Chapter 1

Exponentiation

File: `arithmetic/sections/13_exponentiation.ftl.tex`

[readtex `arithmetic/sections/06_multiplication.ftl.tex`]

1.1 Definition of exponentiation

ARITHMETIC_13_2103235571613696

Lemma 1.1. There exists a $\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that for all $n \in \mathbb{N}$ we have $\varphi(n, 0) = 1$ and $\varphi(n, m + 1) = \varphi(n, m) \cdot n$ for any $m \in \mathbb{N}$.

Proof. Take $A = [\mathbb{N} \to \mathbb{N}]$. Define $a(n) = 1$ for $n \in \mathbb{N}$. Then A is a set and $a \in A$.

[skipfail on] Define $f(g) = \lambda n \in \mathbb{N}.g(n) \cdot n$ for $g \in A$. [skipfail off]

Then $f : A \to A$. Indeed $f(g)$ is a map from $\mathbb{N}$ to $\mathbb{N}$ for any $g \in A$. Consider a $\psi : \mathbb{N} \to A$ such that ψ is recursively defined by a and f (by **??**). For any objects n, m we have $(n, m) \in \mathbb{N} \times \mathbb{N}$ iff $n, m \in \mathbb{N}$. Define $\varphi(n, m) = \psi(m)(n)$ for $(n, m) \in \mathbb{N} \times \mathbb{N}$. Then φ is a map from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$. Indeed $\varphi(n, m) \in \mathbb{N}$ for all $n, m \in \mathbb{N}$.

(1) For all $n \in \mathbb{N}$ we have $\varphi(n, 0) = 1$.
Proof. Let $n \in \mathbb{N}$. Then $\varphi(n, 0) = \psi(0)(n) = a(0) = 1$. Qed.

(2) For all $n, m \in \mathbb{N}$ we have $\varphi(n, m + 1) = \varphi(n, m) \cdot n$.
Proof. Let $n, m \in \mathbb{N}$. Then $\varphi(n, m+1) = \psi(m+1)(n) = f(\psi(m))(n) = \psi(m)(n) \cdot n = \varphi(n, m) \cdot n$. Qed.

Hence for all $n \in \mathbb{N}$ we have $\varphi(n,0) = 1$ and $\varphi(n,m+1) = \varphi(n,m) \cdot n$ for any $m \in \mathbb{N}$. □

ARITHMETIC_13_2359278746730496

Lemma 1.2. Let $\varphi, \varphi' : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Assume that for all $n \in \mathbb{N}$ we have $\varphi(n,0) = 1$ and $\varphi(n,m+1) = \varphi(n,m) \cdot n$ for any $m \in \mathbb{N}$. Assume that for all $n \in \mathbb{N}$ we have $\varphi'(n,0) = 1$ and $\varphi'(n,m+1) = \varphi'(n,m) \cdot n$ for any $m \in \mathbb{N}$. Then $\varphi = \varphi'$.

Proof. Define $\Phi = \{m \in \mathbb{N} \mid \varphi(n,m) = \varphi'(n,m) \text{ for all } n \in \mathbb{N}\}$.

(1) $0 \in \Phi$. Indeed $\varphi(n,0) = 1 = \varphi'(n,0)$ for all $n \in \mathbb{N}$.

(2) For all $m \in \Phi$ we have $m+1 \in \Phi$.
Proof. Let $m \in \Phi$. Then $\varphi(n,m) = \varphi'(n,m)$ for all $n \in \mathbb{N}$. $\varphi(n,m), \varphi'(n,m)$ are natural numbers for all $n \in \mathbb{N}$. Hence $\varphi(n,m+1) = \varphi(n,m) \cdot n = \varphi'(n,m) \cdot n = \varphi'(n,m+1)$ for all $n \in \mathbb{N}$. Thus $\varphi(n,m+1) = \varphi'(n,m+1)$ for all $n \in \mathbb{N}$. Qed.

Thus Φ contains every natural number. Therefore $\varphi(n,m) = \varphi'(n,m)$ for all $n, m \in \mathbb{N}$. □

ARITHMETIC_13_3663815629602816

Definition 1.3. exp is the map from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ such that for all $n \in \mathbb{N}$ we have $\exp(n,0) = 1$ and $\exp(n,m+1) = \exp(n,m) \cdot n$ for any $m \in \mathbb{N}$.

Let n^m stand for $\exp(n,m)$.

ARITHMETIC_13_5845266294898688

Lemma 1.4. Let n, m be natural numbers. Then $(n,m) \in \mathrm{dom}(\exp)$.

