Natural Numbers

Notation. *We will use* $\mathbb{N}$ *to denote natural numbers.* [1]

Definition of $\mathbb{N}$

- Axiom 1. $1 \in \mathbb{N}$;
- Axiom 2. For each $x \in \mathbb{N}$ there exists exactly one $x' \in \mathbb{N}$, called the "successor" of x;
- Axiom 3. $\forall x \in \mathbb{N}$, $x' \neq 1$;
- Axiom 4. If $x' = y'$ then $x = y$;
- Axiom 5. (Axiom of Induction): Let $\mathfrak{M} \subseteq \mathbb{N}$ satisfy

    1. $1 \in \mathfrak{M}$;
    2. If $x \in \mathfrak{M}$ then $x' \in \mathfrak{M}$.

    Then $\mathfrak{M} = \mathbb{N}$.

Remark 1. John von Neumann suggested the following construction of $\mathbb{N}$:

Define

$$1 := \{\varnothing\}, \qquad 2 := 1 \cup \{1\}, \qquad 3 := 2 \cup \{2\}, \ldots \tag{1}$$

Note that this does not establish the existence of $\mathbb{N}$. The existence of $\mathbb{N}$ is in fact an axiom:

We accept that there is at least one set S satisfying

i. $1 \in S$;

ii. $x \in S \Longrightarrow x \cup \{x\} \in S$.

Now let W be a collection of all such sets. Define $\mathbb{N} := \cap_{S \in W} S$.

Theorem 2. $x' \neq x$.

Proof. Let $\mathfrak{M} := \{x \in \mathbb{N} | \, x' \neq x\}$. Then by Axiom 3, $1 \in \mathfrak{M}$. Now we show that $x \in \mathfrak{M} \Longrightarrow x' \in \mathfrak{M}$. Once this is done the conclusion follows from Axiom 5.

Assume there is $x \in \mathfrak{M}$ such that $x' \notin \mathfrak{M}$. That is $x' \neq x$, but $(x')' = x'$. However by Axiom 4 we have $(x')' = x' \Longrightarrow x' = x$. Contradiction. □

Lemma 3. *If* $x \neq y$ *then* $x' \neq y'$.

Exercise 1. Prove Lemma 3.

[1]. *There is much debate whether* 0 *should be included in natural numbers. My personal opinion is that* 0 *is definitely not as "natural" as 1,2,3,... and therefore shouldn't be included. Thus in this note* 0 *does not belong to* $\mathbb{N}$.

Lemma 4. *If $x \neq 1$, then there is exactly one u such that $u' = x$.*

Exercise 2. Prove Lemma 4 (Hint: Let $\mathfrak{M} = \{1\} \cup \{\text{all numbers with this property}\}$.

Addition

We need to define $x + y$ for every pair of $x, y \in \mathbb{N}$.

- First define this for $y = 1$: $x + 1 := x'$;
- Now assume that this is done for y. We define $x + y' := (x + y)'$. This way addition is defined for each ordered pair (x, y).

Theorem 5. *The way of defining $x + y$ such that $x + 1 = x'$, $x + y' = (x + y)'$ is unique.*

Proof. Let $+, \oplus$ be two ways of defining addition. Fix an arbitrary $x \in \mathbb{N}$, let $\mathfrak{M} = \{y \in \mathbb{N} | \, x + y = x \oplus y\}$. Then $1 \in \mathfrak{M}$. Now for every $y \in \mathfrak{M}$, we have

$$x + y' = (x + y)' = (x \oplus y)' = x \oplus y'. \tag{2}$$

By Axiom of induction $\mathfrak{M} = \mathbb{N}$. Thus such definition, if it exists, is unique.

Similarly we can prove that such definition indeed exists. Left as exercise. □

Exercise 3. Use induction to prove that $x + y$ can be defined for all $x, y \in \mathbb{N}$.

Theorem 6. $(x + y) + z = x + (y + z)$.

Proof. For any $x, y \in \mathbb{N}$, let $\mathfrak{M} := \{z \in \mathbb{N} | \, (x + y) + z = x + (y + z)\}$. Then we check

$$(x + y) + 1 = (x + y)' = x + y' = x + (y + 1) \tag{3}$$

so $1 \in \mathfrak{M}$.

For every $z \in \mathfrak{M}$, we have

$$(x + y) + z' = [(x + y) + z]' = [x + (y + z)]' = x + (y + z)' = x + (y + z'). \tag{4}$$

Thus ends the proof. □

Theorem 7. $x + y = y + x$.

Proof. Fix any $y \in \mathbb{N}$. First we prove $1 + y = y + 1$. Let $\mathfrak{M} := \{y \in \mathbb{N} | \, 1 + y = y + 1\}$. We have $1 + 1 = 1 + 1$ so $1 \in \mathfrak{M}$. Now if $y \in \mathfrak{M}$, we check

$$1 + y' = 1 + (y + 1) = (1 + y) + 1 = (y + 1) + 1 = y' + 1 \tag{5}$$

so $y' \in \mathfrak{M}$ too. Consequently $1 + y = y + 1$ for all $y \in \mathbb{N}$.

Now we prove that if $x + y = y + x$, then $x' + y = y + x'$. We have

$$x' + y = (x + 1) + y = x + (1 + y) = x + (y + 1) = (x + y) + 1 = (y + x) + 1 = y + (x + 1) = y + x'. \tag{6}$$

Thus ends the proof. □

Lemma 8. *If $y \neq z$ then $x + y \neq x + z$. Or equivalently $x + y = x + z \Longrightarrow y = z$.*

Exercise 4. Prove Lemma 8.

