# Arithmetic

Marcel Schütz

2021

**Abstract**

This is a formalization of Peano Arithmetic with addition, multiplication, exponentiation and factorial. These operations are introduced axiomatically and are accompanied with detailed proofs of their common computation laws. Moreover, the standard ordering on the natural numbers is given, together with proofs of its behaviour with respect to the mentioned operations. Furthermore, the notion of divisibility is introduced which finally leads to some results of basic number theory.

This text can be seen as a collection of basic results from undergraduate mathematics or serve as a foundation for more sophisticated formalizations.

## Contents

# Part I
# Arithmetic

## 1 Peano Arithmetic

[readtex `vocabulary.ftl.tex`]

[readtex `macros.ftl.tex`]

### 1.1 The Peano axioms

This arithmetic is based on the notion of natural numbers. These are introduced as some sort of elements that is equiped with a a unary function succ (which maps any natural number to its direct successor) and that contains a constant 0 (the unique least natural number).

**Signature 1.1.** A natural number is an element.

Let $k, l, m, n$ denote natural numbers.

**Definition 1.2.** $\mathbb{N}$ is the class of natural numbers.

**Signature 1.3.** 0 is a natural number.

Let $n$ is nonzero stand for $n \neq 0$.

**Signature 1.4.** $\mathrm{succ}(n)$ is a natural number.

Let the direct successor of $n$ stand for $\mathrm{succ}(n)$.

The natural numbers are characterized by the following so-called Peano axioms.

**Axiom 1.5 (1st Peano axiom).** If $\mathrm{succ}(n) = \mathrm{succ}(m)$ then $n = m$.

**Axiom 1.6 (2nd Peano axiom).** 0 is not the direct successor of any natural number.

**Axiom 1.7 (3rd Peano axiom).** Let $P$ be a class. Assume $0 \in P$ and for all natural numbers $n$ we have $n \in P \implies \mathrm{succ}(n) \in P$. Then every natural number is an element of $P$.

### 1.2 Immediate consequences

The 3rd Peano axiom (also called the *induction axiom*) allows us to prove that the signature $(0, \mathrm{succ})$ captures the whole class of natural numbers in the sense that every natural number is either zero or a successor:

**Proposition 1.8.** For all $n$ we have $n = 0$ or $n = \mathrm{succ}(m)$ for some natural number $m$.

*Proof.* Define

$$P = \{\, n \in \mathbb{N} \mid n = 0 \text{ or } n = \text{succ}(m) \text{ for some natural number } m \,\}.$$

$0 \in P$ and for all natural numbers $n$ we have $n \in P \implies \text{succ}(n) \in P$. Hence the thesis (by 3rd Peano axiom). □

This allows us to define the direct predecessor of a non-zero natural number as follows.

**Definition 1.9.** Let $n$ be nonzero. $\text{pred}(n)$ is the natural number $m$ such that $\text{succ}(m) = n$.

Let the direct predecessor of $n$ stand for $\text{pred}(n)$.

Note that direct predecessors must be unique by the 2nd Peano axiom. Moreover, we can show that no natural number is its own successor.

**Proposition 1.10.** For no natural number $n$ we have $n = \text{succ}(n)$.

*Proof.* Define

$$P = \{\, n \in \mathbb{N} \mid n \neq \text{succ}(n) \,\}.$$

(BASE CASE) 0 belongs to $P$.

(INDUCTION STEP) For all $n$ we have $n \in P \implies \text{succ}(n) \in P$.
Proof. Let $n$ be a natural number. Assume that $n \in P$. Then $n \neq \text{succ}(n)$. If $\text{succ}(n) = \text{succ}(\text{succ}(n))$ then $n = \text{succ}(n)$. Thus it is wrong that $\text{succ}(n) = \text{succ}(\text{succ}(n))$. Hence $\text{succ}(n) \in P$. Qed.

Therefore every natural number is an element of $P$. Then we have the thesis. □

## 1.3 Additional constants

Let us end this section by introducing new constant symbols for the first few successors of 0.

**Definition 1.11.** $1 = \text{succ}(0)$.

**Definition 1.12.** $2 = \text{succ}(1)$.

**Definition 1.13.** $3 = \text{succ}(2)$.

**Definition 1.14.** $4 = \text{succ}(3)$.

**Definition 1.15.** $5 = \text{succ}(4)$.

**Definition 1.16.** $6 = \text{succ}(5)$.

**Definition 1.17.** $7 = \text{succ}(6)$.

**Definition 1.18.** $8 = \text{succ}(7)$.

**Definition 1.19.** $9 = \mathrm{succ}(8)$.

# 2 Addition

[readtex `arithmetic/sections/01_arithmetic/01_peano-axioms.ftl.tex`]

Let $k, l, m, n$ denote natural numbers.

## 2.1 Axioms

Up to now our arithmetic – if it already deserves this name – is very primitive. In this section we change this by inductively defining an addition operation.

**Signature 2.1.** $n + m$ is a natural number.

Let the sum of $n$ and $m$ stand for $n + m$.

**Axiom 2.2 (1st addition axiom).** $n + 0 = n$.

**Axiom 2.3 (2nd addition axiom).** $n + \mathrm{succ}(m) = \mathrm{succ}(n + m)$.

## 2.2 Immediate consequences

Having this characterization of addition at hand, the successor operation turns out to coincide with the "+1" operation.

**Lemma 2.4.** $\mathrm{succ}(n) = n + 1$.

This enables us to restate all previous axioms purely in terms of addition.

**Corollary 2.5 (1st Peano axiom).** If $n + 1 = m + 1$ then $n = m$.

**Corollary 2.6 (2nd Peano axiom).** For no n we have $n + 1 = 0$.

**Corollary 2.7 (3rd Peano axiom).** Let $P$ be a class. Assume $0 \in P$ and for all $n$: $n \in P \implies n + 1 \in P$. Then every natural number is an element of $P$.

**Corollary 2.8 (2nd addition axiom).** $n + (m + 1) = (n + m) + 1$.

## 2.3 Computation laws

Let us now prove the common computation laws for addition: Associativity, commutativity and the cancellation laws.

**Associativity:**

**Proposition 2.9.** For all $n, m, k$ we have

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

*Proof.* Define

$$P = \{\, k \in \mathbb{N} \mid \text{for all } n, m\text{: } n + (m + k) = (n + m) + k \,\}.$$

(BASE CASE) 0 is contained in $P$. Indeed $n+(m+0) = n+m = (n+m)+0$ for all natural numbers $n, m$.

(INDUCTION STEP) For all $k$ we have $k \in P \implies k + 1 \in P$.
Proof. Let $k$ be a natural number. Assume $k \in P$.

Let us show that $n + (m + (k + 1)) = (n + m) + (k + 1)$ for all natural numbers $n, m$.
Let $n, m$ be natural numbers. Then $n + m$ is a natural number.

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

Hence the thesis. End.

Therefore we have $k + 1 \in P$. Qed.

Thus every natural number is an element of $P$. □

**Commutativity:**

**Proposition 2.10.** For all $n, m$ we have

$$n + m = m + n.$$

*Proof.* Define

$$P = \{\, m \in \mathbb{N} \mid n + m = m + n \text{ for all natural numbers } n \,\}.$$

(BASE CASE 1) 0 is an element of $P$.
Proof. Define

$$Q = \{\, n \in \mathbb{N} \mid n + 0 = 0 + n \,\}.$$

0 belongs to $Q$.

For all $n$ we have $n \in Q \implies n+1 \in Q$.
Proof. Let $n$ be a natural number. Assume $n \in Q$.

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

Qed.

Thus every natural number belongs to $Q$. Therefore 0 is an element of $P$.
Qed.

(BASE CASE 2) 1 is contained in $P$.
Proof. Define

$$Q = \{\, n \in \mathbb{N} \mid n+1 = 1+n \,\}.$$

0 is an element of $Q$.

For all natural numbers $n$ we have $n \in Q \implies n+1 \in Q$.
Proof. Let $n$ be a natural number. Assume that $n$ is contained in $Q$.

$$\begin{aligned}
&(n+1)+1 \\
&= (1+n)+1 \\
&= 1+(n+1).
\end{aligned}$$

Qed.

Thus every natural number belongs to $Q$. Therefore 1 is an element of $P$.
Qed.

(INDUCTION STEP) For all natural numbers $n$ we have $n \in P \implies n+1 \in P$.
Proof. Let $n$ be an natural number. Assume $n \in P$.

$(n+1)+m = m+(n+1)$ for all natural numbers $m$.
Proof. Let $m$ be a natural number.

$$\begin{aligned}
&(n+1)+m \\
&= n+(1+m) \\
&= (1+m)+n \\
&= (m+1)+n
\end{aligned}$$

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

Qed. Qed.

Hence every natural number is an element of $P$. □

**Cancellation:**

**Proposition 2.11.** For all natural numbers $n, m, k$ we have

$$n + k = m + k \implies n = m.$$

*Proof.* Define

$$P = \{\, k \in \mathbb{N} \mid \text{for all natural numbers } n, m \text{ if } n + k = m + k \text{ then } n = m \,\}.$$

(BASE CASE) 0 is an element of $P$.

(INDUCTION STEP) For all $k$ we have $k \in P \implies k + 1 \in P$.
Proof. Let $k$ be a natural number. Assume $k \in P$.

For all natural numbers $n, m$ we have $n+(k+1) = m+(k+1) \implies n = m$.
Proof. Let $n, m$ be natural numbers. Assume $n + (k + 1) = m + (k + 1)$.
Then $(n + k) + 1 = (m + k) + 1$. Hence $n + k = m + k$. Thus $n = m$. Qed.

Hence the thesis (by 3rd Peano axiom). Qed.

Therefore every natural number is an element of $P$. □

**Corollary 2.12.** For all $n, m, k$ we have

$$k + n = k + m \implies n = m.$$

*Proof.* Let $n, m, k$ be natural numbers. Assume $k + n = k + m$. We have $k + n = n + k$ and $k + m = m + k$. Hence $n + k = m + k$. Thus $n = m$. □

# 3 Multiplication

[readtex `arithmetic/sections/01_arithmetic/02_addition.ftl.tex`]

Let $k, l, m, n$ denote natural numbers.

## 3.1 Axioms

Having introduced addition in the last section, we now define a multiplication operation on the natural numbers.

**Signature 3.1.** $n \cdot m$ is a natural number.

Let the product of $n$ and $m$ stand for $n \cdot m$.

**Axiom 3.2 (1st multiplication axiom).** $n \cdot 0 = 0$.

**Axiom 3.3 (2nd multiplication axiom).** $n \cdot (m + 1) = (n \cdot m) + n$.

## 3.2 Computation laws

Let us show some basic computation laws for it.

**Associativity:**

**Proposition 3.4.** For all $n, m, k$ we have

$$n \cdot (m + k) = (n \cdot m) + (n \cdot k).$$

*Proof.* Define

$$P = \{\, k \in \mathbb{N} \mid n \cdot (m+k) = (n \cdot m) + (n \cdot k) \text{ for all natural numbers } n, m \,\}.$$

(BASE CASE) 0 is an element of $P$. Indeed for all natural numbers $n, m$ we have $n \cdot (m + 0) = n \cdot m = (n \cdot m) + 0 = (n \cdot m) + (n \cdot 0)$.

(INDUCTION STEP) For all natural numbers $k$ we have $k \in P \implies k + 1 \in P$.
Proof. Let $k$ be a natural number. Assume $k \in P$.

For all natural numbers $n, m$ we have $n \cdot (m + (k+1)) = (n \cdot m) + (n \cdot (k+1))$.
Proof. Let $n, m$ be natural numbers.

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

Hence the thesis. Qed. Qed.

Therefore every natural number is contained in $P$. □

**Distributivity:**

**Proposition 3.5.** For all $n, m, k$ we have

$$(n + m) \cdot k = (n \cdot k) + (m \cdot k).$$

*Proof.* Define

$$P = \{\, k \in \mathbb{N} \mid (n+m) \cdot k = (n \cdot k) + (m \cdot k) \text{ for all natural numbers } n, m \,\}.$$

(BASE CASE) 0 belongs to $P$. Indeed $(n+m)\cdot 0 = 0 = 0+0 = (n\cdot 0)+(m\cdot 0)$ for all natural numbers $n, m$.

