The Division Algorithm

Learning Objectives. By the end of class, students will be able to:

- Prove existence and uniqueness for the Division Algorithm
- Prove existence and uniqueness for the general Division Algorithm .

Read: Ernst Section 2.2 and Section 2.4

Turn in: Ernst, Problem 2.59 and 2.64

Instructor Notes: Go over reading assignment at the start of class.

This section introduces the division algorithm, which will come up repeatedly throughout the semester, as well as the definition of divisors from last class.

First, let's define a *lemma.* A lemma is a minor result whose sole purpose is to help in proving a theorem, although some famous named lemmas have become important results in their own right.

Definition (greatest integer (floor) function)**.** Let $x \in \mathbb{R}$. The *greatest integer function of* x, denoted $[x]$ or $\lfloor x \rfloor$, is the greatest integer less than or equal to x.

Lemma 1. Let $x \in \mathbb{R}$. Then $x - 1 < [x] \leq x$.

Proof By the definition of the floor function, $[x] \leq x$.

To prove that $x - 1 < [x]$, we proceed by contradiction. Assume that $x - 1 \geq [x]$ (the negation of $x - 1 < [x]$). Then, $x \geq [x] + 1$. This contradicts the assumption that $[x]$ is the greatest integer *less than or equal to* x. Thus, $x - 1 < [x]$. ■

Theorem 1 (Division Algorithm)**.** Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists a unique $q, r \in \mathbb{Z}$ such that

$$a = bq + r, \quad 0 \leq r < b.$$

Before proving this theorem, let's think about division with remainders, ie long division. The quotient q should be the largest integer such that $bq \leq a$. If we divide both sides by b, we have $q \leq \frac{a}{b}$. We have a function to find the greatest integer less than or equal to $\frac{a}{b}$, namely $q = \left\lfloor \frac{a}{b} \right\rfloor$. If we rearrange the equation $a = bq + r$, we gave $r = a - bq$. This is our scratch work for existence.

Proof Let $a, b \in \mathbb{Z}$ with $b > 0$. Define $q = \left\lfloor \frac{a}{b} \right\rfloor$ and $r = a - b \left\lfloor \frac{a}{b} \right\rfloor$. Then $a = bq + r$ by rearranging the equation. Now we need to show $0 \leq r < b$.

Since $x - 1 < \lfloor x \rfloor \leq x$ by Lemma **??**, we have

$$\frac{a}{b} - 1 < \left\lfloor \frac{a}{b} \right\rfloor \leq \frac{a}{b}.$$

Multiplying all terms by $-b$, we get

$$-a + b > -b \left\lfloor \frac{a}{b} \right\rfloor \geq -a.$$

Learning outcomes:
Author(s): Claire Merriman

Adding a to every term gives

$$b > a - b\left\lfloor \frac{a}{b} \right\rfloor \geq 0.$$

By the definition of r, we have shown $0 \leq r < b$.

Finally, we need to show that q and r are unique. Assume there exist $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ with

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b$$

$$a = bq_2 + r_2, \quad 0 \leq r_2 < b.$$

We need to show $q_1 = q_2$ and $r_1 = r_2$. We can subtract the two equations from each other.

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

Rearranging, we get $b(q_1 - q_2) = r_2 - r_1$. Thus, $b \mid r_2 - r_1$. From rearranging the inequalities:

$$\begin{aligned} 0 &\leq r_2 < b \\ -b &< -r_1 \leq 0 \\ -b &< r_2 - r_1 < b. \end{aligned}$$

Thus, the only way $b \mid r_2 - r_1$ is that $r_2 - r_1 = 0$ and thus $r_1 = r_2$. Now, $0 = b(q_1 - q_2) + (r_1 - r_2)$ becomes $0 = b(q_1 - q_2)$. Since we assumed $b > 0$, we have that $q_1 - q_2 = 0$. ■

In-class Problem 1 Use the **??** on $a = 47, b = 6$ and $a = 281, b = 13$.

Solution: For $a = 47, b = 6$, we have that $a = (7)6 + 5, q = 7, r = 5$. For $a = 281, b = 13$, we have that $a = (21)13 + 8, q = 21, r = 8$.

Corollary 1. Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exists a unique $q, r \in \mathbb{Z}$ such that

$$a = bq + r, \quad 0 \leq r < |b|.$$

One proof method is using an existing proof as a guide.

In-class Problem 2 Let a and b be nonzero integers. Prove that there exists a unique $q, r \in \mathbb{Z}$ such that

$$a = bq + r, \quad 0 \leq r < |b|.$$

(a) Use the **??** to prove this statement as a corollary. That is, use the *conclusion* of the **??** as part of the proof. Use the following outline:

(i) Let a and b be nonzero integers. Since $|b| > 0$, the **??** says that there exist unique $p, s \in \mathbb{Z}$ such that $a = p|b| + s$ and $0 \leq s < |b|$.

(ii) There are two cases:

i. When $b > 0$, the conditions are already met and $r = s$ and $q = answer b$.

ii. Otherwise, $b < 0$, $r = s$ and $q = answer - b$. .

(iii) Since both cases used that the p, s are unique, then q, r are also unique

(b) Use the *proof* of the **??** as a template to prove this statement. That is, repeat the steps, adjusting as necessary, but do not use the conclusion.

(i) In the proof of the **??**, we let $q = \left\lfloor \frac{a}{b} \right\rfloor$. Here we have two cases:

i. When $b > 0$, $q = \left\lfloor \frac{a}{b} \right\rfloor$ and $r = a - bq$.

ii. When $b < 0$, $q = -\left\lfloor \frac{a}{b} \right\rfloor$ and $r = a - bq$.

(ii) Follow the steps of the *proof* of the **??** to finish the proof.