1.1 The Division Algorithm

Evan Hughes

January 2023

Revisiting $\mathbb{Z}$

$\mathbb{Z}$ is the set of all integers. $\mathbb{Z} = \{\pm 1, \pm 2, \pm 3, \ldots\}$.

Well Ordering Axiom: Every non-empty set of integers has a smallest element. However this is not true for all sets. For example, $\mathbb{R}$ does not have a smallest element. For any ratio r, there is always a smaller ratio $r/2$. This also does not hold true for $\mathbb{Z}$ because there is no smallest negative integer.

Understanding Division

One can start by writing out what division is verbally. It can be written as:

$$\text{dividend} = (\text{quotient}) \times (\text{divisor}) + (\text{remainder})$$

Theorem 1.1: The Division Algorithm

Let a, b be Integers with $b > 0$. Then there exist unique Integers q and r such that

$$a = bq + r \text{ and } 0 \leq r < b.$$

Theorem 1.1 allows for the possibility of the dividend a being negative. However r, the remainder, is required to be positive and less than the divisor b.
An **example** of why the last requirement is necessary is if $a = -14$ and $b = 3$ as it leaves 3 possibilities for q and r. If you require r to be non negative there is always one solution.

Proof of Theorem 1.1

Let a and b be integers with $b > 0$. Consider the set S of all integers of the form

$$a - bx, \text{ where x is an integer and } a - bx \geq 0.$$

Step 1: Show that S is non-empty. You do this by finding a value for x such that $a - bx \geq 0$. $a - bx$ is in S when $x = |-a|$, which means S is nonempty.

Step 2: Find q and r such that $a = bq + r$ and $0 \leq r < b$. By the **Well Ordering Axiom**, S has a smallest element. This smallest element is r. Since $r \in S \implies r \geq 0$ and $r = a - bx$ for some x, like $x = q$. Meaning $a = bq + r$ and $r \geq 0$.
Step 3: Show that $r < b$. To show that $r < b$, we must show that $r \geq b$ is false. Then $r - b \geq 0$, so that

$$0 \leq r - b = (a - bq) - b = a - b(q + 1).$$
$$a - b(q + 1) = r - b < r.$$
$$a = bq + \text{ and } 0 \leq r < b$$

Step 4: Show that r and q are the only numbers with these properties. To prove uniqueness, we suppose that there are integers q_1 and r_1 such that $a = bq_1 + r_1$ and $0 \leq r_1 < b$, and prove that $q_1 = q$ and $r_1 = r$.