MTHSC 412 Section 1.1 – The Division Algorithm

Kevin James

Theorem (Well-Ordering Principle)

Every nonempty set S of nonnegative integers has a least element. That is, there is $m \in S$ such that $x \in S \Rightarrow m \leq x$.

Note

The well ordering principle is equivalent to the principle of mathematical induction.

Theorem (The Division Algorithm)

Suppose that $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that

1. $a = bq + r$, *and*
2. $0 \le r < b$.

Example

1. Given $a = 14$ and $b = 3$, we can write $14 = 3 * 4 + 2$. So, $q = 4$ and $r = 2$.
2. Given $a = -14$ and $b = 3$, we can write $-14 = 3 * (-5) + 1$. So, $q = -5$ and $r = 1$.

Proof.

Existence: Let $a, b \in \mathbb{Z}$ with $b > 0$.
Let $S = \{a - bq \mid q \in \mathbb{Z}; a - bq \geq 0\}$.
Note that S is a subset of the nonnegative integers.
Now, note that if $a = 0$ then $a - b(-1) = b > 0$. Thus, $b \in S$.
Now, assume $a \neq 0$. Recall that
$b \geq 1 \Rightarrow |a|b \geq |a| \geq -a \Rightarrow a + b|a| \geq 0$.
Thus, $a - b(-|a|) \in S$.
So, $S \neq \emptyset$.
By the Well Ordering Principle, S has a smallest element.
Let r be the smallest element of S.
Then $r \geq 0$ and we have for some $q \in \mathbb{Z}$, $a - bq = r \Rightarrow a = bq + r$.
Also, note that
$r - b = (a - bq) - b == a - b(q + 1)$.
Since $r - b < r$ and r is the least element of S, it follows that
$r - b < 0 \Rightarrow r < b$.
Uniqueness: Exercise. □

Corollary

Let $a, c \in \mathbb{Z}$ with $c \neq 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that

$$a = cq + r \qquad \text{and} \qquad 0 \leq r < |c|.$$

Proof.

Exercise. $\square$