

Notes and Comments on the Addition Theorem

by Leonard Blackburn

The proof of the Addition Theorem given in the Spring '02 3283W class notes entitled “The Peano Postulates, version 4” has a fundamental error. The Theorem is correct. The proof uses a maneuver that is correct, but that cannot be used without proof. These Notes and Comments explain why the argument is incomplete. A correct proof, using a set-theory/Peano theorem called The Recursion Theorem, begins on page 3.

The Addition Theorem. There exists exactly one function $p : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ such that

- (A) $(\forall n \in \mathbb{N}) [p(n, 0) = n]$;
- (B) $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N}) [p(n, s(m)) = s(p(n, m))]$.

Incorrect Proof of Addition Theorem (Outline). First, suppose that $p : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ and $q : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ satisfy (A) and (B). Let $n_0 \in \mathbb{N}$. Let $S := \{m \in \mathbb{N} : p(n_0, m) = q(n_0, m)\}$. Using induction, one easily shows that $S = \mathbb{N}$. Hence $p = q$. Therefore, there is at most one function $p : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ that satisfies (A) and (B).

Now, define E to be the set of all $n \in \mathbb{N}$ such that there exists a function $p_n : \mathbb{N} \rightarrow \mathbb{N}$ such that

- (i) $p_n(0) = n$, and
- (ii) $(\forall m \in \mathbb{N}) [p_n(s(m)) = s(p_n(m))]$.

Now, we will use induction to show that $E = \mathbb{N}$. Define

$$p_0(m) := m$$

for all $m \in \mathbb{N}$. Then, one easily checks that p_0 satisfies (i) and (ii). Hence, $0 \in E$. Now, suppose $n \in E$. Then define

$$p_{s(n)}(m) := s(p_n(m))$$

for all $m \in \mathbb{N}$. Again, one easily checks that $p_{s(n)}$ satisfies (i) and (ii). Hence, $s(n) \in E$. Therefore, by induction, $E = \mathbb{N}$. Now we simply define

$$p(n, m) := p_n(m)$$

for all natural numbers n and m . Then (A) and (B) clearly hold. □

Remarks. First of all, the proof that there is at most one function $p : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ that satisfies (A) and (B) is entirely correct. There are two main errors in the existence part of the proof. One of these errors is easily understood and easily fixed. Let's discuss that one first.

When we are trying to prove by induction that $E = \mathbb{N}$, we correctly prove that $0 \in E$. Then we assume $n \in E$. This means that there exists *at least one* function p_n satisfying (i) and (ii). Therefore our definition of $p_{s(n)}$ in terms of p_n is ambiguous (perhaps there is more than one function p_n satisfying (i) and (ii)—which are we using?). It turns out, actually, that for all $n \in \mathbb{N}$ there is *exactly one* function p_n satisfying (i) and (ii). Once we prove this, then we have solved this difficulty. This is not hard to do. However, this is all irrelevant since the second error in the proof invalidates the entire proof, including the proof that $E = \mathbb{N}$ (even after fixed as noted above).

The second error is much more serious, and much harder to explain. In fact, the error is fatal, i.e. we won't be able to salvage the main structure of our proof. We will have to scrap the proof and start again. The problem is that the author of this proof has failed to understand that *definition* by induction is not the same as *proof* by induction. Let me explain. We all know what a proof by induction is. We begin with some set, say S , and we prove that $S = \mathbb{N}$ by showing that $0 \in S$, and that for all natural numbers n , whenever $n \in S$, then $s(n) \in S$. What is a *definition* by induction? A definition by induction is a means of defining a sequence of objects (sets), A_0, A_1, A_2, \dots , i.e. of defining a function f whose domain is the set of natural numbers (or some other index set) such that for all natural numbers n , $f(n) = A_n$. We *define* this sequence by first explicitly defining A_0 . Then, for an arbitrary $n \in \mathbb{N}$, we define $A_{s(n)}$ in terms of A_n . Thus, our definition takes the following form:

$$\begin{aligned} A_0 &:= B \\ A_{s(n)} &:= F(A_n). \end{aligned}$$

In what sense is this a *definition* of A_0, A_1, A_2, \dots ? The fact that such a sequence exists is not an axiom of set theory, nor is it a Peano Postulate. Thus we are required to prove that this sort of definition by induction is allowed. Let me now explain where the above incorrect proof of the Addition Theorem assumes that definition by induction is OK. The set E is defined to be the set of all $n \in \mathbb{N}$ such that there exists (“exists exactly one,” perhaps) a function $p_n : \mathbb{N} \rightarrow \mathbb{N}$ that has certain given properties (these properties are irrelevant for the present discussion). Now, the definition of this set E is perfectly OK. It is a well-defined set. In fact, it equals \mathbb{N} (this can be proven, but not in the manner of the above incorrect proof). Since E is a subset of \mathbb{N} , it makes sense to try to use induction to show that $E = \mathbb{N}$. Here is the structure of the incorrect induction proof given above: We first showed that $0 \in E$ (this is fine) by constructing a particular function (set) p_0 . Then we assumed $n \in E$, i.e., we assumed that a certain p_n existed, and we proceeded to define a $p_{s(n)}$ in terms of p_n . In other words, we

defined, by *induction*, a sequence of functions (sets)

$$p_0, p_1, p_2, p_3, \dots,$$

in order to simultaneously prove that $E = \mathbb{N}$. The definition of our sequence took the following form:

$$\begin{aligned} p_0 &:= B \\ p_{s(n)} &:= F(p_n) \end{aligned}$$

In fact, notice how the “definition” of the sequence p_0, p_1, p_2, \dots looks very much like the “definition” of one of the individual functions p_n . If we allow ourselves to define the sequence p_0, p_1, p_2, \dots in this way, then why did we bother proving that the functions p_n exist in the first place, since they are defined inductively in this very same way ($p_n(0) := n, p_n(s(m)) := s(p_n(m))$)!

If this doesn’t convince the reader that the above proof of the Addition Theorem is flawed, let us point out the exact point where an “incorrect” statement was made. It occurred exactly when we said: “Then define $p_{s(n)}(m) := s(p_n(m))$ ”. This definition is simply not allowed (and this would be painfully obvious if we were working entirely within *axiomatic* set theory). We cannot define the set $p_{s(n)}$ in terms of a set p_n which we don’t know exists in the first place. I know some readers would object to this by saying that we are, in the course of our proof by induction, *assuming* that the set p_n exists. But this is just an attempt to cleverly disguise a definition by induction. Readers who are still not convinced are invited to read Leon Henkin’s paper “On Mathematical Induction,” in which Henkin emphasizes how definition by induction works. The paper can be found in the American Mathematical Monthly, vol. 67 (1960), pp. 323-338. It may also be helpful to consult two books by Herbert Enderton, one of which is *A Mathematical Introduction to Logic*, in which definition by induction is discussed early in the book. The other book’s title escapes me. It is a book on set theory and it is on reserve in the mathematics library.

Further Remarks. As further evidence that the first proof of the Addition Theorem is incorrect, take note of the fact that the proof does not use the postulates that $0 \notin S(\mathbb{N})$ and that s is one-to-one (the proof of the Recursion Theorem does use these postulates), and as Henkin points out in his paper, the recursion theorem is in general false for systems $(N, 0, s)$ that satisfy the induction postulate but do not satisfy the postulates that $0 \notin s(\mathbb{N})$ and s is one-to-one.

A correct Proof of the Addition Theorem. Now we do not assume the validity of definition by induction in order to prove that a certain definition by induction is valid. The proof begins with the Recursion Theorem as a Lemma. The proof below closely follows that given by Enderton in his set theory book [2], which closely follows the proof given by Henkin [1] in the paper mentioned above.

The Recursion Theorem. Let A be any nonempty set, $a \in A$, and suppose that $F : A \rightarrow A$ is a function. Then there exists exactly one function $h : \mathbb{N} \rightarrow A$ such that

- (1) $h(0) = a$;
- (2) $h(s(n)) = F(h(n))$ for all $n \in \mathbb{N}$.

