Definizione: Siano $a_1, \ldots, a_r$ numeri interi. Allora un numero intero d si dice un *massimo comune divisore* di $a_1, \ldots, a_r$ se sono verificate le seguenti condizioni:
a) $d|a_i$ per ogni $i \in \{1, \ldots, r\}$;
b) per ogni intero e tale che $e|a_i$ per ogni $i \in \{1, \ldots, r\}$ si ha che $e|d$.

Proposizione: Siano $a_1, \ldots, a_r$ numeri interi. Allora esiste un massimo comune divisore d di $a_1, \ldots, a_r$. Inoltre i loro massimi comuni divisori sono d e $-d$.

Dimostrazione: Procediamo per induzione su $r \geq 2$ per provare che, se ∂ è un massimo comune divisore di $a_1, \ldots, a_{r-1}$, allora detto d un massimo comune divisore di ∂ e a_r, si ha che d è un massimo comune divisore di $a_1, \ldots, a_r$. In tal modo dimostreremo l'esistenza a partire dal caso particolare in cui $r = 2$, per il quale la proprietà è stata precedentemente stabilita, e che costituisce la base dell'induzione. Per il passo induttivo sia dunque $r > 2$, e supponiamo che esista un massimo comune divisore ∂ di $a_1, \ldots, a_{r-1}$. Sia d come sopra. Allora $d|\partial$ e $d|a_r$. Poiché $\partial|a_i$ per ogni $i \in \{1, \ldots, r-1\}$, per transitività segue che $d|a_i$ per ogni $i \in \{1, \ldots, r-1\}$. Ciò prova a). Sia ora e un intero tale che $e|a_i$ per ogni $i \in \{1, \ldots, r\}$. Allora, poiché, in particolare, $e|a_i$ per ogni $i \in \{1, \ldots, r-1\}$, si avrà che $e|\partial$. Poiché si ha anche $e|a_r$, segue che $e|d$. Ciò prova b) e conclude la dimostrazione dell'esistenza.
Per la seconda parte dell'enunciato è sufficiente osservare che due massimi comuni divisori di $a_1, \ldots, a_r$ si dividono reciprocamente, ossia sono associati, e, inoltre, due elementi associati hanno gli stessi divisori e gli stessi multipli.

Osservazione: Se $a_1, \ldots, a_r$ non sono tutti nulli, si definisce $\mathrm{MCD}(a_1, \ldots, a_r)$ come il loro massimo comune divisore positivo. Dalla dimostrazione precedente si ricava la seguente formula ricorsiva:

$$\mathrm{MCD}(a_1, \ldots, a_r) = \mathrm{MCD}(\mathrm{MCD}(a_1, \ldots, a_{r-1}), a_r).$$

In modo del tutto analogo si tratta la nozione di minimo comune multiplo di $a_1, \ldots, a_r$.