Part IV. Chapter 15. The division theorem

We take the universal set to be the integers $\mathbb{Z}$. Let $\mathbb{Z}^\geq$ denote the set of nonnegative integers.

When we divide 277 by 5 and obtain a remainder of 2, we really mean that

$$277 = 5 \cdot 55 + 2.$$  

We chose the factor 55 because this is the unique integer that produces a remainder $r = 2$ with $0 \leq r < 5$.

In general, we may divide any integer $a$ by any positive integer $b$ to obtain a remainder $r$ with $0 \leq r < b$. The division theorem says:

**Theorem 1 (Eccles 15.1.1)** Let $a$ be an integer and let $b$ be a positive integer. Then there are unique integers $q$ and $r$ such that

$$a = bq + r \quad \text{and} \quad 0 \leq r < b \quad (1)$$

**Proof in the case where $a \geq 0$.** Note that if $a = bq + r$, then $r = a - bq$.

**Existence.** Consider the set $S$ of all nonnegative remainders, that is, the set

$$S = \{a - bq \mid q \in \mathbb{Z}\} \cap \mathbb{Z}^\geq.$$  

(1) Since $0 \leq a = a - b \cdot 0$, we have $a \in S$, so that $S$ is nonempty.

(2) Since $S \subseteq \mathbb{Z}^\geq$ and $S \neq \emptyset$, there exists a smallest element of $S$, which we call $r$. Since $r \in S$, there exists $q \in \mathbb{Z}$ such that

$$r = a - bq, \quad \text{i.e.,} \quad a = bq + r.$$  

Since $r \in S \subseteq \mathbb{Z}^\geq$ implies $r \geq 0$, we just need to show that $r < b$.

Observe that $r - b$ can be written as

$$r - b = (a - bq) - b = a - b(q + 1)$$

and $q + 1 \in \mathbb{Z}$. On the other hand, since $r - b < r$ and since $r$ is the smallest element of $S$, we must have $r - b \notin S$. By the definition of $S$, this implies $r - b < 0$, i.e., $r < b$.\(^1\) This completes the proof of the existence of $q$ and $r$ satisfying (1).

\(^1\)To wit, $r - b$ is a remainder smaller than $r$ (the smallest nonnegative remainder), so it must be negative.
**Uniqueness.** Suppose that \( q, r \) and \( \tilde{q}, \tilde{r} \) are integers such that both

\[
a = bq + r \quad \text{and} \quad 0 \leq r < b
\]

and

\[
a = b\tilde{q} + \tilde{r} \quad \text{and} \quad 0 \leq \tilde{r} < b.
\]

Then \( bq + r = b\tilde{q} + \tilde{r} \) and hence

\[
\tilde{r} - r = b(q - \tilde{q}).
\]

Since \( -b < \tilde{r} - r < b \), we have

\[
-b < b(q - \tilde{q}) < b, \quad \text{i.e.,} \quad -1 < q - \tilde{q} < 1.
\]

Since \( q - \tilde{q} \) is an integer, we conclude that

\[
q - \tilde{q} = 0,
\]

which in turn by \( \tilde{r} - r = b(q - \tilde{q}) \) implies that

\[
\tilde{r} - r = 0.
\]

This completes the proof of both uniqueness and the division theorem. \( \square \)