Introduction to Mathematical Induction

One of the most important tasks in mathematics is to discover and characterize regular patterns or sequences. The main mathematical tool we use to prove statements about sequences is induction. Induction is a very important tool in computer science for several reasons, one of which is the fact that a characteristic of most programs is repetition of a sequence of statements.

To illustrate how induction works, imagine that you are climbing an infinitely high ladder. How do you know whether you will be able to reach an arbitrarily high rung? Suppose you make the following two assertions about your climbing abilities:

1) I can definitely reach the first rung.
2) Once I get to any rung, I can always climb to the next one up.

If both statements are true, then by statement 1 you can get to the first one, and by statement 2, you can get to the second. By statement 2 again, you can get to the third, and fourth, etc. Therefore, you can climb as high as you wish. Notice that both of these assertions are necessary for you to get anywhere on the ladder. If only statement 1 is true, you have no guarantee of getting beyond the first rung. If only statement 2 is true, you may never be able to get started.

Assume that the rungs of the ladder are numbered with the positive integers (1,2,3...). Now think of a specific property that a number might have. Instead of "reaching an arbitrarily high rung", we can talk about an arbitrary positive integer having that property. We will use the shorthand P(n) to denote the positive integer n having property P. How can we use the ladder-climbing technique to prove that P(n) is true for all positive n? The two assertions we need to prove are:

1) P(1) is true
2) for any positive k, if P(k) is true, then P(k+1) is true

Assertion 1 means we must show the property is true for 1; assertion 2 means that if any number has property P then so does the next number. If we can prove both of these statements, then P(n) holds for all positive integers, just as you could climb to an arbitrary rung of the ladder.

The foundation for arguments of this type is the **Principle of Mathematical Induction**, which can be used as a proof technique on statements that have a particular form. We can state it this way:

> A proof by mathematical induction that a proposition P(n) is true for every positive integer n consists of two steps:
>
> BASE CASE: Show that the proposition P(1) is true.
>
> INDUCTIVE STEP: Assume that P(k) is true for an arbitrarily chosen positive integer k, and show that under that assumption, P(k+1) must be true.
>
> From these two steps we conclude (by the principle of mathematical induction) that for all positive integers n, P(n) is true.

Note that we do not *prove* that P(k) is true (except for k = 1). Instead, we show that ***if*** P(k) is true, then P(k+1) must also be true. That's all that is necessary according to the Principle of Mathematical Induction. The assumption that P(k) is true is called the **induction hypothesis.** Be sure you understand that P(n) and P(k) are not numbers; they are propositions that are true or false.

As an another illustration, consider an infinite number of dominoes positioned one behind the other in such a way that if any given one falls, then the one behind it falls too. In order to establish that the entire chain will fall under a certain set of circumstances, two things are necessary. First, someone has to push over the first domino; this corresponds to the base case of induction. Second, we must also know that whenever any domino falls, it is close enough to the next domino in the chain that it will knock it over. This requirement can be expressed by saying that whenever domino N falls, so does N+1. This corresponds to using the induction hypothesis to establish the result for the next value of N. If you ever get confused about induction, the "domino principle" is a good thing to remember.

Example 1: Suppose that great, great, great.... grandpa Fred married and had two children. Call this generation 1, so generation 1 contains the offspring of Fred (2). Each of these children have two children, so generation 2 has four offspring. Each of these 4 has two children so at generation 3, we have 8 offspring. This continues, without fail, for generation to generation. It appears that generation n will have 2^n offspring. Let P(n) be the assertion that generation n has 2^n offspring. We can use induction to *prove* that P(n) holds for all n.

PROOF:

BASE CASE: P(1) asserts that generation 1 has 2^1 offspring, which is true since we are told that Fred had two children.

INDUCTIVE STEP: We assume that for an arbitrary integer k, P(k) is true, i.e., that generation k has 2^k offspring. We need to show that generation k+1 has 2^{k+1} offspring.

By the rules of this family, each offspring is required to have 2 children, thus the number of offspring at generation k+1 will be twice the number of generation k. By the inductive hypothesis, generation k has 2^k offspring, so :

generation k+1 has $2(2^k) = 2^{(k+1)}$ offspring, i.e., P(k+1) is true.

Thus P(k+1) is true if P(k) is true, and therefore P(n) is true for all natural numbers.

