Matematica discreta 22/03/2017

ESERCIZI:

$$x^2 + 1 \equiv 0 \ (65)$$

Trovare tutte le soluzioni.

→ cercare di fattorizzare.

$$x^2 - 64 \equiv 0 \ (65)$$

$$x^2 - 8^2 \equiv 0 \ (65)$$

$$(*) \quad (x+8)(x-8) \equiv 0 \ (65)$$

già trovate due soluzioni:

$x = 8$

$x = -8$

ma tutte le soluzioni?

$x = 8 + K65$

$x = -8 + K65$

Regola:

$$a \equiv b \ (65)$$

$$\begin{cases} a \equiv b \ (5) \\ a \equiv b \ (13) \end{cases}$$

fattorizziamo il modulo

Se il modulo $M = u \cdot v$

la congruenza $A \equiv B \ (M)$

$$\Updownarrow$$

$$\begin{cases} A \equiv B \ (u) \\ A \equiv B \ (v) \end{cases}$$

Il sistema (*) equivale a:

$$\begin{cases} (x-8)(x+8) \equiv 0 \ (5) \ (*)1 \\ (x-8)(x+8) \equiv 0 \ (13) \ (*)2 \end{cases}$$

siccome 5, 13 non hanno fattori comuni i multipli di 5 e 13 sono i multipli di 65

$A \cdot B \equiv 0 \ (5)$

$5 \mid A \cdot B$

$$\Updownarrow$$

$5 \mid A \ \circ \ 5 \mid B$

$A \equiv 0 \ (5) \ \circ \ B \equiv 0 \ (5)$

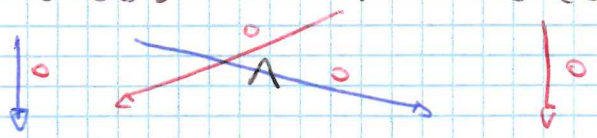
(*)1

$$\begin{cases} x - 8 \equiv 0 \ (5) \\ \circ \\ x + 8 \equiv 0 \ (5) \end{cases}$$

(*)2

$$\begin{cases} x - 8 \equiv 0 \ (13) \\ \circ \\ x + 8 \equiv 0 \ (13) \end{cases}$$

$$\left(X \equiv 8\ (5) \quad \vee \quad X \equiv -8\ (5)\right)$$



$$\left(X \equiv 8\ (13) \quad \vee \quad X \equiv -8\ (13)\right)$$

$\Updownarrow$ 4 casi

$$\begin{cases} X \equiv 8\ (5) \\ X \equiv 8\ (13) \end{cases} \vee \begin{cases} X \equiv -8\ (5) \\ X \equiv +8\ (13) \end{cases} \vee$$

$\vee$ di $8 \pm K65$ già trovate

$$\begin{cases} X \equiv 8\ (5) \\ X \equiv -8\ (13) \end{cases} \vee \begin{cases} X \equiv -8\ (5) \\ X \equiv -8\ (13) \end{cases} \rightarrow -8 + K65 \text{ già trovata}$$

Calcolo le soluzioni mancanti:

$$\begin{cases} X \equiv -8\ (5) \\ X \equiv 8\ (13) \end{cases}$$

I moduli sono primi tra loro si può sempre risolvere.

$$X = -8 + 5K$$

sostituisco

$$-8 + 5K \equiv 8\ (13)$$
$$5K \equiv 16\ (13)$$
$$5K \equiv 3\ (13)$$

- trovo l'inverso di 5 (13) oppure
- moltiplico $\cdot 2$ → possibile perdere 2 tra inverso (13)

$$10K \equiv 6\ (13)$$
$$-3K \equiv 6\ (13)$$

- divido per 3

$$-K \equiv 2\ (13)$$
$$K \equiv -2\ (13) \Rightarrow K = -2 + \ell 13$$

$$X = -8 + 5(-2 + \ell 13)$$
$$X = -8 - 10 + 65\ell$$

$$\underline{X = -18 + 65\ell}$$ soluzione.

$$\begin{cases} x \equiv 8 \ (5) \\ x \equiv -8 \ (13) \end{cases}$$

$x = 8 + 5k$

sostituisco:

$8 + 5k \equiv -8 \ (13)$

$5k \equiv -16 \ (13)$

$5k \equiv 10 \ (13)$

$k \equiv 2 \ (13) \Rightarrow k = 2 + 13\ell$

$x = 8 + 5(2 + 13)\ell$

$x = 18 + 65\ell$. soluzione.

tutte le soluzioni si ottengono aggiungendo / sottraendo multipli di 65.

ESERCIZIO: Trovare tutte le soluzioni nell'intervallo $[10, 1000]$

$51x \equiv 6 \ (69)$ (A)

$\text{mcd}(51, 69) = 3$

$3 \mid 6$? Si $\Rightarrow$ RISOLUBILE.

divido per 3 la congruenza TUTTA (perché divide tutte le moduli).

$17x \equiv 2 \ (23)$

ora 17 e 23 non hanno fattori comuni

$\Downarrow$

ha un inverso. sempre dopo aver diviso per il massimo fattore comune.

cerco l'inverso di $17 \ (23)$ con l'algoritmo di Euclide.

