Risposte Orale Breve MD

Alessandro Pagiaro

Aggiornato al 23 Giugno 2014

Indice

1 Domanda 2 - Somma dei primi n numeri...

$$\sum_{i=0}^{n} i = \frac{(n+1)n}{2}$$

Questo risultato si dimostra facilmente per via grafica. Basterà immaginare un triangolo rettangolo con i cateti di lunghezza n e calcolarne l'area.
Per quanto riguarda la somma dei quadrati possiamo procedere in maniera analoga e ottenere che

$$\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Approfondisci >>

2 Domanda 3 - Induzione

Gli esercizi così si risolvono trovando il minimo numero $n \in \mathbb{N}$ per cui vale la relazione data e la si dimostra per induzione su n.

3 Domanda 4 - Fare una dimostrazione del Principio del minimo

Teorema (Principio del minimo o del Buon Ordinamento)**.** *Ogni sottoinsieme non vuoto di* $\mathbb{N}$ *ha un elemento minimo.*

Una dimostrazione dove lo si usa è quella del Teorema di Bezout.

4 Domanda 8 - $g \circ f$ iniettività

Data $f : X \to Y$ e $g : Y \to Z$
Data $g \circ f : X \to Z$ iniettiva, è vero che:

- $\Rightarrow f$ iniettiva
- $\Rightarrow g$ iniettiva

VERO!

Dimostrazione. difatti, se una delle due non fosse iniettiva potrei avere una $\bar{x}$ e una $\bar{y}$ con $\bar{x} \neq \bar{y}$ tale che $f(\bar{x}) = f(\bar{y})$ per cui $g(f(\bar{x})) = g(f(\bar{y}))$ con $\bar{x} \neq \bar{y}$. Cioè avrei $g \circ f$ non iniettiva, assurdo, visto che per ipotesi la composizione è iniettiva. $\square$

Si dimostra in maniera analoga che g deve essere iniettiva.

5 Domanda 9 - $g \circ f$ surgettività

Data $f : X \to Y$ e $g : Y \to Z$
Data $g \circ f : X \to Z$ surgettiva, è vero che:

- $\Rightarrow f$ surgettiva
- $\Rightarrow g$ surgettiva

Se $g \circ f$ è surgettiva $\Rightarrow |X| \supseteq |Z|$.
È FALSO che $\Rightarrow f$ surgettiva. Costruisco un esempio che mi nega l'affermazione.
Prendo $X = \{1,2,3,4\} = \mathbb{N}_4, Y = \mathbb{N}_5, Z = \mathbb{N}_4$. Definisco ora:

$$f(x) = x$$

$$g(x) = \begin{cases} x & se\ x \in \{1,2,3,4\} \\ 4 & se\ x = 5 \end{cases}$$

La composizione risulterà chiaramente surgettiva eppure la f non è surgettiva, difatti l'elemento $5 \in Y$ non viene mai raggiunto da alcuna $x \in X$ eppure $\forall z \in Z\ \exists x | f \circ g(x) = z$.
È VERO che $\Rightarrow g$ surgettiva.

Dimostrazione. Se infatti non fosse così, poichè per definizione di funzione

$$g \circ f = g(f(x))$$

non riuscirei a raggiungere un elemento in Z poichè qualunque elemento x scelgo, $g(f(x))$ non lo raggiungerebbe e quindi $g \circ f$ risulterebbe non surgettiva. Ma questo va contro la nostra ipotesi iniziale. □

6 Domanda 12 - $\binom{n}{r} = \binom{n}{n-r}$

$\binom{n}{n-1} = \binom{n}{1}$ difatti dato X tale che $|X| = n$ i suoi sottoinsiemi di cardinalità 1 sono tanti quanti sono i sottoinsiemi di cardialità $n-1$. La corrispondenza biunivoca è data dall'operazione di prendere il complementare.
Più in generale, dato $0 \leqslant r \leqslant n$, vale che

$$\binom{n}{r} = \binom{n}{n-r}$$

7 Domanda 13 - $\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$

Dato $1 \leqslant r \leqslant n-1$

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$$

poichè $n \geqslant 1$, posso prendere un elemento $a \in X$. Per calcolare $\binom{n}{r}$ devo calcolare la $|\mathcal{P}_r(X)|$.
Prendo

$$L_1 = \{\mathcal{P}_r(X) \mid a \in \mathcal{P}_r(X)\}$$
$$L_2 = \{\mathcal{P}_r(X) \mid a \notin \mathcal{P}_r(X)\}$$

Quindi

$$\mathcal{P}_r(X) = L_1 \cup L_2$$

Trattandosi di insiemi disgiunti:

$$\binom{n}{r} = |\mathcal{P}_r(X)| = |L_1| + |L_2|$$

Vediamo quindi quanto vale $|L_1|$. L_1 sono tutti quei sottoinsiemi che oltre ad a contengono elementi di X. Cioè:

$$\binom{n-1}{r-1} = |L_1|$$

Analogamente prendo l'insieme $X - \{a\}$, che conterrà quindi $n-1$ elementi, formando sottoinsiemi da r elementi, cioè:

$$\binom{n-1}{r} = |L_2|$$

Quindi:

$$\binom{n}{r} = |\mathcal{P}_r(X)| = \binom{n-1}{r-1} + \binom{n-1}{r}$$

8 Domanda 17 - $\sum_{i=0}^{n}(-1)^i\binom{n}{i}$

Sia $n \in \mathbb{N}$. Quanto vale $\sum_{i=0}^{n}(-1)^i\binom{n}{i}$? Spiegare.
La sommatoria vale 0.

