THE QUOTIENT-REMAINDER THEOREM

MATH 372. FALL 2005. INSTRUCTOR: PROFESSOR AITKEN

Theorem 1. *Given integers $a \in \mathbb{Z}$ and $b \in \mathbb{N}_1$ there are unique integers q and r such that (i) $a = qb + r$, and (ii) $0 \leq r < b$.*

Remark. The integer q in the above is called the *quotient* and the integer r is called the *remainder*.

Remark. Recall that $\mathbb{N}_1$ is the set $\{1, 2, 3, 4, 5, \ldots\}$. The above theorem generalizes to negative b, but we will only need it for positive b.

The general strategy (of the existence part) of the proof is to find a multiple of b, not greater than a, that is as close to a as possible. We use the boundedness principle on a set of multiples to find the desired multiple qb of b.

Proof. Let S be the set of multiples of b which are less than or equal to a:

$$S \stackrel{\text{def}}{=} \{nb \mid nb \leq a,\ n \in \mathbb{Z}\}.$$

We want a maximum element in S, but to use the boundedness principle to get such a maximum we need to verify that (i) S is bounded from above, and (ii) S is non-empty. The first is easy: S is bounded from above by a by definition of S. For the second: note that if $a \geq 0$ then $0 \in S$ since 0 is a multiple of b. So in this case S is non-empty. If $a < 0$ then $ab \in S$. To see this observe that $b \geq 1$ so $ab \leq a$. So in this case S is also non-empty.

Let qb be the maximum of S which exists by the boundedness principle. Define r to be the "gap": $r \stackrel{\text{def}}{=} a - qb$. Thus $a = qb + r$. Since $qb \leq a$ we know that $r \geq 0$.

We still need to show that $r < b$. Suppose otherwise: $r \geq b$. Then $a - qb \geq b$. In this case, $a \geq qb + b$, and $qb + b > qb$ since b is positive. Thus $a \geq (q+1)b > qb$, which implies $(q+1)b \in S$ is larger than bq. This contradicts the maximality of qb. Therefore, $r < b$.

We still need to show uniqueness. Suppose q' and r' also satisfy the desired conditions: (i) $a = q'b + r'$, and (ii) $0 \leq r' < b$.

To show $r = r'$, suppose otherwise that $r \neq r'$. We consider the case where $r > r'$: the case where $r < r'$ is similar. From the equation $a = qb + r = q'b + r'$ we get the equation $r - r' = (q' - q)b$. Since $r - r' > 0$ and $b > 0$ it follows that $q' - q > 0$. From a previous exercise we know that if x, y, z are positive integers with $z = xy$ then $y \leq z$. So, since $r - r' = (q' - q)b$, we conclude that $b \leq (r - r')$. By assumption, $r < b$. Since, $-r' \leq 0$ we also know that $r - r' \leq r$. Thus $r - r' < b$ contradicting $b \leq r - r'$. So $r = r'$.

As before, from $a = qb + r = q'b + r'$ we get the equation $r - r' = (q' - q)b$. Since $r = r'$ we have that $(q' - q)b = 0$. Since $b \neq 0$ it follows that $(q' - q) = 0$. Thus $q = q'$. This completes the proof of uniqueness. □

Date: Fall 2005. Version of October 1, 2005.

I deliberately made this proof long-winded to make it easier to follow. You need to be long-winded at first until you become proficient in proofs. In more advanced textbooks and papers, one finds a more condensed style. For example, here is a shorter version of the above:

Proof. Consider $S \stackrel{\text{def}}{=} \{nb \mid nb \leq a,\ n \in \mathbb{Z}\}$. This set is non-empty: if $a \geq 0$ then $0 \in S$ and if $a < 0$ then $ab \in S$ (since $ab \leq a$ because b is positive). Since this non-empty set is bounded above by a, it has a maximum element qb. Let r be $a - qb$. Thus $a = qb + r$.

Obviously $r \geq 0$. To show that $r < b$, suppose otherwise. Then $a - qb = r \geq b$ so $a \geq qb + b$. Thus $(q+1)b \in S$, contradicting the maximality of qb.

For uniqueness, suppose q' and r' also satisfy the desired conditions. Suppose $r \neq r'$. We can assume $r > r'$. From $a = qb + r = q'b + r'$ we get the $r - r' = (q' - q)b$. Since $r - r'$ is a positive multiple of b we get $b \leq r - r'$. However $r - r' \leq r < b$. Contradiction.

Since $r = r'$ it follows that $qb = q'b$. Since $b > 0$, $q = q'$. □

DR. WAYNE AITKEN, CAL. STATE, SAN MARCOS, CA 92096, USA
E-mail address: waitken@csusm.edu