

Matematica Discreta

Stefano Piccoli

22 marzo 2022

Indice

Introduzione	2
1 Algoritmo di Euclide	3
2 Identità di Bezout	4

Introduzione

Capitolo 1

Algoritmo di Euclide

Siano a e b due interi con $0 \leq b \leq a$

1. Se $b = 0$ allora $MCD(a, b) = a$ e l'algoritmo **termina**
2. Se $b \neq 0$ faccio la **divisione euclidea** tra a e b :

$$a = b \cdot q + r, \quad 0 \leq r \leq b$$

Termina quando si trova $b = 0 \rightarrow MCD(a, b)$ è l'**ultimo resto non nullo**

3. Sostituisco $a = b$ e $b = r$ e riparto da **1**

Esempio $a = 168, b = 132$

$$168 = 132 \cdot 1 + 36 \rightarrow$$

$$132 = 36 \cdot 3 + 24 \rightarrow$$

$$36 = 24 \cdot 1 + 12 \rightarrow$$

$$24 = 12 \cdot 2 + 0$$

Capitolo 2

Identità di Bezout

Siano a e b due interi e $d = MCD(a, b)$ allora esistono \mathbf{x} e \mathbf{y} tali che:

$$a\mathbf{x} + b\mathbf{y} = d$$