Peano Axioms for the Natural Numbers

There are certain facts we tend to take for granted about the natural numbers $\mathbf{N} = \{1, 2, 3, \ldots\}$. To be sure we don't take for granted something that is either false or unprovable, it's best to list as small as possible a set of basic assumptions ("axioms"), and derive all other properties from these assumptions. The axioms below for the natural numbers are called the *Peano axioms*. (The treatment I am using is adapted from the text *Advanced Calculus* by Avner Friedman.)

Axioms: There exists a set $\mathbf{N}$ and an injective function $s : \mathbf{N} \to \mathbf{N}$ satisfying the properties below. For $n \in \mathbf{N}$, we will call $s(n)$ the *successor* of n.

(I) There is an element "1" that is not the successor of any element.

(II) Let $M \subset \mathbf{N}$ be any subset such that (a) $1 \in M$, and (b) if $n \in M$, then $s(n) \in M$. Then $M = \mathbf{N}$.

To make this less abstract, you should think of the successor function as "adding 1". Axiom (I) essentially says that there is a "first" natural number. We can then define an element "2" by $2 = s(1)$, an element "3" by $3 = s(2)$, and so on.

Axiom II is called the "axiom of induction" or "principle of induction"; when invoking it, we usually say that something is true "by induction". You are probably familiar with it in the following equivalent form:

(II)′ Let $P(\cdot)$ be a statement that can be applied to any natural number n (for a specific n, we would write the statement as $P(n)$), and has a true-false value for any n. Suppose that (a) $P(1)$ is true, and (b) for all $n \in \mathbf{N}$, if $P(n)$ is true, then $P(s(n))$ is also true (think: $P(n + 1)$ is also true). Then $P(n)$ is true for all $n \in \mathbf{N}$.

The equivalence of (II) and (II)′ can be seen by identifying the set M of (II) with the set $\{n \mid P(n) \text{ is true}\}$ of (II)′.

We'll see some implications of these axioms in a moment. But first, do we know there is any set at all satisfying the Peano axioms? Yes—provided we assume the axioms of set theory, which I won't state here. From those axioms, one can construct a set $\mathbf{N}$ with the properties above. Why can't we simply say "Of course there exists such a set: the counting numbers $\{1, 2, 3, ...\}$?" Because that would be circular reasoning. If you assume something, you can no longer call that thing "proved". On the other hand, if you assume nothing, you can prove nothing. For many reasons, mathematicians find it convenient to assume the axioms of set theory, and it so happens that the Peano axioms follow from the set theory axioms as theorems. Alternatively, you could say "By golly, I'm just going to assume the natural numbers exist! It's obvious enough to me that they do, and they certainly satisfy the Peano axioms!" But to prove anything, you'd probably end up wanting to use the axioms of set theory anyway, so your extra assumptions would end up being redundant.

All the usual facts about the arithmetic of natural numbers can be deduced from the Peano axioms. For example, there's only one "1"—i.e. there is only one element that isn't the successor of any other. (Do you see how this follows from the axioms? Hint: apply Axiom II to the set $M = \{1\} \bigcup \text{image}(s)$.) For another example, there are functions $plus : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$, $times : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$, which we henceforth denote by

$$plus(m, n) = m + n, \quad times(m, n) = m \cdot n,$$

satisfying

$$
\begin{aligned}
n + 1 &= s(n), \\
n + s(m) &= s(n + m), \\
n \cdot 1 &= n, \\
n \cdot (m + 1) &= (n \cdot m) + n,
\end{aligned}
$$

for all $m, n \in \mathbf{N}$. From these properties of $+$ and $\cdot$, the usual commutative, associative, and distributive laws for natural numbers can be derived.

Once we have the natural numbers, we can proceed to develop other familiar number systems and prove that they have the properties we usually take for granted. First, using $\mathbf{N}$, we can construct a set $\mathbf{Z}$ (the integers—including 0 and negative numbers). From the integers, we can then construct a set $\mathbf{Q}$, the rational numbers; from $\mathbf{Q}$ in hand, we can then construct the real numbers $\mathbf{R}$.

Example of Induction.

Suppose we have already proven all the usual laws of arithmetic for rational numbers and wish to prove the following statement: "The sum of the first n natural numbers is $n(n + 1)/2$." We can proceed as follows. Call the statement in quotes $P(n)$, and let $f(n) = n(n + 1)/2$. Since $f(1) = 1$, the statement $P(1)$ is true. Now suppose that n is any natural number for which $P(n)$ is true. Then

$$
\begin{aligned}
\sum_{i=1}^{n+1} i &= (\sum_{i=1}^{n} i) + (n + 1) \\
&= n(n + 1)/2 + (n + 1) \quad (\text{using } P(n)) \\
&= (n + 1)(n + 2)/2 \quad (\text{after a little algebra}) \\
&= f(n + 1).
\end{aligned}
$$

Hence $P(n + 1)$ is true. By induction, the statement is true for all n. ∎

Hard exercise. In the preceding proof, I used the phrase "the first n natural numbers". What does this mean? Come up with a definition of what it means that isn't intrinsically circular.