Bézout's Lemma

Ryan C. Daileda

Trinity University

Intro to Abstract Mathematics

Bézout's Lemma

As an application of the Well-Ordering Principle and the Division Algorithm we will prove the following important number-theoretic result.

Theorem 1 (Bézout's Lemma)

Let $a, b \in \mathbb{N}^+$. There exist $x, y \in \mathbb{Z}$ so that

$$\gcd(a, b) = xa + yb.$$

Example. We have $\gcd(212, 64) = 4$ and

$$4 = \underbrace{-3}_{x} \cdot 212 + \underbrace{10}_{y} \cdot 64.$$

Remarks

1. Bézout's Lemma is an existence statement. We will give an *nonconstructive proof*: it will ensure that x and y exist, but will not tell us how to find them.

2. A *constructive proof* of Bézout's Lemma can be derived from the *Euclidean algorithm*.

3. Bézout's Lemma is the key ingredient in the proof of *Euclid's Lemma*, which states that if $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.

4. Euclid's Lemma, in turn, is essential to the proof of the *Fundamental Theorem of Arithmetic*.

Proof of Bézout's Lemma

We know $\gcd(a, b)$ divides *every* $\mathbb{Z}$-linear combination $xa + yb$.

So $\gcd(a, b)$ must be $\leq$ *every* (pos.) $\mathbb{Z}$-linear combination $xa + yb$.

So if we expect $\gcd(a, b)$ to *equal* one such $xa + yb$, it must be the least possible. This motivates our proof.

Proof. Let $S = \{xa + yb \,|\, x, y \in \mathbb{Z} \text{ and } xa + yb > 0\}$.

Then $S \subset \mathbb{N}$ (by construction) and $S \neq \varnothing$ ($a \in S$, for instance).

By WOP S has a least element $m \in S$.

Outline of the Argument

Let $d = \gcd(a, b)$. We will show that:

1. $d|m$;
2. m is a common divisor of a and b.

Item **1** implies that $d \leq m$.

Because d is the *greatest* common divisor of a and b, item **2** implies $m \leq d$.

Together these tell us that $d = m$.

Since $m = xa + yb$ for some $x, y \in \mathbb{Z}$ (remember that $m \in S$), this will complete the proof.

The Details

d divides m:

Since $d|a$ and $d|b$, it follows from HW that $d|xa + yb$ for any $x, y \in \mathbb{Z}$.

This means d divides every element of S. So $d|m$.

m divides a:

Use the div. alg. to write $a = qm + r$ with $0 \leq r < m$.

Assume, for the sake of contradiction, that $r \neq 0$ (so $r > 0$).

Write $m = xa + yb$, $x, y \in \mathbb{Z}$.

Then

$$r = a - qm = a - q(xa + yb) = \underbrace{(1 - qx)}_{\in \mathbb{Z}} a + \underbrace{(-qy)}_{\in \mathbb{Z}} b \in S,$$

since $r > 0$.

So m is the least element of S, $r \in S$ and $r < m$.

This is a contradiction. Thus $r = 0$ and $m | a$.

m divides b: Similar to the previous case.

As we have seen, this completes the proof of Bézout's Lemma. $\square$