(INDUCTION STEP) For all natural numbers $k$ we have $k \in P \implies k + 1 \in P$.
Proof. Let $k$ be a natural number. Assume $k \in P$.

$(n+m) \cdot (k+1) = (n \cdot (k+1)) + (m \cdot (k+1))$ for all natural numbers $n, m$.
Proof. Let $n, m$ be natural numbers. We have $((n \cdot k)+((m \cdot k)+n))+m = (((n \cdot k) + n) + (m \cdot k)) + m$. Hence

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

Qed. Qed.

Thus every natural number is an element of $P$. □

**Proposition 3.6.** $n \cdot 1 = n$.

*Proof.* $n \cdot 1 = n \cdot (0 + 1) = (n \cdot 0) + n = 0 + n = n$. □

**Corollary 3.7.** $n \cdot 2 = n + n$.

*Proof.* $n \cdot 2 = n \cdot (1 + 1) = (n \cdot 1) + n = n + n$. □

**Proposition 3.8.** For all $n, m, k$ we have

$$n \cdot (m \cdot k) = (n \cdot m) \cdot k.$$

*Proof.* Define

$$P = \{\, k \in \mathbb{N} \mid n \cdot (m \cdot k) = (n \cdot m) \cdot k \text{ for all natural numbers } n, m \qquad \}\,.$$

(BASE CASE) 0 is contained in $P$. Indeed for all natural numbers $n, m$ we have $n \cdot (m \cdot 0) = n \cdot 0 = 0 = (n \cdot m) \cdot 0$.

(INDUCTION STEP) For all natural numbers $k$ we have $k \in P \implies k + 1 \in P$.
Proof. Let $k$ be a natural number. Assume $k \in P$.

For all natural numbers $n, m$ we have $n \cdot (m \cdot (k + 1)) = (n \cdot m) \cdot (k + 1)$.
Proof. Let $n, m$ be natural numbers.

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

Qed. Qed.

Hence every natural number is contained in $P$. □

**Commutativity:**

**Proposition 3.9.** For all $n, m$ we have

$$n \cdot m = m \cdot n.$$

*Proof.* Define

$$P = \{\, m \in \mathbb{N} \mid n \cdot m = m \cdot n \text{ for all natural numbers } n \,\}\,.$$

(BASE CASE 1) 0 is contained in $P$.
Proof.

For all natural numbers $n$ we have $n \cdot 0 = 0 \cdot n$.
Proof. Define

$$Q = \{\, n \in \mathbb{N} \mid n \cdot 0 = 0 \cdot n \,\}\,.$$

0 is contained in $Q$.

For all natural numbers $n$ we have $n \in Q \implies n + 1 \in Q$.

Proof. Let $n$ be a natural number. Assume $n \in Q$. Then

$$(n+1) \cdot 0 = 0 = n \cdot 0 = 0 \cdot n = (0 \cdot n) + 0 = 0 \cdot (n+1).$$

Qed. Qed. Qed.

(BASE CASE 2) 1 belongs to $P$.
Proof. Let us show that for all natural numbers $n$ we have $n \cdot 1 = 1 \cdot n$. Define

$$Q = \{\, n \in \mathbb{N} \mid n \cdot 1 = 1 \cdot n \,\}.$$

0 is contained in $Q$.

For all natural numbers $n$ we have $n \in Q \implies n+1 \in Q$.
Proof. Let $n$ be a natural number. Assume $n \in Q$. Then

$$\begin{aligned}
&(n+1) \cdot 1 \\
&= (n \cdot 1) + 1 \\
&= (1 \cdot n) + 1 \\
&= 1 \cdot (n+1).
\end{aligned}$$

Qed.

Thus every natural number is contained in $Q$. Hence the thesis. End. Qed.

(INDUCTION STEP) For all natural numbers $m$ we have $m \in P \implies m+1 \in P$.
Proof. Let $m$ be a natural number. Assume $m \in P$.

For all natural numbers $n$ we have $n \cdot (m+1) = (m+1) \cdot n$.
Proof. Let $n$ be a natural number. Then

$$\begin{aligned}
&n \cdot (m+1) \\
&= (n \cdot m) + (n \cdot 1) \\
&= (m \cdot n) + (1 \cdot n) \\
&= (1 \cdot n) + (m \cdot n) \\
&= (1+m) \cdot n \\
&= (m+1) \cdot n.
\end{aligned}$$

Qed. Qed.

Hence every natural number is contained in $P$. $\square$

**Non-existence of zero-divisors:**

**Proposition 3.10.** For all $n, m$ we have

$$n \cdot m = 0 \implies (n = 0 \text{ or } m = 0).$$

*Proof.* Let $n, m$ be natural numbers. Assume $n \cdot m = 0$.

If $n$ and $m$ are not equal to 0 then we have a contradiction.
Proof. Assume $n, m \neq 0$. Take natural numbers $n', m'$ such that $n = (n' + 1)$ and $m = (m' + 1)$. Then

$$\begin{aligned} 0 \\ &= n \cdot m \\ &= (n' + 1) \cdot (m' + 1) \\ &= ((n' + 1) \cdot m') + (n' + 1) \\ &= (((n' + 1) \cdot m') + n') + 1. \end{aligned}$$

Hence $0 = k + 1$ for some natural number $k$. Contradiction. Qed.

Thus $n = 0$ or $m = 0$. □

**Cancellation:**

**Proposition 3.11.** Assume $k \neq 0$. Then for all $n, m$ we have

$$n \cdot k = m \cdot k \implies n = m.$$

*Proof.* Define

$$P = \left\{ n \in \mathbb{N} \;\middle|\; \begin{array}{l} \text{for all natural numbers } m \text{ if } n \cdot k = m \cdot k \text{ and } k \neq 0 \text{ then} \\ n = m \end{array} \right\}.$$

(BASE CASE) 0 is contained in $P$.
Proof. Let us show that for all natural numbers $m$ if $0 \cdot k = m \cdot k$ and $k \neq 0$ then $0 = m$. Let $m, k$ be natural numbers. Assume that $0 \cdot k = m \cdot k$ and $k \neq 0$. Then $m \cdot k = 0$. Hence $m = 0$ or $k = 0$. Thus $m = 0$. End. Qed.

(INDUCTION STEP) For all natural numbers $n$ we have $n \in P \implies n + 1 \in P$.
Proof. Let $n$ be a natural number. Assume $n \in P$.

For all natural numbers $m$ if $(n + 1) \cdot k = m \cdot k$ and $k \neq 0$ then $n + 1 = m$.
Proof. Let $m$ be natural numbers. Assume $(n + 1) \cdot k = m \cdot k$ and $k \neq 0$.

Case $m = 0$. Then $(n + 1) \cdot k = 0$. Hence $n + 1 = 0$. Contradiction. End.

Case $m \neq 0$. Take a natural number $m'$ such that $m = m' + 1$. Then $(n+1) \cdot k = (m' + 1) \cdot k$. Hence $(n \cdot k) + k = (m' \cdot k) + k$. Thus $n \cdot k = m' \cdot k$

(by 2.11). Then we have $n = m'$. Therefore $n + 1 = m' + 1 = m$. End. Qed. Qed.

Thus every natural number is contained in $P$. □

**Corollary 3.12.** Assume $k \neq 0$. Then for all $n, m$ we have

$$k \cdot n = k \cdot m \implies n = m.$$

*Proof.* Let $n, m$ be natural numbers. Assume $k \cdot n = k \cdot m$. We have $k \cdot n = n \cdot k$ and $k \cdot m = m \cdot k$. Hence $n \cdot k = m \cdot k$. Thus $n = m$. □

# 4 Exponentiation

[readtex `arithmetic/sections/01_arithmetic/03_multiplication.ftl.tex`]

Let $k, l, m, n$ denote natural numbers.

## 4.1 Axioms

Another common operation on the natural numbers is exponentiation. Again, we introduce it as an inductively defined operation.

**Signature 4.1.** $n^m$ is a natural number.

Let the square of $n$ stand for $n^2$. Let the cube of $n$ stand for $n^3$.

**Axiom 4.2 (1st exponentiation axiom).** $n^0 = 1$.

**Axiom 4.3 (2nd exponentiation axiom).** $n^{m+1} = n^m \cdot n$.

## 4.2 Computation laws

As in the previous sections let us prove some basic arithmetical properties of our new operation.

### Exponentiation with 0, 1 and 2

**Proposition 4.4.** Assume that $n \neq 0$. Then

$$0^n = 0.$$

*Proof.* Take a natural number $m$ such that $n = m + 1$. Then

$$0^n = 0^{m+1} = 0^m \cdot 0 = 0.$$

□

**Proposition 4.5.** For all natural numbers $n$ we have

$$1^n = 1.$$

*Proof.* Define

$$P = \{\, n \in \mathbb{N} \mid 1^n = 1 \,\}.$$

(BASE CASE) $P$ contains 0.

(INDUCTION STEP) For all natural numbers $n$ we have $n \in P \implies n + 1 \in P$.
Proof. Let $n$ be a natural number. Assume $n \in P$. Then

$1^{n+1} = 1^n \cdot 1 = 1 \cdot 1 = 1$. Qed.

Hence every natural number is contained in $P$ . □

**Proposition 4.6.** $n^1 = n$.

*Proof.* $n^1 = n^{0+1} = n^0 \cdot n = 1 \cdot n = n$. □

**Proposition 4.7.** $n^2 = n \cdot n$.

*Proof.* $n^2 = n^{1+1} = n^1 \cdot n = n \cdot n$. □

**Sums as exponents:**

**Proposition 4.8.** For all $n, m, k$ we have

$$k^{n+m} = k^n \cdot k^m.$$

*Proof.* Define

$$P = \{\, k \in \mathbb{N} \mid n^{m+k} = n^m \cdot n^k \text{ for all natural numbers } n, m \,\}.$$

(BASE CASE) $P$ contains 0.
Proof. Let us show that for all natural numbers $n, m$ we have $n^{m+0} = n^m \cdot n^0$. Let $n, m$ be natural numbers. Then

$n^{m+0} = n^m = n^m \cdot 1 = n^m \cdot n^0$. End. Qed.

(INDUCTION STEP) For all natural numbers $k$ we have $k \in P \implies k + 1 \in P$.
Proof. Let $k$ be a natural number. Assume $k \in P$.

Let us show that for all natural numbers $n, m$ we have $n^{m+(k+1)} = n^m \cdot n^{k+1}$. Let $n, m$ be natural numbers. Then

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

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

End. Qed.

Hence every natural number is contained in $P$. □

**Products as exponents:**

**Proposition 4.9.** For all $n, m, k$ we have

$$k^{n \cdot m} = (k^n)^m.$$

*Proof.* Define

$$P = \left\{ k \in \mathbb{N} \;\middle|\; n^{m \cdot k} = (n^m)^k \text{ for all natural numbers } n, m \right\}.$$

(BASE CASE) $P$ contains 0. Indeed $(n^m)^0 = 1 = n^0 = n^{m \cdot 0}$ for all natural numbers $n, m$.

(INDUCTION STEP) For all natural numbers $k$ we have $k \in P \implies k + 1 \in P$.
Proof. Let $k$ be a natural number. Assume $k \in P$.

For all natural numbers $n, m$ we have $(n^m)^{k+1} = n^{m \cdot (k+1)}$.
Proof. Let $n, m$ be natural numbers. Then

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

Qed. Qed.

Therefore every natural number is contained in $P$. □

**Products as base:**

**Proposition 4.10.** For all natural numbers $n, m, k$ we have

$$((n \cdot m)^k) = n^k \cdot m^k.$$

*Proof.* Define

$$P = \{\, k \in \mathbb{N} \mid (n \cdot m)^k = n^k \cdot m^k \text{ for all natural numbers } n, m \,\}.$$

(BASE CASE) $P$ contains 0. Indeed $((n \cdot m)^0) = 1 = 1 \cdot 1 = n^0 \cdot m^0$ for all natural numbers $n, m$.

