Stage Senior 2016 – Livello Advanced

Stampato integrale delle lezioni

Autori vari

Indice

Combinatoria 1 – Marco Trevisiol 4
Combinatoria 2 – Andrea Bianchi 19
Combinatoria 3 – Massimo Gobbino 33
Geometria 2 – Francesco Sala 46
Geometria 3 – Francesco Sala 60
Miscellanea 1 – Samuele Mongodi 72
Miscellanea 2 – Andrea Bianchi 88
Teoria dei Numeri 2 – Marco Trevisiol 97
Teoria dei Numeri 3 – Andrea Bianchi 118

C1 Advanced Tess

Note Title 9/2/2016

Funzioni generatrici

"funzioni generatrici ordinarie" ogf

Sono "scritture formali"

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots = \sum_{i=0}^{\infty} a_i x^i$$

Le ogf sono in corrispondenza con le successioni

$$f(x) \overset{\text{ogf}}{\longleftrightarrow} (a_i)_{i \in \mathbb{N}}$$

La x non ha alcun valore
la scrivo stare valutazioni di x

Operazioni con le ogf:

Somma $(a_i) \leftrightarrow a(x)$
$(b_i) \leftrightarrow b(x)$

$$(a+b)(x) := \sum_{i \geq 0} (a_i + b_i) x^i$$

Prodotto se ho $a(x)$ e $b(x)$

$$a(x) \cdot b(x) := \sum_i c_i x^i$$

$$c_i = \sum_{k=0}^{i} a_k b_{i-k}$$

$c_0 = a_0 b_0$

$c_1 = a_0 b_1 + a_1 b_0$

$\vdots$

$c_n = a_0 b_n + a_1 b_{n-1} + \dots + a_n b_0$

Inversa: se ho $f(x)$ chi è $f(x)^{-1}$

sarà una $g(x)$ t.c.

$$f(x) \cdot g(x) = 1 \quad \leftrightarrow \quad \begin{pmatrix} 1 \text{ se } i=0 \\ 0 \text{ se } i>0 \end{pmatrix} \; i \in \mathbb{N}$$

se $f(x) \leftrightarrow (f_i)$ ← li conosco

$g(x) \leftrightarrow (g_i)$ ← incognite

$$\begin{matrix} 1 \\ 0 \\ 0 \\ \vdots \end{matrix}$$

avrò

$[x^0]$ $f_0 \cdot g_0 = 1 \Rightarrow g_0 = \frac{1}{f_0}$ se $f_0 \neq 0$

$[x^1]$ $f_0 g_1 + f_1 g_0 = 0 \Rightarrow g_1 = -\frac{f_1}{f_0} g_0$

$\vdots$

$[x^n]$ $f_0 g_n + \dots + f_n g_0 = 0$

$\Rightarrow g_n = \frac{\dots}{f_0}$

$\vdots$

Posso invertire tutte le funzioni generatrici con termine noto $\neq 0$

Es: $f(x) = 1 - x \leftrightarrow (1, -1, 0, 0, \dots)$

$f^{-1}(x) = 1 + x + x^2 + x^3 + \dots \leftrightarrow (1, 1, \dots)$

Derivata: $f(x) \leftrightarrow (f_i)$

$f'(x) \leftrightarrow (f_{i+1}(i+1))$

$$\left(\sum_i f_i x^i\right)' = \sum_i (f_i \cdot i) x^{i-1}$$

$$= \sum_i f_{i+1}(i+1) x^i$$

Integrale: $\int f(x) \longleftrightarrow \left(\frac{f_{i-1}}{i-1} \text{ per } i \geq 1\right.$

il termine noto non è definito possiamo porlo $= 0$ $\left.\right)$

$$a_{n+1} = 2a_n + 1 \quad \forall n \geq 0 \qquad A(x) = \sum_n a_n x^n$$

$$\sum_n a_{n+1} x^n = \sum_n (2a_n + 1) x^n$$

$$\sum_n a_{n+1} x^n = 2\sum_n a_n x^n + \sum_n x^n$$

$$\frac{1}{x}(A(x) - a_0) \qquad A(x) \qquad (1-x)^{-1} = \frac{1}{1-x}$$

$$A(x) - a_0 = 2xA(x) + \frac{x}{1-x}$$

$$A(x) = \frac{a_0 + \frac{x}{1-x}}{1-2x}$$

$$= \frac{a_0(1-x) + x}{(1-x)(1-2x)} = \frac{\alpha_1}{1-x} + \frac{\alpha_2}{1-2x}$$

$$\frac{1}{1-2x} = \sum_n 2^n x^n$$

α_1 e α_2 risolvono un sistema 2x2

se moltiplico per $1-x$ e valuto in $x=1$

$$\frac{1}{1-2} = \alpha_1 + 0 \qquad \alpha_1 = -1$$

$$\alpha_2 = \dots$$

Allora $A(x) = \frac{\alpha_1}{1-x} + \frac{\alpha_2}{1-2x}$

$$= \sum_n (\alpha_1 + \alpha_2 2^n) x^n$$

$$a_n = \alpha_1 + \alpha_2 2^n$$

Un altro esempio: i Fibonacci

$$F_{n+2} = F_{n+1} + F_n \qquad F_0 = 0, \quad F_1 = 1$$

$$f(x) = \sum_n F_n x^n$$

$$\sum_n F_{n+2} x^{n+2} = \sum_n F_{n+1} x^{n+2} + \sum_n F_n x^{n+2}$$

$$(f(x) - 0 - x) = x(f(x) - 0) + x^2 f(x)$$

$$f(x) = \frac{x}{1-x-x^2} = \frac{\alpha_1}{1-r_1 x} + \frac{\alpha_2}{1-r_2 x}$$

con r_1^{-1} e r_2^{-1} radici di x^2+x-1

$$\Rightarrow F_n = (\alpha_1 r_1^n + \alpha_2 r_2^n)$$

ogf e binomiali:

$a_{k,n} = \binom{n}{k}$ $\qquad A_n(x) \longleftrightarrow (a_{k,n})_{k\in\mathbb{N}}$

$= \frac{n(n-1)\cdots(n-k+1)}{k!}$ $\qquad = (1+x)^n$

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

moltiplico per x^k e sommo su k

$$A_n(x) = A_{n-1}(x) + xA_{n-1}(x)$$
$$= (1+x)A_{n-1}(x)$$

ed è ovvio che $A_0(x) = 1$

$b_n = \binom{n}{k}$ $\qquad B_k(x) \longleftrightarrow (b_n)$

$$B_k(x) = \frac{x^k}{(1-x)^{k+1}}$$

Numeri di Stirling (del 2° tipo)

$$\left\{ {n \atop k} \right\} := \#\{\text{partizioni di } \{1,\dots,n\} \text{ in } k \text{ sottoinsiemi}\}$$

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\}$$

↑ l'n-esimo da solo

$$B_k(x) = \sum_n \left\{ n \atop k \right\} x^n$$

$$\sum_n \left\{ n \atop k \right\} x^n = \sum_n \left\{ n-1 \atop k-1 \right\} x^n + k \sum_n \left\{ n-1 \atop k \right\} x^n$$

$$kx \sum_n \left\{ n-1 \atop k \right\} x^{n-1}$$

$$B_k(x) = x B_{k-1}(x) + kx B_k(x)$$

$$B_k(x) = \frac{x}{1-kx} B_{k-1}(x)$$

$$B_k(x) = \frac{x^k}{(1-x)(1-2x)\cdot \ldots \cdot (1-kx)}$$

$$= \frac{\alpha_1}{1-x} + \ldots + \frac{\alpha_k}{1-kx} + C$$

$$\left\{ n \atop k \right\} = \sum_{i=1}^{k} \alpha_i \, i^n$$

- Sia a_n succ. t.c.

$$a_{n+2} - 1 = a_n + a_{n-1} + \ldots + a_0$$

$a_0 = 1, a_1 = 1$ chi è a_n? chi è $A(x)$?

- Sia b_n succ. t.c.

$b_0 = 1$ e $b_{n+1} = \sum_{i=0}^{n} b_i b_{n-i}$

chi è b_n? chi è $B(x)$?

Funzioni generatrici esponenziali "Egf"

$$(a_n) \xleftrightarrow{\text{Egf}} \sum_{n\geq 0} a_n \frac{x^n}{n!}$$

funziona tutto come prima tranne il prodotto

$$A(x)B(x) := \sum_{n\geq 0} c_n \frac{x^n}{n!}$$

però vale $\frac{c_n}{n!} = \sum_{k=0}^{n} \frac{a_k}{k!} \frac{b_{n-k}}{(n-k)!}$

$$\Rightarrow c_n = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}$$

Altre lievi differenze:

$$(1) \leftrightarrow \sum_{n\geq 0} \frac{x^n}{n!} =: e^x = \exp(x)$$

Oss: soddisfa $e^x \cdot e^y = e^{x+y}$

Esempio: permutazioni senza punti fissi

sia $d_n = \#$ perm. di n senza p.ti fissi.

vale che

$$n! = d_n + n d_{n-1} + \binom{n}{2} d_{n-2} + \dots + \binom{n}{n} d_0$$

$$n! = \sum_k \binom{n}{k} d_{n-k}$$

moltiplico per $\frac{x^n}{n!}$ e sommo su n

$$\frac{1}{1-x} = \sum_n x^n = \sum_k \binom{n}{k} d_{n-k} \frac{x^n}{n!}$$

$$\downarrow \Rightarrow D(x) \cdot e^x$$

$$D(x) := \sum_n \frac{d_n x^n}{n!}$$

$$\Rightarrow D(x) = \frac{e^{-x}}{1-x}$$

$$\Rightarrow \left[\frac{x^n}{n!}\right] D(x) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

Funzioni Generatrici di Dirichelet "Dsgf"

$$(a_n) \overset{\text{Dsgf}}{\longleftrightarrow} \sum_{n=1}^{\infty} \frac{a_n}{n^s} = A(s)$$

$$A(s) B(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s} = C(s) \quad \text{chi sono } c_n?$$

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} \cdot \sum_{n=1}^{\infty} \frac{b_n}{n^s} = \sum_{n=1}^{\infty} \frac{c_n}{n^s}$$

guardo il coefficiente di $\frac{1}{m^s}$

$$\sum_{\substack{d \mid m \\ d>0}} a_d \, b_{\frac{m}{d}} = c_m$$

Sia $f(n)$ una funzione moltiplicativa

$$Dsgf(f(n))(s) = \sum_n \frac{f(n)}{n^s}$$

$$= \prod_{p \text{ primo}} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots\right)$$

$\left[\frac{1}{n^s}\right]$: $f(n) = \prod_{p^k \| n} f(p^k)$ è vera per moltiplicatività

$$(1,1,1,\dots) \overset{Dsgf}{\longleftrightarrow} \sum_n \frac{1}{n^s} =: \zeta(s)$$

funzione di Moebius: $\mu : \mathbb{N} \to \mathbb{Z}$ moltiplicativa

$$\mu(1)=1, \quad \mu(p)=-1, \quad \mu(p^k)=0 \ \forall k>1 \ \forall_{p \text{ primo}}$$

$$Dsgf(\mu(n))(s) = \prod_{p \text{ primo}} \left(1 - \frac{1}{p^s}\right)$$

Vale che $\zeta^{-1}(s) = Dsgf(\mu(n))(s)$

Thm: (Formula di inversione di Moebius)

siano $(a_n), (b_n)$ succ. t.c.

$$b_n = \sum_{d \mid n} a_d$$

$$\Rightarrow a_n = \sum_{d \mid n} b_d \mu\left(\frac{n}{d}\right)$$

Dim: moltiplichiamo per $\frac{1}{n^s}$ e sommiamo su n

$$\sum_n \frac{b_n}{n^s} = \sum_n \left(\sum_{d \mid n} a_d \right) \frac{1}{n^s}$$

$$\| \qquad\qquad \|$$

$$B(s) \qquad A(s)\zeta(s)$$

$Dsgf$ (a_i) — $Dsgf$ $(1,1,\dots)$

Abbiamo ottenuto $B(s) = A(s)\zeta(s)$

$A(s) = B(s)\zeta^{-1}(s)$

guardo il coeff. di $\frac{1}{n^s}$: $a_n = \sum_{d \mid n} b_d \mu\left(\frac{n}{d}\right)$

Snake Oil Method

è un metodo per risolvere problemi come:

trovare una formula "esplicita" per

$$f(n) = \sum_k \binom{n+k}{2k} 2^{n-k}$$

dimostrare che $\forall\, m, n \geq 0$

$$\sum_k \binom{m}{k}\binom{n+k}{m} = \sum_k \binom{m}{k}\binom{n}{k} 2^k$$

Esempio 1

$$f(n) = \sum_{k \geq 0} \binom{k}{n-k} \qquad \text{per } n > 0$$

$$F(x) = \sum_n f(n)\, x^n = \sum_n \sum_{k>0} \binom{k}{n-k} x^n$$

$$= \sum_{k>0} \sum_n \binom{k}{n-k} x^n$$

$$= \sum_{k>0} x^k \underbrace{\sum_n \binom{k}{n-k} x^{n-k}}$$

CIP ALLE IMO

$$= (1+x)^k$$

$$F(x) = \sum_{k \geq 0} x^k (1+x)^k = \frac{x(1+x)}{1-x(1+x)} = \frac{x(1+x)}{1-x-x^2}$$

$$= -1 + \frac{1}{1-x-x^2}$$

---

altro esempio:

$$f(n) = \sum_k \binom{n+k}{2k} 2^{n-k} \qquad n \geq 0$$

$$\sum_n f(n) x^n = \sum_k \sum_n \binom{n+k}{2k} 2^{n-k} x^n$$

$$= \sum_k \frac{1}{2^k} \sum_n \binom{n+k}{2k} (2x)^n$$

$$= \sum_k \frac{1}{2^k} \frac{1}{(2x)^k} \sum_n \binom{n+k}{2k} (2x)^{n+k}$$

$$= \sum_k \frac{1}{(4x)^k} \frac{(2x)^{2k}}{(1-2x)^{2k+1}}$$

$$= \frac{1}{1-2x} \frac{1}{1 - \frac{x}{(1-2x)^2}}$$

$$= \frac{1}{(1-2x) - \frac{x}{1-2x}}$$

$$= \frac{1-2x}{(1-2x)^2 - x} = \frac{1-2x}{1-5x+4x^2}$$

$$f(n) = \alpha_1 r_1^n + \alpha_2 r_2^n = \frac{\alpha_1}{1-x} + \frac{\alpha_2}{1-4x}$$

$$r_1 = 1 \quad r_2 = 4$$

$$a(n,m) = \sum_k \binom{m}{k}\binom{n+k}{m}$$

$$b(n,m) = \sum_k \binom{m}{k}\binom{n}{k} 2^k$$

$$\sum_n \sum_m a(n,m)\, x^n y^m = A(x,y)$$

$$= \sum_n \sum_m \sum_k \binom{m}{k}\binom{n+k}{m} x^n y^m$$

$$= \sum_k \sum_m \binom{m}{k} y^m \sum_n \binom{n+k}{m} x^n$$

$$= \sum_k x^{-k} \sum_m \binom{m}{k} y^m \underbrace{\sum_n \binom{n+k}{m} x^{n+k}}$$

$$= \frac{x^m}{(1-x)^{m+1}}$$

$$= \sum_k \frac{x^{-k}}{1-x} \sum_m \binom{m}{k} \left(\frac{yx}{1-x}\right)^m$$

$$= \sum_k \frac{x^{-k}}{1-x} \frac{\left(\frac{yx}{1-x}\right)^k}{\left(1-\frac{yx}{1-x}\right)^{k+1}}$$

$$= \frac{1}{1-x} \frac{1}{1-\frac{yx}{1-x}} \frac{1}{1-\frac{\frac{y}{1-x}}{1-\frac{yx}{1-x}}} = A(x,y)$$

Esercizi assegnati

[Egf]

Calcolare il # di permutazioni su n elementi con ordine ≤ 2

$$\left[Egf(p_n) = e^{\frac{x^2}{2}+x} \right]$$

Calcolare il # di permutazioni su n elementi con solo cicli di ordine $1,3,7$

$$\left[Egf(p_n) \overset{?}{=} e^{\frac{x^2}{2!}+\frac{x^3}{3!}+x} \right]$$

[Dsgf]

Calcolare il # di stringhe di 0,1 con n lettere che non siano ripetizione di una sottostringa

(es: 100100100 NO, 100100101 SÌ)

$$\left[\prod_{\substack{p \text{ primo} \\ p^k \| n}} \left(2^{p^k} - 2^{p^{k-1}}\right) \right]$$

Calcolare $\varphi(n)$ e $Dsgf(\varphi(n))$

$$\left[Dsgf(\varphi(n))(s) = \zeta(s-1) \right]$$

Esprimere $\Phi_n(x)$ come frazione di polinomi del tipo $(1-x^m)$

[Snake Oil Method]

Dimostrare che $\sum_m \binom{r}{m}\binom{s}{t-m} = \binom{r+s}{t}$

calcolare di conseguenza $\sum_i \binom{n}{i}^2$, $\sum_i \binom{n}{i}\binom{2n}{n-i}$

Dimostrare che $\sum_k \binom{2n+1}{2k}\binom{m+k}{2n} = \binom{2m+1}{2n}$

Calcolare $\sum_{i=1}^{n} \binom{n+i-1}{2i-1}$ [F_{2n}]

Mostrare che $\sum_k (-1)^{n-k}\binom{2n}{k}^2 = \binom{2n}{n}$

[hint: mostrare un'identità più generale che contenga più variabili libere, quindi: S.O.M., quindi specializzare l'identità ottenuta]

Senior 2016 - C2 Advanced (Anér)

Note Title 9/3/2016

Spazio di probabilità: insieme (finito) Ω non vuoto + una funzione $P : \Omega \to [0,1]$ con la proprietà $\sum_{\omega \in \Omega} P(\omega) = 1$

Per ogni $S \subseteq \Omega$ definiamo $P(S) = \sum_{\omega \in S} P(S)$

Una variabile aleatoria è una funzione

$$X : \Omega \to \mathbb{R}$$

Il valore atteso, o valor medio, o speranza di X è

$$\mathbb{E}[X] = \sum_{\omega \in \Omega} P(\omega) \cdot X(\omega)$$

LINEARITÀ DI $\mathbb{E}$

Se ho due variabili aleatorie X e Y, e se $\lambda \in \mathbb{R}$, allora

$$\mathbb{E}[X + \lambda \cdot Y] = \mathbb{E}[X] + \lambda \cdot \mathbb{E}[Y]$$

Due eventi (sottoinsiemi di Ω) A e B si dicono indipendenti se

$$P(A \cap B) = P(A) \cdot P(B)$$

(In particolare $\emptyset$ e Ω sono indipendenti da ogni altro evento)

Due variabili X e $Y : \Omega \to \mathbb{R}$ sono indipendenti se per ogni $\lambda, \mu \in \mathbb{R}$

$$P\left(X^{-1}(\lambda) \cap Y^{-1}(\mu)\right) = P\left(X^{-1}(\lambda)\right) \cdot P\left(Y^{-1}(\mu)\right)$$

Teo Se X e Y sono v.a. indip., allora

$$\mathbb{E}[X \cdot Y] = \mathbb{E}[X] \cdot \mathbb{E}[Y]$$

DIM $LHS = \sum_{\omega \in \Omega} P(\omega) \cdot X(\omega) \cdot Y(\omega) =$

$$= \sum_{\substack{\lambda \in \mathrm{Im}\, X \\ \mu \in \mathrm{Im}\, Y}} \sum_{\substack{\omega \in \Omega : X(\omega) = \lambda \\ Y(\omega) = \mu}} P(\omega) \cdot \lambda \cdot \mu =$$

$$= \sum_{\substack{\lambda \in \mathrm{Im}\, X \\ \mu \in \mathrm{Im}\, Y}} \lambda \cdot \mu \cdot P\left(X^{-1}(\lambda) \cap Y^{-1}(\mu)\right) = \overset{X \text{ e } Y \text{ sono indipendenti}}{}$$

$$= \sum_{\substack{\lambda \in \mathrm{Im}\, X \\ \mu \in \mathrm{Im}\, Y}} \lambda \cdot \mu \cdot P\left(X^{-1}(\lambda)\right) \cdot P\left(Y^{-1}(\mu)\right) =$$

$$= \left(\sum_{\lambda \in \mathrm{Im}\, X} \lambda \cdot P\left(X^{-1}(\lambda)\right) \right) \left(\sum_{\mu \in \mathrm{Im}\, Y} \mu \cdot P\left(Y^{-1}(\mu)\right) \right) =$$

$$= \mathbb{E}[X] \cdot \mathbb{E}[Y]$$

Disuguaglianza di Markov

Se X ha valori ≥ 0 e $k > 0$ è un numero reale

allora $$\mathbb{P}(X \geq k) \leq \frac{\mathbb{E}[X]}{k}$$

dove $\mathbb{P}(\text{proposizione}) = \mathbb{P}(\text{evento per cui la prop. è vera})$

DIM $$k \cdot \mathbb{P}(X \geq k) \overset{?}{\leq} \mathbb{E}[X]$$

$$\mathbb{E}[X] = \sum_{\omega : X(\omega) \geq k} \mathbb{P}(\omega) \cdot X(\omega) + \sum_{\omega : X(\omega) < k} \mathbb{P}(\omega) \cdot X(\omega)$$

$$\geq k \cdot \mathbb{P}(X \geq k) + 0$$

Caso particolare X è a valori naturali

allora $$\mathbb{P}(X > 0) \leq \mathbb{E}[X]$$

Dadi a due facce (monete)

Ho n monete con facce segnate come $+1$ e -1.
Se le lancio tutte, ho 2^n possibili esiti. I lanci sono indipendenti, ossia eventi del tipo

$\{$ la i-esima moneta dà $+1\}$ e
$\{$ la j-esima moneta dà $-1\}$ sono indipendenti per $i \neq j$

Considero il prodotto degli esiti delle monete

(ossia la parità del numero di -1)

$X_i : \Omega \to \{\pm 1\}$ la variabile "esito della i-esima moneta"

$\prod_{i=1}^{n} X_i : \Omega \to \{\pm 1\}$

Supponiamo che $\prod X_i$ sia bilanciata (ossia assume con prob. $\frac{1}{2}$ il val. $+1$ e con $\frac{1}{2}$ il val. -1)

Tesi: Una delle monete è bilanciata.

DIM Consideriamo $\mathbb{E}\left[\prod X_i\right] = \prod \mathbb{E}[X_i]$ (perché le X_i sono indip.)

$\frac{1}{2}\cdot(+1) + \frac{1}{2}(-1) = 0$

c'è un $\mathbb{E}[X_i]$ nullo $\Rightarrow$ quella moneta è bilanciata

---

Monete a tre facce (cilindriche?)

Le facce sono contrassegnate dai numeri $1, 2, 3$; le monete sono n e sono indip. Le lanciamo tutte e sommiamo i risultati mod 3.

Supponiamo che la somma assuma con prob. $\frac{1}{3}$ ognuna delle 3 classi mod 3.

Tesi: Una delle monete è "bilanciata", cioè assume i valori $1, 2, 3$ equiprobabilmente.

Estendiamo il concetto di var. al., introducendo le var. al. complesse. $X_i : \Omega \to \mathbb{C}$.

X_i vale 1 se esce 3 sulla i-esima moneta

ζ		1	
ζ^2		2	

ove ζ è una radice cubica primitiva di 1 in $\mathbb{C}$.

Il valore atteso è definito come prima (e ha le stesse proprietà di prima)

Ora $\mathbb{E}\left[\prod X\right] = \prod \mathbb{E}[X_i]$ (implic. delle X_i)

$\| 0$

$$0 = \frac{1}{3}\cdot 1 + \frac{1}{3}\cdot\zeta + \frac{1}{3}\cdot\zeta^2$$

Quindi c'è un X_i per cui $\mathbb{E}[X_i] = 0$

$$P(X_i=1)\cdot\zeta + P(X_i=2)\cdot\zeta^2 + P(X_i=3)\cdot 1 = 0$$

questi sono uguali, altrimenti la parte immaginaria della somma è non nulla.

moltiplicando per ζ e ripplico il ragionamento.

OSS: Da 4 in su l'analogo problema non ha la stessa risposta.

ogf di una variabile aleatoria

$X : \Omega \to \mathbb{R}$

$$\mathrm{ogf}(X) = \sum_{w\in\Omega} P(w)\cdot x^{X(w)}$$

vive nel mondo delle somme di famiglie sommabili di potenze formali di x con esponente reale

(Se X ha valori naturali, allora viene un polinomio)

oss Se X e Y sono indipendenti, allora

$$ogf(X+Y) = ogf(X) \cdot ogf(Y)$$

(verificare...)

GRAFI ALEATORI | Prendiamo n vertici e per ogni coppia di essi scegliamo se collegarli con un arco o no. Ci sono $2^{\binom{n}{2}}$ possibilità, che costituiscono l'insieme degli esiti Ω.

Fissiamo $p \in [0,1]$ e inseriamo ogni arco, indipendentemente dagli altri con probabilità p.

$$P\left(\text{grafo } G = (\{1,\dots n\}, E)\right) = p^{|E|} \cdot (1-p)^{\binom{n}{2} - |E|}$$

Stima dal basso dei numeri di Ramsey

Ricordo Dato $k \geq 0$ naturale, se considero un grafo su N vertici, con N abbastanza grande, questo contiene sicuramente una k-cricca o una k-anticricca.

Basta $N = \binom{2k}{k}$. Il minimo N per cui ogni N-grafo ha una k-cricca o una k-anticricca si chiama $R(k,k)$.

$R(3,3) = 6$ $\quad R(4,4) = 17$ $\quad R(5,5) = ?$

Quanto in fretta cresce? $\binom{2k}{k} = \frac{(2k)!}{k! \cdot k!} \simeq$

$$\simeq \frac{\left(\frac{2k}{e}\right)^{2k} \cdot \sqrt{2\pi \cdot 2k}}{\left[\left(\frac{k}{e}\right)^{k} \cdot \sqrt{2\pi k}\right]^2} \simeq \frac{2^{2k}}{\sqrt{\pi k}} = \frac{4^k}{\sqrt{\pi k}}$$

$$\text{quindi } \sim \left(\sqrt{2}\right)^k \leq R(k,k) \leq \binom{2k}{k} \simeq \frac{4^k}{\sqrt{\pi k}}$$

Per studiare il lower bound, cerchiamo N il più grande possibile, per cui riusciamo a trovare almeno un N-grafo senza k-cricche o k-anticricche.

