Arithmetic of Natural Numbers

Bernd Schröder
The Peano Axioms Can’t Be “It”
The Peano Axioms Can’t Be “It”

1. The natural numbers are about counting objects
The Peano Axioms Can’t Be “It”

1. The natural numbers are about counting objects, about adding and multiplying
The Peano Axioms Can’t Be “It”

1. The natural numbers are about counting objects, about adding and multiplying, subtracting and dividing
The Peano Axioms Can’t Be “It”

1. The natural numbers are about counting objects, about adding and multiplying, subtracting and dividing, comparing numbers to each other.
The Peano Axioms Can’t Be “It”

1. The natural numbers are about counting objects, about adding and multiplying, subtracting and dividing, comparing numbers to each other, etc. (And the Peano Axioms don’t directly provide for these things.)
The Peano Axioms Can’t Be “It”

1. The natural numbers are about counting objects, about adding and multiplying, subtracting and dividing, comparing numbers to each other, etc. (And the Peano Axioms don’t directly provide for these things.)

2. So we need arithmetic.
The Peano Axioms Can’t Be “It”

1. The natural numbers are about counting objects, about adding and multiplying, subtracting and dividing, comparing numbers to each other, etc. (And the Peano Axioms don’t directly provide for these things.)
2. So we need arithmetic.
3. But arithmetic must be constructed within set theory so that it will be part of our framework for mathematics.
The Peano Axioms Can’t Be “It”

1. The natural numbers are about counting objects, about adding and multiplying, subtracting and dividing, comparing numbers to each other, etc. (And the Peano Axioms don’t directly provide for these things.)

2. So we need arithmetic.

3. But arithmetic must be constructed within set theory so that it will be part of our framework for mathematics.

4. Moreover, it turns out that the abstract properties of the operations we consider will have far reaching consequences.
The Peano Axioms Can’t Be “It”

1. The natural numbers are about counting objects, about adding and multiplying, subtracting and dividing, comparing numbers to each other, etc. (And the Peano Axioms don’t directly provide for these things.)

2. So we need arithmetic.

3. But arithmetic must be constructed within set theory so that it will be part of our framework for mathematics.

4. Moreover, it turns out that the abstract properties of the operations we consider will have far reaching consequences.

5. So we also need to prove some properties for the operations.
The Peano Axioms Can’t Be “It”

1. The natural numbers are about counting objects, about adding and multiplying, subtracting and dividing, comparing numbers to each other, etc. (And the Peano Axioms don’t directly provide for these things.)

2. So we need arithmetic.

3. But arithmetic must be constructed within set theory so that it will be part of our framework for mathematics.

4. Moreover, it turns out that the abstract properties of the operations we consider will have far reaching consequences.

5. So we also need to prove some properties for the operations and in another presentation we will consider the consequences of these properties.
We Start Abstractly
We Start Abstractly

Definition.
We Start Abstractly

**Definition.** A *(binary)* operation on a set $S$ is a function

$\circ: S \times S \rightarrow S$. 
We Start Abstractly

**Definition.** A *(binary)* operation on a set $S$ is a function

$\circ : S \times S \rightarrow S$.

Binary operations do exactly what addition and subtraction do: They take two objects and produce a new one.
We Start Abstractly

**Definition.** A *(binary) operation* on a set $S$ is a function

$\circ : S \times S \rightarrow S$.

Binary operations do exactly what addition and subtraction do:
They take two objects and produce a new one.

We need simpler notation.
We Start Abstractly

**Definition.** A *(binary)* operation on a set $S$ is a function

$\circ : S \times S \to S$.

Binary operations do exactly what addition and subtraction do: They take two objects and produce a new one.

We need simpler notation.

**Definition.**
We Start Abstractly

Definition. A (binary) operation on a set $S$ is a function
$\circ : S \times S \rightarrow S$.

Binary operations do exactly what addition and subtraction do: They take two objects and produce a new one.

We need simpler notation.

Definition. Let $S$ be a set and let $\circ : S \times S \rightarrow S$ be a binary operation. For all $a, b \in S$ we set $a \circ b := \circ(a, b)$. 
Adding Natural Numbers
Adding Natural Numbers

Definition.

For all $m, n \in \mathbb{N}$ the relation $+$ defined by $n + 1 := n'$ and $n + m' := (n + m)'$.

Or, in relation notation, for all $n \in \mathbb{N}$, the relation $+ \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$ contains the pair $((n, 1), n')$, and for all $n, m \in \mathbb{N}$ for which there is a $k \in \mathbb{N}$ with $((n, m), k) \in +$ we have that $((n, m'), k') \in +$.

The relation (which turns out to be a binary operation) is called addition.
Adding Natural Numbers

**Definition.** For all $m, n \in \mathbb{N}$ the relation $+: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is defined by $n + 1 := n'$ and $n + m' := (n + m)'$. 

---

Bernd Schröder

Louisiana Tech University, College of Engineering and Science

Arithmetic of Natural Numbers
Adding Natural Numbers

**Definition.** For all $m, n \in \mathbb{N}$ the relation $+ : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ is defined by $n + 1 := n'$ and $n + m' := (n + m)'$.

Or, in relation notation, for all $n \in \mathbb{N}$, the relation $+$ is a subset of $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$.
Adding Natural Numbers

**Definition.** For all $m, n \in \mathbb{N}$ the relation $+ : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ is defined by $n + 1 := n'$ and $n + m' := (n + m)'$.

Or, in relation notation, for all $n \in \mathbb{N}$, the relation $+ \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$ contains the pair $((n, 1), n')$. 
Adding Natural Numbers

**Definition.** For all \( m, n \in \mathbb{N} \) the relation \(+ : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \) is defined by \( n + 1 := n' \) and \( n + m' := (n + m)' \).

Or, in relation notation, for all \( n \in \mathbb{N} \), the relation \(+ \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \) contains the pair \( ((n, 1), n') \), and for all \( n, m \in \mathbb{N} \) for which there is a \( k \in \mathbb{N} \) with \( ((n, m), k) \in + \) we have that \( ((n, m'), k') \in + \).
Adding Natural Numbers

**Definition.** For all \( m, n \in \mathbb{N} \) the relation \(+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \) is defined by \( n + 1 := n' \) and \( n + m' := (n + m)' \).

Or, in relation notation, for all \( n \in \mathbb{N} \), the relation \(+ \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \) contains the pair \( ((n, 1), n') \), and for all \( n, m \in \mathbb{N} \) for which there is a \( k \in \mathbb{N} \) with \( ((n, m), k) \in + \) we have that \( ((n, m'), k') \in + \).

The relation (which turns out to be a binary operation) is called addition.
Adding Natural Numbers

Definition. For all $m, n \in \mathbb{N}$ the relation $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is defined by $n + 1 := n'$ and $n + m' := (n + m)'$.

Or, in relation notation, for all $n \in \mathbb{N}$, the relation $+ \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$ contains the pair $((n, 1), n')$, and for all $n, m \in \mathbb{N}$ for which there is a $k \in \mathbb{N}$ with $((n, m), k) \in +$ we have that $((n, m'), k') \in +$.

The relation (which turns out to be a binary operation) is called addition.

(Keep this definition handy. We’ll use it a lot.)
Proposition. The relation $+$ is a binary operation on $\mathbb{N}$. 
**Proposition.** *The relation + is a binary operation on \( \mathbb{N} \).*

**Proof.** By definition, \( + \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \).
**Proposition.** *The relation* $+$ *is a binary operation on* $\mathbb{N}$.

