Stage Senior 2018 – Livello Medium

Stampato integrale delle lezioni

Autori vari

Indice

A1 MEDIUM

Titolo nota 04/09/2018

Anello = insieme su cui sono definiti $+, -, *$
Campo = " " " ", / (tranne che per 0)

ES: Anelli $\mathbb{Z}, \mathbb{Z}_n, A[x, y, \dots]$
Campi $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$

Se A anello posso considerare $A[x]$

- Funziona tutto bene, tranne se lavoro su $\mathbb{Z}_n$, con n non primo, perché ha divisori di zero:

es: $\mathbb{Z}_6 \quad 2 \cdot 3 = 0$

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

$$(2x^{17} + \dots)(3x^{18} \dots) = 0 \cdot x^{17+18}$$

$$\deg(fg) \neq \deg f + \deg g$$

$x^2 - 1$ in $\mathbb{Z}_{15}$ ha $-1, 1, 4, -4$ come radici

Su tutti gli altri anelli (e campi) visti, non ci sono divisori di zero, e si può sviluppare normalmente una teoria dei polinomi

Fattorizzazione unica: se $a(x) \mid f(x)\,g(x)$, allora:

- $a(x) \mid f(x)$
- $a(x) \mid g(x)$
- $a(x)$ si fattorizza in $a_1(x) \mid f(x)$ e $a_2(x) \mid g(x)$

Altro ⚠

$f(x) = g(x)$ come polinomi se $f_0 = g_0, \dots f_d = g_d$

$f(x) = g(x)$ come funzioni se $f(a) = g(a)$ $\forall a \in$ dominio

In $\mathbb{Z}_p[x]$, esistono f, g che sono diversi come polinomi ma uguali come funzioni:

$$x^p, \quad x$$

(Principio identità polinomi:
Teo: se due polinomi f, g di grado $\leq d$ sono tali che $f(x_i) = g(x_i)$ $\quad x_1, x_2, \dots x_{d+1}$ punti distinti, allora $f(x) = g(x)$ come polinomi]

[ma non posso applicarlo perché in $\mathbb{Z}_p$ ho "solo" p punti distinti]

⚠ Principio di identità dei polinomi vale solo per polinomi in una variabile: esistono $f(x,y), g(x,y) \in \mathbb{R}[x,y]$

tali che esistono infinite coppie (x_i, y_i), $i = 0, 1, 2, \dots$

tali che $f(x_i, y_i) = g(x_i, y_i)$ <u>ma</u> f, g diversi

<u>ES</u>: $f(x,y) = (y - x^2)(x^2+1) + 1$

$g(x,y) = (y - x^2)(y^3 - 57x) + 1$ ⊛

Tutte le coppie (n, n^2), $n \in \mathbb{N}$.

L'unica cosa che si riesce a dire è che

$$y - x^2 \mid f(x,y) - g(x,y)$$

Hint: guardali in $(\mathbb{R}[x])[y]$

$g(x,y) = y^4 - x^2 y^3 - 57xy + 1 + 57x^3$

$g_4 = 1$, $g_3 = -x^2$, $g_2 = 0$, $g_1 = -57x$, $g_0 = 1 + 57x^3$

Vorremmo usare Ruffini: se dimostro che $p(a) = 0$, allora $(y-a) \mid p(y)$ $\quad a = x^2$

Devo dimostrare che $h(x, x^2) = 0$ in $\mathbb{R}[x]$ dove $h = f - g$.

$h(x, x^2)$ è un polinomio nella variabile x tale che valutandolo in $n \in \mathbb{N}$ fa zero $\Rightarrow$ è il polinomio $0 \in \mathbb{R}[x]$.

Quindi per Ruffini $(y - x^2) \mid f(x,y) - g(x,y)$

<u>Lemma di Gauss</u>: se $\underset{\in \mathbb{Z}[x]}{c(x)} = \underset{\in \mathbb{Q}[x]}{a(x)}\ \underset{\in \mathbb{Q}[x]}{b(x)}$,

allora $\exists\, q \in \mathbb{Q}$ t.c. $q a(x)$, $\frac{1}{q} b(x) \in \mathbb{Z}[x]$

ES: $x^2 - 4 = (3x+6)\left(\frac{1}{3}x - \frac{2}{3}\right)$

$= (x+2) \cdot (x-2)$

dim:

Lemma 2: se $\gamma(x) = \alpha(x)\beta(x)$, con $\alpha(x), \beta(x), \gamma(x) \in \mathbb{Z}[x]$,

e $p \mid \gamma_0, \gamma_1, \dots \gamma_{\deg \gamma}$, allora

$p \mid \alpha_0, \dots \alpha_{\deg \alpha}$ oppure $p \mid \beta_0, \beta_1, \dots \beta_{\deg \beta}$

dim: idea: considero $\overline{\gamma}(x)$ il polinomio "proiettato" su $\mathbb{Z}_p$, cioè $\overline{\gamma}_i$ è la classe di resto modulo p di γ_i

$$0 = \overline{\gamma}(x) = \overline{\alpha}(x)\, \overline{\beta}(x) \quad \text{in } \mathbb{Z}_p[x]$$

Su $\mathbb{Z}_p$ funziona annullamento del prodotto:
se $\overline{\alpha}(x)\overline{\beta}(x) = 0$, allora uno dei due dovrebbe essere 0

(per assurdo: $\overline{\alpha}(x) = \overline{\alpha}_n x^n + \dots$ $\overline{\beta}(x) = \overline{\beta}_m x^m + \dots$)

$$c(x) = a(x)\, b(x) = \frac{1}{A}\alpha(x)\ \frac{1}{B}\beta(x) \qquad \alpha, \beta \in \mathbb{Z}[x]$$

$$\Updownarrow$$

$$AB\,c(x) = \alpha(x)\beta(x)$$

$p \mid AB \Rightarrow p \mid$ tutti i coeff. di $\alpha(x)$ o di $\beta(x)$

$\Rightarrow \frac{AB}{p} c(x) = \frac{\alpha}{p}(x)\beta(x)$

... elimino un primo per volta ... $c(x) = \underbrace{\frac{\alpha}{r}}(x)\frac{\beta}{s}(x)$

$\mathbb{Z}[x] \quad \mathbb{Z}[x]$

Criterio di Eisenstein:

$a(x) \in \mathbb{Z}[x]$ di grado d tale che

$p \nmid a_d \quad p \mid a_{d-1}, \dots a_1, a_0 \quad p^2 \nmid a_0 \quad v_p(a_0) = 1$

Allora non esistono $b(x), c(x) \underline{\in \mathbb{Z}[x]}$

tali che $a(x) = b(x)c(x)$ (di grado $\neq 0$)

e neppure in $\mathbb{Q}[x]$, per Gauss

Dim:

Proietto modulo p:

$\bar{a}(x) = Kx^d$ con $K \neq 0$ in $\mathbb{Z}_p$

Se per assurdo $a(x) = b(x)c(x)$

$Kx^d = \bar{a}(x) = \bar{b}(x)\bar{c}(x)$ è una fatt. in $\mathbb{Z}_p[x]$

Per fatt. unica $\bar{b}(x) = K_1 x^{d_1}$, $\bar{c}(x) = K_2 x^{d_2}$

$d_1 + d_2 = d$

$d_1, d_2 \neq 0$

$a(x) = (b_{d_1}x^{d_1} + \dots b_1 x + b_0)(c_{d_2}x^{d_2} + \dots + c_1 x + c_0)$

$p \mid b_0$ $\qquad$ $p \mid c_0$

$p^2 \mid a_0 = b_0 c_0$, assurdo.

Conseguenza di Eisenstein: $x^n - k$, con $k \in \mathbb{Z}$ non quadrato perfetto, è irriducibile in $\mathbb{Z}[x]$, $\mathbb{Q}[x]$

OSS: fattorizzare dà più informazioni che non applicare $b-a \mid p(b)-p(a)$ per $p \in \mathbb{Z}[x]$:

es: se $p \in \mathbb{Z}[x]$, $p(2) = p(4) = 5$, quanto può valere $p(0)$?

Soluzione 1 (incompleta): $2-0 \mid p(2)-p(0) = 5-p(0)$

$\Rightarrow p(0)$ dispari

$4-0 \mid p(4)-p(0) = 5-p(0)$

$\Rightarrow p(0) \equiv 1 \ (4)$

Soluzione 2: $p(x) - 5 = (x-4)(x-2)\, r(x)$ $\qquad r(x) \in \mathbb{Z}[x]$

$\Rightarrow p(0) - 5 = -4 \cdot (-2) \cdot r(0)$

$\Rightarrow p(0) \equiv 5 \pmod 8$

(e si fanno tutti scegliendo r)

Congruenze modulo polinomi:

$$a(x) \equiv b(x) \pmod{m(x)} \iff m(x) \mid a(x) - b(x)$$

Esempio: voglio sapere il resto nella divisione

$$x^6 - x^3 + 1 = (x^2+1)\, q(x) + r(x)$$

Posso pensarlo così: lavoro mod x^2+1:

$-1 \equiv x^2$, quindi $1 \equiv x^4$ $-1 \equiv x^6$

$$x^6 - x^3 + 1 \equiv -1 - x \cdot (-1) + 1 \equiv x.$$

Altro esempio:

Modulo $x+a$ $\quad x \equiv -a$

$$x^{2n+1} \equiv -a^{2n+1} \Rightarrow x+a \mid x^{2n+1} + a^{2n+1}$$

(vero in $(\mathbb{R}[a])[x]$)

Altro esempio:

$$a+b+c \mid a^3+b^3+c^3-3abc$$

$$a+b+x \mid a^3+b^3+x^3-3abx$$

$x \equiv -a-b$, quindi $\qquad$ mod $a+b+x$

$$a^3+b^3+(-a-b)^3 - 3ab(-a-b) \equiv$$

$$\equiv 0 \qquad \Rightarrow a+b+x \mid a^3+b^3+x^3-3abx.$$

Altro trucco: "mettere l'altra radice"

$x^2-2 \qquad \pm\sqrt{2}$

<u>ES</u>: Quanto vale $\left\lfloor (\sqrt{2}+1)^{2018} \right\rfloor$ modulo 5 ?

<u>Idea</u>:

$$(\sqrt{2}+1)^{2018} + (-\sqrt{2}+1)^{2018} \quad \text{è razionale}$$

$$= \sum_{n=0}^{2018} \binom{2018}{n} (\sqrt{2})^n + \sum_{n=0}^{2018} \binom{2018}{n} (-\sqrt{2})^n =$$

$=$ (i termini con n dispari si semplificano) $= \sum_{n \text{ pari}} 2\binom{2018}{n}(\sqrt{2})^{2n} \in \mathbb{Q}$

<u>Idea 2</u>:

$a_n = (\sqrt{2}+1)^n + (-\sqrt{2}+1)^n$ soddisfa una certa relazione per ricorrenza:

pol. minimo $(x-1)^2 = 2 \qquad x^2-2x+1=2$

$x^2 = 2x+1$

Quindi la rel. per ricorrenza sarà $\underline{a_{n+1} = 2a_n + a_{n-1}}$

$a_0 = 2$

$a_1 = 2$

Modulo 5, ho

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
2	2	1	−1	−1	2	3	3	−1

a_9	a_{10}	a_{11}	a_{12}	a_{13}
1	1	3	2	2

ciclica (si ripete ogni

12)

$$2018 \equiv 2 \pmod{12} \Rightarrow Q_{2018} \equiv Q_2 \equiv 1 \pmod 5$$

$$(\sqrt{2}+1)^{2018} + (-\sqrt{2}+1)^{2018} \equiv 1 \pmod 5$$

$(-0.4142\ldots)^{2018}$ " positivo e molto piccolo

$$(\sqrt{2}+1)^{2018} + \text{cose positivo e molto piccole} \equiv 1 \pmod 5$$

$$\lfloor (\sqrt{2}+1)^{2018} \rfloor \equiv 0 \pmod 5$$

Altra variante di "mettici l'altra radice": "mettici la parte immaginaria":

es: $\cos(15°) + \cos(30°) + \cos(45°) + \ldots + \cos(345°)$

reale $[\cos(15°) + \cos(30°) + \cos(45°) + \ldots + \cos(345°)$

immag. $[+i\cdot\sin(15°) + i\cdot\sin(30°) + i\cdot\sin(45°) + \ldots + i\cdot\sin(345°) =$

$$= \exp\left(i\cdot\frac{\pi}{12}\right) + \exp\left(i\cdot\frac{2\pi}{12}\right) + \exp\left(i\cdot\frac{3\pi}{12}\right) + \ldots + \exp\left(i\frac{23}{12}\pi\right)$$

Progressione geometrica! $z + z^2 + \ldots + z^{23} = \dfrac{z - z^{24}}{1-z}$

con $z = \exp\left(i\frac{\pi}{12}\right)$

$$\operatorname{Re}\left(\frac{\exp\left(\frac{i\pi}{12}\right) - \exp\left(i\cdot\boxed{\frac{24}{12}}\pi\right)}{1-\exp\left(\frac{i\pi}{12}\right)}\right) = \cos(15°) + \ldots + \cos(345°)$$

$$= \mathrm{Re}\left(\frac{\exp\left(\frac{i\pi}{12}\right)-1}{1-\exp\left(\frac{i\pi}{12}\right)}\right) = \mathrm{Re}(-1) = -1$$

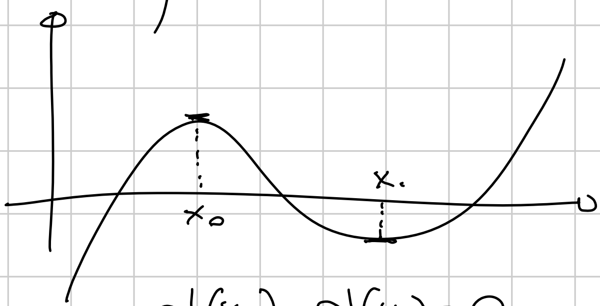
<u>Derivata</u> di un polinomio:

coefficiente di h^1 nello sviluppo di $p(x+h)$

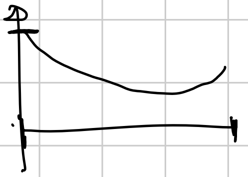
<u>es</u>: $p(x) = x^5$ $\quad p(x+h) = (x+h)^5 = x^5 + \underbrace{5x^4}_{\substack{\shortparallel \\ \text{derivata}}} h + \dots$

$$p'(x) = 5x^4$$

(Risultato: se $p(x)$ ha un massimo/minimo locale in x_0 allora $p'(x_0) = 0$)



$$p'(x_0) = p'(x_1) = 0$$



<u>Teo</u>: se $q^2(x) \mid p(x) \in \mathbb{R}[x]$,

allora $q(x) \mid p'(x)$

(e quindi $q(x) \mid \mathrm{mcd}(p(x), p'(x))$)

CRITERIO DELLA DERIVATA

Regole calcolo derivate:

1) se $p(x) = x^n$, $p'(x) = n x^{n-1}$.

2) $(\alpha p(x) + \beta q(x))' = \alpha p'(x) + \beta q'(x)$. $(\alpha, \beta \in \mathbb{R})$

$\boxed{3}$) $(p(x)q(x))' = p(x)q'(x) + p'(x)q(x)$.

