Division Theorem

Given a positive number, such as 5, we divide any integer by it to get a remainder which is between 0 and 4 inclusive. For example, we can write 277 as

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

In general, we may always divide any integer $a$ by any positive integer $b$ to obtain a remainder $r$ with $0 \leq r < b$.

The **division theorem** says that there is a unique way to do this:

**Eccles Theorem 15.1.1.** Let $a$ be any integer and let $b$ be any positive integer. Then there exist unique integers $q$ and $r$ such that

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

(The integer $r$ is the smallest possible nonnegative remainder.)

**Proof.** For simplicity we shall assume that $a \geq 0$. The general case $a \in \mathbb{Z}$ follows without much difficulty.

(1) **Existence.** The equation $a = bq + r$ in (1) is equivalent to $a - bq = r$. Thus any remainder has the form $a - bq$, where $q \in \mathbb{Z}$. So consider the set of all remainders:

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

We are looking for the *smallest nonnegative* remainder. For this reason we first consider the set

$$T = S \cap \mathbb{Z}^\geq$$

of all nonnegative remainders.

We have $a \in T$ because $a = a - b \cdot 0$ and we are assuming $a \geq 0$. So $T$ is nonempty. Since $T$ is a nonempty set of nonnegative integers, by the ‘well-ordering principle’ (a.k.a. Exercise 11.6), there exists a smallest element of $T$; call this smallest element $r$. We shall show that this is the remainder we are looking for.

Since $r \in T$, there exists $q \in \mathbb{Z}$ such that $r = a - bq$. Then

$$a = bq + r. \quad (2)$$

Moreover since $r \in T \subseteq \mathbb{Z}^\geq$,

$$r \geq 0. \quad (3)$$
Now consider the next smallest remainder than \( r \), namely consider
\[
    r - b = a - b (q + 1) \in S.
\]
Since \( r \) is the smallest element of \( T \) and \( r - b < r \), we have \( r - b \notin T \). This implies \( r - b < 0 \) since \( r - b \in S \). In other words,
\[
    r < b. \tag{4}
\]
By (2), (3) and (4), we have proved the existence of \( q \) and \( r \) satisfying (1).

**Uniqueness.** Suppose that we have to sets of integers \( q, r \) and \( \tilde{q}, \tilde{r} \) satisfying
\[
    a = bq + r \quad \text{and} \quad 0 \leq r < b
\]
and
\[
    a = b\tilde{q} + \tilde{r} \quad \text{and} \quad 0 \leq \tilde{r} < b.
\]
We want to show that \( \tilde{q} = q \) and \( \tilde{r} = r \). We then have
\[
b (\tilde{q} - q) + \tilde{r} - r = 0.
\]
Since \( 0 \leq r < b \) and \( 0 \leq \tilde{r} < b \), we have \( -b < r - \tilde{r} < b \). From this we obtain
\[
-1 < \tilde{q} - q = \frac{r - \tilde{r}}{b} < 1.
\]
Since \( \tilde{q} - q \in \mathbb{Z} \), this implies that
\[
\tilde{q} - q = 0.
\]
This in turn implies that
\[
\tilde{r} - r = 0. \quad \square
\]