ALGO

WWW.ALGORITMOSTEM.IT

SCIENCE TECHNOLOGY ENGINEERING MATHEMATICS

Appunti di Algebra1: Equazioni Diofantee

UNI - Matematica

rev.0.1 - 05 set 2023

Draft version

Appunti in formato bozza, intesi esclusivamente di ausilio alle lezioni, che le integrano nelle descrizioni e nei ragionamenti su quanto viene riportato in queste pagine.

Licenza Creative Commons CCBYNCND.
È consentita la condivisone del documento originale a condizione che non venga modificato né utilizzato a scopi commerciali, sempre attribuendo la paternità dell'opera all'autore

* Algoritmo di Euclide (MCD)
* Identità di Bezout
* Eq. Diofantee I GRADO

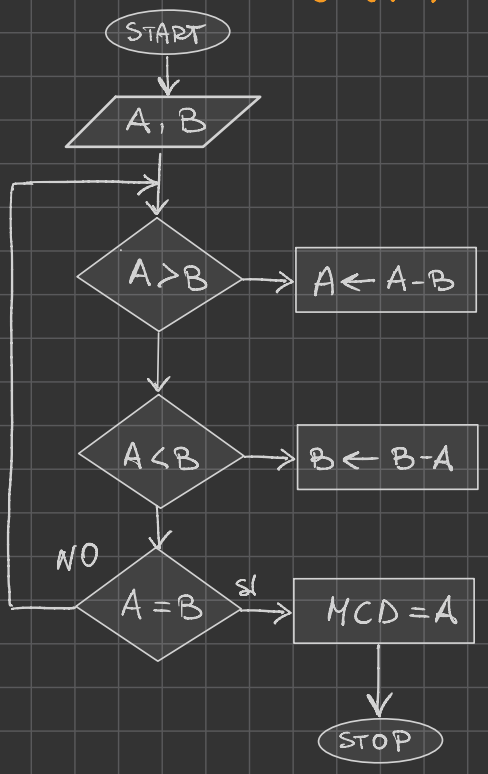
MCD (ALGORITMO DI EUCLIDE)

Si basa sulla divisione euclidea e si usa anche per trovare MCD (max comune divisore) tra polinomi

$0 \leq b < a$

1) se $b = 0$ → $MCD = a$
2) se $b \neq 0$ →
   - $a = bq + r$ con $0 \leq r < b$ — divisione con resto
   - $a = b$ — nuovo valore di a
   - $b = r$ — nuovo valore di b
   - ripeto il punto 2) finché b diventa 0
3) MCD è l'ultimo resto non nullo

Versione semplificata



A = 72
B = 30

A	B
72	30
42	18
12	6
6	→ MCD

A = 56
B = 30

A	B
56	30
26	4
22	2
18	
14	
10	
6	
2	→ MCD

ALGO - licenza d'uso creative common CCBYNCND - www.algoritmostem.it

Teorema (IDENTITÀ DI BEZOUT)

$a, b \in \mathbb{Z} \Rightarrow \exists\, x, y \in \mathbb{Z} \;/\; d = ax + by$

d = MCD = combinazione lineare di a e b

~~$\Leftrightarrow$~~ vale solo se $MCD(a,b) = 1$

per calcolare x e $y \in \mathbb{Z}$ si procede con l'algoritmo di Euclide e delle sostituzioni:

ESEMPIO

Calcolare $MCD(168, 132)$ e verificare l'id. di Bezout

$a=168 \quad b=132 \quad 168 = 132 \cdot 1 + 36 \rightarrow 36 = 168 - 132$

$a=132 \quad b=36 \quad 132 = 36 \cdot 3 + 24 \rightarrow 24 = 132 - 3 \cdot 36$

$= 132 - 3(168 - 132)$

$= -3 \cdot 168 + 4 \cdot 132$

$a=36 \quad b=24 \quad 36 = 24 \cdot 1 + 12 \rightarrow 12 = 36 - 24 =$

$= (168 - 32) - (-3 \cdot 168 + 4 \cdot 132)$

$= 4 \cdot 168 - 5 \cdot 132$

$a=24 \quad b=12 \quad 24 = 12 \cdot 2 + 0$

$a=12 \quad b=0 \rightarrow MCD = 12$

$x = 4 \quad y = -5$

$d = ax + by$

$12 = 168 \cdot 4 - 132 \cdot 5$

BEZOUT

ALGO - licenza d'uso creative common CCBYNCND - www.algoritmostem.it

EQ. DIOFANTEE I° grado

[1] $ax + by = c$ con $a, b, c \in \mathbb{Z}$

Risolvere un'eq. diofantea significa trovare le soluzioni $x, y \in \mathbb{Z}$ che soddisfano la [1]

