Rules of Arithmetic on $\mathbb{N}$

Recall

Recall

The operations $x + y, x \cdot y$ and x^y on $\mathbb{N}$ are defined by recursion on the last variable.

Recall

The operations $x + y$, $x \cdot y$ and x^y on $\mathbb{N}$ are defined by recursion on the last variable. (That is, these operations are defined by recursion on y.)

Recall

The operations $x + y$, $x \cdot y$ and x^y on $\mathbb{N}$ are defined by recursion on the last variable. (That is, these operations are defined by recursion on y.) These definitions are:

Recall

The operations $x + y, x \cdot y$ and x^y on $\mathbb{N}$ are defined by recursion on the last variable. (That is, these operations are defined by recursion on y.) These definitions are:

Addition

$$\begin{aligned} m + 0 &:= m && \text{(IC)} \\ m + S(n) &:= S(m + n) && \text{(RR)} \end{aligned}$$

Recall

The operations $x + y$, $x \cdot y$ and x^y on $\mathbb{N}$ are defined by recursion on the last variable. (That is, these operations are defined by recursion on y.) These definitions are:

Addition

$$\begin{aligned} m + 0 &:= m && \text{(IC)} \\ m + S(n) &:= S(m+n) && \text{(RR)} \end{aligned}$$

Multiplication

$$\begin{aligned} m \cdot 0 &:= 0 && \text{(IC)} \\ m \cdot S(n) &:= (m \cdot n) + m && \text{(RR)} \end{aligned}$$

Recall

The operations $x + y, x \cdot y$ and x^y on $\mathbb{N}$ are defined by recursion on the last variable. (That is, these operations are defined by recursion on y.) These definitions are:

Addition

$$m + 0 := m \quad \text{(IC)}$$
$$m + S(n) := S(m + n) \quad \text{(RR)}$$

Multiplication

$$m \cdot 0 := 0 \quad \text{(IC)}$$
$$m \cdot S(n) := (m \cdot n) + m \quad \text{(RR)}$$

Exponentiation

$$m^0 := 1 \quad \text{(IC)}$$
$$m^{S(n)} := (m^n) \cdot m \quad \text{(RR)}$$

The Laws of 0 and Successor

The Laws of 0 and Successor

The element $0 \in \mathbb{N}$ and the unary (= 1-place) operation $S\colon \mathbb{N} \to \mathbb{N}$ were defined long ago,

The Laws of 0 and Successor

The element $0 \in \mathbb{N}$ and the unary (= 1-place) operation $S\colon \mathbb{N} \to \mathbb{N}$ were defined long ago, without the use of recursion,

The Laws of 0 and Successor

The element $0 \in \mathbb{N}$ and the unary (= 1-place) operation $S\colon \mathbb{N} \to \mathbb{N}$ were defined long ago, without the use of recursion, namely $0 := \emptyset$ and $S(x) = x \cup \{x\}$.

The Laws of 0 and Successor

The element $0 \in \mathbb{N}$ and the unary (= 1-place) operation $S \colon \mathbb{N} \to \mathbb{N}$ were defined long ago, without the use of recursion, namely $0 := \emptyset$ and $S(x) = x \cup \{x\}$. The Laws of Successor are:

The Laws of 0 and Successor

The element $0 \in \mathbb{N}$ and the unary (= 1-place) operation $S\colon \mathbb{N} \to \mathbb{N}$ were defined long ago, without the use of recursion, namely $0 := \emptyset$ and $S(x) = x \cup \{x\}$. The Laws of Successor are:

(a) 0 is not a successor.

The Laws of 0 and Successor

The element $0 \in \mathbb{N}$ and the unary (= 1-place) operation $S\colon \mathbb{N} \to \mathbb{N}$ were defined long ago, without the use of recursion, namely $0 := \emptyset$ and $S(x) = x \cup \{x\}$. The Laws of Successor are:

(a) 0 is not a successor.

The Laws of 0 and Successor

The element $0 \in \mathbb{N}$ and the unary (= 1-place) operation $S\colon \mathbb{N} \to \mathbb{N}$ were defined long ago, without the use of recursion, namely $0 := \emptyset$ and $S(x) = x \cup \{x\}$. The Laws of Successor are:

(a) 0 is not a successor. Every nonzero natural number is a successor.

The Laws of 0 and Successor

The element $0 \in \mathbb{N}$ and the unary (= 1-place) operation $S\colon \mathbb{N} \to \mathbb{N}$ were defined long ago, without the use of recursion, namely $0 := \emptyset$ and $S(x) = x \cup \{x\}$. The Laws of Successor are:

(a) 0 is not a successor. Every nonzero natural number is a successor.

(b) Successor is injective.

The Laws of 0 and Successor

The element $0 \in \mathbb{N}$ and the unary (= 1-place) operation $S\colon \mathbb{N} \to \mathbb{N}$ were defined long ago, without the use of recursion, namely $0 := \emptyset$ and $S(x) = x \cup \{x\}$. The Laws of Successor are:

(a) 0 is not a successor. Every nonzero natural number is a successor.

(b) Successor is injective.

The Laws of 0 and Successor

The element $0 \in \mathbb{N}$ and the unary (= 1-place) operation $S\colon \mathbb{N} \to \mathbb{N}$ were defined long ago, without the use of recursion, namely $0 := \emptyset$ and $S(x) = x \cup \{x\}$. The Laws of Successor are:

(a) 0 is not a successor. Every nonzero natural number is a successor.

(b) Successor is injective. ($S(m) = S(n)$ implies $m = n$.)

We proved these statements already.

The Laws of Addition

The Laws of Addition

We will now practice using Induction to prove the Laws of Addition.

The Laws of Addition

We will now practice using Induction to prove the Laws of Addition. These Laws are:

Laws of addition.

The Laws of Addition

We will now practice using Induction to prove the Laws of Addition. These Laws are:

Laws of addition.

(a) $S(n) = n + 1, 1 + n = S(n)$

The Laws of Addition

We will now practice using Induction to prove the Laws of Addition. These Laws are:

Laws of addition.

(a) $S(n) = n + 1, 1 + n = S(n)$

The Laws of Addition

We will now practice using Induction to prove the Laws of Addition. These Laws are:

Laws of addition.

(a) $S(n) = n + 1, 1 + n = S(n)$

(b) (Associative Law) $m + (n + k) = (m + n) + k$

The Laws of Addition

We will now practice using Induction to prove the Laws of Addition. These Laws are:

Laws of addition.

(a) $S(n) = n + 1, 1 + n = S(n)$

(b) (Associative Law) $m + (n + k) = (m + n) + k$

The Laws of Addition

We will now practice using Induction to prove the Laws of Addition. These Laws are:

Laws of addition.

