Chapter 1

Euclidean division

File: `arithmetic/sections/08_euclidean-division.ftl.tex`

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

1.1 Quotients and remainders

ARITHMETIC_08_7743986617810944

Theorem 1.1. Let n, m be natural numbers such that $m \neq 0$. Then there exist natural numbers q, r such that

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

and $r < m$.

Proof. Define $\Phi = \{n' \in \mathbb{N} \mid$ there exist natural numbers q, r such that $r < m$ and $n' = (m \cdot q) + r\}$.

(1) Φ contains 0. Proof. Take $q = 0$ and $r = 0$. Then $r < m$ and $0 = (m \cdot q) + r$. Hence $0 \in \Phi$. Qed.

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

Let us show that there exist natural numbers q, r such that $r < m$ and $n' + 1 = (m \cdot q) + r$. Take natural numbers q', r' such that $r' < m$ and $n' = (m \cdot q') + r'$. We have $r' + 1 < m$ or $r' + 1 = m$.

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

Hence $n' + 1 \in \Phi$. Qed.

Then Φ contains every natural number. Thus there exist natural numbers q, r such that $n = (m \cdot q) + r$ and $r < m$. □

ARITHMETIC_08_7801804481888256

Proposition 1.2. Let n, m be natural numbers such that $m \neq 0$. Let q, r be natural numbers such that $(m \cdot q) + r = n$ and $r < m$. Let q', r' be natural numbers such that $(m \cdot q') + r' = n$ and $r' < m$. Then $q = q'$ and $r = r'$.

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

Case $q \geq q'$ and $r \geq r'$. (1) $((m \cdot q) + r) - r' = (m \cdot q) + (r - r')$ (by **??**). (2) $((m \cdot q') + r') - r' = (m \cdot q') + (r' - r') = m \cdot q'$. Hence $(m \cdot q) + (r - r') = m \cdot q'$. Thus $((m \cdot q) - (m \cdot q')) + (r - r') = 0$. Consequently $(m \cdot q) - (m \cdot q') = 0$ and $r - r' = 0$. If $(m \cdot q) - (m \cdot q') = 0$ then $q - q' = 0$. Therefore $q - q' = 0$ and $r - r' = 0$. Thus we have $q = q'$ and $r = r'$. End.

Case $q \geq q'$ and $r < r'$. Take $q'' = q - q'$ and $r'' = r' - r$. 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 $m \cdot (q' + q'') = (m \cdot q') + r''$ (by **??**). We have $m \cdot (q' + q'') = (m \cdot q') + (m \cdot q'')$. Hence $(m \cdot q') + (m \cdot q'') = (m \cdot q') + r''$. [prover vampire] Thus $m \cdot q'' = r''$ (by **??**). Then we have $m \cdot q'' < m \cdot 1$. Indeed $m \cdot q'' = r'' \leq r' < m = m \cdot 1$. Therefore $q'' < 1$ (by **??**). Consequently $q - q' = q'' = 0$. Hence $q = q'$. Thus $(m \cdot q) + r = (m \cdot q) + r'$. Therefore $r = r'$. End.

Case $q < q'$ and $r \geq r'$. Take $q'' = q' - q$ and $r'' = r - r'$. 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 $(m \cdot q) + r'' = m \cdot (q + q'')$ (by **??**). We have $m \cdot (q + q'') = (m \cdot q) + (m \cdot q'')$. Hence $(m \cdot q) + r'' = (m \cdot q) + (m \cdot q'')$. [prover vampire] Thus $r'' = m \cdot q''$. Then we have $m \cdot q'' < m \cdot 1$. Indeed $m \cdot q'' = r'' \leq r < m = m \cdot 1$. Therefore $q'' < 1$ (by **??**). Consequently $q' - q = q'' = 0$. Hence $q' = q$. Thus $(m \cdot q) + r = (m \cdot q) + r'$. Therefore $r = r'$. End.

Case $q < q'$ and $r < r'$. (1) $((m \cdot q') + r') - r = (m \cdot q') + (r' - r)$ (by **??**). (2) $((m \cdot q) + r) - r = (m \cdot q) + (r - r) = m \cdot q$. Hence $(m \cdot q') + (r' - r) = m \cdot q$. Thus $((m \cdot q') - (m \cdot q)) + (r' - r) = 0$. Consequently $(m \cdot q') - (m \cdot q) = 0$ and $r' - r = 0$. If $(m \cdot q') - (m \cdot q) = 0$ then $q' - q = 0$. Therefore $q' - q = 0$ and $r' - r = 0$. Thus we have $q' = q$ and $r' = r$. End. □

ARITHMETIC_08_8621463798022144

Definition 1.3. Let n, m be natural numbers such that $m \neq 0$. $n \operatorname{div} m$ 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 $n \operatorname{div} m$.

ARITHMETIC_08_3560980160184320

Definition 1.4. Let n, m be natural numbers such that $m \neq 0$. $n \bmod m$ 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 $n \bmod m$.

1.2 Modular arithmetic

ARITHMETIC_08_5448561831444480

Definition 1.5. Let n, m, k be natural numbers such that $k \neq 0$. $n \equiv m \pmod{k}$ iff $n \bmod k = m \bmod k$.

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

ARITHMETIC_08_3818318544764928

Proposition 1.6. Let n, k be natural numbers such that $k \neq 0$. Then

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

Proof. We have $n \bmod k = n \bmod k$. Hence $n \equiv n \pmod{k}$. □

ARITHMETIC_08_2337210737098752

Proposition 1.7. Let n, m, k be natural numbers such that $k \neq 0$. Then

$$n \equiv m \pmod{k} \quad \text{implies} \quad m \equiv n \pmod{k}.$$

Proof. Assume $n \equiv m \pmod{k}$. Then $n \bmod k = m \bmod k$. Hence $m \bmod k =$

$n \bmod k$. Thus $m \equiv n \pmod{k}$. □

ARITHMETIC_08_7464329746055168

Proposition 1.8. Let n, m, l, k be natural numbers such that $k \neq 0$. Then

$$(n \equiv m \pmod{k} \text{ and } m \equiv l \pmod{k}) \quad \text{implies} \quad n \equiv l \pmod{k}.$$

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

ARITHMETIC_08_2034122983735296

Proposition 1.9. Let n, m, k be natural numbers such that $k \neq 0$. 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 $(q \cdot k) + r < (q' \cdot k) + r$ (by **??**). Indeed $q \cdot k$ and $q' \cdot k$ are natural numbers. 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. □

ARITHMETIC_08_2988318228742144

Proposition 1.10. Let n, m, k, k' be natural numbers such that $k, k' \neq 0$. Then

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

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. □

ARITHMETIC_08_5895145169879040

Corollary 1.11. Let n, m, k, k' be natural numbers such that $k, k' \neq 0$. Then

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

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

ARITHMETIC_08_5984712287846400

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

$$n + k \equiv n \pmod{k}.$$

Proof. Take $r = n \bmod k$ and $r' = (n + k) \bmod k$. Consider a $q \in \mathbb{N}$ such that

$n = (k \cdot q) + r$ and $r < k$. Consider a $q' \in \mathbb{N}$ such that $n + k = (k \cdot q') + r'$ and $r' < k$. Then $(k \cdot q') + r' = n + k = ((k \cdot q) + r) + k = (k + (k \cdot q)) + r = (k \cdot (q + 1)) + r$. Hence $r = r'$. Consequently $n \bmod k = (n + k) \bmod k$. Thus $n + k \equiv n \pmod{k}$. $\square$