Teoria:

$d = \text{Mcd}(a, c)$

$a = da'$, $c = dc'$

$\Downarrow$

$1 = \text{mcd}(a', c')$

$(23,17) \xrightarrow{23-17} (6,17) \xrightarrow{17-2\cdot 6} (6,5) \xrightarrow{6-5} (1,5) =$

$5-5\cdot 1 = (1,0) = 1$

$$23 = \boxed{1}\,23 + \boxed{0}\,17$$
$$17 = \boxed{0}\,23 + \boxed{1}\,17$$
$$23-17 \quad 6 = \boxed{1}\,23 + \boxed{-1}\,17$$
$$17-2\cdot 6 \quad 5 = \boxed{-2}\,23 + \boxed{3}\,17$$
$$6-5 \quad 1 = \boxed{3}\,23 + \boxed{-4}\,17$$

$\boxed{-4}$ ↑ inverso di 17 mod 23

$$\Downarrow$$

$$1 \equiv (-4)\cdot 17 \ (23)$$

-4 è l'inverso di 17 mod (23)

$$\Downarrow \equiv 19 \ (23)$$

moltiplico (A) per l'inverso di 17

$$x \equiv 19\cdot 2 \ (23)$$

$$x \equiv 38 \ (23)$$

$$x \equiv 15 \ (23) \Rightarrow x \equiv -8 \ (23)$$

alla fine:

$$17x \equiv 2 \ (23)$$

$\Updownarrow$ moltiplico per l'inverso di 17.

$$x \equiv -8 \ (23)$$

ma quante soluzioni ci sono nell'intervallo $[10, 1000]$

$$x = 15 + 23k$$

$$10 \le 15 + 23k \le 1000$$

$$\Updownarrow$$

$$\begin{cases} 10 \le 15 + 23k \\ 15 + 23k \le 1000 \end{cases}$$

$$-5 \leq 23k \leq 985$$

$$-\frac{5}{23} \leq k \leq \frac{985}{23}$$

$-0{,}2$ $\qquad$ $42,$

k però deve $\in \mathbb{Z}$

$$0 \leq k \leq 42$$

ci sono 43 valori, la più piccola è 15, la più grande $15 + 23 \cdot 42 = 981$.

es:

$$423x \equiv 81 \mod (17 \cdot a)$$

per quali $a \in \mathbb{Z}$ esiste x?

→ risolubile se $\mcd(17a, 423) \mid 81$

Teoria:

Unicità scomponibile in primi.

es:
$$n = 7^5 \cdot 13^4 \cdot 23^2 \cdot 19^7 \overset{?}{=} 7^4 \cdot 13^5 \cdot 23^7 \cdot 19^8$$

non può essere vero perché avremmo un numero scomposto in primi in 2 modi diversi → IMPOSSIBILE.

c'è da mostrare un primo che compare più volte.

$$7^5 \cdot 23^2 \cdot 19^7 = 7^4 \cdot 13 \cdot 23^4 \cdot 19^8$$

↓

faccio "scomparire" un fattore da una parte dividendo per questo con l'esponente più piccolo con cui compare.

con il teorema: $a \mid b \cdot c$ e $\mcd(a,b) = 1$ $\Rightarrow a \mid c$.

corollario:

$$p \mid b \cdot c \cdot d \Rightarrow p \mid b \vee p \mid c \vee p \mid d \ldots$$

applico il teorema all'es:

$13 \mid n$ → $= 7^4 \cdot 13 \cdot 23^4 \cdot 19^8$

→ $= 7^5 \cdot 23^2 \cdot 19^7$

ne concludo che $13 \mid 7 \vee 13 \mid 23 \vee 13 \mid 19$

ASSURDO.

Teorema: se $n = \prod_{i=1}^{r} p_i^{a_i}$ (*) $\quad p_i \to$ primo

e $n = \prod_{i=1}^{k} p_i^{b_i}$

allora $a_i = b_i \quad \forall i$ (mai si può scomporre un n in 2 modi diversi).

Usiamo lo stesso k, se mancano dei termini li aggiungiamo con esponente = 0.

dim.

Se $a_i \neq b_i$ mettiamo $a_i > b_i$

divido per $p_i^{b_i}$ la (*).

otengo che: $p_i \mid$ la parte sinistra ma non la destra

↓

ASSURDO perché le due parti sono uguali.

es:

tutte le soluzioni di

(*) $\quad 23x + 17y = 0$ EQUAZIONE omogenea associata.

soluzioni ovvie: $\begin{cases} x = 0 \\ y = 0 \end{cases}$ $\quad \begin{cases} x = 17 \\ y = -23 \end{cases}$

sono tutte → $\begin{cases} x = k \cdot 17 \\ y = -k \cdot 23 \end{cases} \quad k \in \mathbb{Z}$

come lo dimostriamo?

↓ succede perché 17 e 23 non hanno fattori comuni.

con coniugate → sono coniugate

↓:

(*) = $23x = 17(-y)$

osservo che $17 \mid \underbrace{17(-y)}_{\Downarrow}$

$(17, 23) = 1 \longrightarrow = 23 \cdot x$

$\Downarrow$

$17 \mid x$ cioè

$x = 17k$

sostituisco $23(17k) + 17y = 0$ ricavo $y \Rightarrow y = -23k$.

Se $(a,b)=1$ allora le soluzioni di

$$ax+by=0 \quad \text{sono} \quad \begin{cases} x=bk \\ y=-ak \end{cases}$$

dim, col congruente:

$$23x+17y=0$$

$$\Downarrow$$

$$23x \equiv 0 \ (17) \qquad \text{(esiste sicuramente l'inverso.)}$$

$$17 \mid 23 \cdot x$$

ma 17 e 23 non hanno fattori comuni $\Rightarrow 17 \mid x \Rightarrow x = 17k$.