(a) $S(n) = n + 1, 1 + n = S(n)$

(b) (Associative Law) $m + (n + k) = (m + n) + k$

(c) (Unit Law for 0) $m + 0 = 0 + m = m$

The Laws of Addition

We will now practice using Induction to prove the Laws of Addition. These Laws are:

Laws of addition.

(a) $S(n) = n + 1, 1 + n = S(n)$

(b) (Associative Law) $m + (n + k) = (m + n) + k$

(c) (Unit Law for 0) $m + 0 = 0 + m = m$

The Laws of Addition

We will now practice using Induction to prove the Laws of Addition. These Laws are:

Laws of addition.

(a) $S(n) = n + 1, 1 + n = S(n)$

(b) (Associative Law) $m + (n + k) = (m + n) + k$

(c) (Unit Law for 0) $m + 0 = 0 + m = m$

(d) (Commutative Law) $m + n = n + m$

The Laws of Addition

We will now practice using Induction to prove the Laws of Addition. These Laws are:

Laws of addition.

(a) $S(n) = n + 1$, $1 + n = S(n)$

(b) (Associative Law) $m + (n + k) = (m + n) + k$

(c) (Unit Law for 0) $m + 0 = 0 + m = m$

(d) (Commutative Law) $m + n = n + m$

The Laws of Addition

We will now practice using Induction to prove the Laws of Addition. These Laws are:

Laws of addition.

(a) $S(n) = n + 1, 1 + n = S(n)$

(b) (Associative Law) $m + (n + k) = (m + n) + k$

(c) (Unit Law for 0) $m + 0 = 0 + m = m$

(d) (Commutative Law) $m + n = n + m$

(e) (Irreducibility of 0) $m + n = 0$ implies $m = n = 0$

The Laws of Addition

We will now practice using Induction to prove the Laws of Addition. These Laws are:

Laws of addition.

(a) $S(n) = n + 1, 1 + n = S(n)$

(b) (Associative Law) $m + (n + k) = (m + n) + k$

(c) (Unit Law for 0) $m + 0 = 0 + m = m$

(d) (Commutative Law) $m + n = n + m$

(e) (Irreducibility of 0) $m + n = 0$ implies $m = n = 0$

The Laws of Addition

We will now practice using Induction to prove the Laws of Addition. These Laws are:

Laws of addition.

(a) $S(n) = n + 1$, $1 + n = S(n)$

(b) (Associative Law) $m + (n + k) = (m + n) + k$

(c) (Unit Law for 0) $m + 0 = 0 + m = m$

(d) (Commutative Law) $m + n = n + m$

(e) (Irreducibility of 0) $m + n = 0$ implies $m = n = 0$

(f) ((Right) Cancellation) $m + k = n + k$ implies $m = n$

The Laws of Addition

We will now practice using Induction to prove the Laws of Addition. These Laws are:

Laws of addition.

(a) $S(n) = n + 1, 1 + n = S(n)$

(b) (Associative Law) $m + (n + k) = (m + n) + k$

(c) (Unit Law for 0) $m + 0 = 0 + m = m$

(d) (Commutative Law) $m + n = n + m$

(e) (Irreducibility of 0) $m + n = 0$ implies $m = n = 0$

(f) ((Right) Cancellation) $m + k = n + k$ implies $m = n$

The Laws of Addition

We will now practice using Induction to prove the Laws of Addition. These Laws are:

Laws of addition.

(a) $S(n) = n + 1, 1 + n = S(n)$

(b) (Associative Law) $m + (n + k) = (m + n) + k$

(c) (Unit Law for 0) $m + 0 = 0 + m = m$

(d) (Commutative Law) $m + n = n + m$

(e) (Irreducibility of 0) $m + n = 0$ implies $m = n = 0$

(f) ((Right) Cancellation) $m + k = n + k$ implies $m = n$

Law (a): $S(n) = n + 1$

Law (a): $S(n) = n + 1$

This proof does not require induction.

Law (a): $S(n) = n + 1$

This proof does not require induction.

$$n + 1$$

Law (a): $S(n) = n + 1$

This proof does not require induction.

$$n + 1 \quad = n + S(0)$$

Law (a): $S(n) = n + 1$

This proof does not require induction.

$$n + 1 = n + S(0) \qquad \text{(Defn of 1)}$$

Law (a): $S(n) = n + 1$

This proof does not require induction.

$$\begin{aligned} n + 1 &= n + S(0) && \text{(Defn of 1)} \\ &= S(n + 0) \end{aligned}$$

Law (a): $S(n) = n + 1$

This proof does not require induction.

$$\begin{aligned} n + 1 &= n + S(0) && \text{(Defn of 1)} \\ &= S(n + 0) && \text{((RR), +)} \end{aligned}$$

Law (a): $S(n) = n + 1$

This proof does not require induction.

$$\begin{aligned} n + 1 &= n + S(0) && \text{(Defn of 1)} \\ &= S(n + 0) && ((\mathrm{RR}), +) \\ &= S(n) \end{aligned}$$

Law (a): $S(n) = n + 1$

This proof does not require induction.

$$
\begin{aligned}
n + 1 &= n + S(0) && \text{(Defn of 1)} \\
&= S(n + 0) && \text{((RR), +)} \\
&= S(n) && \text{((IC), +)}
\end{aligned}
$$

Law (a): $S(n) = n + 1$

This proof does not require induction.

$$\begin{aligned} n + 1 &= n + S(0) && \text{(Defn of 1)} \\ &= S(n + 0) && \text{((RR), +)} \\ &= S(n) && \text{((IC), +)} \quad \square \end{aligned}$$

Review of Induction

Review of Induction

A proof by Induction involves the following items:

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved.

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved.

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved. This should be formulated so that it is clear that the statement is equivalent to a sequence of statements that are indexed by the natural numbers:

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved. This should be formulated so that it is clear that the statement is equivalent to a sequence of statements that are indexed by the natural numbers:

$$S_0, S_1, S_2, S_3, \ldots$$

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved. This should be formulated so that it is clear that the statement is equivalent to a sequence of statements that are indexed by the natural numbers:

$$S_0, S_1, S_2, S_3, \ldots$$

2. A proof of the initial statement, S_0.

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved. This should be formulated so that it is clear that the statement is equivalent to a sequence of statements that are indexed by the natural numbers:

$$S_0, S_1, S_2, S_3, \ldots$$

2. A proof of the initial statement, S_0.

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved. This should be formulated so that it is clear that the statement is equivalent to a sequence of statements that are indexed by the natural numbers:

$$S_0, S_1, S_2, S_3, \ldots$$

2. A proof of the initial statement, S_0. This part of the argument is called the "Basis of Induction",

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved. This should be formulated so that it is clear that the statement is equivalent to a sequence of statements that are indexed by the natural numbers:

$$S_0, S_1, S_2, S_3, \ldots$$

2. A proof of the initial statement, S_0. This part of the argument is called the "Basis of Induction", or the "Base Case" of the proof.