ES: $p(x) = x^3 + 4x + 2$ $\quad p'(x) = 3x^2 + 4 + 0$

$p''(x) = 6x$ $\quad p'''(x) = 6$

$p''''(x) = 0$

$p'''''(x) = 0$

Dim. criterio derivata:

$$p(x) = q(x)^2 r(x) = q(x) \cdot q(x) \cdot r(x)$$

$$p'(x) = \underbrace{q'(x)q(x)r(x) + q(x)q'(x)r(x) + q(x)q(x)r'(x)}_{\text{tutti gli addendi sono multipli di } q(x)} \quad \square$$

Caso particolare: se $p(x)$ ha una radice doppia $p(x) = (x-\alpha)^2 q(x)$, allora $p'(x)$ ha la stessa radice α

(Generalizzazione: se $p(x)$ ha una radice di molteplicità K, allora hanno le stesse radice anche $p'(x), p''(x) \dots p^{\overbrace{''\dots'}^{K-1 \text{ volte}}}(x)$

ES: voglio fattorizzare $x^4 + 2x^3 - 3x^2 - 4x + 4 =: p(x)$

$$p'(x) = 4x^3 + 6x^2 - 6x - 4$$

$$\mathrm{mcd}(p, p') = \mathrm{mcd}(p', \underbrace{x^2+x-2}) = x^2+x-2$$

$$
\begin{array}{l|l}
x^4 \quad 2x^3 \quad -3x^2 \quad -4x \quad 4 & 4x^3+6x^2-6x-4 \\
\cline{2-2}
x^4+\frac{3}{2}x^3-\frac{3}{2}x^2-x & \frac{1}{4}x+\frac{1}{8} \\
\hline
// \quad \frac{1}{2}x^3-\frac{3}{2}x^2-3x+4 & \\
\quad\ \ \frac{1}{2}x^3+\frac{3}{4}x^2-\frac{3}{4}x-\frac{1}{2} & \\
\hline
// \quad -\frac{9}{4}x^2-\frac{9}{4}x+\frac{9}{2} &
\end{array}
$$

$\Rightarrow p$ è multiplo di $(x^2+x-2)^2$

Lemma: $p(x)$, $p(x)+1$ hanno almeno $\deg p + 1$ radici distinte: (per tutti i p non costanti)

$$\left|\{\text{radici di } p(x)\}\right| + \left|\{\text{radici di } p(x)+1\}\right| \geq \deg p + 1$$

dim: criterio della derivata! Poniamo $n = \deg p$

Se $p(x)$ ha radici doppie, sono radici di $\mathrm{mcd}(p, p')$

Se $p(x)+1$ ha radici doppie, sono radici di $\mathrm{mcd}(p+1, p')$

(e queste sono distinte)

$$\#(\text{radici doppie di } p) + \#(\text{radici doppie di } p+1) \leq \underbrace{n-1}_{\substack{\uparrow \\ \text{grado della derivata}}}$$

$$p(x) = (x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}\cdots(x-\alpha_k)^{m_k} \qquad \sum m_i = \sum n_i = n$$

$$p(x)+1 = (x-\beta_1)^{n_1}(x-\beta_2)^{n_2}\cdots(x-\beta_h)^{n_h}$$

$$p'(x) = (x-\alpha_1)^{m_1-1}(x-\alpha_2)^{m_2-1}\cdots(x-\alpha_k)^{m_k-1}\cdot$$
$$\cdot(x-\beta_1)^{n_1-1}(x-\beta_2)^{n_2-1}\cdots(x-\beta_h)^{n_h-1}$$
$$\cdot\, r(x)$$

$$n-1 \geq \sum_{i=1}^{k}(m_i-1) + \sum_{i=1}^{h}(n_i-1) = n-k+n-h$$

$$\boxed{k+h \geq n+1.}$$

Teorema (teorema ABC o Mason-Stothers):

Se $a(x)+b(x)=c(x)$, e $\mathrm{mcd}(a,b,c)=1$

$a(x)b(x)c(x)$ ha almeno grado+1 radici distinte,

dove $\text{grado} = \max(\deg a, \deg b, \deg c) =: n$

(se a,b,c non sono tutti costanti)

Dim:
$$W = a'b - ab'$$

$$\deg W \leq 2n-1$$

Tra le radici di W ci sono le radici doppie di a e le radici doppie di b, e anche quelle di c, perché

$$ac' - a'c = a(\cancel{a'}+b') - a'(\cancel{a}+b) = -W.$$

(+ conto con le molteplicità). $\square$

Questo si usava in RMM 18:

Dire se esistono $p(x), q(x) \in \mathbb{R}[x]$ non costanti tali che $p(x)^{10} + p(x)^9 = q(x)^{21} + q(x)^{20}$.

<u>Modo 1</u>: $p^9(x)\big(p(x)+1\big) = q(x)^{20}\big(q(x)+1\big)$ (*)

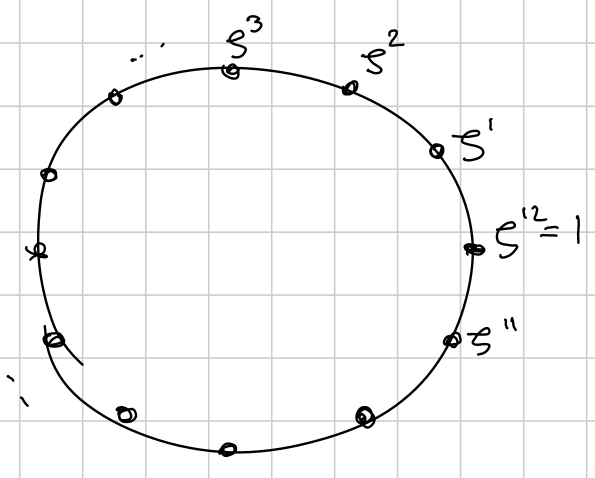
+ lemma di sopra + conti molteplicità.

<u>Modo 2</u>: Derivo la relazione:

$$9p^8(p+1)p' + p^9 p' = 20 q^{19}(q+1)q' + q^{20} q' \quad (*)$$

+ combino le due (*), conto gradi e arrivo a un assurdo.

<u>Ciclotomici</u>



$\zeta^2 \; (\zeta^2)^2 \; (\zeta^2)^3 \cdots (\zeta^2)^6 = 1$

$\Rightarrow \zeta^2$ <u>non</u> è primitiva

$\zeta^5 \; (\zeta^5)^2 \; (\zeta^5)^3 \cdots (\zeta^5)^{12} = 1$

$(\zeta^5)^{12}$ è il primo uguale a 1

ζ^5 è primitiva

ζ^k primitiva $\Leftrightarrow \mathrm{mcd}(k, 12) = 1$

Ci sono $\varphi(12)$ radici primitive.

Gli altri sono radici primitive di ordine un divisore di 12, per esempio ζ^2 è una radice sesta primitiva

$$x^{12}-1 = \underbrace{(x-\zeta^1)(x-\zeta^5)(x-\zeta^7)(x-\zeta^{11})}_{\text{radici 12-esime primitive}}\underbrace{(x-\zeta^2)(x-\zeta^{10})}_{\text{radici 6e primitive}}\underbrace{(x-\zeta^4)(x-\zeta^8)}_{\text{radici 3e prim.}}\cdot$$

$$\cdot\underbrace{(x-\zeta^6)}_{\text{radice 2p.}}\underbrace{(x-\zeta^{12})}_{\text{radice 1}^a\text{p.}}\underbrace{(x-\zeta^3)(x-\zeta^9)}_{\text{radici 4e primitive}}$$

$$(x+1)\quad(x-1)\quad(x-i)\quad(x+i)$$

$$\Phi_n(x) = \prod_{\substack{\zeta \text{ radice } n\text{-esima} \\ \text{primitiva di } 1}} (x-\zeta) \qquad \text{ha grado } \varphi(n)$$

$$x^n - 1 = \prod_{d\mid n} \Phi_d(x) \qquad \left(\text{Confrontando gradi, } n = \sum_{d\mid n} \varphi(d)\right)$$

<u>Lemma</u>: i $\Phi_n(x)$ hanno tutti coeff. interi monici

<u>Dim</u>: induzione estesa: $\Phi_n(x) = \dfrac{x^n-1}{\prod_{\substack{d\mid n \\ d\neq n}} \Phi_d(x)}$

Dividendo per poli. monici a coeff. interi, il quoziente è a coeff. interi.

<u>Fatto</u>: sono irriducibili in $\mathbb{Q}[x]$ (e $\mathbb{Z}[x]$, per Gauss)

<u>Fatto</u>: per ogni $a \in \mathbb{N}$, i divisori primi di $\Phi_n(a)$ sono: – $p \mid n$

- $p \equiv 1 \pmod n$

Esempio di uso: <u>teo</u>: esistono infiniti primi congrui a 1 modulo n, per ogni n intero

<u>Dim</u>: supponiamo per assurdo siano finiti, $p_1, p_2, \dots p_k$

$$\Phi_n(n p_1 p_2 \cdots p_k)$$

Φ_n ha termine costante $=1$, quindi $\Phi_n(np_1 \cdots p_k) \equiv 1 \pmod{p_i}$ e $\Phi_n(np_1 \cdots p_k) \equiv 1\ (n)$

$\Rightarrow$ I suoi fattori primi sono "nuovi" primi $\equiv 1 \pmod n$, assurdo.

<u>Def</u>: un polinomio si dice <u>palindromo</u> se

$$a(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$$

$$a_d = a_0, \quad a_{d-1} = a_1, \quad \dots \quad a_{d-k} = a_k \dots$$

es. $3x^3 + 5x^2 + 5x + 3$

<u>Lemma</u>: i ciclotomici sono tutti palindromi

<u>dim</u>: (se ζ^k è primitivo, allora lo è anche ζ^{n-k} ...)

Lemma: $a(x)$ palindromico $\iff x^d \cdot a\left(\frac{1}{x}\right) = a(x)$

$$x^d a\left(\frac{1}{x}\right) = x^d \left(a_d \frac{1}{x^d} + a_{d-1} \frac{1}{x^{d-1}} + \dots + a_1 \frac{1}{x} + a_0 \right)$$

$$= a_d + a_{d-1} x + \dots + a_1 x^{d-1} + a_0 x^d$$

Da questo segue che:

Lemma: se $a(x)$ palindromo e $a(\lambda) = 0$, allora $a\left(\frac{1}{\lambda}\right) = 0$

e hanno anche la stessa molteplicità: segue da

$a(x) = (x-\lambda)\left(x - \frac{1}{\lambda}\right) b(x)$ con $b(x)$ palindromo

Un poly. palindromo di grado dispari ha la "radice speciale" -1.

$$ax^3 + bx^2 + bx + a = 0$$

I polinomi palindromi di grado pari si possono vedere come polinomi in $\left(x + \frac{1}{x}\right) = z$ (a meno di dividere per potenze)

ES: $\frac{ax^4 + bx^3 + cx^2 + bx + a}{x^2} = ax^2 + bx + c + b\frac{1}{x} + a\frac{1}{x^2} =$

$=$ polinomio in 1, $z = x + \frac{1}{x}$, $z^2 = x^2 + \frac{1}{x^2} + 2$

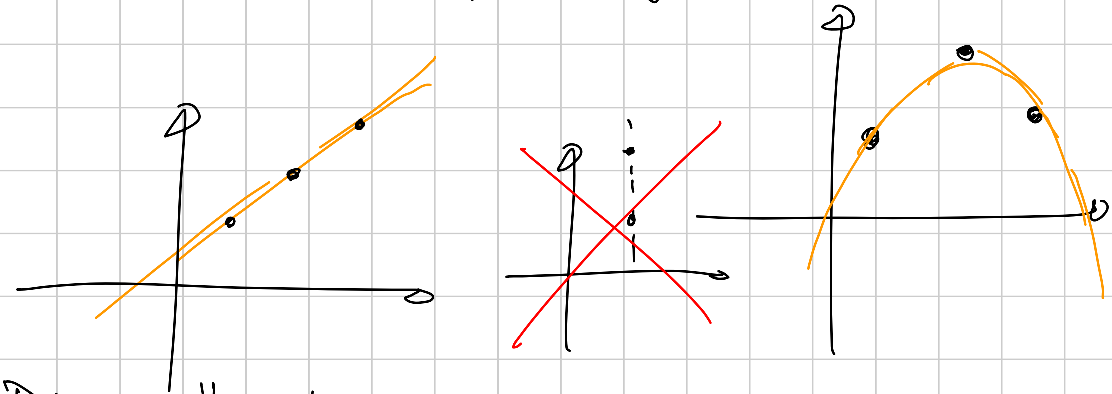
$= az^2 + bz + c - 2a$

(ES: trovare le radici di $\underbrace{x^4 + x^3 + x^2 + x + 1}_{= \Phi_5(x)} = 0$)

(Qualche volta si vedono anche polinomi tali che $a_k = -a_{d-k}$)

Interpolazione polinomiale (o di Lagrange):

Teo: date $n+1$ coppie $(x_1, y_1), (x_2, y_2) \dots$
$\dots (x_{n+1}, y_{n+1})$ in $\mathbb{K}^2$
con x_i distinti a due a due,
esiste uno e un solo polinomio di grado
$\leq n$ tale che $p(x_i) = y_i \ \forall i$



Dim: "Sistemone"

$$a(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^n \\ 1 & x_2 & x_2^2 & \cdots & x_2^n \\ \vdots & & \vdots & & \vdots \\ 1 & x_{n+1} & x_{n+1}^2 & \cdots & x_{n+1}^n \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{n+1} \end{bmatrix}$$

Vogliamo dire che la matrice

$$\begin{bmatrix} 1 & x_1 & \cdots & x_1^n \\ \vdots & & & \vdots \\ 1 & x_{n+1} & \cdots & x_{n+1}^n \end{bmatrix}$$

è invertibile, cioè che produce sistemi lineari con una e una sola soluzione (non importa il termine noto).

Ci basta considerare

$$\begin{bmatrix} 1 & x_1 & \cdots & x_1^n \\ \vdots & & & \vdots \\ 1 & x_{n+1} & \cdots & x_{n+1}^n \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \qquad (*)$$

e dire che ha solo la soluzione 0.

Interpreto le $(*)$ come condizioni su $b(x) = b_0 + b_1 x + \cdots + b_n x^n$

Ci dicono che $b(x_1) = b(x_2) = \cdots = b(x_{n+1}) = 0$.

$\Rightarrow$ b dev'essere il polinomio 0.

