IDENTITA' DI BEZOUT

L'algoritmo di Euclide ci permette, una volta individuato $d = \text{MCD}(a, b)$, di trovare due numeri interi s, t tali che

$$d = s * a + t * b$$

questa relazione si chiama **IDENTITA' DI BEZOUT**.

Vediamo il procedimento per trovare un'identità di Bezout in un esempio, riprendendo i calcoli fatti per calcolaree MCD (44880,5292) = 12.

Dobbiamo individuare $s,t \in Z$ tali che 12 = s * 44880 + t * 5292. Riscriviamo i passaggi dell'algoritmo euclideo nel modo seguente:

44880 = 5292*8+2544 ⟶ r_1= 2544=44880 - 5292*8

5292 = 2544*2+204 ⟶ r_2 = 204 = 5292 - 2544*2

2544 = 204*12+96 ⟶ r_3 = 96 = 2544 - 204*12

204 = 96*2+12 ⟶ MCD =r_4= 12=204 - 96*2

Partiamo dall'ultima relazione scritta e sostituiamo in essa il numero esplicitato nell'equazione subito precedente; raccogliamo i fattori comuni e continuiamo a sostituire il resto dell'equazione precedente (procedendo dal basso verso l'alto) fino ad ottenere un'espressione nei numeri *a, b*. Otteniamo:

12 = 204 –96*2 = 204 – (2544 - 204*12)*2=
= 204 – 2544 *2 – 204*24
= 204 * 25 – 2544 *2 = (5292 - 2544*2) * 25 – 2544 *2
= 5292 * 25 – 2544 *52 = 5292* 25 –(44880-5292*8) *52
= 5292 * 441 – 44880 *52

$$12 = 441 * 5292 - 52 * 4480$$

Quindi abbiamo ottenuto 12 = (-52) * 44880 + 441 *5292, ovvero $s = -52$ e $t = 441$.

Notiamo che l'espressione del MCD (*a, b*) fornita dall'identità di Bezout non è affatto unica.

Per dimostrare l'esistenza dell'identità di Bezout basta far vedere che tutti i resti delle divisioni successive si possono scrivere come combinazioni di a e b. Infatti osserviamo che, riscrivendo le divisioni operate, troviamo le relazioni:

$r_1 = a - b * q_1$
$r_2 = b - r_1 * q_2$
$r_3 = r_1 - r_2 * q_3$
……
$r_{n-1} = r_{n-3} - r_{n-2} * q_{n-1}$
$d = r_n = r_{n-2} - r_{n-1} * q_n$

Consideriamo l'ultima equazione, che descrive il massimo comun divisore d, che coincide con l'ultimo resto non nullo r_n, nei termini dei resti precedenti r_{n-2} e r_{n-1}. Sostituiamo il resto r_{n-1} con l'espressione $r_{n-1} = r_{n-3} - r_{n-2} * q_{n-1}$ ottenuta dalla penultima equazione. Otteniamo una espressione di d nei termini di r_{n-3} e r_{n-2}.
Continuiamo sostituendo il resto r_{n-2} con l'espressione ottenuta dalla terzultima equazione. Otteniamo una espressione di d nei termini di r_{n-3} e r_{n-4}. Si continua, utilizzando, in ordine inverso, tutte le equazioni.
Al termine, si ottiene una espressione di d = MCD(a,b) della forma cercata.

Esercizi

1) Calcola l'identità di Bezout per MCD (1637,31)
2) Calcola l'identità di Bezout per MCD (1763,51)
3) Calcola l'identità di Bezout per MCD (1547,560)