Teorema

$\exists$ sol. $\in \mathbb{Z}$ di $ax+by+c$ $\overset{\text{ssl}}{\Leftrightarrow}$ $MCD(a,b)$ divide c

due casi:

1) se $c = 0$ ∞ soluzioni al variare di $t \in \mathbb{Z}$

$$\begin{cases} x = \dfrac{b}{MCD(a,b)} \cdot t \\ y = \dfrac{-a}{MCD(a,b)} \cdot t \end{cases}$$

2) se $c \neq 0$ ∞ soluzioni al variare di $t \in \mathbb{Z}$

$$\begin{cases} x = x_0 + \dfrac{b}{MCD(a,b)} \cdot t \\ y = y_0 - \dfrac{a}{MCD(a,b)} \cdot t \end{cases}$$

con x_0, y_0 soluz. particolari calcolate con l'identità di Bezout

ALGO - licenza d'uso creative common CCBYNCND - www.algoritmostem.it

ESEMPIO

1) Trovare tutte le soluzioni intere di $100x+102y=9$. $50x+52y=11$

Sol. Si ha che $M.C.D.(100,102)=2$ non divide 9. Quindi non ci sono soluzioni intere.

$(50,52)=2$ non divide 11

ESEMPIO

2) Trovare tutte le soluzioni intere di $168x+132y=0$.

Sol. Abbiamo visto che $M.C.D.(168,132)=12$.

Le soluzioni sono quindi tutte e sole della forma:

$$x=\frac{132}{M.C.D.(168,132)}\cdot t=\frac{132}{12}\cdot t=11t$$

$$y=-\frac{168}{M.C.D.(168,132)}\cdot t=-\frac{168}{12}\cdot t=-14t$$

al variare di $t\in Z$.

ALGO - licenza d'uso creative common CCBYNCND - www.algoritmostem.it

ESEMPIO

3) Trovare tutte le soluzioni intere di $168x+132y=36$.

0) Si ha che $M.C.D.(168,132)=12$ divide $36 \longrightarrow$ l'equazione ha soluzioni intere.

1) Risolvo l'identità di Bezout: trovo $\tilde{x}$ e $\tilde{y}$ t.c. $168\tilde{x}+132\tilde{y}=M.C.D.(168,132)=12$.

2) Le soluzioni particolari saranno:

$$x_0=\frac{36}{M.C.D.(168,132)}\tilde{x}=3\tilde{x} \quad e \quad y_0=\frac{36}{M.C.D.(168,132)}\tilde{y}=3\tilde{y}$$

3) Le soluzioni generali saranno:

$$x=x_0+\frac{132}{M.C.D.(168,132)}\cdot t=x_0+12t \quad e \quad y=y_0-\frac{168}{M.C.D.(168,132)}\cdot t=y_0-14t$$

al variare di $t\in Z$.

1) Risolvo l'identità di Bezout: trovo $\tilde{x}$ e $\tilde{y}$ t.c. $168\tilde{x}+132\tilde{y}=M.C.D.(168,132)=12$.

Si usa l'algoritmo di Euclide come visto in precedenza.

$168 = 132\cdot 1+36 \longrightarrow 36 = 168-132$

$132 = 36\cdot 3+24 \longrightarrow 24 = 132-3\cdot 36 = 132-3\cdot(168-132) = -3\cdot 168+4\cdot 132$

$36 = 24\cdot 1+12 \longrightarrow 12 = 36-24 = 168-132-(-3\cdot 168+4\cdot 132) = 4\cdot 168-5\cdot 132$

$24 = 12\cdot 2+0 \longrightarrow M.C.D.(168,132)=12 \longrightarrow \tilde{x}=4, \tilde{y}=-5$