Strategie per costruire esplicitamente questo polinomio:

(1) "sistemone" (Vandermonde)

(2) "aggiusto un valore senza cambiare gli altri" (Lagrange)

Idea: trovo prima di tutto per ogni i un polinomio $L_i(x)$ tale che

$$L_i(x_1)=0,\ L_i(x_1)=0,\ \dots\ L_i(x_{i-1})=0,\ L(x_i)=1,$$
$$L_i(x_{i+1})=0\ \dots\ L(x_{n+1})=0$$

$$L_i(x)=\frac{(x-x_1)(x-x_2)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_n)(x-x_{n+1})}{(x_i-x_1)(x_i-x_2)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_{n+1})}$$

Ora, $p(x)=\sum_{i=1}^{n+1} y_i L_i(x)$

$$p(x_k)=\sum_{i=1}^{n+1} y_i L_i(x_k)=y_k L_k(x_k)=y_k$$

$x_1=0,\ x_2=1,\ x_3=3$ $\qquad y_1=a \quad y_2=b \quad y_3=c$

$$L_1(x)=\frac{(x-1)(x-3)}{(0-1)(0-3)} \qquad \begin{cases} L_1(0)=1 \\ L_1(1)=0 \\ L_1(3)=0 \end{cases}$$

$$L_2(x)=\frac{x(x-3)}{(1-0)(1-3)} \qquad \begin{cases} L_2(0)=0 \\ L_2(1)=1 \\ L_2(3)=0 \end{cases}$$

$$L_3(x)=\frac{(x-0)(x-1)}{(3-0)(3-1)} \qquad \begin{cases} L_3(0)=0 \\ L_3(1)=0 \\ L_3(3)=1 \end{cases}$$

$$aL_1(x)+bL_2(x)+cL_3(x)$$

3. "aggiusto un valore per volta senza cambiare i precedenti" Newton

Parto prendendo un polinomio tale che $p(x_0)=y_0$, per esempio $p(x)=y_0$

Poi sommo una "correzione" che cambia valore in x_1 ma non in x_0:

$$y_0 + (x-x_0)\cdot\frac{y_1-y_0}{x_1-x_0}$$

Poi sommo "correzione" che cambia $p(x_2)$ ma lascia invariati $p(x_0), p(x_1)$

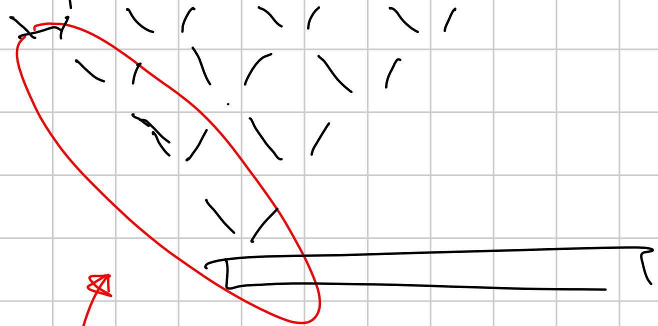
$$y_0 + (x-x_0)\frac{y_1-y_0}{x_1-x_0} + (x-x_0)(x-x_1)\cdot\frac{y_2-\cdots\cdots}{(x_2-x_0)(x_2-x_1)}$$

ES:

$p(0)=3 \qquad p(1)=0 \qquad p(3)=2$

$$3 + x\cdot(-3) + x(x-1)\cdot\frac{8}{6}$$

$p(0) \quad p(1) \quad p(2) \quad p(3) \quad p(4) \quad \cdots$



i coefficienti del metodo-Newton sono la prima colonna della tabella delle differenze finite

A2 MEDIUM

Note Title 9/5/2018

$$\left(\sum_{i=1}^{n} a_i b_i\right)^2 \leq \left(\sum_{i=1}^{n} a_i^2\right)^{\cancel{1/2}} \left(\sum_{i=1}^{n} b_i^2\right)^{\cancel{1/2}}$$

$\boxed{\text{SOS}}$ (sum of squares)

$$LHS = \sum_{i,j=1}^{n} a_i b_i a_j b_j \qquad RHS = \sum_{i,j=1}^{n} a_i^2 b_j^2$$

$$2(RHS - LHS) = \sum_{i,j=1}^{n} \left(\underbrace{a_i b_j - a_j b_i}\right)^2 = \geq 0$$

$$= \underbrace{\boxed{\sum_{i,j=1}^{n} a_i^2 b_j^2}}_{RHS} + \underbrace{\boxed{\sum_{i,j=1}^{n} a_j^2 b_i^2}}_{RHS} \underbrace{\boxed{- 2\sum_{i,j=1}^{n} a_i b_i a_j b_j}}_{2 LHS}$$

$$RHS - LHS \qquad a_i^2 b_j^2 - a_i a_j b_i b_j$$

$$\frac{a^2+b^2}{2} \geq ab \iff (a-b)^2 \geq 0$$

Omogeneizzazione / disomogeneizzazione:

$f(x_1, x_2, \dots x_n)$ si dice

omogenea di grado d se

$$f(\lambda x_1, \lambda x_2, \dots \lambda x_n) = \lambda^d f(x_1, \dots x_n)$$

es: $f(a,b,c) = a^2+b^2+c^2$ $\quad f(\lambda a, \lambda b, \lambda c) = \lambda^2(a^2+b^2+c^2)$

$\Rightarrow$ omogenea di grado 2

$\sum_{cyc} a\sqrt{b} = a\sqrt{b}+b\sqrt{c}+c\sqrt{a}$ om. di grado $3/2$

$\frac{a}{b}+\frac{b}{c}+\frac{c}{a}$ omog. di grado 0

$f(x_1, \dots x_n)$ con f omogenea di grado d'

$g(x_1, x_2, \dots x_n)$ omogenea di grado $d \neq 0$

Allora $f(x_1, \dots x_n) \geq 0$ è vera $\forall (x_1, \dots x_n) \in \mathbb{R}^n$ positivi

se e solo se ($\Leftarrow$) è vera per tutti gli x che soddisfano
$g(x_1 \dots x_n) = C > 0$

Dim: $\Rightarrow$ ovvia

$\Leftarrow$ normalizzo: Data $y_1, \dots y_n$
tale che $g(y_1 \dots y_n) = D \neq C$, scelgo λ
tale che $g(\lambda y_1 \dots \lambda y_n) = \lambda^d \cdot D = C$
Allora, la n-upla $(\lambda y_1 \dots \lambda y_n)$ soddisfa il vincolo

e quindi $f(\lambda y_1, \dots \lambda y_n) \geq 0$

Ma allora $f(y_1, \dots y_n) = \dfrac{f(\lambda y_1, \dots \lambda y_n)}{\lambda^d} \geq 0$

Se ho dimostrato (*) $\dfrac{x^2+y^2}{2} \geq xy$ per tutte le coppie tali che $x^2+y^2=1$, allora l'ho dimostrato per tutte le coppie x, y positive

Tipicamente (*) viene scritta in versione non-omogenea,

(*) $xy \leq \frac{1}{2}$

e devo omogeneizzare, cioè moltiplicare per avere tutti i termini "dello stesso grado"

⚠ serve grado (vincolo) $\neq 0$: se so dimostrare $\dfrac{x^2+y^2}{2} \geq xy$ per tutte le 2-uple con $\dfrac{x}{y} + \dfrac{y}{x} = 1$, allora non basta

---

$$\sum_i a_i b_i \leq \left(\sum_i a_i^2\right)^{\frac{1}{2}} \left(\sum_i b_i^2\right)^{\frac{1}{2}}$$

Omogeneizziamo: posso supporre $\sum_i a_i^2 = 1$

posso supporre $\sum_i b_i^2 = 1$

Posso ricondurmi a dimostrare

$\sum a_i b_i \leq 1$ per tutte le (a_i, b_i) t.c. $\sum_i a_i^2 = \sum_i b_i^2 = 1$

$$\sum_{i=1}^{n} a_i b_i \le \sum_{i=1}^{n} \frac{a_i^2+b_i^2}{2} = \frac{1}{2}\sum_{i=1}^{n} a_i^2 + \frac{1}{2}\sum_{i=1}^{n} b_i^2 = 1 \quad \checkmark$$

Questa dim. si generalizza a molti casi:

G1

- $$\sum a_i b_i c_i \le \left(\sum a_i^3\right)^{1/3} \left(\sum b_i^3\right)^{1/3} \left(\sum c_i^3\right)^{1/3}:$$

omogeneizzo, poi

$$\sum_{i=1}^{n} a_i b_i c_i \le \sum_{i=1}^{n} \frac{a_i^3+b_i^3+c_i^3}{3}$$

G2

- $$\sum a_i b_i \le \sum \left(\frac{1}{2}a_i^2 + \frac{1}{2}b_i^2\right)$$

$$\sum a_i b_i \le \sum \frac{1}{p} a_i^p + \frac{1}{q} b_i^q \quad \text{se } \frac{1}{p}+\frac{1}{q}=1 \quad \left(\begin{array}{l}\text{medie pesate}\\ \text{con pesi } \frac{1}{p}, \frac{1}{q}\end{array}\right)$$

Potete dimostrare

$$\sum_{i=1}^{n} a_i b_i \le \left(\sum_{i=1}^{n} a_i^p\right)^{1/p} \left(\sum_{i=1}^{n} b_i^q\right)^{1/q} \quad \forall\ \frac{1}{p}+\frac{1}{q}=1$$

Hölder

(Generalizzazioni ulteriori sono possibili... n specie diverse con pesi $\frac{1}{r_1}+\frac{1}{r_2}+\dots+\frac{1}{r_n}=1$)

<u>OSS</u>: perché le disuguaglianze sono omogenee?

$$x^3+y^3+z^3 \ge x^2+y^2+z^2 \quad \forall x,y,z \ge 0 \ ?$$

Se fosse vera $\forall x,y,z>0$, allora

$$(\lambda x)^3+(\lambda y)^3+(\lambda z)^3 \geq (\lambda x)^2+(\lambda y)^2+(\lambda z)^2 \quad \forall x,y,z,\lambda$$

impossibile se λ è abb. piccolo.

$$x^3+y^3+z^3 \geq \frac{x^2+y^2+z^2}{\lambda} \quad \forall \lambda, x,y,z$$

Analogamente, $x^2+y^2+z^2 \geq x^3+y^3+z^3$ fallisce se prendete λ abb. grande

---

$$\sum_{i=1}^{n} a_i^2 \leq \sum_{i=1}^{n} \frac{a_i^3+a_i}{2}$$

$$\text{GR}.2 \leq \text{GR}.3+\text{GR}\,1$$

---

medie pesate: $\underbrace{a,\dots,a}_{n_1}, \underbrace{b,b,\dots b}_{n_2}, \underbrace{c,\dots c}_{n_3}$.

$$a^{\overbrace{\frac{n_1}{n_1+n_2+n_3}}^{w_1}} b^{\overbrace{\frac{n_2}{n_1+n_2+n_3}}^{w_2}} c^{\overbrace{\frac{n_3}{n_1+n_2+n_3}}^{w_3}} \leq \frac{n_1 a}{n_1+n_2+n_3}+\frac{n_2 b}{n_1+n_2+n_3}+\frac{n_3 c}{n_1+n_2+n_3}$$

$$\boxed{a^{w_1} b^{w_2} c^{w_3} \leq w_1 a+w_2 b+w_3 c} \quad w_1+w_2+w_3=1.$$

$w_1,w_2,w_3 \in \mathbb{Q}$

ma anche $\in \mathbb{R}$,
Costruendo successioni w_1^n, w_2^n, w_3^n di razionali che tendono a w_1,w_2,w_3

Medie pesate: $\prod a_i^{w_i} \leq \sum w_i a_i$ $\quad \forall a_i \geq 0$, $\forall w_i \in [0,1]$ t.c. $\sum w_i = 1$

(ES: esiste CS pesato?)

Modi "strani" di usare CS:

Disuguaglianza di Nesbitt:

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geq \frac{3}{2}$$

Dimostrazione con CS: $\quad \sum x_i y_i \leq$

tipo: HM-AM

$$\left[\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right)(a+b+c) \geq 9\right]$$

$$\frac{a}{b+c} =: x_1^2 \qquad \frac{b}{c+a} =: x_2^2 \qquad \frac{c}{a+b} =: x_3^2$$

$$x_1 = \frac{\sqrt{a}}{\sqrt{b+c}} \quad \text{e cicliche}$$

$$y_1 = \sqrt{a}\sqrt{b+c} \quad \text{e cicliche}$$

$$\left(\sum_{cyc} \frac{\sqrt{a}}{\cancel{\sqrt{b+c}}} \cdot \sqrt{a}\,\cancel{\sqrt{b+c}}\right)^2 \leq \left(\sum_{cyc} \frac{a}{b+c}\right)\left(\sum_{cyc} a(b+c)\right)$$

$$\sum_{cyc} \frac{a}{b+c} \geq \boxed{\frac{(a+b+c)^2}{\sum_{cyc} a(b+c)}} = \frac{(a+b+c)^2}{2\sum_{cyc} ab} = \boxed{\frac{\sum_{cyc} a^2 + 2\sum_{cyc} ab}{2\sum_{cyc} ab}}$$

$$\geq \frac{3\cancel{\sum ab}}{2\cancel{\sum ab}}$$

$$a^2+b^2+c^2 \geq ab+bc+ca$$

Lemma di Titu:

$$\sum \frac{a_i^2}{b_i} \geq \frac{(\sum a_i)^2}{(\sum b_i)} \quad \text{per } a_i, b_i \text{ n-uple di reali positivi}$$

È CS applicata a $\frac{a_i}{\sqrt{b_i}}$ e $\sqrt{b_i}$

IMO 2001

$$\sum \frac{a}{\sqrt{a^2+8c}} \geq 1$$

IMO 2005/3 se $\boxed{xyz \geq 1}$, allora

$$\sum_{cyc} \frac{x^5-x^2}{x^5+y^2+z^2} \geq 0$$

Trucco 1: manipolare le frazioni per migliorare il numeratore:

$$\sum_{cyc} \frac{\cancel{x^5}-x^2-\cancel{x^5}-y^2-z^2}{x^5+y^2+z^2} \geq -1-1-1$$

$$\sum_{cyc} \frac{x^2+y^2+z^2}{x^5+y^2+z^2} \leq 3$$

Voglio una disuguaglianza con oggetti di questo tipo:

$$x^5+y^2+z^2 \quad \geq \quad x^2+y^2+z^2$$

CS su $(\sqrt{x^5}, y, z)$ e $(\sqrt{\frac{1}{x}}, y, z)$ $\qquad xyz \geq 1 \Rightarrow \frac{1}{x} \leq yz$

$$\underbrace{(x^5+y^2+z^2)}\left(\frac{1}{x}+y^2+z^2\right) \geq \underbrace{(x^2+y^2+z^2)^2}$$

$$\sum_{cyc} \frac{x^2+y^2+z^2}{x^5+y^2+z^2} \leq \sum_{cyc} \frac{\frac{1}{x}+y^2+z^2}{x^2+y^2+z^2} \leq \sum_{cyc} \frac{yz+y^2+z^2}{x^2+y^2+z^2} = \frac{\sum_c yz + 2\sum_c y^2}{x^2+y^2+z^2}$$

$$\leq \frac{\sum_{cyc} y^2 + \sum_{cyc} y^2 + \sum_{cyc} z^2}{x^2+y^2+z^2} = 3$$

(catene di disuguaglianze sono un buon modo di scrivere soluzioni)

<u>Riarrangiamento</u>

Se σ è una permutazione di $\{1, 2, \dots n\}$

se $a_1 \leq a_2 \leq \dots \leq a_n$
$b_1 \leq b_2 \leq \dots \leq b_n$, allora

$$\sum_{i=1}^{n} a_i b_{n+1-i} \leq \sum_{i=1}^{n} a_i b_{\sigma(i)} \leq \sum_{i=1}^{n} a_i b_i$$

<u>Dim</u>: sia σ_* tale che $\sum_{i=1}^{n} a_i b_{\sigma_*(i)}$ = <u>massimo</u>,
(che esiste perché è su un # finito di permutazioni)
supponiamo per assurdo che non sia l'identità.
Allora esisteranno $i<j$ t.c. $\sigma(i) > \sigma(j)$

$$\dots + a_i b_{\sigma(i)} + a_j b_{\sigma(j)} + \dots \quad \text{(altri addendi)}$$

Ma allora se "raddrizzo" i due termini ottengo qualcosa di più grande:

$$a_i b_{\sigma(j)} + a_j b_{\sigma(i)} \geq a_i b_{\sigma(i)} + a_j b_{\sigma(j)}$$

$$\underbrace{(a_j - a_i)}_{\geq 0} \underbrace{(b_{\sigma(i)} - b_{\sigma(j)})}_{\geq 0} \geq 0$$

$\square$

Dimostrazione di AM-GM via "smoothing"

Partiamo da una n-upla

$$(a_1, a_2, \dots a_n)$$

supponiamo che non siano tutti uguali; allora costruisco

$$(b_1, b_2, \dots b_n)$$

tale che $AM(a_1 + a_2 + \dots + a_n) = AM(b_1, b_2, \dots b_n)$,

e $GM(b_1, b_2, \dots b_n) > GM(a_1, a_2, \dots a_n)$

Tra gli a_i ci sarà sicuramente uno, diciamo a_i, tale che $a_i > AM$, e uno a_j con $a_j < AM$.

