Corso di Laurea in Informatica
Algebra. a.a. 2023-24. Canale 1.
Compito in classe per la mattina del 15/11/2023. Soluzioni.

Esercizio 1. Stabilire se l'equazione congruenziale

$$20x \equiv 50\,(\mathrm{mod}30)$$

ammette soluzioni ed in caso affermativo determinare tutte le soluzioni non congruenti.

Soluzione. $(20, 30) = 10$ e $10 \mid 50$. Quindi l'equazione ammette soluzioni e sappiamo, Prop. 2.7.5, che essa ammette precisamente 10 soluzioni non congruenti. Dalla Prop. 2.6.5. di [PC] sappiamo che se $20x \equiv 50\,(\mathrm{mod}30)$ allora $2x \equiv 5\,(\mathrm{mod}\frac{30}{d})$ con $d = (50, 30)$. Si ha $d = 10$ e quindi

$$20x \equiv 50\,(\mathrm{mod}30) \Rightarrow 2x \equiv 5\,(\mathrm{mod}3)$$

Vale anche il viceversa della Prop. 2.7.7. (facile, dimostratelo....) quindi

$$20x \equiv 50\,(\mathrm{mod}30) \text{ se e solo se } 2x \equiv 5\,(\mathrm{mod}3).$$

Quest'ultima equazione è facilmente risolvibile perché equivale a

$$[2][x] = [5] \quad \text{in} \quad \mathbb{Z}_3$$

$[2]$ ha inverso moltiplicativo in $\mathbb{Z}_3$ uguale a $[2]$; quindi otteniamo l'equazione $[x] = [10]$ e cioè $[x] = [1]$. Quindi $x_0 = 1$ è una soluzione di $2x \equiv 5\,(\mathrm{mod}3)$ e quindi dell'equazione originale. Ovviamente si vedeva anche a occhio che $x_0 = 1$ era soluzione dell'equazione originale: mi sono dilungato perché questo è il metodo generale.
Per la Prop. 2.7.5 tutte le soluzioni non congruenti sono, osservato che $30/10 = 3$,

$$\{1, 1 + 3, 1 + 3 \cdot 2, \ldots\ldots, 1 + 3 \cdot 9\}$$

e quindi l'insieme delle soluzioni non congruenti è

$$\{1, 4, 7, 10, 13, 16, 19, 22, 25, 28\}$$

Esercizio 2. Consideriamo il sistema

$$\begin{cases} 4x \equiv 1\,(\mathrm{mod}5) \\ x \equiv 5\,(\mathrm{mod}6) \\ 4x \equiv 3\,(\mathrm{mod}7) \end{cases}$$

Stabilire se il sistema ammette soluzioni ed in caso affermativo determinarle.

Soluzione.
$(4, 5) = 1$ e $1 \mid 1$; $(1, 6) = 1$ e $1 \mid 5$; $(4, 7) = 1$ e $1 \mid 3$; inoltre $(5, 6) = 1$, $(6, 7) = 1$, e $(5, 7) = 1$ e quindi il sistema è risolubile. Possiamo portarlo in forma cinese operando come segue:
moltiplichiamo la prima equazione per l'inverso moltiplicativo di $[4]$ in $\mathbb{Z}_5$, che è $[4]$; otteniamo l'equazione $x \equiv 4\,(\mathrm{mod}5)$; la seconda equazione la teniamo com'è; la terza equazione la moltiplichiamo per l'inverso moltiplicativo di $[4]$ in $\mathbb{Z}_7$ che è $[2]$ e otteniamo $x \equiv 6\,(\mathrm{mod}7)$. In definitiva il sistema è equivalente al sistema cinese:

$$\begin{cases} x \equiv 4\,(\mathrm{mod}5) \\ x \equiv 5\,(\mathrm{mod}6) \\ x \equiv 6\,(\mathrm{mod}7) \end{cases}$$

