

Mathematical Induction

The Principle of Mathematical Induction is a very powerful tool in proving certain theorems. How powerful? Which theorems? I'm glad you asked.

Suppose you wanted to show that a certain fact was true for every natural number. Since there are quite a few such numbers, handling this case by case could take a long time. However, mathematical induction can do this efficiently. That makes it a very powerful theorem-proving technique. But if you were trying to prove something is true for every *real* number, induction would be useless. Essentially, this method is useful when proving something is true for a countable set (such as the natural numbers). [A set is **countable** if there is a one-to-one correspondence with the set of natural numbers. We'll examine this topic more later if we have time.]

Now, suppose again you wanted to show that a certain fact was true for every natural number. Here is the basic idea of Mathematical Induction. Rather than show the property holds for every number individually, we only need to show two things: (1) show that the proposition is true for  $n = 1$ , and (2) show that *if* it is true for some number  $k$ , it must be true for the next number  $k + 1$ . These two facts together show – like dominoes falling – that the statement is true for all natural numbers. Since it was true for  $n = 1$  it must also be true for  $n = 2$ . But since it is true for  $n = 2$  it must also be true for  $n = 3$ . But then it must also be true for  $n = 4$ , and  $n = 5$ , and so on.

**Theorem 1 (Principle of Mathematical Induction):** If  $S$  is a set of natural numbers for which (1)  $1 \in S$  and (2)  $k \in S$  implies  $k + 1 \in S$ , then  $S = \mathbb{N}$ .

Steps for Mathematical Induction

Let  $P(x)$  be a statement dependent on  $x$ . To show  $P(x)$  is true for all natural numbers:

1. Show  $P(1)$  is true.
2. Assume  $P(k)$  is true for some  $k \in \mathbb{N}$ .
3. Show  $P(k + 1)$  is true.

Let's see a few examples.

**Example 1:** Prove that  $\sum_{i=1}^n i = \frac{n(n+1)}{2}$  for all  $n$ .

[This is a rather famous formula and there is an amusing anecdote involving it. The story revolves around Carl Gauss, the “Prince of Mathematicians.” In 1787, at the age of 10, Carl’s arithmetic class was apparently giving his teacher fits. The teacher, in an effort to keep the children busy for a few hours, instructed the students to add the numbers from 1 to 100. The precocious Carl scribbled away for a few moments on his slate, and then turned it over and crossed his arms in satisfaction. The teacher was not amused, but was quite impressed to see what young Carl had done. He had written out the sum to be added two times, once as  $1 + 2 + 3 + \dots + 98 + 99 + 100$  and once as  $100 + 99 + 98 + \dots + 3 + 2 + 1$ . He wrote these two sums one above the other so he could then add numbers in pairs vertically,  $1 + 100$ ,  $2 + 99$ ,  $3 + 98$ , and so on. Since there were 100 such sums, and they all added to 101, Carl knew that this total sum was  $100 \cdot 101 = 10,100$ . But of course this was twice what the teacher had instructed him to find, so he easily divided by two in order to find the requested sum. Carl Gauss has many wonderful stories about his genius, and is widely considered one of the three greatest mathematicians of all time (along with Archimedes and Sir Isaac Newton). Now on to the proof.]

**Proof:** For  $n = 1$  the equation is true since  $\sum_{i=1}^1 i = 1$ . Now suppose it is true

for some natural number  $k$ . So  $\sum_{i=1}^k i = \frac{k(k+1)}{2}$ . We need to show that the

equation must then also hold for  $k + 1$ . In other words, we need to show that

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


If we expand the sum

$$\sum_{i=1}^{k+1} i = 1 + 2 + 3 + \cdots + (k-1) + k + (k+1),$$

and then group the first  $k$  terms, we get

$$\sum_{i=1}^{k+1} i = [1 + 2 + 3 + \cdots + (k-1) + k] + (k+1).$$

By assumption, the first  $k$  terms can be replaced by  $\frac{k(k+1)}{2}$ . So we have,

$$\sum_{i=1}^{k+1} i = [1 + 2 + 3 + \cdots + (k-1) + k] + (k+1) = \frac{k(k+1)}{2} + (k+1).$$


We can then simplify the expressions on the right side of that equation to get the desired result.

$$\frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)}{2} + \frac{2(k+1)}{2} = \frac{k^2 + 3k + 2}{2} = \frac{(k+1)(k+2)}{2}.$$

If the proposition under consideration is not “for all natural numbers”, you should not start at  $n = 1$ . You should always begin with the first “relevant case.” For example, if the proposition you are proving is for all natural numbers  $n \geq 4$ , then start with  $n = 4$ . Identifying the initial case seems trivial, and in fact often is, but it is vitally important. Ignoring the initial case, or starting with an incorrect number can yield incorrect results. We’ll get to more about this in a moment, but first let me illustrate the problem with an example.

**Example 2:** I will “prove” that every horse has the same color.

**“Proof”:** To prove this, I will show that in any set of  $n$  horses, they all have the same color. First consider a set of one horse. Clearly it has the same color as itself. Now assume that in any set of  $k$  horses, they all have the same color. I need to show this is also true for sets of  $k + 1$  horses. Suppose I have  $k + 1$  horses in some order. If I remove the first horse, the remaining  $k$  horses must have the same color as each other (by

assumption). The same is true if I remove the last horse instead. But notice that the first set contains the last horse, and the second set contains the first horse. However, since there is overlap, all  $k + 1$  horses must have the same color. So by induction, all horses have the same color.

