

L'algoritmo di Euclide

L'algoritmo di Euclide permette di determinare il massimo comun divisore di due numeri naturali. Eccone una descrizione in linguaggio naturale.

ALGORITMO DI EUCLIDE

Siano dati due numeri naturali **A** e **B**, di cui si vuole calcolare il *MCD*.

- 1 Si determina il resto **R** della divisione **A : B**.
- 2 Si sostituisce **A** con il valore di **B** e **B** con il valore di **R**.
- 3 Se **R** = 0, allora il *MCD* è **A** e il calcolo è concluso, altrimenti si torna al punto 1.

Proviamo ad applicarlo per determinare il *MCD* di 2322 e 684: dunque poniamo **A** = 2322 e **B** = 684.

	A	B	R
1 Eseguiamo la divisione A : B $2322 : 684 = 3$ con resto 270	2322	684	270
2 Assumiamo A = 684 e B = R = 270: il nuovo valore di A è il vecchio valore di B e il nuovo valore di B è il resto R .	684	270	270
3 Essendo R = 270 $\neq$ 0 non abbiamo terminato; torniamo al punto 1.	684	270	270
1 Eseguiamo la divisione A : B $684 : 270 = 2$ con resto 144	684	270	144
2 Assumiamo A = 270 e B = 144.	270	144	144
3 R = 144 $\neq$ 0, torniamo al punto 1.	270	144	144
1 Eseguiamo la divisione $270 : 144 = 1$ con resto 126	270	144	126
2 A = 144 e B = 126.	144	126	126
3 R = 126 $\neq$ 0, torniamo al punto 1.	144	126	126

1	$144 : 126 = 1$ con resto 18	144	126	18
2	$A = 126$ e $B = 18$.	126	18	18
3	$R = 18 \neq 0$, torniamo al punto 1.	126	18	18
1	$126 : 18 = 7$ resto 0.	126	18	0
2	$A = 18$ e $B = 0$	18	0	0
3	Abbiamo trovato $R = 0$: il MCD è $A = 18$ e abbiamo terminato.	18	0	0

In **FIGURA 1** vediamo il diagramma a blocchi dell'algoritmo di Euclide.

Per comprenderlo devi considerare **A**, **B** e **R** non come numeri, ma come caselle in ciascuna delle quali può essere inserito un numero. Esse sono le **variabili** dell'algoritmo.

Durante l'esecuzione di un algoritmo il contenuto di una variabile può essere sostituito da un numero, dal contenuto di un'altra variabile o dal risultato di un'operazione. Il simbolo $:=$ indica tale sostituzione.

A sinistra di tale simbolo si indica il nome della variabile il cui contenuto deve essere sostituito, a destra il nuovo contenuto della variabile.

SIMBOLI

Abbiamo adottato il simbolo $:=$ per evitare confusioni con il simbolo di uguaglianza che, in matematica, ha un altro significato.

In un algoritmo potrai trovare ad esempio istruzioni del tipo $N := N + 1$. Ciò significa che il contenuto della variabile **N** deve essere sostituito dal suo contenuto attuale aumentato di un'unità. In matematica invece un'uguaglianza del tipo $n = n + 1$ sarebbe impossibile.

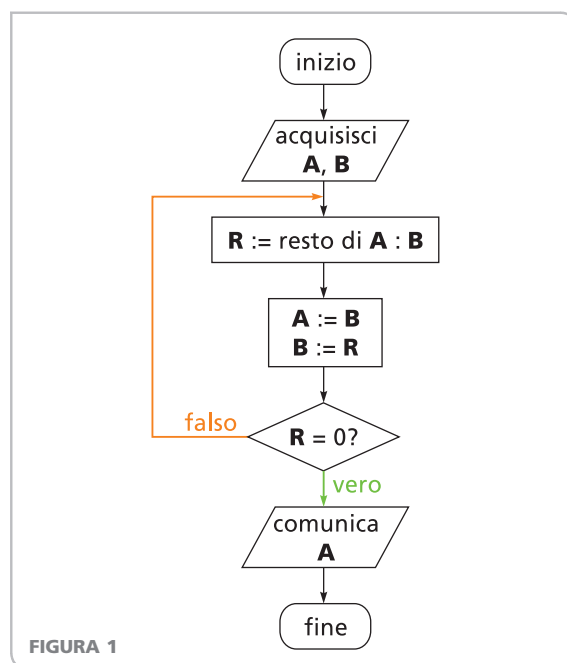


FIGURA 1

La prima operazione che dobbiamo compiere è acquisire i due numeri di cui si vuole trovare il *MCD*, che inseriamo uno nella variabile **A** e l'altro nella variabile **B**.

