Proofs by induction: a guide

Advanced Logic
17th September 2022

Recall that if we want to show that every number has a certain property, we can do so by showing that (a) 0 has the property, and (b) for any n, if n has the property, then $\operatorname{suc} n$ has the property.

For example, suppose we want to prove the following, using just the following equations (which follow from the definition of addition):

(A) $$n + 0 = n$$

(B) $$n + \operatorname{suc} m = \operatorname{suc}(n + m)$$

Theorem 1. $0 + n = n$ for any natural number n.

Proof. The property we want to show that every number has is *being a number n such that* $0 + n = n$. So it suffices to show (a) that 0 has this property, i.e. that $0 + 0 = 0$, and (b) that for any number n, if n has this property, then $\operatorname{suc} n$ does too, i.e. that if $0 + n = n$ then $0 + \operatorname{suc} n = \operatorname{suc} n$.

(a) The fact that $0 + 0 = 0$ follows from fact (A).

(b) Let n be an arbitrary number and suppose that $0 + n = n$. By fact (B), $0 + \operatorname{suc} n = \operatorname{suc}(0 + n)$. But by hypothesis, $\operatorname{suc}(0 + n) = \operatorname{suc} n$; hence $0 + \operatorname{suc} n = \operatorname{suc} n$. □

That's a detailed explanation. Since proof by induction is such a common pattern, we'll need a way of stating such proofs succinctly. Like this:

Proof. By induction.

Base case: $0+0 = 0$ by (B).

Induction step: Suppose $0 + n = n$. Then

$$\begin{aligned} 0 + \operatorname{suc} n &= \operatorname{suc}(0 + n) && \text{by fact (B)} \\ &= \operatorname{suc} n && \text{by the induction hypothesis.} \end{aligned}$$ □

Let's turn to another example.

Theorem 2. $(\operatorname{suc} n) + m = \operatorname{suc}(n + m)$ for any natural numbers n, m.

Unlike the previous example, this one involves *multiple* generality: we are trying to show that something is true for every n, for every m. Here there are four different strategies we could adopt.

1. We could let n be an arbitrary natural number; prove by induction that every number has the property *being a number m such that* $(\operatorname{suc} n)+m = \operatorname{suc}(n+m)$; and then conclude that since n was arbitrary, every number n is such that every number m is such that $(\operatorname{suc} n) + m = \operatorname{suc}(n + m)$.

2. We could let m be an arbitrary natural number; prove by induction that every number has the property *being a number n such that* $(\operatorname{suc} n)+m = \operatorname{suc}(n+m)$; and then conclude that since m was arbitrary, every number m is such that every number n is such that $(\operatorname{suc} n) + m = \operatorname{suc}(n + m)$.

3. We could prove by induction that every number has the property *being a number n such that for every number m,* $(\operatorname{suc} n) + m = \operatorname{suc}(n + m)$.

4. We could prove by induction that every number has the property *being a number m such that for every number n,* $(\operatorname{suc} n) + m = \operatorname{suc}(n + m)$.

Options like 3 and 4 are a bit more complicated, since they will require us to prove two different universal claims, one inside the base case and one inside the inductive step. This strategy is only rarely needed; initially, you'll do better to consider strategies like 1 and 2, where you "fix" all but one of the variables in the universal claim you're trying to prove and then use induction.

But this still leaves two possibilities. In the present case, the option that works turns out to be option 1. Here is a proof that implements that option.

Proof. By induction on m.

Base case:

$$\begin{aligned} \operatorname{suc} n + 0 &= \operatorname{suc} n && \text{by fact (A)} \\ &= \operatorname{suc}(n + 0) && \text{by fact (A) again} \end{aligned}$$

Induction step: Suppose $(\operatorname{suc} n) + m = \operatorname{suc}(n + m)$. Then

$$\begin{aligned} (\operatorname{suc} n) + \operatorname{suc} m &= \operatorname{suc}(\operatorname{suc} n + m) && \text{by fact (B)} \\ &= \operatorname{suc}(\operatorname{suc}(n + m)) && \text{by the IH} \\ &= \operatorname{suc}(n + \operatorname{suc} m) && \text{by fact (B).} \end{aligned}$$ □

Here, 'By induction on n' is short for something like the following: 'Let m be an arbitrary natural number. We will prove by induction that every natural number has the property *being a number n such that* $(\operatorname{suc} n) + m = \operatorname{suc}(n + m)$, and conclude from that that for every m and n, $(\operatorname{suc} n) + m = \operatorname{suc}(n + m)$.'