Dimostrazione. Per n pari è banalmente verificato, difatti $\binom{n}{1} = \binom{n}{n}$. Per n dispari invece io la dimostro così (credo che Gaiffi ce la lasciò per esercizio):
Data la formula del binomio di Newton (Teorema 8.1, pag 79)

$$(a+b)^n = \sum_{i=0}^{n}\binom{n}{i}a^{n-1}b^i \tag{1}$$

Vogliamo ora usare questa formula per dimostrare che:

$$\sum_{i=0}^{n}(-1)^i\binom{n}{i} = 0 \tag{2}$$

Quindi scelgo opportunamente a e b affinché la sommatoria della formula (1) faccia 0. So che la sommatoria $(1) = (a+b)^n$. Data la somiglianza con la formula (2) pongo $a = 1$ e $b = -1$, così facendo il termine a sinistra della formula (1) mi risulterà 0, mentre quello a destra risulterà:

$$\sum_{i=0}^{n} \binom{n}{i} 1^{n-1}(-1)^i$$

1 elevato a qualcosa in un prodotto non mi da alcun contributo, ergo lo posso trascurare, riordinando i termini ottengo proprio la formula (2), che è quella che volevo dimostrare. □

9 Domanda 20 - $ax \equiv b\ (m)$ ha soluzione se...

Siano $a, b, c \in \mathbb{Z}$ con $m \geq 1$. Esporre una condizione necessaria e sufficiente perchè l'equazione $ax \equiv b\ (m)$ abbia soluzione e spiegare la motivazione.

L'equazione $ax \equiv b\ (m)$ non ha soluzione se $MCD(a, m)$ non divide b.

Dimostrazione. Se $ax \equiv b\ (m)$ ha soluzione esiste un interno $\bar{x}$ e un intero k tali che $a\bar{x} = b + km$, ma supponendo che $d = MCD(a, m)$ divide a e m si vede subito che deve dividere anche b. □

L'equazione $ax \equiv b\ (m)$ ha soluzione se $MCD(a, m)$ divide b.

Dimostrazione. Se $MCD(a, m)$ non divide b sappiamo già che la congruenza non ha soluzioni. Quindi consideriamo il caso in cui $MCD(a, m)$ divide b. In questo caso $MCD(a, m)$ è dunque anche il massimo fattore positivo comune a tutti e tre i numeri a, b, m; dividendo per $MCD(a, m)$ otteniamo la congruenza equivalente $a'x \equiv b'\ (m')$. A questo punto osserviamo che, per costruzione, a' e m' sono coprimi e sappiamo che in questo caso a' ha un inverso e' modulo m'. Una volta trovato e' sappiamo che le soluzioni della $a'x \equiv b'\ (m')$, sono tutti e soli gli interi della forma $e'b' + km'$ al variare di k in $\mathbb{Z}$. Visto che $m' = \frac{m}{MCD(a,m)}$ ci sono esattamente $MCD(a, m)$ interi di questa forma in ogni sequenza di m elementi consecutivi. □

10 Domanda 21 - $ax + by = c$ ha soluzione se...

Teorema. *L'equazione diofantea $ax + by = c$ (con a e b non entrambi nulli) ha soluzione se e solo se $MCD(a, b)$ divide c.*

Dimostrazione. Sappiamo, per Bezout, che se l'equazione $ax + by = c$ fosse

$$ax + by = MCD(a, b)$$

questa avrebbe soluzioni certamente.
Ma l'equazione che dobbiamo risolvere differisce da questa perchè abbiamo c invece di $MCD(a,b)$. Quindi, ci basterà chiederci se

$$MCD(a,b)|c\ ?$$

Se sì:
$\rightarrow$ L'equazione ammette soluzioni.
No, altrimenti.
Infatti si parte da una coppia (m,n) che risolve l'equazione $ax+by = MCD(a,b)$:

$$am + bn = MCD(a,b)$$

e si moltiplicano entrambi i membri per k. Troviamo allora:

$$a(mk) + b(nk) = MCD(a,b) \cdot k = c$$

dunque (mk, nk) è una soluzione dell'equazione iniziale.

□

Viceversa, se la risposta è no, cioè $MCD(a,b) \not| c$, allora l'equazione non può avere soluzioni e lo possiamo dimostrare per assurdo.

