Peano Axioms

To present a rigorous introduction to the natural numbers would take us too far afield. We will however, give a short introduction to one axiomatic approach that yields a system that is quite like the numbers that we use daily to count and pay bills. We will consider a set, \( \mathbb{N} \), to be called the \textit{natural numbers}, that has one primitive operation that of \textit{successor} which is a function from \( \mathbb{N} \) to \( \mathbb{N} \). We will think of this function as being given by \( S(x) = x + 1 \)(this will be our definition of addition by 1). We will only assume the following rules.

1. If \( S(x) = S(y) \) then \( x = y \) (we say that \( S \) is one to one).

2. There exists exactly one element, denoted 1, in \( \mathbb{N} \) that is not of the form \( S(x) \) for any \( x \in \mathbb{N} \).

3. If \( X \subset \mathbb{N} \) is such that 1 \( \in X \) and furthermore, if \( x \in X \) then \( S(x) \in X \), then \( X = \mathbb{N} \).

These rules comprise the Peano Axioms for the natural numbers. Rule 3. is usually called the \textit{principle of mathematical induction} As above, we write \( x + 1 \) for \( S(x) \). We assert that the set of elements that are successors of successors consists of all elements of \( \mathbb{N} \) except for 1 and \( S(1) = 1 + 1 \). We will now prove this assertion. If \( z = S(S(x)) \) then since \( 1 \neq S(u) \) and \( S \) is one to one (rule 1.) \( z \neq S(1) \) and \( z \neq 1 \). If \( z \in \mathbb{N} - \{1,S(1)\} \) then \( z = S(u) \) by 2. and \( u \neq 1 \) by 1. Thus \( u = S(v) \) by 2. Hence, \( z = S(S(v)) \).

This small set of rules (axioms) allow for a very powerful system which seems to have all of the properties of our intuitive notion of natural numbers. We will now give evidence for this claim. We first show that we can use the successor function to inductively define addition. We define (as indicated above) \( x + 1 \) to be \( S(x) \) for all \( x \in \mathbb{N} \). If \( x \in \mathbb{N} \) is fixed (but arbitrary) and \( y \in \mathbb{N} \) is such that \( x + y \) has been defined then define \( x + S(y) \) to be \( S(x + y) \).

We first prove that this defines an operation on every pair of natural numbers. Let \( X \) be the set of all \( y \in \mathbb{N} \) such that \( x + y \) has been defined for all \( x \in \mathbb{N} \). Then \( 1 \in X \) and if \( y \in X \) then \( S(y) \in X \) by definition. Thus 3. implies that \( X = \mathbb{N} \).

Let us look at what this means in examples before we derive additional properties of this addition. We started with \( x + 1 = S(x) \) for all \( x \in \mathbb{N} \). We have not yet defined any other addition for all \( x \in \mathbb{N} \). Thus we must set \( x + S(1) = S(x + 1) = S(S(x)) \) for all \( x \in \mathbb{N} \).
Similarly, we must define \( x + S(S(1)) = S(x + S(1)) = S(S(x + 1)) = S(S(S(x))) \). This continues ad infinitum. We now show that this inductive definition of addition satisfies the basic rules of arithmetic.

**Theorem**  
If \( x, y, z \in \mathbb{N} \) then \( x + (y + z) = (x + y) + z \) (associative rule for addition). If \( x, y \in \mathbb{N} \) then \( x + y = y + x \) (commutative rule for addition).

Proof. We first prove the associative rule. Let \( Z \) be the set of all \( z \in \mathbb{N} \) such that \((x + y) + z = x + (y + z)\) for all \( x, y \in \mathbb{N} \). We first show that \( 1 \in Z \). In fact, \((x + y) + 1 = S(x + y) = x + S(y)\) (this is our definition). Now \( x + S(y) = x + (y + 1) \). We have thus shown that

\[(x + y) + 1 = x + (y + 1)\]

Thus, \( 1 \in Z \). Assume that \( z \in Z \) we will now show that \( S(z) \in Z \). Now we apply the definition of addition several times \((x + y) + S(z) = S((x + y) + z) = S(x + (y + z)) = x + S(y + z) = x + (y + S(z))\). Thus \( S(z) \in Z \). This implies that \( Z = \mathbb{N} \) (rule 3.).

