Induction is a powerful method of proof, often useful in cases where we wish to prove that some statement holds for all values of an integer parameter, n, starting at some smallest value n_0. For example, suppose we wish to prove that $\sum_{i=1}^{n} i = n(n+1)/2$, for all $n \geq 1$. Then n_0 will be 1.

The idea behind induction is to show two things: (i) if the statement ever "gets going" by being true for some n then it "keeps going" by staying true for all larger n (what we might acronymize as SIS (StartsImpliesStays), or Evermore, or ForeverAfter – if it ever Starts to be true then it Stays true forever after); and (ii) that the statement does in fact hold for the smallest value, n_0 (the so-called base case).

For another bit of imagery: it is as if we build a pump (i) that, once it has started, never stops; and (ii) that we can "prime" to get it going at the starting value n_0.

We usually do the "priming" (or base) case first, and then show the SIS or "never stops" part (the so-called inductive step); but this is merely a convention, and as long as we have done both parts then we have shown that the statement holds for all $n \geq n_0$.

It is a bit astonishing that one can ever show the SIS part: how can we be sure that the statement stays true forever after, just from it being true for some particular n? Wouldn't we have to check it for every larger value of n, to be sure? Yes and no. We do check it, but (when the method works) we check it by showing that there is a very nice connection between consecutive cases of n. That is, the SIS or inductive step shows (when it works) that the truth of the statement for a given value of n, say $n = k$ implies its truth for $n = k + 1$. This still seems astonishing; and there are two point to be awawre of here: (i) induction does not always work, and (ii) when it works it is because the statement we are trying to prove is one where there is a special relation between consecutive cases of n.

It is time to stop abstract descriptions, and see some examples.

How would we show, for instance, that $\sum_{i=1}^{n} i = n(n+1)/2$ for all $n \geq 1$?

The forever after part requires us to show that, if the statement (which in this case is an equation) is ever true (for some n, say $n = k$) then it stays true for all larger n. We show this by SUPPOSING it does happen to be true for some k (this is called the inductive hypothesis, or IH):

IH: $\sum_{i=1}^{k} i = k(k+1)/2$

and then (by using this truth, IH, at $n = k$) SHOWING that the statement stays true for the next n, namely $n = k + 1$:

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

This always proceeds by rewriting this new case $(k+1)$ in a way that allows us to apply the previous case (k), which we begin here:

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

$$= (k+1) + k(k+1)/2$$

We are not done; but we have taken the crucial step and the rest is just algebra, to show that the above expression is equal to $(k+1)(k+2)/2$. The crucial step was to rewrite at least some piece of the $(k+1)$ case so that the k case can be applied.

Note that we ASSUME the k case (the IH) – this is the "if it ever starts" part – we do NOT show it. What we do show is that, IF it starts (k) then it CONTINUES $(k+1)$. Of course, we do eventually need to show it really does start somewhere, and that is the base case (n_0). We'll get to that in a moment. Let's first finish that inductive step from where we left off above:

$$= [2(k+1) + k(k+1)]/2$$

$$= [2k + 2 + k^2 + k]/2$$

$$= [k^2 + 3k + 2]/2$$

$$= (k+1)(k+2)/2$$

So we have shown that

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

, assuming

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

This means that the original statement, $\sum_{i=1}^{n} i = n(n+1)/2$, will stay true if it ever can get "going", because once it has become true for some value of n then it will be true for the next value, and since it is then true for that next value, it stay true for the one after that, and so on.

It is essential here that k NOT be taken to be any particular constant value, such as n_0. This is why what we have shown is really "once-true, always-true". The point is that if AT ANY TIME (ie for ANY value of n) the statement should happen to be true, that it will forever remain so after that. We need it to be this general – with truth flowing from ANY $n = k$ where truth might be, to the next $n = k + 1$ – and not just that it flows from $n = n_0$ to $n = n_0 + 1$ since the latter condition would not keep the pump pumping on past $n = n_0 + 1$!

Does it ever "get going" at all? This we quickly settle in our present example (although sometimes it can be the hardest part). The base case here is $n = n_0 = 1$, namely:

$$\sum_{i=1}^{1} i = 1(1+1)/2$$

and this is simply $1 = 1$.

Note that not all (true) statements about integers are best proven via inductions. For instance, it is true that if n is even then n^2 is even. Here we do NOT get any advantage from induction; and a more direct approach works just fine:

Let n be any integer. We will show that if n is even then n^2 is even. Suppose n is even; this means $n = 2 \times k$ for some integer k. So $n^2 = 4k^2 = 2 \times (2k^2)$, so n^2 is twice some integer (which is what it means to be even). [Note: the converse is also true: if n^2 is even then so is n, but it is harder to prove.]

