Monday, January 29: More algebraic proofs and the Euclidean algorithm

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

- Understand turning scratch work into proof for algebraic proofs
- Approach the floor function problems from Homework 1
- Prove the Euclidean algorithm halts and generates the greatest common divisor of two positive integers .

Read None

Turn in The Learn TeX assignment using a copy of the Homework Template.

Example of proof like the floor function

Remark 1. *This section was a response to a misconception on the homework. If keeping, it is best to come up with a better example and move to right after Lemma* **??**

Let's explicitly think about the floor function as a function. That is, $f(x) : \mathbb{R} \to \mathbb{Z}$ (a function from the real numbers to the integers). Here is a restatement of the homework problem:

Homework Problem. For each of the following equations, find a domain for $f(x) = \lfloor x \rfloor$ make the statement true. Prove your statement.

(a) $f(x) + f(x) = f(2x)$

(b) $f(x + 3) = 3 + f(x)$

(c) $f(x + 3) = 3 + x$

Here is a similar problem with proofs where $g : \mathbb{R} \to \mathbb{R}$. Note that the scratch work is one way to think about solving the problem but would not be included in the homework writeup.

Example 1. *For each of the following equations, find the full domain for $g(x) = 3\sin(\pi x)$ that makes the statement true. Prove that the equation is always true on this domain.*

(a) $g(x) + g(x) = g(2x)$

Scratch Work. We want to find a restriction such that $3\sin(\pi x) + 3\sin(\pi x) = 3\sin(2\pi x)$. Using the double angle formula, we get

$$3\sin(2\pi x) = 6\sin(\pi x)\cos(2\pi x).$$

This means we are actually looking for

$$\begin{aligned} 6\sin(\pi x)\cos(2\pi x) &= 6\sin(\pi x) \\ \cos(2\pi x) &= 1. \end{aligned}$$

Solution: *If $x \in \mathbb{Z}$, then $g(x) + g(x) = g(2x)$.*

Proof *Let $x \in \mathbb{Z}$. Then $g(x) + g(x) = 3\sin(\pi x) + 3\sin(\pi x) = 0$ and $g(2x) = 3\sin(2\pi x) = 0$. Thus, $g(x) + g(x) = g(2x)$.* ■

(b) $g(x + 3) = 3 + g(x)$

Scratch Work. We want to find a restriction such that $3\sin(\pi(x+3)) = 3+3\sin(\pi x)$. Using the angle addition formula, we get

$$3\sin(\pi x + 3\pi)) = 3\sin(\pi x)\cos(3\pi) + 3\cos(\pi x)\sin(3\pi) = -3\sin(\pi x).$$

This means we are actually looking for

$$\begin{aligned} -3\sin(\pi x) &= 3\sin(\pi x) + 3 \\ -1 &= 2\sin(\pi x) \\ &. \end{aligned}$$

Solution: *If $x = 2k + \frac{7}{6}$ or $x = 2k - \frac{1}{6}$ for some $k \in \mathbb{Z}$, then $g(x+3) = g(x) + 3$.*

Proof *Note that $g(x+3) = 3\sin(\pi x + 3\pi) = -3\sin(\pi x)$ by the angle addition formula. We will consider two cases:*

Case 1: Let $x = 2k + \frac{7}{6}$ for some $k \in \mathbb{Z}$. Then

$$\begin{aligned} g(x+3) &= -3\sin(\pi x) \\ &= -3\sin(2k\pi + \frac{7\pi}{6}) \\ &= \frac{3}{2}, \end{aligned}$$

and $g(x) + 3 = 3\sin(2k\pi + \frac{7\pi}{6}) + 3 = \frac{3}{2}$.

Case 2: Let $x = 2k - \frac{1}{6}$ for some $k \in \mathbb{Z}$. Then

$$\begin{aligned} g(x+3) &= -3\sin(\pi x) \\ &= -3\sin(2k\pi - \frac{\pi}{6}) \\ &= \frac{3}{2}, \end{aligned}$$

and $g(x) + 3 = 3\sin(2k\pi - \frac{\pi}{6}) + 3 = \frac{3}{2}$.

