Establishing some familiar properties of the natural numbers

By working through the exercises below you will establish that any set $\mathbf{N}$ obeying the Peano axioms has the usual properties of the natural number system. Do not assume ahead of time that such a set has any other properties besides those explicitly assumed in the Peano axioms (for instance, don't assume $\mathbf{N}$ is the set of natural numbers, even though that's what we eventually have in mind). The purpose of these exercises is to use the Peano axioms to *derive* the usual properties of arithmetic; you have to avoid circular reasoning. For example, you can't make use of notions like "less than" or "the first n elements of $\mathbf{N}$" until these have been defined in a non-circular way.

The exercises are interspersed with some definitions, some discussion, and with some of the trickier proofs. In some cases the definitions only make sense because of the statement in a preceding exercise. Whenever specific numerals 2,3,4, or 5 appear, they have the meaning you would expect: $2 = s(1)$, $3 = s(2)$, etc.

Exercises

1. Prove that the element "1" in the Peano axioms is unique (i.e. that there is only one element that is not the successor of any element).

2. Prove that no $n \in \mathbf{N}$ satisfies $s(n) = n$.

3. Prove that for all $n \in \mathbf{N}$ with $n \neq 1$, there exists a unique $m \in \mathbf{N}$ with $s(m) = n$.

Definition 1. For each $n \in \mathbf{N}$ with $n \neq 1$, the *predecessor* of n is the unique $m \in \mathbf{N}$ with $s(m) = n$. Let $\mathrm{pre}(n)$ denote the predecessor of n.

Exercises

4. By Definition 1, $s(\mathrm{pre}(n)) = n$ for all $n \neq 1$. Show that $\mathrm{pre}(s(n)) = n$ for all $n \in \mathbf{N}$ as well.

5. Prove that there exists no nonempty subset $A \subset \mathbf{N}$ with the property that the predecessor of every element of A exists and lies in A.

We would next like to come up with a definition of the set that we are accustomed to writing as "$\{1, 2, \ldots, n\}$", where n is an unspecified element of $\mathbf{N}$. As yet this notation has no meaning, since we have no definition of "$\ldots$". We cannot get around this by declaring "$\{1, 2, \ldots, n\}$" to mean "the first n elements of $\mathbf{N}$" since we have no definition of the latter phrase yet either. Without a clear definition of such a set, even our definition of "finite set" makes no sense, since we defined a nonempty finite set to be one that could be put into one-to-one correspondence with a set of the form "$\{1, 2, \ldots, n\}$". The "obvious" way around these problems is to try something like the following:

1. Define $I_1 = \{1\}$.
2. For $n \in \mathbf{N}$, if the set I_n has been defined, define $I_{s(n)} = I_n \bigcup \{s(n)\}$.

The trouble with this definition is that "has been defined" makes implicit reference to a notion of *time*, which does not appear anywhere in the Peano axioms, and of which all properties of $\mathbf{N}$ should be independent.

I encourage you to try to come up with a way to define the set "$\{1, 2, \ldots, n\}$" that does not use any as-yet undefined notions such as "greater than", "less than", or "do something n times". After you've tried, continue reading; perhaps you will have come up with a better solution than the one below.

Definition 2. For $n \in \mathbf{N}$, a subset $I \subset \mathbf{N}$ is an *initial interval of length n* if it satisfies the following conditions.

- $(\mathcal{I}_n^1)$ $1 \in I$ and $n \in I$.
- $(\mathcal{I}_n^2)$ n is the unique element of I whose successor is not in I.
- $(\mathcal{I}_n^3)$ If $m \in I$ and $m \neq 1$, then the predecessor of m is in I.

Note also that we cannot yet refer to "*the* initial interval of length n", since such terminology implicitly assumes both existence and uniqueness of an initial interval of length n. The next lemma and its corollary will fill this gap.

Lemma 1 *(a) If $n \in \mathbf{N}$ and I is an initial interval of length n, then $I \bigcup \{s(n)\}$ is an initial interval of length $s(n)$*

(b) If $n \in \mathbf{N}, n \neq 1$, and I is an initial interval of length n, then $I - \{n\}$ is an initial interval of length $\mathrm{pre}(n)$.

