Induction and Arithmetic in $\mathbb{N}_0$

John McCuan

February 7, 2020

There are a variety of arithmetic assertions concerning numbers (and ultimately natural numbers) we have been using, and should use, without thinking about them too much. These assertions concerning, or properties of, numbers like

$$0 \cdot a = 0 \qquad \text{and} \qquad a(b+c) = d$$

can be proved using only set theory and the Peano axioms. We give here a taste of how that works. We note that what is described here is properly called **ordinal arithmetic**. The text *An Introduction to Analysis* by Gunning basically suggests the use of cardinal arithmetic as a foundation for the numbers of analysis. Gunning does not present proofs of many basic arithmetic facts, but he has essentially the same Peano axioms, and the proofs should go about the same way. More generally, as long as one restricts attention to finite ordinals and cardinals, the discussion should be precisely the same in the sense that there should be an order preserving, operations preserving bijection between the finite ordinals $\mathbb{N}_0$ and the corresponding set of cardinals.

Before, we can offer proofs of arithmetic assertions like those above, we need to make sure we understand the **operations** of addition and multiplication on $\mathbb{N}_0$ and how they work. Everything essentially rests on the **induction axiom** from the Peano axioms. For addition, we define

$$m + 0 = 0. \tag{1}$$

This may be called the **initial definition**, the **initialization**, or the **initiation**. Then we set

$$m + (k+1) = (m+k) + 1 \tag{2}$$

(under the tacit assumption that we know the meaning of $m+k$). This may be called the **recursive definition** or the **recursion**. A few remarks are in order. Perhaps, the

most important thing to point out is that (2) is **not** a consequence of the associative property of addition. The associative property of addition is something that must be proved using (2). It definitely looks like a special case of the associative property with which we are familiar, but it should not be viewed that way. To help with this required refocus, we can make it look less familiar as follows: The Peano axioms postulate the existence of a certain function we may call the **successor function**. Formally, let us denote the successor function by $s : \mathbb{N}_0 \to \mathbb{N}_0$. In terms of the successor function we can write (2) as

$$m + s(k) = s(m + k).$$

I trust this makes clear that (2) is not an application of the associative property of addition. Similarly, the initiation (1) is not an application of the existence of 0 as an additive identity. It is more primitive, and one uses it to prove (or can use it to prove) 0 is an additive identity using the operation thus defined.

Technically, the structure of (1) and (2) together constitute what is called a **recursive definition** or **inductive definition**. The notion of **inductive definition** derives, itself, from the Peano axiom of induction. The idea of the construction is something like the following: We consider the set

$$A = \{n \in \mathbb{N}_0 : m + n \text{ is defined for all } m \in \mathbb{N}_0\}.$$

By (1) we have $0 \in A$. And by (2) if $k \in A$, then $k + 1 \in A$. The axiom of induction then implies $A = \mathbb{N}_0$, i.e., $m + n$ is defined for all m and n in $\mathbb{N}_0$, i.e., we have a well-defined operation of addition.

Exercise 1 *Prove the associative property of addition,*

$$(a + b) + c = a + (b + c) \qquad \textit{for all } a, b, c \in \mathbb{N}_0,$$

by induction.

Similarly, the **operation of multiplication** is defined by

$$m \cdot 0 = 0. \tag{3}$$

$$m(k + 1) = mk + m \qquad \text{or} \qquad ms(k) = mk + m. \tag{4}$$

Again, the recursion (4) is **not** a consequence of the distributive property. One uses (4) to prove the distributive property. Here is the proof:

Lemma 1 *$a(b+c) = ab + ac$ for all $a, b, c \in \mathbb{N}_0$.*

Proof: We use induction on c:

1. $a(b+0) = ab$. And $ab + a \cdot 0 = ab + 0 = ab$. We have used here the initiation for multiplication (3) to conclude $a \cdot 0 = 0$. Therefore, we conclude

$$a(b+c) = ab + ac \qquad \text{when} \qquad c = 0.$$

2. Now we start with $a(b+k) = ab+ak$ as an inductive hypothesis. Then we have

$$\begin{array}{lcll} a(b+(k+1)) = a(b+s(k)) & = & a[s(b+k)] & \text{by (2)} \\ & = & a(b+k) + a & \text{by (4)} \\ & = & ab + ak + a & \text{by inductive hypothesis and} \\ & & & \text{the associative property of } + \\ & = & ab + a(k+1) & \text{by (4) applied to } ak + a. \end{array}$$

These two steps allow us to conclude, by the axiom of induction, that

$$a(b+c) = ab + ac \qquad \text{for every } a, b, c \in \mathbb{N}_0. \qquad \square$$

Lemma 2 *$0 \cdot a = 0$ for every $a \in \mathbb{N}_0$.*

(Notes: This is not going to follow from the commutativity of multiplication; we'll prove that next. Also, there is a version of this assertion that applies in any ring where 0 is the additive identity and one has the distributive property and many other properties we do not have in $\mathbb{N}_0$.)
Proof: Again, we will prove the result by induction.

1. $0 \cdot 0 = 0$. This is the result of the initiation (3).

2. If $0 \cdot k = 0$ (as inductive hypothesis), then

$$\begin{array}{lcll} 0 \cdot (k+1) & = & 0 \cdot k + 0 & \text{by (4)} \\ & = & 0 & \text{by inductive hypothesis and} \\ & & & \text{because 0 is an additive identity.} \end{array}$$

This completes the induction on a. $\square$

Lemma 3 *$ab = ba$ for all $a, b \in \mathbb{N}_0$, i.e., addition is commutative in $\mathbb{N}_0$.*

Proof: This one is a bit tricky. We start with an Induction on b:

1. $a \cdot 0 = 0$ by the initiation for multiplication (3). On the other hand, $0 \cdot a = 0$ by the previous lemma. Therefore, we have the first step $a \cdot 0 = 0 \cdot a$ for our induction.

2. We have as inductive hypothesis

$$ak = ka. \tag{5}$$

Under this hypothesis, we consider

$$\begin{array}{rcll} a(k+1) & = & ak + a & \text{by (4)} \\ & = & ka + a & \text{by inductive hypothesis and} \\ & & & \text{not by commutativity of course.} \end{array}$$

Now we start a second induction on a to show $ka + a = (k+1)a$. Notice we can't use the distributive property, because we only have a left distributive property, and we have not shown commutativity yet. (You could, of course, try to establish a right distributive property independently, and were that effort successful, it could be used here.)

(a) $k \cdot 0 + 0 = 0 = (k+1) \cdot 0$.

(b) Now, we assume $km+m = (k+1)m$ (as inductive hypothesis), and consider

$$\begin{array}{rcll} k(m+1) + (m+1) & = & km + k + m + 1 & \text{by (4) and} \\ & & & \text{associativity of } + \\ & = & km + m + k + 1 & \text{by commutativity of } + \\ & = & (k+1)m + k + 1 & \text{by inductive hypothesis} \\ & = & (k+1)(m+1) & \text{by the recursion (4)} \\ & & & \text{applied recursively to } m. \end{array}$$

This establishes that $ka + a = (k+1)a$ for every $a \in \mathbb{N}_0$. Therefore, we may return to our primary induction and conclude

$$a(k+1) = (k+1)a.$$

We have established the commutativity of multiplication in $\mathbb{N}_0$. $\square$

Exercise 2 *Prove the commutativity of addition in* $\mathbb{N}_0$.