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved. This should be formulated so that it is clear that the statement is equivalent to a sequence of statements that are indexed by the natural numbers:

$$S_0, S_1, S_2, S_3, \ldots$$

2. A proof of the initial statement, S_0. This part of the argument is called the "Basis of Induction", or the "Base Case" of the proof.

3. A proof that the implication $S_k \to S_{k+1}$ holds.

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved. This should be formulated so that it is clear that the statement is equivalent to a sequence of statements that are indexed by the natural numbers:

$$S_0, S_1, S_2, S_3, \ldots$$

2. A proof of the initial statement, S_0. This part of the argument is called the "Basis of Induction", or the "Base Case" of the proof.

3. A proof that the implication $S_k \to S_{k+1}$ holds.

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved. This should be formulated so that it is clear that the statement is equivalent to a sequence of statements that are indexed by the natural numbers:

$$S_0, S_1, S_2, S_3, \ldots$$

2. A proof of the initial statement, S_0. This part of the argument is called the "Basis of Induction", or the "Base Case" of the proof.

3. A proof that the implication $S_k \to S_{k+1}$ holds. This means:

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved. This should be formulated so that it is clear that the statement is equivalent to a sequence of statements that are indexed by the natural numbers:

$$S_0, S_1, S_2, S_3, \ldots$$

2. A proof of the initial statement, S_0. This part of the argument is called the “Basis of Induction”, or the “Base Case” of the proof.

3. A proof that the implication $S_k \to S_{k+1}$ holds. This means: you may assume that the k-th statement is true

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved. This should be formulated so that it is clear that the statement is equivalent to a sequence of statements that are indexed by the natural numbers:

$$S_0, S_1, S_2, S_3, \ldots$$

2. A proof of the initial statement, S_0. This part of the argument is called the "Basis of Induction", or the "Base Case" of the proof.

3. A proof that the implication $S_k \to S_{k+1}$ holds. This means: you may assume that the k-th statement is true (this assumption is called the "Inductive Hypothesis")

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved. This should be formulated so that it is clear that the statement is equivalent to a sequence of statements that are indexed by the natural numbers:

$$S_0, S_1, S_2, S_3, \ldots$$

2. A proof of the initial statement, S_0. This part of the argument is called the "Basis of Induction", or the "Base Case" of the proof.

3. A proof that the implication $S_k \to S_{k+1}$ holds. This means: you may assume that the k-th statement is true (this assumption is called the "Inductive Hypothesis") and use this information to prove that the $(k+1)$-st statement is true.

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved. This should be formulated so that it is clear that the statement is equivalent to a sequence of statements that are indexed by the natural numbers:

$$S_0, S_1, S_2, S_3, \ldots$$

2. A proof of the initial statement, S_0. This part of the argument is called the "Basis of Induction", or the "Base Case" of the proof.

3. A proof that the implication $S_k \to S_{k+1}$ holds. This means: you may assume that the k-th statement is true (this assumption is called the "Inductive Hypothesis") and use this information to prove that the $(k+1)$-st statement is true. This part of the proof showing that the implication $S_k \to S_{k+1}$ holds is called the "Inductive Step".

Review of Induction

A proof by Induction involves the following items:

1. A statement of what is to be proved. This should be formulated so that it is clear that the statement is equivalent to a sequence of statements that are indexed by the natural numbers:

$$S_0, S_1, S_2, S_3, \ldots$$

2. A proof of the initial statement, S_0. This part of the argument is called the "Basis of Induction", or the "Base Case" of the proof.

3. A proof that the implication $S_k \to S_{k+1}$ holds. This means: you may assume that the k-th statement is true (this assumption is called the "Inductive Hypothesis") and use this information to prove that the $(k+1)$-st statement is true. This part of the proof showing that the implication $S_k \to S_{k+1}$ holds is called the "Inductive Step".

If both steps are accomplished, you have shown that S_n is true for all n.

The Associative Law: $m + (n + k) = (m + n) + k$

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction,

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m?

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n?

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable,

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k.

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n,

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n, the k-th statement to be proved is
$m + (n + k) = (m + n) + k$.

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n, the k-th statement to be proved is
$m + (n + k) = (m + n) + k$.

(Base Case: $k = 0$)

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n, the k-th statement to be proved is
$m + (n + k) = (m + n) + k.$

(Base Case: $k = 0$)

$$m + (n + 0)$$

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n, the k-th statement to be proved is
$m + (n + k) = (m + n) + k$.

(Base Case: $k = 0$)

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

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n, the k-th statement to be proved is
$m + (n + k) = (m + n) + k$.

(Base Case: $k = 0$)

$$m + (n + 0) = m + n \qquad ((\text{IC}), +)$$

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n, the k-th statement to be proved is
$m + (n + k) = (m + n) + k$.

(Base Case: $k = 0$)

$$\begin{aligned} m + (n + 0) &= m + n && ((\text{IC}), +) \\ &= (m + n) + 0 && ((\text{IC}), +) \end{aligned}$$

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n, the k-th statement to be proved is
$m + (n + k) = (m + n) + k$.

(Base Case: $k = 0$)

$$\begin{aligned} m + (n + 0) &= m + n && ((\mathrm{IC}), +) \\ &= (m + n) + 0 && ((\mathrm{IC}), +) \quad \square \end{aligned}$$

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n, the k-th statement to be proved is
$m + (n + k) = (m + n) + k$.

(Base Case: $k = 0$)

$$\begin{aligned} m + (n + 0) &= m + n && ((\text{IC}), +) \\ &= (m + n) + 0 && ((\text{IC}), +) \quad \square \end{aligned}$$

(Inductive Step: Assume true for k, prove true for $S(k)$)

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n, the k-th statement to be proved is
$m + (n + k) = (m + n) + k$.

(Base Case: $k = 0$)

$$\begin{aligned} m + (n + 0) &= m + n && ((\text{IC}), +) \\ &= (m + n) + 0 && ((\text{IC}), +) \quad \square \end{aligned}$$

(Inductive Step: Assume true for k, prove true for $S(k)$)

$$m + (n + S(k))$$

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n, the k-th statement to be proved is
$m + (n + k) = (m + n) + k$.