Proof: (a) Let $n \in \mathbf{N}$, let I be an initial interval of length n, and let $I_+ = I \bigcup \{s(n)\}$. Then $1 \in I_+$ and $s(n) \in I_+$, so I_+ satisfies condition $\mathcal{I}_{s(n)}^1$.

To establish condition $\mathcal{I}_{s(n)}^2$ we must show two things: (i) $s(s(n)) \notin I_+$, and (ii) $s(m) \in I_+$ for all $m \in I_+$ other than $s(n)$. If $s(s(n)) \in I_+$ then $s(s(n)) \in I$, since the possibility "$s(s(n)) = s(n)$" is ruled out by Exercise 2. But $s(s(n)) \neq 1$ since 1 is not the successor of any element, so condition $\mathcal{I}_n^3$ implies $\mathrm{pre}(s(s(n))) \in I$. By Exercise 4 this implies $s(n) \in I$, contradicting $\mathcal{I}_n^2$. Hence statement (i) is true. As for (ii), if $m \in I_+$ and $m \neq s(n)$ then $m \in I$. If $m = n$ then $s(n) \in I_+$ by definition of I_+, while if $m \neq n$ then $s(m) \in I$ (and hence $s(m) \in I_+$) by condition I_n^2. Therefore (ii) is true, and I_+ satisfies condition $\mathcal{I}_{s(n)}^2$.

Next, let $m \in I_+, m \neq 1$. If $m = s(n)$ then $\mathrm{pre}(m) = n \in I$, while if $m \neq s(n)$ then $m \in I$, and therefore condition $\mathcal{I}_n^3$ implies that $\mathrm{pre}(m) \in I$. Since $I \subset I_+$, in either case we have $\mathrm{pre}(m) \in I_+$. Thus I_+ satisfies condition $\mathcal{I}_{s(n)}^3$, and therefore is an initial interval of length n.

(b) Let $n \in \mathbf{N}, n \neq 1$, let I be an initial interval of length n, and let $I_- = I - \{n\}$. Then $1 \in I$, so $1 \in I_-$ (the removed element 1 is $\neq n$ by hypothesis). By condition $\mathcal{I}_n^3$ we have $\text{pre}(n) \in I$ and (by Exercise 2) $n \neq \text{pre}(n)$, so $\text{pre}(n) \in I - \{n\} = I_-$. Thus I_- satisfies Condition $\mathcal{I}_{\text{pre}(n)}^1$.

By definition of I_-, $s(\text{pre}(n)) = n \notin I_-$. If $m \in I_-$ and $m \in I$ and $m \neq n$, so $s(m) \in I$, and therefore $s(m) \in I_-$ unless $s(m) = n$, i.e. unless $m = \text{pre}(n)$. Thus I_- satisfies Condition $\mathcal{I}_{\text{pre}(n)}^2$.

Finally, if $m \in I_-$ and $m \neq 1$, then $m \in I$, so $\text{pre}(m) \in I$ by $\mathcal{I}_n^3$, and therefore $\text{pre}(m) \in \mathcal{I}_-$ unless $\text{pre}(m) = n$. But if $\text{pre}(m) = n$ then $m = s(n) \notin I$, and hence $m \notin I_-$. Thus for all $m \in I_-$, if $m \neq 1$ then $s(m) \in I_-$; i.e. I_- satisfies condition $\mathcal{I}_{\text{pre}(n)}^3$. ∎

Corollary 2 *For all $n \in \mathbf{N}$ there exists a unique initial interval I_n of length n, and $I_{s(n)} = I_n \bigcup \{s(n)\}$.*

Proof: Observe that $\{1\}$ is an initial interval of length 1. Let I be an interval of length 1 and let $M_1 = 1 \bigcup \mathcal{C}(I)$, where "$\mathcal{C}$" denotes complement. Then $1 \in M_1$ and $s(1) \notin I$, so $s(1) \in M_1$. If $n \in M_1$ and $n \neq 1$ then $s(n) \in M_1$, for otherwise we would have $s(n) \in I$, implying $\text{pre}(s(n)) \in I$ (by condition $\mathcal{I}_1^3$), implying $n \in I$, implying the contradiction $n \notin M_1$. By induction, $M_1 = \mathbf{N}$, implying that $\mathcal{C}(I) = \mathcal{C}(\{1\})$, and therefore that $I = \{1\}$.

