1 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 1.1. 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 1.2. 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 1.3. 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 1.4. 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 $n \operatorname{div} m$.