(Base Case: $k = 0$)

$$\begin{aligned} m + (n + 0) &= m + n && ((\text{IC}), +) \\ &= (m + n) + 0 && ((\text{IC}), +) \quad \square \end{aligned}$$

(Inductive Step: Assume true for k, prove true for $S(k)$)

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

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n, the k-th statement to be proved is
$m + (n + k) = (m + n) + k$.

(Base Case: $k = 0$)

$$\begin{aligned} m + (n + 0) &= m + n && ((\text{IC}), +) \\ &= (m + n) + 0 && ((\text{IC}), +) \quad \square \end{aligned}$$

(Inductive Step: Assume true for k, prove true for $S(k)$)

$$m + (n + S(k)) = m + S(n + k) \qquad ((\text{RR}), +)$$

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n, the k-th statement to be proved is $m + (n + k) = (m + n) + k$.

(Base Case: $k = 0$)

$$\begin{aligned} m + (n + 0) &= m + n && ((\text{IC}), +) \\ &= (m + n) + 0 && ((\text{IC}), +) \quad \square \end{aligned}$$

(Inductive Step: Assume true for k, prove true for $S(k)$)

$$\begin{aligned} m + (n + S(k)) &= m + S(n + k) && ((\text{RR}), +) \\ &= S(m + (n + k)) && ((\text{RR}), +) \end{aligned}$$

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n, the k-th statement to be proved is
$m + (n + k) = (m + n) + k$.

(Base Case: $k = 0$)

$$\begin{aligned} m + (n + 0) &= m + n && ((\text{IC}), +) \\ &= (m + n) + 0 && ((\text{IC}), +) \quad \square \end{aligned}$$

(Inductive Step: Assume true for k, prove true for $S(k)$)

$$\begin{aligned} m + (n + S(k)) &= m + S(n + k) && ((\text{RR}), +) \\ &= S(m + (n + k)) && ((\text{RR}), +) \\ &= S((m + n) + k) && (\text{IH}) \end{aligned}$$

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n, the k-th statement to be proved is
$m + (n + k) = (m + n) + k$.

(Base Case: $k = 0$)

$$\begin{aligned} m + (n + 0) &= m + n && ((\text{IC}), +) \\ &= (m + n) + 0 && ((\text{IC}), +) \quad \square \end{aligned}$$

(Inductive Step: Assume true for k, prove true for $S(k)$)

$$\begin{aligned} m + (n + S(k)) &= m + S(n + k) && ((\text{RR}), +) \\ &= S(m + (n + k)) && ((\text{RR}), +) \\ &= S((m + n) + k) && (\text{IH}) \\ &= (m + n) + S(k) && ((\text{RR}), +) \end{aligned}$$

The Associative Law: $m + (n + k) = (m + n) + k$

This will be proved by induction, but should we argue by induction on m? n? or k?

Experience shows that, since addition is defined by recursion on its last variable, we should prove properties of addition by induction on the last variable, k. Thus, for fixed values of m and n, the k-th statement to be proved is
$m + (n + k) = (m + n) + k$.

(Base Case: $k = 0$)

$$\begin{aligned} m + (n + 0) &= m + n && ((\text{IC}), +) \\ &= (m + n) + 0 && ((\text{IC}), +) \quad \square \end{aligned}$$

(Inductive Step: Assume true for k, prove true for $S(k)$)

$$\begin{aligned} m + (n + S(k)) &= m + S(n + k) && ((\text{RR}), +) \\ &= S(m + (n + k)) && ((\text{RR}), +) \\ &= S((m + n) + k) && (\text{IH}) \\ &= (m + n) + S(k) && ((\text{RR}), +) \quad \square \end{aligned}$$

Unit Law for 0: $m + 0 = 0 + m = m$

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$.

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

(Base Case:

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

(Base Case: $m = 0$)

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

(Base Case: $m = 0$)

$$0 + 0$$

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

(Base Case: $m = 0$)

$$0 + 0 = 0$$

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

(Base Case: $m = 0$)

$$0 + 0 = 0 \qquad ((\text{IC}), +)$$

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

(Base Case: $m = 0$)

$$0 + 0 = 0 \qquad ((\mathrm{IC}), +) \quad \square$$

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

(Base Case: $m = 0$)

$$0 + 0 = 0 \qquad ((\mathrm{IC}), +) \quad \square$$

(Inductive Step:

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

(Base Case: $m = 0$)

$$0 + 0 = 0 \qquad ((\text{IC}), +) \quad \square$$

(Inductive Step: Assume true for m, prove true for $S(m)$)

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

(Base Case: $m = 0$)

$$0 + 0 \quad = 0 \qquad\qquad ((\mathrm{IC}), +) \quad \square$$

(Inductive Step: Assume true for m, prove true for $S(m)$)

$$0 + S(m)$$

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

(Base Case: $m = 0$)

$$0 + 0 = 0 \qquad ((\text{IC}), +) \quad \square$$

(Inductive Step: Assume true for m, prove true for $S(m)$)

$$0 + S(m) = S(0 + m)$$

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

(Base Case: $m = 0$)

$$0 + 0 = 0 \qquad ((\text{IC}), +) \quad \square$$

(Inductive Step: Assume true for m, prove true for $S(m)$)

$$0 + S(m) = S(0 + m) \qquad ((\text{RR}), +)$$

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

(Base Case: $m = 0$)

$$0 + 0 = 0 \qquad ((\text{IC}), +) \quad \square$$

(Inductive Step: Assume true for m, prove true for $S(m)$)

$$\begin{aligned} 0 + S(m) &= S(0 + m) && ((\text{RR}), +) \\ &= S(m) \end{aligned}$$

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

(Base Case: $m = 0$)

$$0 + 0 = 0 \qquad ((\text{IC}), +) \quad \square$$

(Inductive Step: Assume true for m, prove true for $S(m)$)

$$\begin{aligned} 0 + S(m) &= S(0 + m) && ((\text{RR}), +) \\ &= S(m) && (\text{IH}) \end{aligned}$$

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

(Base Case: $m = 0$)

$$0 + 0 = 0 \qquad ((\text{IC}), +) \quad \square$$

(Inductive Step: Assume true for m, prove true for $S(m)$)

$$\begin{aligned} 0 + S(m) &= S(0 + m) && ((\text{RR}), +) \\ &= S(m) && (\text{IH}) \quad \square \end{aligned}$$

Unit Law for 0: $m + 0 = 0 + m = m$

The fact that $m + 0 = m$ is part of the definition of addition, so we only need to prove that $\boxed{0 + m = m}$. We argue this by induction on m.