ESERCIZIO: per quali b, m si può risolvere la congruenza:

$$2x \equiv b \ (m)$$

2 parametri m, b. Trovare la x.

Si può risolvere se e solo se

$$\text{mcd}(2,m) \mid b$$

- distinguere i casi.

$(2,m)=1$ cioè m è dispari, b qualunque. Si risolve.

$2=(m,2)$ cioè m è pari $\Rightarrow 2 \mid b$ anche b è pari

ESERCIZIO:

$$23x+17y=1$$ tutte le soluzioni?

basta trovare una soluzione e poi aggiungere tutte le soluzioni dell'equazione associata.

$$\begin{cases} x_0=3 \\ y_0=-4 \end{cases}$$ tutte sono $$\begin{cases} x=3+k17 \\ y=-4-k23 \end{cases}$$

Se prendo 2 soluzioni e faccio la differenza:

$$23(x_0-x_1)+17(y_0-y_1)=0$$

(devo fare)

le 2 nozioni differiscono per la nozione delle dimensione associata.

ALGEBRA LINEARE 22/03/2017

TEOREMA del COMPLETAMENTO a una base.

V spazio vettoriale di $\dim(V)=n$ (finita)

$v_1, \dots, v_k \in V$ indipendenti

posso completarli per formare la base.

$\Rightarrow \exists\, w_1, w_2, \dots w_{n-k}$ t.c.

$\underbrace{v_1, v_2, \dots, v_k, w_1, \dots, w_{n-k}}_{n \text{ in tutto}}$ sono una base

dimostrazione:

Indipendente massimale = base
Generante minimale = base

insieme più grande di vettori indipendenti → massimale.
questo è una base
↓
dimostriamo:

Siano $z_1, \dots, z_e$ un insieme indipendente massimale.

prendo $v \in V$, devo mostrare che è nello span $\{z_1, \dots, z_e\}$, se non lo fosse

$\Rightarrow z_1, \dots, z_e, v$ sarebbero indipendenti

↓ ASSURDO.

dimostriamo che se v è indipendente e lo aggiungo ad un insieme di vettori indipendenti questo rimane indipendente.

$a_1 z_1 + \dots + a_e z_e + a_{e+1} v = 0$

se $a_{e+1} \neq 0$ posso dividere per a_{e+1}

$$v = -\frac{a_1}{a_{e+1}} z - \dots - \frac{a_e}{a_{e+1}} z_e$$

così $v \in$ span ✓ assurdo perché $v \notin$ span

$a_{k+1} = 0$ allora otengo

$$a_1 z_1 + \dots + a_k z_k = \bar{0}$$

$$a_1 = a_2 = \dots = a_k = 0 = a_{k+1}$$

se il mio insieme non è ancora una base aggiungo nuovi vettori <u>indipendenti</u> che mi lavorano l'insieme indipendente.
Mi fermo perché so che il numero di vettori per la base è al massimo n (<u>non di più</u>)

es:
$V = \mathbb{R}^4$

$v_1 = (1, 2, 3, 4)$

$v_2 = (1, 2, 8, 10)$

verificare che sono indipendenti:

$$\Downarrow$$

$$v_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \qquad v_2 = \begin{pmatrix} 1 \\ 2 \\ 8 \\ 10 \end{pmatrix}$$

$$a_1 v_1 + a_2 v_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$a_1 \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} + a_2 \begin{pmatrix} 1 \\ 2 \\ 8 \\ 10 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$ risolvo sistema:

$a_1 = a_2 = 0$

$$\begin{cases} a_1 + a_2 = 0 \\ 2a_1 + 2a_2 = 0 \\ 3a_1 + 8a_2 = 0 \\ 4a_2 + 10a_2 = 0 \end{cases}$$

completare ad una base:

Span di vettori non cambia aggiungendo ad uno dei vettori un multiplo di un altro.

$$\begin{matrix} v_1 & v_2 \end{matrix}$$
$$\begin{bmatrix} 1 & 1 \\ 2 & 2 \\ 3 & 8 \\ 4 & 10 \end{bmatrix} \xrightarrow{C2-C1} \begin{bmatrix} 1 & 0 \\ 2 & 0 \\ 3 & 5 \\ 4 & 6 \end{bmatrix}$$
$$w_1 \quad w_2$$

pivot messi a destra

hanno lo stesso span.

completo a una base di $\mathbb{R}^4$ aggiungendo vettori le cui coordinate hanno un numero diverso di 0 iniziali.

nessuno zero	2 zeri	1 zero	3 zeri
1	0	0	0
2	0	1	0
3	5	0	0
4	6	0	1

→ gli 0 iniziali devono essere di un numero diverso

→ solo così metterà tutto.

base di $\mathbb{R}^4$

$$a_1\begin{pmatrix}1\\2\\3\\4\end{pmatrix} + a_2\begin{pmatrix}0\\0\\5\\6\end{pmatrix} + a_3\begin{pmatrix}0\\1\\0\\0\end{pmatrix} + a_4\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$
$$w_1 \qquad w_2 \qquad e_2 \qquad e_4$$

$$\begin{cases} a_1 = 0 \\ a_3 = 0 \\ a_2 = 0 \\ a_4 = 0 \end{cases}$$

sono 4 vettori

↓

insieme massimale

$$\text{span}(w_1, w_2, e_2, e_4) = \text{span}(v_1, v_2, e_2, e_4)$$

($w_2 = v_2 - v_1$)

(=)

Se ho troppi vettori, rispetto alla dimensione, posso estrarre i vettori che sono dipendenti.