Dimostrazione. Ammettiamo che esiste una soluzione $(\bar{x}, \bar{y})$. Consideriamo l'uguaglianza

$$a\bar{x} + b\bar{y} = c$$

ricaveremo che, visto che $MCD(a,b)|a\bar{x}+b\bar{y}$ deve dividere anche quello a destra. Questo è però assurdo poichè eravamo nel caso in cui $MCD(a,b) \not| c$. □

11 Domanda 22 - Se $ax + bt = c$ ha sol $\Rightarrow$ le sol. sono infinite

Prendiamo l'equazione omogenea associata:

$$ax + by = 0$$

Cerchiamo $(\bar{x}, \bar{y})$ che mi risolvono l'equazione:

$$ax + by = 0 \tag{3}$$
$$ax = -by \tag{4}$$
$$\frac{a}{MCD(a,b)}x = -\frac{b}{MCD(a,b)}y \tag{5}$$

Questa equazioni è equivalente a quella iniziale. Supponiamo di avere una soluzione (γ, δ):

$$\frac{a}{MCD(a,b)}\gamma = -\frac{b}{MCD(a,b)}\delta$$

A questo punto, visto che i numeri $\frac{a}{MCD(a,b)}, \frac{b}{MCD(a,b)}$ sono primi fra loro, allora δ è della forma $\frac{a}{MCD(a,b)}t$ e γ risulta uguale a $-\frac{b}{MCD(a,b)}t$. Quindi una qualunque coppia della forma

$$\left(-\frac{b}{MCD(a,b)}t, \frac{a}{MCD(a,b)}t\right)$$

con $t \in \mathbb{Z}$ è una soluzione dell'equazione omogenea associata.

Teorema. *Se l'equazione diofantea ammette soluzioni, allora ammette infinite soluzioni. Presa una soluzione particolare* $(\bar{x}.\bar{y})$*, l'insieme* S *di tutte le soluzioni può essere descritto così:*

$$S = \{(\bar{x}+\gamma, \bar{y}+\delta|(\gamma,\delta) \text{ è soluzione dell'equazione omogenea associata}\}$$

12 Domanda 23 - Bezout

Teorema (di Bezout)**.** *Dati due interi* a *e* b *con* $(a,b) \neq (0,0)$*esistono due numeri interi* m *e* n *tali che*

$$MCD(a,b) = am + bn$$

Dimostrazione. Consideriamo l'insieme $CL(a,b)$ di tutte le possibili combinazioni lineari positive a coefficienti interi di a e b, cioè

$$CL(a,b) = \{ar + bs \mid r \in \mathbb{Z}, s \in \mathbb{Z}, ar + bs > 0\}$$

Tale insieme è non vuoto (difatti $(a,b) \neq (0,0)$).
Inoltre $CL(a,b) \subseteq \mathbb{N}$. Dunque per il principio del buon ordinamento ammette minimo.
Sia d tale minimo: in particolare, dato che $d \in CL(a,b)$, esistono un $m \in \mathbb{Z}$ ed un $n \in \mathbb{Z}$ tali che

$$d = am + bn$$

La dimostrazione del teorema si conclude ora mostrando che $d = MCD(a,b)$. Infatti d soddisfa le proprietà del massimo comune divisore, cioè:

- $d \mid a$
- se $c \mid a$ e $c \mid b$ allora $c \leq d$

Per il primo punto facciamo la divisione euclidea tra a e d. Sarà $a = qd + r$ con $0 \leq r < d$.
Allora

$$a = q(am + bn) + r$$

da cui

$$r = (-qm + 1)a + (-qn)b$$

Ma allora r si esprime come combinazione lineare a coefficienti interi di a e di b. Si fosse $r > 0$ avremmo che $r \in CL(a, b)$ per definizione di $CL(a, b)$. Questo non può succedere perchè $0 \leq r < d$ e d era stato scelto come minimo elemento di $CL(a, b)$. Dunque deve essere $r = 0$. Questo vuol dire che $a = qd + 0$, ossia $d \mid a$. Allo stesso modo si verifica $d \mid b$.

Il secondo punto è immediato. Infatti se $c|a$ e $c|b$ allora $c \mid am + bn$, cioè $c|d$, in particolare $c \leq d$. □

13 Domanda 24 - $\cancel{d} \cdot a \equiv \cancel{d} \cdot b \ (\frac{m}{MCD(d,m)})$

$$d \cdot a \equiv d \cdot b \ (m) \Leftrightarrow a \equiv b \ \left(\frac{m}{MCD(d, m)}\right)$$

Dimostrazione. Dimostriamo $\Leftarrow$)
Supponiamo che $a \equiv b \ \left(\frac{m}{MCD(d,m)}\right)$ e cerchiamo di dimostrare che $d \cdot a \equiv d \cdot b \ (m)$.
Da

$$a \equiv b \ \left(\frac{m}{MCD(d, m)}\right)$$

{per definizione di congruenza}

$$\frac{m}{MCD(d, m)} \mid a - b$$

{che equivale a dire}

$$\frac{m}{MCD(d, m)} \cdot \gamma = a - b$$

$$m \cdot \gamma = (a - b)MCD(d, m)$$

Vorrei quindi ora dimostrare che $m|(a - b) \cdot d \Leftrightarrow a \cdot d \equiv b \cdot d \ (m)$

$$m \cdot \gamma \cdot d_1 = (a - b) \cdot MCD(d, m) \cdot d_1 = (a - b) \cdot d$$