Ora applichiamo la dimostrazione dell'esistenza di una soluzione, che sappiamo sarà unica modulo $5 \cdot 6 \cdot 7$. Quindi

$$R = 5 \cdot 6 \cdot 7 = 210,\ R_1 = 6 \cdot 7,\ R_2 = 5 \cdot 7,\ R_3 = 5 \cdot 6$$

e consideriamo le 3 equazioni

$$R_1 x \equiv 4\,(\mathrm{mod}5),\quad R_2 x \equiv 5\,(\mathrm{mod}6),\quad R_3 x \equiv 6\,(\mathrm{mod}6)$$

con soluzioni rispettivamente

$$\overline{x}_1 = 12,\ \ \overline{x}_2 = 1,\ \ \overline{x}_3 = 24\,.$$

La soluzione è allora

$$\overline{x} = R_1\overline{x}_1 + R_2\overline{x}_2 + R_3\overline{x}_3$$

e cioè 1259; ma $1259 \equiv 209\,(\mathrm{mod}\,5 \cdot 6 \cdot 7)$ e quindi la soluzione è $\overline{x} = 209$ ed è unica modulo 210.

Esercizio 3.
1. Determinare $\mathcal{U}(\mathbb{Z}_{15})$.
2. Per ogni $a \in \mathcal{U}(\mathbb{Z}_{15})$ calcolare a^{1347}

Soluzione.
Gli elementi invertibili di $\mathbb{Z}_{15}$ sono i numeri k fra 1 e 15 che sono coprimi con 15; quindi

$$\mathcal{U}(\mathbb{Z}_{15}) = \{[1], [2], [4], [7], [8], [11], [13], [14]\}$$

Per calcolare a^{1347} per ognuno di questi a applichiamo il Teorema di Eulero: $\phi(15) = 2 \cdot 4 = 8$; ora, $1347 = 168 \cdot 8 + 3$ e quindi

$$a^{1347} = a^{168 \cdot 8 + 3} \equiv a^{168 \cdot \phi(15) + 3} = (a^{\phi(15)})^{168} a^3 = a^3$$

A questo punto dobbiamo solo calcolare il cubo degli elementi in $\mathcal{U}(\mathbb{Z}_{15})$ e questi sono

$$\{[1], [8], [4], [13], [2], [11], [7], [14]\}$$

Esercizio 4. Sia G un gruppo, $f : G \to G$ un endomomorfismo[1] di G e H un sottogruppo di G.

(1) Verificare che, per ogni $a, b \in G$ se $ab = ba$, allora $a^{-1}b = ba^{-1}$.
(2) Verificare che

$$K := \{x \,\big|\, x \in G,\ f(xh) = f(hx)\ \forall h \in H\}$$

è un sottogruppo di G. Suggerimento: dovrete utilizzare (1).
(3) Dimostrare che se H è normale in G allora K è normale in G.

Soluzione.
(1) Siano $a, b \in G$ tali che $ab = ba$. Allora $b = a^{-1}ab = a^{-1}ba$. Dunque $ba^{-1} = a^{-1}baa^{-1} = a^{-1}b$.

(2) K è non vuoto poichè $1_G \in K$ (infatti $f(1_G h) = f(h) = f(h1_G)$ per ogni $h \in H$).

Siano ora $x, y \in K$ e $h \in H$. Vogliamo provare che $xy^{-1} \in K$, ovvero $f(xy^{-1}h) = f(hxy^{-1})$. Poichè f è un omomorfismo,

$$f(xy^{-1}h) = f(x)f(y^{-1}h) = f(x)f(y^{-1})f(h) = f(x)f(y)^{-1}f(h).$$

[1]Un omomorfismo di G in G è detto un endomorfismo

Essendo $y \in K$, $f(y)f(h) = f(h)f(y)$ e, per (1), anche $f(y)^{-1}$ commuta con $f(h)$. Pertanto, sfruttando che anche $x \in K$, si ha

$$f(xy^{-1}h) = f(x)f(h)f(y)^{-1} = f(x)f(h)f(y^{-1}) = f(xh)f(y^{-1}) = f(hx)f(y^{-1}) = f(hxy^{-1}).$$

(3) Siano $x \in K$, $h \in H$ e $g \in G$. Vogliamo provare che K è normale in G, ovvero $f(g^{-1}xgh) = f(hg^{-1}xg)$. A tal fine,

$$f(g^{-1}xgh) = f(g^{-1}xghg^{-1}g) = f(g^{-1}x(ghg^{-1})g).$$

Ma $ghg^{-1} \in H$ dato che H è normale in G. Dunque

$$f(g^{-1}xgh) = f(g^{-1})f(ghg^{-1})f(x)f(g) = f(hg^{-1}xg).$$