**Proof.** By definition $+$ $\subseteq$ $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$, nothing more.
**Proposition.** *The relation $+$ is a binary operation on $\mathbb{N}$.***

**Proof.** By definition $+$ $\subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$, nothing more. So we use relation notation in this proof.
**Proposition.** *The relation $+$ is a binary operation on $\mathbb{N}$.***

**Proof.** By definition $+ \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$, nothing more. So we use relation notation in this proof. Our main tool will be the Principle of Induction.
**Proposition.** The relation $+$ is a binary operation on $\mathbb{N}$.

**Proof.** By definition $+$ $\subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$, nothing more. So we use relation notation in this proof. Our main tool will be the Principle of Induction.

*Step 1: The relation $+$ is totally defined.*
**Proposition.** The relation $+$ is a binary operation on $\mathbb{N}$.

**Proof.** By definition $+$ $\subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$, nothing more. So we use relation notation in this proof. Our main tool will be the Principle of Induction.

*Step 1: The relation $+$ is totally defined.*

Let $n \in \mathbb{N}$ be arbitrary, but fixed.
**Proposition.** The relation $+$ is a binary operation on $\mathbb{N}$.

**Proof.** By definition $+ \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$, nothing more. So we use relation notation in this proof. Our main tool will be the Principle of Induction.

*Step 1: The relation $+$ is totally defined.*

Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

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


**Proposition.** The relation $+$ is a binary operation on $\mathbb{N}$.

**Proof.** By definition $+ \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$, nothing more. So we use relation notation in this proof. Our main tool will be the Principle of Induction.

*Step 1: The relation $+$ is totally defined.*

Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

$$S := \{ m \in \mathbb{N} : [\exists k \in \mathbb{N} : ((n,m),k) \in +] \}.$$

By definition, $((n,1),n') \in +$, so $1 \in S$. 

**Proposition.** The relation $+$ is a binary operation on $\mathbb{N}$.

**Proof.** By definition $+ \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$, nothing more. So we use relation notation in this proof. Our main tool will be the Principle of Induction.

*Step 1: The relation $+$ is totally defined.*

Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

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

By definition, $((n, 1), n') \in +$, so $1 \in S$. For all $m \in S$ we have $((n, m'), (n + m)') \in +$, so $m' \in S$. 

---

**Bernd Schröder**

**Louisiana Tech University, College of Engineering and Science**

**Arithmetic of Natural Numbers**
**Proposition.** The relation $+$ is a binary operation on $\mathbb{N}$.

**Proof.** By definition $+ \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$, nothing more. So we use relation notation in this proof. Our main tool will be the Principle of Induction.

*Step 1: The relation $+$ is totally defined.*

Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

$$S := \{ m \in \mathbb{N} : [\exists k \in \mathbb{N} : ((n,m),k) \in +] \}.$$

By definition, $((n,1),n') \in +$, so $1 \in S$.

For all $m \in S$ we have $((n,m'),(n+m)') \in +$, so $m' \in S$.

By the Principle of Induction, we conclude that $S = \mathbb{N}$. 
Proposition. The relation \(+\) is a binary operation on \(\mathbb{N}\).

Proof. By definition \(+\) \(\subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}\), nothing more. So we use relation notation in this proof. Our main tool will be the Principle of Induction.

Step 1: The relation \(+\) is totally defined.
Let \(n \in \mathbb{N}\) be arbitrary, but fixed. Let
\[ S := \{ m \in \mathbb{N} : \exists k \in \mathbb{N} : ((n, m), k) \in + \} \].
By definition, \(((n, 1), n')\) \(\in +\), so \(1 \in S\).
For all \(m \in S\) we have \(((n, m'), (n + m)')\) \(\in +\), so \(m' \in S\).
By the Principle of Induction, we conclude that \(S = \mathbb{N}\). Thus \(n + m\) is defined for all \(m \in \mathbb{N}\).
**Proposition.** The relation $+$ is a binary operation on $\mathbb{N}$.

**Proof.** By definition $+ \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$, nothing more. So we use relation notation in this proof. Our main tool will be the Principle of Induction.

*Step 1: The relation $+$ is totally defined.*

Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

$$S := \{ m \in \mathbb{N} : [\exists k \in \mathbb{N} : ((n,m), k) \in +] \}.$$  

By definition, $((n,1), n') \in +$, so $1 \in S$.

For all $m \in S$ we have $((n,m'), (n+m)') \in +$, so $m' \in S$.

By the Principle of Induction, we conclude that $S = \mathbb{N}$. Thus $n + m$ is defined for all $m \in \mathbb{N}$.

Because $n \in \mathbb{N}$ was arbitrary, $n + m$ is defined for all $n, m \in \mathbb{N}$.
**Proposition.** The relation $+ \subseteq \mathbb{N} \times \mathbb{N}$, nothing more. So we use relation notation in this proof. Our main tool will be the Principle of Induction.

*Step 1: The relation $+$ is totally defined.*

Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

$$S := \{ m \in \mathbb{N} : [\exists k \in \mathbb{N} : ((n,m), k) \in +] \}.$$ 

By definition, $((n,1),n') \in +$, so $1 \in S$. For all $m \in S$ we have $((n,m'),(n+m)') \in +$, so $m' \in S$. By the Principle of Induction, we conclude that $S = \mathbb{N}$. Thus $n + m$ is defined for all $m \in \mathbb{N}$. Because $n \in \mathbb{N}$ was arbitrary, $n + m$ is defined for all $n, m \in \mathbb{N}$. Hence $+$ is totally defined.
Proof (cont.).
Proof (cont.). Step 2: The relation $+$ is well-defined.
**Proof (cont.).** *Step 2: The relation $+$ is well-defined.*
Let $n \in \mathbb{N}$ be arbitrary, but fixed.
**Proof (cont.).** *Step 2: The relation* $+$ *is well-defined.*

Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

$$S := \{m \in \mathbb{N} : [\forall k, l \in \mathbb{N} : ((n, m), k), ((n, m), l) \in + \Rightarrow k = l]\}.$$
**Proof (cont.). Step 2: The relation + is well-defined.**

Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

$$S := \{ m \in \mathbb{N} : [\forall k, l \in \mathbb{N} : ((n, m), k), ((n, m), l) \in + \Rightarrow k = l] \}. $$

If $((n, 1), k), ((n, 1), l) \in +$, then
**Proof (cont.).** Step 2: The relation $+$ is well-defined.

Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

$$S := \left\{ m \in \mathbb{N} : \forall k, l \in \mathbb{N} : ((n, m), k), ((n, m), l) \in + \Rightarrow k = l \right\}.$$ 

If $((n, 1), k), ((n, 1), l) \in +$, then, because $1$ is not the successor of any natural number
Proof (cont.). Step 2: The relation $+$ is well-defined.
Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

$$S := \{m \in \mathbb{N} : \forall k, l \in \mathbb{N} : ((n, m), k), ((n, m), l) \in + \Rightarrow k = l\}.$$

If $((n, 1), k), ((n, 1), l) \in +$, then, because 1 is not the successor of any natural number, we obtain $k = n' = l$. 
Proof (cont.). Step 2: The relation $+$ is well-defined.

Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

$$S := \{ m \in \mathbb{N} : \forall k, l \in \mathbb{N} : ((n, m), k), ((n, m), l) \in + \Rightarrow k = l \}.$$

If $((n, 1), k), ((n, 1), l) \in +$, then, because 1 is not the successor of any natural number, we obtain $k = n' = l$. So $1 \in S$. 
**Proof (cont.).** *Step 2: The relation + is well-defined.*

Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

$$S := \{ m \in \mathbb{N} : \forall k, l \in \mathbb{N} : ((n, m), k), ((n, m), l) \in + \Rightarrow k = l \}.$$  

If $((n, 1), k), ((n, 1), l) \in +$, then, because 1 is not the successor of any natural number, we obtain $k = n' = l$. So $1 \in S$.

