The Bézout Lemma and an Application

John A. Gubner
Department of Electrical and Computer Engineering
University of Wisconsin–Madison

1. Greatest Common Divisor

Given integers a and d, with $d \neq 0$, if there is an integer λ such that $a = \lambda d$, then we say "d divides a" and write $d|a$. If in addition $d|b$, say $b = \mu d$, then for integers u and v,

$$ua + vb = u(\lambda d) + v(\mu d) = (u\lambda + v\mu)d,$$

and we see that $d|(ua+vb)$.

Given integers a and b with at least one of them nonzero, we say that d is their **greatest common divisor** if the following statements are both true:

- $d|a$, $d|b$.
- For all integers c, if $c|a$ and $c|b$, then $c|d$.

In this case, we put $d := \gcd(a,b)$. Note that the gcd is unique.[1]

Lemma 1 (Bézout). *Given integers a and b not both zero,*

$$d := \min\{ax + by : x \text{ and } y \text{ are integers and } ax + by > 0\}$$

is the greatest common divisor of a and b.

Discussion. Let

$$D := \{ax + by : x \text{ and } y \text{ are integers and } ax + by > 0\}. \tag{1}$$

Then D the set of all integer linear combinations of a and b that yield a positive result. The lemma says that the smallest element of this set is the greatest common divisor. For example, if $a > 0$ and $b = 0$, then

$$D = \{ax : x \text{ is an integer and } ax > 0\} = \{ax : x = 1, 2, \ldots\}.$$

In this case, $\min D = a$, which is indeed $\gcd(a, 0)$.

[1] If d_1 and d_2 both have the above properties, then $d_1|d_2$ and $d_2|d_1$; i.e., $d_2 = \lambda d_1$ and $d_1 = \mu d_2$, which implies $d_2 = \lambda\mu d_2$, or $d_2(1 - \lambda\mu) = 0$. Since $d_2 \neq 0$, we must have $\lambda\mu = 1$. Hence, λ and μ have the same sign and their magnitudes must be one. But since $\lambda d_1 = d_2$ and d_1 and d_2 are both positive, $\lambda = 1$. Thus, $d_2 = d_1$.

Proof of the Bézout Lemma. We first point out that D in (1) is nonempty. To see this, observe that since either a or b is nonzero, we can take x or y to be ± 1 and the other zero so that $ax+by$ is equal to either $|a|$ or $|b|$. Since every nonempty set of positive integers has a smallest element,[2] $d := \min D$ is well defined. Let x and y be such that $d = ax+by$. To show that d divides a, we appeal to the division algorithm [2] to write

$$a = \lambda d + r, \quad 0 \le r < d.$$

If we can show $r = 0$, then it follows that $d|a$. Write

$$r = a - \lambda d = a - \lambda(ax+by) = a(1-\lambda x) + b\lambda y,$$

which is an integer linear combination of a and b. If $r > 0$, then $r \in D$. But then $r < d$ contradicts d being the smallest element of D. Thus, $r = 0$ and $d|a$. A similar argument shows that $d|b$. □

2. A Simple Application

Proposition 2. *Let a and b be positive integers with $\gcd(a,b) = 1$; i.e., a and b are **relatively prime**. If m is a positive integer such that $m\frac{a}{b}$ is a positive integer, then m is a positive integer multiple of b. Conversely, if m is a positive integer multiple of b, then m is a positive integer and so is $m(a/b)$.*

Proof. The converse part is obvious. So assume that m is a positive integer such that $m(a/b) = k$ for some positive integer k. Then $ma = kb$, or equivalently, $b|ma$. We claim that in fact $b|m$, which says that m is a multiple of b. To see this, we use the division algorithm to write

$$m = \lambda b + r, \quad 0 \le r < b. \tag{2}$$

Now, since $\gcd(a,b) = 1$, there exist integers x and y such that

$$1 = ax+by,$$

which implies

$$r = arx+bry.$$

Using this in (2) shows that

$$m = \lambda b + arx + bry = (ar)x + b(\lambda + ry) \tag{3}$$

Next, we also have from (2) that

$$ma = a\lambda b + ar$$

Since $b|ma$ and $b|(a\lambda b)$, we have $b|ar$. Now that b divides both terms on the right in (3), it follows that $b|m$. □

[2] This is known as the **well-ordering principle** [3].

References

[1] Wikipedia contributors, "Bézout's idenity — Wikipedia, The Free Encyclopedia," [Online]. Available: https://en.wikipedia.org/w/index.php?title=B%C3%A9zout%27s_identity&oldid=969272376, accessed Oct. 3, 2020.

[2] Wikipedia contributors, "Euclidean division — Wikipedia, The Free Encyclopedia," [Online]. Available: https://en.wikipedia.org/w/index.php?title=Euclidean_division&oldid=981100122, accessed Oct. 3, 2020.

[3] Wikipedia contributors, "Well-ordering principle — Wikipedia, The Free Encyclopedia," [Online]. Available: https://en.wikipedia.org/w/index.php?title=Well-ordering_principle&oldid=940753179, accessed Oct. 3, 2020.