Allora prendo

$$(b_1, b_2, \dots b_n) = (a_1, a_2, \dots a_i - \varepsilon, \dots a_j + \varepsilon, \dots a_n)$$

$AM(b_i)$ è uguale

$$GM(b) = GM(a) \cdot \frac{\sqrt[n]{a_i - \varepsilon}\,\sqrt[n]{a_j + \varepsilon}}{\sqrt[n]{a_i}\,\sqrt[n]{a_j}}$$

$$(a_i - \varepsilon)(a_j + \varepsilon) = a_i a_j + \underbrace{(a_i - a_j - \varepsilon)}_{+}\varepsilon > a_i a_j$$

> 0 se ε è abbast. piccolo

Se (a_i) non sono tutti uguali, posso far salire la media geometrica avvicinandoli $\Rightarrow$ il max dev'essere quando sono tutti uguali!

non funziona, senza argomenti sull'esistenza del massimo

Teo: il numero intero positivo più grande è 1

Dim: prendiamo $a \neq 1$. Allora $a^2 > a$.

Come si aggiusta la dim. con le medie?

(1) dimostrando che il max. esiste:

Teo: Weierstrass:

Sia $f : U \subseteq \mathbb{R}^n \to \mathbb{R}$. Se U è chiuso e limitato, allora f ammette massimo (e minimo).

Chiuso: definito tramite uguaglianze, $\leq$, $\geq$ (non $<$ e $>$)

limitato: esiste $M \in \mathbb{R}$ tale che $|x_i| \leq M$ per ogni coordinata x_i di $x \in U$

$f(x_1, x_2, \dots x_n) = x_1 x_2 \cdots x_n$

Dove $(x_1, \dots x_n)$ è tale che $x_i \geq 0$

e $x_1 + x_2 + \cdots + x_n = a_1 + a_2 + \cdots + a_n$

chiuso ✓ limitato ✓ $|x_i| \leq a_1 + a_2 + \cdots + a_n$

$\Rightarrow$ (Weierstrass) esiste una n-upla $(x_1, x_2, \dots, x_n)$ che massimizza il prodotto

Ora la dim. funziona:

prendo $(b_1, b_2, \dots b_n)$ che massimizza ($\exists$ per W-strass)

suppongo che b_i non tutti uguali

costruisco una $(c_1, c_2, \dots c_n)$ con prodotto maggiore stretto, assurdo.

(2) oppure:

Lo trasformo in un procedimento che termina in un # finito di passi: prendo $(a_1, \dots a_n)$ t.c. $a_i > M > a_j$,

e lo rimpiazzo con $(a_1, \dots \underset{\cancel{a_i}}{M}, \underset{\cancel{a_j}}{a_i + a_j - M} \dots a_n)$

$$M(a_i + a_j - M) > a_i a_j \text{, perché}$$

$$(a_i - M)(M - a_j) > 0$$

Questo proc. termina in al più n passi, perché ogni volta aumentano il numero degli a_k uguali a M.

Bunching:

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \overset{?}{\geq} 3/2$$

$$2\sum_{cyc} a(a+c)(a+b) \geq 3(b+c)(c+a)(a+b)$$

$$2\sum_{cyc}\left(a^3 + \underbrace{a^2c + a^2b} + abc\right) \geq 3\left(\sum_{sym}(a^2b) + 2abc\right)$$

$$\sum_{sym} a^3 + 2\sum_{sym} a^2b + \sum_{sym} abc \geq 3\sum_{sym} a^2b + \sum_{sym} abc$$

$$[3,0,0] + \cancel{2[2,1,0]} + \cancel{[1,1,1]} \geq \cancel{3}[2,1,0] + \cancel{[1,1,1]}$$

$$[3,0,0] \geq [2,1,0]$$

<u>vera</u> perché le somme parziali di $[3,0,0]$ battono le somme parziali di $[2,1,0]$:

$$3 \geq 2$$
$$3+0 \geq 2+1$$
$$3+0+0 = 2+1+0$$

Schur: $[r+2s,0,0] + [r,s,s] \geq 2[r+s,s,0]$ (*)

(nota che non segue da Bunching, perché $[r+2s,0,0] \geq [r+s,s,0] \geq [r,s,s]$)

Schur-Vornicu:

se $a,b,c \geq 0$ e $x,y,z \geq 0$

sono ordinate nello stesso modo,

allora

$$x(a-b)(a-c)+y(b-a)(b-c)+z(c-a)(c-b)\geq 0$$

Dim: possiamo supporre

$$x\geq y\geq z \quad e \quad a\geq b\geq c$$

Allora,

$$\underbrace{\underbrace{x(a-b)(a-c)}_{\geq 0}+\underbrace{y(b-a)(b-c)}_{\leq 0}}_{\geq 0}+\underbrace{z(c-a)(c-b)}_{\geq 0}\geq 0$$

$$\begin{array}{ccc} x & \geq & y \\ a-c & \geq & b-c \\ a-b & = & a-b \end{array}$$

$$x(a-c)(a-b)\geq -y(b-c)(b-a)$$

Di solito, $x, y, z = a^r, b^r, c^r$

$$\sum_{cyc} a^r(a-b)(a-c)\geq 0$$

oppure

$$\sum_{cyc} a^r(a^s-b^s)(a^s-c^s)\geq 0 \qquad (*)$$

oppure

$$\sum_{cyc} a(a-b)(a-c)\geq 0 \qquad (*)$$

Metodo ABC, SPQ, PQR

Idea 1: tutte le disuguaglianze polinomiali, simmetriche, omogenee in $a,b,c\geq 0$ si possono riscrivere

in funzione di $S = a+b+c$
$Q = ab+bc+ca$
$P = abc$

ES: Schur (*):

$$(*) \quad \sum_{cyc} \left(a^3 - a^2b - a^2c + abc\right) \geq 0$$

$$S^3 = a^3+b^3+c^3+3\left(\sum_{sym} a^2b\right) + 6abc$$

$$a^3+b^3+c^3 = S^3 - 3\sum_{sym} a^2b - 6P$$

$$QS = (ab+bc+ca)(a+b+c) = \sum_{sym} a^2b + 3abc$$

$$\sum_{cyc}\left(a^3-a^2b-a^2c+abc\right) = \left(a^3+b^3+c^3\right) - \sum_{sym} a^2b + 3P =$$

$$= S^3 - 3\sum_{sym} a^2b - \sum_{sym} a^2b - 6P + 3P$$

$$= S^3 - 3P - 4\sum_{sym} a^2b = S^3 - 3P - 4(QS - 3P)$$

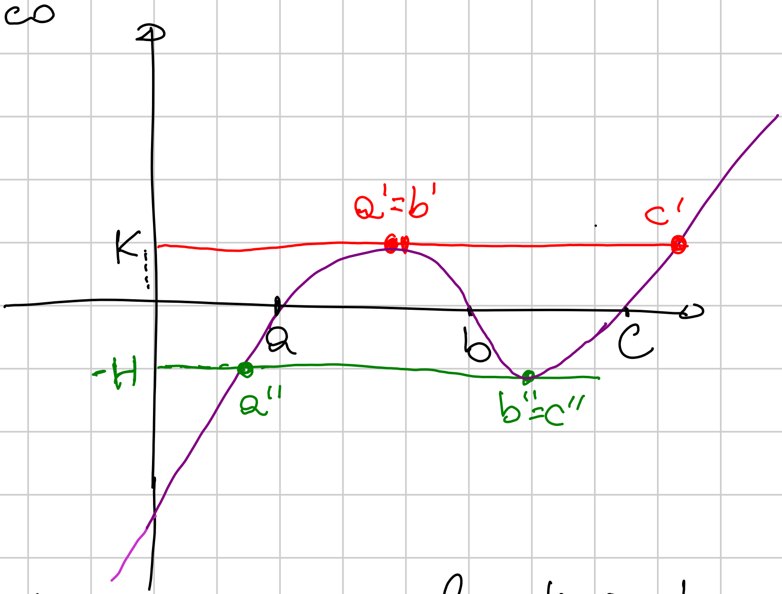
$$= S^3 - 4QS + 9P$$

Schur: $\boxed{S^3 - 4QS + 9P \geq 0}$

Idea 1: dati a,b,c, esistono sempre a', b', c' tali che $S=S'$, $Q=Q'$, $P \geq P'$ (oppure: $P \leq P'$) e ($a'=b'$, oppure $c'=0$)

Scriviamo il polinomio $\lambda^3 - S\lambda^2 + Q\lambda - P =$
$= (\lambda - a)(\lambda - b)(\lambda - c)$

Ha grafico



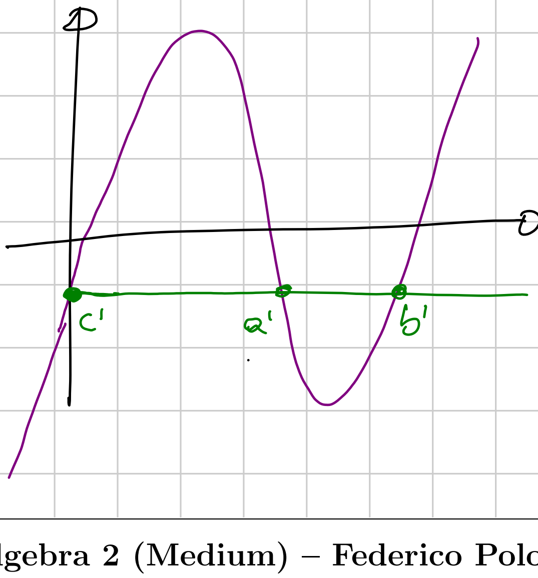
I tre punti in rosso sono le radici di
$\lambda^3 - S\lambda^2 + Q\lambda - P - K = 0$

$a' + b' + c' = S \quad a'b' + b'c' + c'a' = Q \quad a'b'c' = P + K$

I tre pti in verde sono le radici di
$\lambda^3 - S\lambda^2 + Q\lambda - P + H = 0$.

$a'' + b'' + c'' = S \quad a''b'' + b''c'' + c''a'' = Q \quad a''b''c'' = P - H$.

Riesco sempre a trovare a', b', c' o a'', b'', c'' in questo modo?



Idea 2: mi basta dimostrare la mia disuguaglianza per la terna a'', b'', c'', per cui
$$S''=S,\ Q''=Q,\ P''\le P:\ \text{difatti,}$$

$$0\le S''^3-4S''Q''+9P''\le S^3-4SQ+9P$$

$\Rightarrow$ Per dimostrare $S^3-4SQ+9P\ge 0$, mi basta farlo in due casi particolari:
- $a=b$
- $c=0$

Teo: Una disuguaglianza $f(P,Q,S)\ge 0$ (tutte le dis. polinomiali, simmetriche, omogenee, in tre variabili) monotona in P, è vera se e solo se vale nei due casi particolari:
- $a=b$
- $c=0$

ES: Schur:
$$a(a-b)(a-c)+b(b-a)(b-c)+c(c-a)(c-b)\ge 0$$

se $a=b$: diventa $c(c-a)^2\ge 0$ ovvia

se $c=0$: $a^2(a-b)+b^2(b-a)\ge 0 \iff (a^2-b^2)(a-b)\ge 0$

Oss: se la disuguaglianza ha grado ≤ 5, allora è sempre monotona in P.

P^2

$(abc)^2$ ⇒ grado troppo grosso

robe(Q,S) + robe$(Q,S) \cdot P$

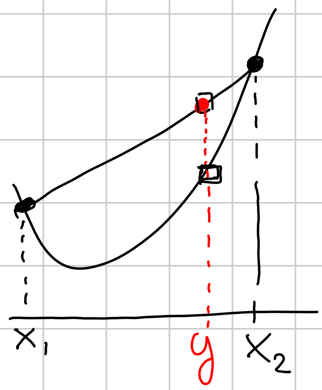
Fissati Q, S, è sempre monotona in P.

Cannone megagalattico: una disuguaglianza simmetrica, omogenea, polinomiale in n variabili di grado d mi basta dimostrarla nel caso in cui le variabili assumono al più $d/2$ valori positivi distinti (e gli altri sono zeri, o copie dei precedenti).

"Half-degree principle".

Convessità:

Def.: f convessa se



$y = \lambda x_1 + (1-\lambda) x_2 \qquad \lambda \in [0,1]$

$$f(y) \leq \lambda f(x_1) + (1-\lambda) f(x_2)$$

$$f(\lambda x_1 + (1-\lambda) x_2) \qquad \forall x_1, x_2 \in \text{dominio}, \quad \forall \lambda \in [0,1]$$

Jensen: dati $x_1, x_2, \dots x_n$ nel dominio della funzione e $w_1, w_2, \dots w_n \in [0,1]$ tali che $w_1 + w_2 + \dots + w_n = 1$,

$$f(w_1 x_1 + \dots + w_n x_n) \leq w_1 f(x_1) + \dots + w_n f(x_n)$$

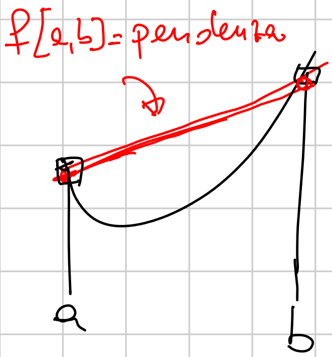
(DIM: induzione "up and down" come per AM-GM.)

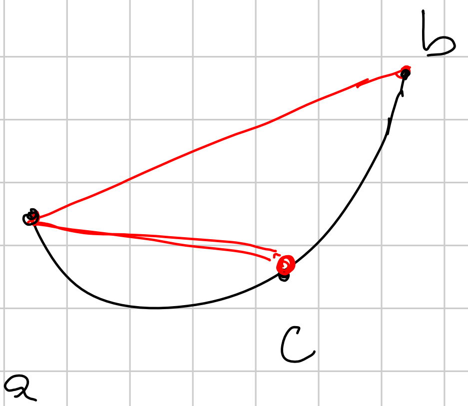
Caratterizzazione alternativa:

f convessa $\Leftrightarrow$ rapporti incrementali sono crescenti

Def: rapporto incrementale:

$$f[a,b] := \frac{f(b) - f(a)}{b - a}$$





per $a \leq c \leq b$

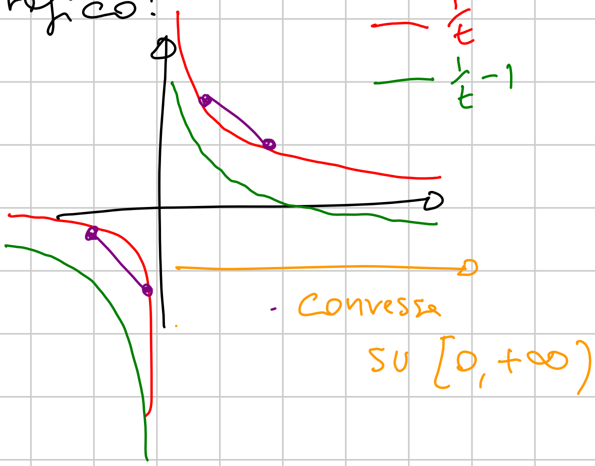
f convessa $\iff f[a,c] \leq f[a,b]$.