(INDUCTION STEP) For all natural numbers $k$ we have $k \in P \implies k + 1 \in P$.
Proof. Let $k$ be a natural number. Assume $k \in P$.

$((n \cdot m)^{k+1}) = n^{k+1} \cdot m^{k+1}$ for all natural numbers $n, m$.
Proof. Let $n, m$ be natural numbers.

(Claim) We have

$$\begin{aligned}
&(n^k \cdot m^k) \cdot (n \cdot m) \\
&= ((n^k \cdot m^k) \cdot n) \cdot m \\
&= (n^k \cdot (m^k \cdot n)) \cdot m \\
&= (n^k \cdot (n \cdot m^k)) \cdot m \\
&= ((n^k \cdot n) \cdot m^k) \cdot m \\
&= (n^k \cdot n) \cdot (m^k \cdot m).
\end{aligned}$$

Hence

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

Qed. Qed.

Therefore every natural number is contained in $P$. □

**Zeroes of exponentiation:**

**Proposition 4.11.** For all $n, m$ we have

$$n^m = 0 \iff (n = 0 \text{ and } m \neq 0).$$

*Proof.* (1) For all $n, m$ if $n^m = 0$ then $n = 0$ and $m \neq 0$.
Proof. Define

$$P = \left\{ m \in \mathbb{N} \;\middle|\; \begin{array}{l} \text{for all natural numbers } n \text{ if } n^m = 0 \text{ then } n = 0 \text{ and} \\ m \neq 0 \end{array} \right\}.$$

(BASE CASE) $P$ contains 0. Indeed for all natural numbers $n$ if $n^0 = 0$ then we have a contradiction.

(INDUCTION STEP) For all natural numbers $m$ we have $m \in P \implies m + 1 \in P$.
Proof. Let $m$ be a natural number. Assume $m \in P$.

For all natural numbers $n$ if $n^{m+1} = 0$ then $n = 0$ and $m + 1 \neq 0$.
Proof. Let $n$ be a natural number. Assume $n^{m+1} = 0$. Then $0 = n^{m+1} = n^m \cdot n$. Hence $n^m = 0$ or $n = 0$. We have $m + 1 \neq 0$ and if $n^m = 0$ then $n = 0$. Hence the thesis. Qed. Qed.

Thus every natural number is contained in $P$. Qed.

(2) For all $n, m$ if $n = 0$ and $m \neq 0$ then $n^m = 0$.
Proof. Let $n, m$ be natural numbers. Assume $n = 0$ and $m \neq 0$. Take a natural number $k$ such that $m = k + 1$. Then

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

Qed. □

# 5 Factorial

[readtex `arithmetic/sections/01_arithmetic/03_multiplication.ftl.tex`]

Let $k, l, m, n$ denote natural numbers.

An operation rather rarely mentioned together with (formal) Peano arithmetic is the factorial operation which we are going to define now.

**Signature 5.1.** $n!$ is a natural number.

**Axiom 5.2 ($1^{\text{st}}$ factorial axiom).** $(0!) = 1$.

**Axiom 5.3 ($2^{\text{nd}}$ factorial axiom).** $((n+1)!) = n! \cdot (n+1)$.

Note that we have to put the LHS of any expression of the form "$x! = y$" in parentheses, because such an expression can either be understood as "$x$ factorial is equal to $y$" or as "$x$ is not equal to $y$" by Naproche since it treats the combination of an exclamation mark followed by an equality sign as a synonym for "$\neq$".

**Proposition 5.4.** $n!$ is nonzero for any natural number $n$.

*Proof.* Define

$$P = \{\, n \in \mathbb{N} \mid n! \neq 0 \,\}.$$

(BASE CASE) $P$ contains 0. Indeed $(0!) = 1 \neq 0$.

(INDUCTION STEP) For every natural number $n$ we have $n \in P \implies n+1 \in P$.
Proof. Let $n$ be a natural number. Assume $n \in P$. We have $((n+1)!) = (n+1) \cdot (n!)$. $n+1$ and $n!$ are nonzero. Hence $(n+1)!$ is nonzero. Qed.

Thus $P$ contains every natural number. □

# Part II
# Ordering

## 6 Ordering

[readtex `arithmetic/sections/01_arithmetic/02_addition.ftl.tex`]

Let $k, l, m, n$ denote natural numbers.

In this section we will establish an order on the natural numbers.

### 6.1 Definitions and immediate consequences

A natural number $m$ should be greater than a natural number $n$ if $m$ can be reached from $n$ by iteratively applying the successor operation to $n$. Or, in other words, if $m$ can be reached by adding a nonzero natural number to $m$.

**Definition 6.1.** $n < m$ iff there exists a nonzero natural number $k$ such that $m = n + k$.

Let $n$ is less than $m$ stand for $n < m$. Let $n > m$ stand for $m < n$. Let $n$ is greater than $m$ stand for $n > m$. Let $n \not< m$ stand for $n$ is not less than $m$. Let $n \not> m$ stand for $n$ is not greater than $m$. Let $n$ is positive stand for $n > 0$.

**Definition 6.2.** $n \leq m$ iff there exists a natural number $k$ such that $m = n + k$.

Let $n$ is less than or equal to $m$ stand for $n \leq m$. Let $n \geq m$ stand for $m \leq n$. Let $n$ is greater than or equal to $m$ stand for $n \geq m$. Let $n \not\leq m$ stand for $n$ is not less than or equal to $m$. Let $n \not\geq m$ stand for $n$ is not greater than or equal to $m$.

**Proposition 6.3.** $n \leq m$ iff $n < m$ or $n = m$.

*Proof.* Case $n \leq m$. Take a natural number $k$ such that $m = n + k$. If $k = 0$ then $n = m$. If $k \neq 0$ then $n < m$. End.

Case $n < m$ or $n = m$. If $n < m$ then there is a positive natural number $k$ such that $m = n + k$. If $n = m$ then $m = n + 0$. Thus if $n < m$ then there is a natural number $k$ such that $m = n + k$. Hence the thesis. End. □

This relation enables us to to generalize the notions of direct predecessors and successors:

**Definition 6.4.** A predecessor of $n$ is a natural number that is less than $n$.

**Definition 6.5.** A successor of $n$ is a natural number that is greater than

$n$.

A direct consequence of the definition of our ordering relation is that the terms "positive" and "non-zero"coincide on the natural numbers.

**Proposition 6.6.** $n$ is positive iff $n$ is nonzero.

*Proof.* Case $n$ is positive. Take a positive natural number $k$ such that $n = 0 + k = k$. Then we have $n \neq 0$. End.

Case $n$ is nonzero. Take a natural number $k$ such that $n = k + 1$. Then $n = 0 + (k + 1)$. $k + 1$ is positive. Hence $0 < n$. End. □

## 6.2 Basic properties

Let us now prove some basic relational properties of the ordering.

**Proposition 6.7.** $n \not< n$.

*Proof.* Assume the contrary. Then we can take a positive natural number $k$ such that $n = n + k$. Then we have $0 = k$. Contradiction. □

**Proposition 6.8.** If $n < m$ then $n \neq m$.

*Proof.* Assume $n < m$. Take a positive natural number $k$ such that $m = n + k$. If $n = m$ then $k = 0$. Hence $n \neq m$. □

**Proposition 6.9.** If $n \leq m$ and $m \leq n$ then $n = m$.

*Proof.* Assume $n \leq m$ and $m \leq n$. Take natural numbers $k, l$ such that $m = n + k$ and $n = m + l$. Then $m = (m + l) + k = m + (l + k)$. Hence $l + k = 0$. Therefore $l = 0 = k$. Then we have the thesis. □

**Proposition 6.10.** If $n < m < k$ then $n < k$.

*Proof.* Assume $n < m < k$. Take a positive natural number $a$ such that $m = n + a$. Take a positive natural number $b$ such that $k = m + b$. Then $k = (n + a) + b = n + (a + b)$. $a + b$ is positive. Hence $n < k$. □

**Proposition 6.11.** If $n \leq m \leq k$ then $n \leq k$.

*Proof.* Case $n = m = k$. Obvious.

Case $n = m < k$. Obvious.

Case $n < m = k$. Obvious.

Case $n < m < k$. Obvious. □

**Proposition 6.12.** If $n \leq m < k$ then $n < k$.

*Proof.* Assume $n \leq m < k$. If $n = m$ then $n < k$. If $n < m$ then $n < k$. □

**Proposition 6.13.** If $n < m \leq k$ then $n < k$.

*Proof.* Assume $n < m \leq k$. If $m = k$ then $n < k$. If $m < k$ then $n < k$. □

**Proposition 6.14.** If $n < m$ then $n + 1 \leq m$.

*Proof.* Assume $n < m$. Take a positive natural number $k$ such that $m = n + k$.

Case $k = 1$. Then $m = n + 1$. Hence $n + 1 \leq m$. End.

Case $k \neq 1$. Then we can take a natural number $l$ such that $k = l + 1$. Then $m = n + (l + 1) = (n + l) + 1 = (n + 1) + l$. $l$ is positive. Thus $n + 1 < m$. End. □

**Proposition 6.15.** For all $n, m$ we have $n < m$ or $n = m$ or $n > m$.

*Proof.* Define

$$P = \left\{ m \in \mathbb{N} \;\middle|\; \begin{array}{l} \text{for all natural numbers } n \text{ we have } n < m \text{ or } n = m \text{ or} \\ n > m \end{array} \right\}.$$

(BASE CASE) $P$ contains 0.

(INDUCTION STEP) For all natural numbers $m$ we have $m \in P \implies m + 1 \in P$.
Proof. Let $m$ be a natural number. Assume $m \in P$.

For all natural numbers $n$ we have $n < m + 1$ or $n = m + 1$ or $n > m + 1$.
Proof. Let $n$ be a natural number.

Case $n < m$. Obvious.

Case $n = m$. Obvious.

Case $n > m$. Take a positive natural number $k$ such that $n = m + k$.

Case $k = 1$. Obvious.

Case$k \neq 1$. Take a natural number $l$ such that $n = (m + 1) + l$. Hence $n > m + 1$. Indeed $l$ is positive. End. End. Qed. Qed.

Thus every natural number is contained in $P$. □

**Proposition 6.16.** $n \not< m$ iff $n \geq m$.

*Proof.* Case $n \not< m$. Then $n = m$ or $n > m$. Hence $n \geq m$. End.

Case $n \geq m$. Assume $n < m$. Then $n \leq m$. Hence $n = m$. Contradiction. End. □

## 6.3 Ordering and successors

We end this section by showing that there are no natural numbers between $n$ and $n+1$.

**Proposition 6.17.** If $n < m \leq n+1$ then $m = n+1$.

*Proof.* Assume $n < m \leq n+1$. Take a positive natural number $k$ such that $m = n+k$. Take a natural number $l$ such that $n+1 = m+l$. Then $n+1 = m+l = (n+k)+l = n+(k+l)$. Hence $k+l = 1$.

We have $l = 0$.
Proof. Assume the contrary. Then $k, l > 0$.

Case $k, l = 1$. Then $k+l = 2 \neq 1$. Contradiction. End.

Case $k = 1 and l \neq 1$. Then $l > 1$. Hence $k+l > 1+l > 1$. Contradiction. End.

Case $k \neq 1 and l = 1$. Then $k > 1$. Hence $k+l > k+1 > 1$. Contradiction. End.

Case $k, l \neq 1$. Take natural numbers $a, b$ such that $k = a+1$ and $l = b+1$. Indeed $k, l \neq 0$. Hence $k = a+1$ and $l = b+1$. Thus $k, l > 1$. Indeed $a, b$ are positive. End. Qed.

Then we have $n+1 = m+l = m+0 = m$. □

**Proposition 6.18.** If $n \leq m < n+1$ then $n = m$.

*Proof.* Assume $n \leq m < n+1$.

Case $n = m$. Obvious.

