Massimo comun divisore

Leonardo Bizzoni

October 10, 2023

Siano $a, b \in \mathbb{Z}$ con $a \neq 0, b \neq 0$. Si dice che un numero $d \in \mathbb{Z}$ è un **MCD** tra a e b se:

1. $d|a$ e $d|b$ (*ovvero d è un divisore di a e b*)
2. $\forall c \in \mathbb{Z} :\ c|a, c|b$ allora $c|d$

1 Teorema di esistenza di un massimo comun divisore

$\forall a, b \in \mathbb{Z}$ positivi esiste sempre un MCD fra a e b.

Inoltre esistono 2 interi $s, t \in \mathbb{Z}$ tali che:

$$d = as + bt \ \textbf{identità di Bezout}$$

2 Esercizi

Siano $(a, b \in \mathbb{Z}) \neq \emptyset$

$a \mid b$ e $b \mid a$

allora $a = \pm b$?

$b \mid a \Rightarrow \exists\, c \in \mathbb{Z} : a = b \cdot c$

$a \mid b \Rightarrow \exists\, d \in \mathbb{Z} : b = a \cdot d$

$b = a \cdot d = b \cdot c \cdot d$

$\cancel{b} = \cancel{b} \cdot c \cdot d$

$c \cdot d = 1$

$d = c = \pm 1$ ✓

---

1) se $c \mid a$ e $c \mid b$ allora $c \mid (a+b)$

2) se $c \mid a$ e $c \mid b$ allora $c \mid (a-b)$

3) se $c \mid a$ e $c \mid b$ allora $c \mid (a \cdot s + b \cdot t)$ $\forall s, t \in \mathbb{Z}$

$\exists\, d \in \mathbb{Z} : a = d \cdot c$

$\exists\, e \in \mathbb{Z} : b = e \cdot c$

① $a + b = dc + ec = c(d+e)$ ✓

② $a - b : dc + ec = c(d-e)$ ✓

③ $as + bt = dcs + ect = c(ds + et)$ $\forall s, t \in \mathbb{Z}$ ✓

MCD tra $a = 3997$

$b = 2947$

$$\begin{array}{r} 3997\ - \\ 2947\ = \\ \hline \end{array}$$

$3997 = 2947 \cdot 1 + 1050$

2947

$$2947 = 1050 \cdot 2 + \frac{2100 =}{847}$$

$$1050 = 847 \cdot 1 + \frac{\begin{array}{r} 1080 - \\ 847 = \end{array}}{203}$$

203
406
609
812

$$847 = 203 \cdot 4 + \frac{\begin{array}{r} 847 - \\ 812 = \end{array}}{35}$$

$$203 = 35 \cdot 5 + \frac{\begin{array}{r} 203 - \\ 175 = \end{array}}{28}$$

35	1
70	2
105	3
140	4
175	5

$$35 = 28 \cdot 1 + \frac{\begin{array}{r} 35 - \\ 28 = \end{array}}{7}$$

$$28 = 7 \cdot 4 + 0$$

$$MCD = 7$$

$$1050 = a - b$$

$$847 = b - 2 \cdot 1050 = b - 2(a-b) = b - 2a + 2b = 3b - 2a$$

$$203 = 1050 - 847 = (a-b) - (3b-2a) = a - b - 3b + 2a = 3a - 4b$$

$$35 = 847 - 4 \cdot 203 = (3b - 2a) - 4(3a - 4b) = 3b - 2a - 12a + 16b$$

$$= 19b - 14a$$

$$28 = 203 - 5 \cdot 35 = (3a - 4b) - 5(19b - 14a) = 3a - 4b - 95b + 70a = -99b + 73a$$

$$7 = 35 - 28 = (19b - 14a) - (-99b + 73a) = 19b - 14a + 99b - 73a = 118b - 87a$$