Prendiamo $p = \frac{1}{2}$ e consideriamo un N-grafo aleatorio.

$\mathbb{P}(\text{esiste una } k\text{-cricca}) = ?$

$X_c = n^\circ$ di k-cricche in un grafo - (v. a. a valori in $\mathbb{N}$)

$$\mathbb{P}(X_c \geq 1) \overset{\text{Markov}}{\leq} \mathbb{E}[X_c]$$

per ogni sottoinsieme $S \subseteq \{1, \dots N\}$, con $|S| = k$

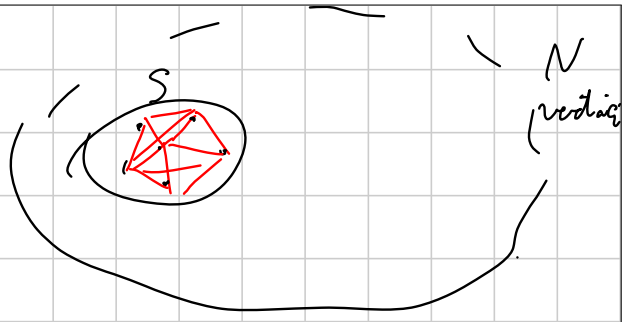
definisco la v. a. $X_c^S = \begin{cases} 0 \text{ se } S \text{ non è una } k\text{-cricca} \\ 1 \text{ se } S \text{ è una } k\text{-cricca} \end{cases}$

$$X_c = \sum_{\substack{S \subseteq \{1,\dots N\} \\ |S| = k}} X_c^S \qquad \mathbb{E}[X_c] = \sum \mathbb{E}[X_c^S] = \binom{N}{k} \cdot \mathbb{E}[X_c^{\bar{S}}]$$

dove $\bar{S}$ è un sottoinsieme scelto $\subseteq \{1, \dots N\}$

$$\mathbb{E}\left[X_c^S\right] = \left(\frac{1}{2}\right)^{\binom{k}{2}}$$

$$\mathbb{E}[X_c] = \binom{N}{k} \cdot \left(\frac{1}{2}\right)^{\binom{k}{2}}$$



$\forall$

$P(\text{esiste una } k\text{-cricca})$

X_a = n° di k-anticricche nel grafo aleatorio

$$P(\text{esista una } k\text{-anticricca}) \leq \binom{N}{k} \cdot \left(\frac{1}{2}\right)^{\binom{k}{2}}$$

$$P(\text{esista una } k\text{-cricca o una } k\text{-anticricca}) \leq 2 \cdot \binom{N}{k} \cdot \left(\frac{1}{2}\right)^{\binom{k}{2}}$$

se scegliamo N il più grande possibile per cui questo numero è < 1, allora esistono N-grafi senza cricche o anticricche

$$2 \cdot \binom{N}{k} \left(\frac{1}{2}\right)^{\binom{k}{2}} < 2 \cdot \frac{N^k}{k!} \cdot \left(\frac{1}{2}\right)^{\binom{k}{2}} \overset{?}{<} 1$$

$$\text{Se } N < \sqrt[k]{2^{\binom{k}{2}-1} \cdot k!} = \frac{1}{\sqrt[k]{2}} \cdot \sqrt[k]{2^{k \cdot \frac{k-1}{2}}} \cdot \sqrt[k]{k!}$$

qui stiamo buoni

$$< 1 \cdot \sqrt{2}^{(k-1)} \cdot \sqrt[k]{k!} \simeq \sqrt{2}^{k-1} \cdot \sqrt[k]{\left(\frac{k}{e}\right)^k \cdot \sqrt{2\pi k}}$$

$$\simeq \sqrt{2}^{k-1} \cdot \frac{k}{e} \cdot 1$$

$$\text{Se } N < \sqrt[k]{2^{\binom{k}{2}-1} \cdot k!} \simeq \frac{1}{\sqrt[n]{2}} \cdot \sqrt{2}^{(k-1)} \cdot \frac{k}{e} \cdot \sqrt[2k]{2\pi k}$$

allora ho un grafo senza k-cricche né k-anticricche

Teo (Erdős) Dati k, l naturali, esistono dei grafi (su un numero opportuno di vertici) senza cicli di lunghezza $< l$, ma privi di una k-colorazione dei vertici.

Def Dato un grafo G, una k-colorazione dei vertici è una partizione dei vertici in k sottoinsiemi per cui 2 vertici nello stesso sottoinsieme non sono collegati da un arco.

Def $\chi(G)$ numero cromatico di un grafo G = min k per cui G ha una k-colorazione

Def $\alpha(G)$ è la massima dimensione di una anticricca in G.

Lemma $\chi(G) \geq \dfrac{|G|}{\alpha(G)}$. Infatti se avessi $\alpha(G) \cdot \chi(G) < |G|$, allora colorando G con $\chi(G)$ colori, almeno un colore ha più di $\alpha(G)$ vertici, assurdo.

1° STRATEGIA
Cerchiamo grafi con α piccolo e senza cicli $< l$.
2° STRATEGIA
Cerchiamo grafi con α piccolo e pochi cicli $< l$
(visto che è un conto lungo, mettiamo da parte un attimo)

Turán Dato un grafo G su N vertici, con $|E|$ archi, quanto vale almeno $\alpha(G)$?

Idea Estraiamo "casualmente" una anticricca da G e vediamo in media quanto è grande.

1) Ordiniamo i vertici casualmente secondo le $N!$ possibili permutazioni, ognuna con probabilità $\frac{1}{N!}$.

2) Consideriamo uno alla volta i vertici $v_1, v_2, \dots v_N$. Mettiamo il vertice v_i nella anticricca se non è collegato ad alcun vertice già messo nell'anticricca, altrimenti lasciamo v_i da parte.

3) Alla fine avrò un'anticricca

Per ogni v vertice, definisco la variabile

$$X_v = \begin{cases} 0 & \text{se } v \text{ viene scartato dall'algoritmo} \\ 1 & \text{se } v \text{ viene selezionato nell'anticricca} \end{cases}$$

$$\mathbb{E}\left[\text{dim. dell'anticricca}\right] = \sum_{v \in G} \mathbb{E}\left[X_v\right]$$

Dato $v \in G$, quanto vale $\mathbb{E}[X_v]$?

$$\mathbb{E}[X_v] = P(X_v = 1) \geq P(v \text{ viene prima dei suoi vicini}) \geq \frac{1}{\deg(v)+1}$$

$\mathbb{E}[\text{dim dell'antic.}] \geq \sum_{v \in G} \frac{1}{\deg(v)+1} \geq$

$\left(\frac{1}{x+1} \text{ è convessa su } [0,\infty)\right)$

$\geq N \cdot \frac{1}{\frac{2|E|}{N}+1} = \frac{N}{\frac{2|E|}{N}+1}$

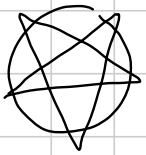
Quindi $\alpha(G) \geq \frac{N}{\frac{2|E|}{N}+1}$

(Trovare un esempio in cui valga l'uguaglianza...)

TARINI ORO

ALICE 101 IPHONE, MP3, MYPC, 1LO, 1BO, 1AO, 10AA

Achtung!



PUBBLICITÀ

Prendiamo un grafo aleatorio su N vertici, ma stavolta prendiamo ogni arco con probabilità p (che sceglieremo dopo $p = N^{-1+\frac{1}{l}}$).

Consideriamo la variabile aleatoria per $3 \le i \le \ell - 1$

$X_i = $ n° di cicli di lunghezza i nel grafo

$X = \sum_{i=3}^{\ell-1} X_i$ $\qquad P(X \ge \text{qualcosa}) \overset{\text{Markov}}{\le} \frac{\mathbb{E}[X]}{\text{qualcosa}}$

$$\mathbb{E}[X] = \sum_{i=3}^{\ell-1} \mathbb{E}[X_i] = \sum_{i=3}^{\ell-1} \frac{\binom{N}{i} \cdot (i-1)!}{2} \cdot p^i <$$

$$< \sum_{i=3}^{\ell-1} \frac{N^i}{2i} \cdot p^i < \sum_{i=3}^{\ell-1} (Np)^i < \sum_{i=0}^{\ell-1} (Np)^i < \frac{(Np)^\ell}{Np - 1}$$

$$\overset{?}{<} \frac{N}{1000}$$

$p = \frac{N^{\frac{1}{\ell}}}{N} \Rightarrow \frac{N}{N^{\frac{1}{\ell}} - 1} < \frac{N}{1000}$ per N grande

Se N è grande, $\mathbb{E}[X] < \frac{N}{1000}$

Markov: $P\left(X > \frac{N}{2}\right) \le \frac{\mathbb{E}[X]}{N/2} \le \frac{1}{500}$

Quindi è altamente improbabile che ci siano più di $N/2$ cicli di lunghezza $< \ell$.

$m = \left\lfloor N^{1 - \frac{1}{2\ell}} \right\rfloor$ $\qquad \mathbb{P}(\alpha(G) < m)$

$\mathbb{P}(\text{non esistono } m\text{-anticicli})$.

$Y = $ n° di m-anticicli nel grafo aleatorio.

$$\mathbb{E}[Y] = \binom{N}{m} (1-p)^{\binom{m}{2}} \le \frac{N^m}{m!} \cdot (1-p)^{\binom{m}{2}}$$

$$\mathbb{P}(Y \geq 1) \leq \frac{N^m}{\left(\frac{m}{e}\right)^m} (1-p)^{m \cdot \frac{m-1}{2}} =$$

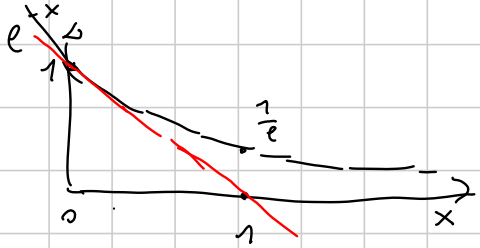
$$= \left[\frac{eN}{m} \cdot (1-p)^{\frac{m-1}{2}} \right]^m <$$

$$< \left[\frac{eN}{N^{1-\frac{1}{2\ell}}} e^{-p\frac{m}{2}} \right]^m$$

$$\left[e \cdot N^{\frac{1}{2\ell}} \cdot e^{-N^{-1+\frac{1}{\ell}+1-\frac{1}{2\ell}}} \right]^m$$

$$\left[N^{\frac{1}{2\ell}} \cdot e^{-\frac{N^{\frac{1}{2\ell}}}{2}+1} \right]^m < \frac{1}{500} \quad \text{per } N \text{ grande}$$

$1-p < e^{-p}$



$$\mathbb{P}(\alpha(G) \geq m) < \frac{1}{500} \qquad \mathbb{P}\left(X > \frac{N}{2}\right) < \frac{1}{500}$$

$$\Rightarrow \mathbb{P}\left(\alpha(G) \geq m \text{ oppure } X > \frac{N}{2}\right) < \frac{1}{250}$$

Esiste, per N grande, un N-grafo con $\alpha < m$ e $X \leq \frac{N}{2}$. O.d. ogni ciclo $< \ell$ associo un suo vertice e tolgo tutti vertici dal grafo. Rimane un grafo con almeno $\frac{N}{2}$ vertici e senza cicli brevi

e con una $\alpha \leq m$

$$\chi(\text{nuovo grafo}) \geq \frac{N/2}{m} \simeq \frac{N^{\frac{1}{2k}}}{2} > k$$

per N abbastanza grande

SENIOR 2016 – Double Counting & Probabilistic Method

Note Title 06/09/2016

http://www.artofproblemsolving.com/community/c2335h1038680

Problem 2: In the Duma, there are 1600 delegates who have formed 16000 committees of 80 persons each. Prove that one can find two committees having at least four common members.

Source: Russian 1996

Idea: scegliendo a caso due commissioni, queste hanno IN MEDIA almeno 4 persone in comune (in realtà basta 3.00001...)

Formalizzazione: fare un DOUBLE COUNTING

$X = \{(C_1, C_2, p) : C_1 \text{ e } C_2 \text{ sono commissioni}$
$p \text{ parlamentare che sta in } C_1 \text{ e } C_2\}$

Contiamo in 2 modi gli elementi di X. Supponiamo per assurdo che due commissioni abbiano max 3 persone in comune

(C_1, C_2) – WISE : $|X| = \sum_{(C_1,C_2)} \overbrace{\text{persone comuni a } C_1 \text{ e } C_2}^{\leq 3}$

$\leq 3 \cdot \#(C_1, C_2) = 3 \binom{16.000}{2}$

p – WISE : $|X| = \sum_p$ coppie comun. che contengono p

$= \sum_p \binom{C(p)}{2}$ $\quad C(p) = \#$ commissioni in cui sta p

$= \frac{1}{2} \sum_p C(p)^2 - C(p)$

$= \frac{1}{2} \sum_p C(p)^2 - \frac{1}{2} \sum_p C(p) \geq \frac{1}{2} \frac{(\sum C(p))^2}{\#p} - \frac{1}{2} \ldots$

Ora $\sum_p C(p) = 80 \cdot 16.000$

$Y = \{ (c,p) : p \in c \}$

p-wise: $|Y| = \sum_p c(p)$

c-wise: $|Y| = \sum_c 80 = 80 \cdot \#\text{comm} = 80 \cdot 16.000$

Concludendo troviamo

$$3\binom{16.000}{2} \geq |X| \geq \frac{1}{2}\frac{1}{1.600}(80 \cdot 16.000)^2 - \frac{1}{2}\,80 \times 16.000$$

Sviluppando il conto trovo un assurdo! ☺

—o—o—

Alternativa: invece dell'assurdo, pone $k = \max$ #persone comuni e scrivere

$$k\binom{16.000}{2} \geq \text{RHS}$$ e sperare di ottenere $k \geq 3,0000\,1$

—o—o—

Problem 3: In an $n\times n$ array, each of the numbers $1, 2, ..., n$ appears exactly n times. Show that there is a row or a column in the array with at least $\sqrt{n}$ distinct numbers.

Source: MOP 2007

$X_R = \{ (R,k) :$ numero k compare nella riga $R \}$
$X_c = \{ (c,k) :$ " " colonna $c \}$

Supponiamo per assurdo che ogni riga o col. ha meno di $\sqrt{n}$ numeri distinti

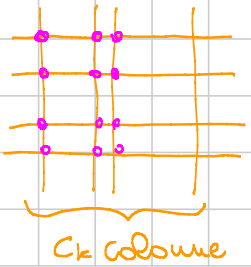
R-wise: $|X_R| = \sum_R \text{numeri}(R) < \sqrt{n}(\#\text{Righe}) = n\sqrt{n}$

$|X_c| < n\sqrt{n}$

$|X_R \cup X_c| < 2n\sqrt{n}$

k-wise: $|X_R \cup X_C| = \sum_k (R(k) + C(k)) \geq \sum_k 2\sqrt{R(k)C(k)}$ ...

$R(k)$ righe in cui appare il numero k



C_k colonne

$R(k) \cdot C(k) \geq n$

ogni numero k appare n volte

... $|X_R \cup X_C| \geq \sum_k 2\sqrt{n} = 2\sqrt{n}(\#k) = 2n\sqrt{n}$

Mettendo insieme $2n\sqrt{n} < 2n\sqrt{n}$ assurdo.

— o — o —

Problem 4: Suppose 799 teams participate in a tournament in which every pair of teams plays against each other exactly once. Prove that there two disjoint groups A and B of 7 teams each such that every team from A defeated every team from B.

Source: Iran TST 2008

$X = \{(A, p) : |A| = 7,\ p \text{ batte tutti i componenti di } A\}$

Ipotesi di assurdo: ogni A è associato al max a 6 persone

A-wise: $|X| \leq 6 \cdot (\#A) = 6 \cdot \binom{799}{7}$

p-wise: $|X| = \sum_p \binom{V(p)}{7}$ ← vittorie di p

$\sum_p V(p) = \#\text{partite} = \binom{799}{2}$

Speriamo che la somma di $\binom{V(p)}{7}$ sia minima quando i $V(p)$ sono tutti uguali, cioè

$V(p) = \frac{1}{799} \cdot \frac{799 \cdot 798}{2} = 399$

Se fosse così concluderei

$$799 \cdot \binom{399}{7} \leq |X| \leq 6 \cdot \binom{799}{7}$$

e questa dovrebbe essere assurda

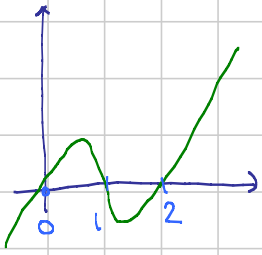
$$799 \cdot \frac{399 \cdot 398 \cdot \ldots \cdot 393}{7!} > 6 \frac{799 \cdot \ldots \cdot 793}{7!}$$

$$\frac{799}{6} > \frac{799}{399} \cdot \ldots \cdot \frac{793}{393}$$

VERA, ma non si verifica con il 2^7 ...

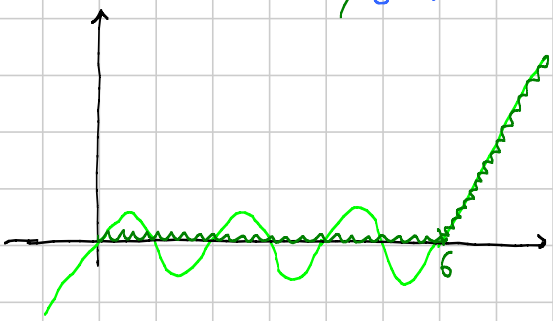
Oss. Tutto sta a dim. una specie di "convessità" del binomiale

$$\binom{x}{2} = \frac{x(x-1)}{2} \qquad \binom{x}{3} = \frac{1}{6} x(x-1)(x-2)$$



Quando facciamo $\sum \binom{v(p)}{7}$ stiamo facendo

$\sum f(v(p))$ dove



quindi basta per $x \geq 6$ e questo si può fare per induzione con la derivata 2ª

$f_k(x) = x f_{k-1}(x-1)$ ↑ a meno di un coeff.

e ora calcolo la derivata 2ª o uso prodotto di funzioni convesse, positive crescenti.

—o— o —

Problem 7 (IMO 1998 [8])
In a competition, there are a contestants and b judges, where b≥3 is an odd integer. Each judge rates each contestant as either"pass" or "fail". Suppose k is a number such that, for any two judges, their ratings coincide for at most k contestants. Prove that

k/a≥(b−1)/(2b).

$X = \{ (g_1, g_2, c) : g_1 \text{ e } g_2 \text{ sono giudici che sono d'accordo sul contestant } c \}$

(g_1, g_2) wise : $|X| = \sum_{(g_1,g_2)} \underbrace{\text{agreement}(g_1,g_2)}_{\leq k}$

$\leq k \, \#(g_1, g_2)$

$= k \binom{b}{2}$

c-wise: $|X| = \sum_c$ giudici d'accordo (c)

$= \sum_c \binom{S(c)}{2} + \binom{P(c)}{2}$ ← giudici che promuovono c

↑ giudici che segano c

$S(c) + P(c) = b$

$\left[\geq \sum_c 2 \binom{b/2}{2} \right]$ Essendo b dispari non è ottimale

$\geq \sum_c \underbrace{\binom{\frac{b+1}{2}}{2} + \binom{\frac{b-1}{2}}{2}}$

↑ questo conto algebrico va giustificato (QM-AM) con il vincolo che sono interi.

Sviluppando tutto viene ...

— o — o —

http://cdn.artofproblemsolving.com/aops20/attachments/probability_problems_306.pdf

Problem 3 (IMO 1987 [8]) Let $p_n(k)$ be the number of permutations of the set $\{1, \ldots, n\}$, $n \geq 1$, which have exactly k fixed points. Prove that

$$\sum_{k=0}^{n} k p_n(k) = n!.$$

(Remark: A permutation f of a set S is a one-to-one mapping of S onto itself. An element i in S is called a fixed point of the permutation f if $f(i) = i$.)

1° modo C'è una formula per $p_n(k)$ con dentro una sommatoria, e riorganizzando i termini DOVREBBE venire.

2° modo $X = \{(\sigma, x) : \sigma \text{ permut. e } \sigma(x) = x\}$

σ-wise : $|X| = \sum_{\sigma} Fix(\sigma) = \sum_{k=0}^{n} k\, p_n(k)$

x-wise : $|X| = \sum_{x} Fix(x) = n \cdot (n-1)! = n!$

$Fix(x)$: permutazioni che fissano x

Problem 1 (IMC for University Students 2002 [5]) Two hundred students participated in a mathematical contest. They had 6 problems to solve. It is known that each problem was correctly solved by at least 120 participants. Prove that there must be two participants such that every problem was solved by at least one of these two students.

$X = \{(p, c_1, c_2) : p \text{ è stato risolto da } c_1 \text{ o } c_2\}$

Supponiamo la tesi falsa. Allora

(c_1, c_2)-wise : $|X| = \sum_{(c_1, c_2)} \text{problemi } (c_1, c_2) \leq 5\,(\#\, c_1, c_2)$

problemi (c_1, c_2): risolti da almeno uno dei due

$= 5 \cdot \binom{200}{2}$

p-wise : $|X| = \sum_{p} \text{Coppie}(p) \geq$

Coppie (p): coppie in cui almeno uno ha risolto p

$\text{Coppie}(p) \geq \binom{200}{2} - \binom{80}{2}$

coppie tot; ↑ entrambi non hanno risolto

$$5\binom{200}{2} \geq |X| \geq 6\left[\binom{200}{2} - \binom{80}{2}\right]$$

Spero che sia assurda: $6\binom{80}{2} < \binom{200}{2}$ VERA?

$$6\,\frac{80\cdot 79}{2} < \frac{200\cdot 199}{2}$$ ok di poco

— o — o —

Oss. Forse conveniva contare

$X = \{(c_1, c_2, p) : c_1 \text{ e } c_2 \text{ non hanno risolto } p\}$

Problem 2 (IMO Shortlist 1987 [8]) Show that we can color the elements of the set $\{1, 2, \ldots, 1987\}$ with 4 colors so that any arithmetic progression of ten terms, each in the set, is not monochromatic.

$X = \{(C, p) : p \text{ è una progressione di 10 termini monocromatica per la colorazione } C\}$

Ipotesi di assurdo: $\forall C$ colorazione $\exists p$ progressione

C-wise $\quad |X| = \sum_c \text{monocrom}(c) \geq \#C = 4^{1987}$

p-wise $\quad |X| = \sum_p \underbrace{\text{Colorazioni che rendono } p \text{ monocrom}}_{4\cdot 4^{1977}}$

4 colore per p

$$= 4^{1978}\cdot(\#p)$$

Quindi ottengo $4^{1978}\cdot(\#p) \geq 4^{1987}$, cioè $(\#p) \geq 4^9$

Idee per contare $\#p$

→ fisso il 1° e vedo quante ragioni posso permettermi

→ fisso la ragione e vedo quanti inizi vanno bene

→ fisso il 1° e l'ultimo in una opportuna classe mod 9.

Idea probabilistica che sta sotto:

$\frac{1}{4^9}$ è la prob. che una progressione colorata a caso sia monocroma.
Moltiplico per il numero di progressioni (sfruttando un po' di linearità) e ottengo che la prob. di avere una monocromatica è < 1 (il numero medio di progr. monocrom è <1, quindi...)

Problem 17 (Szele 1943 [1, Chap. 2]) In a (round-robin) *tournament*, every player plays one game with every other player. A *Hamiltonian path* of the tournament is an ordering of the players from left to right so that every player (except the last) beat the player immediately to its right. Let n be a positive integer. Show that there is a tournament with n players that has at least $n!/2^{n-1}$ Hamiltonian paths.

$X = \{(G, c) : \text{il cammino } c \text{ è Ham. nel grafo } G\}$

Ipotesi di assurdo: $\forall G$ grafo, i cammini $< \frac{n!}{2^{n-1}}$

G-wise: $|X| < \frac{n!}{2^{n-1}} (\#G) = \frac{n!}{2^{n-1}} 2^{\binom{n}{2}}$

c-wise: $|X| = \sum_c \underbrace{\text{Grafi}(c)}_{2^{\binom{n}{2}-n+1}} \qquad \#c = n!$

$n! \cdot 2^{\binom{n}{2}-n+1} < \frac{n!}{2^{n-1}} 2^{\binom{n}{2}} \qquad 1 < 1.$

Problem 28 (IMO Shortlist 1991 [8]) Let A be a set of n residues mod n^2. Show that there is a set B of n residues mod n^2 such that at least half of the residues mod n^2 can be written as $a+b$ with a in A and b in B.

$X = \{ (B, x) : |B| = n, \ x \text{ non si scrive come } a+b \}$

Ipotesi di assurdo: $\forall B$ gli x sono $\geq \frac{n^2}{2}$

B-wise: $|X| = \sum_B \underbrace{\text{residui } (B)}_{< \frac{n^2}{2}} \geq \frac{n^2}{2} (\#B) = \frac{n^2}{2} \binom{n^2}{n}$

x-wise: $|X| = \sum_x \underbrace{\#B \text{ che non permettono di scrivere } x}_{B \text{ deve evitare i valori } x-a \text{ con } a \in A}$

$= \binom{n^2-n}{n}$

$= \binom{n^2-n}{n} \cdot (\#x) = n^2 \binom{n^2-n}{n}$

Ho ottenuto $\frac{n^2}{2} \binom{n^2}{n} \leq n^2 \binom{n^2-n}{n}$ che spero assurda,

cioè vorrei che

$$\binom{n^2}{n} \overset{?}{>} 2 \binom{n^2-n}{n}$$

$$\frac{n^2 (n^2-1) \cdots (n^2-n+1)}{n!} \overset{?}{>} 2 \frac{(n^2-n) \cdots (n^2-2n+1)}{n!}$$

$$\left(\frac{n^2}{n^2-n}\right)\left(\frac{n^2-1}{n^2-n-1}\right) \cdots \left(\frac{n^2-n+1}{n^2-2n+1}\right) \overset{?}{>} 2$$

$$\left(1+\frac{n}{n^2-n}\right)\left(1+\frac{n}{n^2-n-1}\right) \cdots \overset{?}{>} 2$$

$$\text{LHS} > 1 + \frac{n}{n^2-n} + \frac{n}{n^2-n-1} + \cdots$$

$$\geq 1 + \frac{1}{n} + \frac{1}{n} + \cdots + \frac{1}{n} = 2.$$

IMO 2014 – 6 n rette in posizione generica nel piano ne coloro k di blu in modo che nessuna regione limitata del piano abbia il bordo tutto blu.
Domanda: quanto può essere grande k?

