Applications of Bézout's Lemma

Ryan C. Daileda

Trinity University

Number Theory

Introduction

Recall: As a consequence of the Euclidean Algorithm (EA) we deduced:

Theorem 1 (Bézout's Lemma)

For any pair $a, b \in \mathbb{Z}$, there exist $r, s \in \mathbb{Z}$ so that

$$(a, b) = ra + sb.$$

We also gave a procedure for computing r and s based on the quotients in the EA.

Today we will look at a few important consequences of Bézout's Lemma.

Notation

Given $a \in \mathbb{Z}$, let $a\mathbb{Z}$ denote the set of multiples of a:

$$a\mathbb{Z} = \{an \,:\, n \in \mathbb{Z}\} = \{b \in \mathbb{Z} \,:\, a|b\}.$$

If $S, T \subseteq \mathbb{Z}$, we let

$$S + T = \{s + t \,:\, s \in S, t \in T\},$$

the set of pairwise sums of elements from S and T.

It follows that

$$a\mathbb{Z} + b\mathbb{Z} = \{ra + sb \,:\, r, s \in \mathbb{Z}\}$$

is the set of all linear combinations of a and b.

As a corollary to Bézout's Lemma, we can classify the elements of $a\mathbb{Z} + b\mathbb{Z}$ more precisely.

Corollary 1

Let $a, b \in \mathbb{Z}$. Then $a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}$.

That is, the linear combinations of a and b coincide with the multiples of (a, b).

Proof. We show double-containment.

Since $(a, b)|a$ and $(a, b)|b$, (a, b) divides every element of $a\mathbb{Z} + b\mathbb{Z}$. Thus,

$$a\mathbb{Z} + b\mathbb{Z} \subseteq (a, b)\mathbb{Z}.$$

We only need Bézout's Lemma for the reverse containment.

Let $c \in (a, b)\mathbb{Z}$. Then $c = (a, b)d$ for some $d \in \mathbb{Z}$.

Use Bézout's Lemma to write $(a, b) = ra + sb$ with $r, s \in \mathbb{Z}$.

Then we have

$$\begin{aligned} c = (a, b)d &= (ra + sb)d = (ra)d + (sb)d \\ &= (rd)a + (sd)b \in a\mathbb{Z} + b\mathbb{Z}. \end{aligned}$$

Therefore $(a, b)\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$, and the proof is complete. □

Example

Example 1

If a is odd, prove that $(3a, 3a+2) = 1$.

Solution. Since

$$2 = -(3a) + (3a+2) \in 3a\mathbb{Z} + (3a+2)\mathbb{Z} = (3a, 3a+2)\mathbb{Z},$$

it must be that $(3a, 3a+2) | 2$. Thus $(3a, 3a+2)$ is 1 or 2.

If a is odd, then so is $3a$ (odd $\times$ odd $=$ odd), so $2 \nmid 3a$. Therefore $(3a, 3a+2) = 2$ is impossible.

We conclude that $(3a, 3a+2) = 1$. $\square$

Moral: If d is a *specific* linear combination of a and b, then

$$d \in a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z} \;\Rightarrow\; (a, b) | d,$$

so that $|d|$ provides an upper bound on (a, b).

Taking this to the extreme we obtain the following "strong" version of Bézout's Lemma.

Lemma 1

Let $a, b \in \mathbb{Z}$. Then $(a, b) = 1$ if and only if there exist $r, s \in \mathbb{Z}$ so that

$$ra + sb = 1.$$

Proof. The forward implication follows from Bézout's Lemma.

For the converse, simply notice that if $ra + sb = 1$, then

$$1 \in a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z} \ \Rightarrow \ (a, b)|1 \ \Rightarrow \ (a, b) = 1.$$

□

Example 2

Show that for any $a \in \mathbb{Z}$, one has $(3a + 2, 5a + 3) = 1$.

Solution. Since

$$5(3a + 2) - 3(5a + 3) = 10 - 9 = 1,$$

the result follows from Lemma 1.

If $m, n \in \mathbb{Z}$ are nonzero, we know that

$$|m| \leq |mn|.$$

This implies that $|m|$ is the least positive element of $m\mathbb{Z}$.

Corollary 1 now yields:

Corollary 2

If $a, b \in \mathbb{Z}$ are not both zero, then (a, b) is the least positive linear combination of a and b.

Proof. This follows at once since $(a, b) > 0$ and $a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}$. □

We now deduce another useful property of the GCD.

Theorem 2

Let $a, b, k \in \mathbb{Z}$. Then $(ka, kb) = |k|(a, b)$.

Proof.

If $a = b = 0$ or $k = 0$, there is nothing to prove since $(0, 0) = 0$.