Teorema di estrazione di una base.

Se $v_1, \dots, v_e$ generano V. O sono indipendenti
⇓
è una base.

∴ Posso eliminare quelli per ottenere una base.

dimostrazione:
se elimino un vettore che è combinazione degli altri, questo non cambia.
Quindi posso eliminare i vettori che non mi cambiano lo span.
↓
devo eliminare il massimo numero che mi lascia invariato lo span.

Ottengo così un insieme generante minimale (con il minor numero possibile di vettori).

$v_{i_1}, \dots, v_{i_s}$ a quel punto sono tutti indipendenti e quindi base

altrimenti ∃ una combinazione lineare con almeno un $a_j \neq 0$.
↓
$a_1 v_{i_1} + \dots + a_s v_{i_s} = \bar{0}$

$v_{i_j} \in$ span degli altri
⇓
elimino anche lui, ma assurdo perché già ero nell'insieme generante minimale.

es:

$$\begin{pmatrix} v_1 & v_2 & v_3 & v_4 \\ 1 & 1 & 0 & 2 \\ 2 & 0 & 0 & 2 \\ 3 & 1 & 1 & 4 \end{pmatrix}$$

4 vettori e spazio $\mathbb{R}^3$

1) Generano?

2) Se sì, quali si possono eliminare?

1) C4 - 2C2 stesso spazio

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 2 & 0 & 0 & 2 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

3 vettori indipendenti in $\mathbb{R}^3$ generano.

sono ovviamente indipendenti

Sì

2) Che posso eliminare tra v_1, v_2, v_3, v_4?

per capire quali posso eliminare faccio mosse di riga, mantenendo i vettori siano in colonna.

$$\begin{pmatrix} 1 & 2 & 2 & 3 & 4 \\ 1 & 2 & 5 & 7 & 10 \\ 2 & 4 & 7 & 10 & 14 \\ 3 & 6 & 12 & 17 & 24 \\ 5 & 10 & 19 & 27 & 38 \end{pmatrix}$$

riduco a scalini:

Individuare il massimo numero indipendente e completare a base.

Mosse di riga

R2-R1
R3-2R1
R4-3R1
R5-5R1

$$\begin{pmatrix} 1 & 2 & 2 & 3 & 4 \\ 0 & 0 & 3 & 4 & 6 \\ 0 & 0 & 3 & 4 & 6 \\ 0 & 0 & 6 & 8 & 12 \\ 0 & 0 & 9 & 12 & 18 \end{pmatrix}$$

R3-R2
R4-2R2
R5-3R2

$$\begin{pmatrix} 1 & 2 & 2 & 3 & 4 \\ 0 & 0 & 3 & 4 & 6 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

sono indipendenti

posso dire che quelli di partenza nelle stesse posizioni sono indipendenti

Se facendo mosse di riga ottengo una matrice con colonne indipendenti in certe posizioni, allora le colonne nelle stesse posizioni nella matrice di partenza erano indipendenti.

$v_1 | v_2 | v_3 | v_4 | v_5$ in colonna ed effettuate mosse di riga $\Rightarrow$ cambia lo spazio

$\downarrow$

$w_1 | w_2 | w_3 | w_4 | w_5$

se sono indipendenti allora

v_1, v_3, v_5 lo sono a loro volta.

dimostriamo:

osserviamo che facendo le stesse mosse di riga su $v_1 | v_3 | v_5 \xrightarrow[\text{stessi } m]{} w_1 | w_3 | w_5 |$

perché le mosse di riga non hanno peso sui vettori indipendenti. $\rightarrow$ non cambiano le soluzioni del sistema.

Supponiamo

$$a_1 v_1 + a_3 v_3 + a_5 v_5 = 0$$

e voglio dire

$$a_1 = a_2 = a_4 = 0$$

lo scrivo come sistema

$$\begin{pmatrix} a_1 \\ a_3 \\ a_5 \end{pmatrix}$$

risolvo il sistema con matrice

$$5 \left| \underbrace{(v_1 | v_3 | v_5)}_{3} \begin{pmatrix} a_1 \\ a_3 \\ a_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right.$$

gli stessi a_1, a_3, a_5 del primo sistema ci fanno ottenere

$$a_1 w_1 + a_3 w_3 + a_5 w_5 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$a_1 = a_3 = a_5 = 0.$$

es:

$p(x) \in \mathbb{R}[x]^{\leq 3}$ divisibili $\cdot (x-4)$

spazio vettoriale? base?

$$(x-4) \mid p(x) \Rightarrow \exists q(x). \ (x-4) q(x) = p(x)$$

$$p_1(x) = (x-4) q_1(x)$$

$$p_2(x) = (x-4) q_2(x)$$

$$p_1 + p_2 = (x-4)(q_1 + q_2)$$

moltiplicazione vale ✓
lo 0 appartiene ✓.