Ordering

Theorem 9. *For any $x, y \in \mathbb{N}$, exactly one of the following is true:*

i. $x = y$;

ii. *There is exactly one $u \in \mathbb{N}$ such that $x = y + u$;*

iii. *There is exactly one $v \in \mathbb{N}$ such that $y = x + v$.*

Proof.

First we prove that for any $x, y \in \mathbb{N}$, at most one of the three holds. Three cases:

- $x = y$ and $x = y + u$ hold. Then we have $y = y + u \Longrightarrow y + 1 = y' = (y + u)' = y + u'$ which by Lemma 8 gives $1 = u'$ which contradicts Axiom 3.
- $x = y$ and $y = x + v$ hold. Similar to the above case.
- $x = y + u$ and $y = x + v$ hold. Then we have $x + v = (y + u) + v = y + (u + v)$ which by similar argument as above contradicts Axiom 3.

Fix an arbitrary $x \in \mathbb{N}$. We prove that for any $y \in \mathbb{N}$, at least one of the above holds.

Let $\mathfrak{M} := \{y \in \mathbb{N} |$ exactly one of $x = y, x = y + u, y = x + v\}$ holds.

- $1 \in \mathfrak{M}$. There are two cases.
    - $x = 1$. Then $x = y$.
    - $x \neq 1$. Then by Lemma 4 there is $u \in \mathbb{N}$ such that $x = u'$. Thus $x = u + 1 = 1 + u = y + u$.
- If $y \in \mathfrak{M}$ then $y' \in \mathfrak{M}$. There are three cases.
    - $x = y$. Then $y' = y + 1 = x + 1$ and therefore $y' \in \mathfrak{M}$.
    - $x = y + u$. Then there are two cases.
        - $u = 1$. Then $x = y'$.
        - $u \neq 1$. Then by Lemma 4 there is $v \in \mathbb{N}$ such that $u = v'$. This gives

          $$x = y + u = y + v' = (y + v)' = y' + v. \tag{7}$$

          So $y' \in \mathfrak{M}$.
    - $y = x + v$. Then

      $$y' = (x + v)' = x + v' \tag{8}$$

and $y' \in \mathfrak{M}$.

Thus $y' \in \mathfrak{M}$ and the proof ends. □

Definition 10. (Ordering) *If $x = y + u$, denote $x > y$; If $y = x + v$, denote $x < y$.*

Theorem 11. *For any given x, y, we have exactly one of the following: $x = y, x < y, x > y$.*

Exercise 5. If $x < y$ then $y > x$.

Definition 12. *Define $x \geqslant y$ as $x > y$ or $x = y$. Define $x \leqslant y$ as $x < y$ or $x = y$.*

Exercise 6. If $x \leqslant y$ then $y \geqslant x$; If $x \geqslant y$ then $y \leqslant x$.

Exercise 7. If $x \leqslant y$ and $y \leqslant x$ then $x = y$.

Exercise 8. If $x < y, y < z$ then $x < z$; If $x \leqslant y, y < z$ then $x < z$; If $x < y, y \leqslant z$ then $x < z$; If $x \leqslant y, y \leqslant z$ then $x \leqslant z$.

Exercise 9. If $x > y, z > u$ then $x + z > y + u$.

Exercise 10. If $x < y$, then $x + 1 \leqslant y$.

Theorem 13. *Let $A \subseteq \mathbb{N}$ be nonempty. Then there is a unique least element, that is $a \in A$ such that for all $b \in A$, $a \leqslant b$.*

Proof.

- If $1 \in A$ then 1 is the least element, since for all $x \in \mathbb{N}$, $x \neq 1$, there is u such that $x = u' = 1 + u > 1$.
- If $1 \notin A$, let $\mathfrak{M} := \{x \in \mathbb{N} | \forall b \in A, x \leqslant b\}$. Now if for every $x \in \mathfrak{M}$ we have $x + 1 \in \mathfrak{M}$, by the Axiom of induction $\mathfrak{M} = \mathbb{N}$ and $A = \varnothing$. Contradiction. Thus there is $a \in \mathfrak{M}$ satisfying:

$$a \in \mathfrak{M}, a + 1 \notin \mathfrak{M}. \tag{9}$$

  We claim $a \in A$. Since otherwise, by definition of $\leqslant$, for every $b \in A$ there must hold $a < b$ which implies $a + 1 \leqslant b$. Consequently $a + 1 \in \mathfrak{M}$. Contradiction.

  Now $a \in \mathfrak{M} \Longrightarrow \forall b \in A, a \leqslant b$ so a is a least element. Uniqueness follows from $a \leqslant b, b \leqslant a \Longrightarrow a = b$. □

Multiplication

Theorem 14. *To every pair of $x, y \in \mathbb{N}$, we can assign in exactly one way a $z \in \mathbb{N}$, denoted $x \cdot y$ (or $x\, y$ when no confusion may arise), such that*

i. $x \cdot 1 = x$ *for every* x;

ii. $x \cdot y' = x \cdot y + x$ *for every* x *and every* y.

Proof. Left as exercise. □

Exercise 11. $x \cdot y = y \cdot x$.

Exercise 12. $x\,(y+z)=x\,y+x\,z$.

Exercise 13. $(x\,y)\,z=x\,(y\,z)$.

Exercise 14. If $x>y(=y,<y)$ then $x\,z>y\,z(=y\,z,<y\,z)$. If $x\,y>y\,z(=y\,z,<y\,z)$ then $x>y(=y,<y)$.

Exercise 15. If $x>y,z>u$ then $x\,z>y\,u$.