Now, if $m \in S$, and $((n, m'), k), ((n, m'), l) \in +$
**Proof (cont.). Step 2: The relation $+$ is well-defined.**

Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

$$S := \{ m \in \mathbb{N} : \forall k, l \in \mathbb{N} : ((n, m), k), ((n, m), l) \in + \Rightarrow k = l \}.$$ 

If $((n, 1), k), ((n, 1), l) \in +$, then, because 1 is not the successor of any natural number, we obtain $k = n' = l$. So $1 \in S$.

Now, if $m \in S$, and $((n, m'), k), ((n, m'), l) \in +$, then $k = (n + m)' = l$ and therefore $m' \in S$. 
Proof (cont.). Step 2: The relation $+$ is well-defined.
Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

$$S := \{ m \in \mathbb{N} : \forall k, l \in \mathbb{N} : ((n, m), k), ((n, m), l) \in + \Rightarrow k = l \}.$$

If $((n, 1), k), ((n, 1), l) \in +$, then, because 1 is not the successor of any natural number, we obtain $k = n' = l$. So $1 \in S$.

Now, if $m \in S$, and $((n, m'), k), ((n, m'), l) \in +$, then $k = (n + m)' = l$ and therefore $m' \in S$. By the Principle of Induction, $S = \mathbb{N}$. 
**Proof (cont.).** *Step 2: The relation + is well-defined.*

Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

$$S := \{ m \in \mathbb{N} : [\forall k, l \in \mathbb{N} : ((n, m), k), ((n, m), l) \in + \Rightarrow k = l] \}.$$ 

If $((n, 1), k), ((n, 1), l) \in +$, then, because 1 is not the successor of any natural number, we obtain $k = n' = l$. So $1 \in S$.

Now, if $m \in S$, and $((n, m'), k), ((n, m'), l) \in +$, then $k = (n + m)' = l$ and therefore $m' \in S$. By the Principle of Induction, $S = \mathbb{N}$. Thus $n + m$ is unique for all $n, m \in \mathbb{N}$. We conclude that + is well-defined.
**Proof (cont.). Step 2: The relation $+$ is well-defined.**

Let $n \in \mathbb{N}$ be arbitrary, but fixed. Let

$$S := \{ m \in \mathbb{N} : [\forall k, l \in \mathbb{N} : ((n, m), k), ((n, m), l) \in + \Rightarrow k = l] \}.$$ 

If $((n, 1), k), ((n, 1), l) \in +$, then, because 1 is not the successor of any natural number, we obtain $k = n' = l$. So $1 \in S$.

Now, if $m \in S$, and $((n, m'), k), ((n, m'), l) \in +$, then $k = (n + m)' = l$ and therefore $m' \in S$. By the Principle of Induction, $S = \mathbb{N}$. Thus $n + m$ is unique for all $n, m \in \mathbb{N}$. We conclude that $+$ is well-defined. 

$\blacksquare$
1. To use the Principle of Induction as stated in the Peano Axioms, we define a set that contains all the elements with a certain property and then we prove that that set is $\mathbb{N}$. So, if you already know induction, this approach really is not that different. We'll get back to "the usual way to do induction" in a little while.

2. The idea that a function needs to be proved to be well-defined takes some time getting used to. Arithmetic modulo $m$ will give us a simpler and pretty natural context.
Notes

1. To use the Principle of Induction as stated in the Peano Axioms
Notes

1. To use the Principle of Induction as stated in the Peano Axioms, we define a set that contains all the elements with a certain property
Notes

1. To use the Principle of Induction as stated in the Peano Axioms, we define a set that contains all the elements with a certain property and then we prove that that set is $\mathbb{N}$. 

Arithmetic of Natural Numbers
Notes

1. To use the Principle of Induction as stated in the Peano Axioms, we define a set that contains all the elements with a certain property and then we prove that that set is $\mathbb{N}$. So, if you already know induction, this approach really is not that different.
Notes

1. To use the Principle of Induction as stated in the Peano Axioms, we define a set that contains all the elements with a certain property and then we prove that that set is \( \mathbb{N} \). So, if you already know induction, this approach really is not that different. We’ll get back to “the usual way to do induction” in a little while.
Notes

1. To use the Principle of Induction as stated in the Peano Axioms, we define a set that contains all the elements with a certain property and then we prove that that set is $\mathbb{N}$. So, if you already know induction, this approach really is not that different. We’ll get back to “the usual way to do induction” in a little while.

2. The idea that a function needs to be proved to be well-defined takes some time getting used to.
Notes

1. To use the Principle of Induction as stated in the Peano Axioms, we define a set that contains all the elements with a certain property and then we prove that that set is $\mathbb{N}$. So, if you already know induction, this approach really is not that different. We’ll get back to “the usual way to do induction” in a little while.

2. The idea that a function needs to be proved to be well-defined takes some time getting used to. Arithmetic modulo $m$ will give us a simpler and pretty natural context.
Proposition.
Proposition. *Properties of the addition operation on* \(\mathbb{N}\).
Proposition. Properties of the addition operation on $\mathbb{N}$.

1. Addition is **associative**
**Proposition.** Properties of the addition operation on $\mathbb{N}$.

1. *Addition is associative*, that is, for all $n, m, k \in \mathbb{N}$ we have that $(n + m) + k = n + (m + k)$. 
**Proposition.** *Properties of the addition operation on $\mathbb{N}$.*

1. *Addition is associative,* that is, for all $n, m, k \in \mathbb{N}$ we have that $(n + m) + k = n + (m + k)$.

2. *Addition is commutative*
**Proposition.** Properties of the addition operation on \( \mathbb{N} \).

1. *Addition is associative*, that is, for all \( n, m, k \in \mathbb{N} \) we have that \( (n + m) + k = n + (m + k) \).

2. *Addition is commutative*, that is, for all \( n, m \in \mathbb{N} \) we have that \( n + m = m + n \).
Proposition. Properties of the addition operation on $\mathbb{N}$.

1. Addition is **associative**, that is, for all $n, m, k \in \mathbb{N}$ we have that $(n + m) + k = n + (m + k)$.

2. Addition is **commutative**, that is, for all $n, m \in \mathbb{N}$ we have that $n + m = m + n$.

(We need to get used to the vocabulary.)
Proof.
**Proof.** We must prove associativity and commutativity, and we will use the Principle of Induction.
**Proof.** We must prove associativity and commutativity, and we will use the Principle of Induction.
To prove associativity, let $n, m \in \mathbb{N}$ be arbitrary, but fixed.
**Proof.** We must prove associativity and commutativity, and we will use the Principle of Induction.

To prove associativity, let $n, m \in \mathbb{N}$ be arbitrary, but fixed. Let $S := \{ k \in \mathbb{N} : (n + m) + k = n + (m + k) \}$. 
**Proof.** We must prove associativity and commutativity, and we will use the Principle of Induction.

To prove associativity, let $n, m \in \mathbb{N}$ be arbitrary, but fixed. Let $S := \{ k \in \mathbb{N} : (n + m) + k = n + (m + k) \}$.

$1 \in S$, because

$$(n + m) + 1$$
**Proof.** We must prove associativity and commutativity, and we will use the Principle of Induction.

To prove associativity, let \( n, m \in \mathbb{N} \) be arbitrary, but fixed. Let 
\[
S := \{ k \in \mathbb{N} : (n + m) + k = n + (m + k) \}.
\]

1 \( \in \) \( S \), because 
\[
(n + m) + 1 = (n + m)
\]
**Proof.** We must prove associativity and commutativity, and we will use the Principle of Induction.

To prove associativity, let $n, m \in \mathbb{N}$ be arbitrary, but fixed. Let $S := \{ k \in \mathbb{N} : (n + m) + k = n + (m + k) \}$.

