Greatest Common Divisors

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

- Define the greatest common divisor of two integers
- Prove basic facts about the greatest common divisor .

Definition (greatest common divisor)**.** If $a \mid b$ and $a \mid c$ then a is a *common divisor* of b and c.

If at least one of b and c is not 0, the greatest (positive) number among their common divisors is called the *greatest common divisor of a and b* and is denoted $gcd(a, b)$ or just (a, b).

If $gcd(a, b) = 1$, we say that a and b are *relatively prime.*

If we want the greatest common divisor of several integers at once we denote that by $\gcd(b_1, b_2, b_3, \ldots, b_n)$.

For example, $\gcd(4, 8)$ is 4 but $\gcd(4, 6, 8)$ is 2.

The GCD always exists when at least one of the integers is nonzero. How to show this: 1 is always a divisor, and no divisor can be larger than the maximum of $|a|, |b|$. So there is a finite number of divisors, thus there is a maximum.

Proposition 1 (Bézout's Identity)**.** Let $a, b \in \mathbb{Z}$ with a and b not both zero. Then

$$\{(a, b) = \min\{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\}.$$

This proof brings together definitions (of greatest common divisor), previous results (**??**, factors of linear combinations), the well-ordering principle, and some methods for minimum and maximum/greatest.

Proof Since $a, b \in \mathbb{Z}$ are not both zero, at least one of $1a + 0b, -1a + 0b, 0a + 1b, 0a + (-1)b$ is in $\{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\}$. Therefore, the set is nonempty and has a minimal element by the **??**. Call this element d, and $d = xa + yb$ for some $x, y \in \mathbb{Z}$.

First we will show that $d \mid a$. By the **??**, there exist unique $q, r \in \mathbb{Z}$ such that $a = qd + r$ with $0 \leq r < d$. Then,

$$r = a - qd = a - q(xa + yb) = (1 - qx)a - qyb,$$

so r is an integral linear combination of a and b. Since d is the least positive such integer, $r = 0$ and $d \mid a$. Similarly, $d \mid b$.

It remains to show that d is the *greatest* common divisor of a and$b$. Let $c$be any common divisor of a and b. Then $c \mid ax + by = d$, so $c \mid d$. ■

Since we assume a and b are not both zero, we could also simplify the first sentence using *without loss of generality.* Since there is no difference between a and b, we can assume $a \neq 0$.

Learning outcomes:
Author(s): Claire Merriman