Quindi:

$$m|(a - b) \cdot d$$

Dimostriamo ora $\Rightarrow$)
Dal fatto che

$$da \equiv db \ (m)$$

{per definizione di equivalenza}

$$m|da - db$$

{cioè...}

$$m \cdot \nu = da - db = d(a-b)$$

{divido per $MCD(d,m)$}

$$\frac{m}{MCD(d,m)} \cdot \nu = \frac{d}{MCD(d,m)}(a-b)$$

{Poichè $MCD\left(\frac{m}{MCD(d,m)}, \frac{d}{MCD(d,m)}\right) = 1$, cioè sono coprimi, per Bezout}

$$MCD(d,m) = \lambda d + \mu m$$

{divido per $MCD(d,m)$}

$$1 = \lambda \frac{d}{MCD(d,m)} + \mu \frac{m}{MCD(d,m)}$$

Per Bezout, 1 allora è l'MCD cercato (non so cosa intendevo con quest'ultima frase).
Poichè sono primi tra loro:

$$\frac{m}{MCD(d,m)} | \frac{d}{MCD(d.m)}(a-b)$$

Difatti $\frac{m}{MCD(d,m)}, \frac{d}{MCD(d.m)}$ sono primi tra loro.

$$\frac{m}{MCD(d,m)} | (a-b)$$

cioè

$$a \equiv b \ \left(\frac{m}{MCD(d,m)}\right)$$

□

14 Domanda 25 - Moltiplicare a destra e a sinistra una congruenza

Teorema. *Sia $MCD(k,m) = 1$, allora $ak \equiv bk \ (m) \Rightarrow a \equiv b \ (m)$*

Dimostrazione. Dall'ipotesi che $MCD(k,m) = 1$ segue che $1 = \lambda k + \mu m$ e quindi λ è l'inverso di k. Moltiplicando entrambi i membri per λ otteniamo $\lambda ak = \lambda bk \ (m)$. Siccome $\lambda k = 1 \ (m)$ otteniamo allora

$$a \equiv b \ (m)$$

□

15 Domanda 26 - Piccolo teorema cinese del resto con moduli coprimi

$$\begin{cases} x \equiv a \ (m_1) \\ x \equiv b \ (m_2) \end{cases}$$

Osserviamo che le soluzioni della prima equazione sono

$$x = a + km_1 \text{ con } k \in \mathbb{Z}$$

Mi chiedo se tale numero risolve la seconda soluzione. Sostituisco quindi x nella seconda equazione ottendendo

$$a + km_1 \equiv b \ (m_2)$$

Qui la nostra variabile è quindi diventata k:

$$m_1 k \equiv b - a \ (m_2)$$

E sappiamo che ha soluzione solo se $MCD(m1, m2)|b - a$
Poichè noi abbiamo che $MCD(m_1, m_2) = 1$, il nostro sistema ammetterà sempre soluzione. Tale soluzione sarà $0 \leq x_o < m_1 m_2$. Tutte le soluzioni del sistema sono della forma $x_0 + qm_1 m_2$ con $q \in \mathbb{Z}$.

16 Domanda 27 - Ancora roba cinese...

Le soluzioni di

$$ax \equiv b \ (m_1 m_2)$$

coincidono con le soluzioni di

$$\begin{cases} ax \equiv b \ (m_1) \\ ax \equiv b \ (m_2) \end{cases}$$

VERO!

Dimostrazione. Se $\bar{x}$ è soluzione di

$$ax \equiv b \ (m_1 m_2)$$

allora $\bar{x}$ è soluzione anche di

$$ax \equiv b \ (m_1)$$

e di

$$ax \equiv b \ (m_2)$$

Detto in altro modo

$$m_1 m_2 | a\bar{x} - b \Leftrightarrow m_1 | a\bar{x} - b \ \wedge \ m_2 | a\bar{x} - b$$

Viceversa se $\bar{x}$ risolve il sistema allora posso dire che

$$m_1|a\bar{x}-b \ \wedge \ m_2|a\bar{x}-b$$

e quindi

$$m_1 m_2|a\bar{x}-b$$

□

17 Domanda 28 - $ax + by = c$ e $ax = c$ (b) in che modo sono collegate?

Data (x, y) la soluzione della diofantea $ax + by = c$, il numero intero x deve anche soddisfare $ax \equiv c$ (b). Infatti $by = c - ax$, cioè $b|c - ax$. Dunque se esiste una x che soddisfa $ax \equiv c$ (b) allora soddisfa anche $b|ax - c$ e quindi esiste una y tale $by = ax - c$ trova soluzione.

