MCD (Algoritmo Euclideo)

- MCD(76, 60)

$76 = 60 \cdot 1 + 16 \Rightarrow 60 = 16 \cdot 3 + 12 \Rightarrow 16 = 12 \cdot 1 + 4 \Rightarrow 12 = 4 \cdot 3 + 0$ $\quad MCD(76, 60) = 4$

EQUAZIONI CONGRUENZIALI

$299x \equiv 52 (247)$ vediamo se esistono soluz. Trovando MCD(299, 247)

$299 = 247 \cdot 1 + 52, 247 = 52 \cdot 4 + 39, 52 = 39 \cdot 1 + 13, 39 = 13 \cdot 3$ $\quad MCD(299, 247) = 13$

13 divide 52 quindi l'equazione ammette soluzioni in $\mathbb{Z}$

$d = au + bv \quad x_0 = \frac{b}{d} u = \frac{52}{13} u = 4u$

$13 = 52 - 39 = 52 - (247 - 52 \cdot 4) = 52 - 247 - 52 \cdot 4 = 52 \cdot 5 - 247 - 5(299 - 247) - 247 =$

$= 299 \cdot 5 - 247 \cdot 5 - 247 = 299 \cdot 5 + 247(-6)$ 13 combinaz. lineare di a e b

$u = 5 \quad x_0 = 4 \cdot 5 = 20 \rightarrow 299 \cdot 20 - 52 = k247 = 26 \cdot 247$ si trova!

SISTEMI DI EQUAZIONI CONGRUENZIALI

$\begin{cases} x \equiv 1 (2) \\ x \equiv 2 (3) \\ x \equiv 3 (5) \end{cases}$ $\quad (2,3) = 1$ sono a due a due coprimi quindi il $\quad (3,5) = 1$ sistema ammette soluzioni.

1) $t \equiv 1 (2) \Leftrightarrow t - 1 = 2k \Leftrightarrow t = 2k + 1 \quad I_1 = \{2k + 1, k \in \mathbb{Z}\}$

2) $2k + 1 \equiv 2 (3) \Leftrightarrow 2k \equiv 1 (3) \Leftrightarrow 2k - 1 = 3h \quad k = 2 \quad x = 2k + 1 = 2 \cdot 2 + 1 = 5 \quad I_2 = [5]_6$

$I_1 \cap I_2 = \{5 + 6k, k \in \mathbb{Z}\}$

3) $5 + 6k \equiv 3 (5) \Leftrightarrow 6k \equiv -2 (5) \Leftrightarrow 3k \equiv -1 (5) \Leftrightarrow 3k + 1 = 5h$

$k = 3 \quad x = 5 + 6 \cdot 3 = 23 \quad I_3 = [23]_{30} \quad I_1 \cap I_2 \cap I_3 = \{23 + 30k, k \in \mathbb{Z}\}$

CICLI E PERMUTAZIONI

--File not found--