

Math 74 Homework 5, Problem 2: Solution

October 1, 2008

The *division algorithm* for \mathbb{N} says the following: if n and m are any two non-zero natural numbers, then there exist unique numbers $q, r \in \mathbb{N}$ such that $n = qm + r$ and $0 \leq r < m$. (You should think of this as saying that “ m divides n q -times with remainder r .”)

1. Fix an $m \in \mathbb{N} \setminus \{0\}$. Use the well-ordering principle to show that for every $n \in \mathbb{N} \setminus \{0\}$, there exist numbers $q, r \in \mathbb{N}$ such that $n = qm + r$ with $0 \leq r < m$.
2. Repeat the previous part of the problem, but give a proof using induction on n instead of the well-ordering principle.
3. Let $n, m \in \mathbb{N} \setminus \{0\}$ be arbitrary, and suppose that $q, q', r, r' \in \mathbb{N}$ such that $0 \leq r < m$, $0 \leq r' < m$, $n = qm + r$, and $n = q'm + r'$. Show that $q = q'$ and $r = r'$. (This is what was meant by “unique” in the statement of the division algorithm.)

Solution to 1): Let $m \in \mathbb{N} \setminus \{0\}$ be arbitrary. Assume the statement is false, that is, assume there is some $n \in \mathbb{N}$ such that there do not exist $q, r \in \mathbb{N}$ with $0 \leq r < m$ and $n = qm + r$. Let $S = \{n \in \mathbb{N} \mid \text{There do not exist } q, r \in \mathbb{N} \text{ such that } 0 \leq r < m \text{ and } n = qm + r\}$.

By assumption, S is non-empty, so by well-ordering, S has a smallest element; call this element n_0 . Note that since $0 = 0m + 0$, it follows that 0 is not in S , so $n_0 \neq 0$ and hence $n_0 - 1 \in \mathbb{N}$. By minimality of n_0 , we know that $n_0 - 1 \notin S$, and hence there exist some $q, r \in \mathbb{N}$ such that $0 \leq r < m$ and $n_0 - 1 = qm + r$, i.e. $n_0 = qm + r + 1$. We consider two cases:

Case I: $r = m - 1$. Then $n_0 = qm + m - 1 + 1 = (q + 1)m + 0$. Then $q' = q + 1$ and $r' = 0$ are two natural numbers such that $0 \leq r' < m$ and $n_0 = q'm + r'$. This contradicts the fact that $n_0 \in S$.

Case II: $0 \leq r < m - 1$. Then $r + 1 < m$, so $q' = q$ and $r' = r + 1$ are two natural numbers such that $0 \leq r' < m$ and $n_0 = q'm + r'$. Again, this contradicts the fact that $n_0 \in S$.

So in all cases we have a contradiction. Hence our assumption was false, and the desired statement is true.

Solution to 2): This is really the same as (1); all changes are purely cosmetic.

Let $P(n)$ be the statement “There exist $q, r \in \mathbb{N}$ such that $0 \leq r < m$ and $n = qm + r$.” We want to show that $P(n)$ is true for all n .

Induction Beginning: $P(0)$ says that there exist $q, r \in \mathbb{N}$ such that $0 \leq r \leq m$ and $0 = qm + r$. Taking $q = 0 = r$ suffices.

Induction Step: We want to show $P(k) \Rightarrow P(k + 1)$. So, assume $P(k)$ is true, i.e. assume that there exist $q, r \in \mathbb{N}$ such that $0 \leq r < m$ and $k = qm + r$. Then $k + 1 = qm + r + 1$. If $r = m - 1$, then this says that $k + 1 = (q + 1)m + 0$, so taking $q' = q + 1$ and $r' = 0$ shows that $k + 1 = q'm + r'$ with $q', r' \in \mathbb{N}$ and $0 \leq r' < m$. On the other hand, if $0 \leq r < m - 1$, then $r + 1 < m$, so taking $q' = q$, $r' = r + 1$ shows that $k + 1 = q'm + r'$ with $q', r' \in \mathbb{N}$ and $0 \leq r' < m$.

Solution to 3): As suggested, suppose we have some $q, q', r, r' \in \mathbb{N}$ with $0 \leq r < m$ and $0 \leq r' < m$ such that $n = qm + r$ and $n = q'm + r'$. Then $qm + r = q'm + r'$. Without loss of generality, we can assume that $r' \leq r$. Rearranging terms gives $r - r' = q'm - qm$, and hence $r - r' = m(q' - q)$. Hence m divides the non-negative number $r - r'$, so since $m \neq 0$, we have that either $q' - q = 0$ or else $r - r' \geq m$. Now, I claim that $r - r' \geq m$ is impossible. Indeed, since $r < m$ and $0 \leq r'$, we have that $r - r' < m$. Hence we must have that $q - q' = 0$, and so also $r - r' = m(q - q') = 0$. Hence $q = q'$ and $r = r'$.