18 Domanda 29 - I numeri primi sono infiniti

Teorema. *I numeri primi sono infiniti.*

Dimostrazione. Sia P l'insieme dei numeri primi.
Supponiamo per assurdo che P sia finito e dunque siano

$$p_1, p_2, ..., p_n$$

tutti i numeri primi. Consideriamo allora il numero

$$a = (p_1 \cdot p_2 \cdot ... \cdot p_n) + 1$$

Come accade per tutti i numeri maggiori o uguali a 2, c'è un numero primo che divide a. Nel nostro caso vuol dire che uno dei p_i divide a. Ma nessuno dei nostri p_i divide a, visto che, per ogni $i = 1, 2, .., n$ vale $a \equiv 1$ $(mod\ p_i)$. □

19 Domanda 30 - $a' = \frac{a}{MCD(a,b)}$ e $b' = \frac{b}{MCD(a,b)}$ sono coprimi

Teorema. *Presi due numeri interi a e b non entrambi nulli, se li dividiamo per il loro MCD, cioè:*

$$a' = \frac{a}{MCD(a,b)} \ \text{e} \ b' = \frac{b}{MCD(a,b)}$$

$MCD(a', b') = 1$.

Dimostrazione. Se ci fosse un divisore $d > 1$ di a' e b', allora $d \cdot MCD(a, b)$ dividerebbe sia a che b e sarebbe più grande di $MCD(a, b)$, assurdo. □

20 Domanda 31 - Perchè l'algoritmo di Euclide funziona

Perchè l'algoritmo di Euclide termina?

$$
\begin{aligned}
a &= bq + r \\
b &= b'q' + r' \\
&\dots
\end{aligned}
$$

r^n nel nostro algoritmo sarà sempre

$$0 \leq r^n < r^{n-1}$$

cioè prima o poi arriverà a 0.

Perchè funziona?

Funziona poichè:

Teorema. *Se* $c \equiv c'$ (m) *allora* $MCD(c, m) = MCD(c', m)$. *In particolare* $MCD(c, m) = MCD(Resto(c, m), m)$.

Dimostrazione. Consideriamo un divisore d di m. Allora, visto che per la definizione di congruenza deve valere $c = c' + mk$ per un certo intero k, possiamo concludere che $d|c \Leftrightarrow d|c'$. Quindi i divisori comuni di m e c coincidono con i divisori comuni di m ed c'. Anche i massimo devono allora coincidere. □

21 Domanda 32 - Criteri di divisibilità

21.1 Criterio di divisibilità per 3

Cosa dice il criterio

Sommo le cifre che compongono il numero, se il risultato che ottengo è divisibile per 3 allora anche il numero iniziale risulta divisibile per 3.

Perchè funziona

Prendiamo ad esempio 18743291.
$18743291 = 1 \cdot 10^7 + 8 \cdot 10^6 + 7 \cdot 10^5 + 4 \cdot 10^4 + 3 \cdot 10^3 + 2 \cdot 10^2 + 9 \cdot 10^1 + 1$

$$10 \equiv 1 \ (mod\ 3)$$

Quindi: $18743291 = 1 + 8 + 7 + 4 + 3 + 2 + 9 + 1 = 8 = 2 \ (mod\ 3)$

21.2 Criterio di divisibilità per 7

Cerco un multiplo di 10 comodo per l'operazione *mod* 7

$$\begin{aligned}10 &\equiv 3\ (7)\\ 100 &\equiv 2\ (7)\\ 1000 &\equiv -1\ (7)\end{aligned}$$

Prendiamo 3417822.

$$3417822 = 3 \cdot 1000^2 + 417 \cdot 1000 + 822$$

Essendo $1000 \equiv -1\ (7)$:

$$\begin{aligned}3417822 &= 3 \cdot (-1)^2 + 417 \cdot (-1) + 822\\ &= 3 - 417 + 822\\ &= 408\\ &= 7 \cdot 58 + 2\\ &\equiv 2\ (mod\ 7)\end{aligned}$$

21.3 Criterio di divisibilità per 11

$$10 \equiv -1\ (11)$$

Prendiamo 78922.

$$\begin{aligned}78922 &= 7 \cdot 10^4 + 8 \cdot 10^3 + 9 \cdot 10^2 + 2 \cdot 10 + 2\\ &\equiv 7 \cdot (-1)^4 + 8 \cdot (-1)^4 + 9 \cdot (-1)^2 + 2 \cdot (-1) + 2\\ &= 7 - 8 + 9 - 2 + 2\\ &\equiv 8\ (mod\ 11)\end{aligned}$$

22 Domanda 33 - Classi di resto et alia

Sia m un numero intero positivo. Per ogni $i = 0, 1, 2, ..., m - 1$ chiamiamo $[i]_m$ la classe di resto di i modulo m, ossia l'insieme dei numeri che danno resto i quando si considerano la loro divisione euclidea per m:

$$[i]_m = \{x \in \mathbb{Z} \mid x \equiv i\ (m)\}$$

Definiamo poi $\mathbb{Z}_m$ l'insieme di tutte le classi di resto modulo m:

$$\mathbb{Z}_m = \{[0]_m, [1]_m, ..., [m-1]_m\}$$

Teorema. *Se p è un numero primo, allora $\mathbb{Z}_p$ è un campo.*

Dimostrazione. Se prendiamo una classe di resto $[a]_p \neq [0]_p$ in $\mathbb{Z}_p$, allora deve valere che $MCD(a, p) = 1$. allora la congruenza $ax \equiv 1\ (p)$ ha soluzione, dunque esiste $b \in \mathbb{Z}$ tale che $ab \equiv 1\ (p)$. Come conseguenza in $\mathbb{Z}_p$ vale

$$[a]_p[b]_p = [ab]_p = [1]_p$$

Abbiamo allora dimostrato che $[a]_p$ è invertibile in $\mathbb{Z}_p$ e che $[b]_p$ è il suo inverso. Quindi $\mathbb{Z}_p$ ha l'inverso per ogni numero $\Rightarrow$ è un campo. □

