The Division Algorithm

Theorem 1 (Division Algorithm)**.** *If a and b are integers with $b > 0$, then there exist integers q and r such that $a = qb + r$ and $0 \leq r < b$.*

The q and r given by the Division Algorithm are called the *quotient* and *remainder*, respectively. We will give two proofs of this result, one constructive and one nonconstructive, and compare them.

Proof. **Nonconstructive.** Our strategy is to use the Well-Ordering Property. To this end, define a set S of integers as follows.

$$S = \{a - qb \mid q \in \mathbb{Z}\} \cap \mathbb{N}.$$

First, note that $S \subseteq \mathbb{N}$ by definition. Next, we claim that S is not empty. To see this, note that $-a \leq |a| \leq |a|b$, since $1 \leq b$. Rearranging, we have

$$0 \leq a + |a|b = a - (-|a|)b,$$

so that in particular $a - (-|a|)b \in S$.

So S is a nonempty subset of $\mathbb{N}$. By WOP, S has a $\leq$-smallest element; say r. Now $0 \leq r$ and $r = a - qb$ for some integer q, so that $a = qb + r$.

Finally, we claim that $r < b$. To see this, assume by way of contradiction that $r \geq b$. Now $r - b \geq 0$, and moreover

$$r - b = a - qb - b = a - (q + 1)b.$$

Thus we have $r - b \in S$. However we also have $r > r - b$ (strict) since $b \geq 1$; this contradicts the minimalness of r in S. So our assumption that $r \geq b$ was false, and in fact $r < b$.

Thus we have found integers q and r such that $a = qb + r$ and $0 \leq r < b$. □

Proof. **Constructive.** We will consider two cases separately; first with $a \geq 0$ and second with $a < 0$.

- Let B be the set

  $$B = \{a \in \mathbb{N} \mid a = qb + r \text{ for some } q, r \in \mathbb{N} \text{ with } 0 \leq r < b\}.$$

  We claim that $B = \mathbb{N}$. Our strategy is to use the Principle of Mathematical Induction.

  - **Base Case.** Note that $0 = 0 \cdot b + 0$. Letting $q = r = 0$, we have $0 \in B$.
  - **Inductive Step.** Suppose that $a - 1 \in B$. That is, for any integer b, there exist integers q' and r' such that $a - 1 = q'b + r'$ and $0 \leq r' < b$. If $a = b$, then letting $q = 1$ and $r = 0$ we have $a \in B$. If $a < b$, then letting $q = 0$ and $r = a$ we have $a \in B$. Otherwise, there are two possibilities: either $r' + 1 < b$ or $r' + 1 \geq b$.

-
    -
        - Suppose $r' + 1 < b$. Then $a = q'b + r' + 1$ and $0 \leq r' + 1 < b$. Letting $q = q'$ and $r = r' + 1$, we have $a \in B$.
        - Suppose $r' + 1 \geq b$. Then in fact we must have $r' + 1 = b$. Now $a = q'b + r' + 1 = q'b + b = (q' + 1)b$. Letting $q = q' + 1$ and $r = 0$, we have $a \in B$.

  By PMI, $B = \mathbb{N}$. That is, if $a \geq 0$ then there exist integers q and r such that $a = qb + r$ and $0 \leq r < b$.

- Now suppose $a < 0$, so that $-a > 0$. By the previous discussion, there exist integers q' and r' such that $-a = q'b + r'$ and $0 \leq r' < b$. There are two possibilities: either $r' = 0$ or $r' > 0$.
    - Suppose $r' = 0$. Now $a = -q'b$. Letting $q = -q'$ and $r = 0$ we have $a = qb + r$ with $0 \leq r < b$.
    - Suppose $r' > 0$. Now

      $$a = -q'b - r' = -q'b - b + b - r' = (-q' - 1)b + b - r'.$$

      Moreover, note that $0 \leq b - r' < b$; the left inequality because $r' < b$, and the right because $r' > 0$. Letting $q = -q' - 1$ and $r = b - r'$ we have q and r so that $a = qb + r$ and $0 \leq r < b$. □

Remarks

Different proofs of the same result using different strategies, as we have here, can frequently offer different insights into "why" the result is true.

- The constructive proof is tedious, requiring several different case analyses. (This is when a proof splits into cases.) Generally a brute-force case analysis is seen as the least enlightening kind of proof. On the other hand, this is called a constructive proof because it gives us a strategy – an *algorithm* – to actually *find* the integers q and r. Given particular a and b, we can find q and r by tracing through the cases of the proof.

- The nonconstructive proof is short and sweet (the technical term for this is *elegant*), especially compared to the constructive proof. Logically it is much less complicated. It also does not depend as much on the details of $\mathbb{Z}$, and so is easier to generalize to other situations. However, it tells us nothing about how to *find* the q and r; it guarantees their existence, but offers no computational guidance.

These two proofs are a great example of the difference between the two major points of view in algebra – abstract and concrete. Abstraction can bring elegance and concision by throwing away unnecessary detail at the expense of computability, while keeping it concrete allows us to compute in exchange for getting our hands a little dirty, so to speak.

Corollaries

Two important corollaries of the Division Algorithm will be useful later.

Corollary 2. *If a and b are integers with $b \neq 0$, then there exist integers q and r such that $a = qb + r$ and $0 \leq r < |b|$.*

Proof. If $b < 0$, then $-b > 0$. Using the Division Algorithm find q' and r' such that $a = q'(-b) + r'$ and $0 \leq r' < -b$. Let $q = -q'$ and $r = r'$. □

Corollary 3. *The q and r given by the Division Algorithm are unique in the following sense; if $a = qb + r$ and $a = q'b + r'$ and $0 \leq r, r' < |b|$, then $q = q'$ and $r = r'$.*

Proof. Note that $-|b| < -r' \leq 0$, so that $-|b| < r - r' < |b|$. In particular we have $|r - r'| < |b|$. On the other hand we have $qb + r = q'b + r'$, so that $r - r' = b(q' - q)$ and thus $|r - r'| = |b||q' - q|$. Thus $|b||q' - q| < |b|$, and so $|q' - q| < 1$. Thus $q' = q$. Now $r = a - qb = a - q'b = r'$. □