Università di Pisa - CdL in Informatica

Correzione prova scritta

Alessio Del Vigna

13 Maggio 2020

Esercizio 1. Si consideri la matrice a coefficienti reali

$$A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 2 & -2 \\ -1 & 1 & -3 \end{pmatrix}.$$

(i) La matrice A è invertibile?

(ii) Calcolare $\dim \mathrm{Ker}(A)$.

(iii) Determinare se la matrice A è diagonalizzabile su $\mathbb{R}$.

(iv) Determinare se la matrice A è diagonalizzabile su $\mathbb{Z}/(3)$.

Soluzione 1. (i) Poiché $\det A = 0$ la matrice A non è invertibile.

(ii) Dal punto (i) segue che le tre colonne di A non sono indipendenti. Del resto le prime due lo sono, per cui $\dim \mathrm{Imm}(A) = 2$ e quindi $\dim \mathrm{Ker}(A) = 3 - 2 = 1$.

(iii) Il polinomio caratteristico di A è $p_A(\lambda) = 3\lambda - \lambda^3$, da cui segue che gli autovalori di A sono 0, $\sqrt{3}$ e $-\sqrt{3}$. Poiché A possiede tre autovalori reali distinti segue che è diagonalizzabile.

(iv) Il polinomio caratteristico di A è $p_A(\lambda) = -\lambda^3$, polinomio a coefficienti in $\mathbb{Z}/(3)[\lambda]$. Quindi la matrice A ha solo l'autovalore 0 con molteplicità algebrica 3. Dato che $\dim \mathrm{Ker}(A) = 1$ (analogo a (ii)) segue che la matrice non è diagonalizzabile su $\mathbb{Z}/(3)$.

Esercizio 2. Si consideri il polinomio $p(x) = x^3 + 2x^2 + 2x + 1$.

(i) Visto come polinomio in $\mathbb{R}[x]$, il polinomio $p(x)$ è fattorizzabile in fattori lineari?

(ii) E visto come polinomio in $\mathbb{Z}/(7)[x]$?

(iii) Determinare le radici di $p(x)$ come polinomio in $\mathbb{Z}/(7)[x]$.

Soluzione 2. (i) Si osserva che $p(-1) = 0$, da cui segue che $(x+1) \mid p(x)$ per il teorema di Ruffini. Dalla regola di Ruffini si ha poi

$$p(x) = (x+1)(x^2 + x + 1).$$

Il fattore $x^2 + x + 1$ è irriducibile su $\mathbb{R}$, dato che è di secondo grado con discriminante negativo, quindi p non si fattorizza in fattori lineari.

(ii) Si osservi che su $\mathbb{Z}/(7)$ vale $x^2 + x + 1 = x^2 + x - 6 = (x+3)(x-2)$, da cui $p(x) = (x+1)(x-2)(x+3)$.

(iii) Le radici sono $[2]_7$, $[4]_7$ e $[6]_7$.

Esercizio 3. Risolvere la congruenza esponenziale

$$3^x \equiv 15 \pmod{22}.$$

Soluzione 3. Dato che $\varphi(22) = \varphi(11) = 10$ abbiamo che l'ordine di 3 modulo 22 è un divisore di 10. Si trova immediatamente che tale ordine è 5 e che $3^4 \equiv -7 \equiv 15 \pmod{22}$, da cui la soluzione $x \equiv 4 \pmod{5}$.

Esercizio 4. Sia $n \geq 1$ un intero e supponiamo che $x^6 \equiv 1 \pmod{n}$ e $x^{10} \equiv 1 \pmod{n}$. Stabilire quali delle seguenti affermazioni sono necessariamente vere:

(i) $x^4 \equiv 1 \pmod{n}$

(ii) $x^2 \equiv 1 \pmod{n}$

(iii) $x^{16} \equiv 1 \pmod{n}$

(iv) $x^{30} \equiv 1 \pmod{n}$

(v) $x^{60} \equiv 1 \pmod{n}$

(vi) $x^7 \equiv 1 \pmod{n}$

Soluzione 4. La (iv) e la (v) sono banalmente vere, dato che hanno esponente multiplo di 10 e che $x^{10} \equiv 1 \pmod{n}$ per ipotesi. Anche la (iii) è vera poiché $x^{16} = x^6 \cdot x^{10}$. Inoltre, dalle ipotesi si ha anche che $x^{(6,10)} \equiv 1 \pmod{n}$ (vedi il Teorema 1 sotto e il suo corollario), quindi anche la (ii) è vera, e di conseguenza anche la (i).

Teorema 1. *Siano a e $n \geq 1$ due interi primi tra loro e sia k un intero positivo. Vale $a^k \equiv 1 \pmod{n}$ se e solo se $\mathrm{ord}_n(a) \mid k$.*

Dimostrazione. ($\Rightarrow$) Dal teorema di divisione euclidea $k = \mathrm{ord}_n(a) \cdot s + r$, con $0 \leq r < \mathrm{ord}_n(a)$. Se fosse $r \neq 0$ allora avremmo

$$1 \equiv a^k \equiv a^{\mathrm{ord}_n(a) \cdot s + r} \equiv a^r \pmod{n},$$

che contraddice la minimalità di $\mathrm{ord}_n(a)$.

($\Leftarrow$) Ovvia. □

Corollario 1. *Siano a e $n \geq 1$ due interi primi tra loro e siano k e h due interi positivi. Se $a^k \equiv 1 \pmod{n}$ e $a^h \equiv 1 \pmod{n}$ allora $a^{(h,k)} \equiv 1 \pmod{n}$.*

Dimostrazione. Dal Teorema 1 si ha che $\mathrm{ord}_n(a) \mid h$ e $\mathrm{ord}_n(a) \mid k$. Dunque per le proprietà del massimo comune divisore segue $\mathrm{ord}_n(a) \mid (h, k)$. □

Questo corollario può essere anche mostrato usando il lemma di Bézout (esercizio).