# 0 *Nonnegative integers*


Last Updated: 9 January 2023

Leopold Kronecker (1823–1891) famously declared that "Dear God made the whole numbers, all else is the work of man". This phrase ambiguously refers to the set $\mathbb{N}$ of nonnegative integers or the larger set $\mathbb{Z}$ of integers, but this chapter focuses exclusively on the smaller set. Familiar to people of ancient times, it actually took over two millennia to gain a full understanding of these numbers.

The dictum "Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk" was allegedly uttered by Kronecker in Berlin in 1886. It first appeared in print in the memorial article: H. Weber, *Leopold Kronecker*, Mathematische Annalen **43** (1893) 1–25.

## 0.0 Principle of Induction

What are the nonnegative integers $\mathbb{N} := \{0, 1, 2, \dots\}$? To understand this fundamental set, we examine an axiomatic characterization.

**Definition 0.0.0.** A triple $(\mathcal{X}, \mathrm{S}, e)$ consisting of a set $\mathcal{X}$, a function $\mathrm{S} \colon \mathcal{X} \to \mathcal{X}$, and a distinguished element $e \in \mathcal{X}$ is a *Peano system* if the following three axioms hold:

(A0) For any element $x$ in $\mathcal{X}$, we have $\mathrm{S}(x) \neq e$.

(A1) The function $\mathrm{S} \colon \mathcal{X} \to \mathcal{X}$ is injective; for any two elements $x$ and $y$ in $\mathcal{X}$, the equation $\mathrm{S}(x) = \mathrm{S}(y)$ implies that $x = y$.

(A2) For any subset $\mathcal{Y} \subseteq \mathcal{X}$ such that $e \in \mathcal{Y}$ and $\mathrm{S}(y) \in \mathcal{Y}$ for all $y \in \mathcal{Y}$, we have $\mathcal{Y} = \mathcal{X}$.

The Italian mathematician Giuseppe Peano (1858–1932) introduced these axioms in his 1889 treatise titled *Arithmetices principia, nova methodo exposita*.

The next result indicates that one may take the Peano axioms as the definition of the nonnegative integers.

**Theorem 0.0.1.** *For the* successor function $\mathrm{S} \colon \mathbb{N} \to \mathbb{N}$, *the triple* $(\mathbb{N}, \mathrm{S}, 0)$ *is a Peano system. For any Peano system* $(\mathcal{X}, \mathrm{S}', e)$*, there exists a bijection* $\pi \colon \mathbb{N} \to \mathcal{X}$ *such that* $\pi(0) = e$ *and* $\pi\big(\mathrm{S}(n)\big) = \mathrm{S}'\big(\pi(n)\big)$ *for any* $n$ *in* $\mathbb{N}$.

Every Peano system is isomorphic to the canonical triple $(\mathbb{N}, \mathrm{S}, 0)$.

*Sketch of proof.* To prove the first part requires an independent definition for the set $\mathbb{N}$. In set theory, the nonnegative integers are usually constructed recursively as

$$
\begin{aligned}
0 &:= \{\} = \varnothing \\
1 &:= \{0\} = 0 \cup \{0\} = \{\varnothing\} \\
2 &:= \{0, 1\} = 1 \cup \{1\} = \big\{\varnothing, \{\varnothing\}\big\} \\
3 &:= \{0, 1, 2\} = 2 \cup \{2\} = \big\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\big\} \\
4 &:= \{0, 1, 2, 3\} = 3 \cup \{3\} = \big\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}\big\} \\
&\ \vdots
\end{aligned}
$$

and the *successor function* $S \colon \mathbb{N} \to \mathbb{N}$ is defined by $\mathrm{S}(n) := n \cup \{n\}$.

In other words, the successor function on $\mathbb{N}$ satisfies $\mathrm{S}(n) = n + 1$.

For the second part, consider the function $\pi \colon \mathbb{N} \to \mathcal{X}$ defined, via induction, by $\pi(0) = e$ and $\pi\big(\mathrm{S}(n)\big) = \mathrm{S}'\big(\pi(n)\big)$. Since $e$ is not in the image of $\mathrm{S}'$ and $\mathrm{S}'$ is injective, the function $\pi$ is also injective. To establish that $\pi$ is surjective one uses axiom (A2). □

The axiom (A2), referred to as the principle of induction, is the most complex and most frequently used. It may be more familiar in the another guise. A *property* of the set $\mathbb{N}$ is a function $P \colon \mathbb{N} \to \{\mathsf{true}, \mathsf{false}\}$. We say that the property $P(n)$ holds for some nonnegative integer $n$ if and only if $P(n) = \mathsf{true}$. The common form of induction is prescribed as follows.