1 $\in S$, because

\[(n + m) + 1 = (n + m)' = n + m'\]
\textbf{Proof.} We must prove associativity and commutativity, and we will use the Principle of Induction. To prove associativity, let \( n, m \in \mathbb{N} \) be arbitrary, but fixed. Let \( S := \{ k \in \mathbb{N} : (n + m) + k = n + (m + k) \} \).

1 \( \in S \), because

\[(n + m) + 1 = (n + m)' = n + m' = n + (m + 1).\]
**Proof.** We must prove associativity and commutativity, and we will use the Principle of Induction.

To prove associativity, let $n, m \in \mathbb{N}$ be arbitrary, but fixed. Let $S := \{ k \in \mathbb{N} : (n + m) + k = n + (m + k) \}$.

$1 \in S$, because

$$(n + m) + 1 = (n + m)' = n + m' = n + (m + 1).$$

Now let $k \in S$. 
**Proof.** We must prove associativity and commutativity, and we will use the Principle of Induction.

To prove associativity, let \( n, m \in \mathbb{N} \) be arbitrary, but fixed. Let \( S := \{ k \in \mathbb{N} : (n + m) + k = n + (m + k) \} \).

1 \( \in S \), because

\[
(n + m) + 1 = (n + m)' = n + m' = n + (m + 1).
\]

Now let \( k \in S \). Then \( k' \in S \), because
**Proof.** We must prove associativity and commutativity, and we will use the Principle of Induction.

To prove associativity, let \( n, m \in \mathbb{N} \) be arbitrary, but fixed. Let 
\[ S := \{ k \in \mathbb{N} : (n + m) + k = n + (m + k) \}. \]

1 \( \in S \), because 
\[ (n + m) + 1 = (n + m)' = n + m' = n + (m + 1). \]

Now let \( k \in S \). Then \( k' \in S \), because 
\[ (n + m) + k' \]
**Proof.** We must prove associativity and commutativity, and we will use the Principle of Induction.

To prove associativity, let \( n, m \in \mathbb{N} \) be arbitrary, but fixed. Let
\[
S := \{ k \in \mathbb{N} : (n + m) + k = n + (m + k) \}.
\]

1 \( \in \) \( S \), because
\[
(n + m) + 1 = (n + m)' = n + m' = n + (m + 1).
\]

Now let \( k \in S \). Then \( k' \in S \), because
\[
(n + m) + k' = ((n + m) + k)'.
\]
Proof. We must prove associativity and commutativity, and we will use the Principle of Induction.

To prove associativity, let \( n, m \in \mathbb{N} \) be arbitrary, but fixed. Let

\[ S := \{ k \in \mathbb{N} : (n + m) + k = n + (m + k) \} \]

1 \( \in S \), because

\[ (n + m) + 1 = (n + m)' = n + m' = n + (m + 1) \]

Now let \( k \in S \). Then \( k' \in S \), because

\[ (n + m) + k' = ((n + m) + k)' = (n + (m + k))' \]
Proof. We must prove associativity and commutativity, and we will use the Principle of Induction.
To prove associativity, let \( n, m \in \mathbb{N} \) be arbitrary, but fixed. Let
\[ S := \{ k \in \mathbb{N} : (n + m) + k = n + (m + k) \} \]
1 \( \in S \), because
\[
(n + m) + 1 = (n + m)' = n + m' = n + (m + 1).
\]
Now let \( k \in S \). Then \( k' \in S \), because
\[
(n + m) + k' = ((n + m) + k)' = (n + (m + k))' = n + (m + k)'.
\]
Proof. We must prove associativity and commutativity, and we will use the Principle of Induction. To prove associativity, let \( n, m \in \mathbb{N} \) be arbitrary, but fixed. Let \( S := \{ k \in \mathbb{N} : (n + m) + k = n + (m + k) \} \).

1 \in S, because
\[
(n + m) + 1 = (n + m)' = n + m' = n + (m + 1).
\]

Now let \( k \in S \). Then \( k' \in S \), because
\[
(n + m) + k' = ((n + m) + k)' = (n + (m + k))' \\
= n + (m + k)' = n + (m + k').
\]
Proof. We must prove associativity and commutativity, and we will use the Principle of Induction.
To prove associativity, let \( n, m \in \mathbb{N} \) be arbitrary, but fixed. Let \( S := \{ k \in \mathbb{N} : (n + m) + k = n + (m + k) \} \).
1 \( \in S \), because
\[
(n + m) + 1 = (n + m)' = n + m' = n + (m + 1).
\]
Now let \( k \in S \). Then \( k' \in S \), because
\[
(n + m) + k' = ((n + m) + k)' = (n + (m + k))' \\
= n + (m + k)' = n + (m + k').
\]
By the Principle of Induction, \( S = \mathbb{N} \)
**Proof.** We must prove associativity and commutativity, and we will use the Principle of Induction.

To prove associativity, let \( n, m \in \mathbb{N} \) be arbitrary, but fixed. Let \( S := \{ k \in \mathbb{N} : (n + m) + k = n + (m + k) \} \).

1 \( \in S \), because

\[
(n + m) + 1 = (n + m)' = n + m' = n + (m + 1).
\]

Now let \( k \in S \). Then \( k' \in S \), because

\[
(n + m) + k' = ((n + m) + k)' = (n + (m + k))' = n + (m + k)' = n + (m + k').
\]

By the Principle of Induction, \( S = \mathbb{N} \), so \( (n + m) + k = n + (m + k) \) for all \( k \in \mathbb{N} \).
**Proof.** We must prove associativity and commutativity, and we will use the Principle of Induction.

To prove associativity, let \( n, m \in \mathbb{N} \) be arbitrary, but fixed. Let \( S := \{ k \in \mathbb{N} : (n + m) + k = n + (m + k) \} \).

1 \( \in \) \( S \), because

\[
(n + m) + 1 = (n + m)' = n + m' = n + (m + 1).
\]

Now let \( k \in S \). Then \( k' \in S \), because

\[
(n + m) + k' = ((n + m) + k)' = (n + (m + k))' = n + (m + k)' = n + (m + k').
\]

By the Principle of Induction, \( S = \mathbb{N} \), so

\[
(n + m) + k = n + (m + k) \text{ for all } k \in \mathbb{N}.
\]

Because \( n \) and \( m \) were arbitrary, \( + \) is associative.
Proof (cont.).
Proof (cont.). To prove commutativity, let $n \in \mathbb{N}$ be arbitrary, but fixed.
Proof (cont.). To prove commutativity, let $n \in \mathbb{N}$ be arbitrary, but fixed. Let $S := \{ m \in \mathbb{N} : n + m = m + n \}$. 
Proof (cont.). To prove commutativity, let $n \in \mathbb{N}$ be arbitrary, but fixed. Let $S := \{m \in \mathbb{N} : n + m = m + n\}$.

To prove that $1 \in S$, we will perform an induction inside an induction.
Proof (cont.). To prove commutativity, let $n \in \mathbb{N}$ be arbitrary, but fixed. Let $S := \{m \in \mathbb{N} : n + m = m + n\}$.

To prove that $1 \in S$, we will perform an induction inside an induction.

Let $T := \{k \in \mathbb{N} : k + 1 = 1 + k\}$. 

Trivially, $1 \in T$. Now let $k \in T$. Then $k' + 1 = (k + 1) + 1 = (1 + k) + 1 = 1 + (k + 1) = 1 + k'$, so $k' \in T$. Hence $T = \mathbb{N}$, that is, $k + 1 = 1 + k$ for all $k \in \mathbb{N}$. (Back to the "main induction".)
Proof (cont.). To prove commutativity, let \( n \in \mathbb{N} \) be arbitrary, but fixed. Let \( S := \{ m \in \mathbb{N} : n + m = m + n \} \).

