1.1 The Division Algorithm

The first portion of this course will be focused on ring theory; informally, a ring is a setting where we can do addition, subtraction, and multiplication. In many ways, the integers

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

are the prototypical example of a ring. Therefore we begin the course by noting some important properties of the integers. Later, we will try to generalize these properties to other rings. The first property we note is the fact that we can do division with remainder in $\mathbb{Z}$.

Well-Ordering Principle. The non-negative integers ($\mathbb{Z}_{\geq 0}$) are *well-ordered*, meaning that every non-empty subset of $\mathbb{Z}_{\geq 0}$ has a smallest element.

The fact that $\mathbb{Z}_{\geq 0}$ is well-ordered is intuitively obvious, because we have a simple algorithm for finding the smallest element in any subset S of $\mathbb{Z}_{\geq 0}$. Namely, if $0 \in S$ then 0 is the smallest element. Otherwise, if $1 \in S$ then 1 is the smallest element, and so on. Since S is non-empty, it is clear that this algorithm must eventually terminate.

Now we can use the well-ordering principle to prove the Division Algorithm. Recall that you learned how to divide a by b (with remainder) in elementary school. The theorem ensures that for any choice of a and b, it is always possible to perform division with remainder and get a valid answer. Furthermore, it also ensures that there is only one possible answer. (The theorem is traditionally referred to as the division algorithm, even though the theorem itself does not contain an actual algorithm for performing division, only the statement that we can perform division in theory.)

Theorem. ***(The Division Algorithm)*** *Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that*

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

The number q is called the *quotient* and r is called the *remainder.* Note that the remainder is always non-negative, even if a is negative. For example, if we want to divide -14 by 3, we write

$$-14 = 3 \cdot (-5) + 1,$$

so the quotient is -5 and the remainder is 1. (That is, when we divide a by b, we round a/b down to get the quotient. Here $-14/3 = -4.66\ldots$, so we round down to get a quotient of -5. This is different from the convention used in some programming languages, which round towards 0.)

The idea of the proof is essentially to use a child's algorithm for dividing by b by repeatedly subtracting off b. For example, if we want to divide 23 by 7, we subtract repeatedly:

$$\begin{aligned} 23 - 7 &= 16 \\ 16 - 7 &= 9 \\ 9 - 7 &= 2 \end{aligned}$$

Thus the remainder is $r = 2$; since we had to subtract off three 7's, the quotient is $q = 3$. Note that the above equations do in fact tell us that $23 = 7 \cdot 3 + 2$.

By repeatedly subtracting b, we are essentially looking at the numbers a, $a-b$, $a-2b$, $a-3b$, etc. Therefore, we begin our proof by looking at numbers of the form $a - bx$.

Proof. We first prove existence of q and r satisfying the theorem; we will worry about uniqueness afterward. Let

$$S = \{a - bx \mid x \in \mathbb{Z} \text{ and } a - bx \geq 0\}.$$

Note that S is non-empty, meaning that there is some integer x such that $a - bx \geq 0$; this is obvious, because $a - bx$ will be positive for any large negative x.

Since S is a non-empty set of non-negative integers, the Well-Ordering Principle ensures that S has a smallest element r. This means that $r = a - bq$ for some integer q. Therefore $a = bq + r$ as desired, so we need only check that $0 \leq r < b$. The fact that $r \in S$ ensures that $r \geq 0$. Since r is the minimal element of S, we know that $r - b \notin S$. But

$$r - b = (a - bq) - b = a - b(q + 1),$$

so this must mean that $r - b < 0$. Thus $r < b$, as we wanted to show.

Now we check uniqueness. Suppose that $a = bq_1 + r_1 = bq_2 + r_2$ for some $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ with $0 \leq r_1, r_2 < b$; we need to show that $q_1 = q_2$ and $r_1 = r_2$. We can see that

$$-b < r_1 - r_2 < b.$$

Since $r_1 - r_2 = b(q_2 - q_1)$, this says that

$$-b < b(q_2 - q_1) < b,$$

so $-1 < q_2 - q_1 < 1$. Since $q_2 - q_1 \in \mathbb{Z}$, it follows that $q_2 - q_1 = 0$, so $q_1 = q_2$. Therefore $r_1 - r_2 = b(q_2 - q_1) = 0$, so $r_1 = r_2$. □