4° Esame di MDAL
6 giugno 2016

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. Motivare in modo chiaro le risposte.

Esercizio 1. Si consideri la successione $\{a_n\}_{n\geq 0}$ definita per ricorrenza da

$$\begin{cases} a_0 = 2, a_1 = 1; \\ a_{n+1} = a_n + a_{n-1} \text{ per } n \geq 1. \end{cases} \quad (*)$$

(i) Dimostrare che per ogni $n \geq 0$ si ha

$$a_0^2 + a_1^2 + \cdots + a_n^2 = a_n a_{n+1} + 2.$$

(ii) Determinare il termine generale della successione a_n.

(i) Induzione: passo base, $n=0$: $a_0^2 = a_0 a_1 + 2$

$2^2 = 2 \cdot 1 + 2$ è vera

Passo induttivo:

Hp: $a_0^2 + \dots + a_n^2 = a_n a_{n+1} + 2$

Th: $a_0^2 + \dots + a_n^2 + a_{n+1}^2 = a_{n+1} a_{n+2} + 2$

$a_0^2 + \dots + a_n^2 + a_{n+1}^2 = \left(a_0^2 + \dots + a_n^2\right) + a_{n+1}^2 = a_n a_{n+1} + 2 + a_{n+1}^2 =$

$= a_{n+1}\left(a_n + a_{n+1}\right) + 2 = a_{n+1} a_{n+2} + 2$

↳ vera perché $a_{n+2} = a_n + a_{n+1}$, che è la (*) con gli →

- indici spostati di 1.

(ii) L'equazione associata è $\lambda^2 = \lambda + 1$, la stessa dei numeri di Fibonacci, con soluzioni: $\frac{1 \pm \sqrt{5}}{2}$.

Il termine generico dev'essere della forma

$$a_n = \alpha\left(\frac{1+\sqrt{5}}{2}\right)^n + \beta\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Trovo α, β imponendo

$$\begin{cases} 2 = a_0 = \alpha + \beta \\ 1 = a_1 = \alpha\left(\frac{1+\sqrt{5}}{2}\right) + \beta\left(\frac{1-\sqrt{5}}{2}\right) \end{cases}$$

che dà $\alpha = \beta = 1$.

Quindi

$$\boxed{a_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n}$$

Esercizio 2. Avete organizzato una prova didattica del metodo RSA, e avete scelto i primi $p = 7$ e $q = 13$. Avete reso pubblico il prodotto $pq = 91$ e l'esponente $e = 5$. Ricevete il messaggio 44.
a) Qual è l'esponente 'segreto' d a cui dovete elevare 44 per riottenere il messaggio originale?
b) Qual è il messaggio originale $m \equiv 44^d \bmod 91$ che vi è stato inviato?

$(p-1)(q-1) = 6 \cdot 12 = 72$

a) Vogliamo trovare l'inverso di 5 modulo 72, cioè d tale che $d \cdot 5 = K \cdot (72) + 1$.

$d \cdot 5 = 72 + 1$ è impossibile perché i multipli di 5 terminano con 5 o 0.

$d \cdot 5 = 72 \cdot 2 + 1 = 145$ è possibile e dà $\boxed{d = 29}$

b) Devo calcolare 44^{29} modulo 91. Cerco m tale che

$44^{29} \equiv m \pmod{91}$ $\overset{\text{(teo. cinese)}}{\iff}$ $\begin{cases} 44^{29} \equiv m \pmod{13} & (i) \\ 44^{29} \equiv m \pmod{7} & (ii) \end{cases}$

(i): $44^{29} \equiv 5^{29} \equiv 5^5 \equiv 25 \cdot 25 \cdot 5 \equiv (-1) \cdot (-1) \cdot 5 \equiv 5 \pmod{13}$

perché $44 \equiv 5 \pmod{13}$

perché $5^{12} \equiv 1 \pmod{13}$ per il piccolo teo. di Fermat

e anche $5^{24} \equiv 1$

→

(ii) $44^{29} \equiv 2^{29} \equiv 2^5 \equiv 32 \equiv 4$

perché $44 \equiv 2 \ (7)$ — perché $2^6 \equiv 1 \pmod 7$ per Fermat e anche $2^{24} \equiv 1$

Cerco un numero tale che $\begin{cases} m \equiv 4 \ (7) \\ m \equiv 5 \ (13) \end{cases}$

Provo tra i numeri della forma $5+13k$ quali vanno bene...

$5 + 13 \cdot 0 \equiv 5 \not\equiv 4 \pmod 7$ no

$5 + 13 \cdot 1 \equiv 18 \equiv 4 \pmod 7$ sì!

Per il teo. cinese del resto la soluzione è $\boxed{m \equiv 18 \pmod{91}}$

Esercizio 3. Sia $f : \mathbb{R}^3 \to \mathbb{R}^2$ un'applicazione lineare tale che

$$f\left(\begin{bmatrix}1\\2\\3\end{bmatrix}\right) = \begin{bmatrix}2\\1\end{bmatrix} \quad \text{e} \quad f\left(\begin{bmatrix}2\\3\\4\end{bmatrix}\right) = \begin{bmatrix}2\\4\end{bmatrix}$$

(a) Determinare $f\left(\begin{bmatrix}8\\13\\18\end{bmatrix}\right)$.

