Division Theorem Proof

April 29, 2017

Theorem
Let a and b be integers, with b being positive. Then are are unique integers q and r such that $a = q \cdot b + r$ and $0 \leq r < b$.
Proof
First we prove existence. Take a set of non-negative integers of the form $\{a-k \cdot b\}$. By the well-ordering principle, every non-empty set of positive integers contains a least element. Thus, if we have a set of non-negative integers of the form $\{a-k \cdot b\}$, we have pick the smallest one if we can show that this set is non-empty. Choosing $k = -|a|$, we have $a+|a| \cdot b$. Since $b \geq 1$, we have $a+|a| \cdot b \geq a+|a| \geq 0$. Since for $k = -|a|$, we have a positive integer, the set is non-empty. Now suppose that the smallest such integer in $\{a - k \cdot b\}$ occurs when $k = q$, and let $a - q \cdot b = r$. Suppose that $r \geq b$, then we have $r = a - q \cdot b \geq b$. We can write this as $a - q \cdot b - b \geq 0 \iff a - (q + 1) \cdot b \geq 0$. But since $q + 1 > q$, $a - (q + 1) \cdot b < a - q \cdot b \iff 0 < b$. But we already assumed $a - q \cdot b$ was the smallest element. This is a contradiction, and thus $r < b$, and so $0 \leq r < b$. Hence, we have proved existence. Now we prove uniqueness. Suppose there are integers q_1, q_2, r_1, r_2 satisfying $a = q_1 \cdot b + r_1 = q_2 \cdot b + r_2$ with $0 \leq r_1, r_2 < b$. Then we can rewrite the above as $q_1 \cdot b - q_2 \cdot b = r_1 - r_2 \iff (q_1 - q_2) \cdot b = r_1 - r_2$, hence $r_1 - r_2$ is some multiple of b. However, since $0 \leq r_1, r_2 < b$ and r_1 and r_2 are integers, $r_1 - r_2$ must be 0. Hence, we have $r_1 = r_2$ and $q_1 = q_2$. Hence, we have proved uniqueness. Since we have proved existence and uniqueness, we have proved the theorem.
QED