Let $M = \{n \in \mathbf{N} : \exists \text{ unique initial interval of length } n\}$. We have just shown that $1 \in M$. Suppose $n \in M$, and let I_n be the unique initial interval of length n. Then by Lemma 1, part (a), $I_n \bigcup \{s(n)\}$ is an initial interval of length $s(n)$. Suppose there were two initial intervals I, I' of length $s(n)$. Then by part (b) of the lemma, both $I - \{s(n)\}$ and $I' - \{s(n)\}$ would be initial intervals of length n, but since I_n is unique this would imply $I - \{s(n)\} = I' - \{s(n)\}$, and hence $I = I'$. Thus $I_n \bigcup \{s(n)\}$ is the *unique* initial interval of length $s(n)$, so $s(n) \in M$. By induction, $M = \mathbf{N}$, and we are done. ∎

Henceforth the initial interval of length n will also be called the set of the *first* n elements of $\mathbf{N}$. We define the notation "$\{1, \ldots, n\}$", or "$\{1, 2, \ldots, n\}$", etc., to mean I_n.

Remark. It may seem at first that condition $\mathcal{I}_n^3$ in Definition 2 is redundant, but it is not. Were we to require only conditions $\mathcal{I}_n^1$ and $\mathcal{I}_n^2$, there would be infinitely many initial intervals of length 1. For example $\{1\} \bigcup \{3, 4, 5 \ldots\}$ (i.e. $\mathcal{C}(\{2\})$, where $2 = s(1)$) would be such a set; more generally for any $n \neq 1$, $\{1\} \bigcup \mathcal{C}(I_n)$ satisfies the first two conditions for an initial interval of length 1.

In Lemma 1 we used induction to define the sets I_n, the critical step being the construction of $I_{s(n)}$ from I_n. Such a use of induction to define some collection of sets,

functions, numbers, or other objects indexed by $n \in \mathbf{N}$, is called *recursion*. Usually this is done more informally, as in our "time-dependent" first attempt at the definition of the I_n. Now that we have defined the sets I_n properly (using Corollary 2) we can handle recursion cleanly. This is important because we will later use recursion to help define addition and multiplication.

Proposition 3 *Let X be any nonempty set, let $f : \mathbf{N} \times X \to X$, and let $g_1 \in X$. Then there exists a unique function $g : \mathbf{N} \to X$ satisfying*
(i) $g(1) = g_1$, and
(ii) $g(s(n)) = f(s(n), g(n))$ for all $n \in \mathbf{N}$.

We will prove this shortly, but first, to understand what this has to do with recursion, consider these examples. To make the illustrations clearer, I'll assume in these examples that $\mathbf{N}$ has all the properties we know and love about the natural numbers.

1. $X = \mathbf{N}, f(n, m) = nm$, $g_1 = 1$. Then the function g given by the Proposition satisfies $g(n+1) = (n+1)g(n) = (n+1)n\ g(n-1) = \ldots = (n+1) \cdot n \cdot \ldots \cdot 2 \cdot g(1) = (n+1)!$. Thus we construct the function "factorial".

2. $X = P(\mathbf{N})$ (the power set of $\mathbf{N}$), $g_1 = \{1\}$, $f(n, A) = A \bigcup \{n\}$. Then $g(1) = \{1\} = I_1, g(2) = I_1 \bigcup \{2\} = I_2, g(3) = I_2 \bigcup \{3\} = I_3, \ldots$. Thus $g(n) = I_n$ for all n. This example illustrates the usefulness of recognizing that a collection of sets indexed by $\mathbf{N}$ can be viewed as a function whose domain is $\mathbf{N}$.

Although the second example is a useful *illustration* of what Proposition 3 has to do with recursion in general, we will use our previous construction of the sets I_n to prove Proposition 1 3, so we cannot literally use Proposition 3 to construct the I_n. The examples are meant to illustrate what role the function f plays: it's the rule by which we combine a "new" number $s(n)$ with a "previously defined" object $g(n)$ to produce a "new" object $g(s(n))$. (I've put quotes around the terms that implicitly refer to time.)