$\iff f[a,b] \leq f[c,b]$.

Come si riconosce la convessità?

1) ragionamenti sul grafico:

$f(t) = \frac{1-t}{t} = \frac{1}{t} - 1$



2) Se f è derivabile, f convessa in un intervallo $\iff f''(x) \geq 0$ in ogni punto dell'intervallo.

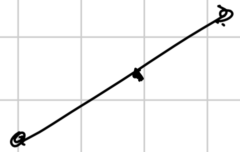
es: $f(t) = \frac{1}{t} - 1 \quad f'(t) = -\frac{1}{t^2} \quad f''(t) = \frac{2}{t^3} \geq 0$ per $t > 0$

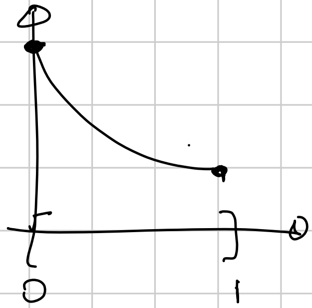
Come si usa?

- $\frac{1}{3}\frac{1-a}{a} + \frac{1}{3}\frac{1-b}{b} + \frac{1}{3}\frac{1-c}{c} \geq \dfrac{1-\left(\frac{a+b+c}{3}\right)}{\frac{a+b+c}{3}}$

$f(t) = \frac{1-t}{t}$, pesi $= \frac{1}{3}, \frac{1}{3}, \frac{1}{3}$ (Nesbitt dopo aver posto $a+b+c=1$)

- Se f convessa in $[a,b]$ $\Rightarrow \max(f)$ sta sul bordo, cioè $f(a)$ o $f(b)$





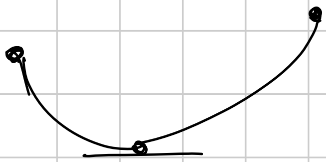
Per ogni $x_i \in [0,1]$

ES: $x_1+x_2+\dots+x_n-(x_1x_2+\dots+x_nx_1) \leq \left\lfloor \frac{n}{2} \right\rfloor$

lineare in $x_1 \Rightarrow$ max assunto o per $x_1=0$
o per $x_1=1$

stessa cosa vale in tutti gli x_i

$\Rightarrow$ max assunto quando un po' degli x_i sono uguali a 1 e gli altri sono uguali a 0.

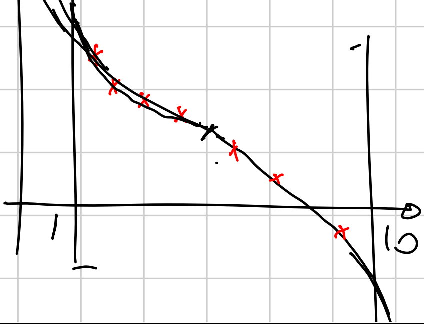


$$f\left(\frac{a+b}{2}\right) \leq \frac{1}{2}f(a)+\frac{1}{2}f(b)$$

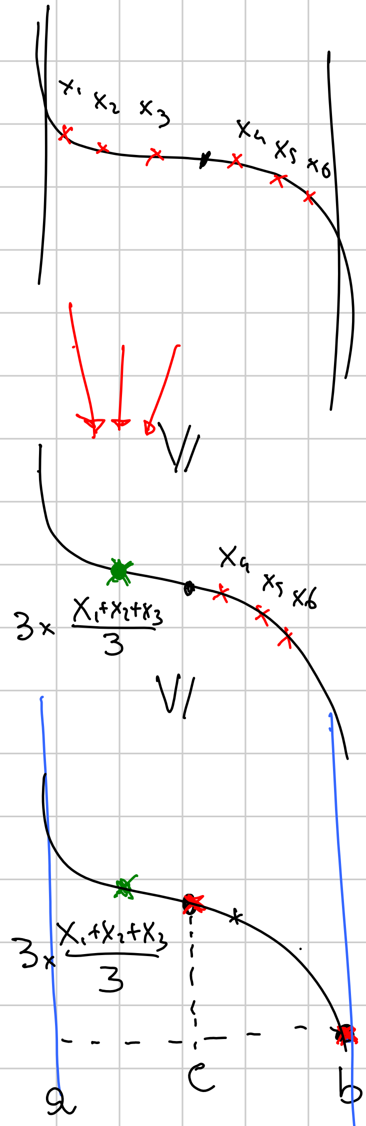
$f(a)+f(b) \geq 2f\left(\frac{a+b}{2}\right) \Rightarrow$ se $a+b$ è fissato,

$f(a)+f(b)$ è minimo quando sono uguali

Idea più avanzata che si vede qualche volta:



funzione convessa-concava
$x_1, \dots, x_n$ dentro
l'intervallo,
$x_1+x_2+\dots+x_n$ fissato



Quando è minimo
$f(x_1)+f(x_2)+\dots+f(x_n)$?

Posso rimpiazzare $f(x_1), f(x_2), f(x_3)$ (zona convessa) con $3f\left(\frac{x_1+x_2+x_3}{3}\right)$

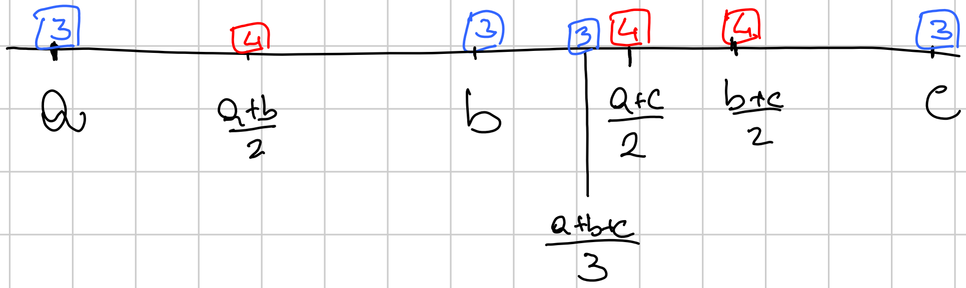
e posso rimpiazzare $f(x_4)+f(x_5)+f(x_6)$ con una combin. di $f(c)$ e $f(b)$

$x_4=\lambda c+(1-\lambda)b$

$f(x_4)\geq \lambda f(c)+(1-\lambda)f(b)$

ES: Sia f convessa, $f:[0,1]\to\mathbb{R}$ dimostrare che a,b,c nel suo dominio
Dimostrare che

$$4f\left(\frac{a+b}{2}\right)+4f\left(\frac{b+c}{2}\right)+4f\left(\frac{c+a}{2}\right)\leq 3f(a)+3f(b)+3f(c)+3f\left(\frac{a+b+c}{3}\right).$$



$$f\left(\frac{a+b}{2}\right) \leq \frac{1}{2}f(a) + \frac{1}{2}f(b)$$

$$2f\left(\frac{a+b}{2}\right) \leq f(a) + f(b)$$

$$4f\left(\frac{a+b}{2}\right) \leq 2f(a) + 2f(b)$$

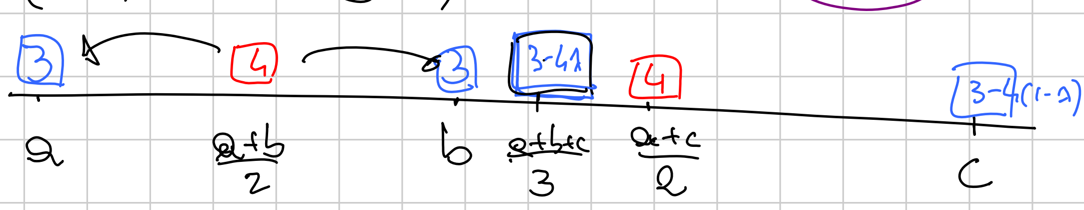
$$f\left(\frac{a+b+c}{3}\right) \leq \frac{1}{3}f(a) + \frac{1}{3}f(b) + \frac{1}{3}f(c)$$

$$\frac{a+b+c}{3} =: m$$

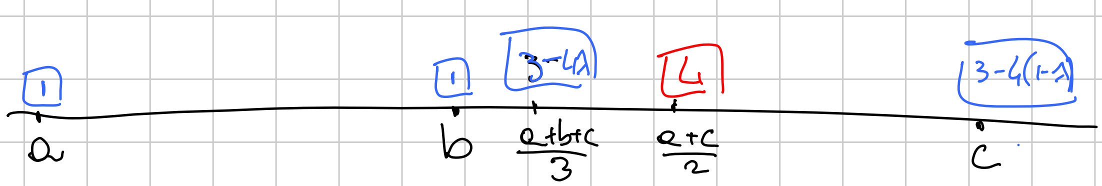
$$\frac{b+c}{2} = \lambda \cdot \frac{a+b+c}{3} + (1-\lambda)c \qquad \lambda(c-m) = c - \frac{b+c}{2} = \frac{c-b}{2}$$

$$\lambda = \frac{c-b}{c-m} \cdot \frac{1}{2}$$

$$4f\left(\frac{b+c}{2}\right) \leq 4\lambda f\left(\frac{a+b+c}{3}\right) + 4(1-\lambda)f(c)$$ iii



$$4f\left(\frac{a+b}{2}\right) \leq 2f(a) + 2f(b)$$ ii



Nota che $\quad 1+1+(3-4\lambda)+3-4(1-\lambda)=4$

$$1\cdot a+1\cdot b+(3-4\lambda)\cdot\frac{a+b+c}{3}+(3-4(1-\lambda))\cdot c=4\,\frac{a+c}{2}$$

$$\frac{1}{4}f(a)+\frac{1}{4}f(b)+\frac{3-4\lambda}{4}f\left(\frac{a+b+c}{3}\right)+\frac{3-4(1-\lambda)}{4}f(c)\geq f\left(\frac{a+c}{2}\right) \quad (i)$$

(Resta da verificare che $3-4\lambda\geq 0$
$3-4(1-\lambda)\geq 0$)

(Provate a farlo anche con <u>disuguaglianza di Karamata</u>!)

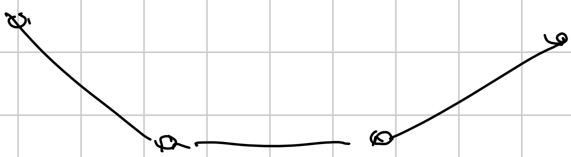
Dati $a_1\leq a_2\leq \dots \leq a_n$
$b_1\leq b_2\leq \dots \leq b_n$

tali che
$$a_n\geq b_n$$
$$a_n+a_{n-1}\geq b_n+b_{n-1}$$
$$a_n+a_{n-1}+\dots+a_k\geq b_n+b_{n-1}+\dots+b_k$$
$$\vdots$$
$$a_n+a_{n-1}+\dots+a_1=b_n+b_{n-1}+\dots+b_1$$

e data f convessa,

<u>allora</u> $f(b_1)+\dots+f(b_n)\leq f(a_1)+\dots+f(a_n)$

<u>ES</u>:



$$f(a_1) \quad f(b_1) \quad f(b_2) \quad f(a_2)$$

$$a_1 \quad b_1 \quad b_2 \quad a_2$$

Sketch dimostrazione:

$$\sum_{i=1}^{n} f(a_i) - f(b_i) = \sum_{i=1}^{n} \underbrace{f[b_i, a_i]}_{\text{crescenti}} \cdot (a_i - b_i)$$

$$f[b_{i+1}, a_{i+1}] - f[b_i, a_i] \geq 0$$

$$\sum_{j \geq i} (a_j - b_j) \geq 0$$

(aggiustare)

$$\sum x_i y_i = \sum_{i=1}^{n-1} (x_{i+1} - x_i)(y_i + y_{i+1} + \dots + y_n)$$

FORMULA DI SOMMAZIONE DI ABEL

(aggiustare)

ALGEBRA 3 medium 4

Titolo nota 07/09/2018

Successioni def. per ricorrenza [LINEARE]

ESEMPIO post-basic

soluzione iniziale

$x_{n+1} = a x_n + b \qquad (x_0 = \text{qualcosa})$

Cerco una "formula chiusa" per x_n

viene da dopo...

$c = ac + b$
$c(1-a) = b$
$\to c = \frac{b}{1-a}$

→ Metodo 1: casi bassi + induzione

$$x_1 = a x_0 + b$$
$$x_2 = a^2 x_0 + ab + b$$
$$x_3 = a^3 x_0 + a^2 b + ab + b$$
$$x_4 = a^4 x_0 + a^3 b + a^2 b + ab + b$$
$$\dots$$
$$x_n = a^n x_0 + a^{n-1} b + a^{n-2} b + \dots + a^0 b$$
$$= a^n x_0 + b\,\frac{a^n - 1}{a-1}$$

(se $a \neq 1$ ... se no succ. aritmetica → + facile)

→ Metodo 2: riduco a una ricorrenza + "standard"

$y_n = x_n + k \qquad y_{n+1} = x_{n+1} + k =$
$a x_n + b + k =$
$= a(x_n + k) - ak + k + b$
$= a y_n + \boxed{b + k(1-a)}$

voglio $= 0$

→ scelgo $k = \frac{b}{a-1}$

NOTA: funziona se $a \neq 1$

→ ottengo

$$y_n = a^n y_0 = a^n \left(x_0 + \frac{b}{a-1}\right)$$
$$x_n = y_n - k = a^n x_0 + \frac{b}{a-1}(a^n - 1)$$

$(x_0 = \text{qualcosa} \ldots)$

$x_{n+1} = 2x_n + n^2$ come faccio?

$y_n = x_n + p(n)$ ← provo a metterci un pol. di 2° grado

$$y_{n+1} = x_{n+1} + p(n+1) = 2x_n + n^2 + p(n+1)$$
$$= \underbrace{2y_n - 2p(n)}_{2x_n} \boxed{- 2p(n) + n^2 + p(n+1)}$$

vorrei $\equiv 0$

$p(n) = an^2 + bn + c$

devo avere
- $a = 1$ $\quad (-2a + 1 + a = 0)$
- $b = 2$ $\quad (-2b + 2a^{=1} + b = 0)$
- $c = 3$ $\quad (-2c + a^{=1} + b^{=2} + c = 0)$

$y_{n+1} = 2y_n$, $\quad y_n = x_n + n^2 + 2n + 3$
$= 2^n y_0$

⇝ formula chiusa per x_n.

PIÚ IN GENERALE

$x_{n+1} = \alpha x_n + \text{roba}(n)$

abbiamo scritto x_n nella forma $y_n + z_n$

risolve l'eq. $y_{n+1} = \alpha y_n$

soluzione dell'equazione originale

... e ancora più in generale

(condizione iniziale: $x_0, \ldots, x_{k-1}$)

$$\underbrace{x_{n+k} - a_{k-1}x_{n+k-1} - a_{k-2}x_{n+k-2} - \ldots - a_0 x_n}_{L(x_n, \ldots, x_{n+k})} = 0 \leftarrow \text{omogenea} \;*$$
$$= \text{roba}(n)$$

LINEARE

NON omogenea *

RICETTA per trovare TUTTE le soluzioni con roba(n)

(ignorando condizioni iniziali):
si scrivono tutte quante come $y_n + z_n$

y_n: soluzione generica dell'omogenea associata (DEVO saperle tutte)

z_n: è UNA soluzione speciale dell'eq. originale

Perché questo è vero?

