

ESEMPIO Calcolare il MCD tra 54 e 39, ed anche $x, y \in \mathbb{Z}$ t.c.

$$x \cdot 54 + y \cdot 39 = (54, 39).$$

SOLUZ. Applichiamo l'algoritmo di Euclide, assieme alla sostituzione "avanzata", alla coppia 54, 39:

$$\begin{array}{ll} 54 = 1 \cdot 39 + 15 & | \quad 15 = 54 - 1 \cdot 39 \\ 39 = 2 \cdot 15 + 9 & | \quad 9 = 39 - 2 \cdot 15 \\ 15 = 1 \cdot 9 + 6 & | \quad 6 = 15 - 1 \cdot 9 \\ 9 = 1 \cdot 6 + 3 & | \quad 3 = 9 - 1 \cdot 6 = 9 - 1 \cdot (15 - 1 \cdot 9) = 2 \cdot 9 - 1 \cdot 15 = \\ 6 = 2 \cdot 3 + 0 & | \quad = 2 \cdot (39 - 2 \cdot 15) - 1 \cdot 15 = 2 \cdot 39 - 5 \cdot 15 = \\ & | \quad = 2 \cdot 39 - 5(54 - 1 \cdot 39) = 7 \cdot 39 - 5 \cdot 54 \end{array}$$

Segue che:

$$(54, 39) = 3 = 7 \cdot 39 - 5 \cdot 54 = (7) \cdot 39 + (-5) \cdot 54.$$

Proprietà dei numeri coprimi e generalizzazione dei numeri primi (pagina 26)

Proposizione 10.1 Siano $n, m \in \mathbb{Z}$ con entrambi nulli, e sia $q \in \mathbb{Z}$. Supponiamo che $(n, m) = 1$. Valgono le seguenti affermazioni.

(1) Se $n|mq$ allora $n|q$.

(2) Se $n|q$ e $m|q$ allora $nm|q$.

(oppure oss. 9.9 sulle dispense)

DIM. (1) Grazie al Golbrio 9.8 sugli appunti della lezione del 01-04-2021, $\exists x, y \in \mathbb{Z}$

t.c. $xn + ym = (n, m) = 1$, ovvero $xn + ym = 1$. Dunque, vale anche che

$$\underline{xnq + ymq} = (xn + ym)q = 1 \cdot q = \underline{q}$$

$$= xqm + ykm = (xq + yk)m.$$

Poiché per ipotesi $n|mq$, $\exists k \in \mathbb{Z}$ t.c. $nk = mq$. Dunque, $q = xqm + ykm - \frac{nk}{n} = \underline{n|q}$.

Dimostrazione(2). Supponiamo che $n|q$ e $m|q$ (risultare $(n, m) = 1$). Perché $n|q$, $\exists h \in \mathbb{Z}$ t.c. $1 nh = q$. Poiché $m|q = nh$, allora $m|nh$, grazie al punto (1) precedente, vale che $m|h$, ovvero $\exists k \in \mathbb{Z}$ t.c. $2 mk = h$. Segue che:

$$q^{\textcolor{red}{1}} = nh^{\textcolor{red}{2}} = n(mk) = nmk = (nm)k \Rightarrow nm|q. \blacksquare$$

Def. 3.4 (pagina 25) Un numero $p \in \mathbb{Z}$ è PRIMO se $p \geq 2$ e i suoi unici divisori sono quelli benati, ovvero ± 1 e $\pm p$ (corretto 1, -1, p, -p).]

Corollario 10.2 Sia $p \in \mathbb{Z}$ con $p \geq 2$. Allora p è primo se e soltanto se possiede le seguenti proprietà (*):

$$\forall m, n \in \mathbb{Z} : (p|m \wedge m \Rightarrow p|m \text{ oppure } p|m).$$

Dif. \Rightarrow) Supp. che p sia primo. Dimostrazione della proprietà (*). Siano $n, m \in \mathbb{Z}$ t.c. $p|m \wedge m$.

(Siano $n, m \in \mathbb{Z}$ t.c. $\underline{p \mid nm}$) Se $p \nmid n$, allora \mathbb{R}^* è verifica e la dimostrazione è omessa.

Sia $p \nmid n$. Poiché p possiede solo i divisori banali ± 1 e $\pm p$ e $\pm p \nmid n$ ($p \nmid n$ e $-p \nmid n$), segue che $p \nmid n$ hanno solo ± 1 come divisori comuni. In particolare, $\underline{(p, n) = 1}$. Grazie al punto (1) della Prop. 10.1 precedente, si ha che $p \mid m$, ovvero vale \mathbb{B} .

\Leftarrow) Supponiamo che p soddisfi \mathbb{B}). Dobbiamo provare che p è primo. Scriviamo p come prodotto

$\underline{p = dh \Rightarrow d \mid p}$ per qualche $d, h \in \mathbb{Z}$. Poiché $p \mid p = dh$, ovvero $p \mid dh$, grazie a \mathbb{B} ,

vale: o $p \mid d$ o $p \mid h$. Supponiamo che $\underline{p \mid d}$, ovvero $\exists k \in \mathbb{Z} \text{ f.t. } K \cancel{p=d}$.