ARITHMETIC_13_4747809204994048

Lemma 1.5. Let n, m be natural numbers. Then n^m is a natural number.

ARITHMETIC_13_5368818025103360

Lemma 1.6. Let n be a natural number. Then $n^0 = 1$.

ARITHMETIC_13_4140498660884480

Lemma 1.7. Let n, m be natural numbers. Then $n^{m+1} = n^m \cdot n$.

1.2 Computation laws

Exponentiation with 0, 1 and 2

ARITHMETIC_13_4673644676513792

Proposition 1.8. Let n be a natural number. Assume $n \neq 0$. Then

$$0^n = 0.$$

Proof. Take a natural number m such that $n = m + 1$. Then $0^n = 0^{m+1} = 0^m \cdot 0 = 0$. □

ARITHMETIC_13_7376849881530368

Proposition 1.9. Let n be a natural number. Then

$$1^n = 1.$$

Proof. Define $\Phi = \{n' \in \mathbb{N} \mid 1^{n'} = 1\}$.

(1) Φ contains 0.

(2) For all $n' \in \Phi$ we have $n' + 1 \in \Phi$.
Proof. Let $n' \in \Phi$. Then $1^{n'+1} = 1^{n'} \cdot 1 = 1 \cdot 1 = 1$. Qed.

Hence every natural number is contained in Φ. Thus $1^n = 1$. □

ARITHMETIC_13_4975279749464064

Proposition 1.10. Let n be a natural number. Then

$$n^1 = n.$$

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

ARITHMETIC_13_8513812055457792

Proposition 1.11. Let n be a natural number. Then

$$n^2 = n \cdot n.$$

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

Sums as exponents

ARITHMETIC_13_8152207530655744

Proposition 1.12. Let n, m, k be natural numbers. Then

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

Proof. Define $\Phi = \{m' \in \mathbb{N} \mid k^{n+m'} = k^n \cdot k^{m'}\}$.

(1) Φ contains 0.
Indeed $k^{n+0} = k^n = k^n \cdot 1 = k^n \cdot k^0$.

(2) For all $m' \in \Phi$ we have $m' + 1 \in \Phi$.
Proof. Let $m' \in \Phi$. Then

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

Qed.

Hence every natural number is contained in Φ. Thus $k^{n+m} = k^n \cdot k^m$. □

Products as exponents

ARITHMETIC_13_7827956571308032

Proposition 1.13. Let n, m, k be natural numbers. Then

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

Proof. Define $\Phi = \{k' \in \mathbb{N} \mid n^{m \cdot k'} = (n^m)^{k'}\}$.

(1) Φ contains 0. Indeed $(n^m)^0 = 1 = n^0 = n^{m \cdot 0}$.

(2) For all $k' \in \Phi$ we have $k' + 1 \in \Phi$.
Proof. Let $k' \in \Phi$. 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.

Therefore every natural number is contained in Φ. Consequently $n^{m \cdot k} = (n^m)^k$. □

Products as base

ARITHMETIC_13_2563032276271104

Proposition 1.14. Let n, m, k be natural numbers. Then

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

Proof. Define $\Phi = \{k' \in \mathbb{N} \mid (n \cdot m)^{k'} = n^{k'} \cdot m^{k'}\}$.

(1) Φ contains 0. Indeed $((n \cdot m)^0) = 1 = 1 \cdot 1 = n^0 \cdot m^0$.

(2) For all $k' \in \Phi$ we have $k' + 1 \in \Phi$.
Proof. Let $k' \in \Phi$.

Let us show that $(n^{k'} \cdot m^{k'}) \cdot (n \cdot m) = (n^{k'} \cdot n) \cdot (m^{k'} \cdot m)$.

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

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

Qed.

Hence

$$(n \cdot m)^{k'+1}$$
$$= (n \cdot m)^{k'} \cdot (n \cdot m)$$
$$= (n^{k'} \cdot m^{k'}) \cdot (n \cdot m)$$
$$= (n^{k'} \cdot n) \cdot (m^{k'} \cdot m)$$
$$= n^{k'+1} \cdot m^{k'+1}.$$

Qed.

Therefore every natural number is contained in Φ. Consequently $(n \cdot m)^k = n^k \cdot m^k$. □

Zeroes of exponentiation

ARITHMETIC_13_3860221447372800

Proposition 1.15. Let n, m be natural numbers. Then

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

Proof. Case $n^m = 0$. Define $\Phi = \{m' \in \mathbb{N} \mid \text{if } n^{m'} = 0 \text{ then } n = 0 \text{ and } m' \neq 0\}$.

