Method of Proof by Mathematical Induction

Principle of Mathematical Induction

Let $P(n)$ be a property that is defined for integers n and let a be a fixed integer. Suppose the following two statements are true:

1. $P(a)$ is true.
2. For every integer $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.

Then the statement

$$\text{for every integer } n \geq a,\ P(n)$$

is true.

Method of Proof by Mathematical Induction

Consider a statement of the form,

“For all integers $n \geq a$, a property $P(n)$ is true.”

To prove such a statement, perform the following two steps:

Step 1 (basis step): Show that $P(a)$ is true.

Step 2 (inductive step): Show that for all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.

To perform this step,

suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq a$.

[This supposition is called the inductive hypothesis.]

Then,

show that $P(k+1)$ is true.

Example: Use mathematical induction to prove that $1+2+\cdots+n=\frac{n(n+1)}{2}$ for all integers $n \geq 1$.

Proof: Let

$$P(n):\ 1+2+\cdots+n=\frac{n(n+1)}{2}$$

Step 1: Show that $\boldsymbol{P(1)}$ is true:

When $n=1$, $P(n)$ becomes

$$L.H.S=1$$

$$R.H.S=\frac{1(1+1)}{2}=\frac{2}{2}=1$$

Since $L.H.S=R.H.S$

Therefore, $P(1)$ is true.

Example: Use mathematical induction to prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all integers $n \geq 1$.

Proof: Let

$$P(n):\ 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Step 2: $\forall$ integers $\boldsymbol{k \geq 1}$, if $\boldsymbol{P(k)}$ is true then $\boldsymbol{P(k+1)}$ is true.

Suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq 1$.

This means that

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}$$

[we need to show that $P(k+1)$ is also true. That is $P(k+1)$: $1 + 2 + \cdots + k + (k+1) = \frac{(k+1)(k+2)}{2}$]

Example: Use mathematical induction to prove that $1+2+\cdots+n=\frac{n(n+1)}{2}$ for all integers $n \geq 1$.

Proof: Let

$$P(n):\ 1+2+\cdots+n=\frac{n(n+1)}{2}$$

Step 2: $\forall$ integers $k \geq 1$, if $P(k)$ is true then $P(k+1)$ is true.

Suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq 1$.

This means that

$$1+2+\cdots+k=\frac{k(k+1)}{2}$$

[we need to show that $P(k+1)$ is also true. That is $P(k+1)$: $1+2+\cdots+k+(k+1)=\frac{(k+1)(k+2)}{2}$]

So, consider the left-hand side of $P(k+1)$

$$\begin{aligned} &1+2+\cdots+k+(k+1) \\ &=\frac{k(k+1)}{2}+(k+1) && \text{by } P(k) \\ &=(k+1)\left(\frac{k}{2}+1\right) \\ &=\frac{(k+1)(k+2)}{2} \end{aligned}$$

Which is equal to the right side of $P(k+1)$.

Thus, the two sides of $P(k+1)$ are equal. Therefore, the equation $P(k+1)$ is true [as was to be shown].

[Since we have proved both the basis step and the inductive step, we conclude that the theorem is true.]

$P(a)$ is true.

For every integer $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.

For every integer $\mathrm{n} \geq a$, $P(n)$ is true

Definition:

If a sum with a variable number of terms is shown to be equal to a formula that does not contain either an ellipsis or a summation symbol, we say that it is written in **closed form**.

Example: Evaluate $5+6+7+8+\cdots+50$.

The sum of first 50 natural numbers is

$$1+2+3+\cdots+50=\frac{50(50+1)}{2}=\frac{50.51}{2}$$

Then our sum

$$5+6+7+8+\cdots+50=\frac{(50)51}{2}-(1+2+3+4)$$

$$=(25)51-10=1265$$

Example: For an integer $h \geq 2$, write $1 + 2 + 3 + \cdots + (h - 1)$ in closed form.

