

# L'algoritmo di Euclide per la ricerca del MCD

The Euclidean algorithm for finding the greatest common divisor of two integers

La divisione di un numero intero  $a$  per un altro intero  $b$  può essere prolungata finché il resto è più piccolo del divisore.

Se  $a = 648$  e  $b = 7$ , si ha un quoziente  $q = 92$  e un resto  $r = 4$ .

$$\begin{array}{r} 648 : 7 = 92 \\ 18 \\ 4 \end{array} \qquad 648 = 7 \cdot 92 + 4$$

## TEOREMA

**Nella divisione tra due numeri naturali  $a$  e  $b$ , con  $b$  diverso da zero, si può sempre trovare una coppia di numeri  $q$  e  $r$ , tali che  $a = b \cdot q + r$  con  $r$  compreso tra  $b$  e zero ( $0 \leq r < b$ )**

Da questo si può dedurre un metodo per la ricerca del M.C.D. di due numeri interi (particolarmente utile per numeri grandi). L'algoritmo (*un algoritmo è un metodo sistematico di calcolo*) si basa sul fatto che ad ogni relazione della forma:

$$a = b \cdot q + r$$

segue che:

$$MCD(a, b) = MCD(b, r)$$

Ripetendo nello stesso modo accade che **il MCD è l'ultimo resto positivo della successione.**

$$\begin{aligned} a &= b \cdot q_1 + r_1 \\ b &= r_1 \cdot q_2 + r_2 \\ r_1 &= r_2 \cdot q_3 + r_3 \\ r_2 &= r_3 \cdot q_4 + r_4 \\ &\dots \\ r_{n-3} &= r_{n-2} \cdot q_{n-1} + r_{n-1} \rightarrow M.C.D. \\ r_{n-2} &= r_{n-1} \cdot q_n + 0 \end{aligned}$$

L'algoritmo è applicato alla risoluzione delle equazioni diofantee nella forma  $ax + by = c$ .

Il teorema di Lamé (1845) stabilisce il numero di passi richiesti per trovare il M.C.D. ( $a, b$ ) con il metodo di Euclide.

Per  $n \geq 1$ , siano dati due numeri interi  $u$  e  $v$ , con  $u > v > 0$  tali che l'applicazione dell'algoritmo di Euclide applicato a  $u$  e  $v$  richiede esattamente  $n$  divisioni e tali che  $u$  sia piccolo tanto da soddisfare queste condizioni. Allora  $u = F_{n+1}$  e  $v = F_n$ , dove  $F_k$  è un numero di Fibonacci.

Il numero di passaggi dell'algoritmo di Euclide non supera di 5 volte il numero delle cifre del numero con meno cifre. Il valore 5 può, inoltre, essere ulteriormente ridotto a  $\ln 10 / \ln \phi \approx 4,785$ , dove  $\phi$  è il rapporto aureo.

Gabriel Lamé (Tours, 22 luglio 1795 – Parigi, 1° maggio 1870) dimostrò nel 1844 che l'algoritmo di Euclide ha un ciclo più lungo se in input ci sono numeri di Fibonacci.