Proof of Proposition 3. Let M be the set of those $m \in \mathbf{N}$ for which there exists a unique function $h_m : I_m \to X$ satisfying the conditions (a_m) $h_m(1) = g_1$ and (b_m) $h_m(s(n)) = f(s(n), h_m(n))$ whenever $s(n) \in I_m$. The function $g_{(1)} : I_1 \to X$ defined by $g_{(1)}(1) = g_1$ satisfies conditions (a_1) and (b_1)—the second condition vacuously—and is the only function from I_1 to X satisfying condition (a_1), so $1 \in M$. Suppose that $m \in M$, and let $h_m : I_m \to X$ be the unique function satisfying (a_m) and (b_m). Define $h_{s(m)} : I_{s(m)} \to X$ by

$$h_{s(m)}(n) = \begin{cases} h_m(n) & \text{if } n \in I_m \\ f(s(m), h_m(m)) & \text{if } n = s(m) \end{cases}$$

Then $h_{s(m)}$ satisfies ($\mathrm{a}_{s(m)}$) and ($\mathrm{b}_{s(m)}$). If $h' : I_{s(m)} \to X$ is another function satisfying these conditions, then the restriction of h' to I_m satisfies (a_m) and (b_m), so (by the

uniqueness statement in the definition of M), the restriction of h' to I_m equals h_m. Thus for $n \in I_m$ we have $h'(n) = h_m(n) = h_{s(m)}(n)$, while if $n = s(m)$ we have $h'(n) = h'(s(m)) = f(s(m), h'(m)) = f(s(m), h_m(m)) = h_{s(m)}(n)$ as well. Thus $h' = h_{s(m)}$ and $h_{s(m)}$ is the unique function from $I_{s(m)}$ to X satisfying $(\mathrm{a}_{s(m)})$ and $(\mathrm{b}_{s(m)})$. Therefore $s(m) \in M$, so by induction $M = \mathbf{N}$.

Define $g : \mathbf{N} \to X$ by $g(m) = h_m(m)$. By property $(\mathrm{b}_{s(m)})$ we have $g(s(m)) = h_{s(m)}(s(m)) = f(s(m), h_{s(m)}(m)) = f(s(m), h_m(m))$ [because the restriction of $h_{s(m)}$ to I_m is h_m] $= f(s(m), g(m))$. Therefore g satisfies condition (ii) in the statement of the proposition, and clearly also satisfies condition (i). Let g' be any other function satisyfing these conditions, and let $M' = \{m \in \mathbf{N} : g(m) = g'(m)\}$. Then $1 \in M'$, and if $m \in M'$, condition (ii) implies that $g'(s(m)) = g(s(m))$, so $s(m) \in M'$. Therefore $M' = \mathbf{N}$, so $g' = g$; i.e. g is the unique function satisfying (i) and (ii).

■

We are now (almost) ready to define addition and multiplication. Intuitively, what we want to do for addition is clear. Addition by 1 should correspond to the successor function; addition by 2 should correspond to applying the successor function twice; addition by n should correspond to applying the successor n times. The trouble is, how do we define "do something n times" when n is not specified, without using circular definitions? Recursion comes to the rescue, in the special form of *iteration*.

Definition. Let Y be any nonempty set, let X be the set of functions from Y to Y, let $G \in X$ and let $f : \mathbf{N} \times X \to X$ be defined by $f(n, h) = G \circ h$. (Note what we are doing here: G and h are *functions* from Y to itself, so their composition is another function from Y to itself. We are in a very special case of Proposition 3 in which the function f happens not to depend on n.) Let $g : \mathbf{N} \to X$ be the function given by Proposition 3 with $g_1 = G$, and for $n \in N$ define G^n, the n^{th} *iterate of* G, to be $g(n)$. Thus, for every n, G^n is a function from Y to Y. (Note: the "n" in "G^n" is just a convenient superscript, not literally an exponent. A notation such as G^n is more convenient than $g(n)$ in this context since "$G^n(y)$" is less confusing to look at than "$g(n)(y)$".)