Solution:

By the formula of the sum of the first n integer is

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Substituting $n = h - 1$, we get

$$1 + 2 + 3 + \cdots + (h - 1)$$
$$= \frac{(h-1)(h-1+1)}{2}$$
$$= \frac{h(h-1)}{2}$$

Example: Use mathematical induction to prove that $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$, for all integers $n \geq 1$.

Proof: Let

$$P(n):\ 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Step 1: Show that $\boldsymbol{P(1)}$ is true:

When $n = 1$, $P(n)$ becomes

$$L.H.S = 1^2 = 1$$

$$R.H.S = \frac{1(1+1)(2(1)+1)}{6} = \frac{(2)(3)}{6} = 1$$

Since $L.H.S = R.H.S$

Therefore, $P(1)$ is true.

Example: Use mathematical induction to prove that $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$, for all integers $n \geq 1$.

Proof: Let

$$P(n):\ 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Step 2: $\forall$ **integers $\boldsymbol{k \geq 1}$,**
if $\boldsymbol{P(k)}$ is true then $\boldsymbol{P(k+1)}$ is true.

Suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq 1$.

This means that

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$$

[we need to show that $P(k+1)$ is also true. That is $P(k+1)$: $1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$]

Example: Use mathematical induction to prove that $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$, for all integers $n \geq 1$.

Proof: Let

$$P(n):\ 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Step 2: $\forall$ integers $k \geq 1$, if $P(k)$ is true then $P(k+1)$ is true.

Suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq 1$.

This means that

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$$

[we need to show that $P(k+1)$ is also true. That is $P(k+1)$: $1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$]

So, consider the left-hand side of $P(k+1)$

$$\begin{aligned}
&1^2 + 2^2 + \cdots + k^2 + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \qquad \text{by } P(k) \\
&= (k+1)\left(\frac{2k^2+k}{6} + (k+1)\right) \\
&= \frac{(k+1)(2k^2+7k+6)}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6}
\end{aligned}$$

Which is equal to the right side of $P(k+1)$.
Thus, the two sides of $P(k+1)$ are equal. Therefore, the equation $P(k+1)$ is true [as was to be shown].
[Since we have proved both the basis step and the inductive step, we conclude that the theorem is true.]

For any real number r except 1, and any integer $n \geq 0$,

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}.$$

Proof: Let

$$P(n): \sum_{i=0}^{n} r^i = r^0 + r^1 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1}$$

Step 1: Show that $\boldsymbol{P(0)}$ is true:

When $n = 0$, $P(0)$ becomes

$$L.H.S = 1$$

$$R.H.S = \frac{r^1 - 1}{r - 1} = 1$$

Since $L.H.S = R.H.S$

Therefore, $P(0)$ is true.

For any real number r except 1, and any integer $n \geq 0$,

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}.$$

Proof: Let

$$P(n): r^0 + r^1 + \cdots + r^n = \frac{r^{n+1}-1}{r-1}$$

Step 2: $\forall$ **integers** $\boldsymbol{k \geq 0}$,
if $\boldsymbol{P(k)}$ **is true then** $\boldsymbol{P(k+1)}$ **is true**.

Suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq 0$.

This means that

$$r^0 + r^1 + \cdots + r^k = \frac{r^{k+1}-1}{r-1}$$

[we need to show that $P(k+1)$ is also true. That is $P(k+1): r^0 + r^1 + \cdots + r^k + r^{k+1} = \frac{r^{k+2}-1}{r-1}$]

For any real number r except 1, and any integer $n \geq 0$,

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}.$$

Proof: Let

$$P(n): r^0 + r^1 + \cdots + r^n = \frac{r^{n+1}-1}{r-1}$$

Step 2: $\forall$ **integers** $\boldsymbol{k \geq 0}$,
if $\boldsymbol{P(k)}$ **is true then** $\boldsymbol{P(k+1)}$ **is true**.

Suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq 0$.

