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

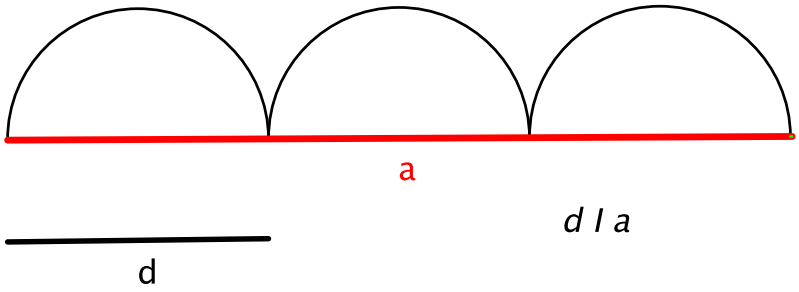
MASSIMO COMUNE DIVISORE E ALGORITMO DI EUCLIDE

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:

Se un numero naturale a è multiplo di un numero naturale d, diciamo che d è un divisore di a e scriviamo:

$d \mid a$



Definizione Siano dati due numeri naturali non nulli a e b. Un loro **massimo comun divisore** è un numero naturale non nullo d, tale che

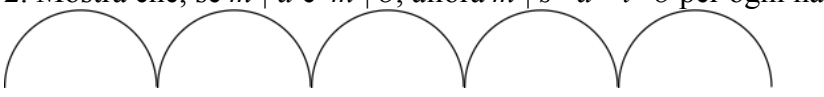
1. d divide a e d divide b (cioè d è un divisore comune)
2. d è il numero più grande con tale proprietà.

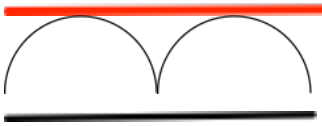
Se a e b non sono entrambi nulli, l'insieme dei loro divisori comuni è non vuoto (contenendo almeno 1) e finito (perchè i divisori di un numero non nullo non possono essere maggiori del numero stesso). Poichè i numeri naturali formano un insieme ordinato, il massimo comune divisore esiste sempre, ed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

Due numeri naturali non nulli a, b tali che MCD(a,b) = 1 si dicono *coprimi* o *relativamente primi*.

Esercizio: Siano m, a, b numeri naturali non nulli con $a > b$.

1. Mostra che, se m divide a e b, allora m divide $a + b$ e anche a-b.
2. Mostra che, se $m \mid a$ e $m \mid b$, allora $m \mid s \cdot a + t \cdot b$ per ogni naturale s e t.





La divisione tra numeri naturali può essere riletta nel modo seguente:

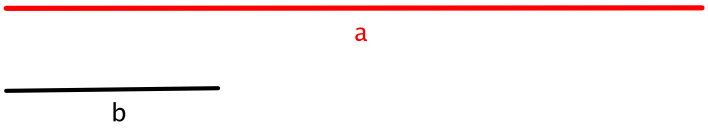
Metodo di Euclide per il calcolo del Massimo comune divisore
di due numeri naturali
Tovena Francesca

Proposizione Siano a, b numeri naturali non nulli. Allora esistono e sono univocamente determinati due interi q e r tali che

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

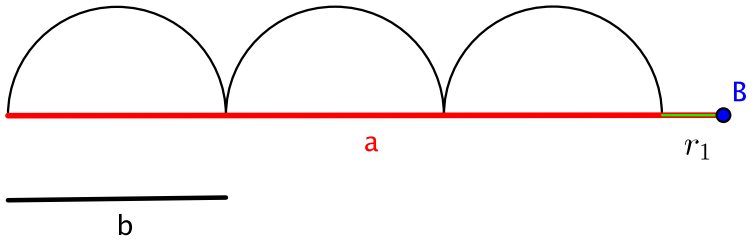
In quest'operazione a è detto *dividendo*, b *divisore*, q *quoziente* e r *resto.*
Risulta, che b divide a se e solo se il resto r è uguale a zero.

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. Rappresentiamo i numeri come lunghezza, e supponiamo $a > b$.

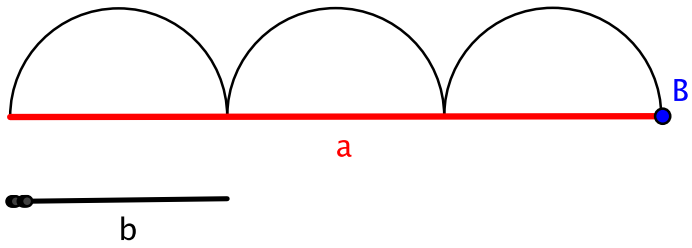


Si inizia dividendo a per b e si ottengono un quoziente q_1 e un resto r_1, tali che