Thus, $g(x+3) = g(x) + 3$ when $x = 2k + \frac{7}{6}$ or $x = 2k - \frac{1}{6}$ for some $k \in \mathbb{Z}$. ■

(c) *Let $h(x) = x^2 - 1$. For each of the following equations, find the full domain for $h(x)$ that makes the statement true. Prove your statement.*

(i) $h(x+3) = h(x) + 3$

(ii) $h(x+3) = x + 3$

Scratch Work. First, $h(x+3) = (x+3)^2 - 1 = x^2 + 6x + 8$.

For (a)

$$\begin{aligned} x^2 + 6x + 8 &= x^2 - 1 + 3 \\ 6x &= -6 \end{aligned}$$

For (b)

$$\begin{aligned} x^2 + 6x + 8 &= x + 3 \\ x^2 + 5x + 5 &= 0 \\ x &= \frac{-5 \pm \sqrt{5}}{2} \end{aligned}$$

Solution: (i) *For $h(x) = x^2 - 1$, $h(x+3) = h(x) + 3$ if and only if $x = -1$.*

Proof *Let $h(x) = x^2 - 1$ and $x = -1$. Then $h(x+3) = 3 = 0 + 3 = h(x) + 3$.*

To prove that this is the only such x, let $h(x+3) = h(x) + 3$. Then $x^2 + 6x + 8 = x^2 + 2$, which simplifies to $x = -1$. ■

(ii) *For $h(x) = x^2 - 1$, $h(x+3) = x + 3$ if and only if $x = \dfrac{-5 \pm \sqrt{5}}{2}$.*

Proof *Let $h(x) = x^2 - 1$. First we consider the case $x = \dfrac{-5 + \sqrt{5}}{2}$. Then $h(x+3) = \dfrac{1 + \sqrt{5}}{2} = \dfrac{-5 + \sqrt{5}}{2} + 3 = x + 3$.*

Next, we consider the case $x = \dfrac{-5 - \sqrt{5}}{2}$. Then $h(x+3) = \dfrac{1 - \sqrt{5}}{2} = \dfrac{-5 - \sqrt{5}}{2} + 3 = x + 3$.

To prove that these are the only such x, let $h(x+3) = x + 3$. Then $x^2 + 6x + 8 = x + 3$, which hasthe solutions $x = \dfrac{-5 \pm \sqrt{5}}{2}$. ■

The Euclidean algorithm

Typically by *Euclidean algorithm*, we mean both the algorithm and the theorem that the algorithm always generates the greatest common divisor of two (positive) integers.

Theorem 1 (Euclidean algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$. By the division algorithm, there exist $q_1, r_1 \in \mathbb{Z}$ such that*

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

If $r_1 > 0$, there exist $q_2, r_2 \in \mathbb{Z}$ such that

$$b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1.$$

If $r_2 > 0$, there exist $q_3, r_3 \in \mathbb{Z}$ such that

$$r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2.$$

Continuing this process, $r_n = 0$ for some n. If $n > 1$, then $\gcd(a, b) = r_{n-1}$. If $n = 1$, then $\gcd(a, b) = b$.

Proof Note that $r_1 > r_2 > r_3 > \cdots \geq 0$ by construction. If the sequence did not stop, then we would have an infinite, decreasing sequence of positive integers, which is not possible. Thus, $r_n = 0$ for some n.

When $n = 1$, $a = bq + 0$ and $\gcd(a, b) = b$.

Lemma 1.12 states that for $a = bq_1 + r_1$, $\gcd(a, b) = \gcd(b, r_1)$. This is because any common divisor of a and b is also a divisor of $r_1 = a - bq_1$.

If $n > 1$, then by repeated application of the Lemma 1.12, we have

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1})$$

Then $r_{n-2} = r_{n-1} q_n + 0$. Thus $\gcd(r_{n-2}, r_{n-1}) = r_{n-1}$. ■

When using the Euclidean algorithm, it can be tricky to keep track of what is happening. Doing a lot of examples can help.

Wednesday, January 31: Practice with the Euclidean algorithm and the Fundamental Theorem of Arithmetic

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

- Use the (extended) Euclidean algorithm to write (a, b) as a linear combination of a and b
- Prove the Fundamental Theorem of Arithmetic
- Prove $\sqrt{2}$ is irrational.