This means that

$$r^0 + r^1 + \cdots + r^k = \frac{r^{k+1}-1}{r-1}$$

[we need to show that $P(k+1)$ is also true. That is $P(k+1): r^0 + r^1 + \cdots + r^k + r^{k+1} = \frac{r^{k+2}-1}{r-1}$]

So, consider the left-hand side of $P(k+1)$

$$r^0 + r^1 + \cdots + r^k + r^{k+1}$$
$$= \frac{r^{k+1}-1}{r-1} + r^{k+1} \quad \text{by } P(k)$$
$$= \frac{r^{k+1} - 1 + r^{k+2} - r^{k+1}}{r-1}$$
$$= \frac{r^{k+2}-1}{r-1}$$

Which is equal to the right side of $P(k+1)$.
Thus, the two sides of $P(k+1)$ are equal. Therefore, the equation $P(k+1)$ is true [as was to be shown].
[Since we have proved both the basis step and the inductive step, we conclude that the theorem is true.]

Exercise:

Prove that

$$\sum_{i=1}^{n-1} i(i+1) = \frac{n(n-1)(n+1)}{3}$$

For every integer $n \geq 2$.

Exercise:

Prove that

$$\sum_{i=1}^{n-1} i(i+1) = \frac{n(n-1)(n+1)}{3}$$

For every integer $n \geq 2$.

Skipping to step 2:

$$P(k): 1(2) + 2(3) + \cdots + (k-1)k = \frac{k(k-1)(k+1)}{3}$$

LHS of $P(k+1)$

$$1(2) + 2(3) + \cdots + (k-1)k + k(k+1) = \frac{k(k-1)(k+1)}{3} + k(k+1)$$

$$= k(k+1)\left[\frac{k-1}{3} + 1\right]$$

Example: Use mathematical induction to prove that for all integers $n \geq 0$, $2^{2n} - 1$ is divisible by 3.

Proof:

$$P(n): 3|(2^{2n} - 1)$$

Step 1: show that $P(0)$ is true.

When $n = 0$,

$$2^{2n} - 1$$

becomes

$$2^0 - 1 = 1 - 1 = 0$$

Because every integer divides 0, therefore $3|0$.

Therefore, $P(0)$ is true.

Example: Use mathematical induction to prove that for all integers $n \geq 0$, $2^{2n} - 1$ is divisible by 3.

Proof:

$$P(n): 3|(2^{2n} - 1)$$

Step 2: Show that $\forall$ int $\boldsymbol{n \geq 0}$, $\boldsymbol{if\ P(k)}$ is true then $\boldsymbol{P(k+1)}$ is true.

Suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq 0$.

This means that

$$2^{2k} - 1 = 3q$$

For some integer q.

[we need to show that $P(k+1)$ is also true. That is

$$P(k+1): 3|2^{2(k+1)} - 1]$$

Consider,

$$\begin{aligned} & 2^{2(k+1)} - 1 \\ &= 2^{2k}.2^2 - 1 \\ &= 2^{2k}.4 - 1 \\ &= 2^{2k}(3+1) - 1 \\ &= 3.2^{2k} + 2^{2k} - 1 \\ &= 3.2^{2k} + 3q \\ &= 3\left(2^{2k} + q\right) = 3q' \end{aligned}$$

Where $q' \in \mathbb{Z}$. Therefore, $P(k+1)$ is true [as was to be shown].

[Since we have proved both the basis step and the inductive step, we conclude that the theorem is true.]

Example: Use mathematical induction to prove that for all integers $n \geq 3$, $2n + 1 < 2^n$.

Proof:

$$P(n): 2n + 1 < 2^n$$

Step 1: show that $P(3)$ is true.

When $n = 3$,

$$L.H.S:\ 2n - 1 = 2(3) - 1 = 5$$

and

$$R.H.S:\ \ 2^n = 2^3 = 8$$

Since L.H.S < R.H.S.

Therefore, $P(3)$ is true.

Example: Use mathematical induction to prove that for all integers $n \geq 3$, $2n + 1 < 2^n$.