(1) Φ contains 0. Indeed if $n^0 = 0$ then we have a contradiction.

(2) For all $m' \in \Phi$ we have $m' + 1 \in \Phi$.
Proof. Let $m' \in \Phi$.

Let us show that if $n^{m'+1} = 0$ then $n = 0$ and $m' + 1 \neq 0$. 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 $n = 0$ and $m' + 1 \neq 0$. End. Qed.

Thus every natural number is contained in Φ. Consequently $m \in \Phi$. Therefore $n = 0$ and $m \neq 0$. End.

Case $n = 0$ and $m \neq 0$. Take a natural number k such that $m = k + 1$. Then $n^m = n^{k+1} = n^k \cdot n = 0^k \cdot 0 = 0$. End. □

1.3 Ordering and exponentiation

ARITHMETIC_13_3373702288769024

Proposition 1.16. Let n, m, k be natural numbers. Assume $k \neq 0$. Then

$$n < m \quad \text{iff} \quad n^k < m^k.$$

Proof. Case $n < m$. Define $\Phi = \{k' \in \mathbb{N} \mid \text{if } k' > 1 \text{ then } n^{k'} < m^{k'}\}$.

(1) Φ contains 0.

(2) Φ contains 1.

(3) Φ contains 2.
Proof. Case $n = 0$ or $m = 0$. Obvious.

Case $n, m \neq 0$. Then $n \cdot n < n \cdot m < m \cdot m$. Hence $n^2 = n \cdot n < n \cdot m < m \cdot m = m^2$. End. Qed.

(4) For all $k' \in \Phi$ we have $k' + 1 \in \Phi$.
Proof. Let $k' \in \Phi$.

Let us show that if $k' + 1 > 1$ then $n^{k'+1} < m^{k'+1}$. Assume $k' + 1 > 1$. 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 $k' + 1 \in \Phi$. 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 $n^{k'} \cdot n < m^{k'} \cdot n < m^{k'} \cdot m$. Indeed $n^{k'} < m^{k'} \neq 0$. Take $A = n^{k'+1}$ and $B = m^{k'+1}$. Then $A = n^{k'+1} = n^{k'} \cdot n < m^{k'} \cdot n < m^{k'} \cdot m = m^{k'+1} = B$. Thus $n^{k'+1} = A < B = m^{k'+1}$. End. End.

Hence $n^{k'+1} < m^{k'+1}$. Indeed $k' \leq 1$ or $k' > 1$. End.

Thus $k' + 1 \in \Phi$. Qed.

Therefore every natural number is contained in Φ. Consequently $n^k < m^k$. End.

Case $n^k < m^k$. Define $\Psi = \{k' \in \mathbb{N} \mid \text{if } n \geq m \text{ then } n^{k'} \geq m^{k'}\}$.

(1) Ψ contains 0.

(2) For all $k' \in \Psi$ we have $k' + 1 \in \Psi$.
Proof. Let $k' \in \Psi$.

Let us show that if $n \geq m$ then $n^{k'+1} \geq m^{k'+1}$. Assume $n \geq m$. Then $n^{k'} \geq m^{k'}$. Hence $n^{k'} \cdot n \geq m^{k'} \cdot n \geq m^{k'} \cdot m$. Take $A = n^{k'+1}$ and $B = m^{k'+1}$. Thus $A = n^{k'+1} = n^{k'} \cdot n \geq m^{k'} \cdot n \geq m^{k'} \cdot m = m^{k'+1} = B$. Therefore $n^{k'+1} = A \geq B = m^{k'+1}$. End.

Hence $k' + 1 \in \Psi$. Qed.

Thus every natural number is contained in Ψ. Therefore if $n \geq m$ then $n^k \geq m^k$. [prover vampire] Consequently $n < m$. End. □

ARITHMETIC_13_2797602550579200

Corollary 1.17. Let n, m, k be natural numbers. Assume $k \neq 0$. Then

$$n^k = m^k \quad \text{implies} \quad n = m.$$

Proof. Assume $n^k = m^k$. Suppose $n \neq m$. Then $n < m$ or $m < n$. If $n < m$ then $n^k < m^k$. If $m < n$ then $m^k < n^k$. Thus $n^k \neq m^k$. Contradiction. □

ARITHMETIC_13_6875081963732992

Corollary 1.18. Let n, m, k be natural numbers. Assume $k \neq 0$. Then

$$n^k \leq m^k \quad \text{iff} \quad n \leq m.$$

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

If $n < m$ then $n^k < m^k$. If $n = m$ then $n^k = m^k$. □

ARITHMETIC_13_3349764703780864

Proposition 1.19. Let n, m, k be natural numbers. Assume $k > 1$. Then

$$n < m \quad \text{iff} \quad k^n < k^m.$$

Proof. Case $n < m$. Define $\Phi = \{m' \in \mathbb{N} \mid \text{if } n < m' \text{ then } k^n < k^{m'}\}$.