To prove that \( 1 \in S \), we will perform an induction inside an induction.

Let \( T := \{ k \in \mathbb{N} : k + 1 = 1 + k \} \). Trivially, \( 1 \in T \).
Proof (cont.). To prove commutativity, let \( n \in \mathbb{N} \) be arbitrary, but fixed. Let \( S := \{ m \in \mathbb{N} : n + m = m + n \} \).

To prove that \( 1 \in S \), we will perform an induction inside an induction.

Let \( T := \{ k \in \mathbb{N} : k + 1 = 1 + k \} \). Trivially, \( 1 \in T \).

Now let \( k \in T \).
Proof (cont.). To prove commutativity, let \( n \in \mathbb{N} \) be arbitrary, but fixed. Let \( S := \{ m \in \mathbb{N} : n + m = m + n \} \). To prove that \( 1 \in S \), we will perform an induction inside an induction.

Let \( T := \{ k \in \mathbb{N} : k + 1 = 1 + k \} \). Trivially, \( 1 \in T \).

Now let \( k \in T \). Then

\[
k' + 1
\]
**Proof (cont.).** To prove commutativity, let $n \in \mathbb{N}$ be arbitrary, but fixed. Let $S := \{m \in \mathbb{N} : n + m = m + n\}$.

To prove that $1 \in S$, *we will perform an induction inside an induction.*

Let $T := \{k \in \mathbb{N} : k + 1 = 1 + k\}$. Trivially, $1 \in T$.

Now let $k \in T$. Then

$$k' + 1 = (k + 1) + 1$$
Proof (cont.). To prove commutativity, let \( n \in \mathbb{N} \) be arbitrary, but fixed. Let \( S := \{ m \in \mathbb{N} : n + m = m + n \} \).

To prove that \( 1 \in S \), we will perform an induction inside an induction.

Let \( T := \{ k \in \mathbb{N} : k + 1 = 1 + k \} \). Trivially, \( 1 \in T \).

Now let \( k \in T \). Then

\[
k' + 1 = (k + 1) + 1 = (1 + k) + 1
\]
Proof (cont.). To prove commutativity, let $n \in \mathbb{N}$ be arbitrary, but fixed. Let $S := \{ m \in \mathbb{N} : n + m = m + n \}$.

To prove that $1 \in S$, we will perform an induction inside an induction.

Let $T := \{ k \in \mathbb{N} : k + 1 = 1 + k \}$. Trivially, $1 \in T$.

Now let $k \in T$. Then

$$k' + 1 = (k + 1) + 1 = (1 + k) + 1 = 1 + (k + 1)$$
Proof (cont.). To prove commutativity, let $n \in \mathbb{N}$ be arbitrary, but fixed. Let $S := \{m \in \mathbb{N} : n + m = m + n\}$.

To prove that $1 \in S$, we will perform an induction inside an induction.

Let $T := \{k \in \mathbb{N} : k + 1 = 1 + k\}$. Trivially, $1 \in T$.

Now let $k \in T$. Then

$$k' + 1 = (k + 1) + 1 = (1 + k) + 1 = 1 + (k + 1) = 1 + k',$$

...
Proof (cont.). To prove commutativity, let \( n \in \mathbb{N} \) be arbitrary, but fixed. Let \( S := \{ m \in \mathbb{N} : n + m = m + n \} \).

To prove that \( 1 \in S \), we will perform an induction inside an induction.

Let \( T := \{ k \in \mathbb{N} : k + 1 = 1 + k \} \). Trivially, \( 1 \in T \).

Now let \( k \in T \). Then

\[
k' + 1 = (k + 1) + 1 = (1 + k) + 1 = 1 + (k + 1) = 1 + k',
\]

so \( k' \in T \).
**Proof (cont.).** To prove commutativity, let \( n \in \mathbb{N} \) be arbitrary, but fixed. Let \( S := \{ m \in \mathbb{N} : n + m = m + n \} \).

To prove that \( 1 \in S \), we will perform an induction inside an induction.

Let \( T := \{ k \in \mathbb{N} : k + 1 = 1 + k \} \). Trivially, \( 1 \in T \).

Now let \( k \in T \). Then

\[
k' + 1 = (k + 1) + 1 = (1 + k) + 1 = 1 + (k + 1) = 1 + k',
\]

so \( k' \in T \). Hence \( T = \mathbb{N} \).
Proof (cont.). To prove commutativity, let $n \in \mathbb{N}$ be arbitrary, but fixed. Let $S := \{m \in \mathbb{N} : n + m = m + n\}$.

To prove that $1 \in S$, we will perform an induction inside an induction.

Let $T := \{k \in \mathbb{N} : k + 1 = 1 + k\}$. Trivially, $1 \in T$.

Now let $k \in T$. Then

$$k' + 1 = (k + 1) + 1 = (1 + k) + 1 = 1 + (k + 1) = 1 + k',$$

so $k' \in T$. Hence $T = \mathbb{N}$, that is, $k + 1 = 1 + k$ for all $k \in \mathbb{N}$. 
Proof (cont.). To prove commutativity, let $n \in \mathbb{N}$ be arbitrary, but fixed. Let $S := \{m \in \mathbb{N} : n + m = m + n\}$. To prove that $1 \in S$, we will perform an induction inside an induction.

Let $T := \{k \in \mathbb{N} : k + 1 = 1 + k\}$. Trivially, $1 \in T$.

Now let $k \in T$. Then

$$k' + 1 = (k + 1) + 1 = (1 + k) + 1 = 1 + (k + 1) = 1 + k',$$

so $k' \in T$. Hence $T = \mathbb{N}$, that is, $k + 1 = 1 + k$ for all $k \in \mathbb{N}$. 

(Back to the “main induction”.)
Proof (cont.).
Proof (cont.). Using \( k := n \) we obtain \( n + 1 = 1 + n \), and hence \( 1 \in S = \{m \in \mathbb{N} : n + m = m + n\} \).
Proof (cont.). Using \( k := n \) we obtain \( n + 1 = 1 + n \), and hence \( 1 \in S = \{ m \in \mathbb{N} : n + m = m + n \} \).

Now let \( m \in S \).
Proof (cont.). Using $k := n$ we obtain $n + 1 = 1 + n$, and hence $1 \in S = \{ m \in \mathbb{N} : n + m = m + n \}$.

Now let $m \in S$. Then

$n + m'$
Proof (cont.). Using $k := n$ we obtain $n + 1 = 1 + n$, and hence $1 \in S = \{m \in \mathbb{N} : n + m = m + n\}$.

Now let $m \in S$. Then

$$n + m' = n + (m + 1)$$
Proof (cont.). Using $k := n$ we obtain $n + 1 = 1 + n$, and hence $1 \in S = \{m \in \mathbb{N} : n + m = m + n\}$. Now let $m \in S$. Then

$$n + m' = n + (m + 1) = (n + m) + 1$$
Proof (cont.). Using $k := n$ we obtain $n + 1 = 1 + n$, and hence $1 \in S = \{m \in \mathbb{N} : n + m = m + n\}$.

Now let $m \in S$. Then

$$n + m' = n + (m + 1) = (n + m) + 1 = (m + n) + 1$$
Proof (cont.). Using \( k := n \) we obtain \( n + 1 = 1 + n \), and hence \( 1 \in S = \{ m \in \mathbb{N} : n + m = m + n \} \).

Now let \( m \in S \). Then

\[
n + m' = n + (m + 1) = (n + m) + 1 = (m + n) + 1 = m + (n + 1)
\]
**Proof (cont.).** Using $k := n$ we obtain $n + 1 = 1 + n$, and hence $1 \in S = \{m \in \mathbb{N} : n + m = m + n\}$.