Proof:

$$P(n): 2n + 1 < 2^n$$

Step 2: Show that $\forall$ int $\boldsymbol{n \geq 3}$, $\boldsymbol{if\ P(k)}$ is true then $\boldsymbol{P(k+1)}$ is true.

Suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq 3$.

This means that

$$2k + 1 < 2^k.$$

[we need to show that $P(k+1)$ is also true.
That is $P(k+1): 2(k+1) + 1 < 2^{k+1}$]

Consider,

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

That is,

$$2(k+1) + 1 < 2^k + 2 \qquad (1)$$

Since $k \geq 3$,

$$2 < 2^k$$

Add 2^k on both sides,

$$2^k + 2 < 2^k + 2^k \qquad (2)$$

Combining (1) and (2), we get

$$2(k+1) + 1 < 2^k + 2^k = 2.2^k = 2^{k+1}$$

Therefore, the $P(k+1)$ is true [as was to be shown].
[Since we have proved both the basis step and the inductive step, we conclude that the theorem is true.]

Example: Use mathematical induction to prove that $1 + 3n \leq 4^n$, for every integer $n \geq 0$.

Proof:

$$P(n): 1 + 3n \leq 4^n$$

Step 1: show that $P(0)$ is true.

When $n = 0$,

$$L.H.S: 1 + 3n = 1$$

and

$$R.H.S: \ 4^n = 4^0 = 1$$

Since L.H.S $\leq$ R.H.S.

Therefore, $P(0)$ is true.

Example: Use mathematical induction to prove that $1 + 3n \le 4^n$, for every integer $n \ge 0$.

Proof:

$$P(n): 1 + 3n \le 4^n$$

Step 2: Show that $\forall$ int $\boldsymbol{k \ge 0}$, $\boldsymbol{if\ P(k)}$ is true then $\boldsymbol{P(k+1)}$ is true.

Suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \ge 0$.

This means that

$$1 + 3k \le 4^k.$$

[we need to show that $P(k+1)$ is also true.
That is $P(k+1): 1 + 3(k+1) \le 4^{k+1}$]

Consider,

$$1 + 3(k+1)$$
$$= 1 + 3k + 3$$
$$\le 4^k + 3$$

That is,

$$1 + 3(k+1) \le 4^k + 3 \qquad (1)$$

For all $k \ge 0$, $1 \le 4^k$ or

$$3 \le 3.4^k$$

Add 4^k on both sides,

$$4^k + 3 \le 4^k + 3.4^k \qquad (2)$$

Combining (1) and (2), we get

$$1 + 3(k+1) < 4^k + 3.4^k = 4^k(1+3) = 4.4^k$$

Therefore, the $P(k+1)$ is true [as was to be shown].
[Since we have proved both the basis step and the inductive step, we conclude that the theorem is true.]

Proposition: For all integers $n \geq 8$, n ¢ can be obtained using 3 ¢ and 5 ¢ coins.

Proof (by mathematical induction):

Let the property

$P(n)$: n¢ can be obtained using 3¢ and 5¢ coins.

Step 1: Show that P(8) is true:

$P(8)$ is true because 8¢ can be obtained using one 3¢ coin and one 5¢ coin.

Proposition: For all integers $n \geq 8$, n ¢ can be obtained using 3 ¢ and 5 ¢ coins.

$P(n)$: n¢ can be obtained using 3¢ and 5¢ coins.

Step2: Show that for all integers $\boldsymbol{k \geq 8}$, if $\boldsymbol{P(k)}$ is true then $\boldsymbol{P(k+1)}$ is also true:

Suppose that $P(k)$ is true for a particular but arbitrarily chosen integer $k \geq 8$. That is

k¢ can be obtained using 3¢ and 5¢ coins.

[We must show that $P(k+1)$ is true. That is

$(k+1)$¢ can be obtained using 3¢ and 5¢ coins.]

Case 1 (There is a 5¢ coin among those used to make up the $\boldsymbol{k}$¢.):

In this case replace the 5¢ coin by two 3¢ coins; the result will be $(k+1)$¢.

