EQUAZIONI CONGRUENZIALI

Siano a, b ed m interi relativi. Si dice equazione congruenziale di termini a, b ed m la seguente applicazione:

$w[a,b,m]: c \in \mathbb{Z} \to [a \cdot c - b]_m \in \mathbb{Z}_m$ e si indica $a \cdot x \equiv b (\mathrm{mod}\, m)$

L'equazione congruenziale ammette soluzioni se esiste $\overline{c} : \left(w[a,b,m]\right)(\overline{c}) = [0]_m$ cioè se $[a \cdot \overline{c} - b]_m = [0]_m$ ovvero se $a \cdot \overline{c} - b \in m\mathbb{Z}$.

Teorema: Siano $a, b, m \in \mathbb{Z}$. L'equazione congruenziale $a \cdot x \equiv b (\mathrm{mod}\, m)$ ammette soluzione se e solo se un massimo comune divisore di a ed m divide b.

Ricerca di una soluzione di un'equazione congruenziale

Sia $a \cdot x \equiv b (\mathrm{mod}\, m)$ l'equazione congruenziale di cui si vuole trovare una soluzione; sia $d = \mathrm{MCD}(a,m)$ (la ricerca del massimo comune divisore può essere effettuata mediante l'opportuno software compreso nel pacchetto Turbo Prolog); si troveranno due interi positivi h, k tali che $d = a \cdot h + m \cdot k$ ed esisterà $b_1 \in \mathbb{Z}$ tale che $b = d \cdot b_1$; a questo punto la soluzione sarà $x = h \cdot b_1$.

Esempio

$$169 \cdot x \equiv 26 (\mathrm{mod}\, 39)$$

Un massimo comune divisore di 169 e 39 è 13; quindi nel caso specifico $a = 169, b = 26, m = 39, d = 13$; si osserva che $13 = 169 \cdot 1 + 39 \cdot (-4)$ dunque $h = 1, k = -4$, inoltre $26 = 13 \cdot 2$ così $b_1 = 2$. In conclusione $x = 1 \cdot 2 = 2$ cioè $x = 2$.

Verifichiamo che $x = 2$

$[169 \cdot 2 - 26]_{39} = [338 - 26]_{39} = [312]_{39} = [0]_{39}$ in quanto $\frac{312}{39} = 8$ con resto nullo.