A proposito dei coefficienti di Bézout

Siano $a, b \in \mathbb{Z},$ con $a \neq 0,$ e sia d un loro massimo comune divisore. Allora, in base al Lemma di Bézout, esistono $s, t \in \mathbb{Z}$ tali che si abbia

$$as + bt = d.$$

I numeri s, t sono detti *coefficienti di Bézout*. Non sono univocamente determinati, e, utilizzando la formula risolutiva per le congruenze lineari, possiamo fornire, per tutte le coppie $(s, t),$ un'espressione generale. Infatti, gli interi s per i quali esiste una coppia siffatta sono tutti e soli quelli per i quali as e d differiscono per un multiplo di $b,$ ossia

$$as \equiv d \pmod{b}$$

ossia, ancora, sono tutte e sole le soluzioni della congruenza lineare

$$ax \equiv d \pmod{b}.$$

Detta s_0 una soluzione particolare, la soluzione generale si potrà esprimere nella forma

$$s_k = s_0 + \frac{b}{d}k,$$

al variare di k in $\mathbb{Z}$. Ora, se t_0 è il numero intero tale che $as_0 - d = -bt_0,$ si avrà che $as_k - d = as_0 + a\frac{b}{d}k - d = -bt_0 + a\frac{b}{d}k = -b\left(t_0 - \frac{a}{d}k\right).$ In altri termini, al primo coefficiente di Bézout s_k corrisponde il secondo coefficiente di Bézout

$$t_k = t_0 - \frac{a}{d}k.$$

L'insieme delle coppie di coefficienti di Bézout è dunque dato da

$$\{(s_k, t_k) | k \in \mathbb{Z}\}.$$

Tale insieme è stato ottenuto a partire da una singola coppia (s_0, t_0) di coefficienti di Bézout, ed è infinito. Ciò è evidente dalla formula per t_k nel momento in cui $a \neq 0$. Ma se $a = b = 0,$ allora $d = 0$ ed ogni coppia di interi è una coppia di coefficienti di Bézout.