Proof by Induction

Proofs by induction are useful when we want to prove that a proposition is true for all natural numbers, or all integers above a particular value. The proof structure has three parts to it (though you often see the second and third parts combined into one step).

The first step is called the **base case**. In this step we prove that the lowest value (or values) that we're interested in makes the proposition we seek to prove true.

Second, we write the **inductive hypothesis**: a statement that says that the proposition is true for a generic case beyond the base case (k).

Last we perform the **inductive step**: we attempt to prove that the proposition is true for the step after the one stated in the inductive hypothesis (k + 1). We must make use of the inductive hypothesis at some point during the proof.

It's probably easiest to see a proof by induction in action.

Example 1: To prove: $3^n - 1$ is divisible by 2, for any $n \in \mathbb{N}$.

Solution: We'll prove this proposition by induction. The base case will consist of the lowest value from $\mathbb{N}$, which is 0:

Check: $2 \mid 3^0 - 1$
$2 \mid 1 - 1$
$2 \mid 0$ ✓

Next we need to write an inductive hypothesis about a generic natural number k. We'll do this by making use of the definition of "is divisible by":

Assume that $2 \mid 3^k - 1$; that is, $2m = 3^k - 1$ for some $m \in \mathbb{Z}$.

Now we'll attempt to prove that the statement is true for (k + 1). If we're asked to do a proof by induction, we ***must*** use the inductive hypothesis we just wrote! Otherwise it's not a proof by induction. (It may still be a valid proof, but then there's no reason to write the inductive hypothesis, etc.)

[*Continued on the next page…*]

Authored by Darren Rigby

Now we seek to prove that $2 \mid 3^{k+1} - 1$; that is $2p = 3^{k+1} - 1$ for some integer $p \in \mathbb{Z}$.

R.H.S. $= 3^{k+1} - 1$
$= 3 \cdot 3^k - 1$

If $2m = 3^k - 1$, where $m \in \mathbb{Z}$, then $2m + 1 = 3^k$:

$= 3 \cdot (2m + 1) - 1$ by I.H.
$= 3 \cdot 2m + 3 - 1$
$= 3 \cdot 2m + 3 - 1$
$= 3 \cdot 2m + 2$
$= 2[3 \cdot (2m - 1) + 1]$

Let $p = 3(2m - 1) + 1$. Since the integers are closed under addition, subtraction and multiplication, and since m is an integer, p must be an integer.

Therefore, by PMI, $3^{k+1} - 1$ is divisible by 2. ■

STRONG INDUCTION

Sometimes it's not enough to have a single base case. Sometimes we need several base cases, or our inductive hypothesis needs to assume that all cases from 1 to k − 1 are valid. In these cases, we can use the Principle of Strong Mathematical Induction to complete the proof.

Example 1: To prove: Given the recursive sequence, $a_1 = 1$; $a_2 = 2$; $a_3 = 3$; $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ for $n > 3$, prove that for all positive integers $a_n < 2^n$.

Solution: This proof is only about one term, by calculating later terms in the sequence requires several previous terms. Our inductive hypothesis will need to refer to those terms.

As a base case, the lowest value that applies for n is n = 1. However since we don't calculate the cases for n = 2 and n = 3, we can't use induction to reach those cases. We'll include them in the base cases we check:

For $n = 1$: $a_n = 1$; $2^n = 2$ and $1 < 2$ ✓
For $n = 2$: $a_n = 2$; $2^n = 4$ and $2 < 4$ ✓
For $n = 3$: $a_n = 3$; $2^n = 8$ and $3 < 8$ ✓

Next we need an induction hypothesis. We will assume that for the case of some integer greater than 4, the given statement is true, and then try to prove that the statement is true for the next successive integer, but this may not be enough. Using ordinary induction, it may be that the statement is true for k = 10, that is that $a_{10} = a_9 + a_8 + a_7 < 2^{10}$. Then we would try to prove that $a_{11} = a_{10} + a_9 + a_8 < 2^{11}$, but we don't know anything about a_9 or a_8. It's possible that they're both large numbers and a_7 is small enough to compensate. We need three statements to complete the IH to cover the numbers we'll need in the calculation:

Assume that the statement is true for (k − 2), (k − 1) and k where $k \geq 4$; that is $a_k < 2^k$, and also $a_{k-1} < 2^{k-1}$ and $a_{k-2} < 2^{k-2}$.