$$a = b\cdot q_1+r_1 .$$

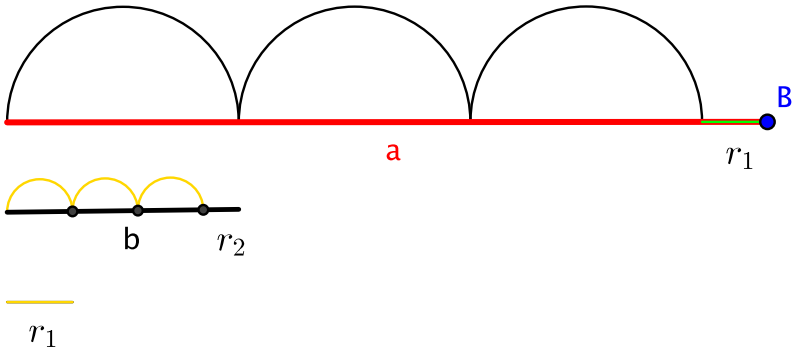


Possono accadere solo due distinti casi: o il resto r_1 è nullo, oppure non è nullo.
Se $r_1 = 0$, allora b divide a e la figura è della forma:

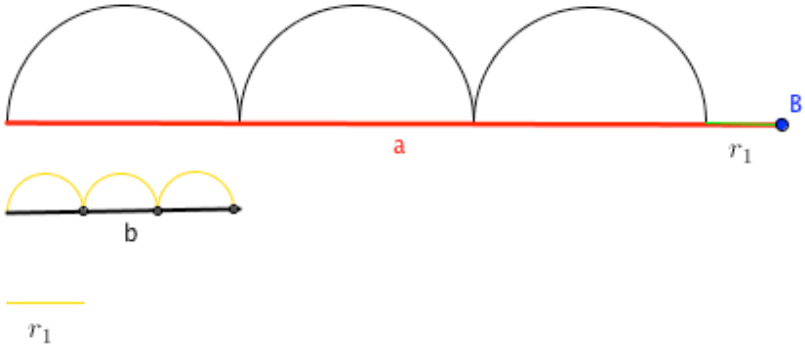


quindi MCD$(a,b)=b$ e ci si ferma;
Se, invece, $r_1 \neq 0$, disegniamo anche il segmento r_1. Confrontiamo il segmento r_1 con il segmento precedente b: dividiamo quindi b per r_1 e otteniamo q_2 e r_2 tali che

$$b= r_1\cdot q_2+r_2 .$$



Nuovamente, si presentano due casi: $r_2 = 0$ oppure $r_2 \neq 0$.
se $r_2 = 0$, la figura è della forma



Sappiamo che r_1 divide b, perché $r_2 = 0$. Ma allora r_1 divide anche a (perché divide b, quindi divide i multipli di b; inoltre, coincide con la parte di differenza tra a e $b \cdot q_1$) . Dunque, r_1 è un divisore comune di a e b. Ma qualsiasi divisore comune di a e b deve dividere r_1 . Concludiamo che

$$r_1 = \text{MCD}(a,b)$$

Osserviamo che r_1 è l'ultimo resto non nullo e che abbiamo ottenuto la risposta cercata.
Se, invece, $r_2 \neq 0$, si ripete il ragionamento precedente:
- disegno un nuovo segmento, r_2
- divido il segmento precedente r_1 per r_2, ottenendo q_3 e r_3 tali che

$$r_1 = r_2 \cdot q_3 + r_3 .$$

- se $r_3 = 0$, allora r_2 divide r_1 . Ma allora r_2 divide anche $b = r_1 \cdot q_2 + r_2$. Concludiamo che r_2 divide $a = b \cdot q_1 + r_1$. Dunque, r_2 è un divisore comune di a e b. Ma qualsiasi divisore comune di a e b deve dividere $r_1 = a - b \cdot q_1$ e quindi anche $r_2 = b - r_1 \cdot q_2$. Concludiamo che

$$r_2 = \text{MCD}(a,b)$$

Osserviamo che il MCD r_2 è l'ultimo resto non nullo e che abbiamo ottenuto la risposta cercata.
Se, invece, $r_3 \neq 0$, si aggiunge un nuovo segmento e si ripete il ragionamento precedente. L'algoritmo termina quando troviamo resto nullo e il MCD è l'ultimo resto diverso da zero. La procedura ha sicuramente termine perché il resto si riduce ad ogni passo.

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

Esempio: Il procedimento è illustrato di seguito, calcolando MCD (44880,5292).

$a = b \cdot q + r$

$44880 = 5292 \cdot 8 + 2544$ $\quad a = 44880$, $b = 5292$, $r_1 = 2544$

$5292 = 2544 \cdot 2 + 204$ $\quad r_2 = 204$

$2544 = 204 \cdot 12 + 96$ $\quad r_3 = 96$

$204 = 96 \cdot 2 + \mathbf{12}$ $\quad \mathbf{r_4 = 12}$

$96 = 12 \cdot 8 + 0$ ← MCD

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

Osservazione: ad ogni passo, il resto ottenuto divide il resto precedente.

