ALGEBRA (M-Z)

(2018-19)

Sistemi di congruenze

1. Risolvere il seguente sistema di congruenze:

$$\begin{cases} 15\,x \equiv 23 \mod 37 \\ 37\,x \equiv 15 \mod 22 \end{cases}$$

Sol.

Passo 1: Compatibilità: MCD(37,22) = 1; 1 = MCD(15,37) / 23; 1 = MCD(37,22) / 15; quindi il sistema è compatibile.

Passo 2: Semplificazione: $37 \equiv 15 \ mod\ 22$. Dunque il sistema è equivalente al sistema:

$$\begin{cases} 15\,x \equiv 23 \mod 37 \\ x \equiv 1 \mod 22 \end{cases}$$

Passo 3: Risoluzione: dalla seconda congruenza si ricava x = 1+ 22*k* (1 sola soluzione *mod* 22) e sostituendo nella prima congruenza si ricava:

$$15(1+22k) \equiv 23 \ mod\ 37 \Rightarrow 15+ 330k \equiv 23\ mod\ 37 \Rightarrow 15 + 34k \equiv 23 \ mod\ 37 \Rightarrow$$
$$34k \equiv 8 \ mod\ 37 \Rightarrow k \equiv (34)^{-1}\ 8 \ mod\ 37.$$

Per determinare l'inverso di 34 in $\mathbf{Z_{37}}$ si usa l'identità di Bézout: 1 = 34 (12) +37(-11) e dunque si ha:

$$k \equiv (34)^{-1}\ 8 \ mod\ 37 \Rightarrow k \equiv (12)\ 8 \equiv 96 \equiv 22 \ mod\ 37.$$

Pertanto l'unica soluzione *mod* [(37x22) = 814] è $x \equiv 1+484 \equiv 485$.
Infatti abbiamo una coppia $([22]_{37}\ ,\ [1]_{22})$ dove la prima coordinata è soluzione della prima congruenza e la seconda coordinata è soluzione della seconda. Poiché
f : $\mathbf{Z_{814}} \rightarrow \mathbf{Z_{37}x\ Z_{22}}$ definito da: $f\,[y]_{814} = ([y]_{37},[y]_{22})$ è un isomorfismo di ha:

$$([22]_{37}\ ,\ [1]_{22}) = ([485]_{37},[485]_{22})$$