Compitino di MDAL
14 giugno 2017

Cognome e nome: .....

Numero di matricola: ..... Corso e Aula: .....

IMPORTANTE: Non si possono consultare libri e appunti. Non si possono usare calcolatrici, computer o altri dispositivi elettronici. Non si può scrivere con il lapis.

Esercizio 1. Risolvere le seguenti equazioni di congruenze:

(a) $4x \equiv a \pmod{15}$, dove $a \in \mathbb{Z}$ è un parametro;

(b) $x^2 \equiv 1 \pmod{143}$;

(c) $3^{x+2} \equiv 5 \pmod{7}$.

Per quali valori di a il sistema con le equazioni (a), (b), (c) ammette soluzione?

Il sistema è risolubile se e solo se $a \equiv 0 \bmod 3$.

Svolgimento:

(a) Siccome $4 \cdot 4 \equiv 1 \bmod 15$, moltiplicando per 4 si vede che la prima congruenza equivale a $\boxed{x \equiv 4a \bmod 15}$, che si può anche scrivere nella forma $\begin{cases} x \equiv a \bmod 3 \\ x \equiv 4a \bmod 5 \end{cases}$

(b) La seconda congruenza si può riscrivere nella forma $(x-1)(x+1) \equiv 0 \bmod 143$ che per il teorema cinese dei resti equivale al sistema
$\begin{cases} (x-1)(x+1) \equiv 0 \bmod 11 \\ (x-1)(x+1) \equiv 0 \bmod 13 \end{cases}$.
Quando il modulo è primo, un prodotto di due numeri è congruo a zero se e solo se uno dei due è congruo a zero. Quindi il nostro sistema equivale alla disgiunzione dei seguenti quattro sistemi:
$\begin{cases} x \equiv 1 \bmod 11 \\ x \equiv 1 \bmod 13 \end{cases}$ oppure $\begin{cases} x \equiv -1 \bmod 11 \\ x \equiv -1 \bmod 13 \end{cases}$ oppure
$\begin{cases} x \equiv 1 \bmod 11 \\ x \equiv -1 \bmod 13 \end{cases}$ oppure $\begin{cases} x \equiv -1 \bmod 11 \\ x \equiv 1 \bmod 13 \end{cases}$
che equivalgono rispettivamente a
$x \equiv 1 \bmod 143$ oppure $x \equiv -1 \bmod 143$ oppure
$x \equiv 12 \bmod 143$ oppure $x \equiv -12 \bmod 143$

(c) Siccome $5 \equiv 3^5 \bmod 7$, la terza congruenza diventa $3^{x+2} \equiv 3^5 \bmod 7$. Dividendo per $3^5 \bmod 7$ otteniamo $3^{x-3} \equiv 1 \bmod 7$. L'ordine di 3 modulo 7 è 6, dunque $3^y \equiv 1 \bmod 7$ equivale a $y \equiv 0 \bmod 6$. Ponendo $y = x - 3$ la nostra

congruenza diventa $x - 3 \equiv 0 \bmod 6$ ovvero $\boxed{x \equiv 3 \bmod 6}$.

Per capire per quali valori di a il sistema (a),(b),(c) ha soluzione consideriamo i 4 casi del punto (b). Nel caso 1, il sistema (a),(b),(c) equivale a

$$\begin{cases} x \equiv a \bmod 3 \\ x \equiv 4a \bmod 5 \\ x \equiv 1 \bmod 11 \\ x \equiv 1 \bmod 13 \\ x \equiv 3 \bmod 6 \end{cases}$$

Se i moduli fossero stati a due a due coprimi il sistema avrebbe avuto soluzione per ogni a, ma nel nostro caso i moduli 3 e 6 non sono coprimi. In generale un sistema di questo genere ha soluzione se è solo se lo hanno i sistemi delle singole congruenze prese a due a due. L'unico problema lo pongono la prima e l'ultima congruenza. Quindi il sistema delle cinque congruenze sopra considerate ha soluzione se e solo se lo ha il sistema $\begin{cases} x \equiv a \bmod 3 \\ x \equiv 3 \bmod 6 \end{cases}$, e questo ha soluzione se e solo se il massimo comun divisore tra 3 e 6 divide $a - 3$, ovvero $\boxed{a \equiv 0 \bmod 3}$.

Gli altri tre casi (corrispondenti agli altri casi del punto (b)) sono del tutto analoghi, basta sostituire ± 1 al posto di 1 nella terza e quarta congruenza, e si ottiene sempre che il sistema è risolubile se e solo se $a \equiv 0 \bmod 3$.

Esercizio 2. Si consideri lo spazio vettoriale $\mathbb{F}^3$, dove $\mathbb{F}$ è un campo. Sia $L : V \to V$ una applicazione lineare che, rispetto alla base standard, è rappresentata dalla matrice

$$\begin{pmatrix} 3 & -1 & 1 \\ -1 & 5 & -1 \\ 1 & -1 & 3 \end{pmatrix}$$

1. Trovare una base per $Ker\ L$ e $Imm\ L$ nel caso in cui $\mathbb{F} = \mathbb{R}$.
2. Trovare la dimensione di $Ker\ L$ e $Imm\ L$ nel caso in cui $\mathbb{F} = \mathbb{Z}_2$.
3. Trovare la dimensione di $Ker\ L$ e $Imm\ L$ nel caso in cui $\mathbb{F} = \mathbb{Z}_3$.

In quale o quali dei casi precedenti $Ker\ L$ e $Imm\ L$ sono in somma diretta?
L'applicazione L è diagonalizzabile nel caso $\mathbb{F} = \mathbb{R}$?
L'applicazione L è diagonalizzabile nel caso $\mathbb{F} = \mathbb{Z}_2$?