

# 6

## Induction

The principle of induction is a one of the most fundamental laws of mathematics. Students come across it, as here, as a method of proof. However, it is a basic property of the natural numbers (i.e. the positive integers) and can be considered as part of the definition of the natural numbers. Since we do not define the natural numbers here, the principle will be simply given as an axiom.<sup>1</sup>

### The Principle of Induction

Suppose the  $P$  is a proposition of integers, that is a sentence such that  $P(s)$  can be interpreted as “ $P$  is true for the number  $s$ .” Suppose further that  $P(1)$  is true. Suppose also that we can show that if  $P(n)$  is true for a positive integer then  $P(n+1)$  is also true. Then we can say that  **$P(n)$  is true for all positive integers.**

The idea behind the principle of induction is this: Suppose we have shown that  $P(1)$  is true and we have shown that  $P(n)$  is true implies  $P(n+1)$  is true. The second statement when applied to  $P(1)$  implies  $P(2)$  must be true. Applying the second statement to  $P(2)$  we have  $P(3)$  is true. Continuing ad infinitum,  $P$  must be true for all positive integers.

---

<sup>1</sup>That is we simply assume it to be true. In defining the natural numbers (positive integers) we either assume this axiom or we assume as true some other basic property and then prove the principle of induction based upon that. The most common such assumption is the rule that any non-empty set of positive integers has a least element. Although this rule seems far more obvious than the principle of induction, they can be shown to be equivalent (depending on what other axioms are given).

## How to Use the Principle of Induction

Most proofs by induction work as follows:  $P(1)$  is demonstrated by inspection (it is often obviously true). Often  $P(2)$  and  $P(3)$  are verified as well simply for reassurance. The critical step is to assume the **induction hypothesis**: that is assume  $P(n)$  is true for an **arbitrary positive integer  $n$** . Now show that it necessarily follows that  $P(n+1)$  is also true.

**Example** Prove by induction that  $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$ . If  $n=1$  we

get  $1^2 = 1 \cdot 2 \cdot 3 / 6$  which is true. Similarly, we can check that the statement holds for  $n=2$  and  $3$  (just to reassure ourselves). Now we assume the induction hypothesis that the statement holds for an arbitrary positive integer  $n$ . We need to verify that it follows that it is true for  $n+1$ . Consider,

$$1^2 + 2^2 + 3^2 + \dots + n^2 + (n+1)^2$$

The induction hypothesis applies

to the first  $n$  terms giving us  $\frac{n(n+1)(2n+1)}{6} + (n+1)^2$  which is equal to

$$\frac{(n+1)(n+2)(2n+3)}{6}$$

which is exactly what we need to prove. Note this last

expression is what you get when you replace  $n$  in  $\frac{n(n+1)(2n+1)}{6}$  by  $n+1$ .

It is generally a good idea to figure out ahead of time what sort of expression you are solving for.

**Example** Prove by induction that the sum of the first  $n$  odd (positive) integers is  $n^2$ . Since  $1 = 1^2$  this hold true for  $n=1$ . Just for reassurance we see that  $1+3 = 2^2$ . Let us then assume that the induction hypothesis is true for  $n$ :  $1+3+\dots+(2n-1) = n^2$ .

Consider now  $1 + 3 + \dots + (2n - 1) + (2n + 1)$  which is the sum of the first  $n + 1$  odd integers. By the induction hypothesis this is  $n^2 + (2n + 1)$  which is  $(n + 1)^2$  and we are done.

**Example** Prove by induction that there are an infinite number of primes.<sup>1</sup> We will let  $P(n)$  be the proposition that there are  $n$  primes. If we can show this is true for all positive integers, then there are an infinite number of primes. The existence of three primes, namely 2, 3, and 5 implies that  $P(1)$ ,  $P(2)$ , and  $P(3)$  are all true. Now assume the induction hypothesis:  $P(n)$  is true; there are  $n$  primes. Let us denote these  $n$  primes by  $p_1, p_2, \dots, p_n$ . Consider the quantity  $x = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1$ . Upon division by any of the primes  $p_1, p_2, \dots, p_n$  there is the remainder 1. Accepting the (non-trivial) proposition that every integer greater than one has at least one prime factor,  $x$  must have a prime factor other than  $p_1, p_2, \dots, p_n$ . This means there are  $n + 1$  primes and  $P(n + 1)$  is true.