Case $n < m$. Then $n < m \leq n+1$. Hence $n = m$. End. □

**Corollary 6.19.** There is no natural number $m$ such that $n < m < n+1$.

*Proof.* Assume the contrary. Take a natural number $m$ such that $n < m < n+1$. Then $n < m \leq n+1$ and $n \leq m < n+1$. Hence $m = n+1$ and $m = n$ (by 6.17, 6.18). Hence $n = n+1$. Contradiction. □

**Proposition 6.20.** $n+1 \geq 1$.

*Proof.* Case $n = 0$. Obvious.

Case $n \neq 0$. Then $n > 0$. Hence $n+1 > 0+1 = 1$. End. □

# 7 Ordering and addition

[readtex `arithmetic/sections/02_ordering/01_ordering.ftl.tex`]

Let $k, l, m, n$ denote natural numbers.

In this section we will briefly study the behaviour of the ordering with respect to addition.

**Proposition 7.1.** We have

$$n < m \iff n + k < m + k.$$

*Proof.* Case $n < m$. Take a positive natural number $l$ such that $m = n + l$. Then $m + k = (n + l) + k = (n + k) + l$. Hence $n + k < m + k$. End.

Case $n + k < m + k$. Take a positive natural number $l$ such that $m + k = (n + k) + l$. $(n + k) + l = n + (k + l) = n + (l + k) = (n + l) + k$. Hence $m + k = (n + l) + k$. Thus $m = n + l$. Therefore $n < m$. End. □

**Corollary 7.2.** We have

$$n < m \iff k + n < k + m.$$

*Proof.* We have $k + n = n + k$ and $k + m = m + k$. Hence $k + n < k + m$ iff $n + k < m + k$. □

**Corollary 7.3.** $n \leq m$ iff $k + n \leq k + m$.

**Corollary 7.4.** $n \leq m$ iff $n + k \leq m + k$.

# 8 Ordering and multiplication

[readtex `arithmetic/sections/01_arithmetic/03_multiplication.ftl.tex`]

[readtex `arithmetic/sections/02_ordering/02_ordering-and-addition.ftl.tex`]

Let $k, l, m, n$ denote natural numbers.

As we did with addition, we will now examine the behaviour of the ordering with respect to multiplication.

**Proposition 8.1.** Assume $k \neq 0$. Then for all $n, m$ we have

$$n < m \iff n \cdot k < m \cdot k.$$

*Proof.* Define

$$P = \{\, n \in \mathbb{N} \mid \text{for all natural numbers } m \text{ if } n \cdot k < m \cdot k \text{ then } n < m \quad \}.$$

Let us show that every natural number is contained in $P$. (BASE CASE) $P$ contains 0.

(INDUCTION STEP) For all natural numbers $n$ we have $n \in P \implies n+1 \in P$. Proof. Let $n$ be a natural number. Assume $n \in P$.

For all natural numbers $m$ if $(n+1) \cdot k < m \cdot k$ then $n+1 < m$.
Proof. Let $m$ be a natural number. Assume $(n+1) \cdot k < m \cdot k$. Then $(n \cdot k) + k < m \cdot k$. Hence $n \cdot k < m \cdot k$. Thus $n < m$. Then $n+1 \leq m$. If $n+1 = m$ then $(n+1) \cdot k = m \cdot k$. Hence the thesis. Qed. Qed.

Therefore every natural number is contained in $P$. End.

Let $n, m$ be natural numbers.

Case $n < m$. Take a positive natural number $l$ such that $m = n + l$. Then $m \cdot k = (n+l) \cdot k = (n \cdot k) + (l \cdot k)$. $l \cdot k$ is positive. Hence $n \cdot k < m \cdot k$. End.

Case $n \cdot k < m \cdot k$. Then $n < m$. Indeed $n$ and $m$ are contained in $P$. End. □

**Corollary 8.2.** Assume $k \neq 0$. Then

$$n < m \iff k \cdot n < k \cdot m.$$

*Proof.* We have $k \cdot n = n \cdot k$ and $k \cdot m = m \cdot k$. Hence $k \cdot n < k \cdot m$ iff $n \cdot k < m \cdot k$. □

**Proposition 8.3.** For all $n, m$ we have

$$n, m > k \implies n \cdot m > k.$$

*Proof.* Define

$$P = \{\, n \in \mathbb{N} \mid \text{for all natural numbers } m \text{ if } n, m > k \text{ then } n \cdot m > k \quad \}.$$

(BASE CASE) $P$ contains 0.

(INDUCTION STEP) For all natural numbers $n$ we have $n \in P \implies n+1 \in P$.
Proof. Let $n$ be a natural number. Assume $n \in P$.

For all natural numbers $m$ if $n+1, m > k$ then $(n+1) \cdot m > k$.
Proof. Let $m$ be a natural number. Assume $n+1, m > k$. Then $(n+1) \cdot m = (n \cdot m) + m$. If $n = 0$ then $(n \cdot m) + m = 0 + m = m > k$. If $n \neq 0$ then $(n \cdot m) + m > m > k$. Indeed if $n \neq 0 then n \cdot m > 0$. Indeed $m > 0$. Hence $(n+1) \cdot m > k$. Qed. Qed.

Hence every natural number is contained in $P$. □

**Corollary 8.4.** We have

$$n \leq m \implies k \cdot n \leq k \cdot m.$$

**Corollary 8.5.** Assume $k \neq 0$. Then

$$k \cdot n \leq k \cdot m \implies n \leq m.$$

**Corollary 8.6.** We have

$$n \leq m \implies n \cdot k \leq m \cdot k.$$

**Corollary 8.7.** Assume $k \neq 0$. Then

$$n \cdot k \leq m \cdot k \implies n \leq m.$$

**Proposition 8.8.** Let $k > 1$ and $m > 0$. Then $k \cdot m > m$.

*Proof.* Take a natural number $l$ such that $k = l + 2$. Then

$$\begin{aligned} & k \cdot m \\ &= (l+2) \cdot m \\ &= (l \cdot m) + (2 \cdot m) \\ &= (l \cdot m) + (m + m) \\ &= ((l \cdot m) + m) + m \\ &= ((l+1) \cdot m) + m \\ &\geq 1 + m \\ &> m. \end{aligned}$$

□

# 9 Ordering and exponentiation

[readtex `arithmetic/sections/01_arithmetic/04_exponentiation.ftl.tex`]

[readtex `arithmetic/sections/02_ordering/03_ordering-and-multiplication.ftl.tex`]

Let $k, l, m, n$ denote natural numbers.

To conclude our investigations about the interplay between the ordering and our arithmetical operations, let us have a look at exponentiation.

**Proposition 9.1.** Assume $k \neq 0$. Then for all $n, m$ we have

$$n < m \iff n^k < m^k.$$

*Proof.* Define

$$P = \left\{ k' \in \mathbb{N} \;\middle|\; \begin{array}{l} \text{for all natural numbers } n, m \text{ if } n < m \text{ and } k' > 1 \text{ then} \\ n^{k'} < m^{k'} \end{array} \right\}.$$

Let us show that every natural number is contained in $P$. (BASE CASE 1) $P$ contains 0.

(BASE CASE 2) $P$ contains 1.

(BASE CASE 3) $P$ contains 2.
Proof. Let us show that for all natural numbers $n, m$ if $n < m$ then $n^2 < m^2$. Let $n, m$ be natural numbers. Assume $n < m$.

Case $n = 0$ or $m = 0$. Obvious.

Case $n, m \neq 0$. Then $n \cdot n < n \cdot m < m \cdot m$ (by 8.1, 8.2). Hence $n^2 = n \cdot n < n \cdot m < m \cdot m = m^2$. End. End. Qed.

(INDUCTION STEP) For all natural numbers $k'$ we have $k' \in P \implies k' + 1 \in P$.
Proof. Let $k'$ be a natural number. Assume $k' \in P$.

For all natural numbers $n, m$ if $n < m$ and $k' + 1 > 1$ then $n^{k'+1} < m^{k'+1}$.
Proof. Let $n, m$ be natural numbers. Assume $n < m$ and $k' + 1 > 1$. Then $n^{k'} < m^{k'}$. Indeed $k' \neq 0$ and $if k' = 1$ then $n^{k'} < m^{k'}$.

Case $k' \leq 1$. Then $k' = 0$ or $k' = 1$. Hence $k' + 1 = 1$ or $k' + 1 = 2$. Thus $k' + 1 \in P$. Therefore $n^{k'+1} < m^{k'+1}$. End.

Case $k' > 1$. Case $n = 0$. Then $m \neq 0$. Hence $n^{k'+1} = 0 < m^{k'} \cdot m = m^{k'+1}$. Thus $n^{k'+1} < m^{k'+1}$. End.

Case $n \neq 0$. Then $n^{k'} \cdot n < m^{k'} \cdot n < m^{k'} \cdot m$ (by 8.1, 8.2). Indeed $n^{k'} < m^{k'} \neq 0$. Hence $n^{k'+1} = n^{k'} \cdot n < m^{k'} \cdot n < m^{k'} \cdot m = m^{k'+1}$. Thus $n^{k'+1} < m^{k'+1}$ (by 6.10). End. End.

Hence the thesis. Indeed $k' \leq 1$ or $k' > 1$. Qed.

$k' + 1 \in P$. Qed.

Therefore every natural number is contained in $P$. End.

Define

$$Q = \left\{ k' \in \mathbb{N} \;\middle|\; \text{for all natural numbers } n, m \text{ if } n \geq m \text{ then } n^{k'} \geq m^{k'} \right\}.$$

Let us show that every natural number is contained in $Q$. (BASE CASE) $Q$ contains 0.

(INDUCTION STEP) For all natural numbers $k'$ we have $k' \in Q \implies k'+1 \in Q$.
Proof. Let $k'$ be a natural number. Assume $k' \in Q$.

For all natural numbers $n, m$ if $n \geq m$ then $n^{k'+1} \geq m^{k'+1}$.
Proof. Let $n, m$ be natural numbers. Assume $n \geq m$. Then $n^{k'} \geq m^{k'}$. Hence $n^{k'} \cdot n \geq m^{k'} \cdot n \geq m^{k'} \cdot m$. Thus $n^{k'+1} = n^{k'} \cdot n \geq m^{k'} \cdot n \geq m^{k'} \cdot m = m^{k'+1}$. Therefore $n^{k'+1} \geq m^{k'+1}$ (by 6.11). Qed.

Hence the thesis. Indeed $k'+1$ is a natural number. Qed.

Thus every natural number is contained in $Q$. End.

Let $n, m$ be natural numbers.

Case $n < m$. Case $k = 1$. Obvious.

Case$k \neq 1$. Then $k > 1$. Indeed $k < 1$ or $k = 1$ or $k > 1$. Hence $n^k < m^k$. Indeed $n$ and $m$ belong to $P$. End. End.

Case $n^k < m^k$. Then $n^k \not\geq m^k$. Hence $n \not\geq m$. Indeed $n$ and $m$ are contained in $Q$. Thus $n < m$. End. □

**Corollary 9.2.** Assume $k \neq 0$. Then

$$n^k = m^k \implies n = m.$$

*Proof.* Assume $n \neq m$. Then $n < m$ or $m < n$. If $n < m$ then $n^k < m^k$ (by 9.1). If $m < n$ then $m^k < n^k$. Thus $n^k \neq m^k$. Hence the thesis. □

**Corollary 9.3.** Assume $k \neq 0$. Then

$$n^k \leq m^k \iff n \leq m.$$

*Proof.* If $n^k < m^k$ then $n < m$. If $n^k = m^k$ then $n = m$.

If $n < m$ then $n^k < m^k$ (by 9.1). If $n = m$ then $n^k = m^k$. □

**Proposition 9.4.** Assume $k > 1$. Then for all $n, m$ we have

$$n < m \iff k^n < k^m.$$

*Proof.* Define

$$P = \left\{ m \in \mathbb{N} \;\middle|\; \begin{array}{l} \text{for all natural numbers } n \text{ if } k > 1 \text{ and } n < m \text{ then} \\ k^n < k^m \end{array} \right\}.$$

Let us show that every natural number is contained in $P$.

(BASE CASE) $P$ contains 0.

(INDUCTION STEP) For all natural numbers $m$ we have $m \in P \implies m+1 \in P$.
Proof. Let $m$ be a natural number. Assume $m \in P$.

