Soluzioni proposte appello del 10/06/2024

Fondamenti Matematici dell'Informatica

Esercizio 1. Si determinino tutte le soluzioni del seguente sistema di congruenze:

$$\begin{cases} x \equiv 28 \pmod{108} \\ x \equiv 64 \pmod{78} \end{cases}.$$

Si dimostri inoltre che tutte le soluzioni del sistema sono divisibili per 4.

Svolgimento. Sia $S \subset \mathbb{Z}$ l'insieme delle soluzioni del sistema.
Passo 1: Compatibilità. Grazie al teorema cinese del resto, sappiamo che $S \neq \emptyset$ se e soltanto se

$$\mathrm{MCD}(108, 78) \mid 64 - 28 = 36. \tag{1}$$

Decomponendo in fattori primi, si trova $108 = 2^2 \cdot 3^3$ e $78 = 2 \cdot 3 \cdot 13$, da cui $\mathrm{MCD}(108, 78) = 6$. Pertanto la (1) è verificata e $S \neq \emptyset$. Osserviamo inoltre che

$$64 - 28 = 6 \cdot \mathrm{MCD}(108, 78). \tag{2}$$

Passo 2: Calcolo di una soluzione particolare. Determiniamo una soluzione $x_0 \in S$. Iniziamo applicando l'algoritmo di Euclide con sostituzione "a ritroso" dei resti alla coppia (108,78):

$$\begin{array}{r|l}
108 = 1 \cdot 78 + 30 & 30 = 108 - 1 \cdot 78 \\
78 = 2 \cdot 30 + 18 & 18 = 78 - 2 \cdot 30 \\
30 = 1 \cdot 18 + 12 & 12 = 30 - 1 \cdot 18 \\
18 = 1 \cdot 12 + 6 & 6 = 18 - 1 \cdot 12 = 18 - (30 - 1 \cdot 18) = 2 \cdot 18 - 30 = \\
\cancel{12 = 2 \cdot = 6 + 0} & \quad = 2 \cdot (78 - 2 \cdot 30) - 30 = 2 \cdot 78 - 5 \cdot 30 = \\
 & \quad = 2 \cdot 78 - 5 \cdot (108 - 1 \cdot 78) = 7 \cdot 78 - 5 \cdot 108
\end{array}$$

Otteniamo quindi

$$\mathrm{MCD}(108, 78) = 7 \cdot 78 - 5 \cdot 108$$

e, sostituendo nell'equazione (2) otteniamo

$$64 - 28 = 6 \cdot (7 \cdot 78 - 5 \cdot 108) = 42 \cdot 78 - 30 \cdot 108.$$

Ricaviamo adesso una soluzione particolare x_0 a partire dalla precedente uguaglianza:

$$64 - 28 = 42 \cdot 78 - 30 \cdot 108 \iff 64 - 42 \cdot 78 = 28 - 30 \cdot 108 \iff -3212 = -3212.$$

Pertanto $x_0 = -3212 \in S$ è una soluzione particolare del sistema.
Passo 3: calcolo di S. Grazie al teorema cinese del resto sappiamo quindi che

$$S = [-3212]_{\mathrm{mcm}(108,78)}.$$

Ma

$$\mathrm{mcm}(108, 78) = \frac{108 \cdot 78}{\mathrm{MCD}(108, 78)} = \frac{2^2 \cdot 3^3 \cdot 2 \cdot 3 \cdot 13}{6} = 2^2 \cdot 3^3 \cdot 13 = 1404$$

e quindi abbiamo trovato che

$$S = [-3212]_{1404} = [-3212 + 3 \cdot 1404]_{1404} = [1000]_{1404} = \{1000 + 1404 \cdot k : k \in \mathbb{Z}\} \subset \mathbb{Z}.$$

Domanda finale. Osserviamo che

$$1000 = 4 \cdot 250, \quad 1404 = 4 \cdot 351 \implies [1000]_4 = [0]_4 \text{ e } [1404]_4 = [0]_4.$$

Sia ora $x \in S$ una soluzione del sistema. Per definizione, esiste $k \in \mathbb{Z}$ tale che $x = 1000 + 1404 \cdot k$: la richiesta è adesso equivalente a dimostrare che $[x]_4 = [0]_4$. Vale

$$\begin{aligned} [x]_4 &= [1000 + 1404 \cdot k]_4 \\ &= [1000]_4 + [1404]_4 \cdot [k]_4 \\ &= [0]_4 + [0]_4 \cdot [k]_4 \\ &= [0]_4 \end{aligned}$$

come volevamo mostrare. Pertanto ogni soluzione del sistema è divisibile per 4.