**Example** Let us concentrate for the moment on undirected graphs. A spanning tree of a graph  $G$ , is a tree that contains all of the vertices of  $G$ . Prove by induction that every connected graph with  $n$  vertices has a spanning tree with  $n - 1$  edges. If you consider graphs with one and two vertices you can see that  $P(1)$  and  $P(2)$  indeed hold. Assuming that the proposition holds for  $n$  vertices, we want to show that it holds for  $n + 1$  vertices. Suppose that we have a connected graph of  $n + 1$  vertices. Choose an arbitrary vertex  $v_1$ . Since the graph is connected, there must be at least one arc connecting  $v_1$  to some other vertex,  $v_2$ . Similarly, another vertex  $v_3$  can be joined to  $v_1$  and  $v_2$  so that the resulting graph is connected. We continue in this

---

<sup>1</sup>This proof is a variation on the very famous proof by contradiction of Euclid. Euclid's proof is interesting in that it is still rigorous and also it is both an existence proof and a constructive proof.

fashion until we have a connected graph,  $H$ , containing  $n$  vertices and there is a left over vertex  $v$ . Since  $H$  has  $n$  vertices, we know by the induction hypothesis that it has a spanning tree  $T$ . Since  $G$  is connected, there must be at least one arc connecting  $v$  to  $H$ . We pick a single such arc and join it and  $v$  to the tree  $T$ . The resultant graph contains all the vertices of  $G$ . It is a tree because the arc joined to the tree  $T$  only had one end vertex in  $T$ . Hence we have a spanning tree of  $G$ . By the induction hypothesis,  $H$  had  $n-1$  arcs. Hence the new tree has  $n+1-1 = n$  arcs, which is what we needed to show.

## Variations on Induction

Here are two variations of the principle of induction. Both are equivalent to the induction principle as given above which we will call *standard induction*.

### Induction Variation One

Suppose the proposition  $P$  is shown to be true for 1. That is,  $P(1)$  holds. Suppose further that it can be shown that for an arbitrary positive integer  $n$  that if  $P(1), P(2), P(3)$  through  $P(n)$  hold then  $P(n+1)$  holds. Then  $P$  is true for all positive integers. This principle is equivalent to standard induction. To see this, consider the proposition  $Q$ , where  $Q$  is true for  $n$  if  $P$  is true for 1 through  $n$ .  $P(n)$  is true for all integers if and only if  $Q(n)$  is true for all integers. But applying the (standard) principle of induction to  $Q$  is equivalent to using the principle just given.

### Induction Variation Two

Let  $k$  be an arbitrary integer (positive, negative or zero). Suppose that  $P(k)$  holds. Suppose further that it can be shown that for an arbitrary integer,  $n$ , greater than  $k$ , that if  $P(n)$  holds then so does  $P(n+1)$ , then  $P$  is true for all integers greater than or equal to  $k$ . The proof of this proposition is very simple and deserves thought. Take proposition  $P$  which is to be shown to be true for integers  $\geq k$  and replace it by proposition  $Q$  where  $Q(i)$  is defined to be  $P(i + k - 1)$ . Then  $Q(1)$  is the same proposition as  $P(k)$  and  $Q(2)$  is the same as  $P(k + 1)$ . Hence to prove  $P$  is

true for all integers starting with  $k$ , is the same as proving that  $P$  is true for all integers starting with 1.

□ **Exercise 1** Prove by induction that  $1 + 2 + 3 + \dots + n = \frac{n+1}{2}$ . Note that one of the

most celebrated proofs in mathematics is Gauss's childhood non-inductive proof. He wrote "1+2+...+n" twice; the second time underneath and in the opposite order. Adding column-wise he got  $n$  pairs of "n+1." (Actually in that case  $n = 100$ .)

□ **Exercise 2** Prove by induction  $1^3 + 2^3 + 3^3 + \dots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$

The finite geometric series is so important that later it gets a whole section and other proofs. It is:  $1 + x + x^2 + x^3 + \dots + x^n = \frac{1 - x^{n+1}}{1 - x}; x \neq 1$

□ **Exercise 3** Prove, by induction, the finite geometric formula just given.

□ **Exercise 4** If  $G$  is a connected graph with  $v$  vertices and  $a$  arcs then  $v \leq a+1$ . Prove this by induction.

## An Algorithm For Card Shuffling

In the section on the Chinese Remainder Theorem we address the problem of how to assign card values to the numbers 0 through 51 (or 1 through 52). A tougher problem is how to put those numbers in a random order, by which we mean to order the numbers in a way such that any sequence is equally likely as any other sequence. The algorithm below tells you how to randomize the integers 1 through  $n$ . The variables  $x_1$  through  $x_n$  are basically place-holders. In an actual program they would be an array with the  $i$ 'th element denoted something like this:  $X[i]$ .

