Chapter 1

Divisibility

File: `arithmetic/sections/07_divisibility.ftl.tex`

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

ARITHMETIC_07_4239998993825792

Definition 1.1. Let n, m be natural numbers. n divides m iff there exists a natural number k such that $n \cdot k = m$.

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

ARITHMETIC_07_1478855118290944

Lemma 1.2. Let n, m be natural numbers. n divides m iff there exists a natural number k such that $k \cdot n = m$.

ARITHMETIC_07_1311437490225152

Definition 1.3. Let n be a natural number. A factor of n is a natural number that divides n.

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

ARITHMETIC_07_2242720387039232

Proposition 1.4. Let n be a natural number. Then

$$n \mid 0.$$

Proof. We have $n \cdot 0 = 0$. Hence $n \mid 0$. □

ARITHMETIC_07_8611150130315264

Proposition 1.5. Let n be a natural number. Then

$$0 \mid n \quad \text{implies} \quad n = 0.$$

Proof. Assume $0 \mid n$. Consider a natural number k such that $0 \cdot k = n$. Then $n = 0$. □

ARITHMETIC_07_1259086070939648

Proposition 1.6. Let n be a natural number. Then

$$1 \mid n.$$

Proof. We have $1 \cdot n = n$. Hence $1 \mid n$. □

ARITHMETIC_07_3944887330275328

Proposition 1.7. Let n be a natural number. Then

$$n \mid n.$$

Proof. We have $n \cdot 1 = n$. Hence $n \mid n$. □

ARITHMETIC_07_6917446193643520

Proposition 1.8. Let n be a natural number. Then

$$n \mid 1 \quad \text{implies} \quad n = 1.$$

Proof. 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. □

ARITHMETIC_07_7463519983239168

Proposition 1.9. Let n, m, k be natural numbers. Then

$$n \mid m \quad \text{implies} \quad n \mid m \cdot k.$$

Proof. Assume $n \mid m$. Take $l \in \mathbb{N}$ such that $n \cdot l = m$. Then $n \cdot (l \cdot k) = (n \cdot l) \cdot k = m \cdot k$. Hence $n \mid m \cdot k$. □

ARITHMETIC_07_1588185794609152

Corollary 1.10. Let n, m, k be natural numbers. Then

$$n \mid m \quad \text{implies} \quad n \mid k \cdot m.$$

ARITHMETIC_07_7863858316181504

Proposition 1.11. Let n, m, k be natural numbers. Then

$$n \mid m \mid k \quad \text{implies} \quad n \mid k.$$

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 $n \mid k$. □

ARITHMETIC_07_4933275640397824

Proposition 1.12. Let n, m be natural numbers such that $n \neq 0$. Then

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

Proof. Assume $n \mid m$ and $m \mid n$. 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 $n = m$. □

ARITHMETIC_07_1283495225720832

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

$$n \mid m \quad \text{implies} \quad k \cdot n \mid k \cdot m.$$

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 $k \cdot n \mid k \cdot m$. □

ARITHMETIC_07_6469492028735488

Proposition 1.14. Let n, m, k be natural numbers. Assume $k \neq 0$. Then

$$k \cdot n \mid k \cdot m \quad \text{implies} \quad n \mid m.$$

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 $n \mid m$. □

ARITHMETIC_07_4700711333920768

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

$$(k \mid n \text{ and } k \mid m) \quad \text{implies} \quad (k \mid (n' \cdot n) + (m' \cdot m) \text{ for all natural numbers } n', m').$$

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

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

□

ARITHMETIC_07_1556786209357824

Corollary 1.16. Let n, m, k be natural numbers. Then

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

Proof. Assume $k \mid n$ and $k \mid m$. Take $n' = 1$ and $m' = 1$. Then $k \mid (n' \cdot n) + (m' \cdot m)$.

$(n' \cdot n) + (m' \cdot m) = n + m$. Hence $k \mid n + m$. ☐

ARITHMETIC_07_1076947887063040

Proposition 1.17. Let n, m, k be natural numbers. Then

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

Proof. Assume $k \mid n$ and $k \mid n + m$.

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 $(k \cdot l) + m = k \cdot l' = k \cdot (l + l'') = (k \cdot l) + (k \cdot l'')$. Indeed $k \cdot (l + l'') = (k \cdot l) + (k \cdot l'')$ (by **??**). Thus $m = (k \cdot l'')$. Therefore $k \mid m$. End. ☐

ARITHMETIC_07_2187144577679360

Proposition 1.18. Let n, m be natural numbers such that $n, m \neq 0$. Then

$$m \mid n \quad \text{implies} \quad m \leq n.$$

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. ☐