(b) Determinare la dimensione del nucleo di f.

(a) $\vec{w} = \begin{bmatrix}8\\13\\18\end{bmatrix}$ dev'essere nello span di $\vec{v}_1 = \begin{bmatrix}1\\2\\3\end{bmatrix}$ e $\vec{v}_2 = \begin{bmatrix}2\\3\\4\end{bmatrix}$, altrimenti non avrei dati sufficienti per rispondere.

Infatti, risolvo il sistema

$$\begin{bmatrix}1 & 2\\2 & 3\\3 & 4\end{bmatrix}\begin{bmatrix}x_1\\x_2\end{bmatrix} = \begin{bmatrix}8\\13\\18\end{bmatrix}, \quad \text{ottenendo} \quad \begin{bmatrix}x_1\\x_2\end{bmatrix} = \begin{bmatrix}2\\3\end{bmatrix},$$

quindi $2\vec{v}_1 + 3\vec{v}_2 = \vec{w}$.

Quindi per linearità

$$f(\vec{w}) = f(2\vec{v}_1 + 3\vec{v}_2) \overset{\text{linearità}}{=} 2f(\vec{v}_1) + 3f(\vec{v}_2) =$$

$$= 2\begin{bmatrix}2\\1\end{bmatrix} + 3\begin{bmatrix}2\\4\end{bmatrix} = \begin{bmatrix}10\\14\end{bmatrix}.$$

(b) Devo avere $\dim \operatorname{Im} f + \dim \ker f = 3$ (dimensione del dominio).

$\operatorname{Im} f$ è un sottospazio di $\mathbb{R}^2$ e contiene i vettori $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$ e $\begin{bmatrix} 2 \\ 4 \end{bmatrix}$, che sono linearmente indipendenti (e quindi il loro span è $\mathbb{R}^2$).

Allora $\operatorname{Im} f = \mathbb{R}^2$ e $\dim \operatorname{Im} f = 2$.

Perciò $\dim \ker f = 3 - \dim \operatorname{Im} f = 1$.

(Notate che i valori dati non determinano univocamente f).

Esercizio 4. Sia

$$M = \begin{bmatrix} 3 & 3 & 2 \\ 0 & 1 & 0 \\ 2 & -2 & 3 \end{bmatrix}.$$

1. Calcolare autovalori e autovettori della matrice M sul campo $\mathbb{R}$.
2. La matrice è diagonalizzabile su $\mathbb{R}$?
3. La matrice è diagonalizzabile su $\mathbb{Z}_5$?

1. Laplace su 2ª riga

$$\det(M-\lambda I) = \det\begin{bmatrix} 3-\lambda & 3 & 2 \\ 0 & 1-\lambda & 0 \\ 2 & -2 & 3-\lambda \end{bmatrix} = (1-\lambda)\det\begin{bmatrix} 3-\lambda & 2 \\ 2 & 3-\lambda \end{bmatrix} =$$

$$= (1-\lambda)\left[(3-\lambda)^2-4\right] = (1-\lambda)(\lambda^2-6\lambda+9-4) = (1-\lambda)(\lambda^2-6\lambda+5) =$$

$$= (1-\lambda)(\lambda-1)(\lambda-5)$$

autovalori: $1 \quad m_a(1)=2$

$5 \quad m_a(5)=1$

Autovettori di autovalore $\lambda=5$:

$$\ker(M-5I) = \ker\begin{bmatrix} -2 & 3 & 2 \\ 0 & -4 & 0 \\ 2 & -2 & -2 \end{bmatrix} = \ker\begin{bmatrix} -2 & 3 & 2 \\ 0 & -4 & 0 \\ 0 & 1 & 0 \end{bmatrix} =$$

$$= \ker\begin{bmatrix} -2 & 3 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \operatorname{span}\left(\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}\right) \quad \text{(tranne lo } \vec{0}\text{)}$$

Autovettori di autovalore $\lambda=1$:

$$\ker(M-I) = \ker\begin{bmatrix} 2 & 3 & 2 \\ 0 & 0 & 0 \\ 2 & -2 & 2 \end{bmatrix} = \ker\begin{bmatrix} 2 & 3 & 2 \\ 0 & 0 & 0 \\ 0 & 5 & 0 \end{bmatrix} = \ker\begin{bmatrix} 2 & 3 & 2 \\ 0 & 5 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \longrightarrow$$

$= \text{span}\left(\begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix}\right)$ (tranne lo $\vec{0}$)

2. $m_g(1) = 1 \neq m_a(1)$, quindi la matrice non è diagonalizzabile.

3. La fattorizzazione del polinomio è valida anche in $\mathbb{Z}_5$, quindi gli autovalori sono

$\lambda_1 = 1 \quad m_a(1) = 2$

$\lambda_2 = 5 \equiv 0 \quad m_a(0) = 1$

Per vedere se è diagonalizzabile devo trovare $m_g(1)$:

$$\ker(M-I) = \ker \begin{bmatrix} 2 & 3 & 2 \\ 0 & 5 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \ker \begin{bmatrix} 2 & 3 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

(come prima; perché $5 \equiv 0$)

quindi $m_g(1) = \dim \ker(M-I) = 2$.

λ_i	m_a	m_g
1	2	2
0	1	1

quindi la matrice è diagonalizzabile.