1 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.

1.1 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 1.1. 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 1.2. A factor of n is a natural number that divides n.

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

Definition 1.3. n is even iff n is divisible by 2.

Definition 1.4. n is odd iff n is not divisible by 2.

1.2 Basic properties

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

Proposition 1.5. Every natural number divides 0.

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

Proposition 1.6. 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 1.7. 1 divides every natural number.

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

Proposition 1.8. Every natural number n divides n.

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

Proposition 1.9. 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 1.10. 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 1.11. 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 1.12. 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 1.13. 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 1.14. 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 1.15. 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 1.14). $(n' \cdot n) + (m' \cdot m) = n + m$. Hence $k \mid n + m$. □

Proposition 1.16. 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 **??**). Thus $m = (k \cdot l'')$. Therefore $k \mid m$. End. □

Proposition 1.17. 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 1.18. 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 **??**). 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. □