Natural Numbers II - Cancellation and multiplication

So far, we've defined $+$ on $\mathbb{N}$ and developed some of its basic properties, especially commutativity and associativity.

<u>Cancellation Law</u> (for $+$ on $\mathbb{N}$)

For all $n, m, k \in \mathbb{N}$, if $n+k = m+k$, then $n=m$.

[To compensate for not doing subtraction, which properly needs negative numbers.]

<u>proof:</u> We proceed by induction on k.

<u>Base step:</u> $(k=0)$ If $n, m \in \mathbb{N}$ and $n+0 = m+0$, then
$$n = n+0 = m+0 = m.$$

<u>I.H.:</u> For all $n, m \in \mathbb{N}$ and some $k \geq 0$, we have $n+k = m+k \Rightarrow n=m$.

<u>I.S.:</u> We need to show that if $n+S(k) = m+S(k)$, then $n=m$.

Suppose $\underset{\substack{\| \\ S(n+k)}}{n+S(k)} \overset{\xleftarrow{\text{by defn of } +}}{=} \underset{\substack{\| \\ S(m+k)}}{m+S(k)}$, but then, by axiom (5) of our augmented Peano axioms, we have $n+k = m+k$.

By the IH, it follows that $n=m$.

$\therefore$ By induction, the Cancellation Law hold for $+$ on $\mathbb{N}$. //

Def'n: $\cdot$ on $\mathbb{N}$ is a two-place function given by

(1) For all $n \in \mathbb{N}$, $n \cdot 0 = 0$.

(2) For all $n, k \in \mathbb{N}$, $n \cdot S(k) = (n \cdot k) + n$.

Distributive Law: For all $n, m, k \in \mathbb{N}$, $n \cdot (m+k) = (n \cdot m) + (n \cdot k)$.

proof: By induction on k.

Base step: $(k=0)$ For any $n, m \in \mathbb{N}$,

$$\begin{aligned} n \cdot (m+0) &= n \cdot m && (\text{def'n of } +) \\ &= (n \cdot m) + 0 && (\text{—''—}) \\ &= (n \cdot m) + (n \cdot 0) && (\text{def'n of } \cdot) \quad \checkmark \end{aligned}$$

I.H.: For all $n, m \in \mathbb{N}$ and some $k \geq 0$, $n \cdot (m+k) = (n \cdot m) + (n \cdot k)$.

I.S.: We need to show that $n \cdot (m + S(k)) = (n \cdot m) + (n \cdot S(k))$.

$$\begin{aligned} n \cdot (m + S(k)) &\overset{\text{def'n of } +}{=} n \cdot (S(m+k)) \overset{\text{def'n of } \cdot}{=} n \cdot (m+k) + n \\ &\overset{\text{Dist. Law (IH)}}{=} ((n \cdot m) + (n \cdot k)) + n \overset{\text{Associativity}}{=} (n \cdot m) + ((n \cdot k) + n) \\ &\overset{\text{def'n of } \cdot}{=} (n \cdot m) + (n \cdot S(k)) \quad \checkmark \end{aligned}$$

$\therefore$ By induction, the Distributive Law holds for $+$ & $\cdot$ on $\mathbb{N}$. //

Lemma: For all $n \in \mathbb{N}$, $n \cdot 1 = n$

proof: $n \cdot 1 = n \cdot S(0) = (n \cdot 0) + n = 0 + n = n$
& this works for all n. //

Theorem: $\cdot$ is associative, ie for all $n, m, k \in \mathbb{N}$, $(n \cdot m) \cdot k = n \cdot (m \cdot k)$.

proof: By induction on k.

B.S.: $(k = 0)$ For any $n, m \in \mathbb{N}$, $(n \cdot m) \cdot 0 = 0 = n \cdot 0 = n \cdot (m \cdot 0)$. ✓

I.H.: For any $n, m \in \mathbb{N}$ and some $k \geq 0$, $(n \cdot m) \cdot k = n \cdot (m \cdot k)$.

I.S.: We need to show that for any $n, m \in \mathbb{N}$, $(n \cdot m) \cdot S(k) = n \cdot (m \cdot S(k))$.

$$
\begin{aligned}
(n \cdot m) \cdot S(k) &= ((n \cdot m) \cdot k) + (n \cdot m) && \text{Def'n of } \cdot \\
&= (n \cdot (m \cdot k)) + (n \cdot m) && \cancel{\text{Dist. Law}}\text{. I.H.} \\
&= n \cdot ((m \cdot k) + m) && \text{Dist. Law.} \\
&= n \cdot (m \cdot S(k)) \quad ✓ && \text{Def'n of } \cdot
\end{aligned}
$$

$\therefore$ By induction, the Distributive Law holds. //

Theorem: $\cdot$ is commutative, ie for all $n, m \in \mathbb{N}$, $n \cdot m = m \cdot n$.

proof: Exercise! You can use the proof that $+$ is commutative as a model (to some extent). //

Theorem: (Cancellation Law for $\cdot$)

For all $n, m \in \mathbb{N}$ and all $k \geq 1$, if $n \cdot k = m \cdot k$, then $n = m$.

proof: By induction on k.

B.S.: $(k=1)$ For any $n, m \in \mathbb{N}$, $n = n \cdot 1 = m \cdot 1 = m$, so $n = m$.

I.H.: For any $n, m \in \mathbb{N}$ and some $k \geq 1$, $n \cdot k = m \cdot k \Rightarrow n = m$.

I.S.: We need to show that $n \cdot S(k) = m \cdot S(k) \Rightarrow n = m$.

Suppose $n \cdot S(k) = m \cdot S(k)$

$$\begin{array}{ccc} n \cdot S(k) & = & m \cdot S(k) \\ \parallel & & \parallel \\ (n \cdot k) + n & & (m \cdot k) + m \\ \parallel & & \parallel \\ \cancel{n \cdot (k+n)} & & \\ (n \cdot k) + (n \cdot 1) & & (m \cdot k) + (m \cdot 1) \\ \parallel & & \parallel \\ n \cdot (k+1) & & m \cdot (k+1) \end{array}$$

& now what? Think about it before next time!