Bezout

1 Il teorema di Bezout per gli interi

Se a e b sono due interi e d è il loro massimo comun divisore (M.C.D.), esistono due interi m ed n tali che

$$ma + nb = d\,.$$

La determinazione dei numeri m ed n si può fare sfruttando l'algoritmo di Euclide delle *divisioni successive*, o *iterate*, utilizzato per trovare il massimo comun divisore di due numeri interi. Un esempio chiarirà il modo di procedere.

Siano dati i due numeri interi $a = 40278$ e $b = 8494$. Cominciamo ad eseguire la divisione intera (o *divisione con resto*) tra a (dividendo) e b (divisore), ottenendo un quoziente e un resto; procediamo poi dividendo il divisore per il resto, fin quando non otteniamo resto nullo.

$$\begin{array}{r|l} 40278 & 8494 \\ \cline{2-2} 6302 & 4 \end{array} \quad \Rightarrow \quad 40278 = 8494 \cdot 4 + 6302$$

$$\begin{array}{r|l} 8494 & 6302 \\ \cline{2-2} 2192 & 1 \end{array} \quad \Rightarrow \quad 8494 = 6302 \cdot 1 + 2192$$

$$\begin{array}{r|l} 6302 & 2192 \\ \cline{2-2} 1918 & 2 \end{array} \quad \Rightarrow \quad 6302 = 2192 \cdot 2 + 1918$$

$$\begin{array}{r|l} 2192 & 1918 \\ \cline{2-2} 274 & 1 \end{array} \quad \Rightarrow \quad 2192 = 1918 \cdot 1 + 274$$

$$\begin{array}{r|l} 1918 & 274 \\ \cline{2-2} 0 & 7 \end{array} \quad \Rightarrow \quad 1918 = 274 \cdot 7 + 0$$

Questo procedimento ci fornisce intanto il M.C.D tra a e b, che è l'ultimo resto non nullo nel processo delle divisioni iterate, cioè 274. Inoltre, partendo dal M.C.D. e procedendo a ritroso, ricavando nelle varie righe il resto, si ottiene:

$$\begin{aligned} 274 &= 2192 - 1918 \cdot 1 = \\ &= 2192 - (6302 - 2192 \cdot 2) \cdot 1 = 2192 \cdot 3 - 6302 = \\ &= (8494 - 6302\dot{1}) \cdot 3 - 6302 = 8494 \cdot 3 - 6302 \cdot 4 = \\ &= 8494 \cdot 3 - (40278 - 8494 \cdot 4) \cdot 4 = -40278 \cdot 4 + 8494 \cdot 19\,. \end{aligned}$$

Abbiamo così trovato due numeri che soddisfano il teorema di Bezout:

$$m = -4\,, \quad n = 19\,.$$

È chiaro che non esiste una sola coppia di numeri m ed n con la proprietà richiesta, anzi ce ne sono infinite. Se infatti (m, n) è una coppia soluzione del problema, anche

$$\left(m - k\,\frac{b}{d}\,,\, n - k\,\frac{a}{d}\right)\,, \quad k \in \mathbb{Z}$$

è una coppia soluzione del problema, in quanto a/d e b/d sono interi e inoltre

$$\left(m - k\,\frac{b}{d}\right) a + \left(n + k\,\frac{a}{d}\right) b = ma + nb - ka\,\frac{b}{d} + kb\,\frac{a}{d} = ma + nb = d\,.$$

Il teorema di Bezout si può esprimere a parole dicendo che il massimo comun divisore di due interi è una combinazione lineare, con opportuni coefficienti interi, dei due numeri.

Si tenga comunque presente che, come appena visto, esistono infinite coppie di coefficienti adatti e che, come è evidente, non ogni combinazione lineare dei due numeri fornisce il massimo comun divisore.