Read Strayer, Section 1.5 through Proposition 1.17

Turn in

- Answer these questions about the proof of the Fundamental Theorem of Arithmetic (taken from Helping Undergraduates Learn to Read Mathematics):
  - Can you write a brief outline (maybe 1/10 as long as the theorem) giving the logic of the argument – proof by contradiction, induction on n, etc.? (This is KEY.)
  - What mathematical raw materials are used in the proof? (Do we need a lemma? Do we need a new definition? A powerful theorem? and do you recall how to prove it? Is the full generality of that theorem needed, or just a weak version?)
  - What does the proof tell you about why the theorem holds?
  - Where is each of the hypotheses used in the proof?
  - Can you think of other questions to ask yourself?
- Strayer states that the proof of Proposition 1.17 is "obvious from the Fundamental Theorem of Arithmetic and the definitions of (a, b) and $[a, b]$." Is this true? If so, why? If not, fill in the gaps.

Solution: Answers to both questions will vary between students.

Practice with the Euclidean algorithm

Work in pairs to answer the following. Each pair will be assigned parts the following question.

In-class Problem 1 *Find the greatest common divisors of the pairs of integers below and write the greatest common divisor as a linear combination of the integers.*

32(b) $(32, 56)$

54(b) $(78, 708)$

Fundamental Theorem of Arithmetic

Theorem 2 (Fundamental Theorem of Arithmetic)**.** *Every integer greater than one can be written in the form* $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ *where the* p_i *are distinct prime numbers and the* a_i *are positive integers. This factorization into primes is unique up to the ordering of the terms.*

Alternate proof for existence We will show that every integer n greater than 1 has a prime factorization. First, note that all primes are already in the desired form. We will use induction to show that every composite integer can be factored into the product of primes. When $n = 4$, we can write $n = 2^2$, so 4 has the desired form.

Assume that for all integers k with $1 < k < n$, k can be written in the form $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ where the p_i are distinct prime numbers and the a_i are positive integers. If n is prime, we are done, otherwise there exists $a, b \in \mathbb{Z}$ with $1 < a, b < n$ such that $n = ab$. By the induction hypothesis, there exist primes $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ and positive integers $a_1, a_2, \ldots, a_r, b_1, b_2, \ldots b_s$ such that $a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ and $b = q_1^{b_1} q_2^{a_2} \cdots q_s^{b_a}$. Then

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} q_1^{b_1} q_2^{a_2} \cdots q_s^{b_a}.$$

■

We will use an idea similar to the proof of the Fundamental Theorem of Arithmetic to proof the following:

In-class Problem 2

Proposition. $\sqrt{2}$ *is irrational*

As class, put the steps of the proof in order, then fill in the missing information.

In-class Problem 3 [1] *Let p be prime.*

(a) *If $(a, b) = p$, what are the possible values of (a^2, b)? Of (a^3, b)? Of (a^2, b^3)?*

Solution: *If $(a, b) = p$, then there exist $j, k \in \mathbb{Z}$ such that $a = pj, b = pk$, and $p \nmid j$ or $p \nmid k$ (otherwise $(a, b) = p^2$).*

$$a^2 = p^2 j^2, \quad a^3 = p^3 j^3, \quad b^3 = p^3 k^3$$

Then (a^2, b) is p if $p \nmid k$ or p^2 if $p \mid k$; and (a^3, b) is p if $p \nmid k$, p^2 if $p \mid k$ and $p^2 \nmid k$, or p^3 if $p^2 \mid k$.

If $p \mid j$, then $p \nmid k$ and $(a^2, b^3) = p^3$. If $p \nmid j$, then $(a^2, b^3) = p^2$.

(b) *If $(a, b) = p$ and $(b, p^3) = p^2$, find (ab, p^4) and $(a + b, p^4)$.*

Solution: *There exists $j, k \in \mathbb{Z}$ such that $a = pj, b = p^2 k$, and $p \nmid k, p \nmid k$. Then $ab = p^3 jk$ and $a + b = pj + p^2 k = p(j + pk)$. Thus, $(ab, p^4) = p^3$ and $(a + b, p^4) = p$.*

Friday, February 2: Quiz 2, Greatest Common Divisors and Diophantine Equations

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

- Prove the formula for integer solutions to $ax + by = c$.
- State when integer solution exist for $a_1 x_1 + \cdots + a_k x_k = c$. .

