3. Bezout's Identity

Bezout's Identity is, unsurprisingly, a statement about integers $a, b \in \mathbb{Z}$ and their gcd. In words, it says the following

Bezout's Identity. There exists a(n integer) linear combination of $a, b \in \mathbb{Z}$ that equals $\gcd(a, b)$.

In purely symbolic terms here it says:

Bezout's Identity. $\exists\, x, y \in \mathbb{Z},\ ax + by = \gcd(a, b)$.

Example 3.1. *We used the Euclidean Algorithm to compute* $\gcd(120, 34) = 2$ *and one can readily check Bezout's Identity is true in this instance since*

$$2 \cdot 120 + (-7) \cdot 34 = 2.$$

In this equation we are using $x = 2$ *and* $y = -7$. *The values of these coefficients are not unique, though! Generally speaking, there are* lots *of integer values for* x *and* y *that make Bezout's Identity hold. For instance*

$$(-15) \cdot 120 + 53 \cdot 34 = 2.$$

Bezout's Identity is an interesting fact. For instance, it can be used to prove the Proposition made in Example 2.3 – or at least as a key step in its proof. However, you may be curious: *why is Bezout's Identity true? Where's the proof?*

As it turns out, one of the more interesting ways to prove this fact is to use the Euclidean Division Algorithm. Given integers $a, b \in \mathbb{Z}$, one can find coefficients $x, y \in \mathbb{Z}$ that satisfy

$$ax + by = \gcd(a, b)$$

by implementing the following procedure:

(1) Use the Euclidean Algorithm to compute $\gcd(a, b)$

(2) Work backwards through the computations in the first step

(3) This will produce an equation of the form

$$\gcd(a, b) = ax + by.$$

where $x, y \in \mathbb{Z}$.

This procedure works because we can "reverse" or "undo" the equations resulting from repeated use of the Division "Algorithm" to express the gcd as (integer) combinations of various remainders and divisors. If we keep careful track of these combinations, we end up with an expression involving a and b.

The following example should help clarify how this works.

Example 3.2. *We recall the steps from the Euclidean Division Algorithm used to compute* $\gcd(120, 34) = 2$*:*

$$\begin{aligned} 120 &= 3 \cdot 34 + 18 \\ 34 &= 1 \cdot 18 + 16 \\ 18 &= 1 \cdot 16 + 2 \\ 16 &= 8 \cdot 2 + \boxed{0} \end{aligned}$$

Beginning with the second to the last line, we can solve for $2 = \gcd(120, 34)$ *to obtain*

$$(1) \qquad 2 = 18 - 1 \cdot 16 = 18 - 16$$

and the second equation from our Euclidean algorithm allows us to write $16 = 34 - 18$*. Plugging this into equation (1) gives us*

$$(2) \qquad 2 = 18 - (34 - 18) = 2 \cdot 18 - 34.$$

We can then use the first equation from our Euclidean Algorithm to express 18 as a combination of 120 and 34, namely $18 = 120 - 3 \cdot 34$*. Plugging this into equation (2) gives us*

$$\begin{aligned} (3) \qquad 2 &= 2 \cdot (120 - 3 \cdot 34) - 34 \\ &= 2 \cdot 120 - 6 \cdot 34 - 34 \\ &= 2 \cdot 120 - 7 \cdot 34 \\ &= 2 \cdot 120 + (-7) \cdot 34 \end{aligned}$$

It follows that the coefficients $x = 2$ *and* $y = -7$ *can be used so that* $120x + 34y = \gcd(120, 34)$*.*