$$\{p(x)\} = \{(x-4)(ax^2+bx+c) \mid a,b,c \in \mathbb{R}\}$$

$$a(x-4)x^2 + b(x-4)x + c(x-4)$$

$$\text{span}\left(\underbrace{(x-4)x^2}_{\text{base}}; (x-4)x, (x-4)\right)$$

Matematica discreta 23/03/2017

ESERCIZI: Successioni definite per ricorrenza lineare

$$a_{n+2} = 6a_{n+1} - 9a_n$$

con $a_0 = 1$
$a_1 = 6$

$a_{n+k} = c_1 a_{n+k-1} + \dots + c_k a_n$ ← generale

polinomio caratteristico

$$a_{n+2} - 6a_{n+1} + 9a_n = 0$$

[cerco soluzioni del tipo:]

$p(x)$ $x^2 - 6x + 9 = 0$ polinomio associato.

$$(x-3)^2 = 0$$

una sola radice con molteplicità 2.
$r_1 = 3$

↓
"cade x contare due volte"

So provo a risolvere con:

$$a_n = r_1^n \quad \text{oppure} \quad a_n = n r_1^n$$

cerchiamo con una combinazione lineare

$$a_n = A r_1^n + B n r_1^n$$ (perché molteplicità 2).

In generale si tenta con

$$p(x) = (x-r_1)^{d_1}(x-r_2)^{d_2}\cdots(x-r_k)^{d_k}$$

$$r_1^n,\ r_2^n,\ \dots$$

$$n r_1^n,\ n r_2^n$$

al massimo si tenta

$$n^{d-1} r_1^n$$

es: $p(x) = (x-7)^4(x-6)$

si tenterà con: $7^n,\ 6^n$

$$n7^n,\ n^2 7^n,\ n^3 7^n$$

tentativo finale: combinazione lineare

$$a_n = A7^n + B6^n + Cn7^n + Dn^2 7^n + En^3 7^n$$

esercizio era:

$$a_{n+2} - a_{n+1} + 9a_n = 0$$

$$x^2 - 6x + 9 = 0$$

$$(x-3)^2 = 0$$

$$x = 3$$

quindi tento con

$$3^n,\ n3^n,\ A3^n + Bn3^n$$

Sostituendo al posto di a_n i tentativi, la (*) è sempre verificata.
Scegliendo A, B verifico le condizioni iniziali.

Le costanti sono tante quante le condizioni iniziali.

$a_n = 3^n$ $\quad P(3)=0$

$3^2 - 6\cdot 3 + 9 = 0$

$\cdot 3^n$ ↳ $3^{n+2} - 6\cdot 3^{n+1} + 9\cdot 3^n = 0$

sostituisco ↳ $a_{n+2} - 6a_{n+1} + 9a_n = 0$

$a_n = n3^n$ vorrei ottenere che

$a_{n+2} - 6a_{n+1} + 9a_n = 0$

sostituisco:

$(n+2)3^{n+2} - 6(n+1)3^{n+1} + 9n3^n = 0$

$3^n[n\cdot 3^2 - 6n3 + 9n] + [2\cdot 3^2 - 6\cdot 3] = 0$

$n3^n[\underbrace{3^2 - 6\cdot 3 + 9}_{0}] + [\underbrace{2\cdot 3^2 - 6\cdot 3}_{0}] = 0$ ✓

Il 3 è radice anche della derivata → per questo viene $\emptyset$ ↗

- mancano le condizioni iniziali.

$A3^n + Bn3^n = a_n$

$a_0 = 1 \Rightarrow A3^0 + B\cdot 0\cdot 3^0 = 1$

$A = 1$

$a_1 = 6 \Rightarrow A3 + B\cdot 1\cdot 3 = 6$

$3(A+B) = 6$

$A + B = 2$

$1 + B = 2$

$\begin{cases} B = 1 \\ A = 1 \end{cases}$

$a_n = 3^n + n3^n$ soluzione

es: $a_n = 8a_{n-2} - 16a_{n-4}$

$$a_{n+4} - 8a_{n+2} + 16a_n = 0$$

$$p(x) = x^4 - 8x^2 + 16 = 0$$

$t = x^2$

$$t^2 - 8t + 16 = 0$$

$$(t^2 - 4)^2 = 0$$

$$t = 4$$

$$x^2 = 4 \quad x = \pm 2$$

2^n, $n2^n$

$(-2)^n$, $n(-2)^n$ + coi coefficienti:

$$a_n = A2^n + Bn2^n + C(-2)^n + Dn(-2)^n$$

teorema cinese dei resti:

$$\begin{cases} x \equiv b_1 (m_1) \\ x \equiv b_2 (m_2) \\ \vdots \end{cases}$$

→ studio dei m_i

presi i moduli 2 e 2 (primi tra loro) allora il sistema ha soluzione.

es:

$$\begin{cases} 3x \equiv 1 (3) \\ 2x \equiv 3 (5) \\ 4x \equiv 2 (7) \end{cases}$$

mai si risolve.

1) affanno togliendo gli a.

es:

$$\begin{cases} 2x \equiv 1 (3) \\ 3x \equiv 2 (5) \\ 4x \equiv 2 (7) \end{cases}$$

1) moltiplico per l'inverso così mi libero degli a. →

$$\begin{cases} x \equiv 2 (3) & \cdot 2 \\ x \equiv 4 (5) & \cdot 3 \\ x \equiv 4 (7) & \cdot 2 \end{cases}$$

risolvo il sistema:

$$x = 2 + 3k$$

$$2 + 3k \equiv 4 \ (5)$$

$$3k \equiv 2 \ (5)$$

$$k \equiv 4 \ (5)$$

$$k = 4 + 5\ell$$

risostituisco nella x

$$x = 2 + 3(4 + 5\ell)$$

$$x = 2 + 12 + 15\ell$$

$$x = 14 + 15\ell$$

$$x \equiv 14 \ (15)$$

$$\begin{cases} x \equiv -1 \ (15) \\ x \equiv 4 \ (7) \end{cases}$$

→ Ho ridotto le prime due ad una sola congruenza.