We need to prove that the statement is true for (k + 1): $a_{k+1} < 2^{k+1}$.

L.H.S. $= a_{k+1}$
$= a_k + a_{k-1} + a_{k-2}$

The Triangle Inequality says that if $m < x$ and $n < y$, then $m + n < x + y$. Using the IH on all three terms, we get:

$$
\begin{aligned}
&< 2^k + 2^{k-1} + 2^{k-2} = 4 \cdot 2^{k-2} + 2 \cdot 2^{k-2} + 2^{k-2} \\
&\qquad = 7 \cdot 2^{k-2} \\
&\qquad < 8 \cdot 2^{k-2} = 2^3 \cdot 2^{k-2} \\
&\qquad\qquad = 2^{k+1} = \text{R.H.S.}
\end{aligned}
$$

Thus, because inequalities are transitive (i.e., $[(a < b) \wedge (b < c) \rightarrow (a < c)]$):
$a_{k+1} < 2^{k+1}$.
Therefore, by PSMI, $a_n < 2^n$. ■

EXERCISES

A. Use the Principle of Mathematical Induction in each of the following problems.

1) A bank of light switches has a number of possible *positions*. A set of three switches might have the position on-on-off, for example. Prove that if you have n switches, there are 2^n possible positions.

2) Prove that for $n \in \mathbb{Z}^+$, $n^2 + n$ is divisible by 2.

3) Prove that the product of any three consecutive positive integers, $n_1 \cdot n_2 \cdot n_3$, is divisible by 6.

4) Prove that $3^n + 5^n \leq 8^n$ for $n \geq 2$.

5) Find the largest integer n such that $2^n \leq 10n$.

B. Use the Principle of Strong Mathematical Induction for the following problem.

1) Prove that given an unlimited supply of 3¢ stamps and 8¢ stamps, any amount of postage 14¢ and above can be paid. [*Hint:* The trick is to figure out how to procedurally generate any amount of postage. That will tell you how many base cases to prove.]

SOLUTIONS

A: 1) (BC) For $n = 1$ light switch, there are clearly two (2^1) positions, on and off.

(IH) Assume that for a row of k switches there are 2^k possible positions.

(IS) We need to prove that there are 2^{k+1} possible positions for $k + 1$ switches.

The $(k + 1)$th switch can be either on or off. The full list of all possible positions for $k + 1$ switches would be every position for k switches followed by "-on" and then every position for k switches followed by "-off". This would be double the length of the list for k positions. There would therefore be $2 \cdot 2^k$ positions in the list, which is 2^{k+1}.

Therefore, by PMI, there are 2^n possible positions for n switches. ■

2) (BC) $1^2 + 1 = 2$ and $2 \mid 2$.

(IH) Assume that for some integer k, that $k^2 + k \mid 2$. By the definition of "divisible", that means that there is some integer, which we will call "a", such that $k^2 + k = 2a$.

(IS) We need to prove that $(k + 1)^2 + (k + 1)$ is divisible by 2:

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

Since a and k are integers, $a + k + 1$ is an integer, since integers are closed under addition. Thus we have written $(k + 1)^2 + (k + 1)$ as 2 times some integer, and therefore $(k + 1)^2 + (k + 1)$ is divisible by 2.

Therefore, by PMI, $n^2 + n$ is divisible by 2. ■

3) (BC) $1 \cdot 2 \cdot 3 = 6$ and $6 \mid 6$.

(IH) Assume that $n_k \cdot n_{k+1} \cdot n_{k+2} \mid 6$. Since they're consecutive numbers, this means $(n_k)(n_k + 1)(n_k + 2) \mid 6$. If we expand the left side:

$n_k^3 + 3n_k^2 + 2n_k \mid 6$.

By the definition of "divisible" we know that there is some integer, which we will call b such that $n_k^3 + 3n_k^2 + 2n_k = 6b$

(IS) We need to prove that the next three consecutive integers have a product that is divisible by 6, i.e.: $(n_k + 1)(n_k + 2)(n_k + 3) \mid 6$

$$\begin{aligned}(n_k + 1)(n_k + 2)(n_k + 3) &= (n_k^2 + 3n_k + 2)(n_k + 3) \\ &= n_k^3 + 3n_k^2 + 2n_k + 3n_k^2 + 9n_k + 6 \\ &= 6b + 3n_k^2 + 9n_k + 6 \\ &= 6b + 3n_k^2 + 3n_k + 6n_k + 6 \\ &= 6b + 3(n_k^2 + n_k) + 6n_k + 6\end{aligned}$$

