Metodo di Euclide per il calcolo del Massimo comune divisore
di due numeri naturali
Tovena Francesca

MASSIMO COMUNE DIVISORE E ALGORITMO DI EUCLIDE

L'algoritmo di Euclide permette di calcolare il massimo comun divisore tra due numeri, anche se questi sono molto grandi, senza aver bisogno di fattorizzarli come prodotto di fattori primi.
Ricordiamo, per completezza, alcune definizioni:

Definizione Siano dati due numeri naturali non nulli a e b. Un loro **massimo comun divisore** è un intero positivo d, $d > 0$ tale che

1. d divide a e d divide b (cioè d è un divisore comune)
2. d è il numero più grande con tale proprietà.

Se a e b non sono entrambi nulli, l'insieme dei loro divisori comuni è non vuoto (contenendo almeno 1) e finito (perchè i divisori di un numero non nullo non possono essere maggiori del numero stesso). Poichè i numeri naturali formano un insieme ordinato, il massimo comune divisore esiste sempre, ed è unico: esso viene indicato con il simbolo MCD(a,b).
Se a=b=0, si dice che 0 è il loro massimo comune divisore. Se solo uno tra a e b, è non nullo, esso coincide con il massimo comune divisore.

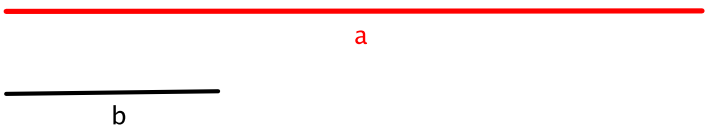
se d' divide sia a che b allora d' divide d
Due numeri naturali non nulli a, b tali che MCD(a,b) = 1 si dicono *coprimi* o *relativamente primi*.

La divisione tra numeri naturali può essere riletta nel modo seguente:
Proposizione Siano a, b numeri naturali non nulli. Allora esistono e sono univocamente determinati due interi q e r tali che

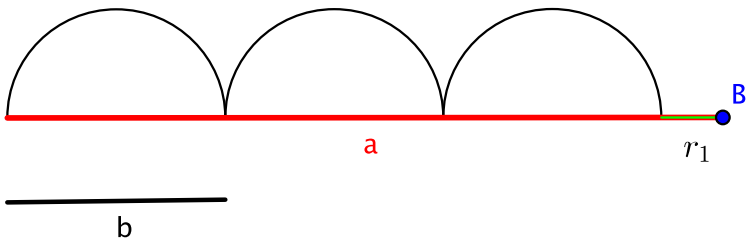
$$a = b \cdot q + r \text{ con } 0 \le r < b$$

In quest'operazione a è detto *dividendo*, b *divisore*, q *quoziente* e r *resto.*

L'**algoritmo di Euclide** (o **metodo delle divisioni successive**), che consente di calcolare il M.C.D. tra due qualsiasi numeri, si basa su una serie di divisioni successive:

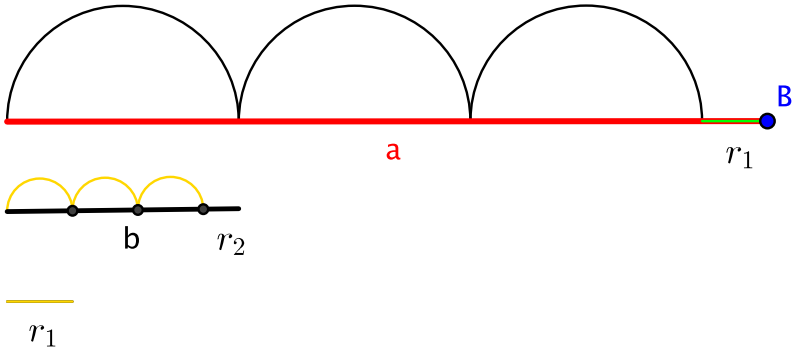


si inizia dividendo a per b e si ottengono un quoziente q_1 e un resto r_1;



se $r_1 = 0$, allora MCD(a,b)=b e ci si ferma;

se $r_1 \neq 0$ si prosegue dividendo b per r_1 : si ottengono q_2 e r_2;



se $r_2 = 0$, si interrompe il procedimento;
se $r_2 \neq 0$, si ripete il ragionamento.

L'algoritmo termina quando troviamo resto nullo e il MCD è l'ultimo resto diverso da zero.

Questa procedura ha sicuramente termine perché il resto si riduce ad ogni passo.
Il procedimento è illustrato di seguito, calcolando MCD (44880,5292).
$a = b \cdot q + r$

44880 = 5292 · 8+2544

5292 = 2544 · 2 +204

2544 = 204 · 12 + 96

204 = 96 · 2 + **12**

96 = 12 · 8 + 0 MCD

MCD (44880,5292) = 12 (=ultimo resto non nullo)

Più in generale, dobbiamo calcolare MCD (a, b). Supponiamo $a \geq b > 0$ e operiamo le divisioni.

$$a = b * q_1 + r_1 \qquad 0 < r_1 < b$$

$$b = r_1 * q_2 + r_2 \qquad 0 < r_2 < r_1$$

$$r_1 = r_2 * q_3 + r_3 \qquad 0 < r_3 < r_2$$

$$\ldots\ldots\ldots$$

$$r_{i-2} = r_{i-1} * q_i + r_i \qquad 0 < r_i < r_{i-1}$$

$$\ldots\ldots\ldots$$

$$r_{n-2} = r_{n-1} * q_n + r_n \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n * q_{n+1} + 0$$

Allora MCD (a, b) = r_n (=ultimo resto non nullo).

Osservazioni.

1. L'ultimo resto non nullo r_n divide il resto precedente r_{n-1} , e dunque tutti i resti di indice più piccolo. Inoltre, r_n divide a e b. Dunque r_n divide il MCD che stiamo cercando.
2. Ogni divisore comune di a e b è anche divisore di r_1, perché se un numero divide a e b allora ne divide anche la differenza. Tale ragionamento vale per tutti i resti delle divisioni successive fino al resto r_n che è l'ultimo diverso da 0. Dunque ogni divisore comune di a e b deve dividere anche r_n.
3. Mettendo assieme le osservazioni 1 e 2 concludiamo che $r_n = MCD(a,b)$.
4. Al massimo occorre fare b operazioni, perché ogni resto r_i delle divisioni è minore del resto precedente, quindi abbiamo una catena $b>r_1>r_2>r_3>\ldots$ di numeri che sono interi positivi e decrescenti, quindi hanno un minimo che è 0 e sono al massimo b.

Esempio

1) Calcola MCD (1637,31)

44880 = 31 · 52 + 25

31 = 25 · 1 + 6

25 = 6 · 4 + 1 ← MCD

6 = 1 · 6 + **0**

MCD (1637,31) = 1 (=ultimo resto non nullo)

2) Calcola MCD (1763,51)

1763 = 51 · 34 + 29

51 = 29 · 1 + 22

29 = 22 · 1 + 7

22 = 7 · 3 + **1**

7 = 1 · 7 + 0 ← MCD

MCD (1763,51)= 1 (=ultimo resto non nullo)

3) Calcola MCD (1547,560)

1547 = 560 · 2 + 427

560 = 427 · 1 + 133

427 = 133 · 3 + 28

133 = 28 · 4 + 21

28 = 21 · 1 + 7 ← MCD

21 = 7 · 1 + 0

MCD (1547,560)= 7 (=ultimo resto non nullo)