

ALGORITMO DI EUCLIDE: per trovare il $\text{MCD}(A, B)$

$$A = B \cdot q_1 + r_1$$

$$B = r_1 \cdot q_2 + r_2$$

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

.....

$$r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1}$$

$$r_{n-2} = r_{n-1} \cdot q_n + r_n \rightarrow r_n = \emptyset$$

$\text{MCD} = r_{n-1}$

[se $B > A$]

$$A = B \cdot \emptyset + A$$

$$B = A \cdot \dots$$

lemma:

$$\text{MCD}(A, B) = \text{MCD}(B, r)$$

$(r = A \% B = \text{resto di } \frac{A}{B} = A \bmod B)$ dim.

$$\left[\begin{array}{l} r_0 = A \\ r_1 = B \\ r_2 = r_0 \bmod r_1 \\ r_3 = r_1 \bmod r_2 \\ \dots \end{array} \right]$$

$$\begin{aligned} A &= B \cdot q + r \\ r &= A - Bq \rightarrow \left(\begin{array}{l} A = \alpha \cdot \text{MCD} \\ B = \beta \cdot \text{MCD} \end{array} \right) \rightarrow r = \text{MCD}(\alpha - \beta q) \rightarrow \text{anche } r \text{ è} \\ &\quad \text{multiplo di MCD} \\ &\quad \downarrow \\ &\quad r = \lambda \cdot \text{MCD} \\ &\quad \rightarrow A = \text{MCD}(B \cdot q + \lambda) \end{aligned}$$

dimostrazione algoritmo:

- $B \geq r_1 > r_2 > \dots > r_{n-1} > r_n = \emptyset$

- dal lemma: $\text{MCD}(A, B) = \text{MCD}(B, r_1) = \text{MCD}(r_1, r_2) = \dots = \text{MCD}(r_{n-1}, r_n) = \text{MCD}(r_{n-1}, \emptyset) = r_{n-1}$

minimo comune multiplo: $\text{mcm}(A, B) = \text{per piccolo n. multiplo di entrambi}$

es. $\text{mcm}(588, 2490)$:

$588 = 2^2 \cdot 3 \cdot 7^2$	$2490 = 2 \cdot 5^2 \cdot 7^2$	$\left\{ \text{mcm} = 2^2 \cdot 3 \cdot 5^2 \cdot 7^2 = 14700$
-------------------------------	--------------------------------	--

(punto era che sotto i numeri dei
sono in entrambi)

- $\text{mcm}(A, B) = \frac{|A \cdot B|}{\text{MCD}(A, B)}$

massimo comune divisore: più grande divisore comune, $\text{MCD}(A, B) = \text{EUCLIDE}$

ALGORITMO DI EUCLIDE ESTESO

trovo S, T tali che $A \cdot S + B \cdot T = \text{MCD}(A, B)$

① ALGORITMO NORMALE

$$② A = B + C \rightarrow C = A - B$$

③ sostituisco A e B con i risultati delle operazioni precedenti

④ esprimi C come combinazione di A, \dots, B

⑤ arrivati all'ultima riga $C = \text{MCD}$ e: numeri moltiplicanti sono S e T

es.

$$\text{MCD}(519, 123) =$$

$$519 = 123 \cdot 4 + 27 \rightarrow 27 = 519 - 123 \cdot 4$$

$$123 = 27 \cdot 4 + 15 \rightarrow 15 = 123 - 27 \cdot 4 \rightarrow 123 + [519 + 123(-4)] = 519(-4) + 123(17)$$

$$27 = 15 \cdot 1 + 12 \rightarrow 12 = 27 - 15 \rightarrow [519 + 123(-4)] - [519(-4) + 123(17)] = 519(5) + 123(-21)$$

$$15 = 12 \cdot 1 + 3 \rightarrow 3 = 15 - 12$$

$$12 = 3 \cdot 4 + 0,$$

$$519 \cdot (-4) + 123 \cdot 38 = 3$$

$\underbrace{}_A \quad \underbrace{}_S \quad \underbrace{}_B \quad \underbrace{}_T \quad \underbrace{}_{\text{MCD}}$

EQUAZIONE DIOFANTINA:

trovo x, y (intei) in $A \cdot x + B \cdot y = C$

① con l'algoritmo di Euclide esteso trovo S, T, MCD

② moltiplico o divido per k per trasformare MCD in C (trovo x, y)

③ trovo le ∞ soluzioni

es.

