Bézout's Identity

lemma

Let $a, b \in \mathbb{N}$, i.e. $\{1, 2, 3, \ldots\}$. There exist $x, y \in \mathbb{Z}$ (integers) such that

$$\text{gcd }(a, b) = xa + yb$$

Bézout's lemma (or identity) is a statement about the *greatest common divisor* of two numbers $a, b \in \mathbb{N}$. It says that we can always find two integers x and y, such that the resulting linear combination of a and b is equal to the $\text{gcd}(a, b)$.

examples

Two primes:

$$\text{gcd }(3, 2) = x \cdot 3 + y \cdot 2 = 3 \cdot 3 + (-4) \cdot 2 = 1$$

One of x, y is either negative or zero, since the gcd is less than or equal to the smaller of a, b. Next, a multiple. Here one of x, y is zero:

$$\text{gcd }(4, 2) = x \cdot 4 + y \cdot 2 = 0 \cdot 4 + 1 \cdot 2 = 2$$

Finally:

$$\text{gcd }(81, 45) = x \cdot 81 + y \cdot 45 = (-1) \cdot 81 + 2 \cdot 45 = 9$$

The lemma does not say how to find the gcd. But we know a good method for that: Euclid's algorithm.

preliminary

Let $d = \gcd(a, b)$.

We use the symbol | to mean "divides", or is a factor of, leaving no remainder. If n is any even number, then $2|n$, since $n = 2 \cdot q +$ r where r is zero.

We know that $d|a$ and $d|b$ so d divides *every* linear combination $xa+yb$ for integer x, y.

> *Proof*: If $p|m$ then $m = jp$ for some (integer) j, similarly if $p|n$ then $n = kp$ for some k. Thereefore, $m + n = (j + k)p$, which means that $p|(m + n)$.

We consider only positive combinations: $xa + by > 0$. Since d divides all of them, d must be smaller than or equal to every such combination. So we expect it will be equal to the least of them.

If S is the set of such combinations, we know that S is not empty (clearly, $a \in S$), and also $S \subset \mathbb{N}$. As a consequence, the well-ordering principle applies, and we know there is a least element.

outline

Let the least element of S be m, and as we said, let $d = \gcd(a, b)$.

We will show that $d = m$, and since $m \in S$ whose elements are all linear combinations $xa + yb$, that will complete the proof that there is a linear combination of a and b that is equal to d.

We will do this by showing first that $d|m$ which implies that $d \leq m$.

And then second, m is a common divisor of (a, b). But d is the *greatest* common divisor of the same two numbers, so $m \leq d$.

Since $d \leq m$ and $m \leq d$, therefore $m = d$.

d divides m

Again, $d = \gcd(a, b)$ so $d|a$ and $d|b$. It follows that $d|(xa + yb)$ for any integer x, y.

That is, d divides every element of S so it must be that $d|m$.

Therefore, $d \leq m$.

m divides a and b

We claim that $m|a$, in other words $a = qm + r$ with $r = 0$.

Proof. (By contradiction).

In the expression $a = qm + r$, suppose r is not zero, that is, suppose $0 \leq r < m$. Recall that $m = xa + yb$:

$$\begin{aligned} r &= a - qm = a - q(xa + yb) \\ &= (1 - qx)a + (-qy)b \end{aligned}$$

But $1 - qx$ and $-qy$ are both $\in \mathbb{Z}$. It follows that r is a linear combination of a and b and $r \in S$, since $r > 0$.

We have that m is the smallest element in S, $r \in S$ and $r < m$.

This is a contradiction.

Therefore, $r = 0$ and thus, $m|a$.

The same reasoning will show that $m|b$. Since $m|a$ and $m|b$ so $m \leq d$.

This completes the proof.

$\square$

`http://ramanujan.math.trinity.edu/rdaileda/teach/s20/m3326/lectures/bezout_handout.pdf`