## Algoritmo Euclideo per divisioni successive

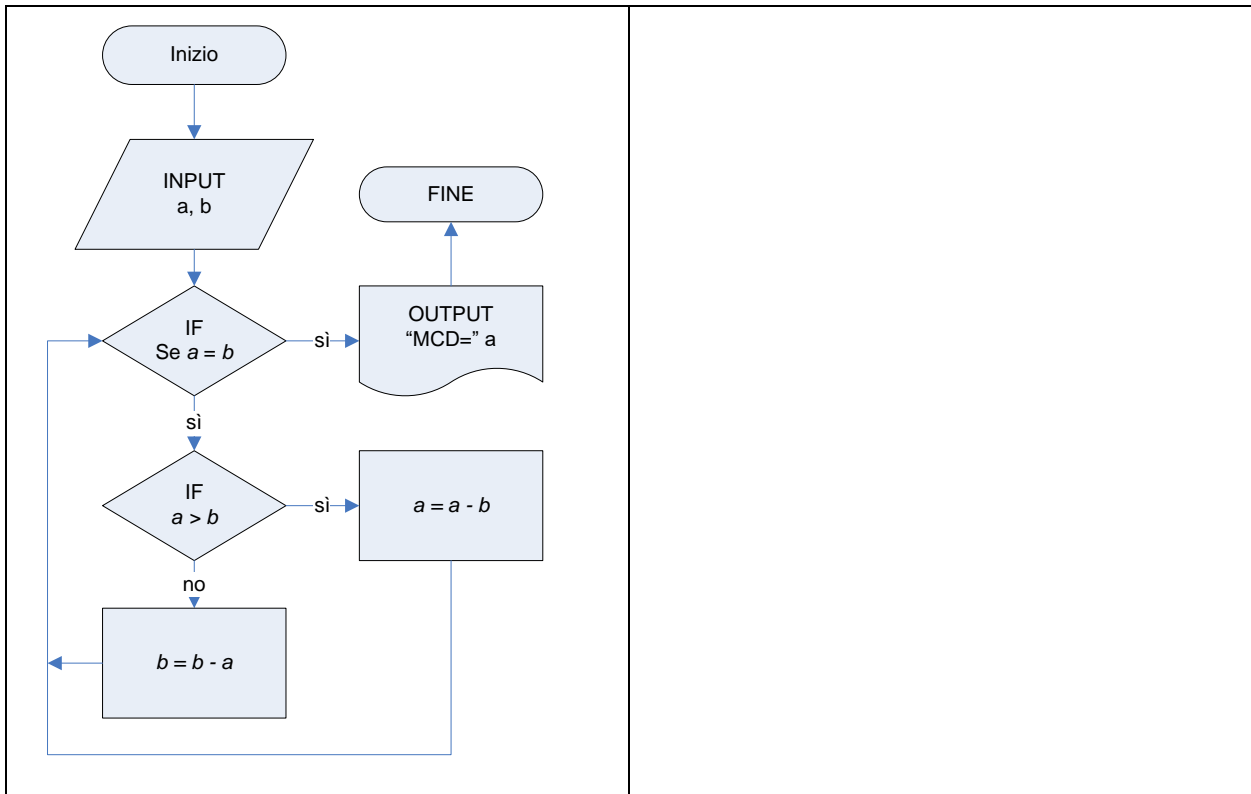
L'algoritmo non richiede la fattorizzazione dei due interi (realizzazione Scratch).

### Rappresentazione dell'algoritmo in pseudocodice e realizzazione in C++ e Python

<p><i>Prendi i valori da tastiera <b>a</b> e <b>b</b></i>  <i>Se <b>a &lt; b</b> allora scambiali</i>  <i>Metti in <b>resto</b> il resto tra <b>a</b> e <b>b</b></i></p> <p><i>Ripeti finché <b>resto</b> &lt;&gt; 0</i>              <i>Metti in <b>a</b> il contenuto di <b>b</b></i>              <i>Metti in <b>b</b> il contenuto di <b>resto</b></i>              <i>Metti in <b>RESTO</b> il resto tra <b>a</b> e <b>b</b></i></p> <p><i>Fine Ripeti</i></p> <p><i>Mostra il MCD che è pari a <b>b</b></i></p>	<p><b>C++</b></p> <pre style="background-color: #ffffcc; padding: 5px;">int gcd(int a, int b) {     if (b == 0)         return a;     else         return gcd(b, a % b); }</pre> <p><b>Python</b></p> <pre style="background-color: #ffffcc; padding: 5px;">a=28 b=70 def euclide(a, b):     while(b != 0):         r=a%b         a=b         b=r     return a print(euclide(a,b))</pre>
---	--

## Algoritmo Euclideo per differenze successive

L'algoritmo non richiede la fattorizzazione dei due interi.