$$x = -1 + 15k$$

$$-1 + 15k \equiv 4 \ (7)$$

$$15k \equiv 5 \ (7)$$

$$k \equiv 5 \ (7)$$

$$k = 5 + 7\ell$$

$$x = -1 + 15(5 + 7\ell)$$

$$x = -1 + 75 + 105\ell$$

$$x = 74 + 105\ell$$

$105 = 3 \cdot 5 \cdot 7$ → possibile perché i moduli erano primi due a due.

es:
$$\begin{cases} x \equiv 1 \ (6) \\ x \equiv 2 \ (9) \end{cases}$$

risolubili se $\text{mcd}(6,9) \mid 2-1$

!
mai succede

ESERCIZIO:

$2^x \equiv 4 \ (7)$ tutte le soluzioni?

teorema se p è <u>primo</u>, ie più piccolo n tale che

$$\alpha^n \equiv 1 \ (p)$$ con $n>0$, $\alpha>1$, $\alpha \not\equiv 0 \ (p)$

$\Rightarrow n \mid p-1$

E se faccio $\alpha^{p-1} \equiv 1 \ (p)$

Torniamo all'es:

so che $2^3 \equiv 1 \ (7)$ più piccolo periodicità

$$2^{k3} \equiv 1 \ (7)$$

$$2^2 \cdot 2^{3k} \equiv 2^2 \ (7)$$

$$2^{3k+2} \equiv 2^2 \ (7)$$

se $x = 3k+2$ allora $2^x \equiv 4 \ (7)$

$x \equiv 2 \ (3)$ soluzione

es:
$$\begin{cases} 2^x \equiv 4 \ (7) \\ 5x \equiv 1 \ (12) \end{cases}$$

1) Trasformiamo la congruenza esponenziale in "lineari" poi risolvo come sempre.

anche se fossero tutte congruenze esponenziali

Teorema del Binomio di Newton.

$(x+y)^n = ?$

$(x+y)^2 = x^2 + 2xy + y^2$

$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$

$$
\begin{array}{ccccccc}
 & & & 1 & & & \leftarrow (x+y)^0 \\
 & & 1 & & 1 & & (x+y)^1 \\
 & 1 & & 2 & & 1 & (x+y)^2 \\
1 & & 3 & & 3 & & 1 \quad (x+y)^3 \\
\end{array}
$$

$1 \quad 4 \quad 6 \quad 4 \quad 1 \quad (x+y)^4$

$1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \quad (x+y)^5$

$\vdots$

calo le x e aumento le y:

$(x+y)^5 = \underline{1}x^5 + \underline{5}x^4y + \underline{10}x^3y^2 + \underline{10}x^2y^3 + \underline{5}xy^4 + \underline{1}y^5$

numeri che si trovano nel triangolo di Tartaglia.

$(x+y)^{1000} = ?$ troppo lungo da fare con Tartaglia.

alla riga $n+1$-esima con il triangolo avrò i coefficienti per calcolare $(x+y)^n$

$$
\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & 1 & & 1 & & \\
 & 1 & & 2 & & 1 & \\
 & & & \vdots & & &
\end{array}
$$

$\binom{n}{0}\binom{n}{1} \dots \binom{n}{n}$

$\binom{n}{k}$ = il numero che si trova nella posizione k della riga per il calcolo di $(x+y)^n$.

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

dov'è $\binom{n}{i}$?

$$\binom{n}{i} = \frac{n!}{i!\,(n-i)!}$$

dimostrazione per induzione.

la sommatoria è $p(n)$.

$$(x+y)^0 = \sum_{i=0}^{0} \binom{0}{i} x^{0-i} y^i$$

$p(0)$ $\Downarrow$ 1

$$1 = 1$$

$$(x+y)^1 = \sum_{i=0}^{1} \binom{1}{i} x^{1-i} y^i$$

$$x+y = \binom{1}{0} x + \binom{1}{1} x^0 y^1$$

$$x+y = 1\cdot x + 1\cdot y \quad \checkmark$$

ALGEBRA lineare 28/03/2017

es: $\exists\ L : \mathbb{R}^4 \to \mathbb{R}^4$

applico a vettore della matrice

$$\begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 5 & 6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

studiare la dimensione del nucleo e dell'immagine.

$$L(x,y,z,t) = \begin{pmatrix} x+2y+3z+4t \\ 5z+6t \\ 0 \\ 0 \end{pmatrix}$$

così trovo l'applicazione lineare associata

$\dim(\ker L) = 2$

$$\begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \in \ker(L) \iff A\begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

un elemento sta nel ker se viene "spedito" in 0.

$$\begin{cases} x + 2y + 3z + 4t = 0 \\ 5z + 6t = 0 \end{cases}$$

t e y si scelgono libere

z e x si calcolano

la $\dim(\ker)$ = numero delle variabili libere

sentiti dal sistema.

per sapere esattamente il ker risolvo il sistema e trovo la base.

base del ker:

isolo le variabili libere

$$\begin{pmatrix} \square \\ y \\ \square \\ t \end{pmatrix} = t\begin{pmatrix} \square \\ 0 \\ -\frac{6}{5} \\ 1 \end{pmatrix} + y\begin{pmatrix} -2 \\ 1 \\ \square \\ 0 \end{pmatrix}$$

$-4 + \frac{18}{5} = -\frac{2}{5}$

base del ker.

per calcolare i valori dei quadratini parto prima

$t=1$ e $y=0$ poi $t=0$ e $y=1$

e calcolo i valori sostituendo nelle equazioni

$\dim(\text{Imm } L)$ = numero dei pivot che abbiamo nella matrice.