Quindi eseguiamo la divisione tra il numero contenuto nella variabile **A** e il numero contenuto nella variabile **B** e inseriamo il resto nella variabile **R**.

Inseriamo nella variabile **A** il numero contenuto nella variabile **B** e quindi nella variabile **B** inseriamo il numero contenuto nella variabile **R**.

A questo punto dobbiamo prendere una *decisione*, basandoci sulla risposta a una domanda: **R** è uguale a zero?

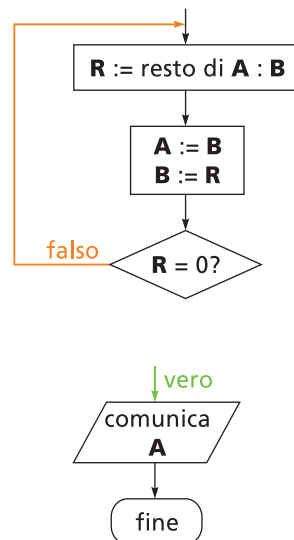
acquisisci
A, B

R := resto di A : B

A := B
B := R

R = 0?

Se la risposta è negativa, ossia se il contenuto della variabile **R** è diverso da zero, seguiamo la freccia arancio; poi, sempre seguendo le frecce, torniamo a eseguire la divisione **A : B**.



Se invece la risposta è positiva comunichiamo il risultato, ossia il *MCD*, che è il numero contenuto nella casella **A**, e terminiamo l'esecuzione dell'algoritmo.

Vediamo ora una descrizione in pseudolinguaggio, su cui torneremo nei prossimi paragrafi.

Inizio

Acquisisci **A**, **B**

Ripeti

R := resto della divisione **A : B**

A := **B**

B := **R**

Finché **R** = 0

Comunica "il MCD è ", **A**

Fine

PERCHÉ FUNZIONA?

Perché l'algoritmo di Euclide funziona? Esso si basa su due considerazioni.

- Se il resto della divisione $a : b$ è 0, allora b è il *MCD* di a e b .
Infatti in questo caso b è divisore di a , ed è anche divisore di se stesso, dunque b è un divisore comune di a e b ; d'altra parte tutti gli altri divisori di b sono minori di b , quindi b è il massimo tra i divisori comuni di a e b .
- Se il resto della divisione $a : b$ è $r \neq 0$, allora i divisori comuni di a e b sono gli stessi di b e r .
Infatti indicando il quoziente e il resto della divisione $a : b$ rispettivamente con q e r , si ha $a = bq + r$, ossia

$$r = a - bq$$

Se k è un divisore sia di a sia di b , allora b e a sono multipli di k ; ciò significa che esistono due numeri naturali a' e b' diversi da zero tali che $a = ka'$ e $b = kb'$ e dunque, sostituendo nella relazione $r = a - bq$ e applicando la proprietà distributiva si ha

$$r = ka' - kb'q \longrightarrow r = k(a' - b'q)$$

Ciò significa che r è il prodotto di k per il numero naturale $a' - b'q$, e quindi k è un divisore, oltre che di b , anche di r .

Viceversa, se k è un divisore sia di b sia di r , ragionando allo stesso modo a partire dall'uguaglianza $a = bq + r$, si vede che k è anche divisore di a .

Pertanto, in ogni passaggio, sostituendo i valori di a e b con nuovi valori, ossia con i numeri b e r , pur cambiando i numeri, non cambia l'insieme dei loro divisori comuni e quindi non cambia il loro *MCD*; perciò quello determinato al termine del procedimento è il *MCD* dei due numeri iniziali.

LE VARIABILI

Abbiamo detto che le variabili possono essere considerate come caselle in cui inserire un contenuto. Esse corrispondono a delle aree di memoria in cui il computer codifica questo contenuto: è perciò opportuno specificare di quale tipo può essere questo contenuto, affinché il computer possa codificarlo correttamente. Nell'algoritmo di Euclide le variabili utilizzate rappresentano dei numeri naturali.

In generale distingueremo i seguenti tipi di variabile:

variabili intere: possono contenere numeri interi relativi;

variabili reali: possono contenere numeri reali;

variabili stringa: possono contenere una sequenza di caratteri;

variabili logiche o booleane: possono contenere uno dei due valori *Vero* o *Falso*.

Nel seguito indicheremo in grassetto maiuscolo il nome delle variabili per distinguerle dal loro contenuto: ad esempio **N** può indicare una variabile intera che può contenere un numero che indicheremo con *n*.