For all natural numbers $n$ if $k > 1$ and $n < m + 1$ then $k^n < k^{m+1}$.
Proof. Let $n$ be natural numbers such that $k > 1$ and $n < m + 1$. Then $n \leq m$. We have $k^m \cdot 1 < k^m \cdot k$. Indeed $k^m \neq 0$. Case $n = m$. Then $k^n = k^m < k^m \cdot k = k^{m+1}$. End.

Case $n < m$. Then $k^n < k^m < k^m \cdot k = k^{m+1}$. End. Qed. Qed.

Hence every natural number is contained in $P$. End.

Define

$$Q = \left\{ n \in \mathbb{N} \;\middle|\; \begin{array}{l} \text{for all natural numbers } m \text{ if } n \geq m \text{ then } k^n \geq k^m \text{ or} \\ k \leq 1 \end{array} \right\}.$$

Let us show that every natural number is contained in $Q$.

(BASE CASE) $0 \in Q$.

(INDUCTION STEP) For all natural numbers $n$ we have $n \in Q \implies n + 1 \in Q$.
Proof. Let $n$ be a natural number. Assume $n \in Q$.

For all natural numbers $m$ if $n + 1 \geq m$ then $k^{n+1} \geq k^m$ or $k \leq 1$.
Proof. Let $m$ be natural numbers. Assume $n + 1 \geq m$.

Case $n + 1 = m$. Obvious.

Case $n + 1 > m$. Then $n \geq m$. Hence $k^n \geq k^m$ or $k \leq 1$.

Case $k \leq 1$. Obvious.

Case $k^n \geq k^m$. We have $k^n \cdot 1 \leq k^n \cdot k$. Indeed $1 \leq k$ and $k^n \neq 0$. Hence $k^m \leq k^n = k^n \cdot 1 \leq k^n \cdot k = k^{n+1}$. End. End. Qed. Qed.

Thus every natural number is contained in $Q$. End.

Let $n, m$ be natural numbers.

Case $n < m$. Then $k^n < k^m$. Indeed $n$ and $m$ are contained in $P$. End.

Case $k^n < k^m$. Then it is wrong that $k^n \geq k^m$ or $k \leq 1$. Hence $n \not\geq m$. Indeed $n$ and $m$ are contained in $Q$. Thus $n < m$. End. □

**Corollary 9.5.** Assume $k > 1$. Then

$$k^n = k^m \implies n = m.$$

*Proof.* Assume $n \neq m$. Then $n < m$ or $m < n$. If $n < m$ then $k^n < k^m$. If $m < n$ then $k^m < k^n$. Thus $k^n \neq k^m$. Hence the thesis. □

**Corollary 9.6.** Assume $k > 1$. Then

$$n \leq m \iff k^n \leq k^m.$$

# 10 Induction

[readtex `arithmetic/sections/02_ordering/01_ordering.ftl.tex`]

Let $k, l, m, n$ denote natural numbers.

When we introduced the Peano axioms we came across an induction axiom which gives us a method to prove universal assertions about the natural numbers. In this section we will give some reformulations of this induction principle.

## 10.1 Least natural numbers

As a first example of such a reformulation we will show in this paragraph that every collection of natural numbers admits a smallest element.

Let $P$ denote a class.

**Definition 10.1.** A least natural number of $P$ is a natural number $n$ such that $n \in P$ and no natural number that is less than $n$ belongs to $P$.

**Lemma 10.2.** Let $n, m$ be least natural numbers of $P$. Then $n = m$.

*Proof.* Assume $n \neq m$. Then $n < m$ or $m < n$. If $n < m$ then $n \notin P$ and if $m < n$ then $m \notin P$. Contradiction. Therefore $n = m$. □

**Theorem 10.3.** Assume that $P$ contains some natural number. Then $P$ has a least natural number.

*Proof.* Assume the contrary. Define

$$Q = \{\, n \in \mathbb{N} \mid \text{n is less than any natural number } m \text{ such that } m \in P \,\}.$$

Let us show that every natural number belongs to $Q$.

(BASE CASE) $Q$ contains 0.
Proof. If $P$ contains 0 then 0 is the least natural number of $P$. Hence 0 is less than any natural number $m$ such that $m \in P$. Therefore $Q$ contains 0. Qed.

For all natural numbers $n$ we have $n \in Q \implies n + 1 \in Q$.
Proof. Let $n$ be a natural number. Assume $n \in Q$. Then $n$ is less than any natural number $m$ such that $m \in P$. Assume that $Q$ does not contain $n+1$. Then we can take a natural number $m$ such that $m \in P$ and $n + 1 \not< m$. Hence $n < m \leq n + 1$. Thus $m = n + 1$. Then $n + 1$ is the least natural number of $P$. Contradiction. Qed. End.

Then every natural number is less than any natural number $n$ such that $n \in P$. Hence there is no natural number $n$ such that $n \in P$. Contradiction. □

## 10.2 Induction via predecessors

Next we will see how to merge the base and induction step of a proof by induction into a single step. This yields a new induction principle.

**Theorem 10.4.** Assume for all natural numbers $n$ if $P$ contains all predecessors of $n$ then $P$ contains $n$. Then $P$ contains every natural number.

*Proof.* Assume the contrary. Take a natural number $n$ such that $P$ does not contain $n$. Define $Q = \{ k \in \mathbb{N} \mid k \notin P \}$. Then $Q$ contains $n$. Thus we can take a least natural number $m$ of $Q$. Hence $Q$ does not contain any predecessor of $m$. Therefore $P$ contains all predecessors of $m$. Thus $P$ contains $m$. Contradiction. □

## 10.3 Induction above a certain number

In our induction principle given by the 3rd Peano axiom we considered the number 0 as the starting point of an inductive proof. But we can as well start at any arbitrary number $k$ to prove that a statement holds for all natural numbers from $k$ on.

**Theorem 10.5.** Let $k$ be a natural number such that $k \in P$. Suppose that for all natural numbers $n$ such that $n \geq k$ we have $n \in P \implies n+1 \in P$. Then for every natural number $n$ such that $n \geq k$ we have $n \in P$.

*Proof.* Define

$$Q = \{ n \in \mathbb{N} \mid \text{if } n \geq k \text{ then } n \in P \}.$$

Let us show that every natural number belongs to $Q$.

(BASE CASE) We have $0 \in Q$.

(INDUCTION STEP) For all natural numbers $n$ we have $n \in Q \implies n+1 \in Q$.
Proof. Let $n$ be a natural number. Assume $n \in Q$.

If $n+1 \geq k$ then $n+1 \in P$.
Proof. Assume $n+1 \geq k$.

Case $n < k$. Then $n+1 = k$. Hence $n+1 \in P$. End.

Case $n \geq k$. Then $n \in P$. Hence $n+1 \in P$. End. Qed.

Thus we have $n+1 \in Q$. Qed. End.

Therefore $Q$ contains every natural number. Hence the thesis. □

# 11 Standard exercises

[readtex `arithmetic/sections/01_arithmetic/04_exponentiation.ftl.tex`]

[readtex `arithmetic/sections/01_arithmetic/05_factorial.ftl.tex`]

[readtex `arithmetic/sections/02_ordering/04_ordering-and-exponentiation.ftl.tex`]

[readtex `arithmetic/sections/02_ordering/05_induction.ftl.tex`]

Let $k, l, m, n$ denote natural numbers.

In this section we will have a look some standard text book exercises on induction and prove them within our arithmetic.

**Proposition 11.1.** We have

$$(n+1)^2 = (n^2 + (2 \cdot n)) + 1.$$

*Proof.* We have

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

□

**Proposition 11.2.** For all $n$ if $n \geq 3$ then

$$n^2 > (2 \cdot n) + 1.$$

*Proof.* Define

$$P = \left\{ n \in \mathbb{N} \;\middle|\; n^2 > (2 \cdot n) + 1 \right\}.$$

(BASE CASE) $P$ contains 3.

(INDUCTION STEP) For all natural numbers $n$ such that $n \geq 3$ we have $n \in P \implies n + 1 \in P$.
Proof. Let $n$ be a natural number. Suppose $n \geq 3$. Assume $n \in P$.

$(n^2 + (2 \cdot n)) + 1 > (((2 \cdot n) + 1) + (2 \cdot n)) + 1$. Indeed $n^2 + (2 \cdot n) > ((2 \cdot n) + 1) + (2 \cdot n)$.

$(2 \cdot (n + n)) + 1 > (2 \cdot (n + 1)) + 1$. Indeed $2 \cdot (n + n) > 2 \cdot (n + 1)$. Indeed $n + n > n + 1$ and $2 \neq 0$.

Hence

$$\begin{aligned} & (n+1)^2 \\ & = (n^2 + (2 \cdot n)) + 1 \\ & > (((2 \cdot n) + 1) + (2 \cdot n)) + 1 \\ & > ((2 \cdot n) + (2 \cdot n)) + 1 \\ & = (2 \cdot (n + n)) + 1 \\ & > (2 \cdot (n + 1)) + 1. \end{aligned}$$

Thus $(n + 1)^2 > (2 \cdot (n + 1)) + 1$ (by 6.10). Qed.

Therefore $P$ contains every natural number $n$ such that $n \geq 3$ (by 10.5). □

**Proposition 11.3.** For all $n$ if $n \geq 5$ then

$$2^n > n^2.$$

*Proof.* Define

$$P = \left\{ n \in \mathbb{N} \;\middle|\; 2^n > n^2 \right\}.$$

(BASE CASE) $P$ contains 5. Indeed $2^5 = 2 \cdot (2 \cdot (2 \cdot (2 \cdot 2))) = (5 \cdot 5) + 7 > 5 \cdot 5 = 5^2$. Indeed $((5 \cdot 5) + 7) > 5 \cdot 5$.

(INDUCTION STEP) For all natural numbers $n$ such that $n \geq 5$ we have $n \in P \implies n + 1 \in P$.
Proof. Let $n$ be a natural number. Suppose $n \geq 5$. Assume $n \in P$. Then $2^n > n^2$.

(1) $2^n \cdot 2 > n^2 \cdot 2$ (by 8.1). Indeed $2 \neq 0$.

(2) $n^2 \cdot 2 = n^2 + n^2$.

(3) $n^2 + n^2 > n^2 + ((2 \cdot n) + 1)$ (by 7.2). Indeed $n^2 > (2 \cdot n) + 1$.

(4) $n^2 + ((2 \cdot n) + 1) = (n + 1)^2$.

Hence

$$\begin{aligned} & 2^{n+1} \\ & = 2^n \cdot 2 \\ & > n^2 \cdot 2 \\ & = n^2 + n^2 \end{aligned}$$

$$> n^2 + ((2 \cdot n) + 1)$$
$$= (n+1)^2.$$

Thus $2^{n+1} > (n+1)^2$. Qed.

Therefore $P$ contains every natural number $n$ such that $n \geq 5$ (by 10.5). □

**Proposition 11.4.** For all $n$ if $n \geq 2$ then

$$n^n > n!.$$

*Proof.* Define

$$P = \{\, n \in \mathbb{N} \mid n^n > n! \,\}.$$

(BASE CASE) $P$ contains 2.

(INDUCTION STEP) For all natural numbers $n$ such that $n \geq 2$ we have $n \in P \implies n+1 \in P$.
Proof. Let $n$ be a natural number. Suppose $n \geq 2$. Assume $n \in P$.

(1) $(n+1)^n \cdot (n+1) > n^n \cdot (n+1)$.
Proof. We have $n+1 > n$ and $n \neq 0$. Thus $(n+1)^n > n^n$ (by 9.1). $n+1$ is nonzero. Hence the thesis (by 8.1). Qed.

(2) $n^n \cdot (n+1) > n! \cdot (n+1)$ (by 8.1). Indeed $n^n > n!$ and $n+1 \neq 0$.

Hence

$$(n+1)^{n+1}$$
$$= (n+1)^n \cdot (n+1)$$
$$> n^n \cdot (n+1)$$
$$> n! \cdot (n+1)$$
$$= (n+1)!.$$

Thus $(n+1)^{n+1} > (n+1)!$. Qed.