- sicuramente $y_n + z_n$ risolve ☆; infatti
  $L(y_n + z_n) = L(y_n) + L(z_n) = 0 + \text{roba}(n)$ ✓
- se ho w_n sol. di ☆, dico che $w_n - z_n$ risolve ☆ (quindi w_n si scrive come $z_n + (w_n - z_n)$). $L(w_n - z_n) =$
  $= L(w_n) - L(z_n) = \text{roba}(n) - \text{roba}(n) = 0$

La ricetta funziona se
- sappiamo risolvere ☆ ← risolto! :)
- sappiamo trovare una soluzione di ☆

RIPASSO: come si risolve ☆?

Si guarda il polinomio di deg k
$$x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \dots - a_0 \ ;$$
Considero le sue sol. $\lambda_1, \dots, \lambda_k$; se sono tutte distinte, le sol. di ☆ sono tutte e sole
$$\mu_1(\lambda_1)^n + \mu_2(\lambda_2)^n + \dots + \mu_k(\lambda_k)^n$$

Se ho soluzioni multiple ($\lambda_1, \dots, \lambda_t$ con λ_i di molteplicità $m(i)$)
$$p_1(n)\lambda_1^n + p_2(n)\lambda_2^n + \dots + p_t(n)\lambda_t^n$$
con $p_i(n)$ pol. di deg $m(i)-1$; ovvero

uso come sol. "fondamentali" per λ_i:
$\lambda_i^n \quad n\lambda_i^n \quad n^2\lambda_i^n \quad \dots \quad n^{m(i)-1}\lambda_i^n$.

Cosa sappiamo "indovinare"?
Se roba(n) è un pol. di deg k, provo un pol. di deg k; se roba$(n) = k^n$, provo $c \cdot k^n$.

ESERCIZIO VERO
(quasi)

$$x_{n+2} = x_n + (-1)^n$$
$$c(-1)^{n+2} = c(-1)^n + (-1)^n$$
$$c(-1)^n = (c+1)(-1)^n$$
$$\to c = c+1 \quad ?!?$$

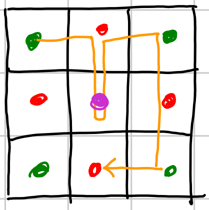
perché ho fallito?

Altro esempio: $x_{n+2} - x_{n+1} - 2x_n = 2^n$
$$4c - 2c - 2c = 1$$

AAAAH! Non funziona perché 2^n è sol di $\mathcal{A}$
Come faccio?! Provo $cn2^n$; lo stesso succede con i polinomi se 1^n è sol. dell'omogenea. Questo metodo (con pol. di grado appropriato a moltiplicare) funziona.
(se roba(n) = somme di polinomi per k^n ...)

... ma a cosa servono?

Problema tipico: ricorrenza in "combinatoria"



percorsi di lunghezza 8
che si muovono da casella
a casella adiacente.

X_n = # percorsi di lunghezza n

A_n = # n che finiscono in •

B_n

C_n

$$\begin{cases} A_n = 2B_{n-1} \\ B_n = 2A_{n-1} + C_{n-1} \\ C_n = 4B_{n-1} \end{cases}$$

$$B_n = 4B_{n-2} + 4B_{n-2} = 8B_{n-2}$$

$$B_{2n} = 8^n B_0 \qquad B_{2n+1} = 8^n B_1$$

(parentesi: $B_n = \mu_1(\sqrt{8})^n + \mu_2(-\sqrt{8})^n$

$$B_{2n} = 8^n(\mu_1+\mu_2)$$

$$B_{2n+1} = 8^n\sqrt{8}(\mu_1-\mu_2)\ )$$

invece ... un problema di algebra

$$a_{n+1} = \frac{a_{n-1}}{1+n\,a_n a_{n-1}} \qquad a_1 = a_0 = 1$$

quanto fa $a_{199} \cdot a_{200}$?

$$a_{n+1}\,a_n = \frac{a_{n-1}\,a_n}{1+n\,a_n a_{n-1}}$$

$$b_n = a_n a_{n-1} \longrightarrow b_{n+1} = \frac{b_n}{1+nb_n} \qquad n \geq 1, \quad b_1 = 1$$

$$\frac{1}{b_{n+1}} = \frac{1}{b_n} + n$$

$$\rightsquigarrow \quad c_{n+1} = c_n + n \qquad \left(c_n = 1/b_n\right) \quad c_1 = 1$$

$$c_n = 1 + 1 + 2 + \dots + n-1 = 1 + \frac{n(n-1)}{2}$$

$$a_n^2 = 1 + a_{n+1} a_{n-1}$$
$$a_{n+1}^2 = 1 + a_{n+2} a_n$$

$$a_n^2 + \cancel{1} + a_{n+2} a_n = a_{n+1}^2 + \cancel{1} + a_{n+1} a_{n-1}$$
$$a_n(a_n + a_{n+2}) = a_{n+1}(a_{n+1} + a_{n-1})$$

$$\lambda = \underbrace{\frac{a_n + a_{n+2}}{a_{n+1}}}_{f(n)} = \underbrace{\frac{a_{n+1} + a_{n-1}}{a_n}}_{f(n-1)}$$

$$\forall n \quad \frac{a_n + a_{n+2}}{a_{n+1}} = \lambda$$

$$\rightsquigarrow \quad a_{n+2} = \lambda a_{n+1} - a_n$$

Dimostrare che $\lfloor (5+\sqrt{21})^n \rfloor + 1$ è divisibile per 2^n.

la soluzione è lei!

$$(5+\sqrt{21})^n + (5-\sqrt{21})^n$$

risolve $x_{n+2} - 10x_{n+1} + 4x_n = 0 \qquad x_0 = 2, \quad x_1 = 10$

$\rightsquigarrow$ tesi

EQUAZIONI FUNZIONALI

$$f(f(m)^2+2f(n)^2)=m^2+2n^2 \quad \text{per } m,n\in\mathbb{Z}^+$$

$*$ f è INIETTIVA: fisso n, se $m_1\neq m_2$ ma $f(m_1)=f(m_2)$ $LHS(m_1,n)=LHS(m_2,n)$ ma $RHS(m_1,n)\neq RHS(m_2,n)$.

$*$ SE avessi un'identità tipo

$$m^2+2n^2 = m'^2+2n'^2$$

avrei $f(m)^2+2f(n)^2 = f(m')^2+2f(n')^2$

IDEA: cerco una tale identità con $m, m+a, m+b, m+c \dots$

$$(m+3)^2+2m^2=(m-1)^2+2(m+2)^2$$

$g(x):=f(x)^2$

$$g(m+3)+2g(m)=g(m-1)+2g(m+2)$$

RISOLVO la ricorrenza

(p.c. $x^4-2x^3+2x-1=0$
$=(x-1)^3(x+1)$

$$g(m)=am^2+bm+c+d(-1)^m\ )$$

Velocemente: si finisce dimostrando $b=0$ e imponendo $am^2+c+d(-1)^m$ $\square$ $\forall m$.

$\rightarrow$ da qua finisco

$f(xy+f(x)) = xf(y)+f(x)$ $\qquad f:\mathbb{R}\circlearrowleft$

f è iniettiva? $f(a)=f(b)=c$

$$\underbrace{bc+c = f(ab+c)}_{x=b\ y=a} = \underbrace{ac+c}_{x=a\ y=b} \Rightarrow c(b+1)=c(a+1)$$

$\Rightarrow c=0 \lor a=b$ Ehm...

PROSSIMO PASSAGGIO:

$x=y=0$: $f(f(0))=f(0) \Rightarrow f(0)=0$ oppure $f(0)=0$ WOW!

$y=0$: $f(f(x))=f(x) \Rightarrow f(x)=0$ oppure $f(x)=x$

NOTA $f(x)=0$ e $f(x)=x$ soddisfano.

Suppongo ci siano $a,b\neq 0$ $f(a)=0$ $f(b)=b$

$y=a, x=b$: $f(ab+b)=f(b) \Rightarrow f(b)=0$ FALSO

oppure

$ab+\cancel{b}=\cancel{b}$ FAKE NEWS!!!

$a=0$ o $b=0$

→ assurdo

$\Rightarrow$ le uniche soluzioni sono $f(x)=0$; $f(x)=x$

Sulla surgettività:

(Senior 2016: $f(x-f(y)) = f(f(y))+xf(y)+f(x)-1$ $\quad f:\mathbb{R}\circlearrowleft$)

$\exists? f:\mathbb{R}\circlearrowleft$ t.c. $f(f(x))=x^2-2$ $\forall x$?

IDEA: guardo i punti fissi!

$g(x)=x^2-2$ ha 2 pti fissi a,b

$g\circ g$ ha 4 pti fissi a,b,c,d

DOMANDA: come "agisce" f su $\{a,b,c,d\}$?

C1 - MEDIUM

Titolo nota 03/09/2018

PROBLEMA. $a_1, a_2, \dots, a_{17}$ reali distinti.
Esiste una sottosequenza di lunghezza 5 crescente ★, o ne esiste una decrescente ★.

$1 \leq i \leq 17$ $\quad f(i) = (x_i, y_i)$

x_i: lunghezza max di una sottoseq. crescente che finisce con a_i

y_i: lungh. max sottoseq. decrescente che finisce con a_i.

Cosa succede a f se NON ho ★ né ★?
Ho $f(\{1, \dots, 17\}) \subseteq \{1, 2, \dots, 4\} \times \{1, \dots, 4\}$
$\Rightarrow$ f prende al più 16 valori.
$\rightsquigarrow$ PIGEONHOLE: dovrei avere $i < j$ t.c. $f(i) = (x_i, y_i) = (x_j, y_j) = f(j)$. Ma è possibile?
Se $i < j$ e $a_i < a_j$, allora $x_j > x_i$; se $a_i > a_j$, allora $y_j > y_i$, quindi NO.
$\Rightarrow$ ASSURDO.

(1) [ERDÖS - SZEKERES] Se ho $a_1, a_2, \dots, a_{nm+1}$ reali distinti allora c'è una sottoseq crescente da $n+1$ o una decrescente da $m+1$.

(2) Se ho $nm+1$ interi positivi, ce ne sono $n+1$ tali che, comunque ne scelga 2, NON si dividono, oppure $m+1$ che si dividono a coppie.

(3) Se ho $nm+1$ intervalli, o ne trovo $n+1$

disgiunti (2 a 2), o $m+1$ che si intersecano tutti in uno stesso punto.

POSET $X, \leq$

insieme, diciamo finito

insieme Parzialmente Ordinato

insieme di coppie di elementi (ordinate)

* $a \leq a \ \forall a \in X$
* $a \leq b$ e $b \leq a \Rightarrow a = b \ \forall a, b \in X$
* $a \leq b \leq c \Rightarrow a \leq c \ \forall a, b, c \in X$

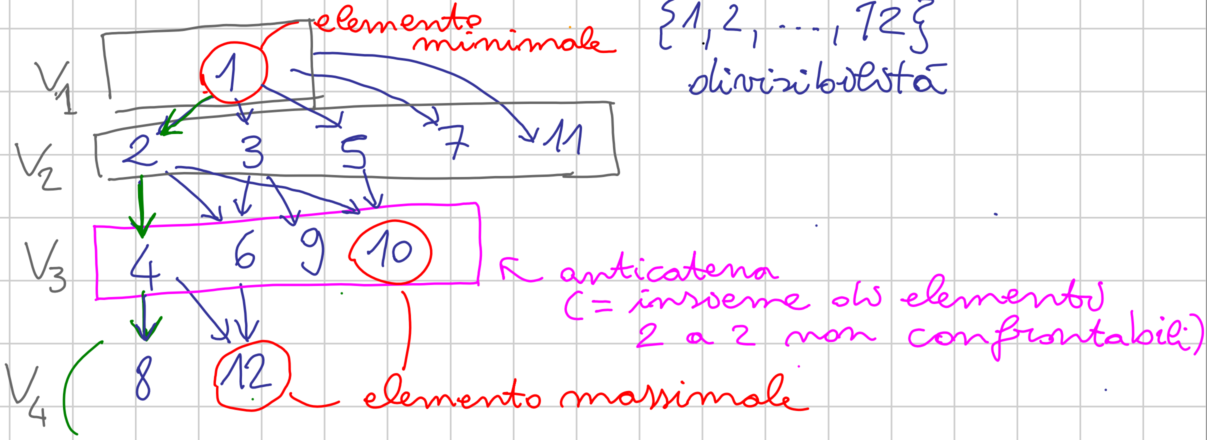
ESEMPI: (1) prendo $X = \{1, 2, \dots, mn+1\}$
$i \preccurlyeq j$ se $i \leq j$ E $a_i \leq a_j$

(2) $\mathbb{Z}^+, \ |$

(3) $\{[a,b]$ con $a < b \in \mathbb{R}\}$
$[a,b] \prec [c,d]$ se $b < c$

Rappresentazione "a strati"

$\{1, 2, \dots, 12\}$ divisibilità



catena = seq. $x_1 < x_2 < \dots \leq x_n$

V_1 = insieme degli el. minimali

V_2 = el. $\geq$ solo di elementi in V_1

V_3 = el. ≥ SOLO di el. in V_1 e V_2

...

V_i = el. ≥ SOLO di el. in $V_1, \dots, V_{i-1}$

...

V_n ← fatto tutto di el. massimali

$X = \underbrace{V_1 \sqcup V_2 \sqcup \dots \sqcup V_n}_{\text{anticatene}}$; inoltre ho

che la catena + lunga è lunga esattamente n.

$X, \leq$ poset;
la lunghezza della max catena ≥ cardinalità del minimo ricoprimento in anticatene

l'altra disug è OVVIA!

Duale del teorema di Dilworth. Vale = nell'enunciato di sopra.

Conseguenza super-utile di Dilworth duale

Ho $(X, \leq)$ poset con $nm+1$ elementi; allora c'è una catena da $n+1$ o un'anticatena da $m+1$.

perché? Non c'è una catena da $n+1$; allora copro $nm+1$ elementi con $\leq n$ anticatene. Se ciascuna avesse $\leq m$ elementi avrei $|X| \leq nm$, assurdo.

(1), (2), (3)

(1) catena = sottoseq. crescente. anticatena = sottoseq. decrescente

(2) catena di divisibilità $x_1 | x_2 | \dots | x_n$
anticatena = insieme in cui nessuna coppia si divide

(3) catena = insieme di intervalli disgiunti 2 a 2.

anticatena = insieme di intervalli che s' intersecano 2 a 2.

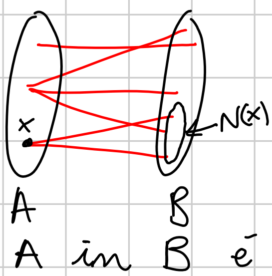
Attenzione a (3)! Non è completamente automatico. Se k intervalli s'intersecano 2 a 2 allora s'intersecano tutti in un punto! Considero l'intervallo che finisce più a sx ...