Marking scheme:

- $k \geq cn^\alpha$ — 1 pto
- $k \geq c\sqrt{n}$ con $0 < c < \frac{1}{\sqrt{2}}$ — 2 pti
- $k \geq \frac{\sqrt{n}}{\sqrt{2}}$ — 4 pti
- $k \geq \sqrt{n}$ — 7 pti

Tentativo basic

$X = \{ (C, R) : C$ è una scelta di k rette blu
R è una regione blu $\}$

Ipotesi di assurdo: $\forall C$ esiste una regione blu

C-wise: $|X| = \sum_C$ regioni blu (C)

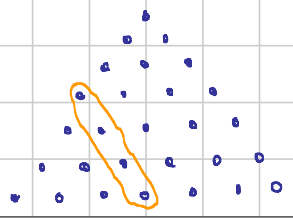
$\geq \#C = \binom{n}{k}$

R-wise: $|X| = \sum_R$ colorazioni che rendono R blu

$= \sum_R \binom{n-\ell(R)}{k-\ell(R)} \leq \sum_R \binom{n-3}{k-3}$

$\ell(R)$: lati della regione

$= \binom{n-3}{k-3} (\#R)$



3 rette → 1 n rette = $\Delta(n-2) = \frac{(n-2)(n-1)}{2}$

4 → 3

5 rette → 6 Abbiamo ottenuto

$$\binom{n}{k} \le \binom{n-3}{k-3} \frac{(n-2)(n-1)}{2}$$

$$\frac{n!}{k!\,(n-k)!} \le \frac{(n-3)!}{(k-3)!\,(n-k)!} \cdot \frac{(n-2)(n-1)}{2}$$

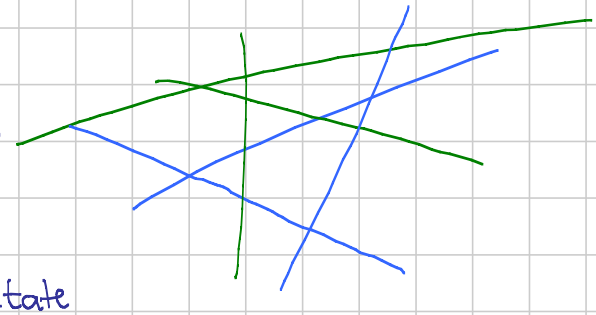
$k(k-1)(k-2)$

$$2n \le k(k-1)(k-2) \quad \rightsquigarrow \quad \boxed{k \ge c\sqrt[3]{n}}$$

— o — o —

Idea più fine: prendiamo config. con k ottimale non migliorabile (cioè se aggiungo una retta blu, rendo blu almeno una regione)

A ogni retta verde associo una delle regioni che diventano blu se lo diventa anche lei



rette verdi → regioni limitate

$n-k$ ↑ $\frac{(n-1)(n-2)}{2}$

INIETTIVA, cioè |arrivo| ≥ |partenza|, il che è ovvio

Definisco punto blu ogni incrocio di 2 rette blu

rette verdi → p.to blu a caso della regione (o di una delle regioni) che diventa blu.

$n-k$ ↑ $\binom{k}{2}$

non è detto che sia iniettiva, ma al max 4:1

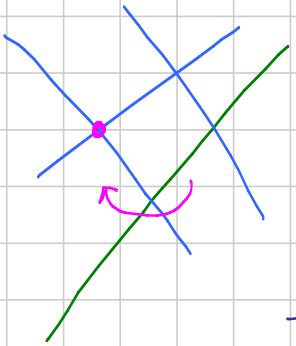
$n-k \le \binom{k}{2} 4$

$n-k \le 2k(k-1)$

$n-k \le 2k^2-2k$

$n \le 2k^2 \quad k \ge \frac{\sqrt{n}}{\sqrt{2}}$

Se voglio migliorare il $\frac{1}{\sqrt{2}}$ devo migliorare il 4:1, migliorando la scelta del p.to blu associato.



Posso prendere il primo blu in senso orario.

Problem 18 (Erdős 1963 [1, Chap. 1]) Let k be a positive integer. Say that a (round-robin) tournament is *k-unrankable* if for every set of k players, there is another player who beat all of them. Show that there is a tournament with more than k players that is k-unrankable.

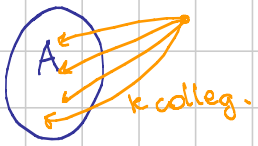
$X = \{ (G, A) :$ in G non esiste p che batte tutti gli elem. di $A \}$

Ipotesi di assurdo: $\forall G \ \exists A$ t.c. $(G,A) \in X$

G-wise: $|X| \geq \#G = 2^{\binom{n}{2}}$

A-wise: $|X| = \sum_A$ grafi in cui A non è dominato da nessun p

$$2^{\binom{k}{2}} \cdot 2^{\binom{n-k}{2}} \cdot \left(2^k - 1\right)^{n-k}$$



$\binom{k}{2}$: Dentro A a caso

$\binom{n-k}{2}$: Fuori da A a caso

$(2^k - 1)^{n-k}$: Da ogni vertice fuori avrei 2^k possibilità dentro

$$= 2^{\binom{k}{2} + \binom{n-k}{2}} \cdot \left(2^k - 1\right)^{n-k} \cdot \#A$$

$$\binom{n}{k}$$

Spero che

$$\binom{n}{k} \cdot 2^{\binom{k}{2} + \binom{n-k}{2}} \cdot \left(2^k - 1\right)^{n-k} < 2^{\binom{n}{2}}$$

per n grande

$\binom{n}{k}(2^k-1)^{n-k} < 2^{\binom{n}{2}-\binom{k}{2}-\binom{n-k}{2}} = 2^{k(n-k)}$

$\binom{n}{k}\left(1-\frac{1}{2^k}\right)^{n-k} < 1$

$\sim n^k$ esponenziale con base < 1.

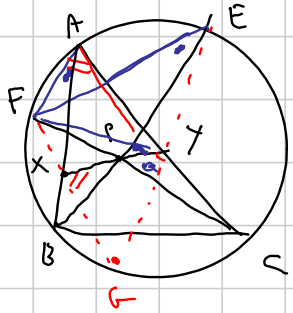
—o—o—

SENIOR 2016 G2 ADVANCED

Note Title 9/4/2016

Introduzione:

ES 1 PASCAL



$Q \in XY$ t.c. $FEPQ$ ciclico

$\Rightarrow$ $AFXQ$, $AQYE$ ciclici

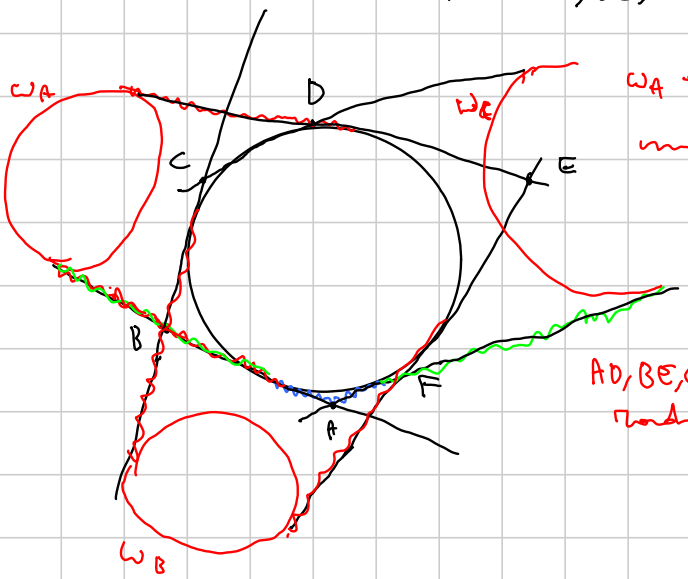
$\Rightarrow E\hat{G}F = 180° - \hat{A} - \hat{A}$

$= 180° - F\hat{A}Q - Q\hat{A}E$

$= 180° - F\hat{A}E$

ES 2 BRIANCHON

TS: AD, BE, CF concorrono



ω_A tangente BA, DE

$\Rightarrow$ lung. p fissata

ω_B, ω_C simili

AD, BE, CF conc. nel centro radicale di AD, BE, CF

PIANO PROIETTIVO, PROIETTIVITÁ

Def $\mathbb{RP}^2 = \{ [x,y,z] \mid (x,y,z) \neq (0,0,0) \in \mathbb{R}^3 \}$

$[x,y,z] = \{ (kx,ky,kz) \mid (x,y,z) \in \mathbb{R}^3 \text{ fissato}, \ k \in \mathbb{R}^* \}$

retta: $\{ [x,y,z] \in \mathbb{RP}^2 \mid \forall (x,y,z) \in [x,y,z], \ lx+my+nz=0 \}$

$(l,m,n) \neq (0,0,0)$

ora considero $\Gamma = \{ \dots, \ ux+vy+wz=0 \}$

$[x,y,z] \to (\tilde{x},\tilde{y},\tilde{z}) = \left(\frac{x}{ux+vy+wz}, \dots \right)$

in $\mathbb{RP}^2 / \Gamma$

ora ho che $u\tilde{x}+v\tilde{y}+w\tilde{z}=1$

PROIETTIVITÁ

(semi) Formale: $T: \mathbb{RP}^2 \to \mathbb{RP}^2$ $\quad T(x+y)=T(x)+T(y)$, $T(\lambda x)=\lambda T(x)$

$[X] \to [AX]$

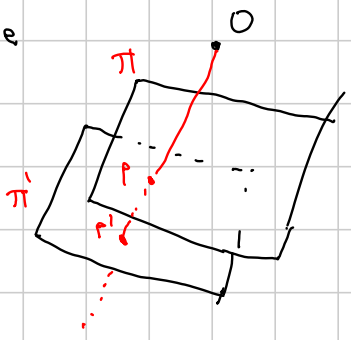
$\left[\begin{pmatrix} a \\ b \\ c \end{pmatrix} \right] \to \left[\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} \right]$

$=$

$\left[\begin{pmatrix} a_{11}a+a_{12}b+a_{13}c, & \dots \end{pmatrix} \right]$

la matrice è invertibile

Intuitivamente



$P \to P' = T(P)$

oss le T_∞ è la retta all'infinito di π:
- considero il fascio delle rette per o parallele a Π
- le loro intersezioni con π' sono $T(T_\infty)$

oss $A=[(a_1,a_2,a_3)]$ $B=[(b_1,b_2,b_3)]$ $C=[(c_1,c_2,c_3)]$ $D=[(d_1,d_2,d_3)]$ voglio T: $T(1,0,0)=A$, $T(0,1,0)=B$, $T(0,0,1)=C$, $T(1,1,1)=D$.

$$\left[\begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix}\begin{pmatrix}1\\0\\0\end{pmatrix}\right]=\left[\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix}\right]=\begin{bmatrix}ka_1\\ka_2\\ka_3\end{bmatrix}$$

$$M(T)=\begin{pmatrix} ka_1 & hb_1 & jc_1 \\ ka_2 & hb_2 & jc_2 \\ ka_3 & hb_3 & jc_3 \end{pmatrix}$$

Impongo che

$$\begin{cases} ka_1+hb_1+jc_1=d_1 \\ ka_2+hb_2+jc_2=d_2 \\ ka_3+hb_3+jc_3=d_3 \end{cases}$$

$$\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}\begin{pmatrix}k\\h\\j\end{pmatrix}=\begin{pmatrix}d_1\\d_2\\d_3\end{pmatrix}$$

$\exists!$ soluzione perché N è invertibile (ABCD non degenere)

CONICHE

$$Ax^2+By^2+Cz^2+2Dyz+2Exz+2Fxy=0$$

$$(x,y,z)\underbrace{\begin{pmatrix} A & F & E \\ F & B & D \\ E & D & C \end{pmatrix}}_{M}\begin{pmatrix}x\\y\\z\end{pmatrix}=0$$

oss. M è simmetrica $M^T=M$ $\left((AB)^T=B^TA^T\right)$

Tr. polari (dualità)

conica $X=\begin{pmatrix}x\\y\\z\end{pmatrix}$ $X^TMX=0$

dato $P \in \mathbb{RP}^2$ chiamo retta polare di P

$$r_P = \{ X \in \mathbb{RP}^2 \mid P^T M X = 0 \}$$

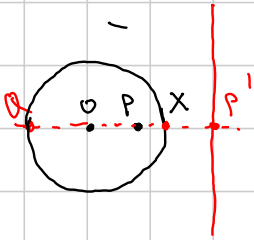
oss $Q \in pol(P) \iff P^T M Q = 0$

$\Updownarrow$

$Q^T M P = 0 \iff P \in pol(Q)$

oss 2 (non lo dimostro)

se $P \in$ (conica) la polare è tangente



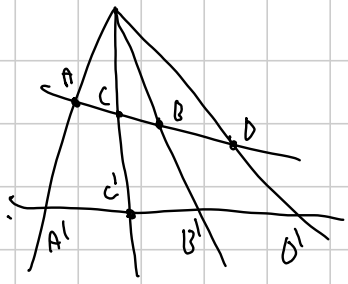
$\Rightarrow (QX, PP') = -1$ (*)

(Q, X, P, P')

oss. 3 (*) vale in generale per le coniche

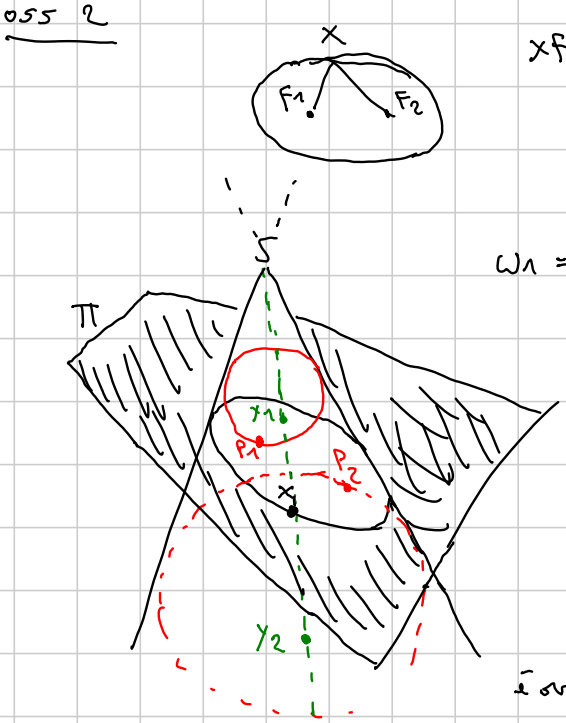
CONICHE E PROIETTIVITÀ (MA NON SOLO)

oss 1 Le proiettività conservano i birapporti



$(A, B, C, D) = (A', B', C', D')$

oss 2



$XF_1 + XF_2 = \text{cost.}$

ω_1 = sfera tangente al cono e a π (sopra)

ω_2 = stessa cosa sotto

$X \in$ piano $\cap$ cono

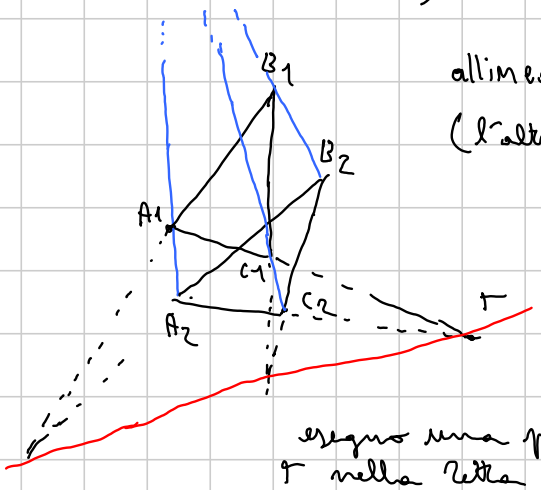
SX tange ω_1 in Y_1
tange ω_2 in Y_2

è ovvio che $XP_1 = XY_1$ (segm. di tang.)
$XP_2 = XY_2$

$XP_1 + XP_2 = XY_1 + XY_2 = Y_1Y_2$

non dipende da X per simmetria

ESERCIZIO 1 (DESARGUES)

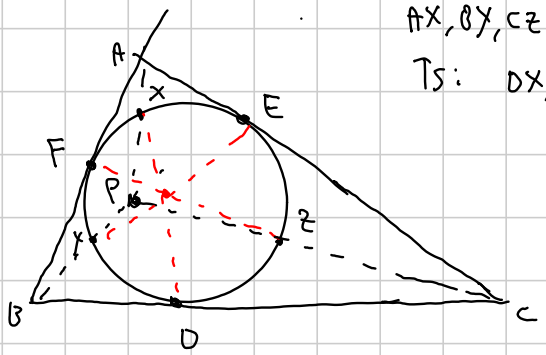


allineamento ⇒ concorrenza
(l'altra freccia per esercizio)

esegno una proiettività che manda r nella retta all'infinito r_∞

Vera $A_1B_1 \parallel A_2B_2$ e simili
⇒ $A_1B_1C_1$ e $A_2B_2C_2$ sono omotetici
⇒ A_1A_2, B_1B_2, C_1C_2 concorrono nel centro di omotetia
ma la concorrenza è un invariante proiettivo !

ESERCIZIO 2 (STEINBART)



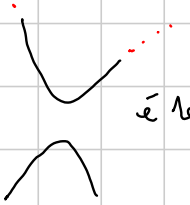
AX, BY, CZ concorrono in P (interno)

TS: DX, EY, FZ concorrono

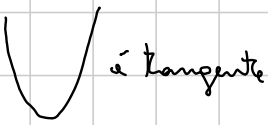
Voglio una proiettività che manda (DEF) in un cerchio ω e P nel suo centro.

Cosa faccio? prendo la polare di P e la mando all'infinito

(DEF) non interseca la polare quindi la sua immagine non interseca r_∞ $\Rightarrow$ l'immagine è un'ellisse

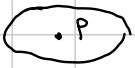


è secante r_∞

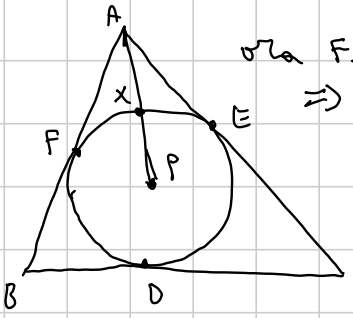


è tangente

e P è il suo centro



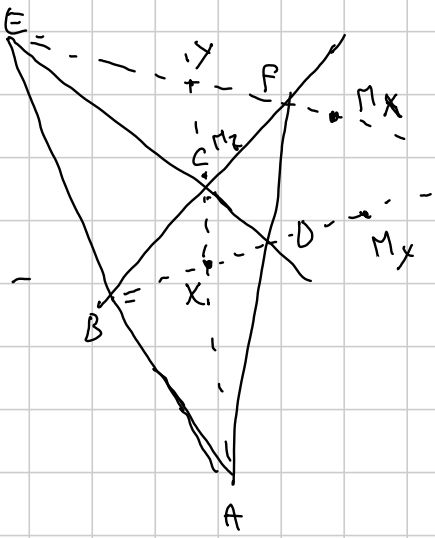
Infine possiamo fare un'affinità che manda l'ellisse in una circonferenza di centro P.



ora FX = XE ecc.

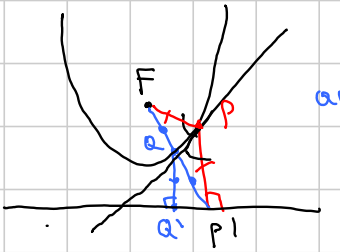
$\Rightarrow$ DX, EY, FZ concorrono nell'incentro di DEF.

ESERCIZIO 3 (TH. EMELYANOV)



tesi: il pt. di Miquel di $\{AB, BC, CD, DA\}$ sta sulla circonferenza di Feuerbach di XYZ

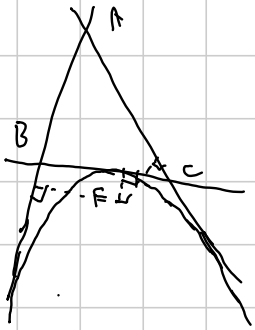
LEMMA 1: la bisettrice di $F\hat{P}P'$ è tangente alla parabola



$QF \parallel QQ'$, $QQ' = QP'$ simmetria

dunque se $MF = MP' \Rightarrow PM \perp FP'$

$\Rightarrow$ la proiezione di F sulla tangente sta sulla tangente per il vertice

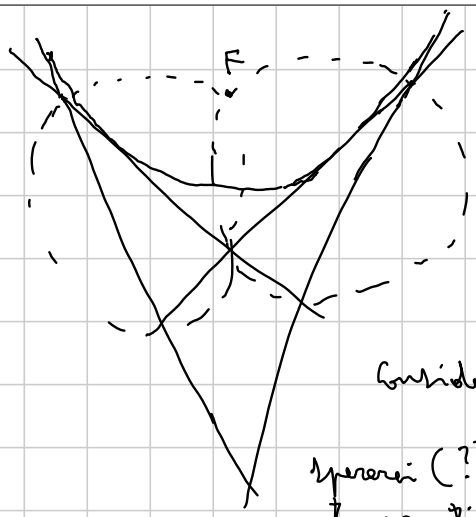


$\Rightarrow$ le proiezioni di F sui tre lati sono allineate su una retta tangente alla parabola (per il vertice)

SIMSON $\Rightarrow F \in \odot(ABC)$

□

Dunque se prendo la parabola tangente ai quattro lati (esiste!)



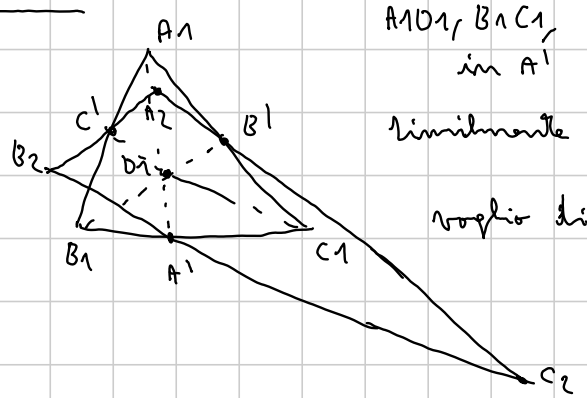
il fuoco è punto di Miquel

Considero $\{M_xM_y, M_xM_z, M_yM_z, r_\infty\} = Q_1$

Spero (?) che anche queste rette siano tangenti alla parabola

OSS: $ABCDEF$ e Q_1 hanno le stesse diagonali (XY, XZ, YZ)

LEMMA 2:



$A_1D_1, B_1C_1, A_2D_2, B_2C_2$ concorrono in A'

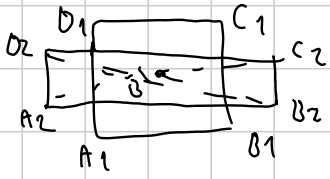
similmente B', C'

voglio dire che $A_1, B_1, C_1, D_1, A_2, B_2, C_2, D_2$ stanno tutti nella stessa conica

Dim: mando $A_1B_1C_1D_1$ in un quadrato

ora $A', C' \in r_\infty \Rightarrow B_2C_2 \parallel B_1C_1$ ecc.

$\Rightarrow A_2B_2C_2D_2$ è un rettangolo con i lati paralleli a $A_1B_1C_1D_1$



Inoltre per hp $A_1C_1, B_1D_1, A_2C_2, B_2D_2$ concorrono in B' che è centro comune

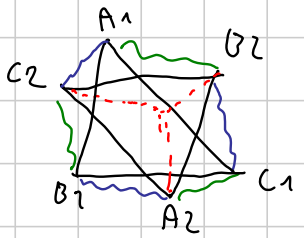
$\Rightarrow$ la conica per $A_1B_1C_1D_1A_2$ ha centro in B'

$\Rightarrow$ passa anche per B_2, C_2, D_2 □

Ora con una trasformazione duale la tesi segue.

ESERCIZIO 4 (SONDAT)

Def:



ortologici
: la ⊥ da A_2 a B_1C_1 ecc. concorrono in Q_1

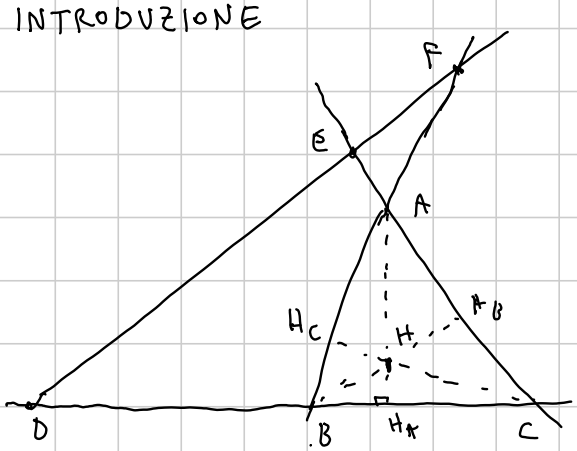
si vede da questo $\Leftrightarrow B_1A_2^2 + C_1B_2^2 + A_1C_2^2 = A_2C_1^2 + A_1B_2^2 + C_2B_1^2$

$\Leftrightarrow$ la ⊥ da A_1 a B_2C_2 ecc. concorrono in Q

e $A_1B_1C_1$, $A_2B_2C_2$ sono ortologici e soddisfano Desargues (A_1A_2, B_1B_2, C_1C_2 concorrono in P)

$\Rightarrow$ esiste una retta per P, Q, Q_1

INTRODUZIONE



ω_A = cfr. di diametro AD
ω_B = " " BE
ω_C = " " CF

$H_A \in \omega_A$ ecc.