Therefore $P$ contains every natural number $n$ such that $n \geq 2$ (by 10.5). □

**Proposition 11.5.** For all $n$ if $n \geq 4$ then

$$n! > 2^n.$$

*Proof.* Define

$$P = \{\, n \in \mathbb{N} \mid n! > 2^n \,\}.$$

(BASE CASE) $P$ contains 4.
Proof.

(4!)

$$
\begin{aligned}
&= 4 \cdot (3 \cdot 2) \\
&= 2 \cdot (2 \cdot (3 \cdot 2)) \\
&= 3 \cdot (2 \cdot (2 \cdot 2)) \\
&> 2 \cdot (2 \cdot (2 \cdot 2)) \\
&= 2^4.
\end{aligned}
$$

Qed.

(INDUCTION STEP) For all natural numbers $n$ such that $n \geq 4$ we have $n \in P \implies n+1 \in P$.
Proof. Let $n$ be a natural number. Suppose $n \geq 4$. Assume $n \in P$. Then $n! > 2^n$.

(1) $0 \neq n+1 > 2$. Indeed $n > 1$.

(2) $n! \cdot (n+1) > 2^n \cdot (n+1)$ (by 8.1).

(3) $2^n \cdot (n+1) > 2^n \cdot 2$ (by 8.2). Indeed $2^n \neq 0$.

Hence

$$
\begin{aligned}
&((n+1)!) \\
&= n! \cdot (n+1) \\
&> 2^n \cdot (n+1) \\
&> 2^n \cdot 2 \\
&= 2^{n+1}.
\end{aligned}
$$

Thus $(n+1)! > 2^{n+1}$. Qed.

Therefore $P$ contains every natural number $n$ such that $n \geq 4$ (by 10.5). □

# 12 Subtraction

[readtex `arithmetic/sections/01_arithmetic/03_multiplication.ftl.tex`]

[readtex `arithmetic/sections/02_ordering/01_ordering.ftl.tex`]

Let $k, l, m, n$ denote natural numbers.

The notion of an ordering on the natural numbers enables us to (partially) define an inverse operation of addition, namely the subtraction operation.

**Definition 12.1.** Let $n \geq m$. $n - m$ is the natural number $k$ such that $n = m + k$.

Let the difference of $n$ and $m$ stand for $n - m$.

As we did for the previously introduced operations let us prove some basic facts about subtraction.

**Proposition 12.2.** Let $n \geq m$. Then $n - m = 0$ iff $n = m$.

*Proof.* Case $n - m = 0$. Then $n = (n - m) + m = 0 + m = m$. End.

Case $n = m$. We have $(n - m) + m = n = m = 0 + m$. Hence $n - m = 0$. End. □

**Corollary 12.3.** $n - n = 0$.

**Proposition 12.4.** $n - 0 = n$.

*Proof.* We have $n = (n - 0) + 0 = n - 0$. □

**Proposition 12.5.** Let $n \geq m$. Then $n - m \leq n$.

*Proof.* We have $(n - m) + m = n$. Hence $n - m \leq n$. □

**Proposition 12.6.** Let $n$ be nonzero. $n - 1$ is the direct predecessor of $n$.

*Proof.* We have $(n-1)+1 = n = \text{pred}(n)+1$. Hence $n-1 = \text{pred}(n)$. □

**Proposition 12.7.** Let $n > m$. Assume $m \neq 0$. Then $n - m < n$.

*Proof.* We have $(n - m) + m = n$. Assume $n - m = n$. Then $n + m = (n - m) + m = n = n + 0$. Hence $m = 0$. Contradiction. □

**Proposition 12.8.** Assume $n \geq m$. Then

$$(n - m) + k = (n + k) - m.$$

*Proof.* Assume $n \geq m$. We have

$$\begin{aligned} &((n - m) + k) + m \\ &= ((n - m) + m) + k \\ &= n + k \\ &= ((n + k) - m) + m. \end{aligned}$$

Hence $(n - m) + k = (n + k) - m$. □

**Proposition 12.9.** Assume $n \geq m + k$. Then

$$(n - m) - k = n - (m + k).$$

*Proof.* We have

$$\begin{aligned}
&((n-m)-k)+(m+k)\\
&=(((n-m)-k)+k)+m\\
&=(n-m)+m\\
&=n\\
&=(n-(m+k))+(m+k).
\end{aligned}$$

Hence $(n-m)-k=n-(m+k)$. □

**Proposition 12.10.** Let $n \geq m$. Then

$$(n-m)\cdot k=(n\cdot k)-(m\cdot k).$$

*Proof.* We have

$$\begin{aligned}
&((n-m)\cdot k)+(m\cdot k)\\
&=((n-m)+m)\cdot k\\
&=n\cdot k\\
&=((n\cdot k)-(m\cdot k))+(m\cdot k).
\end{aligned}$$

Hence $(n-m)\cdot k=(n\cdot k)-(m\cdot k)$. □

# Part III
# Divisibility

## 13 Divisibility

[readtex `arithmetic/sections/01_arithmetic/03_multiplication.ftl.tex`]

[readtex `arithmetic/sections/02_ordering/03_ordering-and-multiplication.ftl.tex`]

[readtex `arithmetic/sections/02_ordering/04_ordering-and-exponentiation.ftl.tex`]

Let $k, l, m, n$ denote natural numbers.

### 13.1 Definitions

Just as the standard ordering on the natural numbers determines whether for any two natural numbere $n$ and $m$ there exists a natural number $k$ that we can add to $n$ to reach $m$, we now do the same with multiplication instead of addition. This leads us to the notion of *divisibility*.

**Definition 13.1.** $n$ divides $m$ iff there exists a natural number $k$ such that $n \cdot k = m$.

Let $n \mid m$ stand for $n$ divides $m$. Let $m$ is divisible by $n$ stand for $n$ divides $m$. Let $n \nmid m$ stand for $n$ does not divide $m$.

**Definition 13.2.** A factor of $n$ is a natural number that divides $n$.

Let a divisor of $n$ stand for a factor of $n$.

**Definition 13.3.** $n$ is even iff $n$ is divisible by 2.

**Definition 13.4.** $n$ is odd iff $n$ is not divisible by 2.

### 13.2 Basic properties

As we always did when introducing a new operation or relation, let us now prove some basic properties of divisibility.

**Proposition 13.5.** Every natural number divides 0.

*Proof.* Let $n$ be a natural number. We have $n \cdot 0 = 0$. Hence $n \mid 0$. □

**Proposition 13.6.** Every natural number that is divisible by 0 is equal to 0.

*Proof.* Let $n$ be a natural number. Assume $0 \mid n$. Take a natural number $k$ such that $0 \cdot k = n$. Then we have $n = 0$. □

**Proposition 13.7.** 1 divides every natural number.

*Proof.* Let $n$ be a natural number. We have $1 \cdot n = n$. Hence $1 \mid n$. □

**Proposition 13.8.** Every natural number $n$ divides $n$.

*Proof.* Let $n$ be a natural number. We have $n \cdot 1 = n$. Hence $n \mid n$. □

**Proposition 13.9.** Every natural number that divides 1 is equal to 1.

*Proof.* Let $n$ be a natural number. Assume $n \mid 1$. Take a natural number $k$ such that $n \cdot k = 1$. Suppose $n \neq 1$. Then $n < 1$ or $n > 1$.

Case $n < 1$. Then $n = 0$. Hence $0 = 0 \cdot k = n \cdot k = 1$. Contradiction. End.

Case $n > 1$. We have $k \neq 0$. Indeed if $k = 0$ then $1 = n \cdot k = n \cdot 0 = 0$. Hence $k \geq 1$. Take a positive natural number $l$ such that $n = 1 + l$. Then $1 < 1 + l = n = n \cdot 1 \leq n \cdot k$. Hence $1 < n$. Contradiction. End. □

**Proposition 13.10.** We have

$$(n \mid m \text{ and } m \mid k) \implies n \mid k.$$

*Proof.* Assume $n \mid m$ and $m \mid k$. Take natural numbers $l, l'$ such that $n \cdot l = m$ and $m \cdot l' = k$. Then $n \cdot (l \cdot l') = (n \cdot l) \cdot l' = m \cdot l' = k$. Hence $n \mid k$. □

**Proposition 13.11.** Let $n$ be nonzero. Assume $n \mid m$ and $m \mid n$. Then $n = m$.

*Proof.* Take natural numbers $k, k'$ such that $n \cdot k = m$ and $m \cdot k' = n$. Then $n = m \cdot k' = (n \cdot k) \cdot k' = n \cdot (k \cdot k')$. Hence $k \cdot k' = 1$. Thus $k = 1 = k'$. Therefore $n = m$. □

**Proposition 13.12.** We have

$$n \mid m \implies k \cdot n \mid k \cdot m.$$

*Proof.* Assume $n \mid m$. Take a natural number $l$ such that $n \cdot l = m$. Then $(k \cdot n) \cdot l = k \cdot (n \cdot l) = k \cdot m$. Hence $k \cdot n \mid k \cdot m$. □

**Proposition 13.13.** Assume $k \neq 0$. Then

$$k \cdot n \mid k \cdot m \implies n \mid m.$$

*Proof.* Assume $k{\cdot}n \mid k{\cdot}m$. Take a natural number $l$ such that $(k{\cdot}n){\cdot}l = k{\cdot}m$. Then $k \cdot (n \cdot l) = k \cdot m$. Hence $n \cdot l = m$. Thus $n \mid m$. □

**Proposition 13.14.** If $k \mid n$ and $k \mid m$ then $k \mid (n' \cdot n) + (m' \cdot m)$ for all natural numbers $n', m'$.

*Proof.* Assume $k \mid n$ and $k \mid m$. Let $n', m'$ be natural numbers. Take natural numbers $l, l'$ such that $k \cdot l = n$ and $k \cdot l' = m$. Then

$$\begin{aligned} & k \cdot ((n' \cdot l) + (m' \cdot l')) \\ = {} & (k \cdot (n' \cdot l)) + (k \cdot (m' \cdot l')) \\ = {} & ((k \cdot n') \cdot l) + ((k \cdot m') \cdot l') \\ = {} & (n' \cdot (k \cdot l)) + (m' \cdot (k \cdot l')) \\ = {} & (n' \cdot n) + (m' \cdot m). \end{aligned}$$

□

**Corollary 13.15.** We have

$$(k \mid n \text{ and } k \mid m) \implies k \mid n + m.$$

*Proof.* Assume $k \mid n$ and $k \mid m$. Take $n' = 1$ and $m' = 1$. Then $k \mid (n'{\cdot}n){+}(m'{\cdot}m)$ (by 13.14). $(n'{\cdot}n){+}(m'{\cdot}m) = n{+}m$. Hence $k \mid n{+}m$. □

**Proposition 13.16.** Assume $k \mid n$ and $k \mid n + m$. Then $k \mid m$.

*Proof.* Case $k = 0$. Obvious.

Case $k \neq 0$. Take a natural number $l$ such that $n = k \cdot l$. Take a natural number $l'$ such that $n + m = k \cdot l'$. Then $(k \cdot l) + m = k \cdot l'$. We have $l' \geq l$. Indeed if $l' < l$ then $n + m = k \cdot l' < k \cdot l = n$. Hence we can take a natural number $l''$ such that $l' = l + l''$. Then $(k \cdot l) + m = k \cdot l' = k \cdot (l + l'') = (k \cdot l) + (k \cdot l'')$ (by 3.4). Thus $m = (k \cdot l'')$. Therefore $k \mid m$. End. □

**Proposition 13.17.** Let $n, m$ be nonzero. If $m \mid n$ then $m \leq n$.

*Proof.* Assume $m \mid n$. Take a natural number $k$ such that $m \cdot k = n$. If $k = 0$ then $n = m \cdot k = m \cdot 0 = 0$. Thus $k \geq 1$. Assume $m > n$. Then $n = m \cdot k \geq m \cdot 1 = m > n$. Hence $n > n$. Contradiction. □

**Proposition 13.18.** Let $n, m$ be nonzero and $k > 1$. Then $k^n \mid k^m$ iff $n \leq m$.

*Proof.* Case $k^n \mid k^m$. Assume $n > m$. Take a nonzero natural number $l$ such that $n = m + l$. Then $k^n = k^{m+l} = k^m \cdot k^l$. Hence $k^m \mid k^n$. Thus $k^m = k^n$. Therefore $m = n$ (by 9.5). Contradiction. End.

