Natural Numbers and Induction

Javier Rodriguez-Laguna, UC3M

Sept 7, 2008

[Calculus lecture notes for the engineering degree, Universidad Carlos III de Madrid, 2008 Fall term.]

Axioms for the Natural Numbers

Natural numbers (you know: 0,1,2,3...) can give more trouble than other sets of numbers, like rational or real, which have more apparent complexity... Why that? OK, let us give an example: equations in natural numbers are usually called *diophantine equations*, after certain Greek mathematician of the late Antiquity. for example:

$$2n + 4m = 15$$

If n and m were real numbers, the equation would be rather easy to solve: $n = 15/2 - 2m$, it represents a straight line in the mn plane. But if n and m are restricted to be natural numbers, then that equation has no solution! Why? $2n$ is an even number, and so is $4m$. How can two even numbers add up to 15? Probably, the most famous diophantine equation was last Fermat's theorem: for any natural $n > 2$ there are no natural a, b and c such that

$$a^n + b^n = c^n$$

Fermat wrote this down at the margin of his copy of Diophantus' *Arithmetics*, saying that he had a wonderful proof, but that unfortunately it didn't fit in that narrow margin. That was in the middle XVII century. A proof was given finally by Andrew Wiles in 1995, and required techniques and ideas that Fermat wouldn't have dreamed. Yet... can we be sure that Fermat didn't have *a* proof?

Like all branches of mathematics, natural numbers can be defined by a series of *axioms*. Axioms can't be proved or disproved, they can only be accepted or rejected. They're part of a definition. If I define an *oompa* to be a red pen, you can't disprove my assertion, the worse you can do is to consider it stupid... So, let's discuss briefly the *axioms for natural numbers*, adapted from the version given by Giuseppe Peano by the turn of the (XX) century:

1.- Zero (0) is a natural number.
2.- The successor of a natural number is a natural number.
3.- No two numbers share successor.
4.- Zero is not the successor of any natural number.
5.- If a property P is stated of zero, $P(0)$, and it is known that $P(n) \Rightarrow P(n+1)$, then it can be stated of all natural numbers.

That set of sentences uniquely determine the natural numbers. I would like you to appreciate the trick, so I will discuss a little bit the reason for each of them.

1.- Zero is a natural number... What I am really stating here is that at least there is one natural number. I could have called it oompa!

2.- The successor of a natural number is a natural number. The chain starts running! Now we have the successor of zero, let us call it "one", the successor of one, let us call it "two"... and so on! So, in an excess of optimism, we might argue that we already have *all* the natural numbers. Not so! The axioms so far do not exclude the possibility that natural numbers might "close" in a circle, like numbers in a clock, so the successor of "twelve" is again "one"...

3.- No two numbers share successor. This excludes the clock! How? If the successor of twelve was one, then twelve and one would share successor! So, circles forbidden! Did we rule out all nasty possibilities? No! What about negative numbers?

4.- Zero is not the successor of any number. OK, so there is a clear-cut start of the chain!! Done? No! Still some nasty thing can happen. Who says there can't be several "chains" running in parallel? I mean: several zeroes, all of them having their chain of successors?

5.- This last one is the most tricky and interesting property of natural numbers. It says that if you can state P of zero (*our* zero), and whenever you state P of a number you can extend that P to its successor, *then* you can state P of *all* natural numbers. This means that there is a single chain. Because, otherwise, you'd need several starts!

This last property is called **induction**, and it will be our next point of discussion...

Before you ask, I tell you all this with the intention of making you grasp the idea behind axiomatic systems. Getting good axioms for some intuitive idea or physical phenomenon is not a trivial task. If you do it correctly, then you can start proving things by working with them, and the things you prove will be also correct. This is the highest achievement of science. But if your axioms are not good, in the sense that they do not really reflect your idea or the real phenomenon, then you're wasting your time and energy in finding out things which do not happen in *this* universe of ours.

Mathematical Induction

The last point, mathematical induction, is the basis of a very powerful proof method. For example, let us discuss a simple algorithm to take the square root of a natural number: to substract the odd numbers in order (1,3,5...) until you can't substract any more. If the number is a perfect square, the number of substractions coincides with its square root and we reach zero. If it is not, then it is the highest integer which is lower than its square root. Hard to believe? OK, let's make a test:

$$64-1=63; \quad 63-3=60; \quad 60-5=55; \quad 55-7=48;$$

$$48-9=39; \quad 39-11=27; \quad 27-13=15; \quad 15-15=0$$

Eight substractions, and we reach zero, so $\sqrt{64}=8$, right? *Why that?* OK, let's formulate it in reverse:

Statement: If you add up odd numbers in order, you always end up with the square of the number of terms you used.

So: 1 is a perfect square, $1+3=4$ is also, $1+3+5=9$ is also... Hey, it seems to work! Let's try to write that down in mathematical notation. Odd numbers have the form $2n+1$ for n natural. So, check that this is the same as our statement:

$$\sum_{i=0}^{n} 2i+1 = n^2$$

How to prove it? Let's try to use *mathematical induction*. Again, this means that we assume it to be true for 0 (or 1), which is correct. Now we want to prove that if that formula is valid up to n, then it is also valid for $n+1$. So, let's start by writing the formula for $n+1$:

$$\sum_{i=0}^{n+1} 2i+1 = \sum_{i=0}^{n} 2i+1+(2n+1)$$

Now we use the "basis of induction", i.e.: the fact that the sum is just n^2. Then, that's equal to

$$n^2+(2n+1)=(n+1)^2$$

Just the square of $n+1$!! So, we proved that, if the formula holds for n, it holds for $n+1$. So, we proved that from 1 we can go to 2, from 2 to 3, pssssst... up to infinity. The good point of mathematical infinite ladders is that they can be climbed in a single jump!

E1. There is a nice geometrical way to prove the same formula. Check it with two squares, of sizes $n \times n$ and $(n+1) \times (n+1)$.

But, **beware!** There are dangers to induction! Consider this example. We'll prove that all horses are the same color. If there were just one horse, then it would be the same color as itself, so the thing would be proved. Now, let's assume all horses of the universe numbered from 1 to $n+1$, and let's assume that all sets of n horses *are* the same color. Then, horses 1 to n are the same color, and so are horses 2 to $n+1$. But the middle horses, 2 to n can't change color when they're in different groups (they're horses, not chameleons). So, horses 1 and $n+1$ must be the same color also. QED.

(Pedantic note: QED means *quod erat demonstrandum*, i.e.: what we intended to prove, and is used by pedantic mathematicians when they believe they've proved something.)

E2. What, if anything, is wrong in the previous reasoning?

E3. Prove the following formulas using mathematical induction:

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$$

$$\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{j=0}^{n} r^j = \frac{r^{n+1}-1}{r-1}$$

$$10^n-1 \qquad \text{is a multiple of 9 for all } n$$