Research Methods in Mathematics
Lecture 3: Induction is inescapable. Addition and multiplication.

T. PERUTZ

More on the axioms for natural numbers

Of the axioms explained in the last lecture, the principle of induction seems much more subtle than the rest. Here's a consequence of those axioms:

Proposition 1 *If n is a natural number then either $n = 1$ or there is a natural number m such that $n = S(m)$.*

Intuitively: unless $n = 1$, you can subtract 1 from n within the realm of natural numbers.

We'll prove the proposition (which is a statement $P(n)$ about a natural number n) by induction. It's manifestly true for $n = 1$ (since $1 = 1$). If it's true for n, we can prove if for $S(n)$. Well, it's also manifestly true for $S(n)$ (since $S(n)$ is the successor of n). That does it.

This is a very unusual induction, in that it doesn't really use the inductive hypothesis that the statement is true for n.

We can now ask whether this proposition could *replace* the principle of induction. Consider the following axioms:

NEW AXIOMS.

- There's a natural number called 1, and every natural number n has a 'successor' $S(n)$.
- 1 is not a successor.
- If $n \neq m$ then $S(n) \neq S(m)$.
- If n is a natural number then either $n = 1$ or there is a natural number m such that $n = S(m)$.

Only the last axiom differs from the old ones; it replaces the principle of induction. We know, by the proposition, that the new axioms are true if the old ones are. Is the converse true? Does the principle of induction follow from the new axioms?

The answer is no. Induction is strictly stronger. We can prove this by exhibiting a number system that satisfies the axioms given here, but in which the principle of induction is false. Here's such a system, denoted $\mathbb{F}$:

Let's assume we've used the natural numbers to set up the system of rational numbers $\mathbb{Q}$. We'll do this later. We can then consider the number system $\mathbb{F}$ formed by all rational numbers *except* the non-positive integers $0, -1, -2$, etc. The rational number 1 will also be the 1 in $\mathbb{F}$ required by the new axioms. The successor function S will add 1: $S(x) = x + 1$. (Notice that if x is in $\mathbb{F}$ then the rational number $x + 1$ again lies in $\mathbb{F}$.)

In $\mathbb{F}$, 1 is not a successor (it ought to be $S(0)$), but 0 is not in $\mathbb{F}$). If $x \neq y$ then $x + 1 \neq y + 1$. And if x is in $\mathbb{F}$ then, unless $x = 1$, the rational number $x - 1$ is also in $\mathbb{F}$, and we have $x = S(x - 1)$. So, our new system of axioms is satisfied.

But the principle of induction fails in $\mathbb{F}$, and that shows that $\mathbb{F}$ does not behave like the natural numbers. Consider the following statement about natural numbers:

Let f be any function which inputs natural numbers n and for each of them gives an output which is 0 or 1. Suppose that f satisfies $f(S(n)) = f(n)$. Then $f(n) = f(1)$ for all n.

This is a true statement about natural numbers; it's true by induction. But it's not a true statement if we replace 'natural numbers' by 'numbers from the system $\mathbb{F}$'. The function f given by $f(x) = 0$ if x is a positive integer and $f(x) = 1$ otherwise does satisfy the hypotheses (because $f(x + 1) = f(x)$ for all x in $\mathbb{F}$), yet it's not constant.

The principle of induction is not just a useful mathematical tool: it's an essential part of our characterization of natural numbers. If we want to prove things about natural numbers, it's vital to have induction in our toolkit. In this sense, *induction is inescapable*.

Addition

The definition of addition of done natural numbers is done inductively. We want to define $n + m$. We first define $n + 1 = S(n)$. Next, we define $n + S(1) = S(n + 1)$. In general, if $n + m$ has already been defined, we set $n + S(m) = S(n + m)$.

Is this a valid definition? Yes: let $P(m)$ be the statement '$n+m$ has been defined'. Then, by induction, $P(m)$ is true for all natural numbers m.[1]

As an example, let's see what this definition says about $n+4$. What it says is that

$$\begin{aligned} n+4 = n+S(3) &= S(n+3) \\ &= S(n+S(2)) \\ &= S(S(n+2)) \\ &= S(S(n+S(1))) \\ &= S(S(S(n+1))) \\ &= S(S(S(S(n)))). \end{aligned}$$

That is, to add 4, just add one four times.

A theorem about addition—one we will not prove—is as follows:

Theorem 2 *For all natural numbers m, n and p, we have*

(1) $(m+n)+p = m+(n+p)$;

(2) $m+n = n+m$.

Because of (1), we can unambiguously write $m+n+p$ without specifying the brackets.

Notice that these things are not evident from the definition. Is it true that $1+3 = 3+1$? Yes, but we have to work a little to verify it. We have

$$3+1 = S(3) = S(S(2)) = S(S(S(1)))),$$

while

$$1+3 = 1+S(2) = S(1+2) = S(1+S(1)) = S(S(1+1)) = S(S(S(1))).$$

Next we come to multiplication. Again, we define mn by induction on n: we set $m1 = m$ and $mS(n) = mn+n$.

Theorem 3 *For all natural numbers m, n and p, we have*

(1) $(mn)p = m(np)$;

(2) $m1 = m$ *(this is true by definition!);*

(3) $mn = nm$.

[1] You might ask: is the sentence '$n+m$ has been defined' something that should be legitimately considered a statement? What *is* a statement? Logicians attempt to answer this question, but we shall go no deeper into this particular rabbit-hole.

There is also a result that relates addition to multiplication:

Theorem 4 *For all natural numbers m, n and p, we have $(m+n)p = mp + np$.*

The properties of addition and multiplication described by the three theorems are fundamental ones that will be shared by several number systems which appear in this course.