Proof of The Recursion Theorem. First, suppose that $g : \mathbb{N} \rightarrow A$ and $h : \mathbb{N} \rightarrow A$ both satisfy (1) and (2). Let $S := \{n \in \mathbb{N} : g(n) = h(n)\}$. Note that $g(0) = a = h(0)$, and so $0 \in S$. Suppose that $n \in S$. Then $g(s(n)) = F(g(n)) = F(h(n)) = h(s(n))$, and so $s(n) \in S$. Therefore by mathematical induction, $S = \mathbb{N}$. Therefore, $g = h$, and so, there is at most one function $h : \mathbb{N} \rightarrow A$ that satisfies (1) and (2).

Now, we prove that there is a function $h : \mathbb{N} \rightarrow A$ that satisfies (1) and (2). Call a function f *acceptable* iff $\text{dom } f \subseteq \mathbb{N}$, $\text{ran } f \subseteq A$, and if the following conditions hold:

- (i) If $0 \in \text{dom } f$, then $f(0) = a$;
- (ii) If $s(n) \in \text{dom } f$ (where $n \in \mathbb{N}$), then $n \in \text{dom } f$ and $f(s(n)) = F(f(n))$.

Let \mathcal{H} be the collection of all acceptable functions, and let $h = \bigcup \mathcal{H}$ (i.e., h , as a set of ordered pairs, is the union of all acceptable functions, each of which is a set of ordered pairs). Thus,

- (iii) $(n, y) \in h$ iff (n, y) is a member of some acceptable f
iff $f(n) = y$ for some acceptable f .

We claim that h meets the demands of the theorem. We break the proof into three parts, which involve showing that (I) h is a function, (II) h is acceptable, and (III) $\text{dom } h$ is all of \mathbb{N} .

(I) Define $S := \{n \in \mathbb{N} : \text{for at most one } y, (n, y) \in h\}$. We use induction to show that $S = \mathbb{N}$. Suppose $(0, y_1) \in h$ and $(0, y_2) \in h$. By (iii), there exist acceptable f_1 and f_2 such that $f_1(0) = y_1$ and $f_2(0) = y_2$. But by (i), it follows that $y_1 = a = y_2$. Thus $0 \in S$. Next suppose that $n \in S$. Suppose that $(s(n), y_1) \in h$ and $(s(n), y_2) \in h$. Again there must exist acceptable f_1

and f_2 such that $f_1(s(n)) = y_1$ and $f_2(s(n)) = y_2$. By (ii) it follows that $y_1 = f_1(s(n)) = F(f_1(n))$ and $y_2 = f_2(s(n)) = F(f_2(n))$. But since $n \in S$, we have $f_1(n) = f_2(n)$ (since $(n, f_1(n))$ and $(n, f_2(n))$ are in h). Therefore, $y_1 = F(f_1(n)) = F(f_2(n)) = y_2$. So, $s(n) \in S$, and hence, $S = \mathbb{N}$. Consequently, h is a function.

(II) First, it is clear from (iii) that $\text{dom } h \subseteq \mathbb{N}$ and $\text{ran } h \subseteq A$. If $0 \in h$, then there must be some acceptable f with $f(0) = h(0)$. Since $f(0) = a$, we have $h(0) = a$. So, (i) holds for h . Next, assume $s(n) \in \text{dom } h$. There must be some acceptable f with $f(s(n)) = h(s(n))$. Since f is acceptable we have $n \in \text{dom } f$ (and $f(n) = h(n)$) and $h(s(n)) = f(s(n)) = F(f(n)) = F(h(n))$. Thus h satisfies (ii) and so it is acceptable.

(III) We use induction to show that $\text{dom } h = \mathbb{N}$. The function $\{(0, a)\}$ is acceptable and hence $0 \in \text{dom } h$. Suppose that $k \in \text{dom } h$. We will show that $s(k) \in \text{dom } h$. Define $f := h \cup \{(s(k), F(h(k)))\}$. Then f is a function, $\text{dom } f \subseteq \mathbb{N}$, and $\text{ran } f \subseteq A$. We will show that f is acceptable. Condition (i) holds since $f(0) = h(0) = a$. For condition (ii) there are two cases. If $s(n) \in \text{dom } f$ where $s(n) \neq s(k)$, then $s(n) \in \text{dom } h$ and $f(s(n)) = h(s(n)) = F(h(n)) = F(f(n))$. The other case occurs if $s(n) = s(k)$. Then $n = k$, since s is one-to-one. By assumption, $k \in \text{dom } h$. Thus $f(s(k)) = F(h(k)) = F(f(k))$ and (ii) holds. Hence f is acceptable. Therefore $f \subseteq h$, so that $s(k) \in \text{dom } h$. Therefore $\text{dom } h = \mathbb{N}$. \square

