Definition: (addition) Let $m, n \in \mathbb{N}$.

Let $f : \mathbb{N} \to \mathbb{N}$, $f(n) = n^+$.

We induce, for each $m \in \mathbb{N}$,

a function $g_m : \mathbb{N} \to \mathbb{N}$

from the Recursion Theorem

such that

1) $g_m(0) = m$

2) $g_m(n^+) = f(g_m(n))$

$$= (g_m(n))^+.$$

Then we *define*

$$\boxed{m + n = g_m(n)} \quad \forall\, n \in \mathbb{N}$$

Theorem: 1) Addition on $\mathbb{N}$ is associative.

2) Addition on $\mathbb{N}$ is commutative.

proof: Start 1) : We want to show that, $\forall\, m, n, k \in \mathbb{N}$,

$$(m+n)+k = m+(n+k)$$

Use induction on k.

Let

$$S = \{k \in \mathbb{N} \mid (m+n)+k = m+(n+k)\}.$$

Step 1: OES If $k=0$, the statement is

$$(m+n)+0 = m+(n+0)$$

$$(m+n)+0 = g_{m+n}(0) = m+n$$

Similarly, $n+0 = g_n(0) = n$, so we get

$$(m+n)+0 = m+n = m+(n+0)$$

So OES!

Step 2: Induction

We assume $k \in S$; that is,

$$(m+n)+k = m+(n+k)$$

We want to deduce from this

that $(m+n)+k^+ = m+(n+k^+)$,

so $k^+ \in S$. By the Principle

of Mathematical Induction,

we will have $S = \mathbb{N}$.

Then

$$\left.\begin{aligned}(m+n)+k^+ &= g_{m+n}(k^+)\\ &= (g_{m+n}(k))^+\end{aligned}\right\}\ \text{definition of } g$$

$$\begin{aligned}
&= ((m+n)+k)^+\\
\text{inductive assumption}\quad &= (m+(n+k))^+\\
&= (g_m(n+k))^+\\
&= g_m((n+k)^+)\\
&= g_m((g_n(k))^+)\\
&= g_m((g_n(k^+)))\\
&= g_m(n+k^+)\\
&= m+(n+k^+)
\end{aligned}$$

We have shown

1) $0 \in S$

2) If $k \in S$, then $k^+ \in S$

So by the Principle of Mathematical Induction, $S = \mathbb{N}$, and so

$$(m+n)+k = m+(n+k)$$

$\forall\ m, n, k \in \mathbb{N}$.

We've proved associativity, now for commutativity, 2) !

Again going to use the principle of mathematical induction - eventually.

Step 1: $0+m = m+0 \quad \forall \, m \in \mathbb{N}$

Note that

$$m+0 = g_m(0) = m.$$

We want to show that

$$0+m = m \quad \forall \, m \in \mathbb{N}.$$

Then we'll have step 1.

More induction:

Let $T = \{m \in \mathbb{N} \mid 0+m=m\}$.

$\underline{0 \in T}$ $\quad 0+0 = g_0(0) = 0$

$\underline{\text{If } m \in T,\ m^+ \in T}$

If $m \in T$, then $0+m=m$.

$$\begin{aligned} 0+m^+ &= g_0(m^+) \\ &= g_0(m)^+ \\ &= (0+m)^+ \quad \text{$0+m=m$ by induction} \\ &= m^+ \end{aligned}$$

By the Principle of Mathematical Induction, $T = \mathbb{N}$, so

$0 + m = m \quad \forall \ m \in \mathbb{N}$, and

$0 + m = m = m + 0$ ✓

Step 2: Show that for any fixed m, $m^+ + n = (m+n)^+ \quad \forall \ n \in \mathbb{N}$.

Again use induction:

let

$T_m = \{ n \in \mathbb{N} \mid m^+ + n = (m+n)^+ \}$

$0 \in T_m$ $\quad m^+ + 0 = m^+$ by definition

$(m+0)^+ = m^+$ by definition,

So $\quad m^+ + 0 = (m+0)^+$

If $n \in T_m$, then $n^+ \in T_m$

We assume that

$m^+ + n = (m+n)^+$

Show

$m^+ + n^+ = (m+n^+)^+$

Then

$$
\begin{aligned}
m^+ + n^+ &= g_{m^+}(n^+) \\
&= (g_{m^+}(n))^+ \\
&= (m^+ + n)^+ \\
&= ((m+n)^+)^+ \\
&= (g_m(n)^+)^+ \\
&= (g_m(n^+))^+ \\
&= (m + n^+)^+
\end{aligned}
$$

inductive step

✓

By the Principle of Mathematical Induction, $T_m = \mathbb{N}$, so

$$m^+ + n = (m+n)^+$$

$\forall\ n \in \mathbb{N}$.

Step 3: Show $m+n = n+m \ \forall\ n, m \in \mathbb{N}$.

Use Step 2 and induction on m.

Let $n \in \mathbb{N}$ and let

$$S = \{ m \in \mathbb{N} \mid n+m = m+n \}.$$

$0 \in S$ $\quad m=0, \quad n+0=0+n$, done

by Step 1 ◡̈

If $m \in S$, then $m^+ \in S$

We assume $n+m=m+n$.

Show $n+m^+ = m^+ + n$.