(Base Case: $m = 0$)

$$0 + 0 = 0 \qquad ((\text{IC}), +) \quad \square$$

(Inductive Step: Assume true for m, prove true for $S(m)$)

$$\begin{aligned} 0 + S(m) &= S(0 + m) && ((\text{RR}), +) \\ &= S(m) && (\text{IH}) \quad \square \end{aligned}$$

This proves that $0 + m = m$ for all $m \in \mathbb{N}$.

Commutative Law: $m + n = n + m$

Commutative Law: $m + n = n + m$

We argue this by induction on n.

Commutative Law: $m + n = n + m$

We argue this by induction on n.

(Base Case:

Commutative Law: $m + n = n + m$

We argue this by induction on n.

(Base Case: $n = 0$)

Commutative Law: $m + n = n + m$

We argue this by induction on n.

(Base Case: $n = 0$)

$$m + 0$$

Commutative Law: $m + n = n + m$

We argue this by induction on n.

(Base Case: $n = 0$)

$$m + 0 \quad = 0 + m$$

Commutative Law: $m + n = n + m$

We argue this by induction on n.

(Base Case: $n = 0$)

$$m + 0 \quad = 0 + m \qquad\qquad \text{(Part (c), +)}$$

Commutative Law: $m + n = n + m$

We argue this by induction on n.

(Base Case: $n = 0$)

$$m + 0 = 0 + m \qquad \text{(Part (c), +)}$$

At this point we should expect to prove the Inductive Step.

Commutative Law: $m + n = n + m$

We argue this by induction on n.

(Base Case: $n = 0$)

$$m + 0 \quad = 0 + m \qquad \text{(Part (c), +)}$$

At this point we should expect to prove the Inductive Step. However, an attempt to do this reveals that it would help if we already knew that the "$n = 1$ case" of the Commutative Law was true.

Commutative Law: $m + n = n + m$

We argue this by induction on n.

(Base Case: $n = 0$)

$$m + 0 = 0 + m \qquad \text{(Part (c), +)}$$

At this point we should expect to prove the Inductive Step. However, an attempt to do this reveals that it would help if we already knew that the "$n = 1$ case" of the Commutative Law was true. That is, it would help to know that "$m + 1 = 1 + m$" holds for all m.

Commutative Law: $m + n = n + m$

We argue this by induction on n.

(Base Case: $n = 0$)

$$m + 0 = 0 + m \qquad \text{(Part (c), +)}$$

At this point we should expect to prove the Inductive Step. However, an attempt to do this reveals that it would help if we already knew that the "$n = 1$ case" of the Commutative Law was true. That is, it would help to know that "$m + 1 = 1 + m$" holds for all m. Let's separate this out as a Lemma, which we will prove by induction.

Proving the Lemma

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$0 + 1$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$0 + 1 \quad = 0 + S(0)$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$0 + 1 = 0 + S(0) \qquad \text{(Defn of 1)}$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$\begin{aligned} 0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\ &= S(0 + 0) \end{aligned}$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$\begin{aligned} 0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\ &= S(0 + 0) && ((\text{RR}), +) \end{aligned}$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$\begin{aligned} 0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\ &= S(0 + 0) && ((\mathrm{RR}), +) \\ &= S(0) \end{aligned}$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$\begin{aligned} 0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\ &= S(0 + 0) && ((\mathrm{RR}), +) \\ &= S(0) && ((\mathrm{IC}), +) \end{aligned}$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$\begin{aligned} 0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\ &= S(0 + 0) && ((\text{RR}), +) \\ &= S(0) && ((\text{IC}), +) \\ &= 1 \end{aligned}$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$
\begin{aligned}
0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\
&= S(0 + 0) && ((\text{RR}), +) \\
&= S(0) && ((\text{IC}), +) \\
&= 1 && \text{(Defn of 1)}
\end{aligned}
$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$
\begin{aligned}
0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\
&= S(0 + 0) && ((\text{RR}), +) \\
&= S(0) && ((\text{IC}), +) \\
&= 1 && \text{(Defn of 1)} \\
&= 1 + 0
\end{aligned}
$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$\begin{aligned} 0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\ &= S(0 + 0) && ((\text{RR}), +) \\ &= S(0) && ((\text{IC}), +) \\ &= 1 && \text{(Defn of 1)} \\ &= 1 + 0 && ((\text{IC}), +) \end{aligned}$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$\begin{aligned} 0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\ &= S(0 + 0) && ((\text{RR}), +) \\ &= S(0) && ((\text{IC}), +) \\ &= 1 && \text{(Defn of 1)} \\ &= 1 + 0 && ((\text{IC}), +) \quad \square \end{aligned}$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$\begin{aligned} 0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\ &= S(0 + 0) && ((\text{RR}), +) \\ &= S(0) && ((\text{IC}), +) \\ &= 1 && \text{(Defn of 1)} \\ &= 1 + 0 && ((\text{IC}), +) \quad \square \end{aligned}$$

(Inductive Step:

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$\begin{aligned} 0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\ &= S(0 + 0) && ((\text{RR}), +) \\ &= S(0) && ((\text{IC}), +) \\ &= 1 && \text{(Defn of 1)} \\ &= 1 + 0 && ((\text{IC}), +) \quad \square \end{aligned}$$

(Inductive Step: Assume $m + 1 = 1 + m$ for some m, prove $S(m) + 1 = 1 + S(m)$)

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$
\begin{aligned}
0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\
&= S(0 + 0) && ((\text{RR}), +) \\
&= S(0) && ((\text{IC}), +) \\
&= 1 && \text{(Defn of 1)} \\
&= 1 + 0 && ((\text{IC}), +) \quad \square
\end{aligned}
$$

(Inductive Step: Assume $m + 1 = 1 + m$ for some m, prove $S(m) + 1 = 1 + S(m)$)

$$1 + S(m)$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$\begin{aligned} 0+1 &= 0 + S(0) && \text{(Defn of 1)} \\ &= S(0+0) && \text{((RR), +)} \\ &= S(0) && \text{((IC), +)} \\ &= 1 && \text{(Defn of 1)} \\ &= 1+0 && \text{((IC), +)} \quad \square \end{aligned}$$

(Inductive Step: Assume $m + 1 = 1 + m$ for some m, prove $S(m) + 1 = 1 + S(m)$)

$$1 + S(m) \quad = S(1+m)$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$
\begin{aligned}
0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\
&= S(0 + 0) && \text{((RR), +)} \\
&= S(0) && \text{((IC), +)} \\
&= 1 && \text{(Defn of 1)} \\
&= 1 + 0 && \text{((IC), +)} \quad \square
\end{aligned}
$$