$AH \cdot H_AH = BH \cdot H_BH = CH \cdot H_CH$

$\Rightarrow$ H ha la stessa potenza risp. $\omega_A, \omega_B, \omega_C$

Ulteriore con gli ortocentri di $A\hat{E}F$, $C\hat{E}D$, $B\hat{D}F$

$\Rightarrow \omega_A, \omega_B, \omega_C$ sono coassiali e i 4 ortocentri sono allineati sul comune asse radicale (retta di AUBERT/STEINER)

LEMMA (1):
Esso è il luogo dei punti P t.c. la ⊥ da A a DP e cyc concorrono

Si vede facilmente che il luogo è una retta (cartesiano)

$D(a_d, b_d)$
$E(a_e, b_e)$
$F(a_f, b_f)$

P_A: $X(x_p - a_d) + Y(y_p - b_d) = f_A(x_p, y_p)$
P_B:
P_C:

$p_A - p_B$: $\quad X(a_e - a_d) + Y(b_e - b_d) = g_1(x_p, y_p)$ di 1° grado

$p_B - p_C$: $\quad X(a_f - a_e) + Y(b_f - b_e) = g_2(x_p, y_p)$ di 1° grado

i LHS sono proporzionali $\frac{a_e - a_d}{a_f - a_e} = \frac{b_e - b_d}{b_f - b_e} = c$

perché D, E, F sono allineati

$\Rightarrow g_1(x_p, y_p) = g_2(x_p, y_p) \cdot c$: è una retta

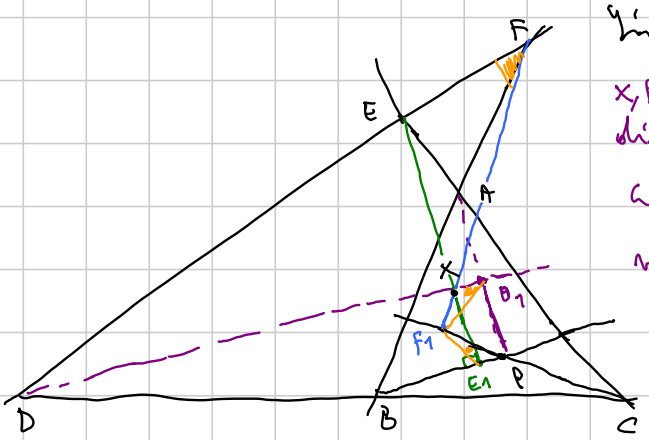
Ci basta mostrare che la retta di AUBERT soddisfa

Una X è retta di AUBERT

X, P_1, E_1, P sono sul cerchio di diametro XP, che chiamo ω

$\omega \cap DX = \{X, D_1\}$

vorrei P, D_1, A allineati



$XE \cdot XE_1 = XF \cdot XF_1 = \rho^2$ (X ∈ AUBERT line)

$X\hat{D}_1F_1 = X\hat{E}_1F_1 = X\hat{F}E$ $\Rightarrow$ DF F_1D_1 ciclico

EFE_1F_1 è ciclico

ma allora $XD \cdot XD_1 = \rho^2 \Rightarrow D_1 \in \omega_A \Rightarrow A\hat{D}_1D = 90° \Rightarrow$ Ts. □

LEMMA 2 : $\hat{ABC}$, $\hat{A_1B_1C_1}$ soddisfano DESARGUES

AA1, BB1, CC1 concorrono in P

AB ∩ A1B1 ecc. stanno su una retta t

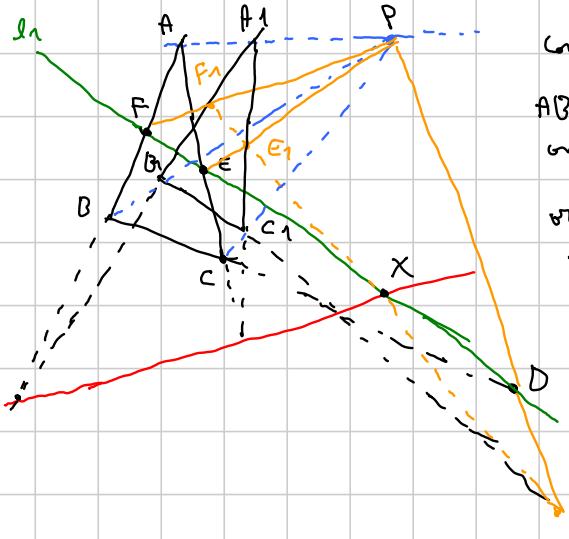
prendiamo una retta l_1

$D = BC \cap l_1$, $E = AC \cap l_1$, $F = AB \cap l_1$

$X = t \cap l_1$

$D_1 = DP \cap B_1C_1$
$E_1 = EP \cap A_1C_1$
$F_1 = FP \cap A_1B_1$

TS: D_1, E_1, F_1, X allineati

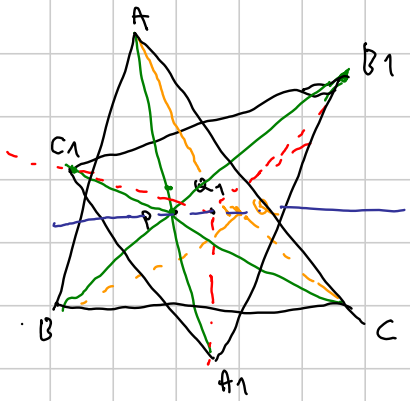


Mando t all'infinito
come in DESARGUES
ABC, $A_1B_1C_1$ diventano omotetici (via φ l'omotetia)
ove P è il centro di omotetia
$\Rightarrow \varphi(D) = \varphi(BC \cap DP)$
$= \varphi(BC) \cap \varphi(DP)$
$= B_1C_1 \cap DP = D_1$

$\Rightarrow D_1, E_1, F_1$ sono allineati in $\varphi(l_1) = l_2$
$\Rightarrow l_2 // l_1 \Rightarrow l_2 \cap l_1 \in t$ (retta all'infinito) □

OSS: nel Lemma 2, se l_2 è all'infinito, allora $l_1 // t$

SONDAT:



OSS (corollario LEMMA 1) se ho ΔABC e due punti X, P
e r_A = retta per X $\perp$ ad AP ecc.
e suppongo che $r_A \cap BC$ ecc. sono allineati in l
allora $l \perp XP$

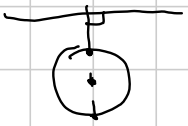
Dim per LEMMA 2, $X \in$ AUBERT LINE di ABCDEF

$\Rightarrow XD_1 \cdot XD = XE_1 \cdot XE = XF_1 \cdot XF = \rho^2$

$\Rightarrow$ le inverte di centro X, raggio ρ e poi simm. in X

allora ω (cfr. $(XPE_1P_1D_1)$ del LEMMA 1) $\rightarrow \overline{DEF}$

da cui la tesi:



Ora mostriamo SONDAT:

l_A = retta per P che è $\perp$ ad AQ (parallela a B_1C_1)

$l_A \cap BC = D$; definisco similmente E, F.

LEMMA 2 $\Rightarrow$ $\overline{DEF} \parallel t$ (prospettrica)

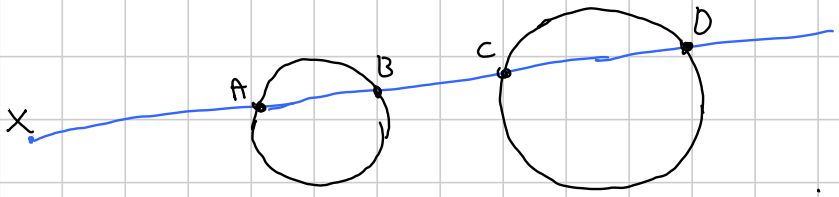
e sono allineati

(oss.) LEMMA 1 $\Rightarrow$ $\overline{DEF} \perp PQ \Rightarrow t \perp PQ$

similmente $t \perp PQ_1 \Rightarrow$ Ts.

ULTIMO ESERCIZIO

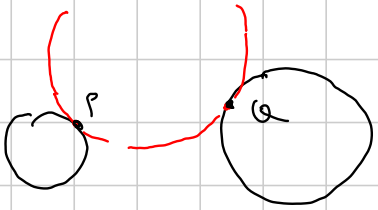
L'inversione è legata a nozioni proiettive



– A, C sono omologhi
sono OMOLOGHI

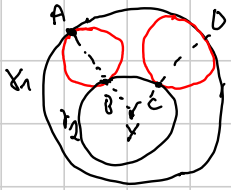
– A, D sono inversi
si chiamo ANTIOMOLOGHI

0551



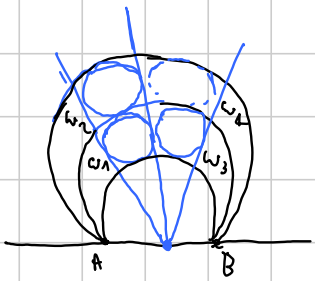
la circ. nulla esiste
$\Leftrightarrow$ P, Q sono ANTIOMOLOGHI
(per MONGE)

In particolare

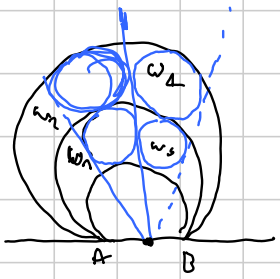


allora ABCD è ciclico
$XA \cdot XB = XD \cdot XC$
= raggio^2 dell'inversione di centro X che scambia γ_1, γ_2

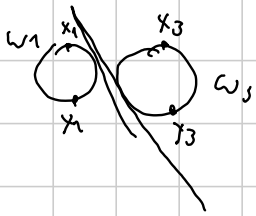
ESERCIZIO IMO SL 2010 – G7



STRATEGIA:



$X_1X_3Y_1Y_3$ è ciclico (come prima)



$\Rightarrow X_1X_3,\ Y_1Y_3,\ AB$ concorrono in un punto $P_{1,3}$

per MONGE $P_{1,3}$ è il centro di sim. est. di $\omega_1\omega_3$

$\Rightarrow$ sempre per Monge, il centro di sim. est. di ω_2, ω_3 sta su BA

Ora consideriamo $\omega_2, \omega_3, \omega_4$

Come prima, il centro di sim. esterna di ω_2, ω_4 sta su AB

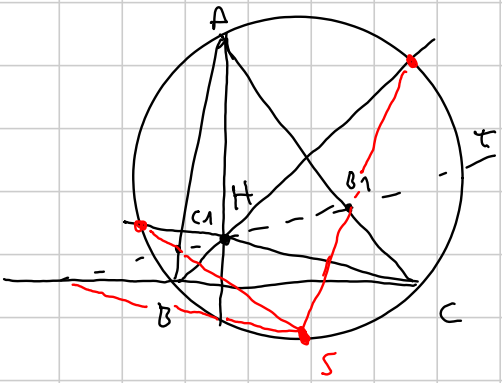
ma vale anche per ω_2, ω_3

MONGE $\Rightarrow$ le tang. comm. esterne di ω_3, ω_4 si incontrano su AB $\Rightarrow$ TS.

SENIOR 2016 G3 – ADVANCED

Note Title 9/6/2016

Linea di Steiner

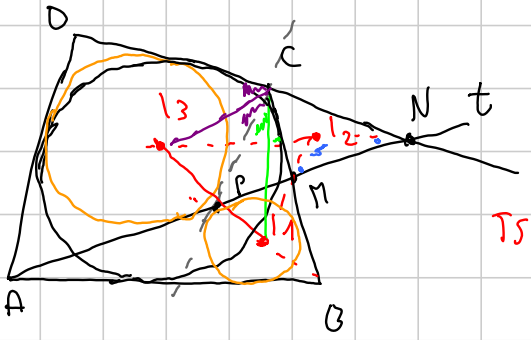


oss: rette rosse = simm. di t nei lati AB, BC, CA.

S = anti-steiner point di t

Inverso: $\forall S \in (ABC)$, i cui simm. nei lati sono allineati con H

ESERCIZIO 1 IMO SL 2009 – G8



I_1 = incentro di ΔABM
I_2 = " " CMN
" " AON

TS: l'ortocentro di $I_1I_2I_3$ sta su t

Dim:

oss il simm. di C in I_2I_3 sta su t
di C in I_1I_2 sta su t

per quanto visto sopra, spero $C \in (I_1I_2I_3)$

mostro che $C \in$ triang. comune int. di $(I_1), (I_3)$

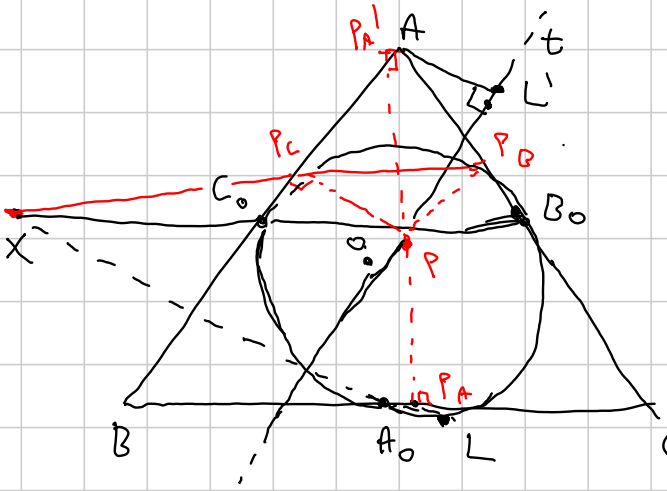
$\Rightarrow \widehat{I_3CI_1} = \frac{1}{2}\widehat{DCB} = \widehat{I_3I_2I_1}$

prendo $P \in t$ t.c. CP tange (I_3):

$CP - AP = DC - DA = BC - BA$

$\Rightarrow CPAB$ (non convesso) è inscritto $\Rightarrow$ TS. ∎

APPLICAZIONE 2 (Th. di Fonténe)



Ts: Se t è fissa e P varia, $(P_A P_B P_C)$ passa per un punto fisso.

oss: thm su $(A_0 B_0 C_0)$

Claim: è l'anti-Steiner point di OP in $A_0 B_0 C_0$, che chiamo L

$\forall$ a, a' simm. in $B_0 C_0$

oss' $L' \in t$, $L' \in (AC_0 OB_0) \Rightarrow A\hat{L'}O = 90°$

$\Rightarrow A P_C P P_B L'$ è ciclico (su ω)

e anche $P_A' \in \omega$

Claim 1: $L' P_C C_0 X$ ciclico

Dim: $\angle(L'C_0, L'P_C) = \angle(L'C_0, L'A) + \angle(L'A, L'P_C)$

$= \angle(B_0C_0, B_0A) + \angle(P_BA, P_BX)$

$= \angle(XC_0, XP_C)$

Claim 2: L, P_A, X allineati

Ora mostro che L', P_A', X sono allineati

$\angle(L'P_A', L'X) = \angle(L'P_A', L'P_C) + \angle(L'P_0, L'X)$

$= \angle(PP_A', PP_C) + \angle(C_0P_C, C_0X)$

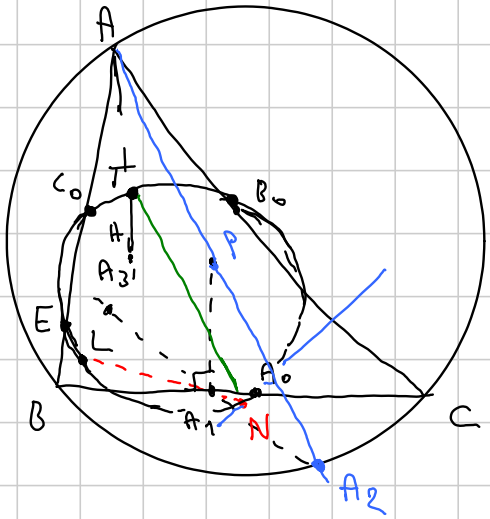
$= \angle(BP_A, BP_C) + \angle(BA, BC) = 0$ □

Ora scrivo $XP_A \cdot XL = XP_A' \cdot XL'$

$\Rightarrow L \in (P_A P_B P_C)$

$XP_C \cdot XP_B$

ESERCIZIO 3



A_3 = Simm. di A_2 in A_1, ecc.

TS: H, A_3, B_3, C_3 ciclici.

Dim: $N = LA_1 \cap (A_0B_0C_0)$

(oss: $A_1B_1C_1 \sim A_2B_2C_2$)

mostro che $A_0N \perp AP$.

$$\angle(A_0N, AP) = \angle(A_0N, LN) + \angle(LN, PA_1) + \angle(PA_1, AP)$$

$$= \angle(AB, EL) + \angle(AP, AL') + \angle(PA_1, AP)$$

$$= \angle(AB, B_0C_0) + \angle(B_0C_0, B_0L) + \angle(PA_1, AB) + \angle(AB, AL')$$

$$= \angle(PA_1, B_0C_0) + \angle(B_0C_0, B_0L') + \underbrace{\angle(B_0C_0, B_0L)}_{0}$$

$$= 90°$$

T = pt. medio AH $\Rightarrow TN \perp NA_0$

$\Rightarrow TN \parallel AP$

per ovvie omotetie, N è il pt. medio di HA_2

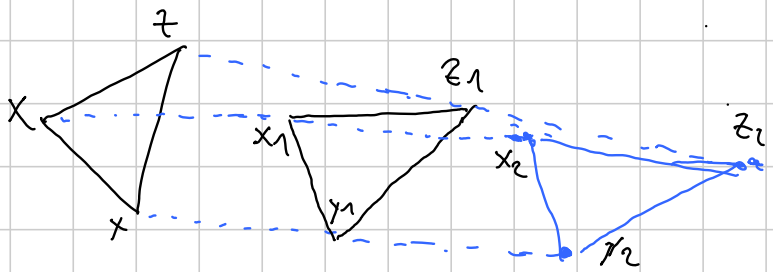
$\Rightarrow A_3H \parallel NL = A_1L$

$\Rightarrow \angle(A_3H, B_3H) = \angle(A_1L, B_1L) = \angle(A_1C_1, C_1B_1)$

LEMMA CHE CONCLUDE:

se $\hat{XYZ} \sim \hat{X_1Y_1Z_1}$ e X_2 = simm. di X in X_1, ecc.

$\Rightarrow \hat{X_2Y_2Z_2} \sim \hat{X_1Y_1Z_1}$



Dim: con la rototomotetia per cui $XX_1 \to YY_1$ manda anche X_2X_2. Sia S il suo centro.

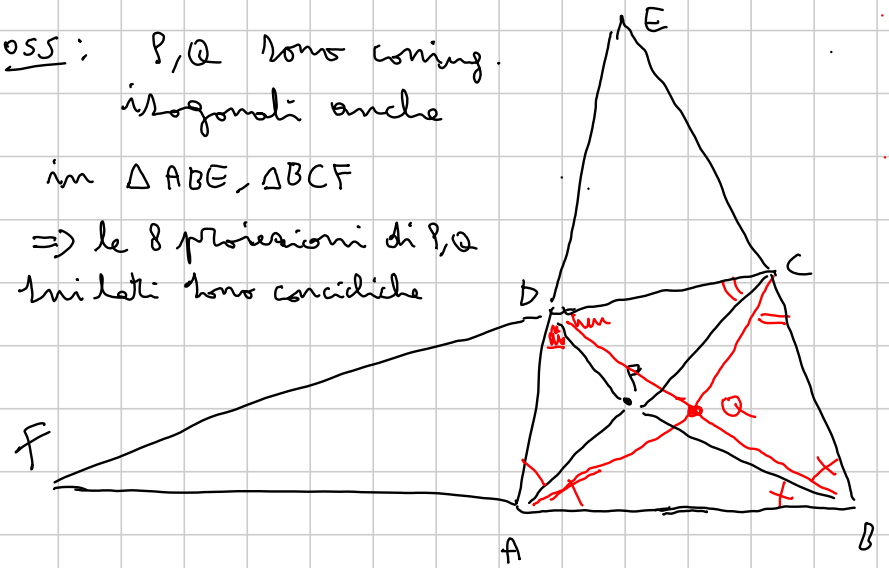
S è anche il centro di quella che manda $XY \to X_1Y_1$ e quella che manda $X_1Y_1 \to X_2Y_2$.

Allora $X_1Y_1S \simeq X_2Y_2S \simeq XYS$

$X_1Z_1S \simeq X_2Z_2S \simeq XZS$

"incastrandoli" ottengo $XYZS$ e $X_2Y_2Z_2S$ □

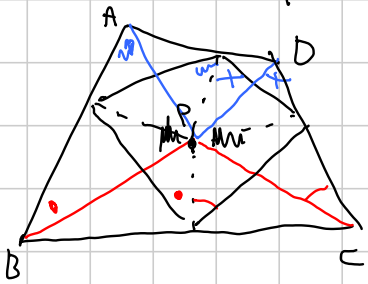
SECONDA Parte: CONIUGATI ISOGONALI (nei quadrilateri)



oss: P, Q sono coniug. isogonali anche in $\Delta ABE, \Delta BCF$

$\Rightarrow$ le 8 proiezioni di P, Q sui lati sono concicliche

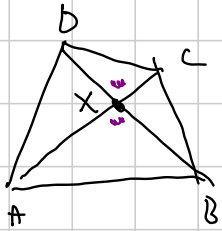
$\Rightarrow$ Il quadr. pedale di P è ciclico



rossi + blu = 180°

$\Rightarrow$ neri = 180°

APPLICAZIONE: IMO SL 2008 – G6



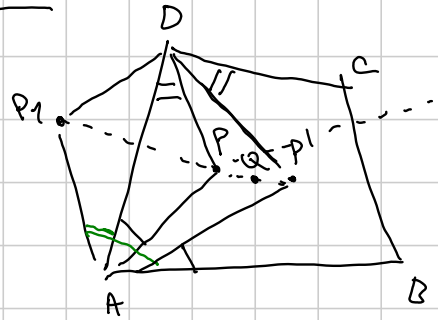
Quando X ha un cer. insieme?

$A\hat{X}B + C\hat{X}D = 180°$

$AC \perp OD$ □

ESERCIZIO PER CASA: prop. inversa.

ESERCIZIO:



Def: retta di GAUSS P_2 di ABCD (la chiamo g) luogo degli X tali che

$[ABX] + [CDX] = [BCX] + [ADX]$

Ts: il pt. medio di PP' $\in g$ (lo chiamo Q)

Dim: P_1 simm. di P in AD

oss: $2[ABQ] = [ABP] + [ABP']$

calcolo $2([ADQ] + [BCQ])$

$= [ADP] + [ADP'] + [BCP] + [BCP']$

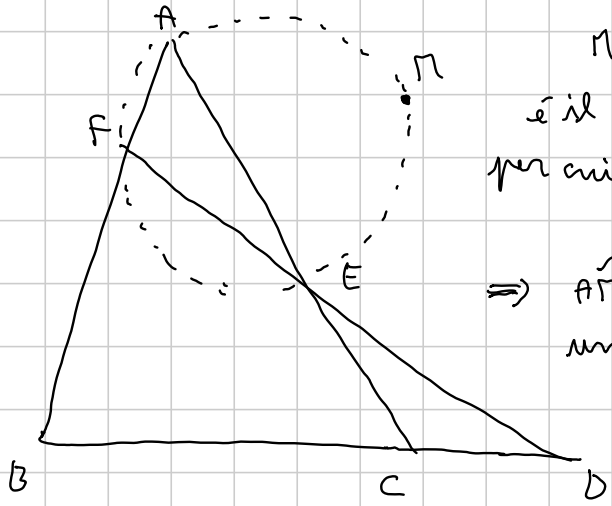
$[ADP] = [ADP_1]$ $\quad$ $[BCP] = [BCP_2]$

$[AP_1P'] + [DP_1P'] + [BP_2P'] + [CP_2P']$

$= \frac{1}{2}(AP \cdot AP' \sin\hat{A} + BP \cdot BP' \sin\hat{B} + CP \cdot CP' \sin\hat{C} + DP \cdot DP' \sin\hat{D})$

espr. simm. in A, B, C, D come voluto □

LEMMA (CLAWSON–SHMIDT CONJUGATION)



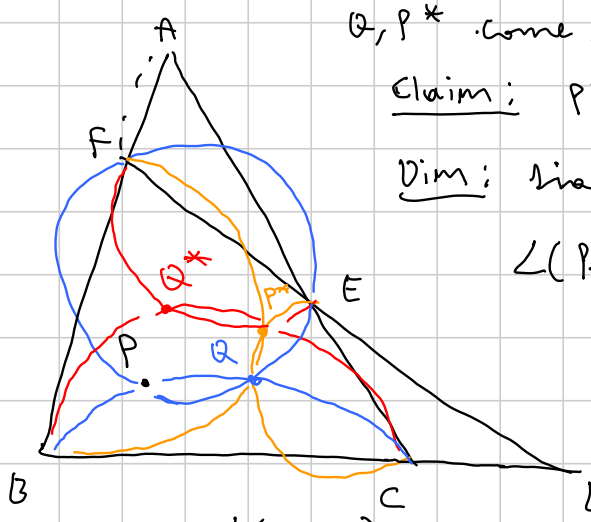
M pt. di Miquel $ABCDEF$ è il centro di rotomotetia per cui ad es. $EF \to CB$, $BF \to CE$

$\Rightarrow$ $A\hat{M}D$, $B\hat{M}E$, $C\hat{M}F$ hanno una bisettrice comune t

Inoltre $MA \cdot MD = MB \cdot ME = MC \cdot MF = \rho^2$

$\Rightarrow$ l'inversione di centro M e raggio ρ seguita da simmetria in t (via essa φ) fa sì che $A \leftrightarrow D$, $B \leftrightarrow E$, $C \leftrightarrow F$.

OSS: Se P, P' sono con. isogonali, allora $P \Leftrightarrow P'$ (in $BCEF$)



Q, P^* come in disegno

Claim: $P^* = \varphi(P)$

Dim: Sia $P_1 = \varphi(P)$

$$\angle(P_1F, P_1E) = \angle(P_1F, P_1M) + \angle(P_1M, P_1E)$$

$$= \angle(CP, CM) + \angle(BM, BP)$$

$$= \angle(CP, BC) + \angle(BC, CM) + \angle(BM, BC) + \angle(BC, BP)$$

$$= \angle(CP, BP) + \angle(MB, MC)$$

$$= \angle(CP, BP) + \angle(AB, AC)$$

Calcolo $\angle(PF, FQ^*) = \angle(FP, FE) - \angle(FQ^*, FE)$

$= \angle(QP, QE) - \angle(P^*Q^*, P^*E)$

$= \angle(QP, QC) + \angle(QC, QB) - \angle(P^*Q^*, P^*C) - \angle(P^*C, P^*E)$

$= \angle(BP, BC) - \angle(BQ^*, BC) = \angle(BP, BQ^*)$

$\Rightarrow$ BPQ^*F è ciclico

e lim. anche CPQ^*E.

