Proof. (Proof of Lemma 4.0.1)

Proof of existence

Let $a, b \in \mathbb{N}$. Consider the set

$$B = \{kb \,|\, k \in \{0, 1, 2, \dots\}\}.$$

Then $B \subseteq \mathbb{N}$. Also $0 \in B$ so $\emptyset \neq B$. Moreover, there exists $q \in \mathbb{Z}$ such that $qb \in B$ and $a < qb$ since $a < (a+1)b \in B$. Let

$$C = \{q \in \mathbb{Z} \,|\, a < qb\}.$$

Then $a + 1 \in C$. Since $C \neq \emptyset$ and $C \subseteq \mathbb{Z}$ it follows that C has a least element, say $q_0 + 1$ by the Well-ordering principle. Hence

$$\begin{aligned} q_0 b \leq a < (q_0+1)b &\Rightarrow q_0 b \leq a < q_0 b + b \\ &\Rightarrow 0 \leq a - q_0 b < b. \end{aligned}$$

By letting $r = a - q_0 b$ we get that $a = q_0 b + r$ and $0 \leq r < b$ as desired.

Proof of Uniqueness

Assume $a = q_1 b + r_1$ and $a = q_2 b + r_2$ where $0 \leq r_1, r_2 < b$. Then $q_1 b + r_1 = q_2 b + r_2$ which implies $(q_1 - q_2)b = r_2 - r_1$. Since $r_2 - r_1$ is a multiple of b and $r_2 - r_1 < b$ it must be the case that $r_2 - r_1 = 0$ which implies $q_1 - q_2 = 0$. Therefore $r_1 = r_2$ and $q_1 = q_2$.

□

Lemma 4.0.1 can be extended to all integers as in Problem 4.0.4. In both cases, a common mistake made when finding q and r it to pick r to be negative. This happens exactly when the q chosen is too large. If the q chosen is too small then the r will be too large.

Problem 4.0.4 (The Division Algorithm)**.** *Let $a, b \in \mathbb{Z}, b \neq 0$. Then there exist unique integers q and r, with $0 \leq r < |b|$ such that $a = qb + r$.*

Hint: Try using proof by cases.

Case 1: $a = 0, b \neq 0$.

Case 2: $a, b > 0$.

Case 3: $a < 0, b > 0$.

Case 4: $a > 0, b < 0$.

Case 5: $a < 0, b < 0$.

It is worth noting that some books label Lemma 4.0.1 as the Division Algorithm. In the Division Algorithm q is the *quotient* and r is the *remainder* when a is divided by b.

Example 4.0.5. Find integers q and r, with $0 \leq r < 20$ such that $2,345 = -20q + r$.