So $m^+ + n = (m+n)^+$ (Step 2)

inductive step $= (n+m)^+$

$= (g_n(m))^+$

$= g_n(m^+)$

$= n+m^+$

By the Principle of Mathematical Induction, $S = \mathbb{N}$, so

$$m+n = n+m \quad \forall\ n,m \in \mathbb{N}$$

$\square$

Definition: (multiplication) Let $m \in \mathbb{N}$ and define $f_m : \mathbb{N} \to \mathbb{N}$,

$f_m(n) = m + n$. Then by the Recursion Theorem,

$\exists \; g_m : \mathbb{N} \to \mathbb{N}$ with

1) $g_m(0) = 0$

2) $g_m(n^+) = f_m(g_m(n))$

$$= g_m(n) + m$$

Set $\boxed{m \cdot n = g_m(n)}$

Check this works . . .

$$g_m(1) = f_m(g_m(0))$$

$$= g_m(0) + m$$

$$= m$$

$$g_m(2) = f_m(g_m(1))$$

$$= g_m(1) + m$$

$$= m + m$$

looks like it does what it is supposed to do!

Theorem: (multiplication properties)

Let $m, n, k \in \mathbb{N}$.

Then

1) $(m \cdot n) \cdot k = m \cdot (n \cdot k)$

(associativity)

2) $m \cdot n = n \cdot m$

(commutativity)

3) $m \cdot (n + k) = m \cdot n + m \cdot k$

(distributivity over addition)

Proof: Try it! $\square$

Definition: (exponentiation) Let $m \in \mathbb{N}$.

Let $f_m : \mathbb{N} \to \mathbb{N}$,

$f_m(n) = m \cdot n \quad \forall\, n \in \mathbb{N}$.

Then by the Recursion Theorem, $\exists\ g_m : \mathbb{N} \to \mathbb{N}$ such that

1) $g_m(0) = 1$

2) $g_m(n^+) = f_m(g_m(n))$

$= m \cdot g_m(n)$

$$\boxed{\text{Set} \quad m^n = g_m(n)}$$

Theorem: (order) Let $m, n \in \mathbb{N}$.

Then either

$m \in n$, $n \in m$, or $n = m$.

proof: Lots of induction!

Let $n \in \mathbb{N}$. Let

$$S_n = \{ m \in \mathbb{N} \mid \text{either } m \in n, n \in m, \text{ or } n = m \}.$$

Let

$$S = \{ n \in \mathbb{N} \mid S_n = \mathbb{N} \}.$$

Use induction to show

$S = \mathbb{N}$.

Step 1: $0 \in S$

We want to show that

$$S_0 = \mathbb{N}.$$

Show this via induction!

$0 \in S_0$ $\quad 0 = 0$, so $0 \in S_0$.

$m \in S_0 \Rightarrow m^+ \in S_0$

Since $m \in S_0$, either

- $m = 0$, in which case

$$m^+ = 0^+ = \emptyset^+ = \emptyset \cup \{\emptyset\}$$
$$= \{\emptyset\}$$

$$\Rightarrow \emptyset \in m^+.$$

- $0 \in m$, in which case,

$$m^+ = m \cup \{m\}, \text{ so}$$
$$0 \in m \subseteq m \cup \{m\} = m^+$$

- $m \in 0$, impossible since $0 = \emptyset$ has no elements ✓

By the Principle of mathematical Induction, $S_0 = \mathbb{N}$, so $0 \in S$.

Step 2: If $n \in S$, then $n^+ \in S$

If $n \in S$, this means $S_n = \mathbb{N}$. We want to show $S_{n^+} = \mathbb{N}$.

We'll do this by induction(!)

$0 \in S_{n^+}$ From step 1, we know $\underline{0 \in n^+}$ since $n^+ \in 0$ is impossible and $0 = n^+$ is impossible since we proved (Peano Axiom) that $0 \neq n^+$ for any $n \in \mathbb{N}$.

Since $S_0 = \mathbb{N}$, $0 \in n^+$.

If $m \in S_{n^+}$, then $m^+ \in S_{n^+}$

We know $m \in S_{n^+}$, so either

- $m = n^+$, in which case,

  $m^+ = m \cup \{m\}$, so

  $n^+ = m \in m \cup \{m\} = m^+$

or

- $n^+ \in m$, in which case,

  $n^+ \in m^+$ as above

or

- $m \in n^+$.

We know $S_n = \mathbb{N}$ by induction

Either $*)$ $m^+ = n$, so

then $m^+ \in n^+$

or

*) $n \in m^+$. We also know $m \in n^+$.

$n = m$ or $n \in m$

$m = n$ or $m \in n$

- $n = m$, $m = n$ $\Rightarrow m^+ = n^+$
- $n = m$, $m \in n$ impossible
- $n \in m$, $m \in n$ impossible
- $n \in m$, $m = n$ impossible

*) $m^+ \in n$. Then

$n^+ = n \cup \{n\}$, so

$m^+ \in n \subseteq n^+ \Rightarrow$

$m^+ \in n^+$

So by induction, $S_{n+} = \mathbb{N}$,

which shows, yet again by induction, that

$$S = \{ n \in \mathbb{N} \mid S_n = \mathbb{N} \}$$

is equal to $\mathbb{N}$.

$\square$