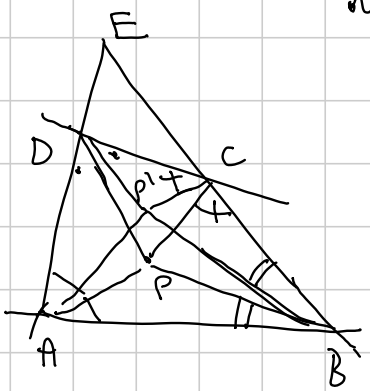
Infine calcolo

$$\angle(P^*F, P^*E) = \angle(P^*F, FE) + \angle(FE, P^*E)$$
$$= \angle(P^*F, PB) + \angle(FB, FE) + \angle(FE, EC) + \angle(EC, P^*E)$$
$$= \angle(AB, AC) + \angle(QP^*, QB) + \angle(QE, QP^*)$$
$$= \angle(AB, AC) + \angle(QC, QB)$$
$$= \angle(AB, AC) + \angle(PC, PB)$$

$\Rightarrow P_1 \in (P^*EFQ^*)$; facendo la stessa cosa risp. agli altri lati $\Rightarrow P^* \equiv P_1$

OSS: se P ammette coniug. isogonale in $ABCD$ e P^* è def. come immaginata, è lui il coniug.

Dim



La prima fa che

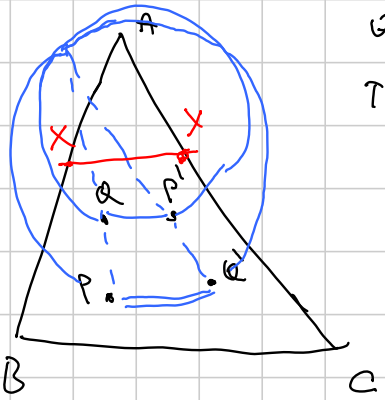
$$\angle(P^*D, P^*E) = \angle(EA, EB) + \angle(PB, PA)$$

calcolo

$$\angle(P'D, P'C) = \angle(P'D, DC) + \angle(DC, P'C)$$
$$= \angle(AD, DP) + \angle(PC, CB)$$
$$= \angle(CP, PD) + \angle(EA, EB)$$
$$= \angle(EA, EB) + \angle(PB, PA)$$

cicando luo che $P^* \equiv P'$

APPLICAZIONE:



P, P' con. isog.
Q, Q' con. isog.
TS: il pt. di Miquel di $\{PQ, PQ', Q'P', P'Q\}$ sta su $\odot(ABC)$

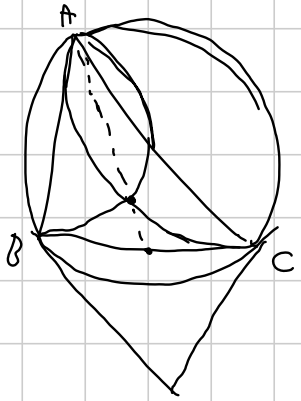
Dim $X \in AB$, $Y \in AC$ t.c. le coniugazioni valgono in $BCXX$

Ora se M è pt. di Miquel di $BCXX$ vale che $\varphi(P) = P'$, $\varphi(Q) = Q'$ $\Rightarrow$ $MXP \simeq MP'C$ ecc.

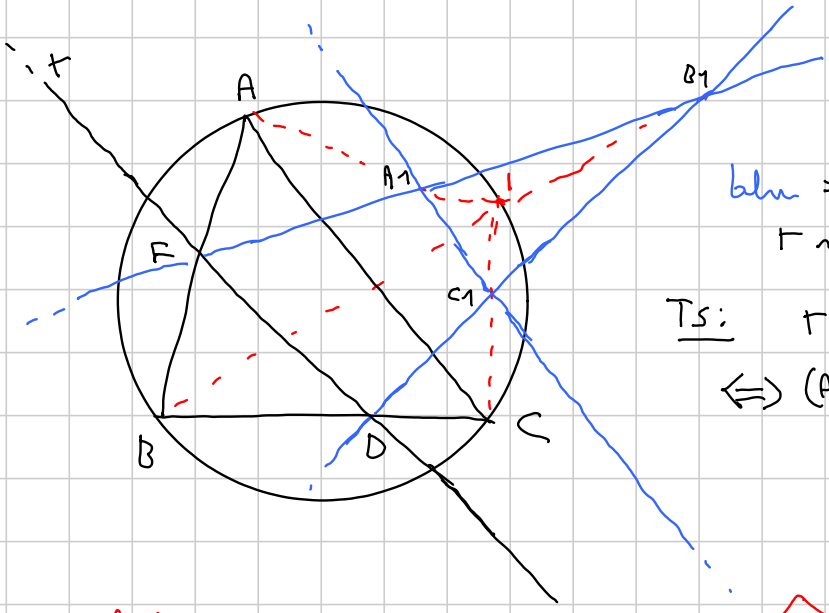
Ora la rotom. che manda $PQ' \to QP'$ deve avere centro M $\Rightarrow$ TS.

D

TERZA PARTE



IMO 2011 – 6



blu = simm. di Γ nei lati

Ts: Γ tange (ABC) $\Leftrightarrow$ ($A_1B_1C_1$) tange (ABC)

oss 1: BC bisettrice di $\widehat{F_a, \Gamma}$ ecc.

$\Rightarrow$ C è in/ex-centro di DEC_1

In ogni caso CC_1 bisca $\widehat{F_a, \Gamma_b}$, ecc.

$\Rightarrow$ AA_1, BB_1, CC_1 concorrono in I, dove I è l'incentro di $A_1B_1C_1$.

Ora $\angle(CB, DE) + \angle(DE, EC) + \angle(C_1C, C_1D) = 90°$

$\Rightarrow \angle(C_1C, CB_1) = 90° - \angle(BC, DE) - \angle(DE, EC) = 90° - \angle(BC, AC)$

$\angle(B_1B, B_1C_1) = 90° - \angle(BC, AB)$.

$\Rightarrow \angle(BB_1, CC_1) = \angle(BC, AC) - \angle(BC, AB) = \angle(AB, AC)$

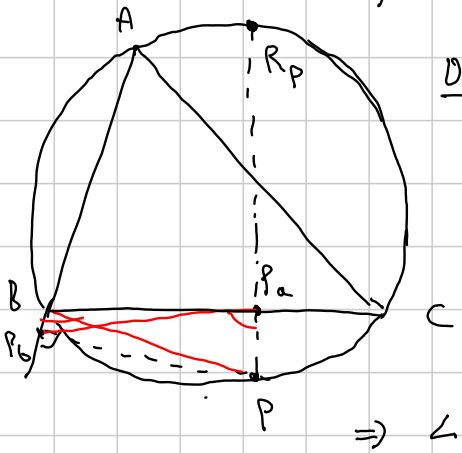
$\Rightarrow I \in (ABC)$.

oss: Se inverto in I, l'imm. di $A_1B_1C_1$ è simile ad ABC, mentre (ABC) va in una retta.

ad es. $A_1 \to A_2$, ecc. e $A \to A'$, spero che

$ABC \cup \Gamma \overset{+}{\simeq} A_2B_2C_2 \cup \overline{A'B'C'}$

LEMMA: dati $P, Q \in (ABC)$ e l_P, l_Q le rispettive linee di Steiner, $\angle(l_P, l_Q) = \angle(AQ, AP)$



Dim $l_P \parallel P_a P_b$ (linea di SIMSON) e PP_bBP_a ciclico

$\angle(R_PA, R_PP) = \angle(BA, BP) = \angle(P_aP_b, P_aP)$

$\Rightarrow P_aP_b \parallel AR_P$

$\Rightarrow \angle(l_P, l_Q) = \angle(AR_P, AR_Q) = \angle(AQ, AP)$ □

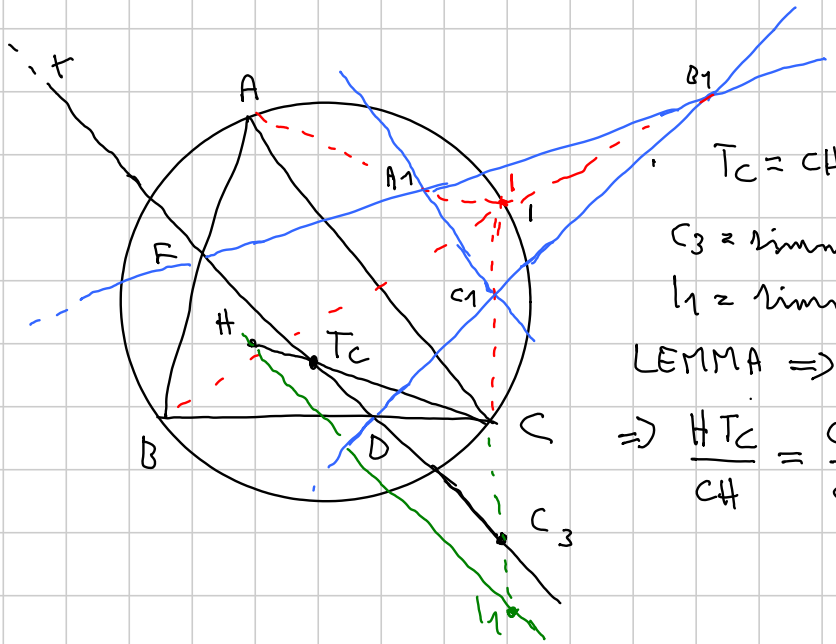
Ora

$$\angle(c_1, cA) = \angle(c_1c, c_1e) + \angle(c_1e, Ec) = 90^\circ - \angle(DC, DE)$$
$$= 90^\circ - \angle(BC, T) = \angle(AH, T).$$

Sia l' l'anti-Str. prim. della retta per H, che è $\parallel$ a T.

per il LEMMA, $(\text{su } l', A)$ $\angle(c_1', cA) = \angle(AH, T) = \angle(c_1, cA)$

analog. $\Rightarrow l \equiv l'$



$T_C = CH \cap T$

C_3 = simm. di C_1 in BC

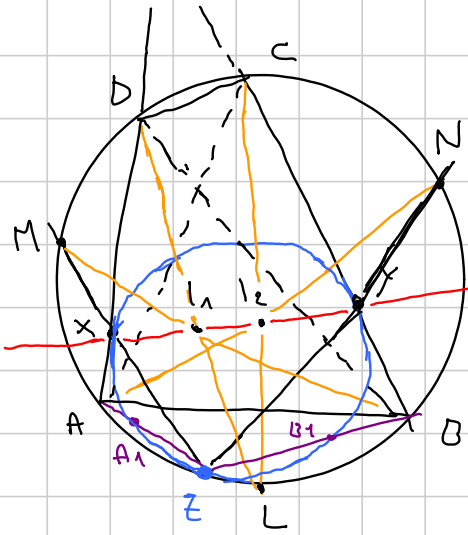
I_1 = simm. di I in BC

LEMMA $\Rightarrow I_1H \parallel T$

$$\Rightarrow \frac{HT_C}{CH} = \frac{C_3I_1}{CI_1} = \frac{IC_1}{IC} = \frac{IC'}{IC_2}$$

Ora $A_2B_2C_2I \stackrel{+}{\sim} ABCH \Rightarrow$ nella similitudine (per sopra), $A_2 \to A$, ecc. e $A' \to T_C$ □

QUARTA PARTE



I_1 = l'incentro di $A\hat{B}D$
I_2 = l'incentro di $A\hat{B}C$
TS: X, Y, I_1, I_2 allineati
$LA = LB$

Idea: Pascal su $ZMBADL$

$\Rightarrow$ $ZM \cap AD = X$
$MB \cap DL = I_1$ allineati.
$AB \cap ZL = K$

Similmente avrò che Y, I_2, K sono allineati
Ora mi basta mostrare che $K \in XY$, cioè XY, AB, ZL concorrono.

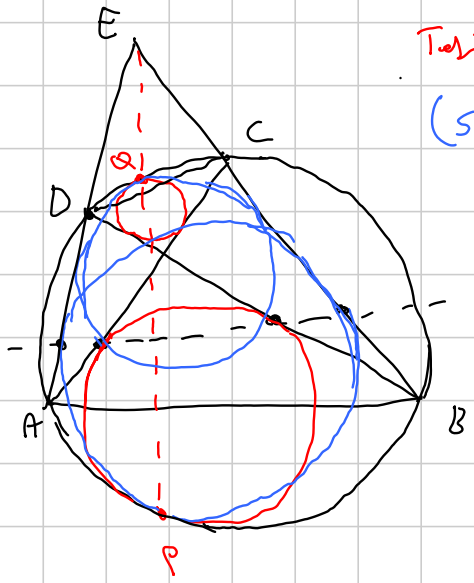
oss: $KA/KB = ZA/ZB$ perché L è pt. medio dell'arco $\overset{\frown}{AB}$ che $AD \cap BC = E$, uso menelao su $A\hat{B}E$

oss $EX = EY \Rightarrow$ mi basta che $KA/KB = AX/BY$
$\parallel$
ZA/ZB

oss: $A_1B_1 \parallel AB$ per omotetia

$$\frac{BY^2}{AX^2} = \frac{BB_1 \cdot BZ}{AA_1 \cdot AZ} = \frac{BZ^2}{AZ^2} \Rightarrow \text{Tesi}$$

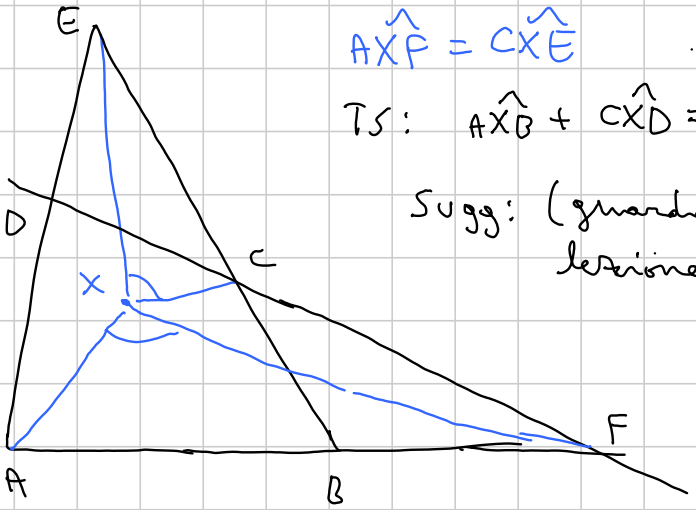
ESERCIZI PER CASA:



Tesi: PQ passa per E

(Sugg: le sfere e blu hanno gli stessi punti di tangenza ho finito per Monge)

ESERCIZIO PER CASA 2:



$A\hat{X}F = C\hat{X}E$

Ts: $A\hat{X}B + C\hat{X}D = 180°$

Sugg: (guardare questa lezione).

G1 - Adv

Note Title 9/3/2016

Campo: $(\mathbb{K}, +, \cdot, 1, 0)$

$+$ si comporta come la somma

$\cdot$ " " " " moltiplicazione

1 el. neutro di $\cdot$

0 el neutro di $+$

$\forall k \in \mathbb{K} \ \exists k' \in \mathbb{K}$ t.c. $k + k' = 0$

$\forall k \in \mathbb{K} \setminus \{0\} \ \exists k' \in \mathbb{K}$ t.c. $kk' = 1$.

Es: $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_p$ $\quad \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ (non c'è nient'altro)

$\mathbb{Q}$ sottocampo di $\mathbb{R}$ (c'è un buco di roba)

$\mathbb{Q}(\sqrt{2}) = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$

Es: $x^2 + 1 \equiv 0 \bmod 7$ non ha soluzioni

Invece II soluzione di "$x^2 + 1 \equiv 0 \bmod 7$"

$\mathbb{F}_{7^2} = \{a + \mathbb{I} b \mid a, b \in \mathbb{F}_7\}$ l'inv. esiste perché -1 non è res. quad.

$\mathbb{F}_{p^2}$ esiste ed è un campo $\forall p$ primo, a patto di aggiungere la radice di un non residuo quadratico.

$\mathbb{F}_{p^k}$

Uno **spazio vettoriale** su $\mathbb{K}$ è un insieme V con

- $+ : V \times V \to V$ una somma
- $\cdot : V \times \mathbb{K} \to V$ una molt. per scalare
- $0 \in V$ el. neutro per $+$

$(k_1 + k_2)\cdot v = k_1 \cdot v + k_2 v$ $\qquad$ $k_1 \cdot (k_2 \cdot v) = (k_1 \cdot k_2)\cdot v$

$+$ somma di $\mathbb{K}$; $v \in V$; $+$ somma di V; $\cdot$ mol. di $\mathbb{K}$; $\cdot$ molt. per scalare in V

$1 \cdot v = v$ $\qquad$ $0 \cdot v = 0$

Es: $\mathbb{R}^n = \{(x_1, \dots, x_n) \mid x_i \in \mathbb{R}\ i = 1, \dots, n\}$ sp. vett. su $\mathbb{R}$

$\mathbb{Q}^n$, $\mathbb{C}^n$, $\mathbb{F}_p^n$

Attenzione: $\mathbb{F}_p^2$ $\mathbb{F}_{p^2}$

$\mathbb{F}_p(\mathrm{II}) \simeq \mathbb{F}_p^2$

$\mathbb{F}_7(\sqrt{3}) \simeq \mathbb{F}_p^2$ $\quad$ $1+\sqrt{-1}\cdot 1$ $\quad$ $(1,1)$ $\quad$ $1+\sqrt{3}\cdot 1$

$\mathbb{R}$ $\quad$ $x^2+1 \longrightarrow \mathbb{C}$

$x^2+x+1 \longrightarrow \mathbb{R}(\xi)$

$\mathbb{F}_{p^2} \supset \mathbb{F}_p$

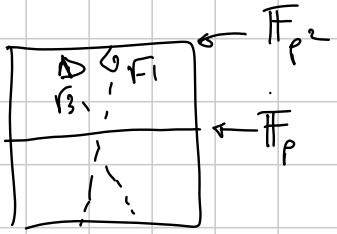
posso definire una "molt. per scalare"

$\alpha \in \mathbb{F}_p$ $\quad$ $\alpha \in \mathbb{F}_{p^2}$ $\quad$ $\alpha \cdot \alpha$

in $\mathbb{F}_{p^2}$ ho una somma

$\Rightarrow$ $\mathbb{F}_{p^2}$ è sp vett su $\mathbb{F}_p$

$\mathbb{F}_{p^2} \longleftrightarrow \mathbb{F}_p^2$



Stesso fenomeno si presenta $\mathbb{R} \subseteq \mathbb{C}$, $\mathbb{Q} \subseteq \mathbb{R}$

$\mathbb{R}$ è sp. vett. su $\mathbb{Q}$.

Dipendenza lineare: $v_1, \dots, v_n \in V$ sono linearmente dipendenti se $\exists\, \lambda_1, \dots, \lambda_n \in \mathbb{K}$ non tutti nulli t.c. $\sum \lambda_i v_i = 0$

Indip. lineare: $v_1 \dots v_n \in V$ sono linearmente indip. se $\sum \lambda_i v_i = 0$ con $\lambda_i \in \mathbb{K} \iff \lambda_i = 0 \ \forall i$

Spazio generato da $v_1, \dots, v_n \in V$

$$\langle v_1, \dots, v_n \rangle_{\mathbb{K}} = \{ \lambda_1 v_1 + \dots + \lambda_n v_n \mid \lambda_i \in \mathbb{K} \}$$

Base di V

$\{v_1, \dots, v_n\}$ base di V se
(i) sono lin. indip
(ii) $\langle v_1, \dots, v_n \rangle = V$

Teo 1: $\exists$ sempre una base.

Teo 2: Due basi possono sempre essere poste in biezione

Es non banale: $\exists$ base di $\mathbb{R}$ su $\mathbb{Q}$

$\exists\, \mathcal{B} \subseteq \mathbb{R}$ t.c. (i) gli el di $\mathcal{B}$ sono indip. su $\mathbb{Q}$
(ii) $\forall x \in \mathbb{R}\ \exists\, b_1, \dots, b_{k(x)} \in \mathcal{B}$ e $q_1, \dots, q_{k(x)} \in \mathbb{Q}$ t.c.
$x = q_1 b_1 + \dots + q_{k(x)} b_{k(x)}$

$f: \mathbb{R} \longrightarrow \mathbb{R}$ $\quad f(x+y) = f(x) + f(y)$

$\forall x \in \mathbb{R} \ \forall q \in \mathbb{Q} \quad f(qx) = q f(x)$

$\mathbb{Q}$- lineare

Es: $f: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ $\quad$ (sp. vett su $\mathbb{R}$)

$f(x+y) = f(x) + f(y) \quad \forall x, y \in \mathbb{R}^2$

$f(\lambda x) = \lambda f(x) \quad \forall x \in \mathbb{R}^2 \ \forall \lambda \in \mathbb{R}$

$\mathcal{B} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ $\quad x \in \mathbb{R}^2$

$\Downarrow$

$x = a \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad a, b \in \mathbb{R}$

$f(x) = f\left(a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = a f\begin{pmatrix} 1 \\ 0 \end{pmatrix} + b f\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Posso definire come mi pare $f\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ e $f\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Poi il resto è passato

(i) (ii)

$f\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix} \quad f\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 2 \end{pmatrix}$

$f\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 2a - b \\ 3a + 2b \end{pmatrix}$

Oss: Questo è vero anche per $f: \mathbb{R} \to \mathbb{R}$ $\mathbb{Q}$-lineare

Divagazione nella divagazione: $\nexists f: \mathbb{N} \longrightarrow \mathbb{R}$ biiettiva

$\exists f: \mathbb{N} \to \mathbb{Q}$ biiettiva $\quad \exists f: \mathbb{Q} \longrightarrow \mathbb{Q}^n$ biiettiva $\forall n$

"La base di $\mathbb{R}$ su $\mathbb{Q}$ ha tanti el. quanti $\mathbb{R}$."

↑

Base di Hamel

Se V è sp. vett. su $\mathbb{K}$, $\mathcal{B}$ è una base di V e $\#\mathcal{B} = n$,
allora $\exists F: V \to \mathbb{K}^n$ t.c.

$F(v_1+v_2) = F(v_1)+F(v_2)$
$F(\lambda v_1) = \lambda F(v_1)$ $\quad \forall v_1, v_2 \in V,\ \forall \lambda \in \mathbb{K}$
F è bigettiva

Matrici e vettori

Vettore $\rightsquigarrow \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

Matrice $\begin{pmatrix} a_{11} & \cdots & a_{1h} \\ \vdots & & \vdots \\ a_{k1} & \cdots & a_{kh} \end{pmatrix}$

$k \times h$

↑ righe ↗ colonne

$$\begin{pmatrix} a_{11} & \cdots & a_{1h} \\ \vdots & & \vdots \\ a_{k1} & \cdots & a_{kh} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_h \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{h} a_{1j} x_j \\ \sum a_{2j} x_j \\ \vdots \\ \sum a_{kj} x_j \end{pmatrix}$$

$k \times h$ $\quad h \times 1$ $\quad k \times 1$

$(k \times h) \cdot (h \times 1) = k \times 1$

$(2 \times 3) \cdot (3 \times 4) = (2 \times 4)$

$$\begin{pmatrix} 2 & 1 & 3 \\ -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 5 & 4 & 0 & -1 \\ 1 & 1 & 0 & 0 \\ 3 & 0 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 20 & 9 & 3 & 4 \\ -2 & -4 & 1 & 3 \end{pmatrix}$$

Se $f: \mathbb{K}^n \to \mathbb{K}^p$ è lineare $\Rightarrow \exists M$ matrice $p \times n$ a coeff in $\mathbb{K}$

t.c. $f(x) = M \cdot x$

Sistemi lineari

$$\begin{cases} 2x + 3y - z = 0 \\ 5x - y = 0 \\ 2x + z = 1 \end{cases}$$

$f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3 \qquad f\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2x + 3y - z \\ 5x - y \\ 2x + z \end{pmatrix}$

mi domando chi è $f^{-1}\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$

Oss: f è lineare. Infatti $f\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 & 3 & -1 \\ 5 & -1 & 0 \\ 2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}$

$$\begin{pmatrix} 2 & 3 & -1 \\ 5 & -1 & 0 \\ 2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$M \cdot x = a$ se $\exists M'$ t.c. $M'M = I$

$\Rightarrow x = M' \cdot a$

Teo: A quadrata $(n \times n)$. Sono equivalenti

(i) $\exists A^{-1}$

(ii) $A \cdot x = 0$ ha solo la soluzione nulla

(iii) $A \cdot x = b$ ha una unica soluzione $\forall b \in \mathbb{K}^n$

(iv) $\det A \neq 0$

$$\det(a_{ij}) = \sum_{\sigma \in S_n} (-1)^{|\sigma|} \cdot \prod_{j=1}^{n} a_{j\sigma(j)}$$

Oss: Se A è una matrice $n \times k$ con $k > n$

$\Rightarrow A \cdot x = 0$ ha sicuramente una sol diversa da $x = 0$

Dim:

$A = \left(A_1 \,|\, \dots \,|\, A_k \right) \qquad A_j \in \mathbb{R}^n$

$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = x_1 A_1 + \dots + x_k A_k$

se $k > n$, $A_1, \dots, A_k \in \mathbb{R}^n$ sono lin. dip. $\Rightarrow \exists x_1, \dots, x_k \in \mathbb{R}$ non $=$ "i multi che risolvono il sistema.

Osservazione sparse

1) $I_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$

I = matr. identità

J = matr. con tutti 1. $\qquad n$ – dimensione

$\det(J - I)$

$n=2 \quad \det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1$

$n=3 \quad \det \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = 2$

$n=4 \quad \det \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} =$

$= 0 \cdot \det \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} - 1 \det \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} +$

$+ 1 \cdot \det \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} - 1 \cdot \det \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} =$

$= -1 - 1 - 1 = -3$

$\det(J - I) = \sum_{\sigma \in S_n} (-1)^{|\sigma|} \cdot \prod_{j=1}^{n} a_{j\sigma(j)} \qquad D_n = (n-1)(D_{n-1} + D_{n-2})$

σ ha pt fix $\to 0$

σ non ha pt fix $\to 1$

2) A_i i-esima colonna di $A = J - I$ $\quad e_j$ = vettore con 1 in pos. j e altrimenti 0.