Esempio

1) Calcola MCD (1637,31)

$1637 = 31 \cdot 52 + 25$

$31 = 25 \cdot 1 + 6$

$25 = 6 \cdot 4 + 1$

$6 = 1 \cdot 6 + \mathbf{0}$ ← MCD

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

2) Calcola MCD (1763,51)

$1763 = 51 \cdot 34 + 29$

$51 = 29 \cdot 1 + 22$

$29 = 22 \cdot 1 + 7$

$22 = 7 \cdot 3 + \mathbf{1}$

$7 = 1 \cdot 7 + 0$ ← MCD

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

3) Calcola MCD (1547,560)

$1547 = 560 \cdot 2 + 427$

$560 = 427 \cdot 1 + 133$

$427 = 133 \cdot 3 + 28$

$133 = 28 \cdot 4 + 21$

$28 = 21 \cdot 1 + 7$ ← MCD

$21 = 7 \cdot 1 + 0$

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

Esercizi Calcola, con il metodo di Euclide, i seguenti numeri:
MCD(2337, 1482)= …..
MCD(16717, 8249)= …..
MCD(4891, 1541)= …..

IDENTITA' DI BEZOUT

L'algoritmo di Euclide ci permette, una volta individuato d = MCD (a, b), di trovare due numeri interi s, t tali che

$$d = s \cdot a + t \cdot b$$

questa relazione si chiama **IDENTITA' DI BEZOUT**.

Vediamo il procedimento per trovare un'identità di Bezout in un esempio, riprendendo i calcoli fatti per calcolaree MCD (44880,5292) = 12.

Dobbiamo individuare $s,t \in Z$ tali che 12 = s * 44880 + t * 5292. Riscriviamo i passaggi dell'algoritmo euclideo nel modo seguente:

$44880 = 5292 \cdot 8 + 2544 \longrightarrow r_1 = 2544 = 44880 - 5292 \cdot 8$

$5292 = 2544 \cdot 2 + 204 \longrightarrow r_2 = 204 = 5292 - 2544 \cdot 2$

$2544 = 204 \cdot 12 + 96 \longrightarrow r_3 = 96 = 2544 - 204 \cdot 12$

$204 = 96 \cdot 2 + 12 \longrightarrow MCD = r_4 = 12 = 204 - 96 \cdot 2$

Partiamo dall'ultima relazione scritta e sostituiamo in essa il numero esplicitato nell'equazione subito precedente; raccogliamo i fattori comuni e continuiamo a sostituire il resto dell'equazione precedente (procedendo dal basso verso l'alto) fino ad ottenere un'espressione nei numeri a, b. Otteniamo:

$$\begin{aligned} 12 &= 204 - 96 \cdot 2 = 204 - (2544 - 204 \cdot 12) \cdot 2 = \\ &= 204 - 2544 \cdot 2 - 204 \cdot 24 \\ &= 204 \cdot 25 - 2544 \cdot 2 = (5292 - 2544 \cdot 2) \cdot 25 - 2544 \cdot 2 \\ &= 5292 \cdot 25 - 2544 \cdot 52 = 5292 \cdot 25 - (44880 - 5292 \cdot 8) \cdot 52 \\ &= 5292 \cdot 441 - 44880 \cdot 52 \end{aligned}$$

$$12 = 441 \cdot 5292 - 52 \cdot 4480$$

Quindi abbiamo ottenuto 12 = (-52) · 44880 + 441 · 5292, ovvero $s = -52$ e $t = 441$.

Notiamo che l'espressione del MCD (a, b) fornita dall'identità di Bezout non è affatto unica.

Per dimostrare l'esistenza dell'identità di Bezout basta far vedere che tutti i resti delle divisioni successive si possono scrivere come combinazioni di a e b. Infatti osserviamo che, riscrivendo le divisioni operate, troviamo le relazioni:

$r_1 = a - b \cdot q_1$
$r_2 = b - r_1 \cdot q_2$
$r_3 = r_1 - r_2 \cdot q_3$
……
$r_{n-1} = r_{n-3} - r_{n-2} \cdot q_{n-1}$

$d = r_n = r_{n-2} - r_{n-1} \cdot q_n$

Consideriamo l'ultima equazione, che descrive il massimo comun divisore d, che coincide con l'ultimo resto non nullo r_n, nei termini dei resti precedenti r_{n-2} e r_{n-1}. Sostituiamo il resto r_{n-1} con l'espressione $r_{n-1} = r_{n-3} - r_{n-2} \cdot q_{n-1}$ ottenuta dalla penultima equazione. Otteniamo una espressione di d nei termini di r_{n-3} e r_{n-2}.
Continuiamo sostituendo il resto r_{n-2} con l'espressione ottenuta dalla terzultima equazione. Otteniamo una espressione di d nei termini di r_{n-3} e r_{n-4}. Si continua, utilizzando, in ordine inverso, tutte le equazioni.
Al termine, si ottiene una espressione di d = MCD(a,b) della forma cercata.

Esercizi
1) Calcola l'identità di Bezout per MCD (1637,31)
2) Calcola l'identità di Bezout per MCD (1763,51)
3) Calcola l'identità di Bezout per MCD (1547,560)