The reason for the terminology "n^{th} iterate" is clear if we write out what this definition tells us: $G^1 = G$, $G^2 = G \circ G$, $G^3 = G \circ G \circ G$ etc.; thus $G^1(y) = G(y), G^2(y) = G(G(y)), G^3(y) = G(G(G(y)))$ etc.

Finally we are ready for arithmetic.

Definition and Notation. For $m \in \mathbf{N}$ let $m + 1$ denote $s(m)$, and if $m \neq 1$ let $m - 1$ denote $\mathrm{pre}(m)$. For $n \in \mathbf{N}$, let s^n be the n^{th} iterate of the function $s : \mathbf{N} \to \mathbf{N}$, and define define $m + n = s^n(m)$ for all $m, n \in \mathbf{N}$. (*Warning*: the definition of $n + m$ is $s^m(n)$, which is not the same as the definition of $m + n$. Later you will prove that $m + n = n + m$, but *until you do, don't assume it.*) We define relations $<, \leq, >$, and $\geq$ on $\mathbf{N}$ as follows. Let $m, n \in \mathbf{N}$. (i) We say $m < n$ iff there exists $k \in \mathbf{N}$ with $n = s^k(m)$. (ii) We say $m \leq n$ iff $m < n$ or $m = n$. (iii) We say $m > n$ iff $n < m$. (iv) We say $m \geq n$ iff $n \leq m$.

The order in which most of the remaining exercises appear is not random. In several cases an earlier exercise is needed to do a later one; if you get stuck, you will not be able to get un-stuck by assuming the result of a later exercise to do an earlier one.

Exercises.

6. Prove that $m \leq n$ iff $m \in I_n$.

7. Prove that for all $m, n \in \mathbf{N}$, exactly one of the following three statements is true: (i) $m < n$; (ii) $m = n$; (iii) $m > n$.

8. Prove that $(m + n) + 1 = m + (n + 1)$ for all $m, n \in \mathbf{N}$.

9. Prove the associative law for addition: $(m+n)+p = m+(n+p)$ for all $m, n, p \in \mathbf{N}$.

10. Prove the generalized associative law for addition: given any finite ordered n-tuple $(m_1, m_2, ..., m_n)$ of elements of $\mathbf{N}$ ($n \geq 3$), the notation $m_1 + m_2 + ... + m_n$ is unambiguous (i.e. it doesn't matter which order the +'s are done in, so long as the order in which the m_i appear is not changed). (For example $(m_1+(m_2+m_3))+m_4 = m_1 + (m_2 + (m_3 + m_4))$.)

11. Prove that for all $n, m \in \mathbf{N}$, $n + m = m + n$. As a corollary, deduce that even the order of the m_i in problem 10 does not matter.

Definition and Notation. For all $n \in \mathbf{N}$, define $n \cdot 1 = n$, and for $m \neq 1$ define $n \cdot m = (n \cdot (m - 1)) + n$. (This is a recursive definition; I leave it to you to see how to write it more formally in the terms of Proposition 3.) We refer to "+" as addition and "$\cdot$" as multiplication. Words such as *add, multiply, sum, product* etc. are taken to have their usual meanings in terms of the operations "+" and "$\cdot$". We will simplify notation in various conventional ways. For example, when using single letters (e.g. m, n) to stand for elements of $\mathbf{N}$, we will take the juxtaposition of those letters (e.g. mn) is taken to mean $m \cdot n$. We will use the familiar convention for implied order of operations when parentheses are omitted; e.g. $mn + p$ equals $(m \cdot n) + p$, not $m \cdot (n + p)$.

12. Prove the left distributive law: $m \cdot (n + p) = mn + mp$, $\forall m, n, p \in \mathbf{N}$.

13. (a) Prove that multiplication in $\mathbf{N}$ is associative. (b) Prove the generalized associative law for multiplication (the multiplicative analog of problem 10 above).

14. Prove the right distributive law: $(m + n) \cdot p = mp + np$, $\forall m, n, p \in \mathbf{N}$.

15. Prove that multiplication in $\mathbf{N}$ is commutative.

16. Figure out how to define subtraction. I.e. for $m, n \in \mathbf{N}$, with $m < n$, figure out how to define $n - m$. Prove that $(n - m) + m = n = (n + m) - m$. Prove the relevant left and right distributive laws (the analogs of problems 12 and 14).