### Rappresentazione dell'algoritmo (pseudocodice)

Prendi i valori da tastiera **a** e **b**

Ripeti finché **a <> b**

Se **a > b**

Sostituisci ad **a** il valore **(a - b)**

Altrimenti

Sostituisci ad **b** il valore **(b - a)**

Fine se

Fine Ripeti

Mostra il MCD che è pari ad **a (a=b)!**

## Esempi risolti

---

$$\text{MCD}(24, 14) = 2$$

$$24 = 2^3 \cdot 3$$

$$14 = 2 \cdot 7$$

### Algoritmo Sottrazioni successive

$$24 - 14 = 10$$

$$14 - 10 = 4$$

$$10 - 4 = 6$$

$$6 - 4 = 2$$

$$4 - 2 = 2$$

$$2 - 2 = 0$$

quindi  $\text{MCD}(24, 14) = 2$

$$\text{MCD}(24, 14) = 2 = \underline{2}$$

ricorda che:

$$m.c.m.(24, 14) = 2^3 \cdot 3 \cdot 7$$

### Algoritmo Divisioni successive

$$24 : 14 = 1 \text{ resto } 10$$

$$14 : 10 = 1 \text{ resto } 4$$

$$10 : 4 = 2 \text{ resto } \underline{2}$$

$$4 : 2 = 2 \text{ resto } 0$$

Quindi  $\text{MCD}(24, 14) = 2$

$$\text{MCD}(1804, 328) = 164$$

$$1804 = 2^2 \cdot 11 \cdot 41$$

$$328 = 2^3 \cdot 41$$

### Algoritmo Sottrazioni successive

$$1804 - 328 = 1476$$

$$1476 - 328 = 1148$$

$$1148 - 328 = 820$$

$$820 - 328 = 492$$

$$492 - 328 = 164$$

$$328 - 164 = 164$$

$$164 = 164$$

quindi  $\text{MCD}(1804, 328) = 164$

$$\text{MCD}(1804, 328) = 2^2 \cdot 41 = \underline{164}$$

ricorda che:

$$m.c.m.(1804, 328) = 2^3 \cdot 11 \cdot 41$$

### Algoritmo Divisioni successive

$$1804 : 328 = 5 \text{ resto } \underline{164}$$

$$328 : 164 = 2 \text{ resto } 0$$

Quindi  $\text{MCD}(1804, 328) = \underline{164}$

$$\text{MCD}(61, 24) = 1$$

$$61 = 61 \text{ (numero primo!)}$$

$$24 = 2^3 \cdot 3$$

#### Algoritmo Sottrazioni successive

$$61 - 24 = 37$$

$$37 - 24 = 13$$

$$24 - 13 = 11$$

$$13 - 11 = 2$$

$$11 - 2 = 9$$

$$9 - 2 = 7$$

$$7 - 2 = 5$$

$$5 - 2 = 3$$

$$3 - 2 = 1$$

$$2 - 1 = 1$$

$$1 - 1 = 0 \text{ quindi MCD}(61, 24) = 1$$

$$\text{MCD}(61, 24) = \underline{1} \text{ (primi tra loro)}$$

*ricorda che:*

$$m.c.m.(61, 24) = 2^3 \cdot 3 \cdot 61$$

#### Algoritmo Divisioni successive

$$61 = 24 \cdot 2 + 13$$

$$24 = 13 \cdot 1 + 11$$

$$13 = 11 \cdot 1 + 2$$

$$11 = 2 \cdot 5 + \underline{1}$$

$$2 = 1 \cdot 2 + 0$$

$$61 : 24 = 2 \text{ resto } 13$$

$$24 : 13 = 1 \text{ resto } 11$$

$$13 : 11 = 1 \text{ resto } 2$$

$$11 : 2 = 5 \text{ resto } \underline{1}$$

$$2 : 1 = 2 \text{ resto } 0$$

$$\text{MCD}(84, 36) = 2^2 \cdot 3 = 12$$

$$84 = 2^2 \cdot 3 \cdot 7$$

$$36 = 2^2 \cdot 3^2$$

#### Algoritmo Sottrazioni successive

$$84 - 36 = 48$$

$$48 - 36 = 12$$

$$36 - 12 = 24$$

$$24 - 12 = 12$$

$$12 - 12 = 0 \text{ quindi MCD}(84, 36) = 12$$

$$\text{MCD}(84, 36) = 2^2 \cdot 3 = 12$$

*ricorda che:*

$$m.c.m.(84, 36) = 2^2 \cdot 3^2 \cdot 7$$

#### Algoritmo Divisioni successive

$$84 = 36 \cdot 2 + \underline{12}$$

$$36 = 12 \cdot 3 + 0$$

$$\text{MCD}(840, 611) = 1$$

$$840 = 2^3 \cdot 3 \cdot 5 \cdot 7$$

$$611 = 13 \cdot 47$$

#### Algoritmo Sottrazioni successive

$$841 - 611 = 229$$

$$611 - 229 = 382$$

$$382 - 229 = 153$$

$$229 - 153 = 76$$

$$153 - 76 = 77$$

$$77 - 76 = 1$$

$$76 - 1 = 75$$

...