23 Domanda 34 - Piccolo Teorema di Fermat

Teorema (Il piccolo teorema di Fermat)**.** *Se p è un numero primo e a è un numero intero che non è multiplo di p, allora vale che*

$$a^{p-1} \equiv 1\ (p)$$

Dimostrazione. Consideriamo l'anello $\mathbb{Z}_p$ delle classi di resto modulo p:

$$\mathbb{Z}_p = \{[0], [1], ..., [p-1]\}$$

Vista la scelta di a, sappiamo che $[a] \neq [0]$. Moltiplichiamo ora tutti gli elementi di $\mathbb{Z}_p$ per $[a]$:

$$[a][0], [a][1], ..., [a][p-1]$$

Questi p elementi sono tutti diversi fra loro?
Se sì $\Rightarrow$ sappiamo esattamente tutti gli elementi di $\mathbb{Z}_p$, che ha cardinalità p.
Verifichiamo dunque che sono tutti diversi fra loro: supponiamo, per assurdo, che esistano i e j, con $(0 \leq i \leq j \leq p-1)$ con $[i] \neq [j]$ ma tali che $[a][i] = [a][j]$.

Poichè p è primo, $\mathbb{Z}_p$ è un campo, quindi ogni elemento $\in \mathbb{Z}_p$ ha un inverso. Sia dunque $[b]$ l'inverso di $[a]$. Moltiplicando per $[b]$ otteniamo:

$$[b][a][i] = [b][a][j]$$

Siccome $[a][b] = 1$

$$[i] = [j]$$

Poichè avevamo supposto $[i] \neq [j]$, abbiamo trovato un assurdo.

Visto ora che sono tutti distinti, sappiamo che la lista

$$[a][0], [a][1], ..., [a][p-1]$$

ha esattamente tutti gli elementi di $\mathbb{Z}_p$. allora facciamo il prodotto degli elementi di questa lista, eccetto di $[a][0] = [0]$, deve valere

$$[a][1]...[a][p-1] = [1][2][3]...[p-1]$$

visto che nel membro a sinistra e in quello a destra abbiamo tutti gli elementi (magari in ordine diverso).
Per la proprietà commutativa possiamo riscrivere l'uguaglianza nella forma

$$[a]^{p-1}[1]...[p-2][p-1] = [1][2][3]...[p-2][p-1]$$

Poichè $[p-1]$ è invertibile in $\mathbb{Z}_p$, moltiplichiamo entrambi i membri per il suo inverso. Otteniamo quindi

$$[a]^{p-1}[1]...[p-2] = [1][2][3]...[p-2]$$

Poi moltiplichiamo entrambi i membri per l'inverso di $[p-2]$, poi di $[p-3]$ e così via...
Alla fine troviamo

$$[a]^{p-1} = [1]$$

che si riscrive, in termini di congruenze come

$$a^{p-1} \equiv 1 \ (p)$$

che è proprio l'enunciato che volevamo dimostrare. □

24 Domanda 36 - $a^{561} \equiv a \ (561)$

Vale poichè 561 è un numero di Carmichael. Approfondisci su Wikipedia >>

25 Domanda 44 - Scrittura unica per i vettori

Teorema. *Ogni elemento di uno spazio vettoriale si scrive in modo unico come combinazione lineare degli elementi di una base.*

Dimostrazione. Prendiamo la base B di V

$$V = \{v_1, v_2, ..., v_n\}$$

Prendiamo il vettore

$$q = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 + ... + \alpha_n v_n$$

e prendiamo anche il vettore

$$t = \beta_1 v_1 + \beta_2 v_2 + \beta_3 v_3 + ... + \beta_n v_n$$

. Visto che questi due vettori sono uguali

$$q = t$$

$$q - t = 0$$

$$\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 + ... + \alpha_n v_n - (\beta_1 v_1 + \beta_2 v_2 + \beta_3 v_3 + ... + \beta_n v_n) = 0$$

$$(\alpha_1 - \beta_1)v_1 + (\alpha_2 - \beta_2)v_2 + ... + (\alpha_n - \beta_n)v_3 = 0$$

Poichè $v_i \neq 0 \forall i$ devono essere $= 0$ i coefficienti $\alpha_i \beta_i \forall i$. Quindi:

$$\alpha_i - \beta_i = 0$$

$$\alpha_i = \beta_i$$

□

26 Domanda 45 - Scarti successivi per estrarre base

Teorema. *Sia V uno spazio vettoriale di dimensione finita su $\mathbb{K}$. Da ogni insieme di generatori di V si può estrarre una base. Formalmente:*

$$\forall g \subseteq V < g >= V \Rightarrow \exists B \subseteq g | B \text{ è una base di } V)$$

Dimostrazione. Se g è linearmente indipendente allora questo è già una base di V.

