

Siano a, b interi non entrambi nulli. Sia r_{n-1} l'ultimo resto non nullo dell'algoritmo delle divisioni successive, i cui passi sono:

$$\begin{aligned} 1) \quad & a = bq_1 + r_1 \\ 2) \quad & b = r_1q_2 + r_2 \\ & \vdots \\ i) \quad & r_{i-2} = r_{i-1}q_i + r_i \\ & \vdots \\ n-1) \quad & r_{n-3} = r_{n-2}q_{n-1} + r_{n-1} \end{aligned}$$

Allora r_{n-1} è combinazione lineare intera di r_{n-2} e r_{n-3} . In generale, ogni resto è combinazione lineare intera dei due resti precedenti, cioè, per ogni indice i tale che $3 \leq i \leq n-1$, r_i è combinazione lineare intera di r_{i-1} e r_{i-2} . Inoltre, r_2 è combinazione lineare intera di $\textcolor{red}{r}_1$ e b , mentre r_1 è combinazione lineare intera di b ed a .

Ragionando ricorsivamente, ripercorrendo l'algoritmo a ritroso, secondo l'ordine decrescente degli indici, si avrà dunque che (per $5 \leq i \leq n$), se r_{n-1} è combinazione lineare intera di $\textcolor{violet}{r}_{i-2}$ e r_{i-3} , allora è anche combinazione lineare intera di $\textcolor{violet}{r}_{i-3}$ e $\textcolor{violet}{r}_{i-4}$, e quindi, alla fine, è combinazione lineare intera di r_2 ed r_1 , e quindi di $\textcolor{red}{a}$ e $\textcolor{red}{b}$.