$\sum A_i = (n-1)\mathbb{1}$ $\qquad \sum A_i - (n-1)A_j = (n-1)e_j$

$\Downarrow$

$\langle A_1, \dots, A_n \rangle \supseteq \{e_1, e_2, \dots, e_n\}$

$\mathbb{R}^n \supseteq \langle A_1, \dots, A_n \rangle \supseteq \langle e_1, \dots, e_n \rangle = \mathbb{R}^n$

$\Rightarrow \det A \neq 0$

Matrici di incidenza

Es 1: Grafo $G = (V, E)$ $\quad \#V = n$

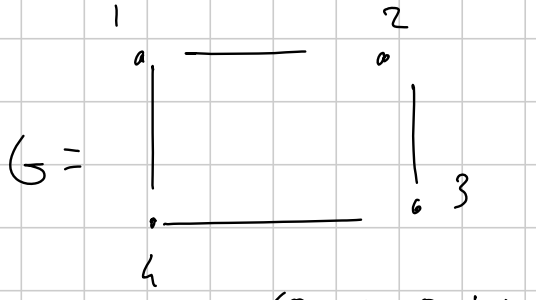
matrice di incidenza di G è $M = (m_{ij})$ $\quad n \times n$

$m_{ij} = 1 \iff (i,j) \in E$

altrimenti $m_{ij} = 0$

K_n = grafo completo su n vertici

$n = 3$ $\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$



$G =$

$M = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

Matrice simmetrica

$a_{ij} = a_{ji} \quad \forall i, j$

$A \longrightarrow (A^T)_{ij} = A_{ji}$

matrice trasposta

Prop: $\det A = \det A^T$

$(AB)^T = B^T \cdot A^T$

$(A^{-1})^T = (A^T)^{-1}$

M simm $\iff M^T = M$

$$M M^T = \begin{pmatrix} 0&1&0&1 \\ 1&0&1&0 \\ 0&1&0&1 \\ 1&0&1&0 \end{pmatrix} \cdot \begin{pmatrix} 0&1&0&1 \\ 1&0&1&0 \\ 0&1&0&1 \\ 1&0&1&0 \end{pmatrix} = \begin{pmatrix} 2&0&2&0 \\ 0&2&0&2 \\ 2&0&2&0 \\ 0&2&0&2 \end{pmatrix}$$

1 e 4

quanti vertici sono collegati a 1 e 4

$(MM^T)_{ii} = \deg(v_i)$

$(MM^T)^T = (M^T)^T M^T = M \cdot M^T$ $\quad M \cdot M^T$ è simmetrica

Es 2: X, $\#X = m$, $\mathcal{F} \subseteq \mathcal{P}(X)$, $\mathcal{F} = \{Y_1, \dots, Y_k\}$

$$M = \begin{matrix} 1 \\ 2 \\ \vdots \\ m \end{matrix} \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix} \qquad 1 \; 2 \; \dots \; k$$

$$M_{ij} = \begin{cases} 0 & x_i \notin Y_j \\ 1 & x_i \in Y_j \end{cases}$$

$MM^T =$ $\quad$ $\#\{Y_j$ che contengono $x_1 = x_k\}$

prod. scalare della 1ª riga con se stessa

$=$ quanti Y_j appartiene x_1

$M^T M =$ $\quad$ $\#Y_j$ $\quad$ $\#(Y_i \cap Y_j)$

Lemma: A matrice $n \times n$, coeff. in $\mathbb{R}$. Con tutte le entrate fuori dalla diagonale $= t \geq 0$, e gli el. sulla diagonale $> t$. Allora A è non singolare ($\det A \neq 0$).

Dim: $A = \begin{pmatrix} a & t & t & t \\ t & a & t & t \\ t & t & a & t \\ t & t & t & a \end{pmatrix}$ $\qquad A - tJ = D$ con $D_{ii} > 0 \; \forall i$

Se $t=0$ è ovvio. $t>0$.

$(tJ+D)x=0$ $\qquad D=\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$ $d_i>0$

$\parallel A$ $\qquad Dx=-tJx$ Per assurdo diciamo $\exists x\neq 0$ soluzione.

$S=x_1+\dots+x_n$ somma entrate di x $\qquad$ di $x_i=-tS$

$x_i=-\left(\frac{t}{d_i}\right)\cdot S$ Assurdo.

$\Rightarrow A$ è non singolare ☐

Esercizio: $\#X=n$ $\mathcal{F}=\{Y_1,\dots,Y_k\}$ sottoins. propri di X t.c. $\forall$ due el. di X $\exists!$ $Y_j\in\mathcal{F}$ che li contiene. Allora $|\mathcal{F}|\geq n$ $(k\geq n)$

Lem: A matrice di incidenza $k\times n$

$\{x_1,\dots,x_n\}=X$ $\qquad A_{ij}=1$ se $x_j\in Y_i$.

A^TA $n\times n$ $\qquad \Pi_{ij}=1$ $i\neq j$ $\qquad \Pi_{ii}=\#$ ins di $\mathcal{F}$ che contengono x_i.

$\parallel M$ $\qquad \Pi_{ii}\geq 1$

A^TA non è singolare. Se $n>k$ $\exists x\neq 0$ t.c. $Ax=0$

$\Rightarrow A^TAx=0$ Assurdo $\Rightarrow n\leq k$. ☐

ES: $\mathcal{F}=\{Y_1,\dots,Y_k\}\subseteq\mathcal{P}(X)$, $X=\{1,\dots,n\}$ t.c.

$\#(Y_i\cap Y_j)=t$ $\forall i\neq j$, con $1\leq t\leq n$ fissato

Allora $k\leq n$.

Dim: $A=$ la i-esima colonna dice quali el. appartengono a Y_i

A è $n\times k$

$A^T A$ $k \times k$ $\quad \Pi = A^T A$ $\quad \Pi_{ij} = t$ $i \neq j$ $\quad \Pi_{ii} = \#Y_i$

se $\exists Y_i$ con $\#Y_i$ + ho finito $\Rightarrow \Pi_{ii} > t$ $\forall i$

$\Rightarrow \det \Pi \neq 0$ ma allora $k \leq n$. (Disuguaglianza di Fisher)

Es: $A_1, \dots, A_k$ sottoins. di $\{1, \dots, n\}$, $\#A_i$ dispari $\forall i$, $\#(A_i \cap A_j)$ pari $\forall i \neq j$. Allora $k \leq n$

dim: Lavoriamo in $\mathbb{F}_2$. v_i il vettore associato a A_i $\quad i = 1, \dots, k$ $\quad v_i \in \mathbb{F}_2^n$

$\begin{cases} v_i \cdot v_j = 0 & i \neq j \\ v_i \cdot v_i = 1 \end{cases}$ ortonormale

$c_i \in \mathbb{F}_2$

$\sum_{i=1}^{k} c_i v_i = 0$

$\Rightarrow$ tutti i $c_i = 0$.

$\left\langle v_j, \sum_{i=1}^{k} c_i v_i \right\rangle = 0$

$c_j = 0$

$\Rightarrow k \leq n$.

Disuguaglianza proiettiva finita

$\mathbb{R}^3 \setminus \{(0,0,0)\} / \sim$

$\| \quad \mathbb{P}^2(\mathbb{R})$

$v \sim w \iff \exists \lambda \in \mathbb{R} \setminus \{0\}$ t.c. $v = \lambda w$

$\mathbb{F}_2^3 \setminus \{(0,0,0)\} / \sim$

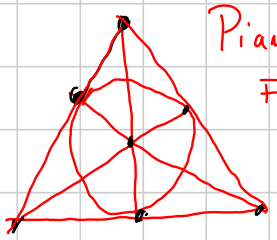
$\| \quad \mathbb{P}^2(\mathbb{F}_2)$

$\#\mathbb{P}^2(\mathbb{F}_2) = 7$

$\sim \to \mathbb{F}_2 \setminus \{0\}$

$\#(\mathbb{F}_2^3 \setminus \{(0,0,0)\}) = 7$

$\#(\mathbb{F}_2 - \{0\}) = 1$



Piano di FANO

Es A: $2n$ persone. Ognuno ha un numero pari di amici
$\Rightarrow \exists$ 2 persone con un numero pari di amici comuni.

Es B: n pari >0, $S_1 \dots S_n \subseteq \{1,\dots,n\}$ t.c. $\#S_i$ pari.
$\Rightarrow \exists i \neq j$ t.c. $\#(S_i \cap S_j)$ è pari:

——— ✗ ———

Autovalori & Autovettori

A $n \times n$ Un vettore $v \in \mathbb{R}^n \setminus \{0\}$ si dice **AUTOVETTORE** di A
se $\exists \lambda \in \mathbb{R}$ t.c. $Av = \lambda v$
λ si dice **AUTOVALORE** (RELATIVO a v)

Es: $A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ e_1 è Autovett. di autoval 1
e_2 è autovett. di autoval. 2

$$A \cdot e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$A \cdot e_2 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \end{pmatrix} = 2 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Es: $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $Ax = \lambda x$ $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$

$$\begin{cases} x_2 = \lambda x_1 \\ x_1 = \lambda x_2 \end{cases} \rightsquigarrow \begin{cases} -\lambda x_1 + x_2 = 0 \\ +x_1 - \lambda x_2 = 0 \end{cases}$$

$\det \begin{pmatrix} -\lambda & 1 \\ 1 & -\lambda \end{pmatrix} = \lambda^2 - 1$ deve essere $0 \Rightarrow \lambda^2 = 1 \Rightarrow \lambda = \pm 1$

$\lambda = 1$ $\quad \begin{cases} -x_1 + x_2 = 0 \\ x_1 - x_2 = 0 \end{cases} \rightsquigarrow \begin{pmatrix} k \\ k \end{pmatrix}$ $k \in \mathbb{R}$ ad es. $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$

$\lambda = -1$ $\quad \begin{cases} x_1 + x_2 = 0 \\ x_1 + x_2 = 0 \end{cases} \rightsquigarrow \begin{pmatrix} k \\ -k \end{pmatrix}$ $k \in \mathbb{R}$ ad es $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$

Es: $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ non ha autovett/autovalori reali.

Oss: $Av = \lambda v \iff (A - \lambda I)v = 0$

$\Rightarrow$ voglio una sol. non banale $\Rightarrow$ voglio che

$\det(A - \lambda I) = 0$

$\|$

$p_A(\lambda)$ polinomio CARATTERISTICO di A

Le radici di $p_A(\lambda)$ sono gli autovalori di A

Es: $\begin{pmatrix} 2 & & 0 \\ & \ddots & \\ 0 & & 2 \end{pmatrix}$ ha $p_A(\lambda) = (\lambda - 2)^n (-1)^n$

$\begin{pmatrix} 2 & 0 & \cdots & 0 & 1 \\ & \ddots & & 0 & \vdots \\ & & \ddots & 0 & \\ 0 & & & 2 & \end{pmatrix}$ ha $p_A(\lambda) = (2 - \lambda)^n$

$n = 3$ $\quad \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2x + z \\ 2y \\ 2z \end{pmatrix}$ $\quad z = 0 \Rightarrow \begin{pmatrix} x \\ y \\ 0 \end{pmatrix}$

$\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} x \\ 0 \\ 0 \end{pmatrix}$

Molt. algebrica di λ_i è l'esp. di $(\lambda-\lambda_i)$ nella fattorizzazione di $P_A(\lambda)$

$m.g \le m.a.$

Molt. geometrica di λ_i è il max numero di autovettori indip. relativi a λ_i = dimensione di $\{Ax=\lambda_i x\}$

Es: $X_n = X_{n-1} + X_{n-2}$

$F: \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \qquad F\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ x \end{pmatrix}$

$$F\begin{pmatrix} X_2 \\ X_1 \end{pmatrix} = \begin{pmatrix} X_3 \\ X_2 \end{pmatrix} \qquad F\begin{pmatrix} X_n \\ X_{n-1} \end{pmatrix} = \begin{pmatrix} X_{n+1} \\ X_n \end{pmatrix}$$

$$F\begin{pmatrix} x \\ y \end{pmatrix} = \underset{A}{\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

$$\det(A-\lambda I) = \det\begin{pmatrix} 1-\lambda & 1 \\ 1 & -\lambda \end{pmatrix} = -\lambda(1-\lambda) - 1 = \lambda^2 - \lambda - 1$$

$$\frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2}$$

$\frac{1+\sqrt{5}}{2} \longrightarrow \begin{pmatrix} \frac{1-\sqrt{5}}{2} & 1 \\ 1 & \frac{-1-\sqrt{5}}{2} \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = 0 \qquad y = \frac{\sqrt{5}-1}{2}x$

$v_+ = \begin{pmatrix} 2 \\ \sqrt{5}-1 \end{pmatrix}$ autovett.

$\frac{1-\sqrt{5}}{2} \longrightarrow \begin{pmatrix} \frac{1+\sqrt{5}}{2} & 1 \\ 1 & \frac{\sqrt{5}-1}{2} \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = 0 \qquad y = -\frac{1+\sqrt{5}}{2}x$

$v_- = \begin{pmatrix} -2 \\ 1+\sqrt{5} \end{pmatrix}$ autovett.

$$\begin{pmatrix} x_1 \\ x_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad \begin{pmatrix} x_{10} \\ x_9 \end{pmatrix} = F^9 \begin{pmatrix} x_1 \\ x_0 \end{pmatrix} = A^9 \begin{pmatrix} x_1 \\ x_0 \end{pmatrix}$$

$$\begin{pmatrix} x_1 \\ x_0 \end{pmatrix} = \alpha v_+ + \beta v_- \qquad \lambda_\pm = \frac{1 \pm \sqrt{5}}{2}$$

$$A^9 (\alpha v_+ + \beta v_-) = \alpha (A^9 v_+) + \beta (A^9 v_-) =$$

$$A v_\pm = \lambda_\pm v_\pm \qquad A^n v_\pm = \lambda_\pm^n v_\pm$$

$$= \alpha \lambda_+^9 v_+ + \beta \lambda_-^9 v_-$$

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \alpha \begin{pmatrix} 2 \\ \sqrt{5}-1 \end{pmatrix} + \beta \begin{pmatrix} -2 \\ \sqrt{5}+1 \end{pmatrix}$$

$$\begin{cases} 2(\alpha - \beta) = 1 \rightsquigarrow \alpha - \beta = \frac{1}{2} = \frac{5}{10} \\ \sqrt{5}(\alpha+\beta) - (\alpha - \beta) = 1 \rightsquigarrow \alpha + \beta = \frac{3}{2\sqrt{5}} = \frac{3\sqrt{5}}{10} \end{cases}$$

$$\alpha = \frac{5+3\sqrt{5}}{20} \qquad \beta = \frac{-5+3\sqrt{5}}{20}$$

Non è sempre possibile trovare

$v_1, \dots, v_k \quad k = \text{m.a.}(A)$

indip. e autovettori.

Però se ne posso trovare $h < k \Rightarrow$ posso trovare k vettori indip, divisi in h sottoinsiemi

$v_i, w_{i,1}, \dots, w_{i,j_i}$ $\qquad v_i = w_{i,0}$

autovettore $\qquad A w_{i,p} = \lambda w_{i,p} + w_{i,p-1}$

5, 2 v_1 v_2

$$A w_{i,1} = \lambda w_{i,1} + v_i$$

$$A^2 = \lambda^2 w_{i,1} + \lambda v_i + \lambda v_i = \lambda^2 w_{i,1} + 2\lambda v_i$$

$$A^n = \lambda^n w_{i,1} + n \lambda^{n-1} v_i$$

$$\begin{pmatrix} d & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & d \end{pmatrix} \leftarrow$$

Senior 2016 - Misc 2 Advanced (Anér)

Note Title 9/4/2016

DISEGUAGLIANZE FUNZIONALI

① RMM 11/1 | Trovare due funzioni $f, g : \mathbb{R} \to \mathbb{R}$ tali che $f \circ g$ è crescente e $g \circ f$ è decrescente. (in senso stretto)
(risolvere lo stesso problema anche su $\mathbb{Z}$)

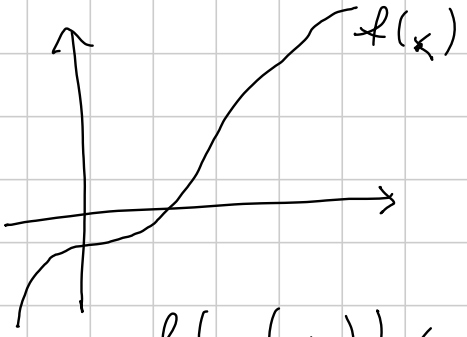
② Trovare le funzioni $f : \mathbb{R}^+ \to \mathbb{R}^+$ t.c.
$$f(x) \cdot f(y) = 1000 \cdot f(x + y f(x))$$
$\forall x, y \in \mathbb{R}^+$

③ Sia $F : \mathbb{R} \to \mathbb{R}$ una funzione. Allora
$\exists x, y \in \mathbb{R}$ t.c. $f(x - F(y)) > y F(x) + x$
(IMO SL 09)

④ $f : \mathbb{N}_{>0} \to \mathbb{N}_{>0}$ $\quad f(m+n) \geq f(m) + f(f(n)) - 1$
$\forall m, n$. Trovare i possibili valori di
$f(2007)$ (IMO SL 07)

---

f, g iniettive perché $f(g(x))$ e $g(f(x))$ lo sono
ci accorgiamo che le funzioni continue falliscono



$f(g(x))$

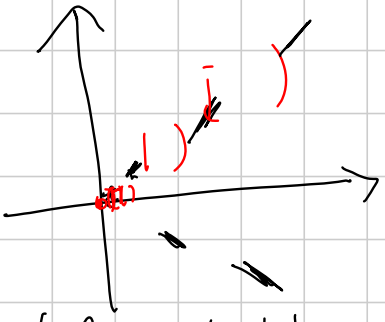
$f(x_1) < f(x_2) \iff x_1 < x_2$

$f(g(x_1)) < f(g(x_2)) \iff g(x_1) < g(x_2)$

$x_2 > x_1$

$g(f(x))$ $\quad g(x_1) < g(x_2) \iff x_1 < x_2$

$g(f(x_1)) < g(f(x_2)) \iff f(x_1) < f(x_2)$



$f(x) = (-1)^{\lfloor \log_2 |x| \rfloor + 1} \cdot x$

$g(x) = (-1)^{\lfloor \log_2 |x| \rfloor} \cdot 2x$

$f(0) = g(0) = 0$

$\lfloor \log_2 |x| \rfloor$ pari $\quad f(x) = -x \quad g(f(x)) = -2x$

$g(x) = 2x \quad f(g(x)) = 2x$

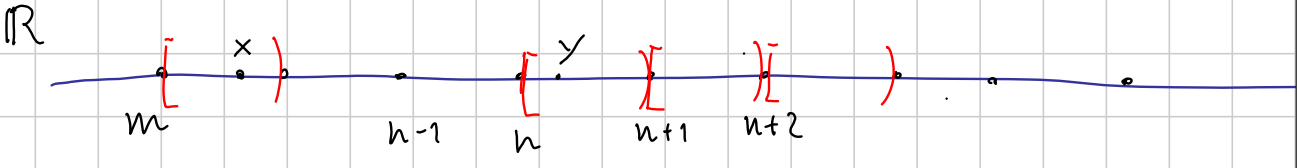
$\lfloor \log_2 |x| \rfloor$ dispari $\quad f(x) = x \quad g(f(x)) = -2x$

$f(g(x)) = 2x$

$f(g(x)) = 2x \quad g(f(x)) = -2x$

Stesso problema su $\mathbb{Z}$

Motivazione Risolto su $\mathbb{Z}$, si può forse anche risolvere su $\mathbb{R}$



Supponga di avere $\tilde{f}, \tilde{g} : \mathbb{Z} \to \mathbb{Z}$ con $\tilde{f}\circ\tilde{g}$ cresc. e $\tilde{g}\circ\tilde{f}$ decr.

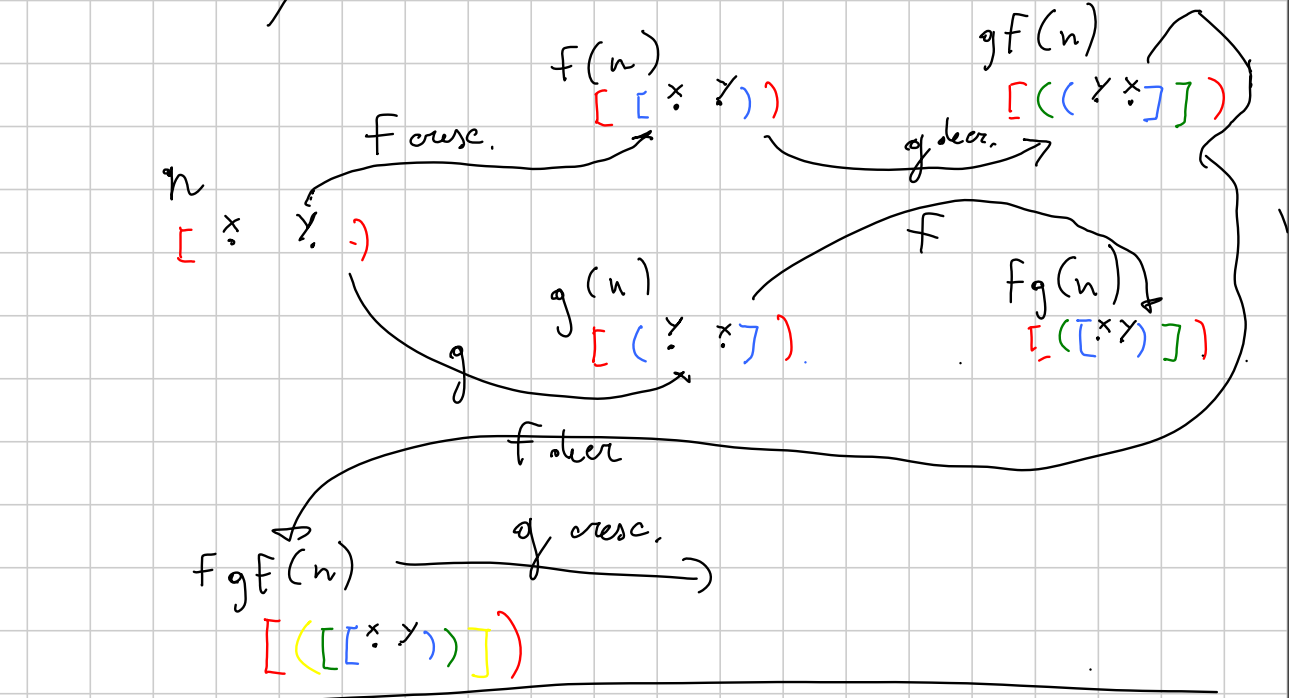
Idea: f mapperà l'intervallo associato a n all'interno dell'int. associato a $\tilde{f}(n)$
idem per g e $\tilde{g}$.

In questo modo, se x è "vicino" a m e y è "vicino" a n, con $m<n$ (anche $x<y$)

$g(f(x))$ è vicino a $\tilde{g}\tilde{f}(m)$ e $gf(y)$ è vicino a $\tilde{g}\tilde{f}(n)$

quindi, poiché $\tilde{g}\tilde{f}(m) > \tilde{g}\tilde{f}(n)$, allora
$gf(x) > gf(y)$, che è ciò che volevamo.

E se x e y sono vicini allo stesso n?



---

(2) Dimostrare che $f(x) \geq 1 \quad \forall x > 0$

$$f(x)\cdot f(y) = 1000 \cdot f(x + y f(x))$$

(Riesco a trovare x e y per cui $y = x + y f(x)$?
$y = \frac{x}{1 - f(x)}$ si risolve (in $\mathbb{R}^+$) se $f(x) < 1$)

Se per assurdo $\exists x$ t.c. $f(x) < 1$, trovo y come sopra e semplifico i fattori $\Rightarrow f(x) = 1000$ ma $f(x) < 1$

$x = y$

$f(x)^2 = 1000 \cdot f\left(x + x f(x)\right) \geq 1000$

$\forall x > 0 \quad f(x) \geq \sqrt{1000} = 1000^{\frac{1}{2}}$

Uso lo stesso ragionamento

$f(x)^2 = 1000\, f(\quad\quad) \geq 1000 \sqrt{1000} = 1000^{\frac{3}{2}}$

$\forall x > 0 \quad f(x) \geq 1000^{\frac{3}{4}}$

$\forall x > 0 \quad f(x) \geq 1000^{\frac{7}{8}}$ . . . .

I numeri $1, \sqrt{1000}, 1000^{\frac{3}{4}}, 1000^{\frac{7}{8}}, 1000^{\frac{15}{16}}, \ldots$ tendono a 1000 e $\forall x > 0$ $f(x) \geq$ tutti questi numeri. Quindi $f(x) \geq 1000$

$f(x) \underbrace{f(y)}_{\forall\, 1000} = \underline{1000}\, \underbrace{f\left(x + y f(x)\right)}_{\forall\, f(x)}$

$f(x) \leq f\left(x + y f(x)\right) \qquad \forall x, y > 0$

al variare di $y > 0$ è il generico reale positivo

f debolmente crescente.

$f\left(x + y f(x)\right) = f\left(y + x F(y)\right) \qquad \forall x, y > 0$ (simmetria equazione)

Se f fosse iniettiva, avrei (con qualche passaggio...) f lineare. Sostituisco ma non funziona.

$\exists\, a < b$ con $f(a) = f(b)$, ma allora f è costante su $[a, b]$

$x = a$

$$f(a)\,f(y) = 1000 \cdot f(a + y\,f(a))$$

Se y è tra 0 e $\dfrac{b-a}{f(a)}$, allora questo numero è $\le b$

Otteniamo $f(y) = 1000$ su un intervallo $(0, \varepsilon)$

$$f(y)^2 = 1000 \cdot f(y + y \cdot 1000)$$

$f(y)^2 = 1000^2$; $f(y + y \cdot 1000) = 1000$

Ma $y \cdot 1001$ è il generico numero in $(0, 1001\,\varepsilon)$

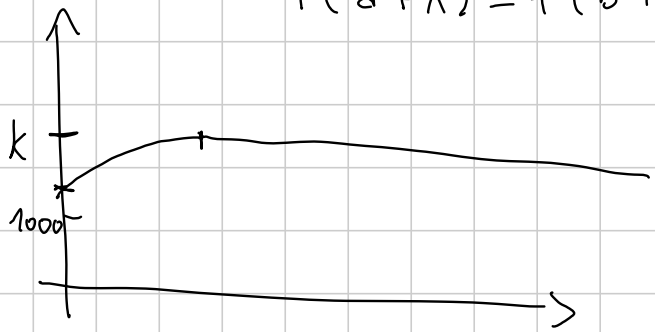
Conclusione l'intervallo...