Example 2: Prove that for every positive integer n, the sum of the first n positive integers is n(n+1)/2. This is the *classic* example of an inductive proof, and we will present it in a slightly more formal style than the example above. Note that to begin the inductive step, we state the inductive hypothesis by writing out the meaning of P(k), then we state what is to be proved based on that hypothesis, P(k+1). We obtain P(k+1) by substituting k+1 for k in P(k). Writing out P(k+1) at this point will often show you what is needed in the proof. *Note: Our first example was somewhat informal; this time we will show you exactly how inductive proofs should be written.*

Theorem. The following proposition is true for all positive integers:

$$P(n): \ 1+2+3+....+n = \frac{n(n+1)}{2}$$

BASE CASE: P(1) asserts that

$$1 = \frac{1(1+1)}{2} = 1, \text{ which is true.}$$

INDUCTIVE STEP:

Assume for some integer k, $P(k): \ 1+2+3+...+k = \frac{k(k+1)}{2}$

Show: $P(k+1): \ 1+2+3+...+(k+1) = \frac{(k+1)\,((k+1)+1)}{2}$

Proof of the Inductive Step:

By the induction hypothesis, we already have a formula for the first k integers. So, a formula for the first (k+1) integers may be found by simply adding (k+1) to both sides of the induction hypothesis, and simplifying:

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

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

$$= \frac{k^2 + 3k + 2}{2}$$

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

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

Thus P(k+1) is true when P(k) is true, and therefore P(n) is true for all natural numbers.

Steps to doing an inductive proof:

1) state the theorem, which is the proposition P(n)
2) show that P(base case) is true
3) state the inductive hypothesis (substitute k for n)
4) state what must be proven (substitute k+1 for n)
5) state that you are beginning your proof of the inductive step, and proceed to manipulate the inductive hypothesis (which we assume is true) to find a link between the inductive hypothesis and the statement to be proven. Always state explicitly where you are invoking the inductive hypothesis.
6) Always finish your proof with something like: P(k+1) is true when P(k) is true, and therefore P(n) is true for all natural numbers.

NOTE: On problem sets and exams, it is important to present your proof in the proper form. You must *always* write out steps 1-6 as shown above. Form is important in inductive proofs.

Example 3: P(n) denotes $1 + 3 + 5 + ... + (2n-1) = n^2$, i.e., the sum of the first n odd integers is n^2. Show that P(n) is true for all positive integers n.

BASE CASE: P(1) asserts that $1 = 1^2 = 1$, which is true.

INDUCTIVE STEP:

Assume P(k): $1 + 3 + 5 + ... + (2k-1) = k^2$
Show P(k+1): $1 + 3 + 5 + ... + (2k-1) + (2k+1) = (k+1)^2$

Proof of the Inductive Step:

We form the sum of the first k+1 odd integers by adding the next odd integer to the sum of the first k. Doing this on both sides of the induction hypothesis gives:

$$\begin{aligned} 1 + 3 + 5 + ... + (2k-1) + (2k+1) &= k^2 + (2k+1) \\ &= k^2 + 2k + 1 \\ &= (k+1)^2 \end{aligned}$$

Thus P(k+1) is true when P(k) is true, and therefore P(n) is true for all natural numbers.

The following example illustrates that the basis of induction does not have to be 1:

Example 4: P(n) denotes $1 + 2 + 2^2 + ... + 2^n = 2^{n+1} - 1$. Show that this is true for all nonnegative integers (this includes 0).

BASE CASE: P(0) asserts that $2^0 = 2^1 - 1 = 1$, which is true.

INDUCTIVE STEP:

Assume P(k): $1 + 2 + 2^2 + ... + 2^k = 2^{k+1} - 1$
Show P(k+1): $1 + 2 + 2^2 + ... + 2^k + 2^{k+1} = 2^{((k+1)+1)} - 1 = 2^{k+2} - 1$

Proof of the Inductive Step:

We begin by adding 2^{k+1} to both sides of the inductive hypothesis:

$(1 + 2 + 2^2 + ... + 2^k) + 2^{k+1} = (2^{k+1} - 1) + 2^{k+1}$

$= (2 * 2^{k+1}) - 1$ factoring

$= 2^{k+2} - 1$ exponent defin

Thus P(k+1) is true when P(k) is true, and therefore P(n) is true for all nonnegative numbers.

Here is an example with two variables (but only one induction variable). It is important in such cases to state which variable you are doing the induction on.

Example 5: P(n) denotes that for any real number $r \neq 1$ and any integer $n >= 0$,

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}$$ We will prove this by induction on n.

BASE CASE: P(0) asserts that $r^0 = \frac{r^{0+1} - 1}{r - 1} = 1$, which is true.

INDUCTIVE STEP:

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

Show P(k+1): $\sum_{i=0}^{k+1} r^i = \frac{r^{k+2} - 1}{r - 1}$

Proof of the Inductive Step:

Adding to both sides of the induction hypothesis, we have

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

:

$$\sum_{i=0}^{k+1} r^i = \frac{r^{k+1} - 1 + r^{k+1}(r - 1)}{r - 1}$$

$$= \frac{r^{k+1} - 1 + r^{k+2} - r^{k+1}}{r - 1}$$

$$= \frac{r^{k+2} - 1}{r - 1}$$

P(k+1) is true when P(k) is true, and therefore P(n) is true for all natural numbers.