If you've ever seen a black horse and a white horse, you know something is wrong here. What is it?

**Example 3:** Prove that  $n! \leq n^n$  for all natural numbers.

**Proof:** For  $n = 1$ , the statement is true since  $1! \leq 1^1$ . Now we assume that  $k! \leq k^k$  for some natural number  $k$ . Consider  $k + 1$ .

$$(k + 1)! = (k + 1) \cdot k! \leq (k + 1) \cdot k^k \leq (k + 1) \cdot (k + 1)^k = (k + 1)^{k+1}.$$

Now we come to other principles of induction. These are equivalent to the original, but they work better in certain circumstances.

**Theorem 2 (Extended Principle of Mathematical Induction):** Let  $N \in \mathbb{N}$ . If  $S$  is a set of natural numbers for which (1)  $N \in S$  and (2) if  $k \geq N$  and  $k \in S$ , then  $k + 1 \in S$ , then  $\{n \in \mathbb{N} : n \geq N\} \subseteq S$ .

We use this version if we want to show that a certain property holds for all natural numbers  $n \geq N$ .

**Theorem 3 (Second Principle of Mathematical Induction):** If  $S$  is a set of natural numbers for which (1)  $1 \in S$  and (2)  $\{1, 2, 3, \dots, k\} \subseteq S$  implies  $k + 1 \in S$ , then  $S = \mathbb{N}$ .

This goes back to showing that a property is true for all natural numbers, but in this version, we don't just assume that the property holds for *some*  $k$ , but rather for *every number up to*  $k$ . It's equivalent, but in some cases, more helpful. You can even combine both these theorems together and form the "Extended Second Principle of Mathematical Induction"...sort a catch-all for induction problems.

**Example 4:** Prove that for all  $n \geq 5$ ,  $n^2 < 2^n$ .

**Proof:** Let  $n = 5$ . Since  $5^2 < 2^5$ , we see the property holds for the initial case. Now assume that  $k^2 < 2^k$  for some  $k$ . Consider  $k + 1$ .

$$(k + 1)^2 = k^2 + 2k + 1 < k^2 + 2k + 2k = k^2 + 4k < k^2 + k^2 < 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$$

**Example 5:** Prove that every natural number greater than or equal to 6 can be written as the sum of natural numbers, each of which is a 2 or a 5.

**Proof:** Since  $6 = 2 + 2 + 2$ , the initial case holds. (For completeness, note that  $7 = 2 + 5$ , so the property holds for 7 also.) Now let  $k \geq 7$  and assume that every natural number from 6 to  $k$  (inclusive) can be written as the sum of 2's and 5's. Consider  $k + 1$ . We can rewrite  $k + 1$  as  $(k - 1) + 2$ . By our inductive hypothesis, we can write  $k - 1$  as a sum of 2's and 5's. Let's say  $k - 1 = 2m + 5n$  for some  $m, n \in \mathbb{N}$ . Then  $k + 1 = 2(m + 1) + 5n$  and the property holds.

Notice that we used the Extended Second principle on this last example. I also want to point out why we needed to verify the property held for 7. If we only verified it by hand for  $n = 6$ , there would be no guarantee that the property held for the previous number. The "initial case" had to include both 6 and 7 so that we could refer to  $k - 1$  in our proof.

**Theorem 4 (Least Natural Number Principle):** Every non-empty set of natural numbers has a least element.

**Proof:** Let  $T$  be a set of natural numbers with no least element. Define  $S = \{n \in \mathbb{N} : \{1, 2, \dots, n\} \subseteq T\}$ . Since  $T$  has no least element,  $1 \notin T$ . So  $1 \notin S$ . Now suppose that  $k \in S$ . We'll show that  $k + 1 \in S$  also. Since  $k \in S$ ,  $\{1, 2, \dots, k\} \subseteq T$ . Now if  $k + 1 \in T$ , then it would be the least element of  $T$ , which is impossible. So  $k + 1 \notin T$ , which means that  $k + 1 \notin S$ . Therefore, by induction  $S = \emptyset$ . Hence  $T = \emptyset$ .

**Example 6:** Every natural number greater than 1 is either a prime number or the product of primes.

**Proof:** Define  $S$  to be the set of all natural numbers that are not prime and are not the product of primes. Assume  $S$  is non-empty. (We'll prove this by contradiction.) By the Least Natural Number Principle this set must have a least element; let's call it  $N$ . Since  $N$  is not prime, it must have non-trivial factors; call them  $a$  and  $b$ . So  $1 < a < N$ ,  $1 < b < N$ , and  $N = ab$ . Since  $a$  and  $b$  are less than  $N$ , they are not elements of  $S$  (recall that  $N$  was the least element). So  $a$  and  $b$  are either prime numbers or product of primes, in either case, this contradicts the fact that  $N$  is not the product of primes. Therefore, the set  $S$  must be empty, and every natural number greater than 1 is a prime or the product of primes.