Case $n \leq m$. Take a natural number $l$ such that $m = n + l$. Then $k^m = k^{n+l} = k^n \cdot k^l$. Hence $k^n \mid k^m$. End. □

# 14 Euclidean division

[readtex `arithmetic/sections/02_ordering/03_ordering-and-multiplication.ftl.tex`]

Let $k, l, m, n$ denote natural numbers.

In this section we will show that for any two natural numbers $n$ and $m$ there exists a unique decomposition $n = m \cdot q + r$ for certain numbers $q$ and $r$ with $r < m$. This is known as *Euclidean division* or *division with remainder*.

**Proposition 14.1.** For all natural numbers $n, m$ such that $m$ is nonzero there exist natural numbers $q, r$ such that

$$n = (m \cdot q) + r$$

and $r < m$.

*Proof.* (1) Define

$$P = \left\{ n \in \mathbb{N} \;\middle|\; \begin{array}{l} \text{for all nonzero natural numbers } m \text{ there exist natural} \\ \text{numbers } q, r \text{ such that } r < m \text{ and } n = (m \cdot q) + r \end{array} \right\}.$$

(BASE CASE) $P$ contains 0. Proof. Take $q = 0$ and $r = 0$. Then for all nonzero natural numbers $m$ we have $r < m$ and $0 = (m \cdot q) + r$. Hence $0 \in P$. Qed.

(INDUCTION STEP) For all natural numbers $n$: $n \in P \implies n + 1 \in P$. Proof. Let $n$ be a natural number. Assume $n \in P$.

Let us show that for all nonzero natural numbers $m$ there exist natural numbers $q, r$ such that $r < m$ and $n + 1 = (m \cdot q) + r$. Let $m$ be a nonzero natural number. Take natural numbers $q', r'$ such that $r' < m$ and $n = (m \cdot q') + r'$ (by 1). Indeed $n \in P$. We have $r' + 1 < m$ or $r' + 1 = m$.

Case $r' + 1 < m$. Take natural numbers $q, r$ such that $q = q'$ and $r = r' + 1$. Then $r < m$ and $n + 1 = ((q' \cdot m) + r') + 1 = (q' \cdot m) + (r' + 1) = (q \cdot m) + r$. End.

Case $r' + 1 = m$. Take natural numbers $q, r$ such that $q = q' + 1$ and $r = 0$. Then $r < m$ and $n + 1 = ((q' \cdot m) + r') + 1 = (q' \cdot m) + (r' + 1) = (q' \cdot m) + m = (q' + 1) \cdot m = (q \cdot m) + r$. End. End.

Hence the thesis (by 1). Qed.

Then $P$ contains every natural number. Let $n, m$ be a natural numbers such that $m$ is nonzero. Then $n \in P$. Hence we can take natural numbers $q, r$ such that $r < m$ and $n = (m \cdot q) + r$ (by 1). Then we have the thesis. □

**Proposition 14.2.** Let $m$ be nonzero. Let $q, q', r, r'$ be natural numbers such that $(m \cdot q) + r = n = (m \cdot q') + r'$ and $r, r' < m$. Then $q = q'$ and $r = r'$.

*Proof.* We have $(m \cdot q) + r = (m \cdot q') + r'$.

Case $q \geq q'$ and $r \geq r'$. Take natural numbers $q'', r''$ such that $q = q' + q''$ and $r = r' + r''$. Then $(m \cdot (q' + q'')) + (r' + r'') = (m \cdot q') + r'$. We have $(m \cdot (q' + q'')) + (r' + r'') = (m \cdot (q' + q'')) + (r'' + r') = ((m \cdot (q' + q'')) + r'') + r'$. Hence $((m \cdot (q' + q'')) + r'') + r' = (m \cdot q') + r'$. Thus $(m \cdot (q' + q'')) + r'' = m \cdot q'$. We have $m \cdot (q' + q'') = (m \cdot q') + (m \cdot q'')$. Hence $((m \cdot q') + (m \cdot q'')) + r'' = (m \cdot q') + ((m \cdot q'') + r'') = m \cdot q'$. Thus $(m \cdot q'') + r'' = 0$. Therefore $r'' = 0$ and $m \cdot q'' = 0$. Consequently $q'' = 0$. Indeed $m \neq 0$. Then we have $q = q' + 0 = q'$ and $r = r' + 0 = r'$. End.

Case $q \geq q'$ and $r < r'$. Take a natural number $q''$ such that $q = q' + q''$. Take a nonzero natural number $r''$ such that $r' = r + r''$. Then $(m \cdot (q' + q'')) + r = (m \cdot q') + (r + r'')$. We have $(m \cdot q') + (r + r'') = (m \cdot q') + (r'' + r) = ((m \cdot q') + r'') + r$. Hence $(m \cdot (q' + q'')) + r = ((m \cdot q') + r'') + r$. Thus $m \cdot (q' + q'') = (m \cdot q') + r''$. We have $m \cdot (q' + q'') = (m \cdot q') + (m \cdot q'')$. Hence $(m \cdot q') + (m \cdot q'') = (m \cdot q') + r''$. Thus $m \cdot q'' = r'' < r' < m$. Therefore $q'' = 0$. Indeed if $q'' \geq 1$ then $m \cdot q'' \geq m$. Consequently $q = q' + 0 = q'$. Hence we have $(m \cdot q) + r = (m \cdot q) + r'$. Thus $r = r'$. End.

Case $q < q'$ and $r \geq r'$. Take a nonzero natural number $q''$ such that $q' = q + q''$. Take a natural number $r''$ such that $r = r' + r''$. Then $(m \cdot q) + (r' + r'') = (m \cdot (q + q'')) + r'$. We have $(m \cdot q) + (r' + r'') = (m \cdot q) + (r'' + r') = ((m \cdot q) + r'') + r'$. Hence $((m \cdot q) + r'') + r' = (m \cdot (q + q'')) + r'$. Thus $(m \cdot q) + r'' = m \cdot (q + q'')$. We have $m \cdot (q + q'') = (m \cdot q) + (m \cdot q'')$. Hence $(m \cdot q) + r'' = (m \cdot q) + (m \cdot q'')$. Thus $m > r > r'' = m \cdot q''$. Indeed $r'$ is nonzero. Therefore $q'' = 0$. Indeed if $q'' \geq 1$ then $m \cdot q'' \geq m$. Consequently $q' = q + 0 = q$. Hence we have $(m \cdot q) + r = (m \cdot q) + r'$. Thus $r = r'$. End.

Case $q < q'$ and $r < r'$. Take nonzero natural numbers $q'', r''$ such that $q' = q + q''$ and $r' = r + r''$. Then $(m \cdot (q + q'')) + (r + r'') = (m \cdot q) + r$. We have $(m \cdot (q + q'')) + (r + r'') = (m \cdot (q + q'')) + (r'' + r) = ((m \cdot (q + q'')) + r'') + r$. Hence $((m \cdot (q + q'')) + r'') + r = (m \cdot q) + r$. Thus $(m \cdot (q + q'')) + r'' = m \cdot q$. We have $m \cdot (q + q'') = (m \cdot q) + (m \cdot q'')$. Hence $((m \cdot q) + (m \cdot q'')) + r'' = (m \cdot q) + ((m \cdot q'') + r'') = m \cdot q$. Thus $(m \cdot q'') + r'' = 0$. Therefore $r'' = 0$ and $m \cdot q'' = 0$. Consequently $q'' = 0$. Indeed $m \neq 0$. Then we have $q' = q + 0 = q$ and $r' = r + 0 = r$. End. □

**Definition 14.3.** Let $m$ be nonzero. $n \bmod m$ is the natural number $r$ such that $r < m$ and there exists a natural number $q$ such that $n = (m \cdot q) + r$.

Let the remainder of $n$ over $m$ stand for $n \bmod m$.

**Definition 14.4.** Let $m$ be nonzero. $n \operatorname{div} m$ is the natural number $q$ such

that $n = (m \cdot q) + r$ for some natural number $r$ that is less than $m$.

Let the quotient of $n$ over $m$ stand for $n \operatorname{div} m$.

# 15 Modular arithmetic

[readtex `arithmetic/sections/03_divisibility/02_euclidean-division.ftl.tex`]

Let $k, k', l, m, n, n', n''$ denote natural numbers.

Having seen Euclidean division we now can establish a new kind of arithmetic, called *modular arithmetic*. To do this we fix a natural number $k$ and identify any two natural numbers if they have the same remainder when divided by $k$.

**Definition 15.1.** Let $k$ be nonzero. $n \equiv m \pmod{k}$ iff $n \bmod k = m \bmod k$.

Let $n$ and $m$ are congruent modulo $k$ stand for $n \equiv m \pmod{k}$.

**Proposition 15.2.** Let $m$ be nonzero. Then

$$n \equiv n \pmod{m}.$$

*Proof.* We have $n \bmod m = n \bmod m$. $n \equiv n \pmod{m}$. □

**Proposition 15.3.** Let $m$ be nonzero. Then

$$n \equiv n' \pmod{m} \implies n' \equiv n \pmod{m}.$$

*Proof.* Assume $n \equiv n' \pmod{m}$. Then $n \bmod m = n' \bmod m$. Hence $n' \bmod m = n \bmod m$. Thus $n' \equiv n \pmod{m}$. □

**Proposition 15.4.** Let $m$ be nonzero. Then

$$(n \equiv n' \pmod{m} \text{ and } n' \equiv n'' \pmod{m}) \implies n \equiv n'' \pmod{m}.$$

*Proof.* Assume $n \equiv n' \pmod{m}$ and $n' \equiv n'' \pmod{m}$. Then $n \bmod m = n' \bmod m$ and $n' \bmod m = n'' \bmod m$. Hence $n \bmod m = n'' \bmod m$. Thus $n \equiv n'' \pmod{m}$. □

**Proposition 15.5.** Let $k$ be nonzero. Assume $n \geq m$. Then $n \equiv m \pmod{k}$ iff $n = (k \cdot x) + m$ for some natural number $x$.

*Proof.* Case $n \equiv m \pmod{k}$. Then $n \bmod k = m \bmod k$. Take a natural number $r$ such that $r < k$ and $n \bmod k = r = m \bmod k$. Take a nonzero natural number $l$ such that $k = r + l$. Consider natural numbers $q, q'$ such that $n = (q \cdot k) + r$ and $m = (q' \cdot k) + r$.

Then $q \geq q'$.
Proof. Assume the contrary. Then $q < q'$. Hence $q \cdot k < q' \cdot k$. Thus $(q \cdot k) + r < (q' \cdot k) + r$. Therefore $n < m$. Contradiction. Qed.

Take a natural number $x$ such that $q = q' + x$.

Let us show that $n = (k \cdot x) + m$. We have

$$\begin{aligned}
&(k \cdot x) + m \\
&= (k \cdot x) + ((q' \cdot k) + r) \\
&= ((k \cdot x) + (q' \cdot k)) + r \\
&= ((k \cdot x) + (k \cdot q')) + r \\
&= (k \cdot (q' + x)) + r \\
&= (k \cdot q) + r \\
&= n.
\end{aligned}$$

End. End.

Case $n = (k \cdot x) + m$ for some natural number $x$. Consider a natural number $x$ such that $n = (k \cdot x) + m$. Take natural numbers $r, r'$ such that $n \bmod k = r$ and $m \bmod k = r'$. Then $r, r' < k$. Take natural numbers $q, q'$ such that $n = (k \cdot q) + r$ and $m = (k \cdot q') + r'$. Then

$$\begin{aligned}
&(k \cdot q) + r \\
&= n \\
&= (k \cdot x) + m \\
&= (k \cdot x) + ((k \cdot q') + r') \\
&= ((k \cdot x) + (k \cdot q')) + r' \\
&= (k \cdot (x + q')) + r'.
\end{aligned}$$

Hence $r = r'$. Thus $n \bmod k = m \bmod k$. Therefore $n \equiv m \pmod{k}$. End. □

**Proposition 15.6.** Let $k, k'$ be nonzero. Then

$$n \equiv m \pmod{k \cdot k'} \implies n \equiv m \pmod{k}.$$

*Proof.* Assume $n \equiv m \pmod{k \cdot k'}$.