$$3 - 1 = 2$$

$$2 - 1 = 1$$

$$1 - 1 = 0 \text{ quindi } \text{MCD}(840, 611) = 1$$

$$\text{MCD}(840, 611) = \underline{1} \text{ (primi tra loro)}$$

ricorda che:

$$m.c.m.(840, 611) = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 47$$

#### Algoritmo Divisioni successive

$$840 = 611 \cdot 1 + 229$$

$$611 = 229 \cdot 2 + 153$$

$$229 = 153 \cdot 1 + 76$$

$$153 = 76 \cdot 2 + \underline{1}$$

$$76 = 1 \cdot 76 + 0$$

$$\text{MCD}(648, 7) = 1$$

$$648 = 2^3 \cdot 3^4$$

$$7 = 7 \text{ (numero primo!)}$$

#### Algoritmo Sottrazioni successive

$$841 - 7 = 834$$

$$834 - 7 = 827$$

...

$$22 - 7 = 15$$

$$15 - 7 = 8$$

$$8 - 7 = 1$$

$$7 - 1 = 6$$

$$6 - 1 = 5$$

$$5 - 1 = 4$$

$$4 - 1 = 3$$

$$3 - 1 = 2$$

$$2 - 1 = 1$$

$$1 - 1 = 0 \text{ quindi } \text{MCD}(648, 7) = 1$$

$$\text{MCD}(648, 7) = \underline{1} \text{ (primi tra loro)}$$

ricorda che:

$$m.c.m.(648, 7) = 2^3 \cdot 3^4 \cdot 7$$

#### Algoritmo Divisioni successive

$$648 = 7 \cdot 92 + 4$$

$$7 = 4 \cdot 1 + 3$$

$$4 = 3 \cdot 1 + \underline{1}$$

$$3 = 1 \cdot 3 + 0$$

Matematica e storia

**Euclide, matematico greco** nato ad Alessandria d'Egitto e fiorito intorno al **300 a.C.**, è famoso per la sua opera "**Elementi**" (in greco *Stoichêia*) dove tratta tra l'altro questo procedimento in modo geometrico. Ricordiamo, legati al suo nome, il termine **geometria euclidea** o elementare (comprendente la geometria piana e la geometria solida e contrapposta a quelle non euclidee), il **postulato di Euclide** (libro I, *aitémata* quinto) ed i due importanti **teoremi di Euclide** (libro I, assieme al teorema di Pitagora).

L'algoritmo di Euclide è proposto come soluzione alla Proposizione VII.2 degli Elementi  
 Euclid's algorithm appears as the solution to the Proposition VII.2 in the Element's  
[aleph0.clarku.edu/~djoyce/java/elements/toc.html](http://aleph0.clarku.edu/~djoyce/java/elements/toc.html)  
[it.wikipedia.org/wiki/Algoritmo\\_di\\_Euclide](http://it.wikipedia.org/wiki/Algoritmo_di_Euclide)  
[it.wikipedia.org/wiki/Euclide](http://it.wikipedia.org/wiki/Euclide)



Matematica e storia











**Gabriele Lamé** (Tours 22.7.1795 – Paris, 1.5.1870) è stato matematico e fisico francese.

Il teorema di Lamé (1845 G. Lamé) stabilisce il numero di passi richiesti per trovare il MCD(a,b) con il metodo di Euclide.






