



divisibilità in \mathbb{Z}


DEFINIZIONE 1 Dati due interi a e b , con $b \neq 0$, si dice che b **divide** a se esiste un intero c tale che $a = bc$. In questo caso si usa la notazione $b \mid a$ e si dice anche che b è un **divisore** o **fattore** di a , ovvero che a è un **multiplo** di b , o ancora che a è **divisibile** per b . 


Valgono le seguenti proprietà:


- 1 e -1 sono gli unici divisori di 1.
- 0 è divisibile per ogni intero non nullo.
- 0 non divide alcun intero .
- $b \mid a \Leftrightarrow$ il resto della divisione tra a e b è 0.
- $a \mid b$ e $b \mid a \Leftrightarrow a = \pm b$ (in questo caso a e b si dicono **associati**).
- Se c è un divisore di a e di b , allora c divide ogni intero del tipo $ma + nb$, ove m, n sono interi.


OSSERVAZIONE 2 E' chiaro che ogni intero non nullo a è multiplo di 1, -1 , a , $-a$. Per tale motivo 1, -1 , a , $-a$ si dicono **divisori banali** di a . Un divisore non banale di a , se esiste, si dice **proprio**. 

massimo comune divisore

DEFINIZIONE 3 Un intero d si dice *massimo comune divisore* di due assegnati interi a e b se d divide a e b e se ogni divisore di a e b é anche un divisore di d . 

OSSERVAZIONE 4 Se a e b hanno un massimo comune divisore d , allora ne hanno esattamente due: d e $-d$. 

OSSERVAZIONE 5 Un massimo comune divisore di a e b é anche un massimo comune divisore di a e $-b$. 


OSSERVAZIONE 6 Sia $a = bq + r$. Un intero d é massimo comune divisore di a e b se, e soltanto se, d é massimo comune divisore di b ed r . 

algoritmo di Euclide

TEOREMA 7 (algoritmo di Euclide) Se a, b sono interi non nulli, allora esiste un massimo comune divisore di a e b .

DIM. In forza delle ultime osservazioni non é restrittivo supporre che a e b siano positivi. Costruiamo la seguente successione di divisioni, fino ad ottenere un resto uguale a zero:

$$\begin{aligned} a &= bq_1 + r_1 && \text{con } 0 \leq r_1 < b, \\ b &= r_1q_2 + r_2 && \text{con } 0 \leq r_2 < r_1, \\ r_1 &= r_2q_3 + r_3 && \text{con } 0 \leq r_3 < r_2, \\ r_2 &= r_3q_4 + r_4 && \text{con } 0 \leq r_4 < r_3, \\ &\dots && \\ r_{k-4} &= r_{k-3}q_{k-2} + r_{k-2} && \text{con } 0 \leq r_{k-2} < r_{k-3}, \\ r_{k-3} &= r_{k-2}q_{k-1} + r_{k-1} && \text{con } 0 \leq r_{k-1} < r_{k-2}, \\ r_{k-2} &= r_{k-1}q_k + r_k && \text{con } r_k = 0. \end{aligned}$$


Allora, in forza dell'osservazione precedente, abbiamo che r_{k-1} é un massimo comune divisore di a e b . 

TEOREMA 8 (identità di Bézout) Siano a, b interi non nulli e d un loro massimo comune divisore. Allora d si può scrivere come combinazione lineare di a e b a coefficienti in \mathbb{Z} , esistono cioè due interi m, n tali che

$$d = ma + nb.$$

DIM. Partendo dalla prima delle divisioni scritte nel corso della dimostrazione precedente e andando verso le successive, abbiamo

$$\begin{aligned} r_1 &= a - bq_1, \\ r_2 &= b - r_1q_2 = (-q_2)a + (1 + q_1q_2)b \\ r_3 &= r_1 - r_2q_3 = (1 + q_2q_3)a + [-q_1 - (1 + q_1q_2)q_3]b \end{aligned}$$

e, così continuando, abbiamo che ogni r_j é combinazione lineare a coefficienti in \mathbb{Z} di a e b . In particolare questa proprietà sarà vera per r_{k-1} e, essendo $d = \pm r_{k-1}$, l'asserto é completamente provato. 

esercizio

ESEMPIO 9 Vediamo come lavora l'algoritmo di Euclide nel caso $a = 306$ e $b = 135$:

$$\begin{aligned} 306 &= 135 \cdot 2 + 36 && \text{con } 0 \leq 36 < 135, \\ 135 &= 36 \cdot 3 + 27 && \text{con } 0 \leq 27 < 36, \\ 36 &= 27 \cdot 1 + 9 && \text{con } 0 \leq 9 < 27, \\ 27 &= 9 \cdot 3 + 0. \end{aligned}$$

L'ultimo resto non nullo é 9, che quindi é un massimo comune divisore di 306 e 135.

Adesso scriviamo $d = 9$ come combinazione lineare a coefficienti interi di $a = 306$ e $b = 135$. Abbiamo:

$$36 = 306 - 2 \cdot 135,$$

$$27 = 135 - 3 \cdot 36 = 135 - 3(306 - 2 \cdot 135) = -3 \cdot 306 + 7 \cdot 135,$$

$$9 = 36 - 27 = (306 - 2 \cdot 135) + (-3 \cdot 306 + 7 \cdot 135) = 4 \cdot 306 - 9 \cdot 135.$$

Gli interi cercati sono, dunque, $m = 4$ e $n = -9$.



esercizi

ESERCIZIO 10 *Provare che due interi non nulli a, b hanno un unico massimo comune divisore positivo (che si denota con $MCD(a, b)$).*

ESERCIZIO 11 *Sia $d = \pm MCD(a, b)$ e supponiamo $a = da_1$ e $b = db_1$. Provare che risulta $MCD(a_1, b_1) = 1$ (in questo caso a_1 e b_1 si dicono coprimi).*

ESERCIZIO 12 *Siano a e b coprimi e a divida bc . Provare che a divide c .*

ESERCIZIO 13 *Dare la definizione di minimo comune multiplo di due interi non nulli.*

ESERCIZIO 14 *Sia $d = MCD(a, b)$ e $ab = dm$. Provare che m é un minimo comune multiplo di a, b .*

ESERCIZIO 15 *Se a e b sono coprimi, provare che ab é un minimo comune multiplo di a e b .*

ESERCIZIO 16 *Provare che due interi non nulli a, b hanno esattamente due minimi comuni multipli, che sono l'uno l'opposto dell'altro (l'unico minimo comune multiplo positivo di a, b si denota con $mcm(a, b)$).*

ESERCIZIO 17 *Estendere le definizioni di minimo comune multiplo e di massimo comune divisore al caso di piú di due interi.*