Notes on Chapter 6: Division with Remainder

Theorem (Division with Remainder). *Let $n \in \mathbb{N}$ and $m \in \mathbb{Z}$. There exist unique integers $q, r \in \mathbb{Z}$ such that*

$$m = nq + r \qquad \text{and} \qquad 0 \le r < n. \tag{$*$}$$

Proof. The proof is two parts: (1) existence of q and r such that $(*)$ is true, and (2) uniqueness of q and r. We'll start with existence. Consider the set

$$S = \{m + an : a \in \mathbb{Z}\} \cap \mathbb{Z}_{\ge 0}.$$

Step 1a. $S \neq \varnothing$.

Proof of Step 1a. We'll consider two cases: $m \ge 0$ and $m < 0$. If $m \ge 0$, let's take $a = 1$. Then, since $n > 0$, we have $m + an = m + n \ge 0$, so $m + an$ is an element of S. This shows that $S \neq \varnothing$.

If $m < 0$, then let's take $a = -m$. In this case, we have $m + an = m - mn = m(1 - n)$. Since $n \ge 1$, we know that $1 - n \le 0$. We also have $m < 0$ by assumption, so it follows that $m(1 - n) \ge 0$. This shows that $m + an \in S$, so again, $S \neq \varnothing$. ◻

Note that for all $c \in S$, we have $0 \le c$. Therefore, applying Proposition 2.33 (a variant of the Well-Ordering Principle) to the set S and the integer 0, we learn that S has a smallest element. Let

$$r = \text{the smallest element of } S.$$

Since $r \in S$, there is some $a \in \mathbb{Z}$ such that $r = m + an$. Let

$$q = -a.$$

From these definitions, it follows that $m = nq + r$. To complete the existence part of the proof, we must show that the second condition in $(*)$ holds.

Step 1b. $0 \le r < n$.

Proof of Step 1b. The fact that $r \ge 0$ is obvious, since $r \in S$, and every element of S lies in $\mathbb{Z}_{\ge 0}$ by the very definition of S. It remains to prove that $r < n$. We will do this by contradiction. Assume that $r \ge n$. Then, it follows that $r - n \ge 0$. We also have $r - n = (m - nq) - n = m + (-q - 1)n$. Let $b = -q - 1$. Since $r - n \ge 0$ and $r - n = m + bn$, we have shown that $r - n \in S$. We also have $r - n < r$, since $n \in \mathbb{N}$. That is, $r - n$ is an element of S that is smaller than r. But that's a contradiction: r was *defined* to be the smallest element of S. Therefore, $r < n$. ◻

The existence part of the proof is done. To prove uniqueness, suppose we have $q, r, q', r' \in \mathbb{Z}$ such that

$$\begin{aligned} m &= nq + r, & 0 &\le r < n, \\ m &= nq' + r', & 0 &\le r' < n. \end{aligned}$$

We must prove that $q = q'$ and $r = r'$.

Step 2a. $r = r'$.

Proof of Step 2a. We will prove this by contradiction. Assume that $r \neq r'$. Then either $r < r'$ or $r > r'$. Assume without loss of generality[1] that $r > r'$. Then $r - r' > 0$, i.e., $r - r' \in \mathbb{N}$. Next, note that $r - r' = (m - nq) - (m - nq') = n(q' - q)$. This shows that $r - r'$ is a natural number divisible by n, so by Proposition 2.23, we have $r - r' \ge n$. But on the other hand, since $r' \ge 0$, we have $r - r' \le r$, and since $r < n$, it follows that $r - r' < n$, a contradiction. Therefore, $r = r'$. ◻

Step 2b. $q = q'$.

Proof of Step 2b. We have $m = nq + r = nq' + r'$, and since $r = r'$, it follows that $nq = nq'$. Finally, since $n \neq 0$, we have $q = q'$ by Axiom 1.5. ◻ □

[1] This means: the reasoning will be exactly the same in the case $r < r'$, so we will skip writing it down.