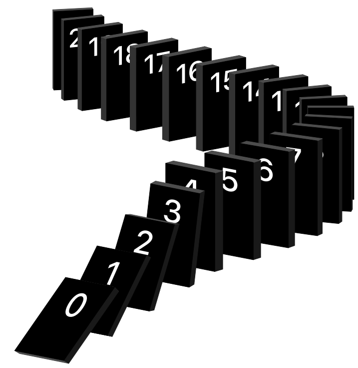


*Figure 0.1:* Induction is like toppling dominoes. Pushing the zeroth one is the base case. Each subsequent domino being knocked over by its predecessor is the induction step.

**Theorem 0.0.2.** *To demonstrate that a property $P(n)$ holds for any nonnegative integer $n$, it is enough to prove*

Base case: *$P(0)$ holds, and*

Induction step: *for any nonnegative integer $n$, the assumption that $P(n)$ holds implies that the property $P(n+1)$ holds.*

*Proof.* Each property $P$ satisfied by (some or all of) the elements in $\mathbb{N}$ corresponds to a subset of $\mathbb{N}$, namely $\mathcal{Y} := \{m \in \mathbb{N} : P(m) \text{ holds}\}$. The principle of induction establishes that $\mathcal{Y} = \mathbb{N}$. □

The next two problems typify the basic use of induction. Notice that the base case need to be 0.

**Problem 0.0.3.** For any positive integer $n$, verify that

$$\sum_{j=0}^{n-1} (2j+1) = n^2 \,.$$

*Inductive solution.* When $n = 1$, we have $2(0) + 1 = (1)^2$, so the base case holds. Assuming that $\sum_{j=0}^{n-2} (2j+1) = (n-1)^2$ holds, we show that the equation $\sum_{j=0}^{n-1} (2j+1) = n^2$ also holds. The induction step is

$$\begin{aligned} \sum_{j=0}^{n-1} (2j+1) &= \left( \sum_{j=0}^{n-2} (2j+1) \right) + \Big( 2(n-1) + 1 \Big) \\ &= (n-1)^2 + 2(n-1) + 1 = \big( (n-1) + 1 \big)^2 = n^2 \,. \end{aligned}$$ □

**Remark 0.0.4.** Despite verifying the correctness of the formula, the inductive solution to Problem 0.0.3 is unsatisfying. It feels overly formal and does not seem to explain the true origins of this equation. Figure 0.2 suggests a better way to understand this sum.

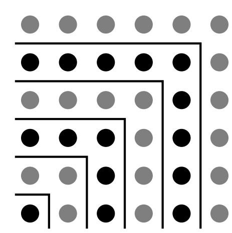

*Figure 0.2:* Sum of odd integers

**Problem 0.0.5.** For any integer $n$ satisfying $n \geqslant 4$, prove that

$$2^n \geqslant n^2 \,.$$

*Inductive solution.* For any integer $n$ greater than 1, we first prove, by induction, that $n^2 \geqslant 2$. When $n = 2$, we have $2^2 = 4 > 2$, so the base case holds. Assuming that the inequality $n^2 - 2 \geqslant 0$ holds, we show that $(n+1)^2 - 2 \geqslant 0$ also holds. The induction step is

$$(n+1)^2 - 2 = (n^2 + 2n + 1) - 2 \geqslant 2n + 1 \geqslant 5 \geqslant 0 \,.$$

For any integer $n$ such that $n \geqslant 4$, we now prove, via induction on $n$, that $2^n \geqslant n^2$. When $n = 4$, we have $2^4 = 16 = 4^2$, so the base case holds. Assuming that the inequality $2^n - n^2 \geqslant 0$ holds, we show that $2^{n+1} - (n+1)^2 \geqslant 0$. For the induction step, we have

$$\begin{aligned} 2^{n+1} - (n+1)^2 &= 2\,(2^n) - n^2 - 2\,n - 1 \\ &\geqslant 2\,(n^2) - n^2 - 2\,n - 1 = (n-1)^2 - 2\,. \end{aligned}$$