$\Downarrow$

pari delle colonne con pivot

$\dim(\text{Imm } L) = 2$ ← n° pivot.

Per trovare la base dell'imm.

prendo la 1 e 3 colonna (in questo caso).

teorema: $L: V \to W$ lineare

$$\dim(\ker L) + \dim(\mathrm{Im}\, L) = \dim(V) = n$$

$V \to \dim n$, $W \to \dim k$ (dominio)

$$k\{\underbrace{[L]}_{k\times n}\underbrace{[\ ]^n}_{n\times 1} = k\times 1[\ ]$$

dimostrazione:

caso 1) supponiamo $\ker(L) = V \Rightarrow L(v) = 0 \ \forall v \in V$ tutto va in $\emptyset$.

$\mathrm{Im}(L) = \{\bar{0}\}$ vettore $\emptyset$. $\Rightarrow$ base vuota.

$\dim n$, $L: V \to W$, $\dim k$

$\dim(\ker(L)) + \dim(\mathrm{Im}(L)) = n = \dim V$

$\dim(L)$ perché è un punto.

caso 2) $\ker(L) = \{\bar{0}\} \Rightarrow L$ è iniettiva.

prendiamo una base di V.

$e_1, e_2, \dots, e_n \in V$ (ho n vettori)

$$\mathrm{Im}(L) = \mathrm{span}\{L(e_1), \dots, L(e_n)\}$$

lemma: $L: V \to W$ lineare $e_1, \dots, e_n$ base di V

$$\Rightarrow \mathrm{Im}(L) = \mathrm{span}\{L(e_1), \dots, L(e_n)\}$$

dimostro! $L(e_1) \in W$, $L(e_n) \in W$ perché ho applicato L.

devo che $L(e_1), \dots, L(e_n) \in \mathrm{Im}(L)$

cioè $\mathrm{Im}(L)$ ci stanno tutti gli $L(v)$ con $v \in V$.

$v \in V \Rightarrow v = a_1 v_1 + \dots + a_n v_n \ \exists a_i \in K$ (scalare)

v generico si può scrivere come combinazione lineare della base.

$$w = L(v) = L(a_1 e_1 + \dots + a_n e_n) = a_1 L(e_1) + \dots + a_n L(e_n)$$

$\in \mathrm{Im}(L)$ $\in \mathrm{span}\{L(e_1), \dots, L(e_n)\}$

quindi $\mathrm{Im}(L) \subseteq \mathrm{span}\{L(e_1), \dots, L(e_n)\}$

Vicevers $x \in \text{span}\{L(e_1), \dots, L(e_n)\} \Rightarrow$

$\exists a_1, \dots, a_n \; . \; w = a_1 L(e_1) + \dots + a_n L(e_n) =$

$= L(a_1 e_1 + \dots + a_n e_n)$

quindi $\text{span}\{L(e_1), \dots, L(e_n)\} \subseteq \text{Imm}(L)$

span delle colonne della matrice

□ lemma.

Siamo nel caso 2.

altro lemma:

se L è iniettiva, lineare

Allora L porta vettori indipendenti in vettori indipendenti

dimostro!

$v_1, \dots, v_n$ indipendenti $\in V$.

voglio dimostrare che $L(v_1), \dots, L(v_n)$ sono indipendenti.

Suppongo:

$a_1 L(v_1) + \dots + a_n L(v_n) = 0$

$L(a_1 v_1 + \dots + a_n v_n) = 0$

$L\bar{0} = \bar{0}$ siccome iniettiva

allora $a_1 v_1 + \dots + a_n v_n = \bar{0}$

$\Leftrightarrow \quad a_1 = a_2 = \dots = a_n = 0$. □ lemma

caso 2, di nuovo:

$\ker(L) = \{\bar{0}\} \Rightarrow$ funzione iniettiva.

$L(e_1), \dots, L(e_n)$ sono indipendenti

quindi sono anche una base

- indipendenti
- generatori

$\neq$ vettori.

$\dim(\text{Imm}\, L) = n$

$\dim(\ker L) + \dim(\mathrm{Im}\, L) = 0 + n = n = \dim V.$

caso 2 → vero ✓.

caso 3 → "misto".

$$\underbrace{\dim(\ker L)}_{= l \leq n} + \underbrace{\dim(\mathrm{Im}\, L)}_{=} = \dim V.$$

base di $\ker = \{z_1, \dots, z_l\}$ (ciascuno $\in V$)

per il teorema di completamento a una base esistono vettori $v_1, \dots, v_{n-l} \in V$ tali che

$$\underbrace{z_1, \dots, z_l, v_1, \dots, v_{n-l}}_{n} \text{ sono base di } V.$$

Ho preso una base del $\ker(L)$ e l'ho estesa alla base di V.

$\mathrm{Im}(L) = \mathrm{span}(L(z_1), \dots, L(z_l), L(v_1), \dots L(v_{n-l}))$

non sono indipendenti:

$L(z_1) = L(z_2) = \dots = L(z_l) = 0$ perché erano nel ker e dopo aver applicato L siamo in 0.

ci chiediamo se

$L(v_1), \dots, L(v_{n-l})$ sono indipendenti.