Case $n \geq m$. We can take a natural number $x$ such that $n = ((k \cdot k') \cdot x) + m$. Then $n = (k \cdot (k' \cdot x)) + m$. Hence $n \equiv m \pmod{k}$. End.

Case $m \geq n$. We have $m \equiv n \pmod{k \cdot k'}$. Hence we can take a natural number $x$ such that $m = ((k \cdot k') \cdot x) + n$. Then $m = (k \cdot (k' \cdot x)) + n$. Thus $m \equiv n \pmod{k}$. Therefore $n \equiv m \pmod{k}$. End. □

**Corollary 15.7.** Let $k, k'$ be nonzero natural numbers. Then

$$n \equiv m \pmod{k \cdot k'} \implies n \equiv m \pmod{k'}.$$

*Proof.* Assume $n \equiv m \pmod{k \cdot k'}$. Then $n \equiv m \pmod{k' \cdot k}$. Hence $n \equiv m \pmod{k'}$. □

# 16 Primes

[readtex `arithmetic/sections/01_arithmetic/04_exponentiation.ftl.tex`]

[readtex `arithmetic/sections/02_ordering/04_ordering-and-exponentiation.ftl.tex`]

[readtex `arithmetic/sections/02_ordering/05_induction.ftl.tex`]

[readtex `arithmetic/sections/03_divisibility/01_divisibility.ftl.tex`]

[readtex `arithmetic/sections/03_divisibility/02_euclidean-division.ftl.tex`]

Let $k, l, m, n$ denote natural numbers.

## 16.1 Definitions

Let us turn back to the notion of divisibility. We will now investigate natural numbers which cannot be decomposed into a product of two (non-trivial) smaller numbers. Such numbers are called *prime*.

**Definition 16.1.** A trivial divisor of $n$ is a divisor $m$ of $n$ such that $m = 1$ or $m = n$.

**Definition 16.2.** A nontrivial divisor of $n$ is a divisor $m$ of $n$ such that $m \neq 1$ and $m \neq n$.

**Definition 16.3.** $n$ is prime iff $n > 1$ and $n$ has no nontrivial divisors.

Let $n$ is compound stand for $n$ is not prime. Let a prime number stand for a natural number that is prime.

**Definition 16.4.** $n$ is composite iff $n > 1$ and $n$ has a nontrivial divisor.

**Proposition 16.5.** Let $n > 1$. Then $n$ is prime iff every divisor of $n$ is a trivial divisor of $n$.

Let us have a look at what the first few prime numbers are.

**Proposition 16.6.** 2, 3, 5 and 7 are prime.

*Proof.* Let us show that 2 is prime. Let $k$ be a divisor of 2. Then $0 < k \leq 2$. Hence $k = 1$ or $k = 2$. Thus $k$ is a trivial divisor of 2. End.

Let us show that 3 is prime. Let $k$ be a divisor of 3. Then $0 < k \leq 3$. Hence $k = 1$ or $k = 2$ or $k = 3$. 2 does not divide 3. Therefore $k = 1$ or $k = 3$. Thus $k$ is a trivial divisor of 3. End.

Let us show that 5 is prime. Let $k$ be a divisor of 5. Then $0 < k \leq 5$. Hence $k = 1$ or $k = 2$ or $k = 3$ or $k = 4$ or $k = 5$. 2 does not divide 5. 3 does not divide 5. 4 does not divide 5. Therefore $k = 1$ or $k = 5$. Thus $k$ is a trivial divisor of 5. End.

Let us show that 7 is prime. Let $k$ be a divisor of 7. Then $0 < k \leq 7$. Hence $k = 1$ or $k = 2$ or $k = 3$ or $k = 4$ or $k = 5$ or $k = 6$ or $k = 7$. 2 does not divide 7. 3 does not divide 7. 4 does not divide 7. 5 does not divide 7. 6 does not divide 7. Therefore $k = 1$ or $k = 7$. Thus $k$ is a trivial divisor of 7. End. □

**Proposition 16.7.** 4, 6, 8 and 9 are compound.

*Proof.* $4 = 2 \cdot 2$. Hence 2 divides 4. Thus 4 is compound.

$6 = 2 \cdot 3$. Hence 2 divides 6. Thus 6 is compound.

$8 = 2 \cdot 4$. Hence 2 divides 8. Thus 8 is compound.

$9 = 3 \cdot 3$. Hence 3 divides 9. Thus 9 is compound. □

**Proposition 16.8.** Let $p$ be a prime number. If $p$ is even then $p = 2$.

*Proof.* Assume that $p$ is even. Then 2 divides $p$. Hence 2 is a trivial divisor of $p$. Thus $p = 2$. □

An important fact about primes is that every natural number has a prime divisor. From this the *fundamental theorem of arithmetic* can be derived, namely the assertion that every natural number has a unique decomposition into prime factors.

**Proposition 16.9.** Every natural number that is greater than 1 has a prime divisor.

*Proof.* Define

$$P = \{\, n \in \mathbb{N} \mid \text{if } n > 1 \text{ then } n \text{ has a prime divisor} \,\}.$$

Let us show that (1) for every natural number $n$ if $P$ contains all predecessors of $n$ then $P$ contains $n$. Let $n$ be a natural number. Assume that $P$ contains all predecessors of $n$. $n = 0$ or $n = 1$ or $n$ is prime or $n$ is composite.

Case $n = 0$ or $n = 1$. Trivial.

Case $n$ is prime. Obvious.

Case $n$ is composite. Take a nontrivial divisor $m$ of $n$. Then $1 < m < n$. $m$ is contained in $P$. Hence we can take a prime divisor $p$ of $m$. Then we have $p \mid m \mid n$. Thus $p \mid n$. Therefore $p$ is a prime divisor of $n$. End. End.

Thus every natural number belongs to $P$ (by 10.4, 1). □

**Proposition 16.10.** Let $n$ be composite. Then $n$ has a nontrivial divisor $m$ such that $m^2 \leq n$.

*Proof.* Define

$$A = \{\, m \in \mathbb{N} \mid m \text{ is a nontrivial divisor of } n \,\}.$$

$A$ contains some natural number. Hence we can take a least natural number $m$ of $A$. Consider a natural number $k$ such that $m \cdot k = n$. Then $m \leq k$. Indeed if $k < m$ then $k$ is the least natural number of $A$. Hence $m^2 = m \cdot m \leq m \cdot k = n$. Therefore $m^2 \leq n$. □

Let us now have a look at natural numbers which have no (non-trivial) common divisor. Such numbers are called *coprime*.

**Definition 16.11.** $n$ and $m$ are coprime iff for all nonzero natural numbers $k$ such that $k \mid n$ and $k \mid m$ we have $k = 1$.

Let $n$ and $m$ are relatively prime stand for $n$ and $m$ are coprime. Let $n$ and $m$ are mutually prime stand for $n$ and $m$ are coprime. Let $n$ is prime to $m$ stand for $n$ and $m$ are coprime.

**Proposition 16.12.** $n$ and $m$ are coprime iff for no prime number $p$ we have $p \mid n$ and $p \mid m$.

*Proof.* Case $n$ and $m$ are coprime. Let $p$ be a prime number such that $p \mid n$ and $p \mid m$. Then $p$ is nonzero and $p \neq 1$. Contradiction. End.

Case for no prime number $p$ we have $p \mid n$ and $p \mid m$. Let $k$ be a nonzero natural number such that $k \mid n$ and $k \mid m$. Assume that $k \neq 1$. Consider a prime divisor $p$ of $k$. Then $p \mid k \mid n, m$. Hence $p \mid n$ and $p \mid m$. Contradiction. End. □

**Proposition 16.13.** Let $p$ be a prime number. If $p$ does not divide $n$ then $p$ and $n$ are coprime.

*Proof.* Assume $p \nmid n$. Suppose that $p$ and $n$ are not coprime. Take a nonzero natural number $k$ such that $k \mid p$ and $k \mid n$. Then $k = p$. Hence $p \mid n$. Contradiction. □

**Proposition 16.14.** Let $p$ be a prime number. Then

$$p \mid n \cdot m \implies (p \mid n \text{ or } p \mid m).$$

*Proof.* Assume $p \mid n \cdot m$.

Case $p \mid n$. Trivial.

Case $p \nmid n$. Define

$$N = \{\, x \in \mathbb{N} \mid x \neq 0 \text{ and } p \mid x \cdot m \,\}.$$

We have $p \in N$ and $n \in N$. Hence $N$ contains some natural number. Thus we can take a least natural number $n'$ of $N$.

Let us show that $n'$ divides all elements of $N$. Let $x \in N$. Take natural numbers $q, r$ such that $x = (n' \cdot q) + r$ and $r < n'$ (by 14.1). Indeed $n'$ is nonzero. Then $x \cdot m = ((q \cdot n') + r) \cdot m = ((q \cdot n') \cdot m) + (r \cdot m)$. We have $p \mid x \cdot m$. Hence $p \mid ((q \cdot n') \cdot m) + (r \cdot m)$. Thus $p \mid r \cdot m$ (by 13.16). Indeed $p \mid ((q \cdot n') \cdot m) = (q \cdot (n' \cdot m))$. Indeed $p \mid n' \cdot m$. Therefore $r = 0$. Indeed if $r \neq 0$ then $r$ is an element of $N$ that is less than $n'$. Hence $x = q \cdot n'$. Thus $n'$ divides $x$. End.

Then we have $n' \mid p$ and $n' \mid n$. Hence $n' = p$ or $n' = 1$. Thus $n' = 1$. Indeed if $n' = p$ then $p \mid n$. Then $1 \in N$. Therefore $p \mid 1 \cdot m = m$. End. □

**Proposition 16.15.** Let $k$ be nonzero. Then for all nonzero $n, m$ if $k \cdot m^2 = n^2$ then $k$ is compound.

*Proof.* Case $k = 1$. Obvious.

Case $k > 1$. (1) Define

$$P = \left\{ n \in \mathbb{N} \;\middle|\; \begin{array}{l} \text{for all natural numbers } m \text{ if } n \text{ and } m \text{ are nonzero and} \\ k \cdot m^2 = n^2 \text{ then } k \text{ is compound} \end{array} \right\}.$$

Let us show that for all natural numbers $n$ if $P$ contains all predecessors of $n$ then $P$ contains $n$. Let $n$ be a natural number. Presume that $P$ contains all predecessors of $n$.

Let $m$ be a natural number. Assume that $n$ and $m$ are nonzero and $k \cdot m^2 = n^2$.

Suppose that $k$ is prime. $k$ is a nontrivial divisor of $n^2$. Hence $k$ divides $n$. Take a natural number $l$ such that $k \cdot l = n$.

(2) Then $m^2 = k \cdot l^2$ (by 3.12). Indeed $k \cdot m^2 = (k \cdot l)^2 = k \cdot (k \cdot l^2)$.

(3) $m$ is an element of $P$.
Proof. We have $n^2 > m^2$ (by 8.8). Indeed $k \cdot m^2 = n^2$ and $k > 1$ and $m^2 > 0$. Hence $m < n$. Indeed if $n \leq m$ then $n^2 \leq m^2$. Thus $m \in P$. Qed.

(4) $m$ is nonzero. Indeed $m = 0 \implies n^2 = k \cdot 0^2 = k \cdot 0 = 0$ and $n^2 = 0 \implies n = 0$.

(5) $l$ is nonzero. Indeed $l = 0 \implies m^2 = k \cdot 0^2 = k \cdot 0 = 0$ and $m^2 = 0 \implies m = 0$.

Therefore $k$ is compound (by 2, 3, 4, 5). Contradiction. End.

Thus $P$ contains every natural number (by 10.4). Hence the thesis (by 1). End. □