LECTURE 7

The Division Algorithm

We are now ready to embark on our study of algebra. Our first task will be to look at the formal structures underlying basic arithmetic.

As usual let $\mathbb{Z}$ denote the set of all integers

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$$

and let $\mathbb{N}$ denote the set

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\} \quad .$$

of non-negative integers. (Strictly speaking, $\mathbb{N}$ is the union of the set of natural numbers $\{1, 2, 3, \ldots\}$ and $\{0\}$. Unfortunately the notion of natural numbers has more to do with historical precedence than mathematical convenience; in this course we shall henceforth presume the set $\mathbb{N}$ to include 0.)

We regard both $\mathbb{Z}$ and $\mathbb{N}$ to be endowed with the usual ordering of integers:

$$a > b \quad \Leftrightarrow \quad a \neq b \text{ and } a - b \in \mathbb{N}.$$

We shall also assume the Well Ordering Axiom:

Axiom 1 (The Well-Ordering Axiom). *Every non-empty subset $S \subseteq \mathbb{N}$ has a smallest element.*

The following theorem is the foundation of much of what we will do during the rest of the course.

Theorem 7.1 (The Division Algorithm). *Let a, b be integers with $b > 0$. Then there exists unique integers q and r such that*

(i) $a = bq + r \imath$
(ii) $0 \leq r < b$

Proof.

Let a, b be fixed integers with $b \neq 0$. Consider the set

$$S = \{z \in \mathbb{N} \mid z = a - bx \quad , \quad x \in \mathbb{Z}\} \quad .$$

We shall first show that this set S is non-empty: There are two possibilities:

(i) If $a \geq 0$, then $a - (b)(0) = a \geq 0$. So $a - bx$ is non-negative for $x = 0$ (when $a \geq 0$).
(ii) If $a < 0$, then $-a > 0$. Since b is a positive integer we must have

$$b \geq 1 \quad .$$

Multiplying the inequality above by the positive number $-a$ yields

$$-ab \geq -a$$

or equivalently

$$a - ab \geq 0 \quad .$$

So $a - bx$ is non-negative for $x = a$ (when $a < 0$).

Therefore the set S is non-empty.

Since S is a subset of $\mathbb{N}$, by the Well-Ordering Axiom, we know that S contains a smallest element; call it r. Since r is in S, r is of the form

$$r = a - bx$$

for some x; say $x = q$. Thus, we have found integers r and q such that

$$r = a - bq$$

or, equivalently,

$$a = bq + r \quad .$$

Since $r \in S$, we know that $r \geq 0$. We now show that $r < b$. Suppose on the contrary that $r \geq b$. Then

$$r - b \geq 0 \quad ,$$

so

$$0 \leq r - b = (a - bq) - b = a - b(q + 1).$$

Since $a - b(q + 1)$ is non-negative, it is an element of S by definition. But since b is positive, it is certainly true that

$$r - b < r \quad .$$

Thus,

$$r - b = (a - bq) - b = a - b(q + 1) < r \quad .$$

But r was to be the least element of S and the equation above seems to say that there is another element of S smaller than r. We have thus run into a contradiction. Therefore, $r < b$.

Hence we have found integers q and r such that $a = bq + r$ and $0 \leq r < b$.

To complete the proof, we must show that the numbers q and r found above are the **only** numbers with these properties. To do this, we suppose that there are two sets of integers r_1 , q_1 and r_2 , q_2 such that

$$bq_1 + r_1 = a = bq_2 + r_2 \tag{7.1}$$

with

$$0 \leq r_1 < b \quad \text{and} \quad 0 \leq r_2 < b \quad . \tag{7.2}$$

and then we will prove that necessarily $r_1 = r_2$ and $q_1 = q_2$.

Suppose $r_2 \geq r_1$. Then (7.1) implies

$$\begin{aligned} 0 &= bq_1 + r_1 - bq_2 - r_2 \\ &= b(q_1 - q_2) - (r_2 - r_1) \end{aligned}$$

or

$$b(q_1 - q_2) = r_2 - r_1 \quad . \tag{7.3}$$

Since, by hypothesis $b > 0$, and because we are supposing $r_2 \geq r_1$, $(q_1 - q_2)$ must be a non-negative integer. Therefore, $r_2 - r_1$ must be one of $0, b, 2b, 3b, \ldots$. But by (4)

$$0 \leq r_1 \leq r_2 < b \quad ,$$

so $r_2 - r_1$ must be zero. Therefore, $r_2 = r_1$. But this conclusion, together with (7.3) and the hypothesis $b > 0$, implies

$$q_1 - q_2 = 0$$

or $q_2 = q_1$.

A similar argument with the roles of r_2 and r_1 reversed proves the uniqeness of r and q in the case when when $r_1 \geq r_2$ and completes the proof of the theorem. ∎

Application. Show that if a is an odd integer, then a^2 has the form $8k + 1$ for some $k \in \mathbb{Z}$.

Well, if we apply the Division Algorithm with $b = 2$, we find we have only two possibilities for r: either

$$a = 2q + 0$$

or

$$a = 2q + 1 \quad .$$

Only in the latter case is a odd. So we can assume $a = 2q + 1$. But then

$$\begin{aligned} a^2 &= 4q^2 + 4q + 1 \\ &= 4(q^2 + q) + 1 \quad . \end{aligned}$$

Now recall that if q is odd, q^2 is odd; and so $q^2 + q$ is an even number. On the other hand, if q is even, then so is q^2 and also $q^2 + q$. Hence, in all cases,

$$q^2 + q = 2k$$

for some $k \in \mathbb{Z}$. Thus,

$$a^2 = 4(2k) + 1 = 8k + 1 \quad .$$

∎