Since the first paragraph establishes that $(n-1)^2 - 2 \geqslant 0$, we deduce that $2^{n+1} - (n+1)^2 \geqslant 0$ as required. □

*Exercises*

**Problem 0.0.6.** For all nonnegative integers $n$, give two different proofs for the equation

$$\sum_{k=0}^{n} \frac{1}{(k+1)(k+2)} = \frac{n+1}{n+2}$$

**(i)** Verify this equation via induction on $n$.
**(ii)** Derive this equation using partial fractions.

**Problem 0.0.7.** For all nonnegative integers $n$, verify that

$$\sum_{j=0}^{n} j^3 = \left( \sum_{j=0}^{n} j \right)^2$$

**Problem 0.0.8.** For any nonnegative integer $n$, prove that either $n = 0$ or there exists a nonnegative integer $k$ such that $n = \mathrm{S}(k)$.

**Problem 0.0.9.** Establish the following variant on the principle of induction.

> To verify that a property $P(n)$ holds for all nonnegative integers $n$, it is enough to prove that
> *Base case:* $P(0)$ holds, and
> *Induction step:* for any nonnegative integer $n$, the assumption that the property $P(k)$ holds for all $k \leqslant n$ implies that the property $P(n+1)$ holds.

**Problem 0.0.10.** The sequence of *square triangular numbers* is defined by $N_0 := 0$, $N_1 := 1$, and $N_k := 34\,N_{k-1} - N_{k-2} + 2$ for all $k \geqslant 2$. The first few terms are $0, 1, 36, 1225, 41616, 1413721, 48024900, \dots$.
**(i)** Prove that $N_{k-1}\,N_{k+1} = (N_k - 1)^2$ for all $k \geqslant 1$.
**(ii)** Verify that

$$N_k = \left( \frac{(3+2\sqrt{2})^k - (3-2\sqrt{2})^k}{4\sqrt{2}} \right)^2 .$$

## 0.1 Peano Arithmetic

How is a Peano system equipped with addition and multiplication? To prove the well-known properties of these binary operations, we start with simple result.

 

**Proposition 0.1.0.** *For any two functions $\varphi \colon \mathbb{N} \to \mathbb{N}$ and $\psi \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, there exists a unique function $\theta \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that, for any $m$ in $\mathbb{N}$,*
- *$\theta(m, 0) = \varphi(m)$, and*
- *$\theta(m, \mathrm{S}(n)) = \psi(\theta(m, n), m)$ for any $n$ in $\mathbb{N}$.*

*Proof.* For each nonnegative integer $m$, the principle of induction determines a function $\beta_m \colon \mathbb{N} \to \mathbb{N}$ such that $\beta_m(0) := \varphi(m)$ and $\beta_m(\mathrm{S}(n)) := \psi(\beta_m(n), m)$ for any nonnegative integer $n$. Define the function $\theta \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $\theta(m, n) := \beta_m(n)$. By construction, the function $\theta$ satisfies the two conditions. Since the conditions also specify all the outputs, the function $\theta$ is uniquely determined. □

Our definition for the addition of nonnegative integers is an application of this proposition.

**Definition 0.1.1.** The unique function $\alpha \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that for any two nonnegative integers $m$ and $n$, we have
- $\alpha(m, 0) = m$ and
- $\alpha(m, \mathrm{S}(n)) = \mathrm{S}(\alpha(m, n))$,

is called *addition* and denoted by $m + n := \alpha(m, n)$.

Apply Proposition 0.1.0 when $\varphi = \mathrm{id}_{\mathbb{N}}$ and $\psi(m, n) = \mathrm{S}(m)$.

**Remark 0.1.2.** Since $1 := \mathrm{S}(0)$, the conditions in the definition of addition demonstrate that, for any nonnegative integer $m$, we have $m + 1 = m + \mathrm{S}(0) = \mathrm{S}(m + 0) = \mathrm{S}(m)$.

**Lemma 0.1.3.** *For any nonnegative integer $m$, we have $0 + m = m$.*

The distinguished element 0 in $\mathbb{N}$ is the additive identity.