2) Le soluzioni particolari saranno:

$$x_0=\frac{36}{M.C.D.(168,132)}\tilde{x}=3\tilde{x} \quad e \quad y_0=\frac{36}{M.C.D.(168,132)}\tilde{y}=3\tilde{y} \longrightarrow x_0=12 \ e \ y_0=-15$$

3) Le soluzioni generali saranno:

$$x=x_0+\frac{132}{M.C.D.(168,132)}\cdot t=x_0+12t \ e \ y=y_0-\frac{168}{M.C.D.(168,132)}\cdot t=y_0-14t \longrightarrow \begin{matrix} x=12+12t \\ y=-15-14t \end{matrix} \quad t\in Z$$

al variare di $t\in Z$.

ALGO - licenza d'uso creative common CCBYNCND - www.algoritmostem.it

Per risolvere $ax+by=c$ ...

$(c \neq 0)$

1) Calcolo $M.C.D.(a, b)$;

2) Risolvo $ax+by=0$ usando il teorema visto prima;

3) Risolvo l'identità di Bezout: trovo $\tilde{x}$ e $\tilde{y}$ t.c. $a\tilde{x}+b\tilde{y}=M.C.D.(a, b)$;

4) Le soluzioni particolari saranno: $x_0=\frac{c}{M.C.D.(a, b)} \cdot \tilde{x}$ e $y_0=\frac{c}{M.C.D.(a, b)} \cdot \tilde{y}$;

5) Le soluzioni generali si ottengono sommando le soluzioni particolari con quelle trovate al punto 2).

ALGO - licenza d'uso creative common CCBYNCND - www.algoritmostem.it

Esempio

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 6 \\ x \equiv 1 \pmod 7 \end{cases}$$

0) 5, 6 e 7 sono a due a due coprimi.

1) $N = 5 \cdot 6 \cdot 7 = 210$

$N_1 = 6 \cdot 7 = 42$

$N_2 = 5 \cdot 7 = 35$

$N_3 = 5 \cdot 6 = 30$

2) Risolvo le congruenze:

$42\,y_1 \equiv 1 \pmod 5 \longrightarrow 2\,y_1 \equiv 1 \pmod 5 \rightarrow y_1 \equiv 3 \pmod 5$

$35\,y_2 \equiv 1 \pmod 6 \longrightarrow -y_2 \equiv 1 \pmod 6 \rightarrow y_2 \equiv -1 \pmod 6$

$30\,y_3 \equiv 1 \pmod 7 \longrightarrow 2\,y_3 \equiv 1 \pmod 7 \rightarrow y_3 \equiv 4 \pmod 7$

3) La soluzione del sistema è:

$x \equiv 2 \cdot 42 \cdot 3 + 3 \cdot 35 \cdot (-1) + 1 \cdot 30 \cdot 4 \pmod{210} \longrightarrow x \equiv 57 \pmod{210}.$

ESERCIZIO

2. Per quanti interi n, $1 \le n \le 143$ il numero $n^2 - 5n + 6$ è un multiplo di 143?

SOLUZIONE

Scompongo: $n^2 - 5n + 6 = (n-2)(n-3)$ e $143 = 11 \cdot 13$.

Quattri casi possibili:

a) $n-2$ è multiplo di 143; $\longrightarrow$ $n-2 = 0 \rightarrow n = 2$ (perché $1 \le n \le 143$)

b) $n-3$ è multiplo di 143; $\longrightarrow$ $n-3 = 0 \rightarrow n = 3$ // //

c) $n-2$ è multiplo di 11 e $n-3$ è multiplo di 13;

d) $n-2$ è multiplo di 13 e $n-3$ è multiplo di 11.

Il caso c) equivale a:

$$\begin{cases} n \equiv 2 \pmod{11} \\ n \equiv 3 \pmod{13} \end{cases} \longrightarrow \text{1 soluzione modulo 143 } (n = 68)$$

Il caso d) equivale a:

$$\begin{cases} n \equiv 3 \pmod{11} \\ n \equiv 2 \pmod{13} \end{cases} \longrightarrow \text{1 soluzione modulo 143 } (n = 80)$$

In totale, 4 interi.

con algoritmo cinese

con algoritmo cinese

ALGO - licenza d'uso creative common CCBYNCND - www.algoritmostem.it