Theorem 1 (Euclid's Division Theorem: Existence). 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. (a) 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 $0 \in \Phi$. □

(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 $n' = (m \cdot q') + r'$ (by a). 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 $n' + 1 = ((q' \cdot m) + r') + 1 = (q' \cdot m) + (r'$
□

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

End.

Hence $n' + 1 \in \Phi$. □

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

Theorem 2 (Euclid's Division Theorem: Uniqueness). Let n, m be natural numbers such that $m \neq 0$. Let q, r be natural numbers such that

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

and $r < m$. Let q', r' be natural numbers such that

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

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 associativity of addition and subtraction). (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 $r = r'$. □

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 right-cancellability of addition). 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 $m \cdot q'' = r''$. Then we have $m \cdot q'' < m \cdot 1$. Indeed $m \cdot q'' = r'' \leq r' < m = m \cdot 1$. Therefore $q'' < 1$ (by preservation of ordering under left-multiplication). Consequently $q - q' = q'' = 0$. Hence $q = q'$. Thus $(m \cdot q) + r = (m \cdot q) + r'$. Therefore $r = r'$. □

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 right-cancellability of addition). 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 preservation of ordering under left-multiplication). Consequently $q' - q = q'' = 0$. Hence $q' = q$. Thus $(m \cdot q) + r = (m \cdot q) + r'$. Therefore $r = r'$. □

Case $q < q'$ and $r < r'$. (1) $((m \cdot q') + r') - r = (m \cdot q') + (r' - r)$ (by associativity of addition and subtraction). (2) $((m \cdot q) + r) - r = (m \cdot q) + (r - r) = m \cdot q$. Hence $(m \cdot q') + (r' - r) = m \cdot q$. Thus $((m \cdot q') - (m \cdot q)) + (r' - r) = ((m \cdot q') + (r' - r)) - (m \cdot q) = 0$. 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 $r' = r$. □

■