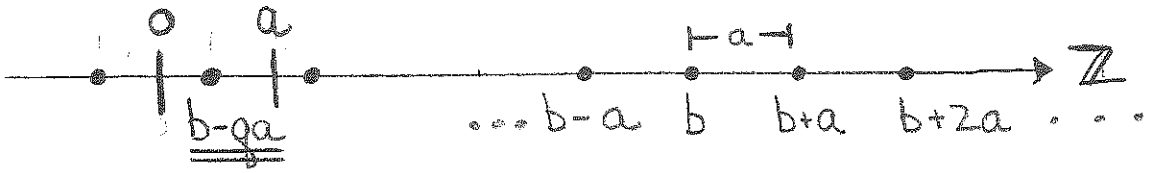
Math 8: The Division Algorithm

Spring 2011; Helena McGahagan

THE DIVISION ALGORITHM Let $a \in \mathbb{N}$. Then, for any $b \in \mathbb{Z}$, there exist unique integers q and r such that $b = qa + r$ and $0 \leq r < a$.

The idea for the proof is to consider all the possible values of $b - xa$, where x is an integer, then take the value that's closest to zero and positive. This should give us the right remainder r (see the picture below.)



Proof. Consider the set

$$S = \{b - xa : x \in \mathbb{Z} \text{ and } b - xa \geq 0\}.$$

Notice there are always elements in S: If $b \geq 0$, then $b \in S$ and if $b < 0$, then $b - ba \in S$ (*show this!*) Therefore, S is a non-empty set consisting of non-negative integers, so we can take the smallest number $r \in \mathbb{S}$. (*This is the well-ordering property again! See the lecture notes on the proof that there are infintely many primes.*) From the definition of S we know that $r = b - qa$ for some integer q and also that $r \geq 0$. Now, we have found integers r and q that solve $b = qa + r$, and we know $0 \leq r$. We still need to show that the inequality $r < a$ holds. We do this by contradiction:

Assume that $r \geq a$. Consider the number $r' = b - (q+1)a$. Since $r' = b - (q+1)a = (b - qa) - a = r - a \geq 0$, we see that $r' \in S$. However, $r' = b - (q+1)a < b - qa = r$ since $a \in \mathbb{N}$. This is a contradiction since r was chosen to be the smallest element of S.

So far, we have shown there exists a solution $q, r \in \mathbb{Z}$ satisfying the equation $b = qa + r$ and the inequality $0 \leq r < a$. To show uniqueness, we assume there are two such solutions, and prove that they must be the same ☺ Assume there exist $q_1, r_1 \in \mathbb{Z}$ and $q_2, r_2 \in \mathbb{Z}$ such that

$$\begin{aligned} b &= q_1 a + r_1 \quad \text{and} \quad 0 \leq r_1 < a \\ b &= q_2 a + r_2 \quad \text{and} \quad 0 \leq r_2 < a \end{aligned}$$

Assume that $r_1 \neq r_2$. Then we may assume, without loss of generality, that $r_1 > r_2$ (if it is instead the case that $r_2 > r_1$, the proof is exactly the same, just with the indices swapped.) Subtracting the two equations, we find that $0 = (q_1 - q_2)a + (r_1 - r_2)$ and $0 < r_1 - r_2 < a$. This equation becomes $r_1 - r_2 = (q_2 - q_1)a$, so we see that $a \mid (r_1 - r_2)$. Since $a \in \mathbb{N}$, $a > 0$, and we also know $r_1 - r_2 > 0$. Therefore, we have from a proposition prove in lecture that $a \leq r_1 - r_2$, a contradiction. This means our assumption that $r_1 \neq r_2$ is false, so we must have $r_1 = r_2$. Now, we have (again from subtracting the two equations) that $(q_1 - q_2)a = 0$. Since $a > 0$, this implies that $q_1 = q_2$. □