Thus far, we have been using **weak** induction in our proofs. There is a variation called **strong** induction. Rather than assume that P(k) is true to prove that P(k+1) is true, we assume that P(i) is true for all i where the (basis of induction) $\leq i \leq k$. From this assumption, we prove P(k+1). It's stronger in the sense that we are allowed to come to the same conclusion while assuming more, but the assumption is a natural one based on our understanding of weak induction. In fact, weak induction and strong induction are equivalent. That is, assuming either one is a valid rule of inference, we can show that the other is.

Strong or Complete Induction:
BASE CASE: Prove P(base) is true
INDUCTION: Assume P(base), P(base+1)...P(k) are true, and prove that P(k+1) is true.

Example 6: P(n) denotes that all positive integers $n > 1$ are either prime or have a prime factorization, i.e., n can be written as the product of primes. (This is the Fundamental Theorem of Arithmetic.)

BASE CASE: P(2) is true since 2 is prime.

INDUCTIVE STEP:

Assume P(i): for all positive integers i where $1 < i \leq k$, i is either prime or has a prime factorization;

Show P(k+1): k+1 is prime or has a prime factorization.

Proof of the Inductive Step:

If k+1 is a prime, then we are done. If k+1 is not a prime, then by the definition of primality, it must be true that for some a and b, a b = k+1. Clearly, $a \leq k$ and $b \leq k$. By the inductive hypothesis, both a and b have a prime factorization too. Thus k+1 is the product

of the prime factors of a multiplied by the prime factors of b, proving that k+1 has a prime factorization.

P(k+1) is true when P(i) is true for $i \leq k$, and therefore P(n) is true for all natural numbers.

Strong induction is often used to prove that a sequence of numbers has a particular property.

Example 7: A jigsaw puzzle consists of a number of pieces. Two or more pieces with matched boundaries can be put together to form a "big" piece. To be more precise, we use the term *block* to refer to either a single piece or a number of pieces with matched boundaries that are put together to form a "big" piece. Thus, we can simply say that blocks with matched boundaries can be put together to form another block. Finally, when all pieces are put together as one single block, the jigsaw puzzle is solved. Putting 2 blocks together with matched boundaries is called one move. We shall prove (using strong induction) that for a jigsaw puzzle of n pieces, it will always take n-1 moves to solve the puzzle.

BASE CASE: P(1) is true--for a puzzle with 1 piece, it does not take any moves to solve it.

INDUCTIVE STEP:

Assume P(i) where $1 \leq i \leq k$: for a puzzle with i pieces, it takes i-1 moves to solve the puzzle.
Show that for a puzzle with k+1 pieces, it takes k moves to solve the puzzle.

Proof of the Inductive Step:

Consider the puzzle with k+1 pieces. For the last move that produces the solution to the puzzle, we have two blocks: one with n_1 pieces and the other with n_2 pieces, where $n1 + n2 = k + 1$. These two blocks will then be put together to solve the puzzle. According to the induction hypothesis, it took $n1 - 1$ moves to put together the one block, and $n2 - 1$ moves to put together the other block. Including the last move to unite the two blocks, the total number of moves is equal to $[(n1 - 1) + (n2 - 1)] + 1 = (k + 1) - 1 = k$

P(k+1) is true when P(i) is true, where $i \leq k$, and therefore P(n) is true for any puzzle size.

The Well-Ordering Property

The validity of mathematical induction follows from the Well-Ordering Property (WOP), which is a fundamental axiom of number theory. WOP states that every nonempty set of non-negative integers has a least element. This axiom can be used directly in proofs of theorems relating to sets of integers.

You can use WOP to prove that P(n) is true for all positive integers . To do this, you assume that the set of integers S for which P(n) is false is nonempty. By WOP, there would be a smallest positive integer k for which P(k) is false. You then obtain a contradiction, showing that S must be empty. The contradiction is derived from the fact that for positive integer j with $j<k$, P(j) must be true due to the way k was chosen.

Example

Theorem: Every natural number *n* can be written as a product of primes.

Proof: Let S be the set of natural numbers that cannot be written as a product of primes. Then by the Well-Ordering Principle, S has a smallest element, which we will call n. n must not be a prime, because if it was, it could be written as a product on one prime, itself. Thus n = rs for some numbers such that $1 < r, s < n$. Since both r and s are smaller that n, both can be written as products of primes. But that means that n is the product of primes, which is a contradiction. Thus the set S must be empty.

The last topic to discuss concerning induction is:

> *The Law of Bad Proofs:*
>
> You can prove anything you want if your proof is wrong.