==

There are various versions of induction. The one presented above is sometimes called "ordinary" (or weak) induction. A fancier version called "course-of-values" (or strong) induction is this: we show that if the pump manages to "pump truth" all the way from $n = n_0$ to $n = k$ then it will also "pump truth" at $n = k + 1$. That is, we show truth flows from a historical trend (from n_0 to k) on to the next step $(k+1)$. (We also still need to show the pump can get started, so we still need a base case here.)

The course-of-values version is sometimes easier to use, since to prove the case $n = k+1$ one has a "bigger IH – more hypotheses – to help out (the past course of truths all the way back to n_0 and not just the immediately previous step $n = k$).

For instance one would now be able to assume not only

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

but also all the earlier cases, in trying to show

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

. It turns out that these extra hypotheses don't help us much in this example, so here is another example where course-of-values induction really helps:

Theorem: Every integer n greater than 1 has a factorization into primes.

Proof: The base case is $n = 2$, and indeed 2 has a (trivial) prime factorization, namely itself, since 2 is prime.

Now suppose the statement of the theorem holds whenever $2 \leq n \leq k$. This is our (strong) IH: that all integers greater than 1, up to k, do have a prime factorization. Using this, we want to show the statement holds for $n = k+1$. Now if $k+1$ is prime, we are done. And if it is not prime, then (by definition) it is a product $k+1 = r \times s$ where $2 \leq r, s \leq k$. So by the IH, each of r and s does have a prime factorization. But since $k+1$ is their product, then it has the prime factorization which is the product of the prime factorizations of r and s.

CONSTRUCTIVE INDUCTION

Constructive induction is best learned by example. Here is a typical one:

Suppose we wish to prove that

```
SUM_i=1_to_n  i
```

is a quadratic expression in n, but we don't know exactly which expression. (We do happen to know, in fact, that it is really n(n+1)/2, but let's pretend we don't).

So, we try to prove the SUM above is equal to an^2 + bn + c, where a,b,c are unknown parameters. (In trying, we will find out what values they need to have.) Suppose we try to prove

SUM = an^2 + bn + c

by induction on n, for n > 0. The base case is n=1:

SUM = a + b + c

which becomes

1 = a + b + c

since for n=1, SUM = 1. So, we will have to make sure that in fact a + b + c = 1, so that the base case will go through.

Now we proceed to the inductive step: Assume

IH: SUM = an^2 + bn + c

for some n > 0, and consider SUM_i=1_to_n+1 i. This is

n+1 + SUM_i=1_to_n i

which by IH is

n+1 + an^2 + bn + c

and we want this to be equal to

a(n+1)^2 + b(n+1) + c

Setting these equal and doing some algebra:

n+1 + an^2 + bn + c = a(n+1)^2 + b(n+1) + c

n+1 = 2an + a + b

Notice that c has dropped out, so we can try letting c = 0, to make things simpler; then a + b = 1, since we had above that a + b + c = 1. Then

```
(*)           n+1  =  2an + 1

or
              2an  =  n

                a  =  1/2
and thus

                b  =  1 - a  =  1/2

Therefore

              SUM  =  1/2 n^2 + 1/2 n

and this is the same as

                       n(n+1)
              SUM  =  -------
                          2
```

Thus, WITHOUT KNOWING IN ADVANCE the exact formual for the sum, we were nonetheless able to FIND IT AND PROVE IT simply by guessing, not the exact formula but rather only its general form (quadratic). The method then determined the exact values of the coefficients, as part of the inductive method of proof.

Had we chosen c = 1 instead of c = 0 (perhaps in order to get a + b = 0) then we'd have found n+1 = 2an (instead of n+1 = 2an + 1 as in (*) above). It would follow that a = (n+1)/2n = 1/2 + 1/2n which is not a constant, and thus the choice of c = 1 cannot give us a solution of the desired form. At this point we should then go back and chose another value for c, such as c=0 as we did above. Does this mean that there might still be other solutions that do not have a=constant? Well, once we do find a solution where a-constant, then any other solutions must be equal to that one (even if in a different form), since all solutions must be equal to the original SUM.

Note that if we feel our original guess is too general (too many parameters to worry about) we could have strengthened (and simplified) it at the beginning by a little more computing. For example for n equal to 2, we get the following condition on a, b, and c:

$$1 + 2 = 3 = a\, 2^2 + b\, 2 + c = 4a + 2b + c$$

which gives us, together with $c = 1 - a - b$,

$$2 = 3a + b$$

a relation between only a and b: $b = 2 - 3a$. We then could use, instead of the original guess $an^2 + bn + c$, the more specific guess $an^2 + (2 - 3a)n + (1 - a - (2 - 3a))$, i.e.,

$$SUM = an^2 + (2 - 3a)n + 2a - 1$$

This we can also prove by induction, first the base case and then the inductive step, finding that for the inductive step to work, we need $a = 1/2$ as before.