We will next prove the commutative rule. We first show that \( 1 + x = x + 1 \) for all \( x \in \mathbb{N} \). Let \( X \) be the set of all \( x \in \mathbb{N} \) such that \( 1 + x = x + 1 \). It is clear that \( 1 \in X \). Now assume that \( x \in X \). Then \( S(x) + 1 = S(S(x)) = S(x + 1) = S(1 + x) \) (since \( x \in X \)). Now, \( S(1 + x) = 1 + S(x) \) by definition. This implies that if \( x \in X \) then \( S(x) \in X \). Thus \( X = \mathbb{N} \) by 3. At this point we have proved that \( x + 1 = 1 + x \) for all \( x \in \mathbb{N} \).

Let \( Y \) denote the set of all \( y \) such that \( x + y = y + x \) for all \( x \in \mathbb{N} \). Then we have just shown that \( 1 \in Y \). We assume that \( y \in Y \). We must show that \( S(y) \in Y \). To prove this we note that if \( x \in \mathbb{N} \) then \( x + S(y) = S(x + y) = S(y + x) \) \((y \in Y)\). Now \( S(y + x) = y + S(x) = y + (x + 1) = (y + x) + 1 \) (the associative rule). Now \((x + y) + 1 = 1 + (y + x) \) \((1 \in Y)\). Continuing,

\[1 + (y + x) = (1 + y) + x = (y + 1) + x = S(y) + x\]

Putting this all together we have \( x + S(y) = S(y) + x \). Thus if \( y \in Y \) then \( S(y) \in Y \). Hence \( Y = \mathbb{N} \) by rule 3. Hence the commutative rule has been proved.

The next step is to define multiplication. We wish to think of it as repeated addition. We first define \( 1 \cdot x = x \) for all \( x \in \mathbb{N} \). If \( u \cdot x \) has been defined then we set \( S(u) \cdot x = (u \cdot x) + x \). Thus \((1 + 1) \cdot x = x + x\).

**Theorem**  
1. If \( x, y, z \in \mathbb{N} \) then \((x \cdot y) \cdot z = x \cdot (y \cdot z)\) (associative rule for multiplication).
2. If \( x, y \in \mathbb{N} \) then \( x \cdot y = y \cdot x \) (commutative rule for multiplication).
3. If \( x, y, z \in \mathbb{N} \) then \( x \cdot (y + z) = (x \cdot y) + (x \cdot z) \) (the distributive rule for multiplication over addition).
Proof. We will prove part 3. of the theorem first by using (what else?) the principle of mathematical induction. Let \( X \) be the set of all \( x \in \mathbb{N} \) such that
\[
x \cdot (y + z) = (x \cdot y) + (x \cdot z)
\]
for all \( y, z \in \mathbb{N} \). Then \( 1 \in X \). Assume that \( x \in X \). We must show that \( S(x) \in X \). As before we will use a chain of equalities.
\[
S(x) \cdot (y + z) = x \cdot (y + z) + (y + z) \quad \text{by the definition.}
\]
Since \( x \in X \), \( x \cdot (y + z) = x \cdot y + x \cdot z \).
Thus \( S(x) \cdot (y + z) = (x \cdot y + x \cdot z) + (y + z) \). If we now apply the associative law for addition we have \((x \cdot y + x \cdot z) + (y + z) = ((x \cdot y + x \cdot z) + y) + z\). Inside the first set of braces we apply the commutative rule for addition and have
\[
((x \cdot y + x \cdot z) + y) + z = (y + (x \cdot y + x \cdot z)) + z = ((y + x \cdot y) + x \cdot z) + z \quad \text{by the associative law of addition applied inside the parentheses.}
\]
We now apply the commutative law of addition within the parentheses and the associative law of addition to find
\[
((y + x \cdot y) + x \cdot z) + z = ((x \cdot y) + y) + ((x \cdot z) + z).\]
By definition the last expression is \( S(x) \cdot y + S(x) \cdot z \). Thus \( Z = \mathbb{N} \) and the distributive law is proved.

We now prove the commutative rule for multiplication by induction. Let \( Y = \{ y \in \mathbb{N}; x \cdot y = x \cdot y \quad \text{for all } x \in \mathbb{N} \} \). We first show that \( 1 \in Y \). That is to say we must show that \( 1 \cdot x = x \cdot 1 \) for all \( x \in \mathbb{N} \). Since \( 1 \cdot x = x \) for all \( x \in \mathbb{N} \), we must show that \( x \cdot 1 = x \) for all \( x \in \mathbb{N} \). We show this by showing that the set \( W \) of elements \( x \in \mathbb{N} \) such that \( x \cdot 1 = x \) is equal to \( \mathbb{N} \). We first observe that \( 1 \in W \). Assume that \( x \in W \) then we must show that \( S(x) \in W \). Now \( S(x) \cdot 1 = x \cdot 1 + 1 \) by the definition. Since \( x \in W \), \( x \cdot 1 = x \). Thus \( x \cdot 1 + 1 = x + 1 = S(x) \). Thus \( W = \mathbb{N} \). This implies that \( 1 \in Y \). Now assume that \( y \in Y \) we must show that \( S(y) \in Y \). Now \( S(y) \cdot x = (y \cdot x) + x = (x \cdot y) + x \). Also \( x \cdot S(y) = x \cdot (y + 1) = (x \cdot y) + (x \cdot 1) = (x \cdot y) + x \). Thus \( S(y) \cdot x = x \cdot S(y) \).