*Proof.* Consider $\mathcal{X} := \{m \in \mathbb{N} \mid 0 + m = m\}$. Since first condition for addition gives $0 + 0 = 0$, so $0 \in \mathcal{X}$. Assuming $n \in \mathcal{X}$, second condition for addition shows that $0 + \mathrm{S}(n) = \mathrm{S}(0 + n) = \mathrm{S}(n)$, so $\mathrm{S}(n) \in \mathcal{X}$. The principle of induction establishes that $\mathcal{X} = \mathbb{N}$. □

**Lemma 0.1.4.** *For any two nonnegative integers $m$ and $n$, we have*
$$\mathrm{S}(m) + n = \mathrm{S}(m + n)\,.$$

*Proof.* Let $m$ be a nonnegative integer. Consider the subset $\mathcal{X} := \{n \in \mathbb{N} \mid \mathrm{S}(m) + n = \mathrm{S}(m + n)\}$. The first condition for addition gives $\mathrm{S}(m) + 0 = \mathrm{S}(m) = \mathrm{S}(m + 0)$, so $0 \in \mathcal{X}$. Assuming $n \in \mathcal{X}$, second condition for addition and the definition of $\mathcal{X}$ show that

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

so $\mathrm{S}(n) \in \mathcal{X}$. Thus, the principle of induction gives $\mathcal{X} = \mathbb{N}$. □

Our definition for multiplication is very similar.

**Definition 0.1.5.** The unique function $\mu \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that for any two nonnegative integers $m$ and $n$, we have
- $\mu(m, 0) = 0$ and
- $\mu(m, \mathrm{S}(n)) = \mu(m, n) + m$.

is called *multiplication* and denoted $m\,n := \mu(m, n)$.

Apply Proposition 0.1.0 when $\varphi(m) = 0$ and $\psi(m, n) = m + n$.

**Remark 0.1.6.** For any nonnegative integer $m$, the second condition in multiplication gives $m\,1 = m\,0 + m = m$.

The successor $1 := \mathrm{S}(0)$ is the multiplicative identity.

**Lemma 0.1.7.** *For any nonnegative integer $m$, we have $0\,m = 0$.*

*Proof.* Consider $\mathcal{X} := \{m \in \mathbb{N} \mid 0\,m = 0\}$. The first condition for multiplication implies that $(0)(0) = 0$, so $0 \in \mathcal{X}$. Assuming $n \in \mathcal{X}$, the second condition for multiplication, the definition of $\mathcal{X}$, and the second condition for addition demonstrate that $0\ \mathrm{S}(n) = 0\,n + 0 = 0 + 0 = 0$, so $\mathrm{S}(n) \in \mathcal{X}$. The principle of induction again yields $\mathcal{X} = \mathbb{N}$. □

We are now in a position to prove the fundamental properties of addition and multiplication.

**Theorem 0.1.8.** *For any nonnegative integers $k$, $m$, and $n$, we have*

$$\begin{aligned}
(k+m)+n &= k+(m+n) && \text{(associativity of addition)}\\
m+n &= n+m && \text{(commutativity of addition)}\\
k(m\,n) &= (k\,m)n && \text{(associativity of multiplication)}\\
m\,n &= n\,m && \text{(commutativity of multiplication)}\\
k(m+n) &= k\,m + k\,n && \text{(distributivity)}
\end{aligned}$$

*Proof.*

- Let $k$ and $m$ be nonnegative integers. Consider the subset $\mathcal{X} := \{n \in \mathbb{N} \mid k + (m+n) = (k+m)+n\}$. The first condition for addition gives $k + (m+0) = k + m = (k+m)+0$, so $0 \in \mathcal{X}$. Assuming $n \in \mathcal{X}$, the second condition for addition yields

$$\begin{aligned}
k + \big(m + \mathrm{S}(n)\big) = k + \mathrm{S}(m+n) &= \mathrm{S}\big(k + (m+n)\big)\\
&= \mathrm{S}\big((k+m)+n\big) = (k+m) + \mathrm{S}(n)
\end{aligned}$$

  so $\mathrm{S}(n) \in \mathcal{X}$. The principle of induction implies that $\mathcal{X} = \mathbb{N}$ and the associativity of addition.
- Let $m$ be a nonnegative integer. Consider the subset $\mathcal{X} := \{n \in \mathbb{N} \mid m + n = n + m\}$. Lemma 0.1.3 shows that $0 \in \mathcal{X}$. Assuming $n \in \mathcal{X}$, Lemma 0.1.4, the definition of $\mathcal{X}$, and the second condition for addition imply that

