L’algoritmo euclideo per il calcolo dell’MCD

Liceo G.B. Brocchi
Classi prime Scientifico – opzione scienze applicate
Bassano del Grappa, Maggio 2023

L’algoritmo di Euclide – definizione ricorsiva

```
gcd(a, b) = {
                a                    if b is 0
                gcd(b, a mod b)      otherwise
            }
```

- **NB**: a >= 0;
  gcd = **G**reatest **C**ommon **D**ivisor;
  a mod b: *a modulo b* (i.e. *resto di a / b*);

L'algoritmo di Euclide - dimostrazione

- Partiamo da questo presupposto:

  se **x** è divisibile per **y**, e **y** è divisibile per **x**, allora **x = +y** o **x = -y**

- Quindi, per mostrare che:

`gcd(a, b) = gcd(b, a mod b)`

mostreremo che **`gcd(a, b)`** è divisibile per **`gcd(b, a mod b)`**, e che **`gcd(b, a mod b)`** è divisibile per **`gcd(a, b)`**

1. Dimostrazione di: *«gcd(b, a mod b) divisibile per gcd(a, b)»*

- Dimostriamo che **`gcd(a, b) | gcd(b, a mod b)`**, ossia che **`gcd(a, b)`** divide **`gcd(b, a mod b)`**
- Sia **`d = gcd(a, b)`**, allora, essendo **`d`** il `MCD` di **`a`** e **`b`**, è vero che:
  - **`d | a`**, ossia **d** divide **a**
  - **`d | b`**, ossia **d** divide **b**

- Prima di procedere, consideriamo questi fatti:
  - **`a mod b = a – bq`**
    ovviamente deriva dalla definizione di divisione intera:
    `a = bq + (a mod b)`, dove **`q`** il quoziente di **`a / b`**
  - se **`d | a`** e **`d | b`**, allora **`d | ax + by`**, ossia **`d`** divide una qualsiasi combinazione lineare di **`a`** e **`b`** (corollario non dimostrato qui **`*`**)

1. Dimostrazione di: «*gcd(b, a mod b) divisibile per gcd(a, b)*»

- Abbiamo visto che **`a mod b = a – bq`**: questo significa che **`a mod b`** può essere visto come combinazione lineare di **`a`** e **`b`**
- Ma abbiamo appena detto (corollario *) che:
  - se **`d | a`** e **`d | b`**, allora **`d`** divide una qualunque combinazione lineare di **`a`** e **`b`**, quindi anche **`a – bq`**
  - concludiamo quindi che:
    - **`d | a – bq`** → **`d | a mod b`**
    - sappiamo dalle premesse che **`d | b`**
    - quindi **`d | gcd(b, a mod b)`** (corollario non dimostrato qui **)

Quindi, visto che avevamo posto **`d = gcd(a, b)`**, risulta:

`gcd(a, b) | gcd(b, a mod b)`

2. Dimostrazione di: «*gcd(a, b) divisibile per gcd(b, a mod b)*»

- Dimostriamo che **`gcd(b, a mod b) | gcd(a, b)`**, ossia che **`gcd(b, a mod b)`** divide **`gcd(a, b)`**

- Posto **`d = gcd(b, a mod b)`**, allora, essendo **`d`** il `MCD` di **`a`** e **`a mod b`**, è vero che:
  - **`d | b`**, ossia **`d`** divide **`b`**
  - **`d | a mod b`**, ossia **`d`** divide **`a mod b`**

2. Dimostrazione di: «*gcd(a, b) divisibile per gcd(b, a mod b)*»

- Ora consideriamo questi fatti:
  - **`a = bq + (a mod b)`**
    ovviamente deriva dalla definizione di divisione intera:

    `a / b = q con resto a mod b`
  - Abbiamo quindi espresso **`a`** come combinazione lineare di **`b`** e **`(a mod b)`**
  - Quindi, considerando che siamo partiti dal fatto che **`d | b`** e **`d | (a mod b)`**, abbiamo che **`d | a`** (perché abbiamo espresso **`a`** come combinazione lineare di **`b`** e **`a mod b`**)
  - Concludiamo che: **`d | b`** e **`d | a`**, e dunque che :

    `d | gcd(a, b)` (corollario non dimostrato qui ******)
  - Ma **`d`** era solo un altro nome per **`gcd(b, a mod b)`**, quindi abbiamo concluso che:

    `gcd(b, a mod b) | gcd(a, b)`

Q.E.D

Corollari * e **

***** Per ogni coppia di interi **a** e **b**, se **d | a** e **d | b**, allora:

$$d \mid ax + by$$

****** Per ogni coppia di interi **a** e **b**, se **d | a** e **d | b**, allora:

$$d \mid \gcd(a, b)$$