Prendiamo $a_1 L(v_1) + \dots + a_{n-l} L(v_{n-l}) = 0$

$L(a_1 v_1 + \dots + a_{n-l} v_{n-l}) = 0$

posso dire che $a_1 v_1 + \dots + a_{n-l} v_{n-l} \in \ker L$

$\Rightarrow \exists b_1, \dots, b_n \in K$ t.c.

$$a_1 v_1 + \dots + a_{n-l} v_{n-l} = b_1 z_1 + \dots + b_k z_k$$

$a_1 v_1 + \dots + a_{n-\ell} v_{n-\ell} - b_1 z_1 - \dots - b_k z_k = 0$

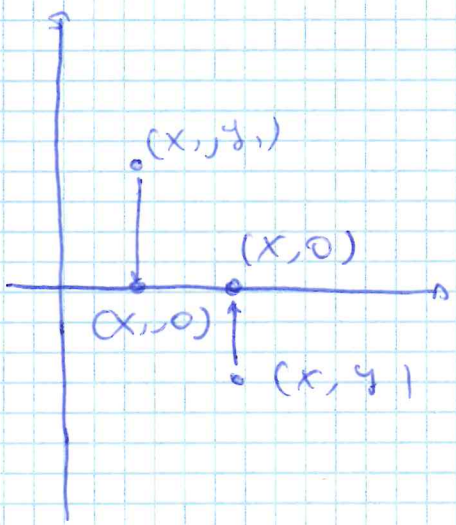
$\bar{v}, \bar{z}$ erano base di V

$$\underbrace{a_1 = \dots = a_{n-\ell}}_{=0} = b_1 = \dots = b_k = 0$$

Quindi $L(v_1), \dots, L(v_{n-\ell})$ sono una base di $\mathrm{Im}(L)$

$$\dim(\ker L) + \dim(\mathrm{Im}\, L) = \dim V$$
$$\ell \qquad\qquad -\ell + n \qquad = n$$

es: $L : \mathbb{R}^2 \to \mathbb{R}^2$



$$(x, y) = (x, 0)$$

$$\ker(L) = \{(0, y) \mid y \in \mathbb{R}\}$$
$$\mathrm{Im}(L) = \{(x, 0) \mid x \in \mathbb{R}\}$$

es: $f : \mathbb{R}^3 \to \mathbb{R}^3$

$f(0,0,1) = (2, 3, 4)$

$f(0,2,0) = (6, 8, 10)$

$f(1,0,0) = (10, 14, 18)$

Calcolare $\dim(\ker f)$, $\dim(\mathrm{Im}\, f)$.

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$ base del dominio $\mathbb{R}^3$.

$$\mathrm{Im}(f) = \mathrm{span}\left(\begin{pmatrix}2\\3\\4\end{pmatrix}, \begin{pmatrix}6\\8\\10\end{pmatrix}, \begin{pmatrix}10\\14\\18\end{pmatrix}\right) = \mathrm{span}\left(\begin{array}{c|c}2 & 6\\3 & 8\\4 & 10\end{array}\right)$$

indipendenti

possibile che non sono base

superflua $\quad C3 = 2C1 + C2$

$\dim(\text{Imm } f) = 2$
$\Rightarrow \dim(\ker f) = 1$ $\not\Rightarrow 3$

Quando trovo l'immagine faccio automaticamente la dim del Ker.

$L: V \to W$ lineare

$[L]$ matrice L.

Facendo mosse di riga

$\ker(L)$ non cambia (l'immagine cambia).

$L \quad\quad L_M$

$\downarrow \quad\quad \uparrow$

$[L] \xrightarrow{\text{riga}} M$ $\qquad \ker(L) = \ker(L_M)$

$\text{Imm}(L)$ può cambiare

però siccome $\dim(\ker L) + \dim(\text{Imm } L) = \dim(V)$

numero fisso

posso dire che la dimensione dell'immagine non cambia.

poiché la somma tra ker e imm non cambia (è un numero fisso).

Con le mosse di colonna è il viceversa:

l'immagine non cambia il ker può cambiare ma la dimensione rimane sempre la stessa.

$\text{Imm}[L] =$ span colonne.

Lavoro in $\mathbb{R}^4$: per sapere se sono indipendenti?

$$\left(\begin{array}{c|c|c} 2 & 5 & 8 \\ 3 & 6 & 9 \\ 4 & 7 & 10 \\ 11 & 12 & 13 \end{array}\right)$$

per essere indipendenti:

$$\ker(?) = 0.$$

$$a_1\begin{pmatrix}1\\2\\3\\4\\11\end{pmatrix} + a_2\begin{pmatrix}5\\6\\7\\12\end{pmatrix} + a_3\begin{pmatrix}8\\9\\10\\13\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

$$a_1 = a_2 = a_3 = 0$$

$$\begin{pmatrix}2 & 5 & 8\\3 & 6 & 9\\4 & 7 & 10\\11 & 12 & 13\end{pmatrix}\begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

quindi

$$\ker(\text{matrice}) = 0$$

se sono indipendenti, l'unica soluzione è $a_1 = a_2 = a_3 = 0$ cioè

Per risolvere portiamo la matrice a scalini e se il numero dei pivot è uguale al numero di colonne i vettori sono indipendenti.