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?

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.