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

  so $\mathrm{S}(n) \in \mathcal{X}$. The principle of induction yields $\mathcal{X} = \mathbb{N}$ and the commutativity of addition.
- Let $k$ and $m$ be nonnegative integers. Consider the subset $\mathcal{X} := \{n \in \mathbb{N} \mid k(m+n) = k\,m + k\,n\}$. The first conditions for addition and multiplication give

$$k(m+0) = k\,m = k\,m + 0 = k\,m + k\,0$$

  so $0 \in \mathcal{X}$. Assuming $n \in \mathcal{X}$, the second conditions for addition and multiplication, the definition of $\mathcal{X}$, and associativity of addition imply that

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

so $\mathrm{S}(n) \in \mathcal{X}$. The principle of induction shows that $\mathcal{X} = \mathbb{N}$ and distributivity.

- Let $k$ and $m$ be nonnegative integers. Consider the subset $\mathcal{X} := \{n \in \mathbb{N} \mid k(m\,n) = (k\,m)n\}$. The first condition for multiplication gives $k(m\,0) = k\,0 = 0 = (k\,m)\,0$, so $0 \in \mathcal{X}$. Assuming $n \in \mathcal{X}$, the second condition for multiplication, distributivity, and the definition of $\mathcal{X}$ yield

$$\begin{aligned} k(m\,\mathrm{S}(n)) = k(m\,n + m) &= k(m\,n) + k\,m \\ &= (k\,m)n + (k\,m) \\ &= (k\,m)(n+1) = (k\,m)\,\mathrm{S}(n) \end{aligned}$$

so $\mathrm{S}(n) \in \mathcal{X}$. The principle of induction implies that $\mathcal{X} = \mathbb{N}$ and the associativity of multiplication.

- We first claim that $\mathrm{S}(m)\,n = mn + n$ for any two nonnegative integers $m$ and $n$. To prove this claim, fix a nonnegative integer $m$ and consider $\mathcal{Y} := \{n \in \mathbb{N} \mid \mathrm{S}(m)\,n = mn + n\}$. The first conditions for multiplication and addition give $\mathrm{S}(m)\,0 = 0 = 0 + 0 = m\,0 + 0$, so $0 \in \mathcal{Y}$. Assuming $n \in \mathcal{Y}$, second condition for multiplication, the definition of $\mathcal{Y}$, the properties of addition, distributivity, and the second condition for addition show that

$$\begin{aligned} \mathrm{S}(m)\,\mathrm{S}(n) = \mathrm{S}(m)n + \mathrm{S}(m) &= (mn + n) + (m+1) \\ &= mn + m + n + 1 \\ &= m(n+1) + (n+1) = m\,\mathrm{S}(n) + \mathrm{S}(n) \end{aligned}$$

so $\mathrm{S}(n) \in \mathcal{Y}$. Thus, the principle of induction gives $\mathcal{X} = \mathbb{N}$ and establishes the claim.

Next, consider the subset $\mathcal{X} := \{n \in \mathbb{N} \mid m\,n = n\,m\}$. The claim, the definition of $\mathcal{X}$, and distributivity imply that

$$\mathrm{S}(n)\,m = nm + m = mn + m = m(n+1) = m\,\mathrm{S}(n)$$

so $\mathrm{S}(n) \in \mathcal{X}$. The principle of induction yields $\mathcal{X} = \mathbb{N}$ and the commutativity of multiplication. □

*Exercises*

**Problem 0.1.9.** For any three nonnegative integers $k$, $m$, and $n$, demonstrate that $k + m = k + n$ if and only if $m = n$.

**Problem 0.1.10.** For any two nonnegative integers $m$ and $n$, show that $m + n = 0$ if and only if $m = n = 0$.

**Problem 0.1.11.** For any three nonnegative integers $k$, $m$, and $n$ such that $k \neq 0$, demonstrate that $k\,m = k\,n$ if and only if $m = n$.

 

**Problem 0.1.12.** For any two nonnegative integers $m$ and $n$, show that $m\,n = 0$ if and only if $m = 0$ or $n = 0$.