Now let $m \in S$. Then

\[
\begin{align*}
n + m' &= n + (m + 1) = (n + m) + 1 = (m + n) + 1 = m + (n + 1) \\
&= m + (1 + n)
\end{align*}
\]
**Proof (cont.).** Using $k := n$ we obtain $n + 1 = 1 + n$, and hence $1 \in S = \{m \in \mathbb{N} : n + m = m + n\}$.

Now let $m \in S$. Then

$$n + m' = n + (m + 1) = (n + m) + 1 = (m + n) + 1 = m + (n + 1)$$

$$= m + (1 + n) = (m + 1) + n$$
Proof (cont.). Using \( k := n \) we obtain \( n + 1 = 1 + n \), and hence 
\( 1 \in S = \{ m \in \mathbb{N} : n + m = m + n \} \).

Now let \( m \in S \). Then

\[
\begin{align*}
n + m' &= n + (m + 1) = (n + m) + 1 = (m + n) + 1 = m + (n + 1) \\
&= m + (1 + n) = (m + 1) + n = m' + n,
\end{align*}
\]
Proof (cont.). Using $k := n$ we obtain $n + 1 = 1 + n$, and hence $1 \in S = \{m \in \mathbb{N} : n + m = m + n\}$.

Now let $m \in S$. Then

$$n + m' = n + (m + 1) = (n + m) + 1 = (m + n) + 1 = m + (n + 1)$$

$$= m + (1 + n) = (m + 1) + n = m' + n,$$

that is, $m' \in S$. 

---

Bernd Schröder  
Louisiana Tech University, College of Engineering and Science  
Arithmetic of Natural Numbers
Proof (cont.).} Using $k := n$ we obtain $n + 1 = 1 + n$, and hence $1 \in S = \{ m \in \mathbb{N} : n + m = m + n \}$. Now let $m \in S$. Then
\[
\begin{align*}
 n + m' & = n + (m + 1) = (n + m) + 1 = (m + n) + 1 = m + (n + 1) \\
 & = m + (1 + n) = (m + 1) + n = m' + n,
\end{align*}
\]
that is, $m' \in S$. Thus $S = \mathbb{N}$,
**Proof (cont.).** Using $k := n$ we obtain $n + 1 = 1 + n$, and hence $1 \in S = \{m \in \mathbb{N} : n + m = m + n\}$.

Now let $m \in S$. Then

\[
\begin{align*}
n + m' &= n + (m + 1) = (n + m) + 1 = (m + n) + 1 = m + (n + 1) \\
&= m + (1 + n) = (m + 1) + n = m' + n,
\end{align*}
\]

that is, $m' \in S$. Thus $S = \mathbb{N}$, and for all $m \in \mathbb{N}$ we have that $n + m = m + n$. 

---

Bernd Schröder

Arithmetic of Natural Numbers
Proof (cont.). Using $k := n$ we obtain $n + 1 = 1 + n$, and hence $1 \in S = \{m \in \mathbb{N} : n + m = m + n\}$.

Now let $m \in S$. Then

$$n + m' = n + (m + 1) = (n + m) + 1 = (m + n) + 1 = m + (n + 1)$$

$$= m + (1 + n) = (m + 1) + n = m' + n,$$

that is, $m' \in S$. Thus $S = \mathbb{N}$, and for all $m \in \mathbb{N}$ we have that $n + m = m + n$.

Because $n \in \mathbb{N}$ was arbitrary, this establishes commutativity. ■
Back to Earth: The Usual Representation of Natural Numbers
Back to Earth: The Usual Representation of Natural Numbers

Definition.
Back to Earth: The Usual Representation of Natural Numbers

**Definition.** We define

\[ 2 := 1 + 1 \]
Back to Earth: The Usual Representation of Natural Numbers

**Definition.** We define

\[ 2 := 1 + 1 \]
\[ 3 := 2 + 1 = (1 + 1) + 1 \]
Back to Earth: The Usual Representation of Natural Numbers

**Definition.** We define

\[
\begin{align*}
2 & := 1 + 1 \\
3 & := 2 + 1 = (1 + 1) + 1 \\
4 & := 3 + 1 = ((1 + 1) + 1) + 1 \\
\end{align*}
\]
Back to Earth: The Usual Representation of Natural Numbers

**Definition.** We define

\[
\begin{align*}
2 & := 1 + 1 \\
3 & := 2 + 1 = (1 + 1) + 1 \\
4 & := 3 + 1 = ((1 + 1) + 1) + 1 \\
5 & := 4 + 1 = (((1 + 1) + 1) + 1) + 1
\end{align*}
\]
Back to Earth: The Usual Representation of Natural Numbers

**Definition.** We define

\[ 2 := 1 + 1 \]
\[ 3 := 2 + 1 = (1 + 1) + 1 \]
\[ 4 := 3 + 1 = ((1 + 1) + 1) + 1 \]
\[ 5 := 4 + 1 = (((1 + 1) + 1) + 1) + 1 \]

and so on, in the usual fashion.
Back to Earth: The Usual Representation of Natural Numbers

**Definition.** We define

\[
2 \ := \ 1 + 1 \\
3 \ := \ 2 + 1 = (1 + 1) + 1 \\
4 \ := \ 3 + 1 = ((1 + 1) + 1) + 1 \\
5 \ := \ 4 + 1 = (((1 + 1) + 1) + 1) + 1
\]

and so on, in the usual fashion.

*Yes, numerals are merely symbols.*
Back to Earth: The Usual Representation of Natural Numbers

**Definition.** We define

\[
\begin{align*}
2 & := 1 + 1 \\
3 & := 2 + 1 = (1 + 1) + 1 \\
4 & := 3 + 1 = ((1 + 1) + 1) + 1 \\
5 & := 4 + 1 = (((1 + 1) + 1) + 1) + 1
\end{align*}
\]

and so on, in the usual fashion.

Yes, numerals are merely symbols. Think of roman numerals if that feels “wrong”.

We Can’t Prove $1 + 1 = 2$, But We Can Prove $4 + 3 = 7$
We Can’t Prove $1 + 1 = 2$, But We Can Prove $4 + 3 = 7$
We Can’t Prove $1 + 1 = 2$, But We Can Prove $4 + 3 = 7$

\[ 4 + 3 = 4 + (2 + 1) \]
We Can’t Prove 1 + 1 = 2, But We Can Prove 4 + 3 = 7

\[
4 + 3 = 4 + (2 + 1) = (4 + 2) + 1
\]
We Can’t Prove $1 + 1 = 2$, But We Can Prove $4 + 3 = 7$

\[
4 + 3 = 4 + (2 + 1) \\
= (4 + 2) + 1 \\
= (4 + (1 + 1)) + 1
\]
We Can’t Prove $1 + 1 = 2$, But We Can Prove $4 + 3 = 7$

\[
4 + 3 = 4 + (2 + 1) \\
= (4 + 2) + 1 \\
= (4 + (1 + 1)) + 1 \\
= ((4 + 1) + 1) + 1
\]
We Can’t Prove $1 + 1 = 2$, But We Can Prove $4 + 3 = 7$

$$4 + 3 = 4 + (2 + 1)$$
$$= (4 + 2) + 1$$
$$= (4 + (1 + 1)) + 1$$
$$= ((4 + 1) + 1) + 1$$
$$= (5 + 1) + 1$$
We Can’t Prove $1 + 1 = 2$, But We Can Prove $4 + 3 = 7$

\[
4 + 3 = 4 + (2 + 1) \\
= (4 + 2) + 1 \\
= (4 + (1 + 1)) + 1 \\
= ((4 + 1) + 1) + 1 \\
= (5 + 1) + 1 \\
= 6 + 1
\]
We Can’t Prove $1 + 1 = 2$, But We Can Prove $4 + 3 = 7$

\[
4 + 3 = 4 + (2 + 1) \\
= (4 + 2) + 1 \\
= (4 + (1 + 1)) + 1 \\
= ((4 + 1) + 1) + 1 \\
= (5 + 1) + 1 \\
= 6 + 1 \\
= 7
\]
We Can’t Prove $1 + 1 = 2$, But We Can Prove $4 + 3 = 7$

$$4 + 3 = 4 + (2 + 1)$$
$$= (4 + 2) + 1$$
$$= (4 + (1 + 1)) + 1$$
$$= ((4 + 1) + 1) + 1$$
$$= (5 + 1) + 1$$
$$= 6 + 1$$
$$= 7$$

