

L'algoritmo di Euclide

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.

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

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

TEOREMA

di zero, si può sempre trovare un numero q tale che Se a è un numero intero e b un altro numero intero maggiore

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

con r compreso tra b e zero ($0 \leq r < b$)

Da questo si può dedurre un metodo per la ricerca del MCD 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:

$$\text{MCD}(a; b) = \text{MCD}(b; r)$$

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

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

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

Il teorema di Lamé (1845 G. Lamé) stabilisce il numero di passi richiesti per trovare il MCD($a;b$) 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 ϕ è il rapporto aureo.

Nota storica

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.

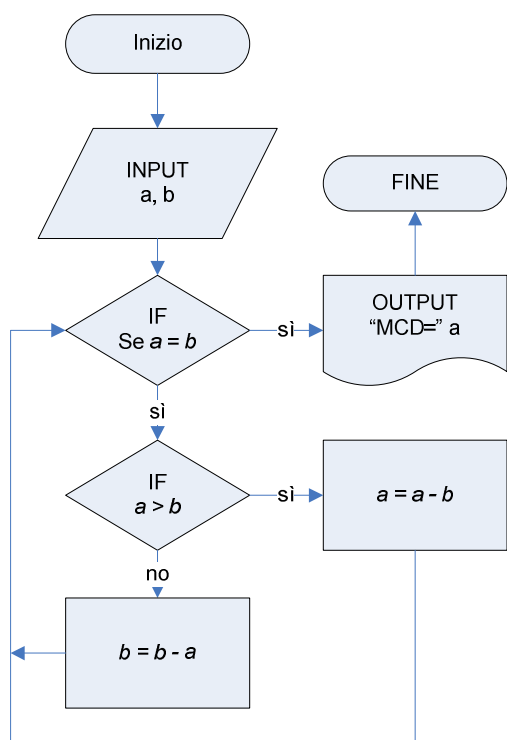
Ricordiamo, legati al suo nome, il termine **geometria euclidea** o elementare (comprendente la geometria piana e la geometria solida e contrapposta a quelle non euclidee), il **postulato di Euclide** (libro I, *aitémata* quinto) ed i due importanti **teoremi di Euclide** (libro I, assieme al teorema di Pitagora).

L'algoritmo di Euclide viene 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 <http://aleph0.clarku.edu/~djoyce/java/elements/toc.html>

Gabriele Lamé (22.7.1795 – 1.5.1870) matematico francese.

Un primo algoritmo Euclideo (diagramma a blocchi)



Rappresentazione dell'algoritmo (pseudocodice)

Prendi i valori da tastiera a e b

Ripeti finché $a \neq b$

Se $a > b$

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

Altrimenti

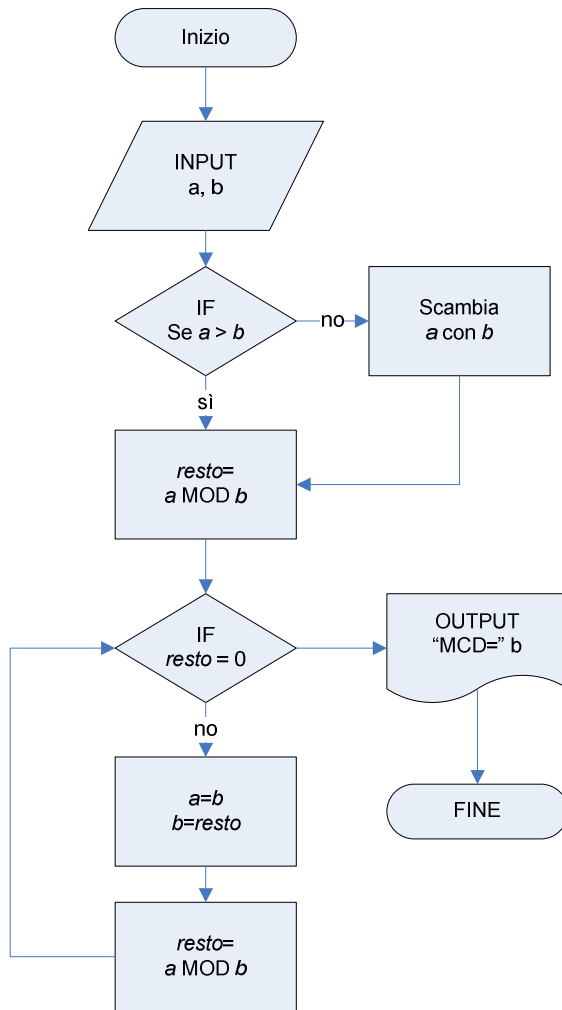
Sostituisci ad b il valore $(b - a)$

Fine se

Fine Ripeti

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

Un secondo algoritmo Euclideo (diagramma a blocchi)



Rappresentazione dell'algoritmo

pseudocodice	C++
Prendi i valori da tastiera a e b Se a < b allora scambiali Metti in resto il resto tra a e b Ripeti finché resto <> 0 Metti in a il contenuto di b Metti in b il contenuto di resto Metti in RESTO il resto tra a e b Fine Ripeti Mostra il MCD che è pari a b	<pre> int gcd(int a, int b) { if (b == 0) return a; else return gcd(b, a % b); } </pre>