Proposition: For all integers $n \geq 8$, n ¢ can be obtained using 3 ¢ and 5 ¢ coins.

$P(n)$: n¢ can be obtained using 3¢ and 5¢ coins.

Step2: Show that for all integers $\boldsymbol{k \geq 8}$, if $\boldsymbol{P(k)}$ is true then $\boldsymbol{P(k+1)}$ is also true:

Suppose that $P(k)$ is true for a particular but arbitrarily chosen integer $k \geq 8$. That is

k¢ can be obtained using 3¢ and 5¢ coins.

[We must show that $P(k+1)$ is true. That is

$(k+1)$¢ can be obtained using 3¢ and 5¢ coins.]

Case 1 (There is a 5¢ coin among those used to make up the $\boldsymbol{k}$¢.):

In this case replace the 5¢ coin by two 3¢ coins; the result will be $(k+1)$¢.

Case 2 (There is not a 5¢ coin among those used to make up the $\mathbf{k}$¢.):

In this case, because $k \geq 8$, at least three 3¢ coins must have been used. So remove three 3¢ coins and replace them by two 5¢ coins; the result will be $(k+1)$¢.

Thus in either case $(k+1)$¢ can be obtained using 3¢ and 5¢ coins [as was to be shown]. [Since we have proved the basis step and the inductive step, we conclude that the proposition is true.]

Example:

A sequence $a_1, a_2, a_3, \dots$ is defined by letting

$$a_1 = 3 \text{ and } a_k = 7a_{k-1}, \qquad \text{for all integers } k \geq 2.$$

Show that

$$a_n = 3 \cdot 7^{n-1}, \qquad \text{for all integers } n \geq 1.$$

$$P(n)\colon\ a_n = 3 \cdot 7^{n-1}$$

Example:

A sequence $a_1, a_2, a_3, \ldots$ is defined by letting

$a_1 = 3$ and $a_k = 7a_{k-1}$, for all integers $k \geq 2$.

Show that

$a_n = 3 \cdot 7^{n-1}$, for all integers $n \geq 1$.

$$P(n)\text{: } a_n = 3 \cdot 7^{n-1}$$

Example:

A sequence $a_1, a_2, a_3, \ldots$ is defined by letting

$a_1 = 3$ and $a_k = 7a_{k-1}$,

for all integers $k \geq 2$.

Show that $a_n = 3 \cdot 7^{n-1}$,

for all integers $n \geq 1$.

$$P(n)\colon\ a_n = 3 \cdot 7^{n-1}$$

Step1: P(?)

Step2: Let k be an int ≥1, such that P(k) is true

$$a_k = 3 \cdot 7^{k-1}$$

By the definition of the seq,

$$\begin{aligned} a_{k+1} &= 7.\,a_k \\ &= 7.\left(3.7^{k-1}\right) \\ &= 3.7^{k-1+1} \\ &= 3.7^{k} \end{aligned}$$

$$P(k+1)\colon a_{k+1} = 3.7^{k}$$

Example:

A sequence $c_0, c_1, c_2, \ldots$ is defined by letting

$$c_0 = 3 \text{ and } c_k = (c_{k-1})^2$$

for all integers $k \geq 1$. Show that

$$c_n = 3^{2^n}$$

for all integers $n \geq 0$.

$$P(n)\colon\ c_n = 3^{2^n}$$

Principle of Strong Mathematical Induction

Let $P(n)$ be a property that is defined for integers n, and let a and b be fixed integers with $a \leq b$. Suppose the following two statements are true:

1. $P(a), P(a+1), \ldots,$ and $P(b)$ are all true. (basis step)
2. For any integer $k \geq b$, if $P(i)$ is true for all integers i from a through k, then $P(k+1)$ is true. (inductive step)

Then the statement

$$\text{For all integers } n \geq a, P(n)$$

is true.

