Seconda parte del Compito di MDAL
10 luglio 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. Motivare in modo chiaro le risposte.

Esercizio 1. Bob sceglie i numeri primi $p = 11, q = 19$ e rende pubblico il loro prodotto $n = 209$ e la chiave pubblica $e = 53$. Tramite l'algoritmo RSA, Alice manda a Bob il messaggio cifrato $c = 162 = m^{53} \bmod 209$. Quale è la chiave privata d alla quale Bob deve elevare 162 modulo 209 per decriptare il messaggio? Quale è il messaggio m?

Risposta: $d = 17$, $m = 2$

l'inverso di 53 modulo $180 = (p-1)(q-1)$ è $\boxed{d = 17}$.

$\Rightarrow m \equiv 162^{17} \ (209)$.

$\Rightarrow \begin{cases} m \equiv 162^{17} \ (11) \\ m \equiv 162^{17} \ (19) \end{cases}$.

Ora $\begin{cases} 162 \equiv 8 \ (11) \\ 162 \equiv 10 \ (19) \end{cases}$

$\Rightarrow \begin{cases} m \equiv 8^{17} \ (11) \\ m \equiv 10^{17} \ (19) \end{cases}$.

Ricordiamo che $8^{10} \equiv 1 \ (11)$

$10^{18} \equiv 1 \ (19)$.

$\Rightarrow \begin{cases} m \equiv 8^{7} \cdot 8^{10} \ (11) \\ m \equiv 10^{17} \ (19) \end{cases}$

$$\Rightarrow \begin{cases} m = 8^7 \ (11) \\ m = 10^{17} \ (19) \end{cases}$$

Calcolo $8^7 = 8^2 \cdot 8^2 \cdot 8^2 \cdot 8 \ (11)$

$\equiv (64)(64)(64) \cdot 8 \ (11)$

$\equiv (-2)(-2)(-2) \cdot 8 \mod 11$

$\equiv -8 \cdot 8 \equiv -64 \equiv 2 \mod 11.$

Calcolo $10^{17} \mod 19$:

$10^{17} \cdot 10 \equiv 10^{18} \equiv 1 \mod (19)$

per Fermat

Quindi 10^{17} è l'inverso di $10 \mod 19$

Cioè $2 \mod 19$

$$\Rightarrow \begin{cases} m \equiv 2 \ (11) \\ m \equiv 2 \ (19) \end{cases} \Rightarrow \boxed{m \equiv 2 \ (209)}.$$

Esercizio 2. Si consideri lo spazio $\mathbb{R}[x]^{\leq 3}$ dei polinomi di grado minore o uguale a 3. Sia $T : \mathbb{R}[x]^{\leq 3} \to \mathbb{R}[x]^{\leq 3}$ l'applicazione lineare definita da

$$T(p(x)) = p(x)'' + p(x)' + xp(x)' \qquad \forall p(x) \in \mathbb{R}[x]^{\leq 3}$$

dove $p(x)'$ indica la derivata prima e $p(x)''$ indica la derivata seconda.

1. Determinare la matrice di T rispetto alla base $1, x, x^2, x^3$.
2. Calcolare una base di $Ker\ T$ e una base di $Imm\ T$.
3. Dire se T è diagonalizzabile e in tal caso trovare una base di $\mathbb{R}[x]^{\leq 3}$ composta da autovettori per T.

$p(x) = a + bx + cx^2 + dx^3$

$p'(x) = b + 2cx + 3dx^2$

$p''(x) = 2c + 6dx$

$T(p(x)) = 2c + 6dx + b + 2cx + 3dx^2 + bx + 2cx^2 + 3dx^3$

$= (b+2c) + x(b+2c+6d) + x^2(2c+3d) + x^3(3d)$

$[T]\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} b+2c \\ b+2c+6d \\ 2c+3d \\ 3d \end{pmatrix}$. $\quad [T] = \begin{pmatrix} 0 & 1 & 2 & 0 \\ 0 & 1 & 2 & 6 \\ 0 & 0 & 2 & 3 \\ 0 & 0 & 0 & 3 \end{pmatrix}$

- Autovalori $0, 1, 2, 3$
- Base Immagine: polinomi con coordinate $\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \\ 2 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 6 \\ 3 \\ 3 \end{pmatrix}$
  ovvero $1+x,\ 2+2x+2x^2,\ 6x+3x^2+3x^3$
- Nucleo: $[T] \overset{\text{II}-\text{I},\ \text{III}-\text{IV}}{\sim} \begin{pmatrix} 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \overset{\text{I}-\text{III},\ \text{II}-2\cdot\text{IV},\ \text{permutaz.}}{\sim} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ forma di riga
  $a\ b\ c\ d$

$d = 0,\ c = 0,\ b = 0,\ a$ libera

$\ker([T]) = \operatorname{span}\left\{\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}\right\} \qquad V_0 = \operatorname{span}\{1\}$

$[T] - I = \begin{pmatrix} -1 & 1 & 2 & 0 \\ 0 & 0 & 2 & 6 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & 1 & 2 & 0 \\ 0 & 0 & 2 & 6 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ $\quad a\ b\ c\ d$

$d = 0$, $c = 0$, $b =$ libera, $a = b$

$\ker([T] - I) = \operatorname{span}\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, $V_1 = \operatorname{span}(1+x)$.

$[T] - 3I = \begin{pmatrix} -3 & 1 & 2 & 0 \\ 0 & -2 & 2 & 6 \\ 0 & 0 & -1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ $\quad a\ b\ c\ d$

$\ker([T] - 3I) = \operatorname{span}\begin{pmatrix} 4 \\ 6 \\ 3 \\ 1 \end{pmatrix}$, $V_3 = \operatorname{span}(4 + 6x + 3x^2 + x^3)$.

d libera

a, b, c vincolate.

$$[T]-2I = \begin{pmatrix} -2 & 1 & 2 & 0 \\ 0 & -1 & 2 & 6 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -2 & 1 & 2 & 0 \\ 0 & -1 & 2 & 6 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$d = 0$

c libera

$b = 2c$

$a = 2c$

$$\ker\left([T]-2I\right) = \operatorname{span}\left\{\begin{pmatrix} 2 \\ 2 \\ 1 \\ 0 \end{pmatrix}\right\}$$

$$V_2 = \operatorname{span}\left\{2 + 2x + x^2\right\}$$

Base autovettori: $\left\{1,\ 1+x,\ 4+6x+3x^2+x^3,\ 2+2x+x^2\right\}$