 1$, $1 \in \mathbb{Z}$. Therefore, we found a counterexample that dispproves the claim.

h.n.

Proof by contradiction

The proof assumes that the opposite proposition or claim is true, then it shows or arrives at a contradiction.

Prove that the $\sqrt{2}$ is irrational

Proof. We assume that the opposite is true. This means we assume that $\sqrt{2}$ is rational. A number is rational if it can expressed as a quotient or ratio p/q, where $p, q \in \mathbb{Z}$ and $q \neq 0$, and p/q is in it lowest terms. So this means that $\sqrt{2} = p/q$.

$$\sqrt{2} = p/q$$
$$2 = p^2/q^2$$
$$2q^2 = p^2$$

This means that p^2 is even because of $2q^2$. Since $q \in \mathbb{Z}$, $q^2 \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under multiplication, p^2 is even. There are 2 possibilities for this. One is if p is odd, and the other is when p is even.
Case p is odd:

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

This tells us that if p is odd, then p^2 is odd as well.
Case p is even:

$$p = 2k$$
$$p^2 = (2k)^2$$
$$p^2 = 4k^2$$
$$p^2 = 2(2k^2)$$

This tells us that there is only one way for p^2 to be even. And that is when p is even.
Since $2q^2$ is even as well, we get the following:

$$2q^2 = (2k)^2 q^2 \quad = \frac{4k^2}{2} q^2 = 2k^2$$

3

Following the same tact as with p^2 above, since q^2 is even, and so is q. Since p and q are both even, they have a common factor making p/q not in its lowest terms, contradicting the assumption. Since this is a contradiction, we have proven that $\sqrt{2}$ is irrational.

<div align="right">**h.n.**</div>

Show that $p^2 - q^2 = 1$ does not have positive integer solutions

Proof. We assume that $p^2 - q^2 = 1$ has positive solutions. And the way to go here is to solve for p and q. And hopefully arrive at a contradiction.

$$p^2 - q^2 = 1$$
$$(p + q)(p - q) = 1$$

There are two possibilities that the above will hold. $p + q$ and $p - q$ are both 1. And both $p + q$ and $p - q$ are -1. Let's look at the first case.

Case 1:
$$p + q = 1$$
$$p - q = 1$$

Solving for p, we get $2p = 2$. Hence, p p is 1. Solving for q, $1 + q = 1$ gives us q equal to 0. This is a contracdiction. Although p has a positive solution, q does does not, since it is 0. We do not stop here since there is still a second case. And that has to be verified as well.

Case 2:
$$p + q = -1$$
$$p - q = -1$$

Solving for p, we get $2p = -2$. Hence, p p is -1. At this point, we may stop. Since p is -1, even if we find a q that is positive, it will not change the fact that p is not. Again, this is a contradiction. Since there are no positive solutions arrived at, we can conclude via contradiction, that indeed, $p^2 - q^2 = 1$ does not have positive solutions.

<div align="right">**h.n.**</div>

Proof by Mathematical Induction

This technique involves three parts. The first step is the **base step**. The claim or proposition is tested or verified for some initial values. This step also helps in seeing or discovering certain patterns from the claim that will prove useful in the next steps.

The second step is the **inductive hypothesis**. This step assumes that the claim holds for values until k.

The third step is the **inductiove step**. This step proves that the claim also holds for values equal to $k + 1$.

Summation - $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Proof. Base Step. Let's check when $n = 1$. The summation from to 1 to 1 is 1. Let's verify this with the formula on the right-hand side.

$$1 \overset{?}{=} \frac{1(1+1)}{2}$$

$$1 \overset{?}{=} \frac{2}{2}$$

$$1 \overset{\checkmark}{=} 1$$

Let's check when $n = 1$. The summation from 1 to 2 is 3. Let's verify this with the formula if it holds.

$$3 \overset{?}{=} \frac{2(2+1)}{2}$$

$$3 \overset{?}{=} \frac{6}{2}$$

$$3 \overset{\checkmark}{=} 3$$

Inductive hypothesis. Assume that for all values $n = k$, $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$ holds.

Inductive Step. We are to show that it also holds for $n = k + 1$.

$$\sum_{i=1}^{k+1} i \overset{?}{=} \frac{(k+1)(k+1+1)}{2}$$

$$\sum_{i=1}^{k} i + (k+1) \overset{?}{=} \frac{(k+1)(k+2)}{2}$$

$$\frac{k(k+1)}{2} + (k+1) \overset{?}{=} \frac{(k+1)(k+2)}{2}, \text{ using the inductive hypothesis}$$

$$\frac{k(k+1) + 2(k+1)}{2} \overset{?}{=} \frac{(k+1)(k+2)}{2}, \text{ adding the fractions (2 as LCD)}$$

$$\frac{(k+1)(k+2)}{2} \overset{\checkmark}{=} \frac{(k+1)(k+2)}{2}, \text{ factoring (k+1) out}$$

Since we were able to show that for $n = k + 1$, the claim still holds, therefore the claim $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ holds.

h.n.

For any positive integer number n, $n^3 + 2n$ is divisible by 3

Proof. Base Step. Let's check when $n = 1$. $1^3 + 2 \cdot 1$ is 3. Indeed, it is divisible by 3. When $n = 2$, $2^3 + 2 \cdot 2$ is 12, also divisible by 3.

Inductive hypothesis. Assume that for all values $n = k$, $k^3 + 2k$ is divisible by 3 holds. This means that $k^3 + 2k = 3j$ where $j \in \mathbb{Z}^+$.

Inductive Step. We are to show that it also holds for $n = k + 1$.

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

Since it is a multiple of 3, it definitely is divisible by 3

Since we were able to show that for $n = k + 1$, the claim still holds, therefore the claim $n^3 + 2n$ is divisible by 3 holds.

h.n.