$$7 = 118(2947) - 87(3997)$$

$$MCD(24, 10) = 2$$

$a = 24$
$b = 10$

$$24 = 10 \cdot 2 + \frac{\begin{array}{r} 24 - \\ 20 \end{array}}{4}$$

identità di Bezout

$4 = 24 - 10 \cdot 2$

10 -

$10 = 4 \cdot 2 + 2$

$2 = 10 - 4 \cdot 2 \Rightarrow 2 = 10 - 2(24 - 2 \cdot 10)$

$2 = 10 - 2 \cdot 24 + 4 \cdot 10$

$4 = 2 \cdot 2 + 0$

$2 = 5 \cdot 10 - 2 \cdot 24$

$2 = 5b - 2a$

$MCD(220, 121) = 11$ $\quad 11 = 5(220) \cdot 9(121)$

$a = 220 \quad b = 121$

121
242

$220 = 121 \cdot 1 + 99$

$-99 + 220 = 121$
$-99 = 121 - 220$
$99 = 220 - 121$

$99 = a - b$

$121 = 99 \cdot 1 + 22$

$22 = b - 99 = b - (a - b) = b - a + b = 2b - a$

22
44
66
88

$99 = 22 \cdot 4 + 11$

$11 = 99 - 4 \cdot 22 = (a - b) - 4(2b - a) = a - b - 8b + 4a = 5a - 9b$

$22 = 11 \cdot 2 + 0$

$MCD(589, 437) = 19$ $\quad 19 = 3(589) - 4(437)$

$a = 589 \quad b = 437$

$589 = 437 \cdot 1 + 152$

$152 = a - b$

152
304

$437 = 152 \cdot 2 + 133$

$133 = b - 2 \cdot 152 = b - 2(a - b) = b - 2a + 2b = 3b - 2a$

$152 = 133 \cdot 1 + 19$

$19 = 152 - 133 = (a - b) - (3b - 2a) = a - b - 3b + 2a = 3a - 4b$

1	19
2	38
3	57
4	76
5	95
6	114

$133 = 19 \cdot 6 + 19$

$19 = 19 \cdot 1 + 0$

$\mathrm{MCD}(12'345, 23'456) = 1$ $1 = 2471(23456) - 4695(12345)$

$a = 23'456$ $b = 12'345$

12345
24690

1 1234
2 2468
3 3702
4 4936
5 6170
6 7404
7 8638
8 9872
9 11106

23456 -
12345
11111

$23456 = 12345 \cdot 1 + 11111$

12345 -
11111
1234

$12345 = 11111 \cdot 1 + 1234$

11111 -
11106
5

$11111 = 1234 \cdot 9 + 5$

$1234 = 5 \cdot 246 + 4$

$5 = 4 \cdot 1 + 1$

$4 = 4 \cdot 1 + 0$

$11\,111 = a - b$

$1\,234 = b - 11\,111 = b - (a-b) = 2b - a$

$5 = 11\,111 - 9 \cdot 1234 = (a-b) - 9(2b-a) = a - b - 18b + 9a$

$= 10a - 19b$

$4 = 1234 - 246 \cdot 5 = (2b - a) - 246(10a - 19b)$

$= 2b - a - 2460a + 4674b = 4676b - 2461a$

246 ·
19
2214 +
2460
4674

$1 = 5 - 4 = (10a - 19b) - (4676b - 2461a)$

$= 10a - 19b - 4676b + 2461a$

$= 2471a - 4695b$

$3170b - 1927a$

$\mathrm{MCD}(15\,678, 25\,791) = 3$ $3 = 3170(15\,678) - 1927(25\,791)$

$a = 25\,791$ $b = 15\,678$

25 791 -
15 678
10 113

$25\,791 = 15\,678 \cdot 1 + 10\,113$

$10\,113 = a - b$

15 678 -
10 113
5565

$15\,678 = 10\,113 \cdot 1 + 5565$

$5565 = b - (a \cdot b) = 2b - a$

5565
11130

10 113 -
5 565
4548

$10\,113 = 5565 \cdot 1 + 4548$

$4548 = (a-b) - (2b-a) = 2a - 3b$

5565 -
4548
1017

$5\,565 = 4548 \cdot 1 + 1017$

$1017 = (2b-a) - (2a-3b) = 5b - 3a$

1017
2034
3051
4068

4548 -
4068
480

$4\,548 = 1017 \cdot 4 + 480$

$480 = (2a-3b) - 4(5b-3a) = 14a - 23b$

1017 -
960
57

$1017 = 480 \cdot 2 + 57$

$57 = (5b-3a) - 2(14a-23b) = 51b - 31a$

480
960

480 -
456
24

$480 = 57 \cdot 8 + 24$

$24 = (14a-23b) - 8(51b-31a) = 262a - 431b$

57 -
48
9

$57 = 24 \cdot 2 + 9$

$9 = (51b-31a) - 2(262a-431b) = 913b - 555a$

1 57
2 114
3 171

24 -
18
6

$24 = 9 \cdot 2 + 6$

$6 = (262a - 431b) - 2(913b - 555a)$

4	228
5	285
6	342
7	399
8	456

$9 = 6 \cdot 1 + 3$

$6 = 3 \cdot 2 + 0$

$= 1372a - 2257b$

$$\begin{array}{r} 913 \cdot \\ 2 \\ \hline 1826 + \\ 431 \\ \hline -2257b \end{array} \qquad \begin{array}{r} 555 \cdot \\ 2 \\ \hline 1110 + \\ 262 \\ \hline +1372a \end{array}$$

$3 = (913b - 555a) - (1372a - 2257b)$

$-1372a + 2257b$

$= 3170b - 1927a$

$$\begin{array}{r} 2257 + \\ 913 \\ \hline 3170 \end{array}$$

$$\begin{array}{r} 1372 + \\ 555 \\ \hline 1927 \end{array}$$