

14 - LE BASI TEORICHE DELL'ALGORITMO DI EUCLIDE PER IL CALCOLO DEL M.C.D.

Siano a, b due interi, e sia d un loro divisore comune.

Dico che d è pure divisore del resto che si ottiene effettuando la divisione intera $a : b$.

Infatti:

la divisione intera $a : b$ produce un "quoziente intero" q e un resto r ($r < b$), legati dalla relazione $a = q \cdot b + r$.
Ma se d è un divisore comune per a e b , allora d è contenuto un "numero esatto" di volte sia in a che in b , e ciò implica che sia contenuto un numero esatto di volte pure in r , perché

$$a = md \quad (m \text{ intero})$$

$$b = nd \quad (n \text{ intero})$$

IMPLICA

$$r = a - q \cdot b = md - qnd = \underbrace{(m - qn)}_{\text{intero}} d$$

Per capire meglio, vediamo un esempio specifico.

$$a = 186, b = 24, d = 6.$$

6 è divisore comune per 186 e 24.

Mi aspetto dunque che 6 sia pure divisore del resto che si ottiene

facendo la divisione intera $186 : 24$. Vediamo.

$$186 : 24 = 7 \text{ col resto di } \boxed{18} \quad (186 = 7 \cdot 24 + 18).$$

In effetti, 6 è divisore di 18!

E d'altronde: dato che 6 è contenuto

– un numero esatto di volte nel 186 (31 volte),

– e un numero esatto di volte nel 24 (4 volte)

PER FORZA 6 doveva essere contenuto un numero esatto di volte nel resto della divisione $186 : 24$, come spiega la catena

$$18 = \underbrace{186}_{31 \cdot 6} - 7 \cdot \underbrace{24}_{4 \cdot 6} = 31 \cdot 6 - 28 \cdot 6 = \underbrace{3}_{\text{intero}} \cdot 6$$

Siano a, b due numeri interi, e sia d un intero, che risulti divisore comune a uno di questi due numeri (ad esempio, b) e al resto della divisione intera $a : b$.

Dico che d è pure divisore dell'altro numero.

La giustificazione generale è analoga alla precedente.

Anche qui, un esempio gioverà alla comprensione.

$$a = 68, b = 20$$

$$68 : 20 = 3 \text{ col resto } r = 8 \quad (68 = 3 \cdot 20 + 8)$$

$d = 4$ è divisore comune per b ed r :

è contenuto un numero esatto di volte in $b = 20$ (5 volte),
e un numero esatto di volte in $r = 8$ (2 volte)

$$68 = 3 \cdot \underbrace{20}_{5 \cdot 4} + \underbrace{8}_{2 \cdot 4} = 15 \cdot 4 + 2 \cdot 4 = \underbrace{17}_{\text{intero}} \cdot 4$$

$d = 4$ è contenuto un numero esatto di volte in $a = 68$

Ricapitoliamo.

Ci sono tre interi in gioco, che sono a, b , ed r (resto di $a : b$).

Abbiamo scoperto che se d è divisore di DUE fra i tre interi considerati, allora sarà necessariamente divisore anche del terzo.

Dal discorso fatto, ci interessa trarre quanto segue.

Detti a, b due interi, e detto r il resto della divisione intera $a : b$, allora:

- se d è divisore comune per a, b , allora d è pure divisore comune per b, r
- se d è divisore comune per b, r , allora d è pure divisore comune per a, b

per cui

**l'insieme dei divisori comuni della coppia a, b
coincide con l'insieme dei divisori comuni della coppia b, r
quindi si ha pure**

$$\mathbf{M.C.D.(a, b) = M.C.D.(b, r)}$$

**Il vantaggio di tutto ciò sta nel fatto che
il calcolo di $M.C.D.(a, b)$
può essere sostituito da quello di $M.C.D.(b, r)$
che è più facile perché più piccoli sono i numeri in gioco.**

E' sulla base di queste considerazioni che "funziona"
l'ALGORITMO DI EUCLIDE per la ricerca del M.C.D.
di cui ci siamo occupati alle pagine precedenti.