In some ways, induction seems like it can prove any property about anything. But you have to watch out for subtle flaws in your thinking. Consider the following:

P(n) denotes that every set of n horses are all the same color.

BASE CASE: prove that P(1) is true. If X is a set of 1 horse, then all the horses in X are the same color.

INDUCTIVE STEP:
Assume P(k) is true: every set of k horses are all the same color.
Show P(k+1): every set of k+1 horses are all the same color.

Proof of the Inductive Step:

Suppose X is a set of k+1 horses. To show that all the horses in X are the same color, it's enough to show that if

h1 is in X and h2 is in X

then h1 is the same color as h2. If we can prove this, we are done because either h1 or h2 is in a set of k horses, and we know that a set of k horses are all the same color.

Let X1 = X - h1 and X2 = X - h2

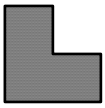
X1 and X2 have k horses and by the inductive hypothesis, the k horses in each of these sets are all the same color. So, if we take a horse z which is a horse in the intersection of X1 and X2 (that being one of the horses that X1 and X2 have in common), we know that h1 must be the same color as z, and h2 must be the same color as z; therefore, h1 is the same color as h2. We have proven that all horses are the same color.

What's wrong with this?

Now another legitimate proof:

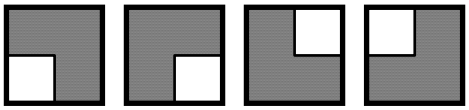
Example 8

Show that any 2^n by 2^n grid can be tiled using "L" shaped pieces (such as the one below) leaving any one square untiled.



Solution: Proof by induction on *n*.

BASE CASE: It is easy to verify the case for $n = 1$ by exhaustively checking all possibilities:



INDUCTIVE STEP:

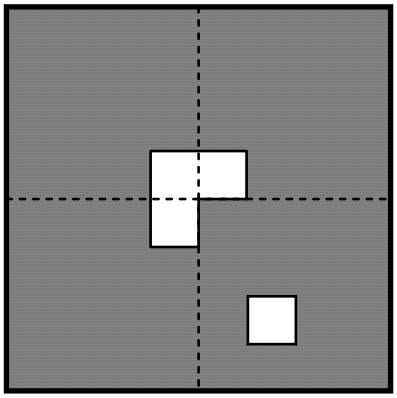
Assume: Any 2^k by 2^k grid can be tiled.

Prove: A 2^{k+1} by 2^{k+1} grid can be tiled as described above.

Proof of the Inductive Step:

We begin with a 2^{k+1} by 2^{k+1} grid. Divide this grid into four sub-grids, each of size 2^k by 2^k. By the inductive hypothesis, each of these grids can be tiled leaving any one square empty.

Tile three of the four sub-grids so that the empty squares are adjacent and form an "L" shaped hole. The fourth sub-grid can be tiled however we please.



Now, simply fill the "L" shaped hole with another tile. Thus a 2^{k+1} by 2^{k+1} grid can be tiled, leaving any one square blank. This completes the proof.

Bibliography

G. Pólya, *Induction and Analogy in Mathematics,* Princeton, NJ: Princeton University Press: 1954.

K. Rosen, *Discrete Mathematics and Its Applications, 5th Ed.*, New York: McGraw-Hill, 2003.

D. Solow, *How to Read and Do Proofs*, New York: Wiley, 1982.

I.S. Sominskii, *Method of Mathematical Induction,* New York: Blaisdell, 1961.

Some Useful Formulas

Here are some formulas for sequences that are great for practicing proofs by induction. You will also find these formulas useful later in 103 when we discuss recursion and recurrence relations. The ones we have proven in this handout are included below.

- $1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$
- $1 + 3 + 5 + ... + (2n-1) = n^2$
- $1 + 2 + 2^2 + ... + 2^n = 2^{n+1} - 1$
- $\sum_{i=0}^{n} r^i = \frac{r^{(n+1)} - 1}{r - 1}$
- $1^2 + 2^2 + 3^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$
- $1^3 + 2^3 + 3^3 + ... + n^3 = [\, n(n+1) / 2]^2$
- $1*2 + 2*3 + ... + n(n+1) = \frac{n(n+1)(n+2)}{3}$
- $1^2 + 3^2 + 5^2 + ... + (2n+1)^2 = \frac{(n+1)(2n+1)(2n+3)}{3}$

Historical Notes

The first known use of mathematical induction was in the work of the 16th-century mathematician Francesco Maurolico (1494-1575). In his book *Arithmeticorum Libri Duo*, he presented a variety of properties of the integers together with proofs of these properties. He used induction to prove some of these properties, the first one being the proof that the sum of the first n odd integers is n^2. The first formal explanation of mathematical induction was presented by Augustus DeMorgan (1806-1871) in 1838. This is also the first time the term "induction" was used in this context.