Last we prove the associative rule. Let \( Z \) be the set of all \( x \in \mathbb{N} \) such that \( x \cdot (y \cdot z) = (x \cdot y) \cdot z \) for all \( y, z \in \mathbb{N} \). Then \( 1 \in Z \). Since \( 1 \cdot (y \cdot z) = y \cdot z \) and \( (1 \cdot y) \cdot z = y \cdot z \). Assume that \( x \in Z \). Then
\[
S(x) \cdot (y \cdot z) = x \cdot (y \cdot z) + (y \cdot z) = ((x \cdot y) \cdot z) + (y \cdot z) = (z \cdot (x \cdot y)) + (z \cdot y) = z \cdot ((x \cdot y) + y) = z \cdot (S(x) \cdot y) = (S(x) \cdot y) \cdot z.
\]

This completes the proof.

We will usually write \( xy = x \cdot y \).

We note that there is a specific structure that we have followed in our proofs. We have an assertion for every natural number. If the assertion is true for 1 and whenever it is true for \( x \) it is true for \( x + 1 \) then it is true for all natural numbers. Let us give an example of this approach.

**Theorem** If \( x, y, z \in \mathbb{N} \) and \( x + y = x + z \) then \( y = z \). *(The cancellation rule for addition.)*

Proof. The assertion for \( x \) is that if \( y, z \in \mathbb{N} \) and if \( x + y = x + z \) then \( y = z \). If \( x = 1 \) then the assertion says that if \( 1 + y = 1 + z \) then \( y = z \). The commutative rule says that we
may formulate this as if \( y + 1 = z + 1 \) then \( y = z \). This says that if \( S(y) = S(z) \) then \( y = z \).
This is true since it is rule 1. above. Now suppose that we have shown, for \( x \), that if \( x + y = x + z \) then \( y = z \). Suppose that \( S(x) + y = S(x) + z \). Then \( y + S(x) = z + S(x) \). Thus \( S(y + x) = S(z + x) \). Hence \( y + x = z + x \) by rule 1. But then \( x + y = x + z \). Hence \( y = z \).
The theorem is therefore true.

The associative rule for addition allows us to introduce an order on \( \mathbb{N} \). If \( x, y \in \mathbb{N} \) then we say that \( x > y \) (or \( y < x \)) if there exists \( u \in \mathbb{N} \) such that \( x = y + u \). We note that if \( x > y \) and \( y > z \) then \( x > y \). Indeed, since \( x > y \) we have \( x = y + u \) with \( u \in \mathbb{N} \). Since \( y > z \) we have \( y = z + v \) with \( v \in \mathbb{N} \). Thus \( x = y + u = (z + v) + u = z + (v + u) \) so \( x > z \).

**Theorem** \textit{If} \( x, y \in \mathbb{N} \text{then precisely one of} \ x > y, x = y \text{or} \ x < y \text{is true.} \text{(This is called trichotomy.)} \}

Proof. If \( x = 1 \) then either \( y = 1 \) or \( y = S(u) \) for some \( u \in \mathbb{N} \) by rule 2. Thus \( y = 1 + u \).
Hence, if \( y \in \mathbb{N} \text{then \( y = 1 \) or \( y > 1 \).} \text{We will prove the assertion by induction on} \ x \text{. If} \ x = 1 \text{then we have shown that trichotomy is true for any element} \ y \in \mathbb{N} \text{. Suppose that} \ u \text{is such that if} \ v \in \mathbb{N} \text{then precisely one of} \ u > v, u = v \text{or} \ u < v \text{is true.} \text{We now consider} \ x = S(u) \text{and} \ y \in \mathbb{N} \text{. We must show that precisely one of the three alternatives is true. If} \ y = 1 \text{then if we interchange the role of} \ x \text{and} \ y \text{we see that trichotomy is true for the pair} \ x, y \text{.} \text{We may thus assume that} \ y = S(v) \text{for some} \ v \in \mathbb{N} \text{. Now} \ u, v \text{satisfy trichotomy. If} \ u > v \text{then there exists} \ w \in \mathbb{N} \text{such that} \ u = v + w \text{. Thus} \ x = S(u) = S(v + w) = (v + w) + 1 = (v + 1) + w = S(v) + w = y + w \text{. Hence if} \ u > v \text{then} \ x > y \text{. If} \ u = v \text{then} \ x = S(u) = S(v) = y \text{. If} \ u < v \text{then} \ v > u \text{so we can use the argument above to show that} \ x = S(u) < S(v) = y \text{. If} \ x < y \text{and} \ x = y \text{then} x = y + u \text{and thus} \ x = x + u \text{. If we add} \ 1 \text{to both sides of this equation we find that} \ x + 1 = x + (u + 1) \text{. But then the cancellation theorem implies that} \ 1 = S(u) \text{which contradicts rule 2. above.} \text{The other alternatives are handled in the same way.} \}