Se invece g è composto da elementi linearmente dipendenti, ovvero $\alpha_1 v_1 + ... + \alpha_n v_n = 0$ per a_i non tutti nulli $\Rightarrow \exists i | \alpha_i \neq 0$ (esiste un elemento non nullo)

ma allora

$$v_i = \frac{-1}{\alpha_i}(\alpha_1 v_1 + ... + \cancel{a_i v_i} + ... + \alpha_n v_n)$$

e quindi abbiamo scoperto che $v_i \in < v_1, ..., v_n >$ cioè v_i è combinazione lineare di $g - \{v_i\}$.

Questo vuol dire che l'insieme g si può ridurre eliminando l'elemento a esso dipendente. □

27 Domanda 48 - Numero di pivot non dipende dalla riduzione a scala

Saper spiegare perchè il numero di pivot di una matrice non dipende dalla riduzione a scala effettuata. Definizione di rango di una matrice.

Diciamo innanzitutto che il rango della matrice è il numero di pivot che presenta la matrice. I pivot sono il numero di righe in una matrice a scala che presentano come primo elemento un numero non nullo.

Ci basta ora dimostrare quindi che la riduzione a scala effettuata, quindi le operazioni elementari di riga effettuate, non alterano il rango di una matrice.

Teorema. *Siano $\{v_1, ..., v_m\} \in \mathbb{K}^n \mid < v_1, ..., v_m >= V \subseteq \mathbb{K}^n$.*

Sia A una matrice e S la sia S la sua riduzione a scala.

Siano $j_1, ..., j_r$ le colonne che contengono i pivot. Allora i vettori $V_{j_1}, ..., v_{j_r}$ (della matrice A) sono una base di V estratta dall'insieme dei generatori $\{v_1, ..., v_m\}$

Dimostrazione. Dimostriamo che $V_{j_1}, ..., v_{j_r}$ sono una base di V.
1) Sono linearmente indipendenti. Data la matrice M, le colonne di M sono linearmente indipendenti $\Leftrightarrow$ $Mx = 0$ ha come unica soluzione $x = 0$ cioè, $\Leftrightarrow$ $rkM = |$Colonne di $M|$

Calcoliamo quindi il rango di M e verificare che sia r.
Agisco su M con le stesse operazioni fatte su A per ottenere S. Il numero di Pivot che ottengo è ancora r e quindi $rkM = r$. ciò dimostra che $\{V_{j_1}, ..., v_{j_r}\}$ sono linearmente indipendenti.

2) Generano V, cioè che $< V_{j_1}, ..., v_{j_r} >=< V_1, ..., v_m >= V$
Vediamo se $< V_{j_1}, ..., v_{j_r} >\subseteq< V_1, ..., v_m >$.
Quest'inclusione è ovvia (mmm, mica tanto ovvia!)
Vediamo ora l'inclusione opposta, cioè: $\forall i \ v_i \in< V_{j_1}, ..., v_{j_r} >$, cioè che ogni vettore è generato da $< V_{j_1}, ..., v_{j_r} >$.
Perchè questo sia vero occorre che $Mx = b$ abbia soluzione. $Mx = b$ ha soluzione se $b \in$ colonne di M $(V_{j_1}, ..., v_{j_r})$
Applichiamo quindi le stesso operazioni fatte su A per ottenere S sulla matrice $M|b$ con $b = v_i$.

$$(M|v_i) \xrightarrow{Gauss} S_0 = (V_{j_1}, ..., v_{j_r}|v_i)$$

e si nota facilmente che $rkM = rkS_o = r$ quindi genera. □

28 Domanda 50 - Inettività $\Leftrightarrow$ $ker = \{O\}$

Teorema. *L'applicazione lineare $f : X \to Y$ è iniettiva $\Leftrightarrow$ $Kerf = \{O\}$*

Dimostrazione. Dimostro $\Rightarrow$)
Supponiamo f iniettiva. Se $x \in Kerf$

$$f(x) = 0 = f(0) \Rightarrow x = 0$$

dunque $Kerf = 0$.
($f(0) = 0$ poichè l'applicazione è **lineare**, poichè avevamo supposto che fosse iniettiva possiamo dire che quella x che abbiamo preso è l'unica x che va in 0.)

