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 $a_1x_1 + \cdots + a_kx_k = c$. .

Instructor Notes: **Read** Strayer, Section 6.1

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

Lemma 1. *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 Lemma 2, which 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 Lemma 2. Thus, e is a common divides of a, b and c ■

Lemma 2. *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 **??**, $(a, b) = am + bn$ for some $n, m \in \mathbb{Z}$. Thus, $d \mid (a, b)$ by linear combination.* ■

Lemma 3. *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 1. *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 **??** of one integer, $(a_1, a_2) = ((a_1, a_2))$. The $k = 3$ case is the first lemma in this section (1).*

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 3. 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 3. 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 3. Thus $e \mid a_1, a_2, \ldots, a_{k+1}$ by repeated applications of Lemma 3. By the generalized version of the Lemma 2 on Homework 3, $e \mid f$.

Learning outcomes:
Author(s): Claire Merriman
This is not true in general and a common mistake. In general $d = \pm e$

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 2 on Homework 3. Since* $e = (d, a_k)$*, we have that* $f \mid e$ *by Lemma 2.* ■