Grazie alla Prop. 9.3 sulle dispense a pagina 24 (oppure sugli appunti della lezione del 30-03-2021), $d = \pm p$ ($\Rightarrow h = \pm 1$), ovvero $(d, h) = (p, 1)$ o $(d, h) = (-p, -1)$.

Similmente, se $p \mid h$, allora vale che $h = \pm p + d = \pm 1$. $\Rightarrow p$ è primo. \mathbb{B}

ESEMPIO Se $p=4$, allora $p \mid 2 \cdot 6$ ma $p \nmid 2$ e $p \nmid 6$.

$$\frac{p \mid 2 \cdot 6}{\downarrow} \quad p \nmid 2 \text{ e } p \nmid 6.$$

$$4 \mid 12$$

ESERCIZIO PER CASO: ESERCIZIO 10.1, pagina 27

Dimostrare ciò che segue (per induz. di 1° forma su $k \geq 1$):

Sia k un numero naturale ≥ 1 , siano $m_1, \dots, m_k \in \mathbb{Z}$ e sia p un numero primo.

Allora vale:

$$p \mid m_1 m_2 \cdots m_k \Rightarrow p \mid m_i \text{ per qualche } i \in \{1, \dots, k\}.$$

Il minimo comune multiplo

Def. 10.3 Dati due numeri interi $n, m \in \mathbb{Z}$ e dato un intero $M \in \mathbb{Z}$ con $M \geq 0$, dico che M è un minimo comune multiplo tra n e m , in breve un m.c.m. tra n e m , se valgono le seguenti proprietà:

(1) $n|M$ e $m|M$.

(2) Se $c \in \mathbb{Z}$ è un intero t.r. $n|c$ e $m|c$, allora $M|c$.

Osservazione 10.3 Siano $n, m \in \mathbb{Z}$ e siano M, M' due m.c.m. tra n e m . Allora $M = M'$.

È suff osservando:

- M' soddisfa (1) $\Rightarrow M$ soddisfa (2) con $c := M' \Rightarrow M|M'$
- M soddisfa (1) $\Rightarrow M'$ soddisfa (2) con $c := M \Rightarrow M'|M$

Grazie alla Prop. 9.3 (2), segue che $M = \pm M'$. Poiché $M \geq 0$ e $M' \geq 0$, vale $M = M'$.

Def. 10.4 Dati $n, m \in \mathbb{Z}$, se il m.c.m. fra n e m esiste, allora lo indichiamo con
 $[n, m]_I.$

Teorema 10.4 Per ogni scelta di $n, m \in \mathbb{Z}$, esiste il m.c.m. $[n, m]_I$ fra n e m .
Inoltre, se n e m non sono entrambi nulli, vale:

$$[n, m]_I = \frac{n m}{(n, m)}.$$

Dif. Se $n = m = 0$, allora n e m hanno solo 0 come multiplo comune e $(n) = 0$ è il m.c.m.
fra $n = 0$ e $m = 0$ (verifica diretta nello DFF. 10.3).

Supponiamo che n e m non siano entrambi nulli, dunque ha senso parlare di MCD fra
 n e m . Dobbiamo provare solo l'esistenza del m.c.m. (per l'unicità si vede l'Oss. 10.3
precedente).

Poiché $(n, m) \mid m$ e $(n, m) \mid m'$, esiste $n', m' \in \mathbb{Z}$ t.c.

$$\underline{n = n'(n, m)} \quad \text{e} \quad \underline{m = m'(n, m)}.$$

Quindi dalla Prop. 3.12 (versione del 01-04-2021), vale

$$\underline{(n', m') = 1}.$$

Definiamo $M \in \mathbb{Z}$ ponendo $M := \frac{nm}{(n, m)}$.

Osserviamo che $M = \frac{nm}{(n, m)} = \frac{n'(n, m) \cdot m'(n, m)}{(n, m)}$ $\cancel{(n, m)}$ $\overbrace{n' m'}$ $\underbrace{(n, m)}$ $= n'm = m'n$

$\Rightarrow m|M$ e $n|M$, ovvero la prop. (1) della DFF 10.3 è verificata.

Verifichiamo la prop. (2) della DFF. 10.3. Sia $c \in \mathbb{Z}$ t.c. $m|c$ e $m'|c$. Dobbiamo provare che $M|c$. Osserviamo che $(m, m')|m$ e $m|c$, da cui $\underline{(m, m')|c}$ (vedi Prop. 9.3 (7)). Dunque, $\exists c' \in \mathbb{Z}$ t.c.

\Downarrow DA PAGINA PRECEDENTE

$$\underline{c = c'(n, m)}.$$

(Ricordiamo: $m = m'(n, m)$ e $m = m'(n, m')$)

Dimostriamo $\underline{m'|c}$. Poiché $n|c$, esiste $h \in \mathbb{Z}$ t.c. $c = hn$. Dunque,

$$c'(n, m) = c = hn = hm'(n, m) \Rightarrow c'(n/m) = hm'(n/m) \Rightarrow r' = hn'$$

Sumilmente, vale $\underline{m'|c'}$. Grazie a Prop. 10.7(2), segue che:

$$\underline{m'm'|c'} \Rightarrow \underline{M} = \underline{n'm'(n, m)} \mid \underline{c'(n, m)} = \underline{c}$$

Dunque M soddisfa la prop. (2) della DFF. 10.3 $\Rightarrow M = [n, m]$. \square