If we do too much of this, people will believe we are nuts.
We Can’t Prove $1 + 1 = 2$, But We Can Prove $4 + 3 = 7$

\[
4 + 3 = 4 + (2 + 1) \\
= (4 + 2) + 1 \\
= (4 + (1 + 1)) + 1 \\
= ((4 + 1) + 1) + 1 \\
= (5 + 1) + 1 \\
= 6 + 1 \\
= 7
\]

If we do too much of this, people will believe we are nuts. But, this is a good exercise in mathematical reasoning nonetheless.
Multiplying Natural Numbers
Multiplying Natural Numbers

Definition.
Multiplying Natural Numbers

**Definition.** *For all* $m, n \in \mathbb{N}$ *the relation* $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *is defined by* $n \cdot 1 := n$ *and* $n \cdot m' := n \cdot m + n$. 
Multiplying Natural Numbers

**Definition.** For all \( m, n \in \mathbb{N} \) the relation \( \cdot : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \) is defined by \( n \cdot 1 := n \) and \( n \cdot m' := n \cdot m + n \). Or, in relation notation, for all \( n \in \mathbb{N} \), the relation \( \cdot \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \).
### Multiplying Natural Numbers

**Definition.** For all $m, n \in \mathbb{N}$ the relation $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is defined by $n \cdot 1 := n$ and $n \cdot m' := n \cdot m + n$. Or, in relation notation, for all $n \in \mathbb{N}$, the relation $\cdot \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$ contains the pair $((n, 1), n)$. 
Multiplying Natural Numbers

**Definition.** For all $m, n \in \mathbb{N}$ the relation $\cdot : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ is defined by $n \cdot 1 := n$ and $n \cdot m' := n \cdot m + n$. Or, in relation notation, for all $n \in \mathbb{N}$, the relation $\cdot \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$ contains the pair $((n, 1), n)$, and for all $n, m \in \mathbb{N}$ for which there is a $k \in \mathbb{N}$ with $((n, m), k) \in \cdot$ we have that $((n, m'), k + n) \in \cdot$. 
Multiplying Natural Numbers

**Definition.** For all $m, n \in \mathbb{N}$ the relation $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is defined by $n \cdot 1 := n$ and $n \cdot m' := n \cdot m + n$. Or, in relation notation, for all $n \in \mathbb{N}$, the relation $\cdot \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$ contains the pair $((n, 1), n)$, and for all $n, m \in \mathbb{N}$ for which there is a $k \in \mathbb{N}$ with $((n, m), k) \in \cdot$ we have that $((n, m'), k + n) \in \cdot$. The relation (which turns out to be a binary operation) is called multiplication.
1. Yes, it's a binary operation.
2. Multiplication is an abbreviation for repeated addition of a number to itself.
3. Multiplication is associative, that is, for all \( n, m, k \in \mathbb{N} \) we have that 
   \[
   (n \cdot m) \cdot k = n \cdot (m \cdot k)
   \]
4. Multiplication is commutative, that is, for all \( n, m \in \mathbb{N} \) we have that 
   \[
   n \cdot m = m \cdot n
   \]
5. The number 1 is a neutral element or identity element with respect to multiplication, that is, for all \( n \in \mathbb{N} \) we have that 
   \[
   n \cdot 1 = 1 \cdot n = n
   \]
6. Multiplication is right distributive over addition. That is, for all \( n, m, k \in \mathbb{N} \) we have 
   \[
   (n + m) \cdot k = n \cdot k + m \cdot k
   \]

The proof of the last four is a bit tricky.
Properties of Multiplication

1. Yes, it’s a binary operation.
Properties of Multiplication

1. Yes, it’s a binary operation.
2. Multiplication is an abbreviation for repeated addition of a number to itself.
Properties of Multiplication

1. Yes, it’s a binary operation.
2. Multiplication is an abbreviation for repeated addition of a number to itself.
3. Multiplication is **associative**, that is, for all $n, m, k \in \mathbb{N}$ we have that $(n \cdot m) \cdot k = n \cdot (m \cdot k)$.
Properties of Multiplication

1. Yes, it’s a binary operation.
2. Multiplication is an abbreviation for repeated addition of a number to itself.
3. Multiplication is associative, that is, for all \( n, m, k \in \mathbb{N} \) we have that \( (n \cdot m) \cdot k = n \cdot (m \cdot k) \).
4. Multiplication is commutative, that is, for all \( n, m \in \mathbb{N} \) we have that \( n \cdot m = m \cdot n \).
Properties of Multiplication

1. Yes, it’s a binary operation.
2. Multiplication is an abbreviation for repeated addition of a number to itself.
3. Multiplication is **associative**, that is, for all \( n, m, k \in \mathbb{N} \) we have that \((n \cdot m) \cdot k = n \cdot (m \cdot k)\).
4. Multiplication is **commutative**, that is, for all \( n, m \in \mathbb{N} \) we have that \( n \cdot m = m \cdot n \).
5. The number 1 is a **neutral element** or **identity element** with respect to multiplication, that is, for all \( n \in \mathbb{N} \) we have that \( n \cdot 1 = 1 \cdot n = n \).
Properties of Multiplication

1. Yes, it’s a binary operation.

2. Multiplication is an abbreviation for repeated addition of a number to itself.

3. Multiplication is **associative**, that is, for all $n, m, k \in \mathbb{N}$ we have that $(n \cdot m) \cdot k = n \cdot (m \cdot k)$.

4. Multiplication is **commutative**, that is, for all $n, m \in \mathbb{N}$ we have that $n \cdot m = m \cdot n$.

5. The number 1 is a **neutral element** or **identity element** with respect to multiplication, that is, for all $n \in \mathbb{N}$ we have that $n \cdot 1 = 1 \cdot n = n$.

6. Multiplication is **right distributive** over addition. That is, for all $n, m, k \in \mathbb{N}$ we have $(n + m) \cdot k = n \cdot k + m \cdot k$. 
Properties of Multiplication

1. Yes, it’s a binary operation.
2. Multiplication is an abbreviation for repeated addition of a number to itself.
3. Multiplication is **associative**, that is, for all $n, m, k \in \mathbb{N}$ we have that $(n \cdot m) \cdot k = n \cdot (m \cdot k)$.
4. Multiplication is **commutative**, that is, for all $n, m \in \mathbb{N}$ we have that $n \cdot m = m \cdot n$.
5. The number 1 is a **neutral element** or **identity element** with respect to multiplication, that is, for all $n \in \mathbb{N}$ we have that $n \cdot 1 = 1 \cdot n = n$.
6. Multiplication is **right distributive** over addition. That is, for all $n, m, k \in \mathbb{N}$ we have $(n + m) \cdot k = n \cdot k + m \cdot k$.