Example:

Define a sequence $s_0, s_1, s_2, \ldots$ as follows:

$$s_0 = 0,\ s_1 = 4,\ s_k = 6s_{k-1} - 5s_{k-2}$$

for all integers $k \geq 2$.

the claim is that all the terms of the sequence satisfy the equation

$$s_n = 5^n - 1.$$

Prove that this is true.

Example:Define a sequence $s_0, s_1, s_2, \dots$ as follows:

$$s_0 = 0,\ s_1 = 4,\ s_k = 6s_{k-1} - 5s_{k-2} \text{ for all integers } k \geq 2.$$

the claim is that all the terms of the sequence satisfy the equation

$$s_n = 5^n - 1.$$

Proof:

let the property

$$P(n): s_n = 5^n - 1$$

We will use strong mathematical induction to prove that for all integers $n \geq 0, P(n)$ is true.

Show that $P(0)$ and $P(1)$ are true:
To establish $P(0)$ and $P(1)$, we must show that

$$s_0 = 5^0 - 1 \text{ and } s_1 = 5^1 - 1.$$

But, by definition of $s_0, s_1, s_2, \dots,$ we have that $s_0 = 0$ and $s_1 = 4$.
Since $5^0 - 1 = 1 - 1 = 0$ and $5^1 - 1 = 5 - 1 = 4$, the values of s_0 and s_1 agree with the values given by the formula.

Example:Define a sequence $s_0, s_1, s_2, \ldots$ as follows:

$$s_0 = 0,\ s_1 = 4,\ s_k = 6s_{k-1} - 5s_{k-2} \text{ for all integers } k \geq 2.$$

the claim is that all the terms of the sequence satisfy the equation

$$s_n = 5^n - 1.$$

Proof:

let the property

$$P(n): s_n = 5^n - 1$$

Step 2: Show that for all integers $k \geq 1$, if $P(i)$ is true for all integers i from 0 through k, then $P(k + 1)$ is also true:

Let k be any integer with $k \geq 1$ and suppose that

$s_i = 5^i - 1$ for all integers i with $0 \leq i \leq k$.

[We must show that

$$s_{k+1} = 5^{k+1} - 1.]$$

But since $k \geq 1$, we have that $k + 1 \geq 2$, and so

$$\begin{aligned} s_{k+1} &= 6s_k - 5s_{k-1} \\ &= 6(5^k - 1) - 5(5^{k-1} - 1) \\ &= 6 \cdot 5^k - 6 - 5^k + 5 \\ &= (6-1)5^k - 1 \\ &= 5 \cdot 5^k - 1 \\ &= 5^{k+1} - 1. \end{aligned}$$

Therefore, the $P(k + 1)$ is true [as was to be shown].

[Since we have proved both the basis step and the inductive step, we conclude that the theorem is true.]

Example:

Suppose that $h_0, h_1, h_2, \ldots$ is a sequence is defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3,$$
$$h_k = h_{k-1} + h_{k-2} + h_{k-3}$$

for each integer $k \geq 3$.

Prove that $h_n \leq 3^n$ for every integer $n \geq 0$.

$$P(n)\text{: } h_n \leq 3^n$$

Example: Suppose that $h_0, h_1, h_2, \ldots$ is a sequence is defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3, \qquad h_k = h_{k-1} + h_{k-2} + h_{k-3}$$

for each integer $k \geq 3$. Prove that $h_n \leq 3^n$ for every integer $n \geq 0$.

Proof:

let the property

$$P(n): h_n \leq 3^n$$

We will use strong mathematical induction to prove that for all integers $n \geq 0, P(n)$ is true.

Step 1: Show that $P(0)$, $P(1)$ and $P(2)$ are true:
Since $h_0 = 1 \leq 3^0$, $h_1 = 2 \leq 3^1$ and $h_2 = 3 \leq 3^2$

Therefore, the values of h_0, h_1 and h_2 agree with the values given by the formula.