**Problem 0.1.13.** For any two nonnegative integers $m$ and $n$, show that $m\,n = 1$ if and only if $m = n = 1$.

**Problem 0.1.14.** Formulate the definition for exponentiation for nonnegative integers and prove that, any three nonnegative integers $k$, $m$, and $n$, we have

$$\begin{aligned} m^0 &= 1\,, & (m\,n)^k &= m^k\,n^k\,, \\ m^{k+n} &= m^k\,m^n\,, & (m^n)^k &= m^{n\,k}\,. \end{aligned}$$

## 0.2 Well-Ordering Principle

How is a Peano system endowed with a total order? We record another basic feature before describing the canonical binary relation on nonnegative integers.

**Lemma 0.2.0.** *Let $n$ be a nonnegative integer such that $n \neq 0$. For any nonnegative integer $m$, we have $m \neq m + n$.*

*Proof.* Consider $\mathcal{X} := \{m \in \mathbb{N} \mid m \neq m + n \text{ for all nonzero } n \text{ in } \mathbb{N}\}$. As $0 \neq n = 0 + n$, we have $0 \in \mathcal{X}$. Assuming $m \in \mathcal{X}$, we claim that $\mathrm{S}(m) \neq \mathrm{S}(m) + n$. Commutativity and second defining condition for addition give $\mathrm{S}(m)+n = n+\mathrm{S}(m) = \mathrm{S}(n+m) = \mathrm{S}(m+n)$. Hence, it suffices to show that $\mathrm{S}(m) \neq \mathrm{S}(m + n)$. Since S is injective, this relation is equivalent to $m \neq m + n$, so $\mathrm{S}(m) \in \mathcal{X}$. The principle of induction implies that $\mathcal{X} = \mathbb{N}$. □

**Definition 0.2.1.** The nonnegative integer $m$ is *less than* the nonnegative integer $n$, denoted by $m < n$, (or $n$ is *greater than* $m$ and $n > m$) if there exists a nonzero $k \in \mathbb{N}$ such that $n = m + k$.

We also use the notation $m \leqslant n$ (or $n \geqslant m$) when $m = n$ or $m < n$.

**Remark 0.2.2.** Let $n$ be a nonnegative integer. Since $n = 0 + n$, we see that $0 \leqslant n$.

An important trichotomy arises from this definition.

**Proposition 0.2.3.** *For any two nonnegative integers $m$ and $n$, exactly one of the following binary relations holds: $m < n$, $m = n$, or $m > n$.*

*Proof.* We first show that the relations are mutually exclusive.

- Suppose that $m < n$ and $m = n$. Hence, there is a nonzero $k \in \mathbb{N}$ such that $m = n = m + k$, which contradicts Lemma 0.2.0.
- Suppose that $m < n$ and $m > n$. Hence, there exists a nonzero $k \in \mathbb{N}$ such that $n = m + k$ and a nonzero $\ell \in \mathbb{N}$ such that $m = n + \ell$. We deduce that $n = n + (k + \ell)$ which again contradicts Lemma 0.2.0.
- Suppose that $m = n$ and $m > n$. By symmetry, this is equivalent to the first case.

 

It remains to show that one of the relations always holds. Fix a nonnegative integer $m$ and consider the subset

$$\mathcal{X} := \{n \in \mathbb{N} \mid m < n \text{ or } m = n \text{ or } m > n\}.$$

When $m = 0$, we have $0 \in \mathcal{X}$. When $m \neq 0$, we have $m = 0 + m$, so $0 < m$ and $0 \in \mathcal{X}$. Assuming that $n \in \mathcal{X}$, there are three cases:

- Suppose that $m < n$. Hence, there exists a nonzero $k \in \mathbb{N}$ such that $n = m + k$. The second defining condition for addition gives $\mathrm{S}(n) = \mathrm{S}(m + k) = m + \mathrm{S}(k)$, so $m < \mathrm{S}(n)$ and $\mathrm{S}(n) \in \mathcal{X}$.
- Suppose that $m = n$. Since $\mathrm{S}(n) = n + 1 = m + 1$, we see that $m < \mathrm{S}(n)$, so $\mathrm{S}(n) \in \mathcal{X}$.
- Suppose that $m > n$. Hence, there exists a nonzero $k \in \mathbb{N}$ such that $m = n + k$. When $k = 1$, we have $m = n + 1 = \mathrm{S}(n)$, so $\mathrm{S}(n) \in \mathcal{X}$. When $k \neq 1$, there exists a nonzero $\ell \in \mathbb{N}$ such that $k = \mathrm{S}(\ell)$. It follows that

$$m = n + k = n + \mathrm{S}(\ell) = n + (\ell + 1) = (n + 1) + \ell = \mathrm{S}(n) + \ell\,,$$

  so $\mathrm{S}(n) < m$ and $\mathrm{S}(n) \in \mathcal{X}$.