VERO teorema di Dilworth: # max anticatena (in un poset) = # minima copertura fatta con catene! (un po' più difficile...)

(SLOVACCHIA 2004) 1001 rettangoli con lati di lunghezze in $\{1, 2, \dots, 1000\}$. Dim che esistono 3 rett. A, B, C nell'insieme tali che $A \hookrightarrow B \hookrightarrow C$.

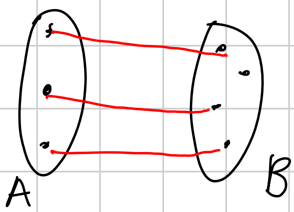
MATCHING

G grafo bipartito $V(G) = A \cup B$

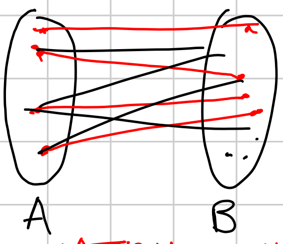


$\forall x \in A \quad N(x) \subseteq B$
$\forall y \in B \quad N(y) \subseteq A$

un matching di A in B è un insieme di archi scelti in $E(G)$ t.c. da ogni elemento di A esce esattamente un arco e da ogni el. di B esce al più un arco:



Un matching di A in B che è anche un matching di B in A è un "perfect matching".



Graf bipartito G $V(G) = A \cup B$

LEMMA dei MATRIMONI (teorema di Hall)

C'è un matching di A in B $\Leftrightarrow [\forall S \subseteq A$ $|N(S)| \geq |S|.]$ $*$ "condizione di matching"

($\Rightarrow$ ovvia)

dimostrazione 1. per induzione su $|A|$.

1. caso in cui $\forall S \subsetneq A$ $|N(S)| > |S|$.

Prendo $x \in A$ e $y \in N(x)$; considero il grafo ottenuto togliendo x e y, che "faccio sposare"; $*$ è soddisfatta sul grafo su $(A \setminus \{x\}) \cup (B \setminus \{y\})$?

Sì! $S' \subseteq A \setminus \{x\} \Rightarrow |N(S') \setminus \{y\}| \geq |N(S')| - 1 \geq |S'| + 1 - 1 = |S'|$, che è $*$ con $|A \setminus \{x\}| = |A| - 1$

$\rightsquigarrow$ finisco il matching per induzione.

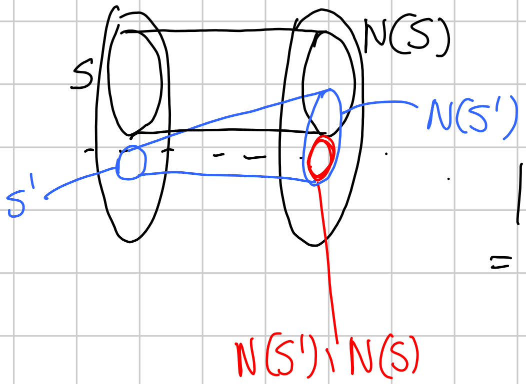
(NOTA: il caso base lo dovevo dire, ma era ovvio)

2. c'è $S \subsetneq A$ tc $|N(S)| = |S|$.

considero $S \cup N(S)$ e $(A \setminus S) \cup (B \setminus N(S))$.

Ho $|S| < |A|$ e $|A \setminus S| < |A|$; se avessi $*$ nei due grafi, avrei finito (hp. induttiva).

$*$ in $S \cup N(S)$ è chiara ($S' \subseteq S$ ha $N(S') \subseteq N(S)$). Mentre se prendo



caso 2

$S' \subseteq A \setminus S$

$$\underbrace{|N(S') \setminus N(S)| + \underbrace{|N(S)|}_{=|S|}}_{=|N(S \cup S')|} \geq |S \cup S'| = |S| + |S'|$$

$$\rightarrow |N(S') \setminus N(S)| \geq \cancel{|S|} + |S'| - \cancel{|S|}$$

⇝ ho vinto! $\ddot{\smile}$

dimostrazione 2. $A \cup B'$ POSET ponendo $x < y$ se $x \in A$ e $y \in N(x)$. Catena = coppia $(x, y) \in A \times B'$ tc $x \sim y$. Copertura in catene è un insieme di archi che copre A e B'.

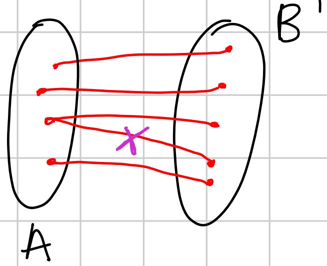
metto $N(A)$

$y \in N(x)$

Chi è una anticatena massimale? Dico che è B'! Supp. F anticatena, $F = (B' \cap F) \cup (A \cap F)$.

$$|F| = |B' \cap F| + |A \cap F| \leq |A \cap F| + |B' \setminus N(A \cap F)|$$
$$\leq |A \cap F| + |B'| - |N(A \cap F)| \underset{*}{\leq} |B'|$$

$\Rightarrow$ per Dilworth esiste una copertura con $|B'|$ catene, una per ogni el. di B'



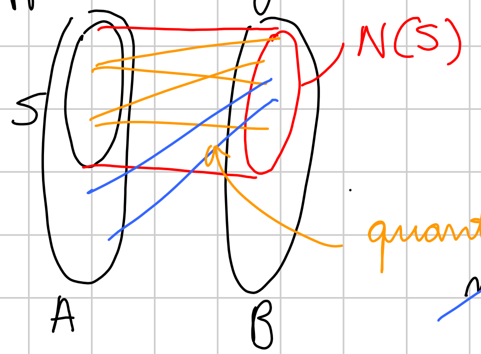
⇝ riesco a estrarne un matching di A in B'.

PROBLEMA: scacchiera $k \times k$, n pedine per riga e per colonna; posso scegliere k pedine in modo da averne una per riga e per colonna.

$$\{R_1, R_2 \dots, R_k\} \cup \{C_1, C_2, \dots, C_k\}$$

$R_i \sim C_j$ quando c'è una pedina in (i,j).

Vogliamo trovare un perfect matching!
Sappiamo $\deg x = n$ per ogni vertice x.



$$\cancel{n}|S| \leq \cancel{n}|N(S)|$$

archi che "entrano" da S in $N(S)$ — archi che escono da $N(S)$

→ è proprio *

Teorema di Sperner. Nel POSET $(\mathcal{P}(\{1,2,\dots,n\}), \subseteq)$ la max cardinalità di un'anticatena è $\binom{n}{\lfloor n/2 \rfloor}$.

Anticatene "naturali": $A_k = \{S \subseteq \{1,\dots,n\} \mid |S| = k\}$
$A_{\lfloor n/2 \rfloor} \rightarrow$ ovvio il "$\geq$" in Sperner.

dimostrazione 1.

Considero A_k e A_{k-1} con $k \leq \frac{n+1}{2}$;
formano un grafo bipartito $(x \sim y$ se $x \leq y)$.
$x \in A_k \Rightarrow \deg x = k$; $y \in A_{k-1} \Rightarrow \deg y = n-k+1$.
$Z \subseteq A_{k-1}$ $\quad |N(Z)| \underset{?}{\geq} |Z|$.

conto archi da Z a $N(Z)$ $\quad |Z|(n-k+1) \leq |N(Z)|k$

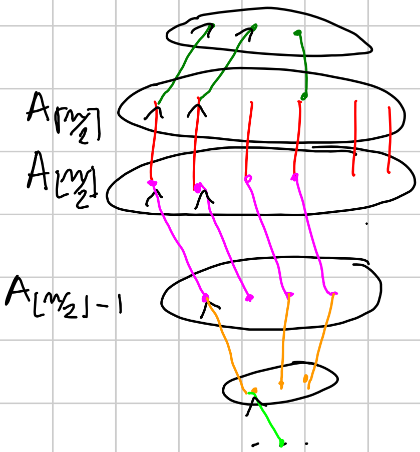
archi che escono da $N(Z)$

$\Rightarrow$ $*$ sul mio grafo.

$\left(\frac{k}{n-k+1} \leq 1 \Leftrightarrow n-k+1 \geq k \Leftrightarrow k \leq \frac{n+1}{2} \right)$

$\Rightarrow$ ho un matching di A_{k-1} in A_k.

Simmetricamente ho un matching di A_{k+1} in A_k per $A_k \geq \frac{n-1}{2}$.



$\rightsquigarrow$ concatenando matching ottengo $\mathcal{P}(\{1, \dots, n\})$ si scrive come unione di $|A_{\lfloor n/2 \rfloor}| = \binom{n}{\lfloor n/2 \rfloor}$.

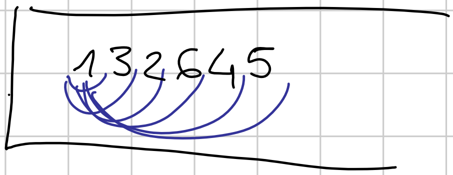
Potrei usarne di meno?
No, perché gli el. di $A_{\lfloor n/2 \rfloor}$ devono stare in catene diverse.

$\Rightarrow$ (Dilworth) $\binom{n}{\lfloor n/2 \rfloor}$ è la cardinalità massima di un'anticatena.

dimostrazione 2. voglio prendere F anticatena in $\mathcal{P}(\{1, \dots, n\})$ e $\sigma = (\sigma(1), \dots, \sigma(n))$

permutazione a caso di $\{1, \dots, n\}$.

Data $\sigma(1) \dots \sigma(n)$ quanti "segmenti iniziali" (cioè insiemi $\{\sigma(1), \dots, \sigma(k)\}$) stanno in F? Al max 1!



$$\sum_{\sigma \in S_n} \frac{1}{n!} \text{ \# segm. iniz. di } \sigma \text{ che stanno in } F \le \frac{1}{n!} \sum_{\sigma \in S_n} 1 = 1$$

(S_n: permutazioni di n elementi)

$$= \sum_{k \le n} \sum_{\substack{S \in F \\ |S| = k}} \frac{1}{n!} \text{ \# permutazioni } \sigma \text{ che hanno } S \text{ come segmento iniziale} =$$

$$= \sum_k \sum_{\substack{S \in F \\ |S| = k}} \frac{1}{n!} k!(n-k)! =$$

$$= \sum_k \sum_{\substack{S \in F \\ |S| = k}} \frac{1}{\binom{n}{k}} \ge \sum_k \sum_{\substack{S \in F \\ |S| = k}} \frac{1}{\binom{n}{\lfloor n/2 \rfloor}}$$

$$= \frac{1}{\binom{n}{\lfloor n/2 \rfloor}} \sum_k \sum_{\substack{S \in F \\ |S| = k}} 1 = \frac{|F|}{\binom{n}{\lfloor n/2 \rfloor}}$$

$$\rightsquigarrow \quad |F| \le \binom{n}{\lfloor n/2 \rfloor} \qquad \square$$

C2 Medium: ? Ludo

Titolo nota 07/09/2018

Permutazioni

Permutazione $\sigma = f : \{1 \dots n\} \to \{1, \dots n\}$ biettiva

$S_n = \{ \sigma : \{1, \dots, n\} \to \{1, \dots n\} \}$ gruppo simmetrico

Problema simmetrico risp. a una trasf. o a un insieme di trasf: non cambia se le applico.

(origine: permutazioni delle radici di un polinomio)

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & & & \sigma(n) \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Oss. Si possono comporre e viene ancora una permutazione

$$\begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix} \circ \begin{pmatrix} 1 & \dots & n \\ \tau(1) & \dots & \tau(n) \end{pmatrix} (i)$$

dopo per prima

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

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

- la compos. è associativa
- esiste l'inversa σ^{-1} $\quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 4 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

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

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

– esiste id: $\begin{pmatrix} 1 & 2 & 3 & & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$

Gruppo: $(S, \circ, e, ^{-1})$ S insieme

$\circ$ operaz. interna assoc.

e el. neutro

-1 esiste inverso

Struttura ciclica delle permutazioni

σ è un k-ciclo se $1, \sigma(1), \sigma(\sigma(1)), \ldots \underbrace{\sigma(\sigma(\cdots(\sigma}_{k-1\ \sigma}(1))$ sono tutti diversi e invece $\underbrace{\sigma(\cdots\sigma}_{n\ \sigma}(1)) = 1$

$\bar\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

1	$\bar\sigma(1)$	$\bar\sigma(\bar\sigma(1))$	$\bar\sigma(\bar\sigma(\bar\sigma(1)))$	$\bar\sigma(\bar\sigma(\bar\sigma(\bar\sigma(1))))$
1	4	3	2	1

$1 \to 4 \to 3 \to 2 \to 1$ $\quad (1\,4\,3\,2) = (3\,2\,1\,4)$ $\quad \bar\sigma$ in forma ciclica

4-ciclo

ma $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ non è un 4-ciclo! È $(1)(2\,3\,4)$ che c'è qui?

Se 1 k ciclo (σ_k) e 1 h ciclo (σ_h) sono disgiunti in S_n

$\sigma_k \sigma_h$ $\quad (\cdots \sigma_k\ )(\cdots \sigma_h\ )$ è una moltiplicazione

o anche la notazione per un'altra permutazione, perché posso farle indipendentemente e contemporan.

Teorema: ogni $\sigma \in S_n$ si può scomporre in cicli disgiunti

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 6 & 2 & 7 & 1 & 9 & 8 & 5 \end{pmatrix}$$

$(1\,3\,6)(2\,4)(5\,7\,9)(8)$

convenzione: i cicli da 1 si possono omettere

non è un gruppo commutativo:

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

$\qquad\qquad\qquad\qquad \neq$

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

però è facile sapere l'ordine di un elemento

$\sigma^k = e \qquad \sigma = k\text{-ciclo} \qquad$ ordine k

se ho, $\sigma = c_1 \cdot c_2 \cdot c_3 \cdots c_\ell \qquad c_i\ \ k_i$-cicli.

ordine di $\sigma = \text{mcm}\,(k_i)$

Segno di una permutazione

Teorema: ogni permutazione si può scrivere come prodotto di 2-cicli (trasposizioni) [NON necessar. disgiunti]

Basta scrivere un k-ciclo

$(1\,2\,3\,4)$ $\qquad$ [id. $\overline{\text{NON è}}$ $(1)(2)(3)(4)$]

$(a_i\ b_i)$ $\qquad (12)(23)(34) = (1234)$

$(41)(31)(21) = (1234)$

Oss. se $\sigma = \prod_{i=1}^{k} \text{trasp}_i = \prod_{j=1}^{h} \text{trasp}_j$, allora

h e k o sono entrambi pari perm. PARI $sgn(\sigma)=+1$

o - - - dispari perm. DISPARI $sgn(\sigma)=-1$

pari ∘ pari = pari
pari ∘ disp = disp
disp ∘ pari = disp.
disp ∘ disp = pari

$$sgn(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(i)-\sigma(j)}{i-j}$$

Azione transitiva (e k-transitiva)

Trasf. di un oggetto (insieme) S

Se $\forall\, s \in S$ e $t \in S$ $\exists\, T$ trasf. $T(s)=t$

si dice che $\{\text{Trasf}\}$ agisce su S in modo trans.

Se $\forall\, s_1, s_2 \quad t_1, t_2 \in S \quad \exists\, T. \quad T(s_1)=t_1,\ T(s_2)=t_2$

... 2-transitiva, così k-transitiva

S_n è n-transitivo

triangolo in problema invar. per affinità $\longrightarrow$
posso wlog supporre che sia equilatero.

affinità del piano sono 3-transitive.