Read Strayer, Section 6.1

Turn in Exercise 2a. Find all integer solutions to $18x + 28y = 10$

[1] Not done 2024

Quiz (10 minutes)

More greatest common divisor

Lemma 3. *Let $a, b, c \in \mathbb{Z}$, with $a \neq 0$. Then $(a, b, c) = ((a, b), c)$.*

Proof Let $a, b, c \in \mathbb{Z}$, with $a \neq 0$. Define $d = (a, b, c)$ and $e = ((a, b), c)$. We will show that $d \mid e$ and $e \mid d$. Since the greatest common divisor is positive, we can conclude that $d = e$.

Since $d = (a, b, c)$, we know $d \mid a$, $d \mid b$, and $d \mid c$. By the lemma we are about to prove, $d \mid (a, b)$. Thus, d is a common divisor of (a, b) and c, so $d \mid e$.

Since $e = ((a, b), c)$, $e \mid (a, b)$ and $e \mid c$. Since $e \mid (a, b)$, we know $e \mid a$ and $e \mid b$ by the same lemma. Thus, e is a common divides of a, b and c ■

Lemma 4. *Let $a, b \in \mathbb{Z}$, not both zero. Then any common divisor of a and b divides the greatest common divisor.*

Proof Let $a, b \in \mathbb{Z}$, not both zero. By Proposition 1.11, $(a, b) = am + bn$ for some $n, m \in \mathbb{Z}$. Thus, $d \mid (a, b)$ by linear combination. ■

Lemma 5. *Let $a, b \in \mathbb{Z}$, not both zero. Then any divisor of (a, b) is a common divisor of a and b.*

Proof Let c be a divisor of (a, b). Since $(a, b) \mid a$ and $(a, b) \mid b$, then $c \mid a$ and $c \mid b$ by transitivity. ■

Proposition. *Let $a_1, \ldots, a_n \in \mathbb{Z}$ with $a_1 \neq 0$. Then*

$$(a_1, \ldots, a_n) = ((a_1, a_2, a_3, \ldots, a_{n-1}), a_n).$$

Proof Let $k = 2$. The since $((a_1, a_2)) = (a_1, a_2)$ by the definition of greatest common divisor of one integer, $(a_1, a_2) = ((a_1, a_2))$. The $k = 3$ case is Lemma 3 in this section.

Assume that for all $2 \leq k < n$,

$$(a_1, \ldots, a_k) = ((a_1, a_2, a_3, \ldots, a_{k-1}), a_k).$$

Let $d = (a_1, a_2, a_3, \ldots, a_k)$, $e = ((a_1, a_2, a_3, \ldots, a_k), a_{k+1}) = (d, a_{k+1})$, and $f = (a_1, a_2, a_3, \ldots, a_k, a_{k+1})$. We will show that $e \mid f$ and $f \mid e$. Since both e and f are positive, this will prove that $e = f$.

Note that $e \mid (a_1, a_2, a_3, \ldots, a_k)$ and $e \mid a_{k+1}$ by definition. Since $(a_1, \ldots, a_k) = ((a_1, a_2, a_3, \ldots, a_{k-1}), a_k)$ by the induction hypothesis, $e \mid (a_1, a_2, a_3, \ldots, a_{k-1})$ and $e \mid a_k$ by Lemma 5. Again, by the induction hypothesis, $(a_1, a_2, a_3, \ldots, a_{k-1}) = ((a_1, a_2, a_3, \ldots, a_{k-2}), a_{k-1})$, so $e \mid a_{k-1}$ and $e \mid (a_1, a_2, a_3, \ldots, a_{k-2})$ by Lemma 5. Repeat this process until we get $(a_1, a_2, a_3) = ((a_1, a_2), a_3)$, so $e \mid a_3$ and $e \mid (a_1, a_2)$ by Lemma 5. Thus $e \mid a_1, a_2, \ldots, a_{k+1}$ by repeated applications of Lemma 5. By the generalized version of the Lemma 4 on Homework 3, $e \mid f$.

To show that $f \mid e$, we note that $f \mid a_1, a_2, \ldots, a_k, a_{k+1}$ by definition. Then $f \mid d$ by the generalized version of the Lemma 4 on Homework 3. Since $e = (d, a_k)$, we have that $f \mid e$ by Lemma 4. ■