So we may assume $(a, b) \neq 0$ and $k \neq 0$. By Corollary 1 we have

$$(ka, kb)\mathbb{Z} = (ka)\mathbb{Z} + (kb)\mathbb{Z} = k(a\mathbb{Z} + b\mathbb{Z}) = k(a, b)\mathbb{Z}.$$

Therefore the sets $(ka, kb)\mathbb{Z}$ and $k(a, b)\mathbb{Z}$ must have the same least positive element. Hence

$$(ka, kb) = |k(a, b)| = |k|(a, b).$$

□

Example 3

We have

$$(100, 28) = 4(25, 7) = 4 \cdot 1 = 4,$$
$$(135, 105) = 5(27, 21) = 15(3, 7) = 15 \cdot 1 = 15.$$

Theorem 2 has some interesting consequences. The first is:

Corollary 3

Let $a, b, c \in \mathbb{Z}$. If $c|a$ and $c|b$, then $c|(a, b)$.

This says that not only is the GCD the *greatest* common divisor, it is also *divisible* by *every* common divisor.

Proof of Corollary 3. Write $a = cd$ and $b = ce$ with $d, e \in \mathbb{Z}$. Then

$$(a, b) = (cd, ce) = |c|(d, e) = (\pm c)(d, e) = c\big(\pm(d, e)\big),$$

showing that $c|(a, b)$. □

Notice that Corollary 3 implies that

$$C(a, b) = \{c \in \mathbb{N} : c|a \text{ and } c|b\} = \{c \in \mathbb{N} : c|(a, b)\},$$

i.e. the positive common divisors of a and b are the same as the positive divisors of (a, b) (alone).

This in turn implies that

$$(a, b) = 1 \;\Rightarrow\; C(a, b) = \{1\}.$$

Corollary 4

Let $a, b \in \mathbb{Z}$, not both zero. Write $a = (a, b)a'$ and $b = (a, b)b'$ with $a', b' \in \mathbb{Z}$. Then $(a', b') = 1$.

Proof. We have

$$(a, b) = \big((a, b)a', (a, b)b'\big) = (a, b)(a', b')$$

by Theorem 2. Since $(a, b) \neq 0$, we can cancel it from both sides, yielding $(a', b') = 1$.

Remark. If we allow ourselves the use of fractions, Theorem 3 says that

$$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1.$$

Theorem 3 shows that given a (non-trivial) pair of integers, once we factor out the GCD, we are left with a new pair that has "no" common factors (other that ± 1).

In the theory of divisibility such pairs are particularly important, so we give them a special name.

Definition

Let $a, b \in \mathbb{Z}$. We say that a and b are *relatively prime* (or *coprime*) if $(a, b) = 1$.

For example, 15 and 28 are relatively prime, since

$$(15, 28) = (15, 13) = (13, 15) = (13, 2) = 1.$$

Pairs of coprime integers have "special" divisibility properties.

For example, consider the following divisibility statements:

$$a|c \text{ and } b|c \quad \Rightarrow \quad ab|c,$$

$$a|bc \text{ and } a \nmid b \quad \Rightarrow \quad a|c.$$

As stated, these are both *false* in general:

$$6|24 \text{ and } 8|24, \ \text{ but } 6 \cdot 8 = 48 \nmid 24;$$
$$6|(9 \cdot 2) \text{ and } 6 \nmid 9, \ \text{ but } 6 \nmid 2.$$

With one additional hypothesis, however, we *can* prove analogous versions of both statements.

Theorem 3

Let $a, b, c \in \mathbb{Z}$. If a and b are relatively prime, then

$$a|c \text{ and } b|c \ \Rightarrow ab|c.$$

Proof. Suppose a and b are relatively prime, and that $a|c$ and $b|c$. Then there are integers r, s, d, e so that

$$ra + sb = 1, \ \ c = ad, \ \ c = be.$$

Multiply the first by c, then substitute in the second and third:

$$c = c(ra + sb) = rac + sbc = ra(be) + sb(ad) = ab(re + sd).$$

This proves that $ab|c$. □

Euclid's Lemma

Finally we come to Euclid's Lemma.

Theorem 4 (Euclid's Lemma)

Let $a, b, c \in \mathbb{Z}$. If $a|bc$ and a is relatively prime to b, then $a|c$.

Proof. Under the stated hypotheses, there must exist integers r, s, d so that

$$ra + sb = 1 \quad \text{and} \quad ad = bc.$$

Multiply the first by c, then substitute in the second:

$$c = c(ra + sb) = (cr)a + s(bc) = (cr)a + s(ad) = a(cr + sd),$$

proving that $a|c$. □