What would have happened if we instead tried strategy 2? Then our base case would require proving that $\operatorname{suc} 0 + m = \operatorname{suc}(0 + m)$ (for a given arbitrary m). But there's no obvious way of proving that using the resources currently on the table! Similarly, our induction step would require proving that $\operatorname{suc}(\operatorname{suc} n) + m = \operatorname{suc}(\operatorname{suc} n + \operatorname{suc} m)$ from the induction hypothesis that $(\operatorname{suc} n) + m = \operatorname{suc}(n + m)$; again, we don't yet have anything that we could use to do that.

There is no fool-proof rule that can tell you what strategy will work for finding an inductive proof of a claim with multiple generality; sometimes, you'll just need to experiment. But as a rule of thumb, when the facts you have to work with are "recursion principles" along the lines of (A) and (B), the variable that'll work for induction is the one in the position where the recursion equations say something different about the base case (for numbers: zero) and the non-base case (for numbers: successors). Looking at (A) and (B), we see that it's the thing on the *right* of the + symbol that's getting this differential treatment; this means that when we're proving facts about + by induction, it's a fair bet that we'll want to pick a variable that only occurs on the right side of the +: that's m in the case of Theorem 2.

Here's an example with *three* variables:

Theorem 3. $k + (m + n) = (k + m) + n$ for any natural numbers k, m, n.

Here there are three basic strategies we could adopt, even setting aside more complicated strategies along the lines of options 3 and 4 above. But bearing in mind our rule of thumb, we see that the variable n is the one that only occurs on the right side of the +, so it looks like the best candidate. And in fact, this strategy turns out to work:

Proof. By induction on n.

Base case:

$$\begin{aligned} k + (m + 0) &= k + m && \text{by fact (A)} \\ &= (k + m) + 0 && \text{by fact (A) again} \end{aligned}$$

Induction step: Suppose that $k + (m + n) = (k + m) + n$. Then

$$\begin{aligned} k + (m + \operatorname{suc} n) &= k + \operatorname{suc}(m + n) && \text{by fact (B)} \\ &= \operatorname{suc}(k + (m + n)) && \text{by fact (B) again} \\ &= \operatorname{suc}((k + m) + n) && \text{by IH} \\ &= (k + m) + \operatorname{suc} n && \text{by fact (B).} \end{aligned}$$ □

Here, 'By induction on n' is short for something like 'Let k and m be arbitrary natural numbers. We will prove by induction that every natural number has the property *being a number n such that* $k + (m + n) = (k + m) + n$, and conclude from that that for any k, m and n, $k + (m + n) = (k + m) + n$.'

In all three of the above proofs, it just so happens that the thing you're trying to prove has the form of a (universally quantified) *identity* claim: this means that the base case and the induction step will also involve proving identity claims, so that the main form of inference you'll be using is reasoning by substitution (analogous to what you do in algebra). But induction is certainly not limited to proving claims of this form! Here's an example of a proof by induction of a universally quantified *conditional* (where the antecedent and consequent are identities):

Theorem 4. For any numbers k, m, and n, if $k + n = m + n$, then $k = m$.

Proof. By induction on n.

Base case: Suppose $k + 0 = m + 0$. Then $k = m$ by fact (A).

Induction step: Suppose for induction that if $k+n = m+n$ then $k = m$. Suppose $k+\operatorname{suc} n = m+\operatorname{suc} n$. Then $\operatorname{suc}(k + n) = \operatorname{suc}(m + n)$ by fact (B). So $k + n = m + n$ by the fact that suc is injective. Given the induction hypothesis, it follows that $k = m$. □

The induction step there involves one supposition inside another. The outer supposition is the induction hypothesis (if $k+n = m+n$ then $k = m$), where k and m are the arbitrary numbers we have introduced for the purposes of this proof. What we need to prove from this assumption in order to carry out the induction is itself a conditional: if $k + \operatorname{suc} n = m + \operatorname{suc} n$, then $k = m$. And of course, the way to prove a conditional like this is to suppose the antecedent and prove the consequent; that's why we have the second 'Suppose. . . '.