Proof of the Quotient-Remainder Theorem

Theorem 4.4.1 : (The Quotient-Remainder Theorem)
For any integer n and any positive integer d, there exist unique integers q and r such that $n = d \cdot q + r$ and $0 \le r < d$.

Proof: Let n be any integer and let d be any positive integer.

[We first prove the **existence** of such integers q and r.]

Let set S be defined as follows:

$$S = \{ x \in Z \mid x \ge 0 \text{ and } x = n - d \cdot k \text{ for some integer } k \}$$

[Later, we will see that the least element of S is the remainder r and the quotient q is the integer k that comes with it in the definition of set S.]

[We verify that set S satisfies the conditions of the Well-Ordering Principle.]
[We show that set S contains at least one integer element, that is, that S is non-empty.]

There are two possibilities for the number n: $n \ge 0$ or $n < 0$.

Case 1: $(n \ge 0)$. Suppose $n \ge 0$.

Let $k = 0$. Then, $n - d \cdot k = n \ge 0$, so $n = n - d \cdot k$ is in set S.

$\therefore$ Set S is non-empty in Case 1.

Case 2: $(n < 0)$. Suppose $n < 0$.

Then, $(-n) > 0$ and $d - 1 \ge 0$, since $d \ge 1$.

$\therefore (-n) \cdot (d - 1) \ge 0$. Let $k = n$.

Then, $n - d \cdot k = n - d \cdot n = -d \cdot n + n = (-n) \cdot (d - 1) \ge 0$.

$\therefore$ $n - d \cdot n$ is in set S and set S is non-empty in Case 2.

$\therefore$ Therefore, set S is non-empty, in general .

[We show that every integer in S is greater than or equal to some fixed integer.]

By definition of set S, every element in S is greater than or equal to 0..

Therefore, set S satisfies the conditions of the Well-Ordering Principle.

Therefore, by the Well-Ordering Principle, set S contains a least element m. [Ultimately, m is r.]

Since $m \in S$, there is some specific integer ℓ such that $m = n - d \cdot \ell$.

$\therefore$ $n = d \cdot \ell + m$. .

[Later, we will find that $\ell = q$ and $m = r$, and then $n = d \cdot q + r$, by substitution.]

[To complete the proof of **existence**, we have left to show that $0 \le r < d$.

That is, we need to show that $0 \le m < d$.]

Since m is an element of S, $0 \le m$.

[We will prove that $m < d$ using proof-by-contradiction.]

Suppose, by way of contradiction, that $m \ge d$.

$\therefore m - d \ge 0$. [We show that $(m - d)$ is in set S.]

[Recall that, by definition of ℓ, $m = n - d \cdot \ell$.]

Now, $m - d = (n - d \cdot \ell) - d$

$= n - d \cdot (\ell + 1)$

$\therefore (m - d) = n - d \cdot k$, where $k = \ell + 1$.

$\therefore (m - d) \ge 0$ and $(m - d) = n - d \cdot k$, for some integer k.

$\therefore (m - d)$ is an element of set S.

But, $(m - d) < m$, which contradicts the fact that m is the least element of set S.

$\therefore m < d$, by proof-by-contradiction.

[Therefore, we have shown the following:]

$\therefore n = d \cdot \ell + m$ and $0 \le m < d$.

Let $q = \ell$ and $r = m$.

Then, q and r are integers such that $n = d \cdot q + r$ and $0 \le r < d$.

[Thus, **existence** of integers q and r has been established.]

[It remains only to show that these integers q and r are **unique**,

that is, if q_1 and r_1 are any two integers

such that $n = d \cdot q_1 + r_1$ and $0 \le r_1 < d$,

then $q_1 = q$ and $r_1 = r$.]

Already, we know, for the integers q and r as defined above, that

$$n = d \cdot q + r \quad \text{and} \quad 0 \le r < d.$$

Let q_1 and r_1 be any two integers such that

$$n = d \cdot q_1 + r_1 \quad \text{and} \quad 0 \le r_1 < d.$$

Since $n = d \cdot q + r$ also,

$$d \cdot q + r = d \cdot q_1 + r_1, \text{ by substitution.}$$

$\therefore \quad r_1 - r = d \cdot q - d \cdot q_1 = d \cdot (q - q_1)$ [***]

We first assume that $r_1 \ge r$. [Case 1]

Since $0 \leqslant r_1 - r \leqslant r_1$ and $r_1 < d$, $0 \leqslant r_1 - r < d$.

$\therefore\ 0 \leqslant d \cdot (q - q_1) < d$, by substitution. [Next, divide all expressions by d.]

$\therefore\ 0 \leqslant (q - q_1) < 1$.

Since $q - q_1$ is an integer such that $0 \leqslant (q - q_1) < 1$, $q - q_1 = 0$.

$\therefore\ q = q_1$, under the assumption that $r_1 \ge r$. [$q = q_1$ in Case 1]

If $r \ge r_1$, then a similar argument shows that $q = q_1$. [$q = q_1$ in Case 2]

Thus, $q = q_1$, in general, and so, $(q - q_1) = 0$.

By [***] above, $r_1 - r = d \cdot (q - q_1)$.

$\therefore\ r_1 - r = d \cdot (q - q_1) = d \cdot 0 = 0$ by [***] above.

$\therefore\ r_1 = r$.

$\therefore\ q_1 = q$ and $r_1 = r$. Thus q and r are unique.

QED