First Correct Proof of the Addition Theorem. The proof that there is at most one function $p : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ that satisfies (A) and (B) is the same as above. We just prove the existence part here. The argument is Enderton's

Now, by the Recursion Theorem, for all $n \in \mathbb{N}$, there exists exactly one function $p_n : \mathbb{N} \rightarrow \mathbb{N}$ such that $p_n(0) = n$ and $p_n(s(m)) = s(p_n(m))$ for all $m \in \mathbb{N}$. (We are using $A = \mathbb{N}$ and $F = s$.) So, define $p(n, m) = p_n(m)$ for all natural numbers n and m . It is clear that this p satisfies (A) and (B). \square

Second Correct Proof of the Addition Theorem. Again, we prove the existence part. This argument is mine. Define

$$p := \{((n, m), k) \in (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} : (\exists f \in \mathbb{N}^{\mathbb{N}})[f(0) = n \wedge (\forall l \in \mathbb{N})(f(s(l)) = s(f(l))) \wedge f(m) = k]\}$$

Proof that p is a function: Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. By the Recursion Theorem we can let f be the unique function such that $f(0) = n$ and $f(s(l)) = s(f(l))$ for all $l \in \mathbb{N}$. Therefore, $((n, m), f(m)) \in p$. This shows that $p(n, m)$ is defined for all natural numbers n and m . Now suppose that $((n, m), k_1) \in p$ and $((n, m), k_2) \in$

p . Then, by the definition of p there are functions $f \in \mathbb{N}^{\mathbb{N}}$ and $g \in \mathbb{N}^{\mathbb{N}}$ such that $f(0) = n$, $(\forall l \in \mathbb{N})(f(s(l)) = s(f(l)))$, $f(m) = k_1$, $g(0) = n$, $(\forall l \in \mathbb{N})(g(s(l)) = s(g(l)))$, and $g(m) = k_2$. But by the uniqueness clause in the Recursion Theorem, $f = g$. Therefore $k_1 = k_2$, and so p is a function.

Proof that p satisfies (A): Let $n \in \mathbb{N}$. By the Recursion Theorem, there is a unique function $f : \mathbb{N} \rightarrow \mathbb{N}$ such that $f(0) = n$ and $f(s(l)) = s(f(l))$ for all $l \in \mathbb{N}$. For this f , $f(0) = n$. Thus, $((n, 0), n) \in p$, i.e., $p(n, 0) = n$.

Proof that p satisfies (B): Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Again, by the Recursion Theorem, we can let f be the unique function from \mathbb{N} to \mathbb{N} such that $f(0) = n$ and $f(s(l)) = s(f(l))$ for all $l \in \mathbb{N}$. Therefore, $((n, m), f(m)) \in p$, i.e. $p(n, m) = f(m)$. Thus, we need to show that $p(n, s(m)) = s(f(m))$, i.e. that $((n, s(m)), s(f(m))) \in p$. But this is immediate by the definition of p since $f(s(m)) = s(f(m))$. \square

References

- [1] Enderton, H., **An Introduction To Set Theory**
- [2] Henkin, Leon, **On Mathematical Induction**, American Mathematical Monthly, vol. 67 (1960), pp. 323-338.

Further Comments on the Recursion Theorem: The recursion theorem has many generalizations that are useful. For example, we can define functions recursively or “by induction,” that satisfy

$$f(0) = a, \quad f(s(n)) = g(f(n), n)$$

instead of just

$$f(0) = a, \quad f(s(n)) = g(f(n)).$$

Also, there are recursion theorems when the domain isn't the natural numbers. The domain may be a set generated from some “initial elements” by several functions (In the case of the natural numbers, 0 is the only initial element and the successor function s is the only function that generates all of the natural numbers). For generalizations like this, see Enderton's *A Mathematical Introduction to Logic*.

There is a more general form of the recursion theorem for ordinals (transfinite recursion) that can be found in any graduate-level book on Zermelo-Fraenkel set theory.