

Proof by Mathematical Induction

The concept of proof by mathematical induction (sometimes abbreviated as “proof by induction”) is connected to both mathematics and computer science. Proof by mathematical induction is an elegant and powerful way of proving that a proposition holds (or is true) for all natural numbers.

The set of natural numbers is the set $\{1, 2, 3, \dots\}$ – the set of non-negative whole numbers (integers). Sometimes 0 is included, in which case the set of natural numbers is taken to mean the set $\{0, 1, 2, 3, \dots\}$. This leeway in terminology will not affect us; the idea behind proof by induction is the same in either case. In this handout we will use the first definition of natural numbers.

Suppose you are asked to prove that something –some proposition– is true for all natural numbers. For example, you are asked to show that no matter what the natural number n is, the sum of the first n natural numbers is $n(n+1)/2$. [If n is 5, this says that the sum of the first five integers is 5 times 6 divided by 2. To check: $1 + 2 + 3 + 4 + 5 = 15$, and $5*6/2 = 15$, so the formula works for $n = 5$.]

How do we proceed?

One method is to try verifying this formula for all natural numbers individually, starting from 1. To do this we would say “The sum of the first 1 numbers is 1, and $1*2/2 = 1$, so it works for 1. Secondly, the sum of the first 2 numbers is $1+2=3$, and $2*3/2=3$, so this formula also holds for 2. Thirdly, the sum of the first 3 numbers is...” We can see that this method will work but not be practical because what we’re asked to show is the truth of the proposition for ALL natural numbers – an infinitely large set. If we continued this way, we’d never finish.

The idea behind proof by induction is this. We want to show that a proposition is true for all natural numbers. Suppose we could show that (1) whenever this proposition is true for a natural number m , then it has to be true for the next bigger natural number, $m+1$. And then suppose we showed that (2) the proposition is true for the very first natural number, 1. Then we’d be done!

If we proved those two things, we can reason as follows. It works for the natural number 1. We’ve shown that whenever it works for a natural number, it works for the next bigger natural number. That means that it must hold for the number 2. That means that it must hold for the number 3 and, by the same logic, for every natural number. We’d be finished.



That is the method of proof by induction. We prove that if a formula holds for a natural number, then it must hold for the next bigger natural number. And we verify that it works for the first natural number by hand, with an individual, and usually simple, calculation.

Let's see how this works for the above example. This example illustrates the idea of proof by induction in particular, but it also sheds light on the more general concept of what is meant by a "mathematical proof."

Prove that the sum of the first n natural numbers is $n(n+1)/2$.

We shall use proof by induction. First let's verify this formula for the first natural number, 1. This is known as the "base case." Let's do it: what is the sum of the first 1 natural numbers? The answer is 1. And what does the formula say the sum of the first 1 natural number should be? It says it should be $1(1+1)/2$, or 1. That was trivially easy.

Next we'll do what's known as the inductive step, which is a way of saying that we'll show that whenever this formula holds for any natural number, it must hold for the next bigger natural number. Here's how we do that: **assume** that this proposition (or formula) holds for a given number i . So, we assume that $1 + 2 + 3 + \dots + i = i(i+1)/2$. This is known as the "inductive hypothesis." Assuming this holds, we must prove that this formula must work for the next bigger natural number, $i+1$. In other words, we must show that the sum of the first $i+1$ natural numbers is $(i+1)(i+2)/2$, or that $1 + 2 + \dots + i + (i+1) = (i+1)(i+2)/2$.

We don't know yet that this must be true. We assume that the formula we're trying to prove holds for the first i numbers, but we are not assuming that it holds for the first $i+1$ numbers. To prove that it does, we have to make use of the inductive hypothesis. By the inductive hypothesis, $1 + 2 + \dots + i + (i+1) = i(i+1)/2 + (i+1)$. [We've used the fact that the sum of the first i natural numbers is $i(i+1)/2$.] Next, we need to see if we can change the right hand side of this equation, $i(i+1)/2 + (i+1)$, into the desired form, $(i+1)(i+2)/2$. With some algebra, $i(i+1)/2 + (i+1) = i(i+1)/2 + 2(i+1)/2 = (i^2 + i + 2i + 2)/2$ becomes $(i^2 + 3i + 2)/2 = (i+1)(i+2)/2$, which is what we wanted. So we've shown that whenever this formula works for (an arbitrary) natural number i , it must work for the next bigger natural number $i+1$.

We're done. We've shown that our proposition holds for 1, and that whenever it holds for a number, it must hold for the next bigger number.

This same idea can be extended to more complicated problems.

The key step is **assuming** that the proposition holds for an arbitrary natural number n , and then **proving** that it must follow that the proposition holds for the next bigger natural number, $n+1$. Also show that the proposition holds for the first natural number. Notice the subtlety in this argument. The idea of proof by mathematical induction is important not only in mathematics, but also in computer science. It is often used to verify the correctness of recursive computer programs.