Thus, the principle of induction implies that $\mathcal{X} = \mathbb{N}$. □

**Corollary 0.2.4.** *Let $k$, $m$, and $n$ be nonnegative integers such that $k \neq 0$. We have $m < n$ if and only if $k\,m < k\,n$.*

*Proof.*
⇐: Suppose that $m < n$. Hence, there exists a nonzero $\ell \in \mathbb{N}$ such that $n = m + \ell$. Distributivity gives $k\,n = \ell\,(m + \ell) = k\,m + k\,\ell$. Since $k\,\ell$ is nonzero, we deduce that $k\,m < k\,n$.
⇒: Suppose that $k\,m < k\,n$ and consider two cases.
- Suppose that $m = n$. It follows that $k\,m = k\,n$ contradicting the inequality $k\,m < k\,n$.
- Suppose that $m > n$. The first direction shows that $k\,m > k\,n$ which also contradicts the inequality $k\,m < k\,n$.

From the trichotomy, we deduce that $m < n$. □

**Lemma 0.2.5.** *Let $m$ and $n$ be nonnegative integers. When $m < n$, we have $\mathrm{S}(m) \leqslant n$.*

*Proof.* Since $m < n$, there is a nonzero $k \in \mathbb{N}$ such that $n = m + k$. When $k = 1$, we have $n = m + 1$. When $k > 1$, there exists a nonzero $\ell \in \mathbb{N}$ such that $k = 1 + \ell$. It follows that $n = m + 1 + \ell$ and $\mathrm{S}(m) = m + 1 < n$. □

Using the total order on nonnegative integers, the principle of induction has another fundamental reformulation.

**Theorem 0.2.6** (Well-ordering of nonnegative integers)**.** *Every nonempty subset of the set $\mathbb{N}$ of nonnegative integers contains a unique least element (with respect to $\leqslant$).*

*Proof.* Let $\mathcal{X}$ be a nonempty subset of nonnegative integers.

*Uniqueness:* Suppose that $x$ and $x'$ are both least elements of $\mathcal{X}$. Since $x \leqslant x'$ and $x' \leqslant x$, the trichotomy implies that $x = x'$.

*Existence:* Suppose that $\mathcal{X}$ has no least element. Consider a second subset $\mathcal{Y} := \{n \in \mathbb{N} \mid n \leqslant x \text{ for all } x \in \mathcal{X}\}$. Remark 0.2.2 proves that $0 \in \mathcal{Y}$. Assume that $n \in \mathcal{Y}$. Since $\mathcal{X}$ has no least element, it follows that $n \notin \mathcal{X}$ and $n < x$ for all $x \in \mathcal{X}$. Lemma 0.2.5 shows that $\mathrm{S}(n) = n + 1 \leqslant x$ for all $x \in \mathcal{X}$, so $\mathrm{S}(n) \in \mathcal{Y}$. Hence, the principle of induction establishes that $\mathcal{Y} = \mathbb{N}$. However, this would imply that $\varnothing = \mathcal{X} \cap \mathcal{Y} = \mathcal{X}$ which contradicts the hypothesis that $\mathcal{X}$ is nonempty. We conclude that every nonempty subset of nonnegative integers has a least element. $\square$

*Exercises*

**Problem 0.2.7.** For any three nonnegative integers $k$, $m$, and $n$, establish the following.

**(i)** When $k \leqslant m$ and $m \leqslant n$, we have $k \leqslant n$.
**(ii)** When $k < m$ and $m \leqslant n$, we have $k < n$.
**(iii)** When $k \leqslant m$ and $m < n$, we have $k < n$.

**Problem 0.2.8.** For any three nonnegative integers $k$, $m$, and $n$ such that $k \neq 0$, prove that $m < n$ if and only if $k + m < k + n$.

**Problem 0.2.9.** Establish that any nonempty subset of $\mathbb{N}$ that is bounded above has a unique greatest element (with respect to $\leqslant$).

**Problem 0.2.10.** For any nonnegative integers $m$ and $n$ with $n \neq 0$, prove that there exists a nonnegative integer $k$ such that $m < k\,n$.