Università di Pisa - CdL in Informatica

Correzione seconda prova scritta

a cura di Alessio Del Vigna

Pisa, 10 Luglio 2019

Esercizio 1. Consideriamo il sistema di congruenze

$$\begin{cases} 4x \equiv 2 \pmod{26} \\ 3^x \equiv 3 \pmod{11}. \end{cases}$$

Determinare:

(a) le soluzioni della prima congruenza;

(b) le soluzioni della seconda congruenza;

(c) le soluzioni del sistema;

(d) il numero di soluzioni x del sistema che soddisfano $0 \leq x \leq 1000$.

Soluzione. (a) La prima congruenza è equivalente a $2x \equiv 1 \pmod{13}$ (è sufficiente dividere per 2). In $\mathbb{Z}/(13)$, l'elemento $[2]_{13}$ è invertibile in quanto 2 e 13 sono primi tra loro, e l'inverso è $[7]_{13}$. Moltiplicando entrambi i membri per l'inverso si ha $x \equiv 7 \pmod{13}$.
(b) Nel gruppo moltiplicativo $\mathbb{Z}/(11)^*$, l'elemento $[3]_{11}$ ha ordine che divide $\phi(11) = 10$. L'ordine non è 2 in quanto $3^2 \equiv -2 \pmod{11}$ e poiché $3^5 \equiv 1 \pmod{11}$ abbiamo che l'ordine di $[3]_{11}$ è 5. Dato che $x = 1$ è una soluzione della congruenza, abbiamo che tutte le soluzioni sono date da $x \equiv 1 \pmod{5}$.
(c) Il sistema è equivalente a

$$\begin{cases} x \equiv 7 \pmod{13} \\ x \equiv 1 \pmod{5} \end{cases},$$

che è risolubile, avendo moduli primi tra loro. Dalla prima si ha che $x = 7 + 13k$ per un qualche intero k, da cui, dalla seconda $3k \equiv 4 \pmod{5} \Leftrightarrow k \equiv 3 \pmod{5} \Leftrightarrow x \equiv 46 \pmod{65}$.
(d) Le soluzioni del sistema sono del tipo $x = 46 + 65k$, con $k \in \mathbb{Z}$. Così si ha $0 \leq x \leq 1000 \Leftrightarrow 0 \leq 46 + 65k \leq 1000 \Leftrightarrow -\frac{46}{65} \leq k \leq \frac{954}{65} \Leftrightarrow 0 \leq k \leq \lfloor \frac{954}{65} \rfloor = 14$, dove l'ultima equivalenza è valida poiché k è intero. Vi sono così 15 valori di k tali per cui x è soluzione del sistema e $0 \leq x \leq 1000$.[1]

[1] Un altro metodo equivalente di risolvere il punto (d) dell'esercizio. Dobbiamo contare gli interi $\equiv 46 \pmod{65}$ compresi tra 0 e 1000. Gli interi da 0 a 64 sono un insieme di interi consecutivi che esauriscono tutte le classi di congruenza modulo 65 (in altre parole, sono un sistema di generatori di $\mathbb{Z}/(65)$). L'insieme dei 65 interi successivi anche, e così via. Negli interi da 0 a 1000 ci sono $\lfloor \frac{1000}{65} \rfloor = 15$ di questi insiemi, ognuno dei quali contribuisce al conteggio con un unico elemento $\equiv 46 \pmod{65}$. Poiché $15 \cdot 65 + 46 > 1000$, non vi sono altri elementi da contare. Quindi abbiamo che l'insieme

$$\{x \in \mathbb{N} : x \equiv 46 \pmod{65} \text{ e } 0 \leq x \leq 1000\}$$

ha 15 elementi.

Esercizio 2. (a) Trovare due numeri reali a e b tali che $\frac{-i}{3i+4} = a + bi$.

(b) Consideriamo un polinomio monico di terzo grado a coefficienti reali $x^3 + bx^2 + cx + d$ e supponiamo che sia 1 sia i siano radici del polinomio. Determinare i coefficienti b, c e d.

Soluzione. (a) Moltiplichiamo numeratore e denominatore per $-3i + 4$ (il coniugato del denominatore), per ottenere

$$\frac{-i}{3i+4} = \frac{-i(-3i+4)}{16+9} = -\frac{3}{25} - \frac{4}{25}i,$$

dove abbiamo ripetutamente usato la proprietà che caratterizza l'unità immaginaria, ossia che $i^2 = -1$.

(b) Il polinomio è di terzo grado, per cui ha esattamente tre radici complesse, contate con molteplicità (per il teorema fondamentale dell'algebra). Sappiamo che 1 e i sono radici e, visto che le radici di un polinomio a coefficienti reali sono o reali o coniugate a coppie, anche $-i$ è una radice del polinomio. Il polinomio in questione ha quindi 1, i e $-i$ come radici, ed essendo monico è necessariamente il polinomio $(x-1)(x+i)(x-i) = x^3 - x^2 + x - 1$.

Un altro modo di risolvere l'esercizio. Sia $p(x)$ il polinomio dato. Dire che 1 e i sono sue radici equivale a

$$\begin{cases} p(1) = 0 \\ p(i) = 0 \end{cases} \quad \Leftrightarrow \begin{cases} 1 + b + c + d = 0 \\ -i - b + ic + d = 0 \end{cases} \quad \Leftrightarrow \begin{cases} 1 + b + c + d = 0 \\ d - b = 0 \\ -1 + c = 0 \end{cases}$$

da cui $b = -1$, $c = 1$, $d = -1$. Notare che nel passare dal secondo sistema al terzo, la seconda equazione è un'equazione a coefficienti complessi, che dà luogo a due equazioni a coefficienti reali separando parte reale e parte immaginaria.