By Question A2, $n_k^2 + n_k$ is divisible by 2, so it can be written 2a, where a is some integer:

$$\begin{aligned}&= 6b + 3(2a) + 6n_k + 6 \\ &= 6(b + a + n_k + 1)\end{aligned}$$

Since b, a and n_k are integers, $b + a + n_k + 1$ is an integer, since integers are closed under addition. Thus we have written $(n_k + 1)(n_k + 2)(n_k + 3)$ as 6 times some integer, and therefore $(n_k + 1)(n_k + 2)(n_k + 3)$ is divisible by 6.

Therefore, by PMI, the product of any three consecutive positive integers is divisible by 6. ■

(4) (BC) L.H.S. = $3^2 + 5^2 = 9 + 25 = 34$; R.H.S. = $8^2 = 64$; $34 \leq 64$ ✓

(IH) Assume that for some integer k, $k \geq 2$, $3^k + 5^k \leq 8^k$.

(IS) We need to prove that $3^{k+1} + 5^{k+1} \leq 8^{k+1}$.

$3^{k+1} + 5^{k+1} = 3 \cdot 3^k + 5 \cdot 5^k$

It's true that $3 \leq 8$ and that $5 \leq 8$, so:

$3 \cdot 3^k \leq 8 \cdot 3^k$ and $5 \cdot 5^k \leq 8 \cdot 5^k$

Therefore by the Triangle Inequality:

$3 \cdot 3^k + 5 \cdot 5^k \leq 8 \cdot 3^k + 8 \cdot 5^k = 8 \cdot (3^k + 5^k)$

From the IH, we know that $3^k + 5^k \leq 8^k$. Therefore:

$8 \cdot (3^k + 5^k) \leq 8 \cdot 8^k = 8^{k+1}$

In summary, $3^{k+1} + 5^{k+1} \leq 8 \cdot (3^k + 5^k) \leq 8^{k+1}$. Since inequalities are transitive, $3^{k+1} + 5^{k+1} \leq 8^{k+1}$.

Therefore, by PMI, $3^n + 5^n \leq 8^n$ for all $n \in \mathbb{Z}$, $n \geq 2$. ■

(5) If n is a negative integer, then $10n < 2^n$, so we only need to consider non-negative integers. If we try the first few non-negative integers, we see that $2^n = 64$ and $10n = 70$ when $n = 6$, and $2^n = 128$ and $10n = 70$ when $n = 7$. Since we expect 2^n to increase faster than 10n, this suggests that 6 is the largest integer such that $2^n \leq 10n$. We can be certain of our answer by proving that $2^n \geq 10n$ for all $n \in \mathbb{Z}$, $n \geq 7$.

(BC) $128 \geq 70$.

(IH) Assume that for some integer k, $k \geq 7$, $2^k \geq 10k$.

(IS) We need to prove that $2^{k+1} \geq 10(k + 1)$.

$2^{k+1} = 2 \cdot 2^k$

We know that $2^k \geq 10k$. Since $k \geq 7$, $10k \geq 70$. Specifically, $10k \geq 10$:

$2^k + 10 \geq 10k + 10$

$2^k + 2^k \geq 2^k + 70 \geq 2^k + 10$

Since inequalities are transitive, $2^k + 2^k \geq 10k + 10$. But $2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$ and $10k + 10 = 10(k + 1)$. Therefore $2^{k+1} \geq 10(k + 1)$.

Therefore, by PMI, $2^n \geq 10n$ for all $n \in \mathbb{Z}$, $n \geq 7$, and therefore 6 is the largest integer such that $2^n \leq 10n$.

B. 1) (BC) Postage of 14¢ can be paid as 8¢ + 2 × 3¢. Postage of 15¢ can be paid as 5 × 3¢. Postage of 16¢ can be paid as 2 × 8¢.

(IH) Assume that three consecutive amounts of postage, $k - 2$, $k - 1$, and k, can all be paid.

(IS) We can easily prove that $k + 1$, $k + 2$ and $k + 3$ can all be paid; we add a 3¢ stamp to the three amounts in the IH:

$(k - 2) + 3 = k + 1$

$(k - 1) + 3 = k + 2$

$(k) + 3 = k + 3$

Therefore, by PMSI, any integer amount of postage equal to or greater than 14¢ can be paid with these stamps. ■