[it.wikipedia.org/wiki/Gabriel\\_Lam%C3%A9](http://it.wikipedia.org/wiki/Gabriel_Lam%C3%A9)


# Approfondimenti


 ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA	MCD e algoritmo di Euclide <a href="http://progettomatematica.dm.unibo.it">progettomatematica.dm.unibo.it</a>	<a href="http://www.dm.unibo.it/matematica/Congruenze/html/pag2/pag2.htm">www.dm.unibo.it/matematica/Congruenze/html/pag2/pag2.htm</a>
 <b>BASE Cinque</b> Appunti di Matematica ricreativa	Algoritmo di Euclide per il calcolo del MCD (programmi in javascript). Serie di Fibonacci.	<a href="http://utenti.quipo.it/base5/numeri/euclidalgor.htm">utenti.quipo.it/base5/numeri/euclidalgor.htm</a> <a href="http://utenti.quipo.it/base5/numeri/fibonacciserie.htm">utenti.quipo.it/base5/numeri/fibonacciserie.htm</a>
 <b>Università degli Studi di Bari</b>	Altro approccio all'algoritmo di Euclide	<a href="http://www.di.uniba.it/~proga/mcd.pdf">www.di.uniba.it/~proga/mcd.pdf</a>
 WIKIPEDIA L'enciclopedia libera	Algoritmo di Euclide	<a href="http://it.wikipedia.org/wiki/Algoritmo_di_Euclide">it.wikipedia.org/wiki/Algoritmo di Euclide</a> <a href="http://it.wikipedia.org/wiki/Massimo_comun_divisore">it.wikipedia.org/wiki/Massimo comun divisore</a> <a href="http://it.wikipedia.org/wiki/Euclide">it.wikipedia.org/wiki/Euclide</a>
 <b>Math Goodies™</b> Your Destination for Math Education!	Number Theory - Math Goodies	<a href="http://www.mathgoodies.com">www.mathgoodies.com</a>
 <b>Matematicamente.it</b>	Insiemi numerici	<a href="http://www.matematicamente.it/staticfiles/formulario/4-Insiemi_numerici.pdf">www.matematicamente.it/staticfiles/formulario/4-Insiemi_numerici.pdf</a>
 <b>Cut The Knot</b>	Euclid's Algorithm from <a href="http://cut-the-knot">cut-the-knot</a>	<a href="http://www.cut-the-knot.org/blue/Euclid.shtml">www.cut-the-knot.org/blue/Euclid.shtml</a> <a href="http://www.cut-the-knot.org/blue/EuclidAlg.shtml">www.cut-the-knot.org/blue/EuclidAlg.shtml</a>
 <b>The Prime Pages</b> prime number research, records, and resources	The Prime Pages <i>Professor Chris Caldwell</i> <a href="http://www.utm.edu">University of Tennessee at Martin</a>	<a href="http://primes.utm.edu">primes.utm.edu</a>
 <b>Libri.eu</b>	"Euclide megarense acutissimo philosopho, solo introduttore delle scienze mathematiche. Diligentemente rassettato, et alla integrità ridotto, per il degno professore di tal scienze Nicolo Tartalea brisciano. Secondo le due tradottioni. Con vna ampla esposizione dello istesso traduttore di nuouo aggiunta", di Euclides; traduzione di Niccolò Tartaglia; a cura di Niccolò Tartaglia; IN VENETIA. Appresso Curtio Troiano 1565	<a href="http://www.liberliber.it/biblioteca/e/euclides/">www.liberliber.it/biblioteca/e/euclides/</a>  Gli Elementi di Euclide - Opera completa e prima traduzione italiana a cura di Niccolò Tartagli.
 <b>CLARK UNIVERSITY</b>	Euclid's Element	<a href="http://aleph0.clarku.edu/~djoyce/java/elements/toc.html">aleph0.clarku.edu/~djoyce/java/elements/toc.html</a>

## Keywords

 *Matematica, Aritmetica, Divisibilità, MCD, mcm, Massimo Comune Divisore, minimo comune multiplo, algoritmo di Euclide, esercizi con soluzioni*

  *Math, Arithmetic, Divisibility, Highest Common Factor, HCF, Greatest Common Factor, GCF, Lowest Common Multiple, LCM, Least Common Multiple, LCM, Greatest common divisor, GDC, Euclidean Algorithm*

 *Matemática, Aritmética, Máximo común divisor, mcd, m.c.d., Mínimo común múltiplo, mcm, m.c.m., algoritmo de Euclides.*

 *Mathématique, Arithmétique, Divisibilité, factorisation, Plus grand commun diviseur, PGDC, Plus petit commun multiple, PPCM, Algorithme d'Euclide*

 *Mathematik, Arithmetik, Größter gemeinsamer Teiler, kleinstes gemeinsames Vielfaches, Euklidischer Algorithmus*