Esercizio 3. Sia

$$A = \operatorname{Span}\left\{ \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} \right\} \subseteq \mathbb{R}^3$$

e sia $B \subseteq \mathbb{R}^3$ il nucleo dell'applicazione lineare $f : \mathbb{R}^3 \to \mathbb{R}$ definita da $f(x, y, z) = 3x + 5y + 2z$. Determinare:

(a) la dimensione dello spazio vettoriale $A + B$;

(b) la dimensione dello spazio vettoriale $A \cap B$;

(c) una base di $A \cap B$.

Soluzione. Osserviamo che $\dim A = 2$ (i due vettori che lo generano sono indipendenti) e che

$$A = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \;:\; x + y + z = 0 \right\}.$$

Inoltre, per definizione di nucleo di un'applicazione lineare, si ha

$$B = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \;:\; 3x + 5y + 2z = 0 \right\} = \operatorname{Span}\left\{ \begin{pmatrix} 2 \\ 0 \\ -3 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ -5 \end{pmatrix} \right\}.$$

(a) Lo spazio $A + B$ è generato dall'unione dei generatori di A e di B. Poiché i primi due generatori di A e il primo generatore di B sono tre vettori indipendenti si ha $\dim(A + B) = 3$.

(b) Dalla formula di Grassmann si ha $\dim(A \cap B) = 2 + 2 - 3 = 1$.

(c) Dato che abbiamo le equazioni cartesiane di entrambi possiamo risolvere il sistema

$$\begin{cases} x + y + z = 0 \\ 3x + 5y + 2z = 0 \end{cases},$$

che sono le equazioni cartesiane di $A \cap B$.

Se si vogliono fare (forse) meno calcoli si può anche ragionare come segue. Dalla scrittura di A come spazio generato, un generico vettore di A è della forma

$$\begin{pmatrix} -a-b \\ b \\ a \end{pmatrix}$$

per opportuni $a, b \in \mathbb{R}$. Questo vettore sta in $B = \operatorname{Ker} f$ se e solo se $3(-a-b) + 5b + 2a = 0 \Leftrightarrow a = 2b$. Così

$$A \cap B = \left\{ \begin{pmatrix} -3b \\ b \\ 2b \end{pmatrix} \in \mathbb{R}^3 \,:\, b \in \mathbb{R} \right\} = \left\{ b \begin{pmatrix} -3 \\ 1 \\ 2 \end{pmatrix} \in \mathbb{R}^3 \,:\, b \in \mathbb{R} \right\} = \operatorname{Span} \left\{ \begin{pmatrix} -3 \\ 1 \\ 2 \end{pmatrix} \right\}.$$

Questo dice che il vettore $\left(\begin{smallmatrix} -3 \\ 1 \\ 2 \end{smallmatrix}\right)$ genera $A \cap B$, costituendone quindi una base.

Esercizio 4. Sia r un parametro reale, e consideriamo la matrice

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ r & 0 & 0 & 1 \end{pmatrix}$$

(a) Per quali valori di r la matrice ha esattamente 3 autovalori reali distinti?

(b) Nel caso in cui ci siano 3 autovalori reali distinti, calcolare la dimensione dell'autospazio associato all'autovalore 1.

(c) Per quali valori di r la matrice è diagonalizzabile?

Soluzione. (a) Il polinomio caratteristico di A è

$$p_A(\lambda) = (1-\lambda)^2 \left[(1-\lambda)^2 - r \right].$$

Se $r < 0$ l'unica radice è 1, con molteplicità algebrica 2; se $r = 0$ l'unica radice è 1, con molteplicità algebrica 4; se $r > 0$ ci sono le tre radici distinte 1, $1+\sqrt{r}$ e $1-\sqrt{r}$, con molteplicità algebrica 2, 1 e 1 rispettivamente. Pertanto la matrice A ha tre autovalori reali e distinti se e solo se $r > 0$.

(b) La dimensione dell'autospazio dell'autovalore 1 è la di $\operatorname{Ker}(A - I)$. Per $r > 0$ si ha

$$A - I = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ r & 0 & 0 & 0 \end{pmatrix},$$

il cui nucleo ha dimensione 2.

(c) Distinguiamo gli stessi tre casi di sopra.

(i) Se $r > 0$ abbiamo gli autovalori 1, $1+\sqrt{r}$ e $1-\sqrt{r}$, con $m_{alg}(1) = 2$, $m_{alg}(1+\sqrt{r}) = 1$ e $m_{alg}(1-\sqrt{r}) = 1$, dal punto (a). Dal punto (b) sappiamo che $m_{geo}(1) = 2$ e del resto $m_{geo}(1+\sqrt{r}) = m_{geo}(1-\sqrt{r}) = 1$[2]. Quindi se $r > 0$ la matrice A è diagonalizzabile.

(ii) Se $r = 0$ abbiamo $m_{alg}(1) = 4$ ma $m_{geo}(1) = 3$, quindi A non è diagonalizzabile.

(iii) Se $r < 0$ la matrice non è diagonalizzabile (su $\mathbb{R}$) perché la somma delle molteplicità algebriche dei suoi autovalori è < 4.

[2]Qui non serve fare altri calcoli: infatti, la molteplicità geometrica di un autovalore è ≥ 1 e minore o uguale alla sua molteplicità algebrica.