

# Matematica per l'eccellenza - Bezout

---

Materiale prelevato da

<http://www.batmath.it/matematica/eccell/eccell.htm>

Versione del 5 marzo 2010

## 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.

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

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

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

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

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

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:

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

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.

## 2 Il teorema di Bezout per i polinomi

Se  $a(x)$  e  $b(x)$  sono polinomi (a coefficienti in  $\mathbb{R}$ , in  $\mathbb{Q}$ , o più generalmente in un campo  $\mathbb{K}$ ), si può definire il massimo comun divisore esattamente come si fa per gli interi e l'algoritmo delle divisioni successive funziona allo stesso modo.

La definizione formale di M.C.D. dei due polinomi si può dare nel seguente modo:  $d(x)$  è un massimo comun divisore dei polinomi  $a(x)$  e  $b(x)$  se

1.  $d(x) \mid a(x) \wedge d(x) \mid b(x)$ ;
2. se  $d_1(x) \mid a(x) \wedge d_1(x) \mid b(x)$ , allora  $d_1(x) \mid d(x)$ .

Il massimo comun divisore di due polinomi non è unico: se  $d(x)$  è un massimo comun divisore, anche  $kd(x)$  è un massimo comun divisore (dove  $k$  è un qualunque elemento di  $\mathbb{K}$ ). Di solito quando ci si riferisce al massimo comun divisore senza altre precisazioni si fa riferimento all'unico polinomio monico che gode delle proprietà dette. Anche negli interi parlando di massimo comun divisore di solito si fa riferimento a quello positivo.

Anche per i polinomi vale il teorema di Bezout: se  $a(x)$  e  $b(x)$  sono polinomi, e  $d(x)$  è (un) loro massimo comun divisore, allora esistono due polinomi  $m(x)$  e  $n(x)$  tali che

$$a(x)m(x) + b(x)n(x) = d(x).$$

Valgono le stesse considerazioni fatte per il teorema di Bezout sugli interi e la l'algoritmo delle divisioni successive fornisce un modo per trovare i due polinomi che soddisfano il teorema di Bezout. Lo mostriamo su un esempio.

Siano  $a(x) = x^3 - 3$  e  $b(x) = x^2 + 1$ . Eseguendo le divisioni successive otteniamo

$$\begin{aligned} x^3 - 3 &= x \cdot (x^2 + 1) + (-x - 3) \\ x^2 + 1 &= (-x + 3)(-x - 3) + 10. \end{aligned}$$

Da qui si deduce che i due polinomi sono primi tra di loro (si dice anche *coprimi*) e che 10 è un M.C.D., ovvero che 1 è l'M.C.D., secondo la convenzione sopra indicata di scegliere un polinomio monico come M.C.D. Procedendo a ritroso otteniamo:

$$\begin{aligned} 10 &= (x^2 + 1) - (-x + 3)(-x - 3) = \\ &= (x^2 + 1) - (-x + 3)[(x^3 - 3) - x(x^2 + 1)] = (x^3 - 3)(x - 3) + (x^2 + 1)(-x^2 + 3x + 1), \end{aligned}$$

che fornisce un'identità di Bezout per i due polinomi dati.