PEANO AXIOMS FOR THE NATURAL NUMBERS AND PROOFS BY INDUCTION

The Peano axioms

The following are the axioms for the natural numbers $\mathbb{N}$. You might think of $\mathbb{N}$ as the set of integers $\{0, 1, 2, \ldots\}$, but it turns out that we need to first define the natural numbers before we can define the integers, so this really is the correct way to go about things.

The point in defining the natural numbers axiomatically is that whenever we want to prove something about them, we'll need to know precisely which "rules" we can use in our arguments. Note that, the fewer rules we have, the more certain we will be that we're not contradicting ourselves. Let's see how this goes.

Peano's axioms. There are three *primitive terms* in our system, namely $\mathbb{N}$, 0 and S. We demand that $\mathbb{N}$ is a collection of objects, which we will call *natural numbers*. We also demand that 0 is a natural number. Finally, we demand that S is a function from $\mathbb{N}$ to $\mathbb{N}$. The previous three sentences are technically axioms themselves, but I want to distinguish them from the really important items below.

The following are the axioms in our system:

(A1) For all $a \in \mathbb{N}$, $S(a) \neq 0$. In other words, 0 is not in the range of the function S.

(A2) For all $a, b \in \mathbb{N}$, if $S(a) = S(b)$, then $a = b$. In other words, S is an injective function.

(A3) If X is a subset of $\mathbb{N}$ such that

(i) $0 \in X$, and

(ii) whenever $a \in X$, then $S(a) \in X$,

then $X = \mathbb{N}$.

Here, the function S is often called a *successor function*. We'll see why below. Axiom 3 is called the *principle of mathematical induction* (PMI). Its purpose is to allow us to prove statements of the form

For all $a \in \mathbb{N}$, $P(a)$ is true.

Here, $P(a)$ is just a statement about the natural number a; for example, $0 + a = a$. But we don't even have a concept of addition defined for us yet, so we'll have to just imagine what sorts of things $P(a)$ will be for now.

Our strategy in proving statements of the above form is to take the set of natural numbers a for which $P(a)$ is true, and then use the PMI to prove that that set is the entirety of the natural numbers.

So let $X = \{a \in \mathbb{N} \mid P(a)\}$. Axiom 3 allows us to conclude that $X = \mathbb{N}$ if we can show the following.

(i) $0 \in X$, and

(ii) whenever $a \in X$, then $S(a) \in X$.

Looking at how we defined X, this is equivalent to showing the following.

(i) $P(0)$ is true, and

(ii) if $a \in \mathbb{N}$ and $P(a)$ is true, then so is $P(S(a))$.

This latter list is the recipe we'll follow when proving statements about natural numbers. The proof of part (i) is usually called the *base step*, and the proof of part (ii) is called the *inductive step*. The assumption "$P(a)$ is true" in part (ii) is called the *inductive hypothesis*. To motivate our first example, we need a very important definition.

Definition. We define the operation of *addition of natural numbers* to be "the" function $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ given by

(i) $a + 0 = a$, and

(ii) for $b \in \mathbb{N}$, $a + S(b) = S(a + b)$.

It is not clear from the wording of the above definition that it actually tells us how to add two natural numbers a and b together, because it only tells us how to produce the output $a + S(b)$ *provided that we already know how to produce the output* $a + b$. This is an example of something called an *inductive definition*. Every time we want to show that an inductive definition makes sense, we should give a proof along the following lines.

Proposition. *For every pair of natural numbers a and b, the sum $a + b$ is well defined (the formula $a + b$ makes sense).*

Proof. We proceed by induction on b. Since this is our first proof by induction, let's be a little careful. Here, the natural number a is fixed, and the statement $P(b)$ is

$$a + b \text{ is well defined.}$$

To prove the base case, let $b = 0$. By rule (i) in the definition of addition, we have

$$a + b = a + 0 = a,$$

so for the pair (a, b), there is a well defined output $a + b$. This shows that $P(b)$ is true for $b = 0$.

For the inductive step, we let $b \in \mathbb{N}$ and assume that the statement $P(b)$ is true, that is, we assume that the output $a + b$ is well defined. By rule (ii) in the definition of addition we have $a + S(b) = S(a + b)$. By our inductive hypothesis, the output $a + b$ is well defined, and since S is a function, the output $S(a + b)$ is also well defined. This shows that the output $a + S(b)$ is well defined. In other words, $P(S(b))$ is also true. By the PMI, this shows that $P(b)$ is true for every natural number b. $\square$

Okay, this result doesn't seem very exciting, but without it, the very concept of adding natural numbers together wouldn't be sound, so our work was important. Now we want to actually prove things about our newly formed operation of addition. Here is a first example.

Proposition. *For every natural number a, we have $S(a) = a + S(0)$.*

Proof. We have

$$\begin{aligned} S(a) &= S(a + 0) && \text{since } a + 0 = a \text{ by part (i) of "addition"} \\ &= a + S(0) && \text{by part (ii) of "addition". } \square \end{aligned}$$

The previous proposition allows us to get a step closer to seeing that our axiomatic definition really does coincide with our intuitive idea of natural numbers. If we denote $S(0)$ by "1", then the above result simply says that $a + 1$ is the successor of a. Yay!

Our goal throughout the rest of the document will be to prove for every pair of natural numbers a and b that $a + b = b + a$, that is, addition of natural numbers is commutative. Here is an introductory lemma.

Lemma. *For every pair of natural numbers a and b, we have $a + S(b) = S(a) + b$.*

Proof. Again, we fix a and proceed by induction on b. If $b = 0$, then

$$\begin{aligned} a + S(b) = a + S(0) &= S(a) && \text{by the previous proposition} \\ &= S(a) + 0 && \text{by part (i) of "addition"} \\ &= S(a) + b. \end{aligned}$$

Thus the statement holds for $b = 0$.