(Inductive Step: Assume $m + 1 = 1 + m$ for some m, prove $S(m) + 1 = 1 + S(m)$)

$$
1 + S(m) = S(1 + m) \qquad \text{((RR), +)}
$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$\begin{aligned} 0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\ &= S(0 + 0) && ((\text{RR}), +) \\ &= S(0) && ((\text{IC}), +) \\ &= 1 && \text{(Defn of 1)} \\ &= 1 + 0 && ((\text{IC}), +) \quad \square \end{aligned}$$

(Inductive Step: Assume $m + 1 = 1 + m$ for some m, prove $S(m) + 1 = 1 + S(m)$)

$$\begin{aligned} 1 + S(m) &= S(1 + m) && ((\text{RR}), +) \\ &= S(m + 1) \end{aligned}$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$\begin{aligned} 0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\ &= S(0 + 0) && ((\text{RR}), +) \\ &= S(0) && ((\text{IC}), +) \\ &= 1 && \text{(Defn of 1)} \\ &= 1 + 0 && ((\text{IC}), +) \quad \square \end{aligned}$$

(Inductive Step: Assume $m + 1 = 1 + m$ for some m, prove $S(m) + 1 = 1 + S(m)$)

$$\begin{aligned} 1 + S(m) &= S(1 + m) && ((\text{RR}), +) \\ &= S(m + 1) && \text{(IH)} \end{aligned}$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$\begin{aligned}
0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\
&= S(0 + 0) && \text{((RR), +)} \\
&= S(0) && \text{((IC), +)} \\
&= 1 && \text{(Defn of 1)} \\
&= 1 + 0 && \text{((IC), +)} \quad \square
\end{aligned}$$

(Inductive Step: Assume $m + 1 = 1 + m$ for some m, prove $S(m) + 1 = 1 + S(m)$)

$$\begin{aligned}
1 + S(m) &= S(1 + m) && \text{((RR), +)} \\
&= S(m + 1) && \text{(IH)} \\
&= S(S(m))
\end{aligned}$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$\begin{aligned} 0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\ &= S(0 + 0) && \text{((RR), +)} \\ &= S(0) && \text{((IC), +)} \\ &= 1 && \text{(Defn of 1)} \\ &= 1 + 0 && \text{((IC), +)} \quad \square \end{aligned}$$

(Inductive Step: Assume $m + 1 = 1 + m$ for some m, prove $S(m) + 1 = 1 + S(m)$)

$$\begin{aligned} 1 + S(m) &= S(1 + m) && \text{((RR), +)} \\ &= S(m + 1) && \text{(IH)} \\ &= S(S(m)) && \text{(Part (a), } S\text{)} \end{aligned}$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$
\begin{aligned}
0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\
&= S(0 + 0) && \text{((RR), +)} \\
&= S(0) && \text{((IC), +)} \\
&= 1 && \text{(Defn of 1)} \\
&= 1 + 0 && \text{((IC), +)} \quad \square
\end{aligned}
$$

(Inductive Step: Assume $m + 1 = 1 + m$ for some m, prove $S(m) + 1 = 1 + S(m)$)

$$
\begin{aligned}
1 + S(m) &= S(1 + m) && \text{((RR), +)} \\
&= S(m + 1) && \text{(IH)} \\
&= S(S(m)) && \text{(Part (a), } S\text{)} \\
&= S(m) + 1
\end{aligned}
$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$
\begin{aligned}
0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\
&= S(0 + 0) && \text{((RR), +)} \\
&= S(0) && \text{((IC), +)} \\
&= 1 && \text{(Defn of 1)} \\
&= 1 + 0 && \text{((IC), +)} \quad \square
\end{aligned}
$$

(Inductive Step: Assume $m + 1 = 1 + m$ for some m, prove $S(m) + 1 = 1 + S(m)$)

$$
\begin{aligned}
1 + S(m) &= S(1 + m) && \text{((RR), +)} \\
&= S(m + 1) && \text{(IH)} \\
&= S(S(m)) && \text{(Part (a), } S\text{)} \\
&= S(m) + 1 && \text{(Part (a), } S\text{)}
\end{aligned}
$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$
\begin{aligned}
0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\
&= S(0 + 0) && \text{((RR), +)} \\
&= S(0) && \text{((IC), +)} \\
&= 1 && \text{(Defn of 1)} \\
&= 1 + 0 && \text{((IC), +)} \quad \square
\end{aligned}
$$

(Inductive Step: Assume $m + 1 = 1 + m$ for some m, prove $S(m) + 1 = 1 + S(m)$)

$$
\begin{aligned}
1 + S(m) &= S(1 + m) && \text{((RR), +)} \\
&= S(m + 1) && \text{(IH)} \\
&= S(S(m)) && \text{(Part (a), } S\text{)} \\
&= S(m) + 1 && \text{(Part (a), } S\text{)} \quad \square
\end{aligned}
$$

Proving the Lemma

Lemma. $m + 1 = 1 + m$ holds for all $m \in \mathbb{N}$.

Proof of Lemma.
(Base Case: $m = 0$)

$$\begin{aligned} 0 + 1 &= 0 + S(0) && \text{(Defn of 1)} \\ &= S(0 + 0) && \text{((RR), +)} \\ &= S(0) && \text{((IC), +)} \\ &= 1 && \text{(Defn of 1)} \\ &= 1 + 0 && \text{((IC), +)} \quad \square \end{aligned}$$

(Inductive Step: Assume $m + 1 = 1 + m$ for some m, prove $S(m) + 1 = 1 + S(m)$)

$$\begin{aligned} 1 + S(m) &= S(1 + m) && \text{((RR), +)} \\ &= S(m + 1) && \text{(IH)} \\ &= S(S(m)) && \text{(Part (a), } S) \\ &= S(m) + 1 && \text{(Part (a), } S) \quad \square \end{aligned}$$

Completing the proof of the Commutative Law

Completing the proof of the Commutative Law

(Inductive Step:

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$m + S(n)$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$m + S(n) \quad = S(m + n)$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$m + S(n) = S(m + n) \qquad ((\mathrm{RR}), +)$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$\begin{aligned} m + S(n) &= S(m + n) && ((\text{RR}), +) \\ &= S(n + m) \end{aligned}$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$\begin{aligned} m + S(n) &= S(m + n) && ((\text{RR}), +) \\ &= S(n + m) && (\text{IH}) \end{aligned}$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$\begin{aligned} m + S(n) &= S(m + n) && ((\mathrm{RR}), +) \\ &= S(n + m) && (\mathrm{IH}) \\ &= n + S(m) \end{aligned}$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$
\begin{aligned}
m + S(n) &= S(m + n) && ((\mathrm{RR}), +) \\
&= S(n + m) && (\mathrm{IH}) \\
&= n + S(m) && ((\mathrm{RR}), +)
\end{aligned}
$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$
\begin{aligned}
m + S(n) &= S(m+n) && ((\text{RR}), +) \\
&= S(n+m) && (\text{IH}) \\
&= n + S(m) && ((\text{RR}), +) \\
&= n + (m+1)
\end{aligned}
$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$\begin{aligned} m + S(n) &= S(m + n) && ((\mathrm{RR}), +) \\ &= S(n + m) && (\mathrm{IH}) \\ &= n + S(m) && ((\mathrm{RR}), +) \\ &= n + (m + 1) && (\text{Part (a)}, S) \end{aligned}$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$
\begin{aligned}
m + S(n) &= S(m + n) && \text{((RR), +)} \\
&= S(n + m) && \text{(IH)} \\
&= n + S(m) && \text{((RR), +)} \\
&= n + (m + 1) && \text{(Part (a), } S\text{)} \\
&= n + (1 + m)
\end{aligned}
$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$
\begin{aligned}
m + S(n) &= S(m + n) && ((\text{RR}), +) \\
&= S(n + m) && (\text{IH}) \\
&= n + S(m) && ((\text{RR}), +) \\
&= n + (m + 1) && (\text{Part (a)}, S) \\
&= n + (1 + m) && (\text{Lemma})
\end{aligned}
$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$
\begin{aligned}
m + S(n) &= S(m + n) && ((\text{RR}), +) \\
&= S(n + m) && (\text{IH}) \\
&= n + S(m) && ((\text{RR}), +) \\
&= n + (m + 1) && (\text{Part (a)}, S) \\
&= n + (1 + m) && (\text{Lemma}) \\
&= (n + 1) + m
\end{aligned}
$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$
\begin{aligned}
m + S(n) &= S(m + n) && \text{((RR), +)} \\
&= S(n + m) && \text{(IH)} \\
&= n + S(m) && \text{((RR), +)} \\
&= n + (m + 1) && \text{(Part (a), } S\text{)} \\
&= n + (1 + m) && \text{(Lemma)} \\
&= (n + 1) + m && \text{(Assoc. Law, +)}
\end{aligned}
$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$
\begin{aligned}
m + S(n) &= S(m+n) && \text{((RR), +)} \\
&= S(n+m) && \text{(IH)} \\
&= n + S(m) && \text{((RR), +)} \\
&= n + (m+1) && \text{(Part (a), } S\text{)} \\
&= n + (1+m) && \text{(Lemma)} \\
&= (n+1) + m && \text{(Assoc. Law, +)} \\
&= S(n) + m
\end{aligned}
$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$
\begin{aligned}
m + S(n) &= S(m + n) && ((\text{RR}), +) \\
&= S(n + m) && (\text{IH}) \\
&= n + S(m) && ((\text{RR}), +) \\
&= n + (m + 1) && (\text{Part (a)}, S) \\
&= n + (1 + m) && (\text{Lemma}) \\
&= (n + 1) + m && (\text{Assoc. Law}, +) \\
&= S(n) + m && (\text{Part (a)}, S)
\end{aligned}
$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m + n = n + m$ holds and derive that $m + S(n) = S(n) + m$.)

$$
\begin{aligned}
m + S(n) &= S(m + n) && ((\text{RR}), +) \\
&= S(n + m) && (\text{IH}) \\
&= n + S(m) && ((\text{RR}), +) \\
&= n + (m + 1) && (\text{Part (a)}, S) \\
&= n + (1 + m) && (\text{Lemma}) \\
&= (n + 1) + m && (\text{Assoc. Law}, +) \\
&= S(n) + m && (\text{Part (a)}, S) \quad \square
\end{aligned}
$$

Completing the proof of the Commutative Law

(Inductive Step: assume that $m+n=n+m$ holds and derive that $m+S(n)=S(n)+m$.)

$$\begin{aligned}
m+S(n) &= S(m+n) && \text{((RR), +)} \\
&= S(n+m) && \text{(IH)} \\
&= n+S(m) && \text{((RR), +)} \\
&= n+(m+1) && \text{(Part (a), } S\text{)} \\
&= n+(1+m) && \text{(Lemma)} \\
&= (n+1)+m && \text{(Assoc. Law, +)} \\
&= S(n)+m && \text{(Part (a), } S\text{)} \quad \square
\end{aligned}$$

This proves that $m+n=n+m$ for all $m,n \in \mathbb{N}$.

$+$-Irreducibility of 0: $m + n = 0$ implies $m = n = 0$.

$+$-Irreducibility of 0: $m + n = 0$ implies $m = n = 0$.

We do not need induction to prove this.

$+$-Irreducibility of 0: $m + n = 0$ implies $m = n = 0$.

We do not need induction to prove this.

Proof.

$+$-Irreducibility of 0: $m + n = 0$ implies $m = n = 0$.

We do not need induction to prove this.

Proof. If $n \neq 0$, then $n = S(k)$ by Part (a) of the Laws of Successor.

$+$-Irreducibility of 0: $m + n = 0$ implies $m = n = 0$.

We do not need induction to prove this.

Proof. If $n \neq 0$, then $n = S(k)$ by Part (a) of the Laws of Successor. Then $0 = m + n = m + S(k) = S(m + k)$,

$+$-Irreducibility of 0: $m + n = 0$ implies $m = n = 0$.

We do not need induction to prove this.

Proof. If $n \neq 0$, then $n = S(k)$ by Part (a) of the Laws of Successor. Then $0 = m + n = m + S(k) = S(m + k)$, contradicting that 0 is not a successor.

+-Irreducibility of 0: $m + n = 0$ implies $m = n = 0$.

We do not need induction to prove this.

Proof. If $n \neq 0$, then $n = S(k)$ by Part (a) of the Laws of Successor. Then $0 = m + n = m + S(k) = S(m + k)$, contradicting that 0 is not a successor. Hence $0 = m + n$ forces $n = 0$.

+-Irreducibility of 0: $m + n = 0$ implies $m = n = 0$.

We do not need induction to prove this.

Proof. If $n \neq 0$, then $n = S(k)$ by Part (a) of the Laws of Successor. Then $0 = m + n = m + S(k) = S(m + k)$, contradicting that 0 is not a successor. Hence $0 = m + n$ forces $n = 0$. But now $0 = m + n = m + 0 = m$, so $m = 0$ too. $\square$

Right Cancellation: $m + k = n + k$ implies $m = n$.