$\exists\, a < b : f(a) = f(b)$

$$f(a + y f(a)) = \frac{f(a) f(y)}{1000} = \frac{f(b) f(y)}{1000} = f(b + y f(a))$$

λ

$$f(a + \lambda) = f(b + \lambda)$$



$\alpha \in \mathrm{Im} f$

$\beta \in \mathrm{Im} f$

$\dfrac{\alpha\beta}{1000} \in \mathrm{Im} f$

$\dfrac{k^2}{1000} > k$

(3) Per assurdo, $\forall x, y \in \mathbb{R}$

$$f(x - F(y)) \leq y f(x) + x$$

$y = 0$ | $f(x - F(0)) \leq x \Rightarrow \forall x \in \mathbb{R} \quad f(x) \leq x + f(0)$

Abbiamo $f(0) = a$

$x = F(y)$ |

$$a \leq y f f(y) + f(y) \leq y f f(y) + y + a$$

$$y \cdot (f f(y) + 1) \geq 0 \qquad \forall y \in \mathbb{R}$$

Quindi se $y > 0$ allora $f f(y) \geq -1$

se $y < 0$ allora $f f(y) \leq -1$

$$f f(y) \leq f(y) + a \Rightarrow \boxed{f(y) \geq -1 - a \text{ se } y > 0}$$

$f f(y)$ vi -1

$$f(x - F(y)) \leq y f(x) + x$$

Vorrei $x - F(y)$ positivo, ma so che $x - f(y) \geq x - y - a$ Vorrei 0

(così LHS $\geq -1 - a$)

vorrei $y < x - a$

Per y piccolo ($y \to -\infty$) $\quad -1 - a \leq y f(x) + x \Rightarrow F(x) \leq 0 \quad \forall x \in \mathbb{R}$

$f(0) \le 0$ in particolare ; $f(x) \le x$

$x = f(y) + \lambda$ | Se $y \to \infty$ questo rischia di $\to -\infty$

$$f(\lambda) \le y \cdot f(f(y)+\lambda) + f(y) + \lambda$$

"tendere a"

$f(f(y)+\lambda)$ deve essere 0 (fissato λ, per y grande)

$f(y) + \lambda \le \lambda$ prendo $\lambda = -1$ e ho finito

$$f(\lambda) \le y\, f(f(y)+\lambda) + f(y) + \lambda \le y(f(y)+\lambda) + 0 + \lambda$$

---

(4) $\in (2007)$ $\quad f: \mathbb{N}_{>0} \to \mathbb{N}_{>0}$

$f(m+n) \ge f(m) + f(f(n)) - 1$

$f(n) = \lfloor \lambda n \rfloor \qquad \lambda \le 1$

$\lfloor \lambda m + \lambda n \rfloor \ge \lfloor \lambda m \rfloor + \lfloor \lambda \lfloor \lambda n \rfloor \rfloor - 1$ $\qquad \lambda n \le n$, $\lfloor \lambda n \rfloor \le n$

$\lfloor \lambda m + \lambda n \rfloor \ge \lfloor \lambda m \rfloor + \lfloor \lambda n \rfloor$ $\qquad \lceil \lambda m + \lambda n \rceil \ge \lceil \lambda m \rceil + \lceil \lambda n \rceil - 1$

$\lfloor \alpha + \beta \rfloor \ge 0$ $\qquad f(2007) = \lfloor \lambda 2007 \rfloor$ $\qquad a + \alpha = \lambda m$, $b + \beta = \lambda n$

$\lceil \alpha + \beta \rceil \ge \lceil \alpha \rceil + \lceil \beta \rceil - 1$

$f(m+1) \ge f(m) + f(f(1)) - 1 \ge f(m)$

$f(n) = n + k$

$f(n+k) \ge f(k) + f(n+k) - 1$

$1 \ge f(k)$

$f(k) = 1$

$f(n) = n + k$

$f(n+n) \geq f(n) + f(n+k) - 1 \geq 2f(n) - 1 \geq 2n + (2k-1)$

$2k - 1 > k$ so $k \geq 2$

$f(n) = \begin{cases} n & \text{se } 2007 \nmid n \\ n+1 & \text{se } 2007 \mid n \end{cases}$

$f(m+n) \geq f(m) + f(f(n)) - 1$

$m+n+1 \geq m+n+1$

Ricerca degli esempi

$f(m+n) \geq f(m) + ff(n) - 1$

$f(n) = n$ soddisfa

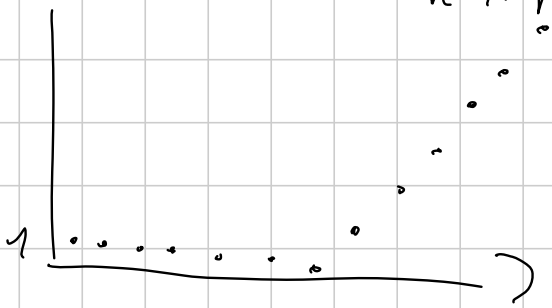
Quando $f(n) = n + k$ funziona?

$m + n + k \geq m + k + n + 2k - 1$

$2k \leq 1$

va bene qualsiasi $k \leq 0$
(in linea di principio)

$n - k$ per n grande



prendo

$f(n) = \max\{n-k, 1\}$

$f(m+n) \overset{?}{\geq} f(m) + ff(n) - 1$

oss f è debb. crescente, quindi se $ff(n) = 1$

allora $f(m+n) \geq f(m)$

Se $f(m) = 1$ allora $f(m+n) \geq ff(n)$ comunque

(verificare ...)

Per $f(2007) = 2008$ va bene anche

$$f(n) = n + 1 \,|_{3 \nmid n}$$

N2 Advanced Tess

Note Title 9/5/2016

Estensioni di campi, in particolare campi finiti;

→ successioni per ricorrenza lineari mod p

Def: $(K, +, \cdot)$ è un campo se
$+$ e $\cdot$ soddisfano: assoc., commut., distr. but. tra
$\exists\, 0, \exists\, 1, \exists\, x^{-1}\ \forall x \neq 0$

Esempi: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ $\mathbb{Z}/p = \mathbb{F}_p$

$\mathbb{R}(x) = \{$ frazioni di polinomi a coeff. in $\mathbb{R}\}$

Def: se K, L sono campi con $K \subseteq L$
L è estensione di K

Esempi: $\mathbb{Q} \subseteq \mathbb{R}$ $\mathbb{R} \subseteq \mathbb{C}$ $\mathbb{Q} \subseteq \mathbb{C}$
$K \subseteq K(x)$
non è vero che $\mathbb{F}_p \subseteq$ qualcuno di questi

infatti: $\mathbb{F}_2 = \mathbb{Z}/2 \not\subseteq \mathbb{R}$
altrimenti: $1+1 \neq 0$
però $\mathbb{F}_2 \subseteq \mathbb{F}_2(x)$

Definiamo la caratteristica di un campo:

Oss: $1 \in K$, $1;\ 1+1;\ 1+1+1; \ldots$

se ci sono 2 termini uguali, allora la diff è 0, cioè $\underbrace{1+1+\dots+1}_{n \text{ volte}} = 0$ ← posso prendere il + piccolo

altrimenti non succede mai (es: $\mathbb{Q}, \mathbb{R}$)

la caratteristica di K è n (se esiste)
altrimenti è 0

Es: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ecc. hanno char $= 0$
$\mathbb{F}_p$ ha char $= p$

Oss: non ci sono K t.c. char $= 1$ (altrimenti: $1 = 0$)

non ci sono K t.c. char $= n$ non primo

altrimenti, $n = ab = \underbrace{(1+\dots+1)}_{a \text{ volte}} \underbrace{(1+\dots+1)}_{b \text{ volte}} = 0$

divido per a e ottengo $b = 0$

Oss: ogni campo contiene $\mathbb{Q}$ oppure uno degli $\mathbb{F}_p$

in particolare: se char $K = p$
$\{0, 1, 1+1, \dots, p-1\} \subseteq K$
si comporta esattamente come $\mathbb{F}_p$

se char $K = 0$
allora $\mathbb{N} \subseteq K$, ma allora anche $\mathbb{Z} \subseteq K$, e anche $\mathbb{Q} \subseteq K$.

Def: se K è un campo, $\mathbb{Q}$ o $\mathbb{F}_p$ è il campo fondam. di K (a seconda della caratteristica)

Allora ogni campo è estensione di un campo fondamentale

Def: se $K \subseteq L$ è un estensione un elemento $\alpha \in L$ è algebrico se $\exists\, p \in K[x]$ t.c. $p(\alpha) = 0$

$K \subseteq L$, se $\forall \alpha \in L$ è algebrico, allora $K \subseteq L$ è estensione algebrica

Esempi: $\mathbb{R} \subseteq \mathbb{C}$ se $z \in \mathbb{C}$, z è zero di $p(x) = (x-z)(x-\bar{z})$
$\rightarrow$ è est. algebrica

$\mathbb{Q} \subseteq \mathbb{R}$ ad es $\sqrt[7]{2}$ è algebrico $(p(x) = x^7 - 2)$
però ci sono elementi non algebrici (ad es. π, e)

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$
$\uparrow$
è algebrica infatti: $a + b\sqrt{2}$ soddisfa $p(x) = (x - a - b\sqrt{2})(x - a + b\sqrt{2})$

anche $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[7]{2})$ è algebrica ...

Piccola osservazione, se $K \subseteq L$ $\quad \mathbb{R} \subseteq \mathbb{C}$

[es: in $\mathbb{R} \subseteq \mathbb{C}$, $r \cdot z \in \mathbb{C}$ $\forall r \in \mathbb{R}, z \in \mathbb{C}$]

allora L è uno spazio vettoriale su K

quindi $\exists$ una base di L su K $\quad B = \{b_i\} \subseteq L$

chiamo grado dell'estensione $[L:K] = \#B$

Es: $[\mathbb{C}:\mathbb{R}] = \#\{1, i\} = 2$

$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$

$[\mathbb{Q}(\sqrt[7]{2}):\mathbb{Q}] = 7$

$1, \sqrt[7]{2}, \sqrt[7]{2}^2, \sqrt[7]{2}^3, \dots, \sqrt[7]{2}^6$

sono indip. perché altrimenti:

$\lambda_0 + \lambda_1 \sqrt[7]{2} + \dots + \lambda_6 \sqrt[7]{2}^6 = 0$

$\Rightarrow \sqrt[7]{2}$ è radice di $p(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_6 x^6$

$\circlearrowleft \mathbb{Q}[x]$

ma anche $q(x) = x^7 - 2$ ha come radice $\sqrt[7]{2}$

ma q è irriducibile su $\mathbb{Q}$ (per Eisenstein)

quindi $(q, p) = 1$ ma allora non possono avere una radice in comune

Se ho un campo K e un polinomio $p \in K[x]$ allora esiste $K \subseteq L$ t.c. p ha tutte le radici in L

Se p è irriducibile, posso fare $\frac{K[x]}{p(x)}$ ← modulo

Esempio: x^2+1, $\mathbb{R}$

$$\frac{\mathbb{R}[x]}{x^2+1} = \{a+bx : a,b \in \mathbb{R}\}$$

ma $x^2 \equiv -1 \pmod{x^2+1}$
quindi la x è come la i

Sia $a+bx \in \frac{\mathbb{R}[x]}{x^2+1}$

dato che x^2+1 è irr allora $(x^2+1, a+bx) = 1$

allora $\exists\, p,q \in \mathbb{R}[x]$ t.c. $(x^2+1)p + (a+bx)q = 1$
↑ è l'inverso di $a+bx$

Serve che x^2+1 è irr.

Se x^2-1, $\frac{\mathbb{R}[x]}{x^2-1}$ $\quad x+1, x-1 \in \frac{\mathbb{R}[x]}{x^2-1}$

$(x+1)(x-1) \equiv 0$

ma $x+1, x-1 \neq 0$ e vorrei fossero invertibili, per avere un

campo.

Con questa costruzione, dato ~~$p(x)$~~ riesco a trovare L

$p(x) = p_1(x) \cdot \ldots \cdot p_n(x)$ ← fatt. in K.

Posso ottenere $K \subseteq L_1$ aggiungendo una radice di $p_1(x)$

(se faccio $\frac{K[x]}{p_1(x)}$, qui x è una radice di $p_1(x)$)

allora $p(x) = q_1(x) \cdot \ldots \cdot q_m(x)$ ← fatt. in L_1
e $m > n$ perché $p_1(x)$ si spezza

$K \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L$

Campi finiti

Sia K un campo con finiti elementi

Oss: $\mathrm{char} K = p$

$\mathbb{F}_p \subseteq K \Rightarrow K$ è $\mathbb{F}_p$ sp. vett.

$\Rightarrow \exists\, B$ base (finita)
$= \{b_1, \ldots, b_n\}$

$\Rightarrow \forall\, \alpha \in K$, $\alpha = \lambda_1 b_1 + \dots + \lambda_n b_n$ (con $\lambda_i \in \mathbb{F}_p$)

$\Rightarrow \# K = p^n$

Sia $\alpha \in K \setminus \{0\}$ campo finito

$1, \alpha, \alpha^2, \dots$ $\exists\, m$ t.c. $\alpha^m = 1$

Se $K = \mathbb{F}_p$ basta $m = p-1$ (LFT)

sicuramente $m \le p^n - 1$, ma in realtà $\alpha^{p^n-1} = 1$ $\forall\, \alpha$

Dim: $\{1, 2, \dots, \alpha, \alpha+1, \dots\} = K \setminus \{0\}$

sia $\beta \in K \setminus \{0\}$

$\{\beta, 2\beta, \dots, \beta\alpha, \beta(\alpha+1), \dots\} = K \setminus \{0\}$

$x \mapsto \beta x$ è iniettiva infatti: $\beta x = \beta y \Rightarrow x = y$ (↑ divido per β)

$$P = \prod_{\alpha \in K\setminus\{0\}} \alpha = \prod_{\alpha \in K\setminus\{0\}} \beta\alpha = P \cdot \beta^{p^n-1}$$

$P \neq 0 \Rightarrow \beta^{p^n-1} = 1$

Quindi $\forall\, \alpha \in K$, α è radice di $X^{p^n} - X$

Anche in questo caso $\exists$ g generatore di $K \setminus \{0\}$

Voglio dim. che $\exists\ \alpha \in K^* := K \setminus \{0\}$ t.c.
$\mathrm{ord}_{K^*}(\alpha) = p^n - 1$

$\forall\ \alpha \in K^*$, $\mathrm{ord}(\alpha) \mid p^n - 1$

$\mathrm{ord}(\alpha) = m$

quanti elementi esistono di ord $= m$? (al max)

sicuramente $x^m - 1$ ha al max m radici;

però se $\mathrm{ord}(\alpha) = m$ α è radice di $x^m - 1$
e non di $x^k - 1$ per $k < m$

(volendo, per inversione di Moebius) otteniamo che

$\#\{\alpha : \mathrm{ord}(\alpha) = m\} \leq \varphi(m)$

D-C su K^* $\quad p^n - 1 = \sum_{m \mid p^n - 1} \#\{\alpha : \mathrm{ord}(\alpha) = m\}$

$$\leq \sum_{m \mid p^n - 1} \varphi(m) = p^n - 1$$

$\Rightarrow$ devono essere tutte $=$
$\Rightarrow$ $\exists\ \varphi(p^n - 1)$ generatori.

$\mathbb{F}_2 = \{0, 1\}$ $\mathbb{F}_4$ si può costruire con x^2+x+1

$= \{0, 1, \alpha, \alpha+1\}$

(poi $\alpha^2 = \alpha+1$, $\alpha(\alpha+1) = 1$ ecc.)

$\mathbb{F}_8$ con x^3+x+1

$= \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$

$\mathbb{F}_{16}$ x^4+x+1 (non ha radici, e l'unico polinomio irr. di deg $=2$ è x^2+x+1, ma $(x^2+x+1)^2 = x^4+x^2+1$)

$= \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1,$
$\alpha^3, \alpha^3+1, \alpha^3+\alpha, \alpha^3+\alpha+1, \alpha^3+\alpha^2, \alpha^3+\alpha^2+1, \alpha^3+\alpha^2+\alpha, \alpha^3+\alpha^2+\alpha+1\}$

$(\alpha^2+\alpha)^2 + (\alpha^2+\alpha) + 1 = \alpha^4 + \alpha + 1 = 0$

$\Rightarrow$ $\alpha^2+\alpha$ è radice di x^2+x+1

Abbiamo trovato $\mathbb{F}_4 \subseteq \mathbb{F}_{16}$

Supponiamo $K \subseteq L$ (finiti)

$\Rightarrow \#L = (\#K)^m$ (perché $\exists$ Base e ogni $\alpha \in L$ si scrive come combinazione lineare a coeff. in K)

Se $\#L = (\#K)^m \Rightarrow K \subseteq L$

infatti: $\alpha \in L \Rightarrow \alpha^{p^{n\cdot m}-1} = 1$, $\beta \in K \Rightarrow \beta^{p^n-1} = 1$

$p^n - 1 \mid p^{n\cdot m} - 1$, $\exists\, \beta \in L$ t.c. $\beta^{p^n-1} = 1$

ma si ha anche che $x^{p^n} - x$ ha tutte le radici in L, infatti: $x^{p^n} - x \mid x^{p^{nm}} - x$ ← ha tutte le radici

e K è unico! (infatti: tutti gli elementi di K devono soddisfare $x^{p^n} - x = 0$)

Thm: Se $\exists\, \mathbb{F}_{p^n}$ è unico e

$$\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \iff n \mid m$$

Osserviamo, infatti, che se α, β sono radici di $x^{p^n} - x$, anche $\alpha+\beta$, $\alpha\beta$ sono radici di $x^{p^n} - x$ ($-\alpha$, α^{-1})

se $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta \Rightarrow (\alpha\beta)^{p^n} = \alpha\beta$

e $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$

↑ i coeff. binomial: $= 0$

Es: ci sono polinomi irriducibili su $\mathbb{Q}$ ($\mathbb{Z}$) che sono riducibili mod p $\forall p$

$x^4 + 1 = (x^2 + i)(x^2 - i)$ vale su $\mathbb{F}_{p^2}$

$= (x^2 + 1 + \sqrt{2}x)(x^2 + 1 - \sqrt{2}x)$ "

$= (x^2 - 1 + \sqrt{-2}x)(x^2 - 1 - \sqrt{-2}x)$

infatti $\not\ni i \in \mathbb{F}_p \subseteq \mathbb{F}_{p^2}$

$\not\ni i \in \mathbb{F}_{p^2}$

Se $i \in \mathbb{F}_p$, o se $\sqrt{2} \in \mathbb{F}_p$ è già riducibile

altrimenti -2 è un quadrato e $\sqrt{-2}$ è in $\mathbb{F}_p$

Quando $\mathbb{F}_p \subseteq \mathbb{F}_{p^2}$ tutti i polinomi di secondo grado si spezzano cioè ho le radici

infatti $(x^2-a)(x^2-b) = p(x)$

$\exists\, L \supseteq \mathbb{F}_p$ t.c. in L ci sono le radici di p

però $L \supseteq \mathbb{F}_p(\sqrt{a})$, ma $\mathbb{F}_p(\sqrt{a}) = \mathbb{F}_{p^2}$

$\supseteq \mathbb{F}_p(\sqrt{b})$ $\mathbb{F}_p(\sqrt{b}) = \mathbb{F}_{p^2}$

Sia $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$

$x \mapsto x^p$

$$\phi(xy) = \phi(x)\phi(y)$$

$$\phi(x+y) = \phi(x) + \phi(y)$$

$(x+y)^p = x^p + y^p$; i coeff. binomiali sono $= 0$

Sia $q(x)$ un polinomio $\in \mathbb{F}_p[x]$

se $\alpha \in \mathbb{F}_{p^n}$ è radice, allora $q(\alpha) = 0$

$$0 = \phi(q(\alpha)) = q(\alpha^p)$$
$$= \phi\left(\sum_i c_i \alpha^i\right) = \sum_i \phi(c_i \alpha^i)$$
$$= \sum_i \phi(c_i)(\phi(\alpha))^i \qquad \phi(c_i) = c_i \in \mathbb{F}_p,\ c_i^p = c_i$$
$$= \sum_i c_i (\alpha^p)^i$$
$$= q(\alpha^p)$$

$\Rightarrow \alpha^p$ è radice!

$\Rightarrow \alpha^{p^k}$ sono tutte radici di q

(È vero che, se q è irriducibile su $\mathbb{F}_p$, α^{p^k} sono tutte le radici di q)

Es: Sia $q(x) = x^3 - 3x - 1$, sia p un primo t.c. $q(x)$ è irriducibile mod p, sia α una radice di $q(x)$

$$\alpha^{p^2+p+1} = 1$$

(perché $\alpha, \alpha^p, \alpha^{p^2}$ sono le radici di q e sono diverse, altrimenti: $\alpha^p = \alpha \Rightarrow \alpha \in \mathbb{F}_p$, $\alpha^p = \alpha^{p^2}$ no e neanche $\alpha = \alpha^{p^2}$ no, perché sono in $\mathbb{F}_{p^3}$, $\alpha^p \in \mathbb{F}_p$, $\alpha^{p \cdot n} = \alpha \in \mathbb{F}_p$ $(p, \operatorname{ord}\alpha) = 1$

Irriducibilità dei $\Phi_n(x)$ su $\mathbb{Z}$

Dim: Supponiamo che $f(x) \mid \Phi_n(x)$ sia irriducibile

allora $f(x) = (x-\xi_1)\cdot\ldots\cdot(x-\xi_m)$ $\quad \xi_1 = \xi$

dimostriamo che se $(p,n)=1 \Rightarrow \xi^p$ è radice di f

da qui ho vinto perché ogni ξ' radice di $\Phi_n(x)$

è t.c. $\xi' = \xi^k$ $\quad (k,n)=1$ con k opportuno.

$$g(x) = (x-\xi^p)\cdot(x-\xi_2^p)\cdot\ldots\cdot(x-\xi_m^p)$$

I coeff. di $g(x)$ sono funzioni polinomiali simmetriche in $\xi^p, \ldots, \xi_m^p$ quindi anche in $\xi, \ldots, \xi_n$

quindi sono interi perché polinomi a coefficienti interi valutati sui coeff. interi di f.

siano $g_1, \ldots, g_m$ e $f_1, \ldots, f_m$ i coeff. di grado $1, \ldots, m$

allora $g_i \equiv f_i \mod p$

$$f_i = e_i(\xi, \ldots, \xi_m), \quad g_i = e_i(\xi^p, \ldots, \xi_m^p)$$

e_i: funzione simm. elem. i-esima

$$e_i(x_1, \ldots, x_m)^p \equiv e_i(x_1^p, \ldots, x_m^p) \mod p$$

$e_i(x_1^p, \dots, x_m^p) = e_i(x_1, \dots, x_m)^p + p\, f(x_1, \dots, x_m)$ ← simmetrico

valuto in $x_1, \dots, x_m = \xi, \dots, \xi^m$

e ottengo $g_i = f_i^p + p \cdot \text{intero}$

mod p $\quad g_i \equiv f_i^p \equiv f_i$

Se $f(x)$ ha ξ^p come radice sono contento

altrimenti $g(x) \neq f(x)$, quindi sono coprimi perché f è irr. e $\deg g = \deg f$

inoltre g è irr., altrimenti: $g = a \cdot b$ ←

e come sono passato da f a g elevando alla p

così posso ottenere f da g elevando alla $p^{-1} \bmod n$

$a(\xi^p) = 0 \Rightarrow a^1(x)$ con radici: quelle di a elevate alla $p^{-1} \bmod n$

quindi c'è anche ξ

quindi $a^1 \in \mathbb{Z}[x]$ e $f \mid a^1$

ma $\deg f = \deg g > \deg a = \deg a^1 \geq \deg f$ ↑

$f(x) \mid \Phi_n(x)$

$g(x) \mid \Phi_n(x)$

$\Rightarrow f(x) g(x) \mid \Phi_n(x) \mid x^n - 1$

assurdo mod p:

$\bar{f} \cdot \bar{g} = \bar{f}^2 \mid x^n - 1$ assurdo

perché per il test derivata x^{n-1} ha radici doppie $\iff$ le condivide con la derivata $= n x^{n-1} \equiv x^{n-1}$

Successioni per ricorrenza mod p

Come al solito, se scrivete il polinomio caratteristico della ricorrenza e avete le radici (per esempio, supponiamole distinte)

$$\Rightarrow a_n = \lambda_1 r_1^n + \lambda_2 r_2^n + \dots + \lambda_m r_m^n$$

con $r_1, \dots, r_m$ radici di $t^m - \dots = 0$ (il pol. caratt.)

$a_{n+2} = a_{n+1} + a_n$ $\quad t^2 - t - 1$

mod $p = 11$ si ha che $t^2 - t - 1 = (t-4)(t+3)$

quindi $a_n = \lambda_1 4^n + \lambda_2 (-3)^n$

quindi è periodica di periodo $\mid 10$

mod 3 non c'è la radice ma posso scrivere

$t^2 - t - 1 = \left(t - \frac{1+\sqrt{5}}{2}\right)\left(t - \frac{1-\sqrt{5}}{2}\right)$ in $\mathbb{F}_9$

$\overset{!}{=} (t + (1+\sqrt{-1}))(t + (1-\sqrt{-1}))$

$\overset{!}{=} (t + (1+i))(t + (1-i))$

$a_n = \lambda_1 (-(1+i))^n + \lambda_2 (-1+i)^n$

qui: il periodo $\mid p^2 - 1 = 8$

perché così è per $-1-i$ e $-1+i$

In generale, se ho 2 radici distinte: il periodo $\mid p^2 - 1$

Invece, solo per $p=5$ $\quad t^2 - t - 1 = (t-3)^2$

in tal caso $a_n = \lambda_1 3^n + \lambda_2 n 3^n$

$\Rightarrow$ il periodo $\mid p \cdot (p-1)$

Es: trovare termini iniziali per Fibonacci per avere

periodo 4 mod 5

Lo stesso discorso funziona per qualsiasi ricorrenza lineare

$$a_{n+m} = c_{m-1} a_{n+m-1} + \dots + c_0 a_0$$

allora il periodo $\mid p^h - 1$ per h opportuno (che dipende dalla fattorizzazione mod p) se le radici sono distinte se ci sono ≥ 2 radici coincidenti, periodo $\mid p \cdot (p^h - 1)$

Es: se $m=3$ se radici distinte ci sono 3 possibilità

$p(x)$ sia irr. $\rightarrow$ per $\mid p^3 - 1$

$p(x) = (x - r_1) q(x)$ $\leftarrow$ irr deg $= 2$ $\rightarrow$ $\mid p^2 - 1$

$p(x) = (x - r_1) \cdots (x - r_k)$ $\rightarrow$ $\mid p - 1$

Oss: con polinomi più grossi basta lavorare in $\mathbb{F}_{p^h}$ con $h = mcm(\deg_i)$ $\uparrow$ quelli che compaiono nella fattorizzazione

Es: $\begin{cases} a_0 = 2 \\ a_{n+1} = 2a_n^2 - 1 \end{cases}$

dimostrare che se $p \mid a_n \Rightarrow 2^{n+3} \mid p^2 - 1$

$b_n(x) = \dfrac{x^n + x^{-n}}{2}$ $\left(= \cosh(y) \text{ per } y \text{ opportuno}\right)$

$\left(\cosh(ix) = \cos(x) \text{ in } \mathbb{C}\right)$

$b_{2n}(x) = 2b_n^2(x) - 1$

Se trovassimo un opportuno c, si avrebbe

$a_n = \dfrac{c^{2^n} + c^{-2^n}}{2}$ vorrei poterla scrivere mod p

c si ottiene guardando $n=0$ $\quad 2 = \dfrac{c + c^{-1}}{2}$

$\rightsquigarrow$ sarebbe $c = 2 + \sqrt{3}$

In $\mathbb{F}_{p^2}$ si ha $a_n = \dfrac{(2+\sqrt{3})^{2^n} + (2+\sqrt{3})^{-2^n}}{2}$

se $p \mid a_n$ $\quad a_n = 0$ in $\mathbb{F}_{p^2}$

$\Rightarrow \underbrace{(2+\sqrt{3})}_{c}^{2^{n+1}} = -1$

$\operatorname{ord} c = 2^{n+2} \mid p^2 - 1$

Se si avesse che $c = D^2$ in $\mathbb{F}_{p^2}$ avremmo finito

$2(2+\sqrt{3}) = (1+\sqrt{3})^2$

mi basterebbe che 2 fosse un $\square$, ma ce l'ho perché sono in $\mathbb{F}_p^2$.