Now let $b \in \mathbb{N}$ and assume the statement holds for b, that is, we are assuming that $a + S(b) = S(a) + b$. We need to show that the statement also holds for $S(b)$, i.e., we need to prove that $a + S(S(b)) = S(a) + S(b)$. We compute that

$$\begin{aligned} a + S(S(b)) &= S(a + S(b)) && \text{by part (ii) of "addition"} \\ &= S(S(a) + b) && \text{by the inductive hypothesis} \\ &= S(a) + S(b) && \text{by part (ii) of "addition"} \end{aligned}$$

as desired. By the PMI, this shows the statement holds for every natural number b. $\square$

We require another lemma in order to prove our main theorem that addition of natural numbers is commutative.

Lemma. *For every natural number a, we have $0 + a = a$.*

Proof. This time we proceed by induction on a. If $a = 0$, then $0 + a = 0 + 0 = 0 = a$ by part (i) of the definition of addition. Thus the statement holds for $a = 0$.

Now let $a \in \mathbb{N}$ and assume that $0 + a = a$. We need to show that $0 + S(a) = S(a)$. We have

$$\begin{aligned} 0 + S(a) &= S(0 + a) && \text{by part (ii) of "addition"} \\ &= S(a) && \text{by the inductive hypothesis.} \end{aligned}$$

By the PMI, this shows the statement holds for every natural number a. □

We are now ready for the proof of the main theorem.

Theorem. *For every pair of natural numbers a and b, we have $a + b = b + a$.*

Proof. We fix a and proceed by induction on b. If $b = 0$, then

$$\begin{aligned} a + b = a + 0 &= a && \text{by part (i) of "addition"} \\ &= 0 + a && \text{by the previous lemma} \\ &= b + a. \end{aligned}$$

Thus the statement holds for $b = 0$.

Now let $b \in \mathbb{N}$ and assume that $a + b = b + a$. We need to show that $a + S(b) = S(b) + a$. We compute that

$$\begin{aligned} a + S(b) &= S(a + b) && \text{by part (ii) of "addition"} \\ &= S(b + a) && \text{by the inductive hypothesis} \\ &= b + S(a) && \text{by part (ii) of "addition"} \\ &= S(b) + a && \text{by the lemma before the last.} \end{aligned}$$

By the PMI, this shows the statement holds for every natural number b. □

We conclude our brief journey through Peano arithmetic by giving the definition of multiplication and leaving the proofs of the obvious results to the reader.

Definition. We define the operation of *multiplication of natural numbers* to be a function $\cdot\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ given by

(i) $a \cdot 0 = 0$, and

(ii) for $b \in \mathbb{N}$, $a \cdot S(b) = (a \cdot b) + a$.

Exercise. Use the Peano axioms and definitions to prove that multiplication of natural numbers is associative, that is, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all natural numbers a, b and c.

Exercise. Given natural numbers a and b, how should one define a^b inductively? Prove that the definition you came up with is actually well defined.

The well ordering principle

We now draw attention to the following axiomatic system.

There are three primitive terms $\mathbb{N}$, 0 and S. As before, $\mathbb{N}$ is a collection of objects, 0 is an element in $\mathbb{N}$ and S is a function from $\mathbb{N}$ to $\mathbb{N}$. The following are the axioms:

(A1) For all $a \in \mathbb{N}$, $S(a) \neq 0$. In other words, 0 is not in the range of the function S.

(A2) For all $a, b \in \mathbb{N}$, if $S(a) = S(b)$, then $a = b$. In other words, S is an injective function.

(A3′)
- For every element $a \in \mathbb{N}$, if $a \neq 0$, then there exists an element $b \in \mathbb{N}$ such that $a = S(b)$. (Every non-zero element is the successor of some element.)
- If X is a non-empty subset of $\mathbb{N}$, then there exists an element $a \in X$ such that, for every finite composition $S \circ S \circ \cdots \circ S$, if
$$a = S \circ S \circ \cdots \circ S(b)$$
for some element $b \in \mathbb{N}$, then $b \notin X$.

Note that Axioms 1 and 2 are the same as those in the Peano axioms. Axiom 3′ is called the *well ordering principle* (WOP). Because the well ordering principle looks so different from the principle of mathematical induction, one might believe that the above axiomatic system describes something other than the natural numbers. The following demonstrates that these two systems are, in fact, equivalent.

Theorem. *In the above system, the PMI is a theorem. Conversely, in the Peano system, the WOP is a theorem.*

Proof. We give a proof of the first statement and leave the other as an exercise. Suppose that the WOP holds. Let X be a subset of $\mathbb{N}$ such that

(i) $0 \in X$, and

(ii) whenever $a \in X$, then $S(a) \in X$.

We need to show that $X = \mathbb{N}$. For the sake of contradiction, assume that $X \neq \mathbb{N}$. Then the set $Y = \mathbb{N} - X$ is non-empty. By the WOP, there exists an element $a \in Y$ that is not of the form $S \circ S \circ \cdots \circ S(b)$ for any finite composition $S \circ S \circ \cdots \circ S$ and any $b \in Y$.

Note that $a \neq 0$, because $0 \in X$. The WOP thus guarantees the existence of an element $b \in \mathbb{N}$ for which $a = S(b)$. By the previous remarks, we cannot have $b \in Y$. It follows that $b \in X$. Condition (ii) above then implies that $a = S(b) \in X$. But $a \in Y$, so $a \notin X$. This is a contradiction. □