Algoritmo euclideo e identita' di Bezout

L'algoritmo euclideo delle divisioni successive per il calcolo del MCD d tra due interi a e b, ci permette di scrivere una relazione che lega a, b, d : $\boldsymbol{ka} + \boldsymbol{hb} = \boldsymbol{d}$.

Calcoliamo MCD(126,35) con il metodo delle divisioni successive e ad ogni divisione scriviamo il dividendo come il prodotto del divisore per il quoziente più il resto.

$$126 = 35 \cdot 3 + 21$$

$$35 = 21 \cdot 1 + 14$$

$$21 = 14 \cdot 1 + 7$$

$$14 = 2 \cdot 7 + 0$$

Dato che l'ultimo resto non nullo è 7, quello sarà il MCD.

Ora riscriviamo a ritroso i resti e vediamo cosa riusciamo ad ottenere con un po' di calcoli:

$$\mathbf{7} = 21 - 14 \cdot 1 = 21 - (35 - 21 \cdot 1) = 21 - 35 + 21 =$$

$$= 2 \cdot 21 - 35 = 2 \cdot (126 - 35 \cdot 3) - 35 = 2 \cdot 126 - 6 \cdot 35 - 35 == 2 \cdot \mathbf{126} - 7 \cdot \mathbf{35}\ .$$

Quindi con l'algoritmo euclideo abbiamo trovato i valori di $K = 2\ e\ h = -7$ che permettono di verificare la relazione $\boldsymbol{ka} + \boldsymbol{hb} = \boldsymbol{d}$.

Esercizi : Calcolare il MCD e la relativa identità di Bezout tra le seguenti coppie di numeri: 44275 e 605; 2470 e 351.

Equazioni lineari diofantee

Vediamo come l'identità di Bezout ci viene in aiuto per aiutare a risolvere delle equazioni lineari in Z : $ax + by = c\ in\ Z(\ con\ a, b, c\ \in\ Z)$.

Il caso in cui $c = 0$ l'equazione si dice **omogenea**, in tal caso dopo aver semplificato i termini $a\ e\ b$ tutte le soluzioni saranno del tipo (bt, at) con t$\in Z$.

Esempio $4x - 6y = 0$, dividiamo per 2 (che è il MCD), l'equazione diventa $2x - 3y = 0$, tutte le soluzioni sono del tipo $(3t, 2t)$. Se fosse stata $2x + 3y = 0$, sarebbe stato $(3t, -2t)$.

Se l'equazione non è omogenea allora $ax + by = c, c \neq 0$.

Vale il seguente **teorema** che non dimostriamo:

L'equazione $\boldsymbol{ax + by = c}$ ha soluzioni in $\boldsymbol{Z}$ se e solo se MCD $(\boldsymbol{a}, \boldsymbol{b})$ divide $\boldsymbol{c}$.

Esempio: $21x + 15y = 14$ ha soluzioni in Z? La risposta è No perché MCD (21,15) =3 e 3 non divide 14, quindi l'equazione non ha soluzioni in Z per il teorema prima enunciato. Invece l'equazione $21x + 5y = 6$ ha soluzioni in Z.

Come possiamo trovare le soluzioni?

Se fosse stato $21x + 15y = 3$ ci ricorderemmo dell'identità di Bezout con $(a, b) = (21,15)$ $d = 3$ e x, y i due valori k e h dell'identità di Bezout.

Allora scriviamo l'identità di Bezout dall'algoritmo euclideo:

$21 = 15 \cdot 1 + 6; \quad 15 = 6 \cdot 2 + 3$

Riscriviamo i resti

$\mathbf{3} = 15 - 6 \cdot 2 = 15 - (21 - 15 \cdot 1) \cdot 2 = 15 - 21 \cdot 2 + 2 \cdot 15 = \mathbf{-2 \cdot 21 + 3 \cdot 15.}$

Abbiamo perciò trovato $x = -2$ e $y = 3$.

Dato che $c = 6$ e $d = 3$ quindi c è il doppio di 2 , allora posso moltiplicare la coppia $(-2,3)$ per 2 e verificherà l'equazione di partenza.

Quindi la coppia $(-4,6)$ è una soluzione dell'equazione di partenza, ma le soluzioni sono infinite e si possono determinare aggiungendo le soluzioni dell'omogenea associata $21x + 15y = 0$ cioè $7x + 5y = 0$ e cioè $(5t, -7t)$. Perciò le soluzioni di $21x + 15y = 6$ saranno tutte le coppie del tipo $(-4 + 5t, 6 - 7t)$ al variare di $t \ in \ Z$.

****Osserviamo che $\boldsymbol{ax + by = c}$ è una equazione con le congruenze $\boldsymbol{ax \equiv cmodb}$ ****

Esercizi: Date le seguenti equazioni in Z dire se ammettono soluzioni e, in caso affermativo, determinarle:

$2x + 7y = 5;$

$6x - 8y = 3;$

$21x + 3y = 6$