Sistemi di ricorrenze e ricorrenze su una sola successione

$$\begin{cases} a_{n+1} = \lambda_1 a_n + \lambda_2 b_n + \dots \\ b_{n+1} = \mu_1 a_n + \mu_2 b_n + \dots \\ \vdots \qquad \ddots \end{cases}$$

$$X_n = \begin{pmatrix} a_n \\ b_n \\ \vdots \end{pmatrix} \qquad M = \begin{pmatrix} \lambda_1 & \lambda_2 & \dots \\ \mu_1 & \mu_2 & \dots \\ \vdots & & \ddots \end{pmatrix}$$

$a_{n+m+1} = \nu_m a_{n+m} + \dots + \nu_0 a_n$

dipende da $m+1$ termini precedenti;

Ho una ricorsione espressa come

$$X_{n+1} = M X_n$$

passaggio facile

$a_{n-1} = b_n$, $b_{n-1} = c_n$, ...

$$\begin{cases} a_{n+1} = v_m a_n + v_{m-1} b_n + \dots + v_0 z_n \\ b_{n+1} = a_n \\ c_{n+1} = b_n \\ \vdots \end{cases}$$

$$M = \begin{pmatrix} v_m & v_{m-1} & \dots & v_0 \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & & \\ 0 & \dots & \dots & 1 \; 0 \end{pmatrix}$$

più difficile →

Sia $p_M(t)$ il polinomio caratteristico di M

allora $p_M(M) = M^n + c_{n-1} M^{n-1} + \dots + c_1 M + c_0 I = 0$

(identità)

Es: $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = M$

$p_M(t) = t^2 - t - 1$

infatti: $M^2 - M - I = 0$

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

$p_M(M)\, x_n = 0 \cdot x_n = 0$

$$\sum_i c_i M^i x_n = 0$$

$$= \sum_i c_i x_{n+i} = 0$$

$\Rightarrow$ $p_M(t)$ è la ricorrenza che soddisfano tutte le coordinate di x_n

Senior 2016 - N3 Advanced (Anér)

Note Title 9/5/2016

- Campi Finiti, qualche conto
- Vieta jumping (+ problema tostissimo)
- Successioni di Mersenne (si chiamano davvero così?)
- Esercizi vari

Dato p primo e $k \geq 2$ naturale, quanti sono i polinomi monici di grado k in $\mathbb{F}_p[x]$ irriducibili?

OSS Se esiste almeno un pol. $q(x) \in \mathbb{F}_p[x]$ irrid. di grado k, allora

$$\mathbb{F}_p[x] / (q(x))$$ è un campo con p^k elementi

(è uno spazio vett. su $\mathbb{F}_p$, e ha come base $1, x, x^2, \dots x^{k-1}$

$\Rightarrow$ $\mathbb{F}_{p^k}$ esiste!

Considero il polinomio $x^{p^k} - x \in \mathbb{F}_p[x]$

Usando i ciclotomici, ottengo la fattorizzazione

$$x^{p^k} - x = x \cdot \left(x^{p^k - 1} - 1\right) = x \cdot \prod_{d \mid p^k - 1} \Phi_d(x)$$

($\Phi_d(x)$ è il d-esimo pol. ciclotomico, e ha grado $\varphi(d)$)

OSS 1 Forse in $\mathbb{F}_p[x]$ qualcuno dei $\Phi_d(x)$ si fattorizza ulteriormente

OSS 2 $\Phi_{p^k-1}(x)$ è tra i fattori (speriamo che contenga le radici di ordine esattamente p^k-1)

Costruiamo un campo finito in cui $q(x)=x^{p^k}-x$ si fattorizza in fattori di grado 1

PASSO 1 $K_0=\mathbb{F}_p$. $q(x)=q_1^0(x)\cdot\ldots\cdot q_{m_0}^0(x)$ fatt. irriduc.

Se un fattore ha grado ≥ 2, $q_i^0(x)$, considero

$$K_0[x]/q_i^0(x) = K_1$$

PASSO 2 K_1 (cambio lettera) $q(y)=q_1^0(y)\cdot\ldots\cdot\overline{q_i^0(y)}^{\,1}\cdot\ldots\cdot q_{m_0}^0(y)$

$K_1[y]$ ↑ è divisibile per $(y-x)$

$\Rightarrow$ ho una fattorizzazione più fine. $q(y)=q_1^1(y)\cdot\ldots\cdot q_{m_1}^1(y)$

$m_1>m_0$. Prendo $q_j^1(y)$ irriduc. di grado ≥ 2

$$K_2=\frac{K_1[y]}{(q_j^1(y))}\left(=\frac{K_0[x,y]}{(q_i^0(x),q_j^1(y))}\right)$$

Ad un certo punto ho un campo K_N in cui

$x^{p^k}-x$ si fattorizza in fattori lineari

K_N contiene come sottoinsieme le radici di $x^{p^k}-x$

Lo chiamo $S=\{\text{radici di } x^{p^k}-x\}\subseteq K_N$

OSS 3 S, come sottoinsieme di K_N, è chiuso per $+, \cdot, -$, c'è 0, se c'è t c'è t^{-1} $(t \neq 0)$.

RIVEDIAMO LA SOMMA $(\alpha+\beta)^{p^k} = \alpha^{p^k} + \beta^{p^k} + \sum_{i=1}^{p^k-1} \binom{p^k}{i} \cdot \alpha^i \beta^{p^k-i}$

multiplo di p

(in K_N) $= \alpha^{p^k} + \beta^{p^k} = \alpha + \beta$

S è un campo con p^k elementi! Quasi, $x^{p^k} - x$ potrebbe avere radici doppie in K_N ...

DERIVIAMO (ma funziona davvero?)

Funzione Sia $q(x)$ un polinomio a coeff. in K $(= K_N)$

$q(x) = (x-\alpha_1) \cdot \ldots \cdot (x-\alpha_m)$ $\quad \alpha_i \in K$

- Se α è radice doppia di q, allora α è radice di q', altrimenti no

$$q'(x) = \sum_{i=1}^{m} \prod_{\substack{j=1 \\ j \neq i}}^{m} (x-\alpha_j)$$

tutti gli addendi si annullano in $\alpha = \alpha_1$ (wlog), tranne (forse) $\prod_{j=2}^{m} (x-\alpha_j)$. Questo si annulla sse $\alpha = \alpha_j$ per qualche $j \geq 2$

REGOLA DI LEIBNITZ $(fg)' = f'g + fg'$ segue dalla def. di der. di un polinomio $\left(\sum a_i x^i\right)' = \sum i a_i x^{i-1}$

$\left(x^{p^k} - x\right)' = p^k \cdot x^{p^k-1} - 1 = -1$ (perché $p = 0$ in K_N)

(Da questo punto $K_N = S$, basta ricostruirlo ...)

Le radici di $x^{p^k} - x$ contenute in $\Phi_{p^k-1}(x)$ hanno ordine esattamente $p^k - 1$, le altre no.

Prendiamone una, diciamo α.

$$\mathbb{F}_p[\alpha] = \{\text{tutti gli el. di } K_N \text{ esprimibili come pol. calcolati in } \alpha, \text{ con coeff. in } K_0\}$$

$$= K_N \quad \text{perché contiene } 1, \alpha, \alpha^2, \dots \alpha^{p^k-2}$$

α ha un polinomio minimo, chiamiamo $q(x)$.
Che grado ha q? k.
Infatti $1, \alpha, \alpha^2, \dots \alpha^{\deg q - 1}$ sono una base di K_N su K_0 (verificatelo...)

q è un pol. di grado k, ed è irriducibile su $\mathbb{F}_p$ perché è il pol. minimo di α su $\mathbb{F}_p$.

Ugualmente, se α è radice di $\Phi_d(x)$ con $d \mid p^k - 1$, $d \neq p^k - 1$, allora $\alpha^{p^h - 1} = 1$ per qualche $h < k$ ($h \mid k$) falso

$K_0[\alpha]$ contiene al massimo p^h elementi, è un campo pure lui, ma è più piccolo di K_N falso falso

$\Rightarrow \dim K_0[\alpha]/\mathbb{F}_p = [K_0[\alpha] : \mathbb{F}_p] \leq h < k$

il pol. minimo di α ha grado al massimo h

OSS Ciò che è falso, a volte è vero. Ci sono alcuni $d \mid p^h - 1$ con $d \nmid p^{h'} - 1$ per alcun $h \mid k$ e ci sono altri d per cui $\nexists h \mid k$ per cui $d \mid p^{h'} - 1 \mid p^k - 1$

$\Phi_d(x)$ ha come radice α. Se d è del primo tipo, allora $K_0[\alpha]$ è tutto K_N, altrimenti no.

è un campo

Fatto Un sottoanello di un campo finito è un campo (finito)

$\beta \in$ sottoanello, $\beta \neq 0$ $\beta, \beta^2, \beta^3, \dots$ sono tutti nel sottoanello.

Siccome il campo è finito $\Rightarrow \beta^n = \beta^m \quad m < n$

$\beta^{n-m} = 1 = \beta \cdot (\beta^{n-m-1}) \quad \frac{1}{\beta}$ è nel sottoanello

Facciamo ordine • $x^{p^n} - x$ ha delle radici, che sono tutti (e soli) gli elementi di K_N.

• Se $\alpha \in K_N \quad K_0[\alpha] \subseteq K_N$ è un sottocampo.

• Poiché $|K_n| = p^k$, $|K_0[\alpha]| = p^h$ con qualche $h \mid k$

• Se $h < k$, allora $\alpha \in \mathbb{F}_{p^h} = \{\text{el. } \beta \in K_N : \beta^{p^h} = \beta\}$

• allora il pol. min. di α ha grado $< k$ (ha grado h)

• Se $h = k$, allora il pol. min. di α ha grado k

• α è radice di $\Phi_d(x)$ per qualche $d \mid p^k - 1$

• Se $\Phi_d(x) \mid x^{p^h} - x$ per qualche $h < k$, siamo nel 1° caso, altrimenti nel secondo.

• $\Phi_d(x)$, se $d \nmid p^h - 1$ per ogni $h < k$, si fattorizza in pol. irr. su $\mathbb{F}_p$ di grado k (tutti distinti)

Successioni di Mersenne (o di MerSam)

$a_0, a_1, a_2, \dots$ succ. di numeri naturali si dice di MerSam se $\forall\, m,n \in \mathbb{N}$

$$a_{(m,n)} = (a_m, a_n)$$

(variante: a_n a valori in un anello in cui il m.c.d. è ben definito. Esempio: $K[x]$)

Esempi ① $a_n = n^k$ (k naturale)

② $a_n = k^n - 1$ $\quad k \geq 2$ fissato

③ $a_n = X^n - 1$ nei polinomi $\mathbb{Q}[x]$

Facciamolo • Se $m \mid n$, $(k^m - 1) \mid (k^n - 1)$ (NOTO)

$\Rightarrow$ $k^{(m,n)} - 1$ divide $(k^m - 1, k^n - 1)$ (idem con X)

• Supponi $m > n$. Se $d = (k^m - 1, k^n - 1)$ $\quad m = bn + c$, $c < n$

$$d \mid (k^m - 1) - (k^m - k^c) = k^c - 1$$

$k^c \cdot (k^{bn} - 1)$ è un multiplo di $k^n - 1$

quindi $d \mid k^c - 1$ $\quad d \mid (k^n - 1, k^c - 1)$

$\dots \Rightarrow d \mid k^{(m,n)} - 1$ (idem con X)

④ Successioni per ricorrenza opportune (a valori interi)

$a_0 = 0$ $\quad a_1 = a$ $\quad a_{n+2} = b\,a_{n+1} + a_n$ (qui si va $+1$)

con b e c coprimi (OSS. Il caso $a = 1$ è quello interessante)

(Caso particolare: $a_n = F_n$ numeri di Fibonacci)

- Se $m \mid n$, allora $a_m \mid a_n$: ragioniamo modulo a_m

$0, 1, b, \ldots$ $\quad a_k \; a_{k+1}$ $\quad a_h \; a_{h+1}$

$\exists\, k, h \leq a_m^2 + 1$ per cui $a_k \equiv a_h$ · $a_{k+1} \equiv a_{h+1}$ mod m $\Rightarrow$ .... eccetera

OSS $a_1 \equiv 0 \; (a_m)$ $\quad a_{m+1} \equiv 1 \; (a_m)$

allora da a_m ad a_{2m} rileto gli stessi resti mod (m) visti da a_0 a a_m, ma moltiplicati per b $\Rightarrow$ $a_{2m} \equiv b \cdot a_m \equiv 0 \; (a_m)$

DOMANDA Esistono altri a_i multipli di a_m, ma con $m \nmid i$? No, perché b (e in generale a_{km+1}) sono coprimi con a_{km} che è multiplo di a_m $\Rightarrow$ a_{km+1} è invertibile mod (a_m) $\Rightarrow$ Se a_i è multiplo di a_m, allora anche $a_{i \bmod (m)}$ lo è. Facciamo che b era > 0, otteniamo un assurdo perché a_n è crescente in n (il caso $b < 0$ comunque è trattabile...)

- $m \mid n \Rightarrow a_m \mid a_n$ fatto $\quad a_{(m,n)} \mid (a_n, a_m)$

- Abbiamo dimostrato che i multipli di a_m sono tutti e soli gli a_{km}. Similmente (stesso procedimento), se $d > 0$ e $d \mid a_m$ ma $d \nmid a_2, a_3, \dots a_{m-1}$ allora i multipli di d sono a_{km}.

  $d = (a_m, a_n)$: i suoi multipli sono tutti gli a_{kh} per qualche h fissato, k variabile.
  h deve però dividere m e n $\Rightarrow h \mid (m,n)$
  $\Rightarrow d \mid a_{(m,n)}$

Lemma utile Se $(a_0), a_1, a_2, \dots$ è una success. di Mersenne, e $k > 0$, $m > 0$, allora

$$\left(\prod_{i=1}^{k} a_i\right) \mid \left(\prod_{i=m+1}^{m+k} a_i\right)$$

[**Esempio** $a_i = i$ | $k! \mid (m+1)\cdot \dots \cdot (m+k)$
vero perché il rapporto è $\binom{m+k}{k}$ che è intero

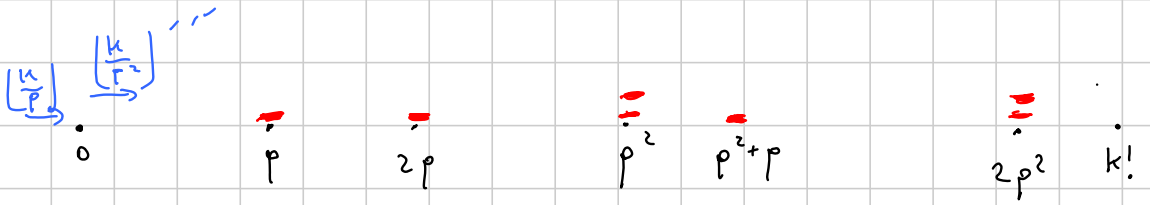
Domanda di Andrea È sempre vero, data (a_n) di Mersenne, che, per ogni k e per ogni N

$$\text{m.c.d}\left\{ \prod_{i=m+1}^{m+k} a_i \right\}_{m \geq N} = \prod_{i=1}^{k} a_i \quad ?$$

DIM lemma utile Scelgo p primo e stimo le valutazioni p-adiche a sinistra e a destra.

RICORDO

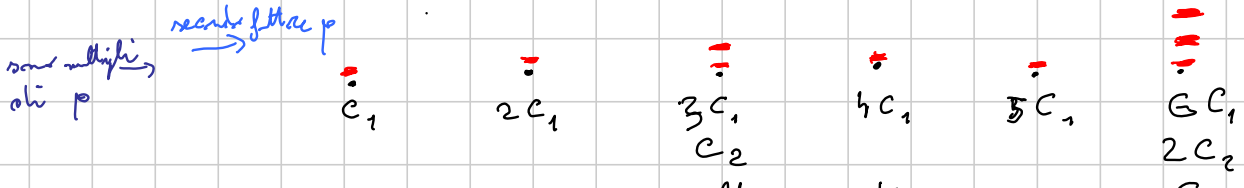
$$v_p(k!) = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \left\lfloor \frac{k}{p^3} \right\rfloor + \dots$$



OSS Fissato $a_1 > 0$, esiste c t.c. gli a_i multipli di a_1 sono esattamente quelli per cui i è un multiplo di c

DIM Come fatto prima (è una riduz. equivalente di successione di Mersenne)

Come sarà fatto il disegno?



c_1 t.c. a_{kc_1} sono i multipli di p
c_2 t.c. // // p^2 (c_2 è multiplo di c_1)
c_3 // // p^3

$$v_p\left(\prod_{i=1}^{k} a_i\right) = \left\lfloor \frac{k}{c_1} \right\rfloor + \left\lfloor \frac{k}{c_2} \right\rfloor + \dots$$

OSS Nell'intervallo $m+1, \dots, m+k$, ci sono almeno

$\left\lfloor \frac{k}{c_i} \right\rfloor$ multipli di c_i, quindi

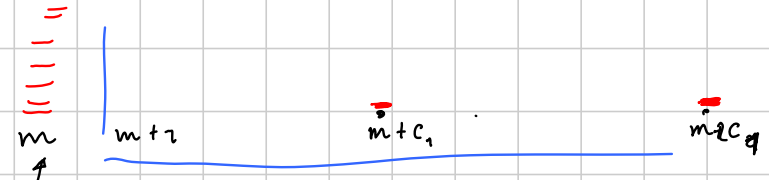
la sequenza $a_{m+1}, \dots, a_{m+k}$ contiene almeno

$\left\lfloor \frac{k}{c_1} \right\rfloor$ multipli di p, almeno $\left\lfloor \frac{k}{c_2} \right\rfloor$ multipli di p^2,

$\dots \Rightarrow v_p\left(\prod_{i=m+1}^{m+k} a_i\right) \geq \sum \left\lfloor \frac{k}{c_i} \right\rfloor$ □

Torniamo alla domanda di prima

Sia c un multiplo di tutti i $c_i < k$. Sia $m > N$ e $m \equiv 0 \pmod{c_i}$. Allora



qui ho tantissimi fattori p, tutti spreciati

Funzione $f : \{\text{primi}\} \to \{\text{primi}\}$ $f(p) =$ il più piccolo primo $> p$

$a_n = f(p_1)^{e_1} \cdot \dots \cdot f(p_k)^{e_k}$ se $n = p_1^{e_1} \cdot \dots \cdot p_k^{e_k}$

Questa è di Mersenne, ma 2 non compare mai.

La risposta alla domanda di Andrea è SÍ !!!

Esercizi • p primo dispari, allora $\prod_{k=1}^{p-1} k^{2k-p+1}$ è intero

• $c_n = n(n+1)$; $l, m, k > 0$ per cui $m+k+1$ è primo $> l+1$. Allora

$$(e_1 : \dots : e_l) \mid \left[(c_{m+1} - c_k) \cdot \dots \cdot (c_{m+l} - c_k) \right]$$

Classici da Vieta jumping (o quasi)

- $x, y > 0$ interi $\dfrac{x^2+y^2+1}{xy}$ è intero, allora vale 3 (già visto ...)
- $x, y, z \geq 0$ interi, $(xy+1)(yz+1)(zx+1)$ è un quadrato. Allora i tre fattori sono quadrati.
- $n > 0$ tale che $2 + \sqrt{12n^2+1}$ è intero; allora è un quadrato.
  Variante: $p \equiv -1 \pmod 4$ $2 + \sqrt{4pn^2+1}$ intero; allora è un quadrato (wow!).

Pubblicità: Volete un problema di TdN da risolvere ma non sapete dove trovarlo? Consultate il PEN (Problems in Elementary Number theory).

Altra pubblicità (proposta da Federico e modificata da cip999)

Auguriamo un oro alle IMO al formulatore della congettura sulle successioni di MerSam che si è rivelata vera:

VIOLAORO, OROACCLE IMO!!!

#CIP999OROPURELUI

VIETA JUMPING / DISCESA INFINITA

$\frac{x^2+y^2+1}{xy}$ intero $\Rightarrow$ è 3

oss Se $x=y=1$ allora viene 3
$x=2 \quad y=1$ //

Facciamo che viene k

$x^2+y^2+1-kxy=0$ lo vedo come polin. in x

$x^2-ky\cdot x+y^2+1=0$ ha due radici:

una è x_1 (quella della coppia (x_1,y) da cui parto)

l'altra è $x_2=\frac{y^2+1}{x_1}>0$ x_2 è intera perché

$x_2=ky-x_1$. Speranza: $x_2<x_1$

Basta (forse) $x_2>y$ perché allora (forse) $x_2\leq y$ ...

$x_2=\frac{y^2+1}{x_1}\leq\frac{y^2+1}{y+1}\leq y$ con $=$ sse $y=1$
$x_1=y+1=2$

Quindi mi riduco quasi sempre a una coppia con una delle comp. invariata e l'altra diminuita, a meno che non capiti una di queste:
- $x=y$ $\Rightarrow$ si finisce in fretta
- $x=2 \quad y=1$ $\Rightarrow$ viene 3

PEN A 1 | $(xy+1)(yz+1)(zx+1)$ è un $\square$, con $x,y,z \geq 0$. Allora i 3 fattori sono quadrati.

Idea Se uno tra x,y,z è 0, allora la tesi è vera.

Idea Se $\overset{\text{wlog}}{x=y}$, allora x deve essere 0 o il prodotto non è un $\square$. Possiamo supporre $x<y<z$ $z \geq 2$ (anzi, $x \geq 1$ altrimenti concludo ...)

Vorrei passare da $(z,y,x) \rightsquigarrow (t,y,x)$ con t più piccolo di z

OSS (Differenza dal problema precedente) Stavolta il polinomio interessante

$$(xy+1)(yz+1)(zx+1) - k^2$$

non è monico in z (se xy divide gli altri coeff. ... ma non c'è da sperarci)

Idea Cerchiamo un polinomio di 2° grado in t, monico, nelle variabili x,y,z,t, con Δ = un prodotto di $(xy+1)(yz+1)(zx+1)$, simmetrico in x,y,z,t

Magia (fare un po' di tentativi)

$$\underbrace{x^2+y^2+z^2+t^2}_{U} + a\underbrace{\sum_{\text{sym}} xy}_{V} + b\underbrace{\sum_{\text{sym}} xyz}_{W} + c\underbrace{xyzt}_{P}$$

$$+ d\underbrace{\sum_{\text{sym}} x}_{S} + \underbrace{e}_{N}$$

qui sym è da intendersi "cum grano salis"

Oss Δ ha solo monomi di grado pari.

Δ è un polinomio in U, V, W, P, S, N (quasi vero)

(Ora non so se si può fare qualche altra considerazione

$$\underbrace{\sum t^2}_{4 \text{ termini}} - 2 \underbrace{\sum xy}_{6 \text{ termini}} - 4xyzt - 4$$

$$\Delta_t = 4(xy+1)(yz+1)(zx+1)$$

Posto $(x,y,z) \rightsquigarrow (x,y,t)$. Vorrei le seguenti cose:

- $t < z$ ✓
- $t \geq 0$ ✓
- $(xt+1)$, $(yt+1)$ e $(xy+1)$ non sono tutti quadrati ✓
- $(xt+1)(yt+1)(xy+1)$ è un $\square$ ✓

$= (x+y-z-t)^2 - 4xy - 4zt - 4xyzt - 4 \geq 0$

$(x+y-z-t)^2 = 4(xy+1)(zt+1)$ e cicliche (magia)

$\square = 4(yz+1)(xt+1)$

$\square = 4(zx+1)(yt+1)$

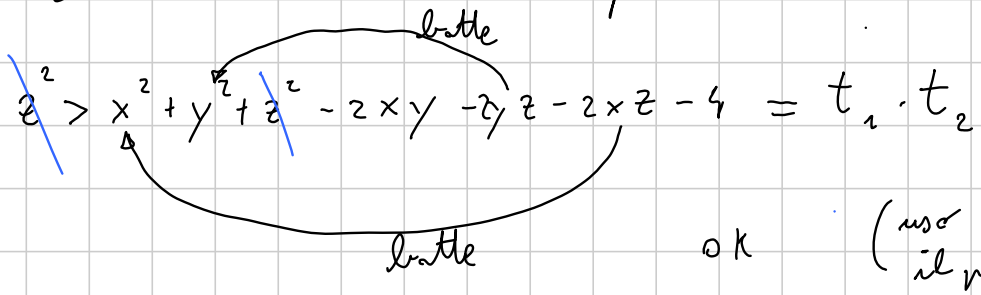
$zt+1 \geq 0 \quad t \geq -\frac{1}{z}$ ma è intero $\Rightarrow t \geq 0$

Almeno un $\_$ non è $\square \Rightarrow t \geq 1$

Direi, almeno oltre $\_$, in particolare almeno uno tra $(xt+1)$ e $(yt+1)$ non è un $\square$

Speranza: $t < z$ (almeno una delle due radici)

Il termine noto di rispetto a t è



ok (uso che z è il più grande)