Dimostro $\Leftarrow$)
Supponiamo che $Kerf = 0$

$$\begin{aligned} f(x) &= f(y) \\ f(x-y) &= 0 \\ \Rightarrow x - y &\in Kerf \\ x - y &= 0 \\ x &= y \end{aligned}$$

Dunque, essendo $x = y$ segue che f è iniettiva. □

29 Domanda 53 - Teorema della dimensione

Teorema (della dimensione)**.** *Sia F un'applicazione lineare da* $X \to Y$*.*
Dim Dom F= Dim Im F+ Dim Ker F

Dimostrazione. Sia $\{u_1, ..., u_r\}$ una base di $KerF$. La completo a base di X: $\{u_1, ..., u_r, v_{r+1}, ..., u_n\}$ {se $KerF = \{O\}$, prendiamo direttamente una base $\{v_1, ..., v_n\}$ di V, e consideriamo $r = 0$ ed $s = n$ nel seguito}. Poniamo $w_j = F(v_{r+j}) \in W$ per $j = 1, ..., s = n - r$; se dimostraimo che $F(u_i) = O$ per $i = 1, ..., r$) sappiamo già che B è un sistema di generatori di ImF; dobbiamo solo far vedere che $w_1, ..., w_s \in \mathbb{R}$ siano tali che

$$\alpha_1 w_1 + ... + \alpha_s w_s = O$$

Allora

$$O = \alpha_1 F(v_{r+1}) + ... + \alpha_s F(v_{r+s}) = F(\alpha_1 v_{r+1} + ... + \alpha_s v_{r+s})$$

per cui $\alpha_1 v_{r+1} + ... + \alpha_s v_{r+s} \in KerT$. Questo vuol dire che esistono $\beta_1, ..., \beta_r \in \mathbb{R}$ tali che $\alpha_1 v_{r+1} + ... + \alpha_s v_{r+s} = \beta_1 u_1 + ... + \beta_r u_r$; quindi

$$\beta_1 u_1 + ... + \beta_r u_r - a_1 v_{r+1} - ... - \alpha_s v_{r+s} = O$$

e l'indipendenza lineare di $\{u_1, ..., u_r, v_{r+1}, ..., v_{r+s}\}$ implica $\alpha_1 = ... = \alpha_s = 0$, come desiderato. □

30 Domanda 58 - Matrice associata e cambiamento di base

Matrice associata ad un'applicazione lineare

La matrice associata ad un applicazione lineare è una matrice che ha per colonne tutti i vettori della base dell'immagine dell'applicazione lineare. Formalmente:

Definizione. *Sia* $f : X \to Y$ *un'applicazione lineare. Sia* $\mathscr{B} = \{v_1, ..., v_n\}$ *una base di X.*
La matrice A associata all'applicazione lineare sarà così formata:

$$A = \begin{pmatrix} \begin{pmatrix} | \\ fv_1 \\ | \end{pmatrix} & \begin{pmatrix} | \\ fv_2 \\ | \end{pmatrix} & ... & \begin{pmatrix} | \\ fv_n \\ | \end{pmatrix} \end{pmatrix}$$

Cambiamento di base

Partiamo da un esempio esplicativo per capire il cambiamento di base:
Sia

$$B = \left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 5 \end{pmatrix} \right\}$$

e sia

$$C = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

Se volessi scrivere il vettore $\begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}$ come combinazione della base B dovrei scriverlo così:

$$\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}_B$$

mentre lo stesso vettore scritto rispetto alla base C lo scrivo così:

$$\begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}_C$$

Ora quindi ci serve solamente trovare un modo per fare questi passaggi più velocemente possibile. Poichè un'applicazione lineare è definita su una base, se io cambio la base cambio l'intera applicazione. Prendiamo la nostra matrice associata all'applicazione lineare

$$A = \left(\begin{pmatrix} | \\ fv_1 \\ | \end{pmatrix} \begin{pmatrix} | \\ fv_2 \\ | \end{pmatrix} \ldots \begin{pmatrix} | \\ fv_n \\ | \end{pmatrix} \right)$$

Per rendere A una matrice del cambiamento di base devo solamente riscrivere i suoi vettori nella nuova base, cioè:

$$A = \left(\begin{pmatrix} | \\ fv_1 \\ | \end{pmatrix}_{B_2} \begin{pmatrix} | \\ fv_2 \\ | \end{pmatrix}_{B_2} \ldots \begin{pmatrix} | \\ fv_n \\ | \end{pmatrix}_{B_2} \right)$$

Quindi avrò così ottenuto una matrice A' con i miei vettori della base B_1 in partenza e quelli della base B_2 in arrivo.
La matrice quindi cambia come cambiano i vettori in essa contenuti rispetto alla nuova base, cioè, al variare della base d'arrivo varieranno i vettori all'interno della matrice A.

31 L_A è invertibile $\Leftrightarrow$ A non è singolare

Definizione. *Una matrice A si dice singolare se $rkA = max$*

Teorema. *Data un'applicazione lineare L_A, quest'applicazione è invertibile $\Leftrightarrow$ la matrice A associata ad L_A è non singolare.*

Dimostrazione. L_A è invertibile $\Leftrightarrow$ è iniettiva e surgettiva $\Leftrightarrow$ L_A è surgettiva.

$$\Leftrightarrow ImL_A = \mathbb{K}^n$$

e sono uguali

$$\Leftrightarrow DimL_A = Dim\mathbb{K}^n = n \Rightarrow rkA = n$$

$\Rightarrow A$ non è singolare. $\square$