$\forall\ int\ k \geq 2$, if P(i) is true where $0 \leq i \leq k$ then P(k+1) is true

Example: Suppose that $h_0, h_1, h_2, \ldots$ is a sequence is defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3, \qquad h_k = h_{k-1} + h_{k-2} + h_{k-3}$$

for each integer $k \geq 3$. Prove that $h_n \leq 3^n$ for every integer $n \geq 0$.

Proof:

let the property

$$P(n): h_n \leq 3^n$$

Step 2: Show that for all integers $k \geq 2$, if $P(i)$ is true for all integers i from 0 through k, then $P(k + 1)$ is also true:

Let k be any integer with $k \geq 2$ and suppose that

$$h_i \leq 3^i$$

for all integers i with $0 \leq i \leq k$.

[We must show that

$$h_{k+1} \leq 3^{k+1}.]$$

By the recursive definition,

$$h_{k+1} = h_k + h_{k-1} + h_{k-2}$$
$$\leq 3^k + 3^{k-1} + 3^{k-2}$$
$$= 3^{k-2}(3^2 + 3 + 1) = 3^{k-2}(13)$$

Therefore,

$$h_{k+1} \leq 3^{k-2}(13)$$

Since $13 \leq 3^3$, we get

$$h_{k+1} \leq 3^{k-2}(13) \leq 3^{k-2}.3^3 = 3^{k+1}$$

Therefore, the $P(k+1)$ is true [as was to be shown].

[Since we have proved both the basis step and the inductive step, we conclude that the theorem is true.]

Application: Correctness of Algorithms

Definitions:

Consider an algorithm that is designed to produce a certain final state from a certain initial state. Both the initial and final states can be expressed as predicates involving the input and output variables.

<u>pre-condition</u>

Often the predicate describing the initial state is called the pre-condition for the algorithm, and

<u>post-condition</u>

the predicate describing the final state is called the *post-condition* for the algorithm.

Example:

Algorithm to compute a product of nonnegative integers

Pre-condition: The input variables m and n are nonnegative integers.

Post-condition: The output variable p equals mn.

Definition:

A ***loop invariant*** is a predicate with domain a set of integers, which satisfies the condition:

For each iteration of the loop, if the predicate is true before the iteration, then it is true after the iteration.

Example: show that if the predicate is true before entry to the loop, then it is also true after exit from the loop.

loop:

while ($m \geq 0$ and $m \leq 100$)

$m := m + 1$

$n := n - 1$

end while

predicate: $m + n = 100$

Example: show that if the predicate is true before entry to the loop, then it is also true after exit from the loop.

loop:

while ($m \geq 0$ and $m \leq 100$)

$m := m + 1$

$n := n - 1$

end while

predicate: $m + n = 100$

Let m_{old}, n_{old} be the values of the algorithm variables before the entry to the loop.

Also assume that the given predicate is true for these values of the algorithm variables, that is

$$m_{old} + n_{old} = 100$$

Now let m_{new}, n_{new} be the values of the algorithm variables after exiting from the loop. Then

$$m_{new} := m_{old} + 1$$

$$n_{new} := n_{old} - 1$$

The sum of the new values of the variables will be

$$\begin{gathered} m_{new} + n_{new} \\ = (m_{old} + 1) + (n_{old} - 1) \\ = 100 \end{gathered}$$

Therefore, the predicate is true after exit from the loop.

Definition:

A loop is defined as *correct* with respect to its pre- and post-conditions if, and only if, whenever

(a) the algorithm variables satisfy the pre-condition for the loop and

(b) the loop terminates after a finite number of steps,

(c) the algorithm variables satisfy the post-condition for the loop.

Establishing the correctness of a loop uses the concept of loop invariant.

If the predicate satisfies the following two additional conditions, the loop will be correct *with respect to it pre- and post-conditions*:

1. It is true before the first iteration of the loop.
2. If the loop terminates after a finite number of iterations, the truth of the loop invariant ensures the truth of the post-condition of the loop.