### Shuffle Algorithm

- Input integer  $n > 0$ ; input variables  $x_1, x_2, \dots, x_n$
- For each  $i$ , set  $x_i \leftarrow i$
- Set  $k \leftarrow n$
- While  $k > 1$ 
  - Choose an integer,  $i$ , randomly (uniformly random) from the interval 1 to  $k$ .
  - $x_i \leftrightarrow x_k$  (exchange  $x_i$  and  $x_k$ )
  - $k \leftarrow k - 1$

The algorithm terminates because eventually  $k$  reaches 1. The algorithm initializes  $x_1$  through  $x_n$  as 1 through  $n$ . Clearly, the numbers are then mixed. What we need to prove is that when the algorithm terminates, each sequence of the numbers 1 through  $n$  is equally likely to occur. The proof is by induction. However, the proof also uses probabilities and conditional probability. These topics will be covered later and you might come back to it then.

### The Proof

If  $n = 1$  there is nothing to prove. If  $n = 2$ , there is a .5 probability that 2 is exchanged with 1. This means that each of the two possible orderings have the same probability. Now assume that the theorem is true for positive integers up to a specific  $n$ . We must show that it

follows that the theorem must be true for  $n + 1$ . If we apply the theorem to  $n + 1$  elements, each

element has the same probability,  $\frac{1}{n + 1}$ , of being stored in  $x_{n+1}$ . After that the algorithm reduces

to the same algorithm applied to the remaining  $n$  variables,  $x_1, x_2, \dots, x_n$ . Each element has a

probability of  $\frac{n}{n + 1}$  of not being stored in  $x_{n+1}$ . By the induction hypothesis these elements then

each have equal probabilities,  $\frac{1}{n}$ , of being in the positions  $x_1$  through  $x_n$ . That means each

element has from the beginning a probability of  $\frac{n}{n + 1} \cdot \frac{1}{n} = \frac{1}{n + 1}$  of being in each of the variables

$x_1$  through  $x_n$ . This is the same probability each element has of winding up in  $x_{n+1}$  and we are done.

1. It is easy to see that the formula is true for  $n = 1, 2,$  and  $3$ . Assume the formula holds for  $n$ . Consider  $1 + 2 + 3 + \dots + n + (n + 1)$ . By the induction hypothesis this is  $\frac{n(n+1)}{2} + (n + 1)$ . This is equal to  $\frac{(n+1)(n+2)}{2}$ , and we are done.
2. It is easy to see that the formula is true for  $n = 1, 2,$  and  $3$ . Assume the formula holds for  $n$ . Consider  $1^3 + 2^3 + 3^3 + \dots + n^3 + (n + 1)^3$ . By the induction hypothesis this is  $\left(\frac{n(n+1)}{2}\right)^2 + (n + 1)^3$ . This is equal to  $\left(\frac{(n+1)(n+2)}{2}\right)^2$ , and we are done.
3. The formula clearly holds for  $n = 1, 2,$  and  $3$ . (Remember, technically it is only necessary to check  $n = 1$ .) Assume that the formula holds for an arbitrary  $n$ . Consider  $1 + x + x^2 + x^3 + \dots + x^n + x^{n+1}$ . By the induction hypothesis, this is equal to  $\frac{1-x^{n+1}}{1-x} + x^{n+1}$ . This is equal to  $\frac{1-x^{n+2}}{1-x}$  and we are done.
4. We will consider graphs without loops. (Remember, a loop is an arc from a vertex to itself.) If the statement is true for graphs without loops it is true for graphs with loops because it only adds to the right side of the inequality. Convince yourself that the formula holds for the trivial cases where  $v = 1, 2,$  and  $3$ . Assume that the hypothesis holds for  $v = n$  (and smaller). Consider a graph (without loops) with  $n+1$  vertices. Pick an arbitrary vertex,  $u$ . Since the graph is connected,  $u$  is connected to other vertices by  $k \geq 1$  arcs. The rest of the Graph is left in one or more connected components. Since each component has  $n$  or fewer vertices, the induction hypothesis holds. If we have  $r$  such components, then we have  $r$  (disjoint) sets of vertices and  $r$  (disjoint) sets of arcs. For each set we have the inequality  $v_i \leq a_i + 1$ . Adding these inequalities together, we get  $v \leq a + 1$  for all of the graph except for  $u$  and the arcs connecting it to the rest of the graph. When we do the entire graph, we add 1 to the left side of the inequality. But since the graph is connected we have at least 1 arc to add to the right side. Hence we maintain the inequality and we have established that it holds for  $v = n+1$ .