Bézout Identity (self-study notes)

Euclidean Algorithm allows us to prove a very important theorem of Number Theory that asserts that the GCD of two integers is a linear combination of them. Such a linear combination is called a **Bézout Identity**.

Theorem 1. Given two integers a, b, there exist integer numbers x, y such that

$$GCD(a,b) = x \cdot a + y \cdot b.$$

An expression of the type $GCD(a,b) = x \cdot a + y \cdot b$ is called a *Bézout Identity*. To compute one of them we can apply Euclidean Algorithm to a and b but, after each division, we write the equality DIVIDEND = DIVISOR × QUOTIENT + REMAINDER and we isolate the REMAINDER. Then, we replace successively the reminders in the previous equalities after obtaining the desired Bézout Identity.

Let us see an example. Let us compute a Bézout Identity for the integers 250 and 111:

$$\begin{array}{l|l} 250 & \underline{111} \\ 28 & 2 \end{array} \qquad 250 = 2 \cdot 111 + 28 \Rightarrow 28 = 250 - 2 \cdot 111$$

$$\begin{array}{l|l} 111 & \underline{28} \\ 27 & 3 \end{array} \qquad \begin{aligned} 111 = 3 \cdot 28 + 27 \Rightarrow 27 &= 111 - 3 \cdot 28 \\ &= 111 - 3 \cdot (250 - 2 \cdot 111) \\ &= -3 \cdot 250 + 7 \cdot 111 \end{aligned}$$

$$\begin{array}{l|l} 28 & \underline{27} \\ 1 & 1 \end{array} \qquad \begin{aligned} 28 = 1 \cdot 27 + 1 \Rightarrow 1 &= 28 - 1 \cdot 27 \\ &= (250 - 2 \cdot 111) - 1 \cdot (-3 \cdot 250 + 7 \cdot 111) \\ &= 4 \cdot 250 - 9 \cdot 111 \end{aligned}$$

$$\begin{array}{l|l} 27 & \underline{1} \\ \mathbf{0} & 27 \end{array} \qquad \textbf{zero remainder} \Rightarrow \boxed{\text{mcd(250,111)} = 1}$$

$x = 4$ and $y = -9$ satisfy the Bézout Identity: $1 = 4 \cdot 250 + (-9) \cdot 111$

Here you have a link to a video where the computation of a Bézout Identity is explained:

`https://www.youtube.com/watch?v=9KM6bX2rud8`

Exercise 1. Compute a Bézout Identity for the integers $a = 7300$ and $b = 1316$.