$$867x + 120y = -15$$

• algoritmo: $867(9) + 120(-65) = 3$

• trasformo 3 in -15: $867(-45) + 120(325) = -15$
moltiplicando per -5

soluzione finale

$$② \left\{ \begin{array}{l} x = \dots \\ y = \dots \end{array} \right.$$

$$③ \alpha = \frac{A}{\text{MCD}}, \beta = \frac{B}{\text{MCD}}$$

$$\left\{ \begin{array}{l} x = \dots + \beta k \\ y = \dots - \alpha k \end{array} \right.$$

dim.

$$\boxed{\begin{aligned} \alpha(x) + \beta(y) &= \text{MCD} \\ A(x'k) + B(y'k) &= \text{MCD} \cdot k \\ A(x) + B(y) &= C \end{aligned}}$$

$$x = \frac{x'c}{k}, y = \frac{y'c}{k} : \text{numeri finiti}$$

Lemma: l'equazione ha soluzione solo se $\left(\exists \frac{C}{\text{MCD}(A, B)} \right) = \text{numero intero}$
t.c. $\text{MCD} \cdot n = C$

altrimenti non ha soluzione

dim.

$$C = Ax + By = \alpha d x + \beta d y = d(\alpha x + \beta y)$$

$$\xrightarrow{\text{impossibile}} \frac{C}{d} = (\alpha x + \beta y)$$

$$d = \text{MCD}$$

$\text{MCD} \neq 1$ ammette sempre soluzioni ($\forall c: \exists \frac{c}{d}$)

Esercizi

$$1) \left(\frac{2x}{3} + 3y = -1 \right) \xrightarrow{x \cdot 3} 2x + 9y = -3$$

$\exists \frac{-3}{\text{MCD}(2,9)} \rightarrow \frac{-3}{1} = -3$

$$\begin{aligned} 2 &= 9 \cdot 0 + 2 \quad \rightarrow 2 = 2 - 0 \\ 9 &= 2 \cdot 4 + 1 \quad \rightarrow 1 = 9 - 2 \cdot 4 \quad \rightarrow 1 = 9(1) + 2(-4) \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$\downarrow x(-3)$

$$-3 = 9(-3) + 2(-12)$$

$$2) \left(\frac{3x}{2} - \frac{y}{6} = \frac{1}{4} \right) \xrightarrow{x \cdot 12} 18x - 2y = 3 \quad \text{MCD}(18, -2) = 2 \quad \frac{2}{3} = \text{non esiste} \rightarrow \text{non ammette soluzioni}$$

$$3) 100x + 120y = w \quad \text{MCD}(100, 120) = 20 \quad \exists \frac{w}{20} = k ? \quad w = 20k$$

$$4) 999x - 99y = a + 5 \quad \text{MCD}(999, -99) = 9 \quad \exists \frac{a+5}{9} = k ? \quad a = 9k - 1$$

$$5) \left(\frac{7x}{6} + 2y = \frac{2}{3} \right) \xrightarrow{x \cdot 6} 7x + 12y = 4 \quad \text{MCD}(7, 12) = 1 \quad \frac{a}{1} = 1$$

$$7(-5) + 12(3) = 1 \quad \xrightarrow{x \cdot 4} \begin{cases} x = -5 \cdot 4 = -20 \\ y = 3 \cdot 4 = 12 \end{cases}$$

$$6) \text{MCD}(935, 363) = 11$$

$$935 = 363 \cdot 2 + 209$$

$$363 = 209 + 154$$

$$209 = 154 + 55$$

$$\begin{aligned} 154 &= 55 \cdot 2 + 44 \\ 55 &= 44 \cdot 1 + 11 \\ 44 &= 11 \cdot 4 + 0 \end{aligned}$$

$$\begin{aligned} 209 &= 935 + 363(-2) \\ 154 &= 363 + [935 + 363(-2)](-1) = 935(-1) + 363(3) \\ 55 &= [935 + 363(-2)] + [935(-1) + 363(3)](-1) = \\ &= 935(-2) + 363(-5) \\ 44 &= 935(-5) + 363(13) \quad \left. \begin{array}{l} \\ \end{array} \right\} 55 \cdot 44 = 11 (\text{MCD}) \\ 11 &= 935(7) + 363(-18) \end{aligned}$$

$$7) 21x + 56y = 1000$$

$$\text{MCD}(21, 56) = 7 \quad \frac{1000}{7} = 142 \rightarrow \text{nessuna soluzione}$$

$$8) ax + by = e \quad \text{MCD}(a, b) = 1 \rightarrow \frac{e}{1} = 1 \rightarrow \text{ammette sempre soluz. ovv.}$$