Esempi risolti

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

$$24 = 2^3 \times 3$$

$$14 = 2 \times 7$$

Algoritmo Sottrazioni successive

$$24 - 14 = 10$$

$$14 - 10 = 4$$

$$10 - 4 = 6$$

$$6 - 4 = 2$$

$$4 - 2 = 2$$

$$2 - 2 = 0 \text{ quindi } \text{MCD}(24; 14) = 2$$



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

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

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

Algoritmo Sottrazioni successive

$$1804 - 328 = 1476$$

$$1476 - 328 = 1148$$

$$1148 - 328 = 820$$

$$820 - 328 = 492$$

$$492 - 328 = 164$$

$$328 - 164 = 164$$

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



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

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

$$24 = 2^3 \times 3$$

Algoritmo Sottrazioni successive

$$61 - 24 = 37$$

$$37 - 24 = 13$$

$$24 - 13 = 11$$

$$13 - 11 = 2$$

$$11 - 2 = 9$$

$$9 - 2 = 7$$

$$7 - 2 = 5$$

$$5 - 2 = 3$$

$$3 - 2 = 1$$

$$2 - 1 = 1$$

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



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

ricorda che:

$$m.c.m.(24; 14) = 2^3 \times 3 \times 7$$

Algoritmo Divisioni successive

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

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

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

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

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

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

ricorda che:

$$m.c.m.(1804; 328) = 2^3 \times 11 \times 41$$

Algoritmo Divisioni successive

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

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

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

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

ricorda che:

$$m.c.m.(61; 24) = 2^3 \times 3 \times 61$$

Algoritmo Divisioni successive

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

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

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

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

$$2 = 1 \times 2 + 0$$

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

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

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

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

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

$$\text{MCD}(84; 36) = 2^2 \times 3 = 12$$

$$840 = 2^2 \times 3 \times 7$$

$$36 = 2^2 \times 3^2$$

Algoritmo Sottrazioni successive

$$84 - 36 = 48$$

$$48 - 36 = 12$$

$$36 - 12 = 24$$

$$24 - 12 = 12$$

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

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

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

$$611 = 13 \times 47$$

Algoritmo Sottrazioni successive

$$841 - 611 = 229$$

$$611 - 229 = 382$$

$$382 - 229 = 153$$

$$229 - 153 = 76$$

$$153 - 76 = 77$$

$$77 - 76 = 1$$

$$76 - 1 = 75$$

...

$$3 - 1 = 2$$

$$2 - 1 = 1$$

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

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

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

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

Algoritmo Sottrazioni successive

$$841 - 7 = 834$$

$$834 - 7 = 827$$

...

$$22 - 7 = 15$$

$$15 - 7 = 8$$

$$8 - 7 = 1$$

$$7 - 1 = 6$$

$$6 - 1 = 5$$

$$5 - 1 = 4$$

$$4 - 1 = 3$$

$$3 - 1 = 2$$

$$2 - 1 = 1$$

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

$$\text{MCD}(84; 36) = 2^2 \times 3 = 12$$

ricorda che:

$$m.c.m.(84; 36) = 2^2 \times 3^2 \times 7$$

Algoritmo Divisioni successive

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

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

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

ricorda che:

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

Algoritmo Divisioni successive

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

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

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

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

$$76 = 1 \times 76 + 0$$

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

ricorda che:

$$m.c.m.(648; 7) = 2^3 \times 3^4 \times 7$$

Algoritmo Divisioni successive

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

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

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

$$3 = 1 \times 3 + 0$$

Sitografia

MCD e algoritmo di Euclide

<http://www.dm.unibo.it/matematica/Congruenze/html/pag2/pag2.htm>

La successione di Fibonacci

<http://utenti.quipo.it/base5/numeri/fibonacciserie.htm>

Algoritmo di Euclide per il calcolo del MCD (programmi in javascript)

<http://utenti.quipo.it/base5/numeri/euclidalgor.htm>

Una soluzione sw brillante

<http://www.elet.polimi.it/upload/agosta/infoC-2001/E0801/node4.html>

Altro approccio all'algoritmo di Euclide

<http://www.di.uniba.it/~proga/mcd.pdf>

Software crittografico e non solo

<http://www.math.unipr.it/~zaccagni/crittografia/Software.html>

Euclide

<http://www.filosofico.net/euclide.htm>

Gli elementi di Euclide

<http://aleph0.clarku.edu/~djoyce/java/elements/toc.html>



Crittologia e Euclide


http://www.amagri.it/Crittologia/Crittografia/Algoritmi_crittografici/RSA/matematica_di_base.htm#Algoritmo_Euclide


Honsberger, R. "A Theorem of Gabriel Lamé." Ch. 7 in *Mathematical Gems II*. Washington, DC: Math. Assoc. Amer., pp. 54-57, 1976.


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*