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$m$$

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$m = m + 0$$

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$m = m + 0 \qquad ((\text{IC}), +)$$

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$\begin{aligned} m &= m + 0 && ((\text{IC}), +) \\ &= n + 0 \end{aligned}$$

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$
\begin{aligned}
m &= m + 0 && ((\text{IC}), +) \\
&= n + 0 && (\text{assumption})
\end{aligned}
$$

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$\begin{aligned} m &= m + 0 && ((\text{IC}), +) \\ &= n + 0 && (\text{assumption}) \\ &= n \end{aligned}$$

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$\begin{aligned} m &= m + 0 && ((\text{IC}), +) \\ &= n + 0 && (\text{assumption}) \\ &= n && ((\text{IC}), +) \end{aligned}$$

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$\begin{aligned} m &= m + 0 && ((\text{IC}), +) \\ &= n + 0 && (\text{assumption}) \\ &= n && ((\text{IC}), +) \end{aligned}$$

(Inductive Step: Assume that $m + k = n + k$ implies $m = n$. Prove that $m + S(k) = n + S(k)$ implies $m = n$.)

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$\begin{aligned} m &= m + 0 && ((\text{IC}), +) \\ &= n + 0 && (\text{assumption}) \\ &= n && ((\text{IC}), +) \end{aligned}$$

(Inductive Step: Assume that $m + k = n + k$ implies $m = n$. Prove that $m + S(k) = n + S(k)$ implies $m = n$.)

Assume that $m + S(k) = n + S(k)$.

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$\begin{aligned} m &= m + 0 && ((\text{IC}), +) \\ &= n + 0 && (\text{assumption}) \\ &= n && ((\text{IC}), +) \end{aligned}$$

(Inductive Step: Assume that $m + k = n + k$ implies $m = n$. Prove that $m + S(k) = n + S(k)$ implies $m = n$.)

Assume that $m + S(k) = n + S(k)$. Then by ((RR), +) we have $S(m + k) = S(n + k)$.

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$\begin{aligned} m &= m + 0 && ((\text{IC}), +) \\ &= n + 0 && (\text{assumption}) \\ &= n && ((\text{IC}), +) \end{aligned}$$

(Inductive Step: Assume that $m + k = n + k$ implies $m = n$. Prove that $m + S(k) = n + S(k)$ implies $m = n$.)

Assume that $m + S(k) = n + S(k)$. Then by ((RR), +) we have $S(m + k) = S(n + k)$. But the successor function is injective, by Part (b) of the Laws of Successor.

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$\begin{aligned} m &= m + 0 && ((\text{IC}), +) \\ &= n + 0 && (\text{assumption}) \\ &= n && ((\text{IC}), +) \end{aligned}$$

(Inductive Step: Assume that $m + k = n + k$ implies $m = n$. Prove that $m + S(k) = n + S(k)$ implies $m = n$.)

Assume that $m + S(k) = n + S(k)$. Then by ((RR), +) we have $S(m + k) = S(n + k)$. But the successor function is injective, by Part (b) of the Laws of Successor. Thus, $m + k = n + k$.

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$\begin{aligned} m &= m + 0 && ((\text{IC}), +) \\ &= n + 0 && (\text{assumption}) \\ &= n && ((\text{IC}), +) \end{aligned}$$

(Inductive Step: Assume that $m + k = n + k$ implies $m = n$. Prove that $m + S(k) = n + S(k)$ implies $m = n$.)

Assume that $m + S(k) = n + S(k)$. Then by ((RR), +) we have $S(m + k) = S(n + k)$. But the successor function is injective, by Part (b) of the Laws of Successor. Thus, $m + k = n + k$. Now, by the inductive hypothesis, we derive that $m = n$.

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$\begin{aligned} m &= m + 0 && ((\text{IC}), +) \\ &= n + 0 && (\text{assumption}) \\ &= n && ((\text{IC}), +) \end{aligned}$$

(Inductive Step: Assume that $m + k = n + k$ implies $m = n$. Prove that $m + S(k) = n + S(k)$ implies $m = n$.)

Assume that $m + S(k) = n + S(k)$. Then by ((RR), +) we have $S(m + k) = S(n + k)$. But the successor function is injective, by Part (b) of the Laws of Successor. Thus, $m + k = n + k$. Now, by the inductive hypothesis, we derive that $m = n$. $\square$

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$\begin{aligned} m &= m + 0 && ((\text{IC}), +) \\ &= n + 0 && (\text{assumption}) \\ &= n && ((\text{IC}), +) \end{aligned}$$

(Inductive Step: Assume that $m + k = n + k$ implies $m = n$. Prove that $m + S(k) = n + S(k)$ implies $m = n$.)

Assume that $m + S(k) = n + S(k)$. Then by ((RR), +) we have $S(m + k) = S(n + k)$. But the successor function is injective, by Part (b) of the Laws of Successor. Thus, $m + k = n + k$. Now, by the inductive hypothesis, we derive that $m = n$. $\square$

Since we have already proved the Commutative Law, the Left Cancellation Law is also valid: $k + m = k + n$ implies $m = n$.

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$\begin{aligned} m &= m + 0 && ((\text{IC}), +) \\ &= n + 0 && (\text{assumption}) \\ &= n && ((\text{IC}), +) \end{aligned}$$

(Inductive Step: Assume that $m + k = n + k$ implies $m = n$. Prove that $m + S(k) = n + S(k)$ implies $m = n$.)

Assume that $m + S(k) = n + S(k)$. Then by ((RR), +) we have $S(m + k) = S(n + k)$. But the successor function is injective, by Part (b) of the Laws of Successor. Thus, $m + k = n + k$. Now, by the inductive hypothesis, we derive that $m = n$. $\square$

Since we have already proved the Commutative Law, the Left Cancellation Law is also valid: $k + m = k + n$ implies $m = n$.
(Proof:

Right Cancellation: $m + k = n + k$ implies $m = n$.

(Base Case: $k = 0$)

$$\begin{aligned} m &= m + 0 && ((\text{IC}), +) \\ &= n + 0 && (\text{assumption}) \\ &= n && ((\text{IC}), +) \end{aligned}$$

(Inductive Step: Assume that $m + k = n + k$ implies $m = n$. Prove that $m + S(k) = n + S(k)$ implies $m = n$.)

Assume that $m + S(k) = n + S(k)$. Then by ((RR), +) we have $S(m + k) = S(n + k)$. But the successor function is injective, by Part (b) of the Laws of Successor. Thus, $m + k = n + k$. Now, by the inductive hypothesis, we derive that $m = n$. $\square$

Since we have already proved the Commutative Law, the Left Cancellation Law is also valid: $k + m = k + n$ implies $m = n$.
(Proof: $k + m = k + n$ implies $m + k = n + k$ implies $m = n$.)