The proof of the last four is a bit tricky.
Using Properties Shortens Proofs

Proposition. Multiplication is left distributive over addition. That is, for all \( n, m, k \in \mathbb{N} \) we have \( n \cdot (m + k) = n \cdot m + n \cdot k \).

Proof. Let \( m, n, k \in \mathbb{N} \) be arbitrary, but fixed. Then \( n \cdot (m + k) = (m + k) \cdot n = mn + kn = nm + nk \).
Proposition.

Multiplication is left distributive over addition. That is, for all \( n, m, k \in \mathbb{N} \) we have \( n \cdot (m + k) = n \cdot m + n \cdot k \).
Using Properties Shortens Proofs

**Proposition.** Multiplication is left distributive over addition.
Using Properties Shortens Proofs

**Proposition.** *Multiplication is left distributive over addition.*

*That is, for all* \( n, m, k \in \mathbb{N} \)* *we have* \( n \cdot (m + k) = n \cdot m + n \cdot k \).*
Using Properties Shortens Proofs

**Proposition.** Multiplication is left distributive over addition. That is, for all \( n, m, k \in \mathbb{N} \) we have \( n \cdot (m + k) = n \cdot m + n \cdot k \).

**Proof.**
Using Properties Shortens Proofs

**Proposition.** Multiplication is left distributive over addition. That is, for all $n, m, k \in \mathbb{N}$ we have $n \cdot (m + k) = n \cdot m + n \cdot k$.

**Proof.** Let $m, n, k \in \mathbb{N}$ be arbitrary, but fixed.
Using Properties Shortens Proofs

**Proposition.** Multiplication is left distributive over addition. That is, for all \( n, m, k \in \mathbb{N} \) we have \( n \cdot (m + k) = n \cdot m + n \cdot k \).

**Proof.** Let \( m, n, k \in \mathbb{N} \) be arbitrary, but fixed. Then

\[
n(m + k)
\]
Using Properties Shortens Proofs

**Proposition.** *Multiplication is left distributive over addition.*

That is, for all \( n, m, k \in \mathbb{N} \) we have \( n \cdot (m + k) = n \cdot m + n \cdot k \).

**Proof.** Let \( m, n, k \in \mathbb{N} \) be arbitrary, but fixed. Then

\[
n(m + k) = (m + k) \cdot n
\]
Using Properties Shortens Proofs

**Proposition.** *Multiplication is left distributive over addition.*
That is, for all \( n, m, k \in \mathbb{N} \) we have \( n \cdot (m + k) = n \cdot m + n \cdot k \).

**Proof.** Let \( m, n, k \in \mathbb{N} \) be arbitrary, but fixed. Then
\[
 n(m + k) = (m + k) \cdot n \\
= mn + kn
\]
Using Properties Shortens Proofs

**Proposition.** *Multiplication is left distributive over addition.*

*That is, for all* $n, m, k \in \mathbb{N}$ *we have* $n \cdot (m + k) = n \cdot m + n \cdot k$.

**Proof.** Let $m, n, k \in \mathbb{N}$ be arbitrary, but fixed. Then

\[
n(m + k) = (m + k) \cdot n
\]
\[
= mn + kn
\]
\[
= nm + nk
\]
Using Properties Shortens Proofs

**Proposition.** *Multiplication is left distributive over addition.*

That is, for all \( n, m, k \in \mathbb{N} \) we have \( n \cdot (m + k) = n \cdot m + n \cdot k \).

**Proof.** Let \( m, n, k \in \mathbb{N} \) be arbitrary, but fixed. Then

\[
\begin{align*}
n(m + k) &= (m + k) \cdot n \\
        &= mn + kn \\
        &= nm + nk
\end{align*}
\]
FOIL
FOIL

Proposition.
**FOIL**

**Proposition.** Let \( a, b, c, d \in \mathbb{N} \). Then

\[
(a + b)(c + d) = (ac + ad) + (bc + bd).
\]
**FOIL**

**Proposition.** Let $a, b, c, d \in \mathbb{N}$. Then

$$(a + b)(c + d) = (ac + ad) + (bc + bd).$$

**Proof.**
FOIL

**Proposition.** Let \( a, b, c, d \in \mathbb{N} \). Then

\[
(a + b)(c + d) = (ac + ad) + (bc + bd).
\]

**Proof.**

\[
(a + b)(c + d)
\]
**FOIL**

**Proposition.** Let $a, b, c, d \in \mathbb{N}$. Then

$$(a + b)(c + d) = (ac + ad) + (bc + bd).$$

**Proof.**

$$(a + b)(c + d) = (a + b)c + (a + b)d$$
FOIL

**Proposition.** Let $a, b, c, d \in \mathbb{N}$. Then

$$(a + b)(c + d) = (ac + ad) + (bc + bd).$$

**Proof.**

$$
(a + b)(c + d) = (a + b)c + (a + b)d \\
= (ac + bc) + (ad + bd)
$$
**FOIL**

**Proposition.** Let $a, b, c, d \in \mathbb{N}$. Then

$$(a + b)(c + d) = (ac + ad) + (bc + bd).$$

**Proof.**

$$(a + b)(c + d) = (a + b)c + (a + b)d$$

$$= (ac + bc) + (ad + bd)$$

$$= ((ac + bc) + ad) + bd$$
**FOIL**

**Proposition.** Let $a, b, c, d \in \mathbb{N}$. Then

$$(a + b)(c + d) = (ac + ad) + (bc + bd).$$

**Proof.**

$$(a + b)(c + d) = (a + b)c + (a + b)d$$
$$= (ac + bc) + (ad + bd)$$
$$= ((ac + bc) + ad) + bd$$
$$= (ac + (bc + ad)) + bd$$
**FOIL**

**Proposition.** Let $a, b, c, d \in \mathbb{N}$. Then

$$(a + b)(c + d) = (ac + ad) + (bc + bd).$$

**Proof.**

$$(a + b)(c + d) = (a + b)c + (a + b)d$$

$$= (ac + bc) + (ad + bd)$$

$$= ((ac + bc) + ad) + bd$$

$$= (ac + (bc + ad)) + bd$$

$$= (ac + (ad + bc)) + bd$$
**FOIL**

**Proposition.** Let $a, b, c, d \in \mathbb{N}$. Then

$$(a + b)(c + d) = (ac + ad) + (bc + bd).$$

**Proof.**

$$(a + b)(c + d) = (a + b)c + (a + b)d$$

$$= (ac + bc) + (ad + bd)$$

$$= ((ac + bc) + ad) + bd$$

$$= (ac + (bc + ad)) + bd$$

$$= (ac + (ad + bc)) + bd$$

$$= ((ac + ad) + bc) + bd$$
**FOIL**

**Proposition.** Let $a, b, c, d \in \mathbb{N}$. Then

$$(a + b)(c + d) = (ac + ad) + (bc + bd).$$

**Proof.**

$$(a + b)(c + d) = (a + b)c + (a + b)d$$

$$= (ac + bc) + (ad + bd)$$

$$= ((ac + bc) + ad) + bd$$

$$= (ac + (bc + ad)) + bd$$

$$= (ac + (ad + bc)) + bd$$

$$= ((ac + ad) + bc) + bd$$

$$= (ac + ad) + (bc + bd)$$
**FOIL**

**Proposition.** Let $a, b, c, d \in \mathbb{N}$. Then

$$(a + b)(c + d) = (ac + ad) + (bc + bd).$$

**Proof.**

$$(a + b)(c + d) = (a + b)c + (a + b)d$$

$$= (ac + bc) + (ad + bd)$$

$$= ((ac + bc) + ad) + bd$$

$$= (ac + (bc + ad)) + bd$$

$$= (ac + (ad + bc)) + bd$$

$$= ((ac + ad) + bc) + bd$$

$$= (ac + ad) + (bc + bd)$$