(1) Φ contains 0.

(2) For all $m' \in \Phi$ we have $m' + 1 \in \Phi$.
Proof. Let $m' \in \Phi$.

Let us show that if $n < m' + 1$ then $k^n < k^{m'+1}$. Assume $n < m' + 1$. Then $n \leq m'$. We have $k^{m'} \cdot 1 < k^{m'} \cdot k$. Indeed $k^{m'} \neq 0$.

Case $n = m'$. Take $A = k^n$ and $B = k^{m'+1}$. Then $A = k^n = k^{m'} < k^{m'} \cdot k = k^{m'+1} = B$. Hence $k^n = A < B = k^{m'+1}$. End.

Case $n < m'$. Take $A = k^n$ and $B = k^{m'+1}$. Then $A = k^n < k^{m'} < k^{m'} \cdot k = k^{m'+1} = B$. Hence $k^n = A < B = k^{m'+1}$. End. Qed. Qed.

Hence every natural number is contained in Φ. Thus $k^n < k^m$. End.

Case $k^n < k^m$. Define $\Psi = \{n' \in \mathbb{N} \mid \text{if } n' \geq m \text{ then } k^{n'} \geq k^m\}$.

(1) 0 is contained in Ψ.

(2) For all $n' \in \Psi$ we have $n' + 1 \in \Psi$.
Proof. Let $n' \in \Psi$.

Let us show that if $n' + 1 \geq m$ then $k^{n'+1} \geq k^m$. Assume $n' + 1 \geq m$.

Case $n' + 1 = m$. Obvious.

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

Thus every natural number is contained in Ψ. Therefore if $n \geq m$ then $k^n \geq k^m$. [prover vampire] Consequently $n < m$. End. □

ARITHMETIC_13_6780506905509888

Corollary 1.20. Let n, m, k be natural numbers. Assume $k > 1$. Then

$$k^n = k^m \quad \text{implies} \quad n = m.$$

Proof. Assume $k^n = k^m$. Suppose $n \neq m$. Then $n < m$ or $m < n$. If $n < m$ then $k^n < k^m$. If $m < n$ then $k^m < k^n$. Thus $k^n \neq k^m$. Contradiction. □

ARITHMETIC_13_2876620253691904

Corollary 1.21. Let n, m, k be natural numbers. Assume $k > 1$. Then

$$n \leq m \quad \text{iff} \quad k^n \leq k^m.$$

ARITHMETIC_13_6984104377581568

Proposition 1.22. Let n be a natural number. Then

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

Proof. We have

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

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

□

ARITHMETIC_13_134060414337024

Proposition 1.23. Let n be a natural number. Assume $n \geq 3$. Then

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

Proof. Define $\Phi = \{n' \in \mathbb{N}_{\geq 3} \mid n'^2 > (2 \cdot n') + 1\}$.

(1) Φ contains 3.

(2) For all $n' \in \Phi$ we have $n' + 1 \in \Phi$.
Proof. Let $n' \in \Phi$. Then $n' \geq 3$.

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

(b) $(((2 \cdot n') + 1) + (2 \cdot n')) + 1 > ((2 \cdot n') + (2 \cdot n')) + 1$.
Proof. We have $((2 \cdot n') + 1) + (2 \cdot n') > (2 \cdot n') + (2 \cdot n')$. Indeed $(2 \cdot n') + 1 > 2 \cdot n'$. Qed.

(c) $(2 \cdot (n' + n')) + 1 > (2 \cdot (n' + 1)) + 1$.
Proof. We have $n' + n' > n' + 1$ and $2 \neq 0$. Thus $2 \cdot (n' + n') > 2 \cdot (n' + 1)$ (by **??**). Indeed $n' + n'$ and $n' + 1$ are natural numbers. Qed.

Take $A = (n' + 1)^2$ and $B = (2 \cdot (n' + 1)) + 1$. Then

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

Thus $(n' + 1)^2 = A > B = (2 \cdot (n' + 1)) + 1$. Qed.

Therefore Φ contains every element of $\mathbb{N}_{\geq 3}$ (by **??**). Consequently $n^2 > (2 \cdot n) + 1$. □