We now apply all of this material to prove the following theorem. In this proof we will use the method of \textit{proof by contradiction}. This is a principle that says that if a statement, \( S \), implies something false then \( S \) is false. Thus the statement that all natural numbers are even (of the form \( u + u = 2u \) for some \( u \in \mathbb{N} \)) implies that \( 1 = u + u \text{ for some} \ u \in \mathbb{N} \). If \( u = 1 \text{ then we have} \ 1 = 1 + 1 = S(1) \text{ which contradicts rule 1. above.} \text{If} u \neq 1 \text{ then rule 2. says that} u = S(v) \text{ for some} \ v \in \mathbb{N} \text{ thus} \ 1 = u + S(v) = S(u + v) \text{ which contradicts 2. Thus the assertion that all natural numbers are even is false.} \text{(Cancellation rule for multiplication).} \}
Proof. The assertion is true for \( x = 1 \) since \( 1y = y \) for all \( y \in \mathbb{N} \). Suppose that \( xy = xz \) and \( y \neq z \). Then either \( y > z \) or \( y < z \). Interchanging the role of \( y \) and \( z \) we may assume that \( y > z \). But then \( y = z + u \) for some \( u \in \mathbb{N} \). Thus \( x(z + u) = xz \). Thus we have \( xz + xu = xz \). If we add 1 to both sides of this equation we have \( xz + (xu + 1) = xz + 1 \). As above we see that \( 1 = S(xu) \) which contradicts rule 2.

**Theorem** If \( n \in \mathbb{N} \) then \( n \geq 1 \). If \( n, m \in \mathbb{N} \) and if \( m > n \) then \( m \geq n + 1 \).

**Proof** If \( n \in \mathbb{N} \) then if \( n \neq 1 \) then \( n = k + 1 \) with \( k \in \mathbb{N} \) (rule 2). Thus if \( n \in \mathbb{N} \) then either \( n = 1 \) or \( n > 1 \). If \( n \in \mathbb{N} \) and if \( m > n \) then \( m = n + k \). Now \( k \geq 1 \) thus \( n + k \geq n + 1 \). The result now follows from Trichotomy.

**Theorem** *(The Least Element Principle)* If \( S \subseteq \mathbb{N} \) and \( S \neq \emptyset \) then \( S \) has a least element. That is, there exists \( n \in S \) such that if \( m \in S \) then \( m \geq n \).

**Proof** Assume that \( S \) is a subset of \( \mathbb{N} \) that has no least element. Let \( S' = \mathbb{N} - S \). We show that \( S' = \mathbb{N} \) which implies \( S = \emptyset \). Let

\[
T = \{ n \in \mathbb{N} : \text{if } 1 \leq m \leq n \text{ then } m \in S' \}.
\]

If \( T = \mathbb{N} \) then \( S' = \mathbb{N} \). We will therefore prove \( T = \mathbb{N} \). If \( 1 \in S \) the previous theorem implies that 1 is the least element of \( \mathbb{N} \) hence of \( S \). Thus since \( S \) has no least element \( 1 \in S' \). Hence \( \{1\} \subseteq S' \) so \( 1 \in T \). Assume that \( n \in T \). Then if \( m \in S \) then by trichotomy \( m > n \) (all of the elements \( p \) with \( 1 \leq p \leq n \) are not in \( S \). Hence \( m \geq n + 1 \) be the previous theorem. If \( n + 1 \in S \) then it would be a minimal element. Hence \( n + 1 \in S' \). The previous theorem now implies that \( n + 1 \in T \). Hence \( T = \mathbb{N} \).

At this point we hope that you are convinced that one can give a rigorous underpinning to a system that we would like to call the natural numbers. We will not pursue this approach any further, since the full development of a system like the real numbers from the Peano axioms would take at least a full quarter course.