The Division Algorithm

Ryan C. Daileda

Trinity University

Intro to Abstract Mathematics

Long Division

Consider the following garden variety long division problem.

Example 1

Find the quotient and remainder when 4982 is divided by 11.

$$
\begin{array}{r|rrrr}
 & & 4 & 5 & 2 \\ \cline{2-5}
11 & 4 & 9 & 8 & 2 \\
 & 4 & 4 & & \\ \cline{2-5}
 & & 5 & 8 & \\
 & & 5 & 5 & \\ \cline{3-5}
 & & & 3 & 2 \\
 & & & 2 & 2 \\ \cline{4-5}
 & & & 1 & 0
\end{array}
$$

So the quotient is $\boxed{452}$ and the remainder is $\boxed{10}$.

Questions

Q1. What do the quotient (452) and remainder (10) mean?

Ans. If we try to divide 4982 (the *dividend*) into groups of size 11 (the *divisor*), there will be 452 groups with 10 units left over.

Q2. What specific relationship between 11, 4982, 452 and 10 is guaranteed by the long division process?

Ans. $4982 = 452 \times 11 + 10$ or, more generally,

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

Q3. What can you say about the size of the remainder?

Ans. $0 \leq 10 < 11$. The remainder is nonnegative and smaller than the divisor.

The Division Algorithm

The existence of quotients and remainders in general is guaranteed by the next fundamental result.

Theorem 1 (The Division Algorithm)

Let $m \in \mathbb{N}^+$. For each $n \in \mathbb{N}$ there exist unique $q, r \in \mathbb{N}$ so that

$$n = qm + r \quad \text{and} \quad 0 \leq r < m.$$

Remarks.

1. Here m is the *divisor*, n is the *dividend*, q is the *quotient* and r is the *remainder* (when n is *divided by* m).
2. Uniqueness means that for each n there is *only one pair* (q, r) satisfying the conclusions of the theorem.

Example

The following is a nice application of the uniqueness of quotients and remainders.

Example 2

Let $m \in \mathbb{N}^+$ and $n \in \mathbb{N}$. Prove that $m|n$ if and only if $r = 0$ in the division algorithm.

Proof. ($\Leftarrow$) Use the div. alg. to write $n = qm + r$ with $q, r \in \mathbb{N}$.

If $r = 0$, then $n = qm$ and hence $m|n$.

($\Rightarrow$) Suppose $m|n$. Then $n = am = \underbrace{am + 0}_{qm+r}$ for some $a \in \mathbb{N}$.

Since $0 < m$, the uniqueness of quotients and remainders implies that $q = a$ and $r = 0$ in the div. alg. □

More Remarks

The condition $0 \leq r < m$ is equivalent to $r \in \{0, 1, 2, \ldots, m-1\}$.

The remainder r tells us *precisely* what “goes wrong” when m fails to divide n.

Modular arithmetic is concerned with how remainders behave under arithmetic operations.

The div. alg. can be used as a substitute for exact divisibility in applications (specifically *Bézout’s lemma*).

The div. alg. is easily implemented on a hand calculator:
$q = \text{floor}(n/m)$ and $r = n - qm$.

Recall

We now turn to proving the division algorithm. We first recall two recently discussed results that will be necessary for our proof.

Axiom (The Well-Ordering Principle)

Every nonempty subset of $\mathbb{N}$ has a least element.

Lemma 1

Let $m \in \mathbb{N}^+$ and $n \in \mathbb{N}$. There is an $a \in \mathbb{N}^+$ so that $am > n$.

Remarks.

1. Remember, the Well-Ordering Principle can only be asserted, it *cannot* be proven.
2. We proved Lemma 1 in class shortly before the break.

Proof of the Division Algorithm: Existence

Let $n \in \mathbb{N}$ and define

$$S = \{t \in \mathbb{N} \mid tm > n\}.$$

By Lemma 1, $S \subset \mathbb{N}$ is nonempty.

S therefore has a least element $t_0 \in S$.

Let $q = t_0 - 1$ and set $r = n - qm$. Then $n = qm + r$ by construction.

By our choice of q we have $qm \leq n < (q+1)m$, so that

$$0 \leq \underbrace{n - qm}_{r} < m.$$

This establishes the *existence* of q and r.

Proof of the Division Algorithm: Uniqueness

Suppose we have a second pair $q', r' \in \mathbb{N}$ with $n = q'm + r'$ and $0 \leq r' < m$.

Then $r - r' = m(q' - q)$. Thus $m | r - r'$.

But $-m < r - r' < m$ as $0 \leq r, r' < m$. This implies $r - r' = 0$.

We then have $0 = m(q' - q)$ with $m \neq 0$. Hence $q' - q = 0$.

We conclude that $r = r'$ and $q = q'$. This proves the *uniqueness* of q and r. □