Loop Invariant Theorem

Let a while loop with guard G be given, together with pre- and post-conditions that are predicates in the algorithm variables. Also let a predicate $I(n)$, called the loop invariant, be given. If the following four properties are true, then the loop is correct with respect to its pre- and post-conditions.

- **Basis Property:** The pre-condition for the loop implies that $I(0)$ is true before the first iteration of the loop.
- **Inductive Property:** For all integers $k \geq 0$, if the guard G and the loop invariant $I(k)$ are both true before an iteration of the loop, then $I(k+1)$ is true after iteration of the loop.
- **Eventual Falsity of Guard:** After a finite number of iterations of the loop, the guard G becomes false.
- **Correctness of the Post-Condition:** If N is the least number of iterations after which G is false and $I(N)$ is true, then the values of the algorithm variables will be as specified in the post-condition of the loop.

Example:

[Pre-condition: m is a nonnegative integer, x is a real number, $i = 0$, and $exp = 1$.]

while ($i \neq m$)
$exp := exp \cdot x$
$i := i + 1$
end while

[Post-condition: $exp = x^m$]

loop invariant: $I(n)$ is "$exp = x^n$ and $i = n$."

Use the loop invariant theorem to prove that the while loop is correct with respect to the given pre- and post-conditions.

[Pre-condition: m is a nonnegative integer, x is a real number, $i = 0$, and $exp = 1$.]

while ($i \neq m$)
    $exp := exp \cdot x$
    $i := i + 1$
end while

[Post-condition: $exp = x^m$]

$I(n)$: $exp = x^n$ and $i = n$

Basis Property: The pre-condition for the loop implies that $I(0)$ is true before the first iteration of the loop.

Pre-condition suggests that the algorithm variable exp has the value 1 and $i = 0$.

When $n = 0$, $I(0)$ is $exp = x^0 = 1$ and $i = 0$, which is in accordance with the pre-condition.

Therefore, $I(0)$ is true before the first iteration of the loop.

[Pre-condition: m is a nonnegative integer, x is a real number, $i = 0$, and $exp = 1$.]

while ($i \neq m$)

$exp := exp \cdot x$

$i := i + 1$

end while

[Post-condition: $exp = x^m$]

$I(n)$: $exp = x^n$ and $i = n$

Inductive Property: For all integers $k \geq 0$, if the guard G and the loop invariant $I(k)$ are both true before an iteration of the loop, then $I(k+1)$ is true after iteration of the loop.

Let k be an arbitrary but particular integer ≥0 such that the guard G and the loop invariant $I(k)$ are both true before an iteration of the loop.
This means that

$exp_{old} = x^k$ and $i_{old} = k$ and

$i_{old} \neq m$ or $i_{old} < m$.

then after $(k+1)$th iteration of the loop, we get

$$\exp_{new} = \exp_{old}. x = x^{k+1},$$

$$i_{new} = i_{old} + 1 = k + 1$$

Which implies that $I(k+1)$ is true after the next iteration of the loop.

[Pre-condition: m is a nonnegative integer, x is a real number, $i = 0$, and $exp = 1$.]

while ($i \neq m$)
    $exp := exp \cdot x$
    $i := i + 1$
end while

[Post-condition: $exp = x^m$]

$I(n)$: $exp = x^n$ and $i = n$

Eventual Falsity of Guard: After a finite number of iterations of the loop, the guard G becomes false.

After m number of iterations of the loop, the guard G becomes false.

[Pre-condition: m is a nonnegative integer, x is a real number, $i = 0$, and $exp = 1$.]

while ($i \neq m$)
    $exp := exp \cdot x$
    $i := i + 1$
end while

[Post-condition: $exp = x^m$]

$I(n)$: $exp = x^n$ and $i = n$

Correctness of the Post-Condition: If N is the least number of iterations after which G is false and $I(N)$ is true, then the values of the algorithm variables will be as specified in the post-condition of the loop.

Since m is the least number of iterations after which G is false and $I(m)$ is true. This means, $exp = x^m$ and $i = m$ which is as specified in the post-condition of the loop.