IMOSL 2002 C3: successione piena di n interi positivi $a_1 \dots a_n$ dove se $k \geq 2$, $k \in \mathbb{N}$ compare, allora compare anche $k-1$ e la prima volta che compare $k-1$ è prima dell'ultima volta in cui compare k. Quante sono?

Cerchiamo una bigezione con qualcosa di noto.

111 112 121 ~~211~~

122 212 123

1111	$\boxed{1112}$	1122	1123	1234
1222	1212	1121	1213	1223
1233	1232	1221	1231	1211
1323	2212	2122	2123	2112
2121	2132	2312	3123	

f

è $n!$??

1234

4321 3214 2143 4123

$S_i = \{k \mid a_k = i\}$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \longrightarrow \begin{array}{cccc} 1 & 2 & 3 & 4 \\ \boxed{2} & \boxed{1} & \boxed{3} & \boxed{2} \end{array}$$

f è iniettiva: se 2 succ. sono $\neq$, almeno 1 degli S_i sarà diverso

f è invertibile: g: la perm. è letta come una lista di succ. decrescenti massimali (è modo unico)

che diventano gli indici dei vari i

$\Rightarrow$ Risp. $n!$

ARG 2016? Trovare tutte le $f: \{1 \dots n\} \to \{1 \dots n\}$ big.
t.c. $|f(1)-f(2)| + |f(2)-f(3)| + \dots + |f(n)-f(1)| = 2n-2$

Sull'id. ok fa $2n-2$.

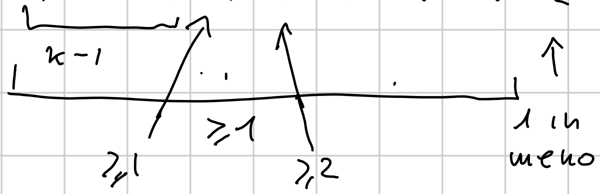
E se è un k-ciclo? $(1 \dots k)(k+1) \dots (n)$

$1 \; 2 \; \dots \; k-1 \; k \; k+1 \; .$

$2 \; 3 \; \quad k \; 1 \; k+1 \; k+2 \; \dots \; n$

$1 \; 1 \; \dots 1 \; k-1 \; k \; 1 \; 1 \; 1 \; n-2$

2-ciclo ok $(1\,2)$



$k=2$ ok $\quad k>2$ no, troppo grande

$n-2+n-3+2k-1 =$

$2n-\cancel{6}+2k$

2-ciclo $(k, k+1)$ qual. no

$1 \; 2 \; - \; . \; k-1 \; k \; k+1 \; k+2 \; . \; . \; . \; n$

$1 \; 2 \quad k-1 \; k+1 \; k \; k+2 \; . \; - \; - \; n$

$1 \; 1 \; 1 \; 2 \; 1 \; 2 \; 1 \; 1 \; -\!- 1 \; n-1$

$1 \; 2 \dots \; j-1 \; j \; j+1 \; \dots \; j+k-2 \; j+k-1 \; j+k \dots n$

$1 \quad j-1 \; j+1 \; j+2 \quad j+k-1 \; j \quad j+k \dots n$

$1 \quad 1 \; 2 \; 1 \; \dots \; 1 \; k-1 \; k \; 1 \dots 1 \; n-1$

$\sigma \longrightarrow \sigma \circ c_n$ ha lo stesso valore, perché sono solo differenze

Posso supporre $\sigma(n) = n$

Quindi ho perm. $\bar{\sigma} \in S_{n-1}$ $\begin{pmatrix} 1 \cdots n-1 & n \\ \boxed{\quad \bar{\sigma} \quad} & n \end{pmatrix}$

$$\sum_{i=1}^{n-1} |\bar{\sigma}(i) - \bar{\sigma}(i+1)| \geq 2(n-1) - 2$$

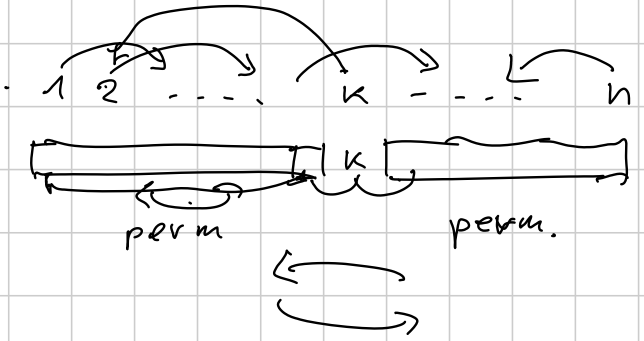
ciclico mod $n-1$ $\searrow |\bar{\sigma}(n-1) - \bar{\sigma}(1)|$

$$\sum_{\substack{i=1 \\ \text{ciclica}}}^{n} |\sigma(i) - \sigma(i+1)| = \sum^{n-1} |\bar{\sigma}(i) - \bar{\sigma}(i+1)| - |\bar{\sigma}(n-1) - \bar{\sigma}(1)| + |\sigma(n-1) - \sigma(n)| + |\sigma(n) - \sigma(1)|$$

≥ 2

$\sigma(n) = n$ quindi è dis. triangolare (stretta) su $\mathbb{R}$ $\Rightarrow \geq 2$

n freeze



$\geq 2k-4$ $\qquad\qquad$ $\geq 2(n-k)-2$

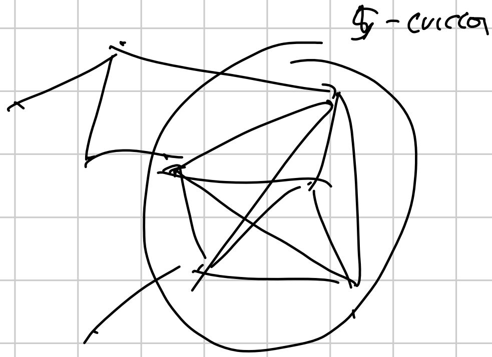
Più in generale, posso calc. il contributo dei vari cicli e mi accorgo che non mi conviene avere più di un ciclo $\to$ $(1\,2)$ e quelli "ruotati"

$(1\,2 \cdots n)$

e non vanno bene gli n-cicli non in ordine

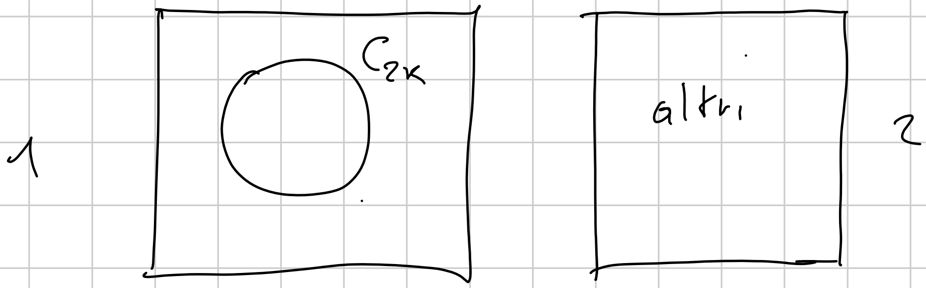
Configurazioni estremali

IMO 2007/3 n partecipanti a uno stage alcuni sono amici (rel. simmetrica). Si sa che la massima dim. di una cricca è pari. Allora dim. che è possibile dividere i partec. in due alberghi in modo che la mass. dim. delle cricche sia la stessa nei due alberghi.



Tentativo: dare un algoritmo di costruzione.

1 o più cricche da $2k$.



m_1 = dim. max. cricca in 1
m_2 = " " 2

<u>Caso 1</u> : $m_2 = m_1 = 2k$ <u>ok</u>

Caso 2: $m_2 < m_1$

Oss. Se tolgo (o metto) un tizio in una scatola, $m_{scatola}$ rimane uguale, o dim (o aum.) di 1

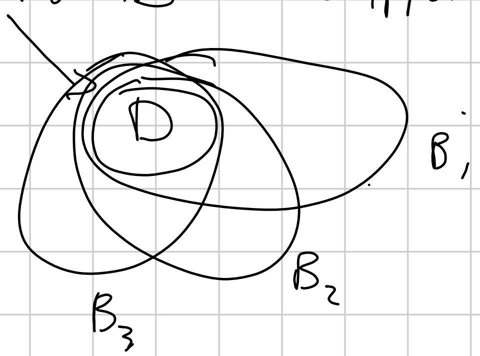
Oss. $m_1 + m_2 \geq 2K$

Spostano 1 a 1 da $\boxed{1}$ a $\boxed{2}$ arrivo al momento in cui $m_1 = m_2 + 1$ o $m_1 = m_2$

1) $\exists$ un tizio in $\boxed{1}$ che portato di là non produce cricche da m_2+1 <u>ok</u>

2) $\nexists$, cioè ogni tizio produce 1 cricca da m_2+1
ne porto comunque di là 1, e ci saranno alcune cricche B_i da m_2+1

Oss. tutti i deportati da $\boxed{1}$ devono appartenere a tutte le B_i



$B_i = D \cup R_i$

Provo a riportare uno di là

Prendo $x_1 \in R_1$ e lo porto di là. Non può essere amico di tutti in $\boxed{1}$, quindi non fa salire m_1

Forse alcune B_i sono ancora grandi m_2+1
In una di queste prendo wlog $x_2 \in B_2$ non

amico di B_1, che starà in R_2 e lo porto di là.

Così $x_3 - - x_s$. L'ultimo è speciale:

o funziona e si pareggia a m_2

o non funziona e basta portare indietro x_{s-1}.

EGMO 2012/4 $\exists A \subseteq \mathbb{Z}$ t.c. 1) $A \subseteq A+A$
2) Tutti i $z \in \mathbb{Z}$ tranne 0 sono somma di un sottoins. di A ?

Risp.: sì.

Algoritmo "greedy" e iterativo: mi preoccupo di un numero per volta.

1 2,3,4, 5,6,7,8,9,10,11,12

$a_1 = 1$ 3 8

−2 −5 −13

−1,−2 −3,−4,−5,−6,−7

Cong.: $(-1)^n F_n$ funziona. 1) ok

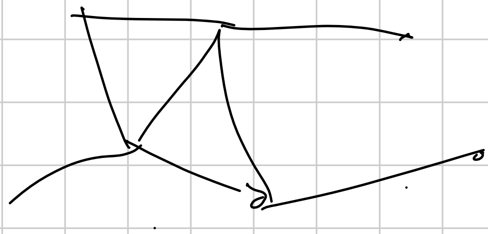
2) $[F_{2n}+1, F_{2n+2}]$ con F_{2n+2}

$[-F_{2n+1}+1, -F_{2n-1}]$ con $-F_{2n+1}$

Ma 0? Se $0 = \sum_i F_{2n_i} - \sum_j F_{2n_j+1}$ non è possibile

perché $\sum_{i=1}^{n} F_{2i} < F_{2n+1}$ e $\sum_{i=0}^{n} F_{2i+1} < F_{2n+2}$

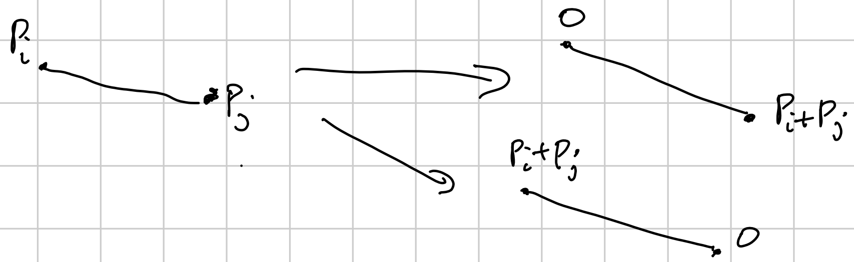
Quanti archi al max su n vertici per <u>non</u> avere nessuna k-cricca.



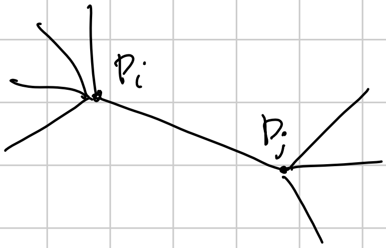
Diamo pesi ai vertici. V_i p_i

All'inizio, $p_i = 1 \quad \forall i = 1 \dots n$

$$E = \sum_{\substack{ij \text{ arco} \\ i<j}} p_i \cdot p_j \qquad (\#\text{archi all'inizio}).$$



Dico che in (almeno) uno dei due casi E aumenta.



$$E = \sum_{\substack{\text{lati che} \\ \text{non passano} \\ \text{da } i \text{ o da } j}} + p_i \cdot \sum_{k \text{ ad. } i} p_k + p_j \cdot \sum_{h \text{ ad. } j} p_h - p_i p_j$$

Supp. $\displaystyle\sum_{k \text{ ad. } i} p_k > \sum_{h \text{ ad. } j} p_h$

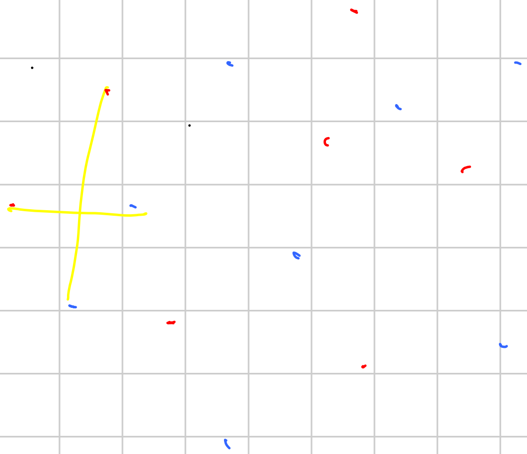
Dopo? $$E = \sum_{\substack{\text{lati che} \\ \text{non toccano} \\ i \text{ o } j}} + \begin{cases} (p_i+p_j)\displaystyle\sum_{k \text{ ad. } i} p_k \\ (p_i+p_j)\displaystyle\sum_{h \text{ ad. } j} p_h \end{cases}$$

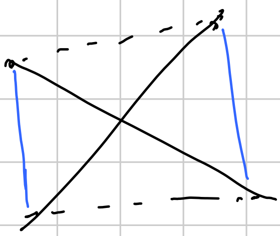
$$\# \text{lati} \le \left(\frac{\sum v_i}{k-1}\right)^2 \binom{k-1}{2} = \left(\frac{n}{k-1}\right)^2 \binom{k}{2}$$

n p. rossi
n p. blu in $\mathbb{R}^2$

$\exists$ n segm. bicolori che non si intersecano?

$Q = \sum$ lungh. segm.

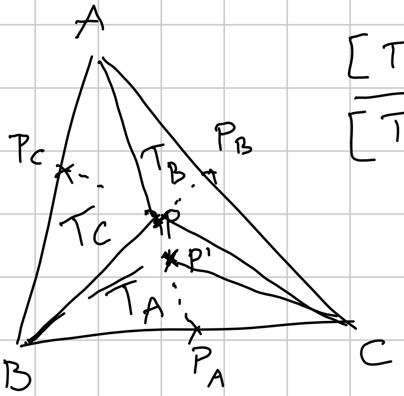




G1 - Medium   Jack / elianto84

Titolo nota   03/09/2018

1) Ceva, Meneleo, Van Obel etc
2) Coord tril e bar
3) $\mathbb{C}$, config di Torricelli / Steiner / Fermat / Napoleone
4) Huygens-Steiner etc (parallel axis theorem)

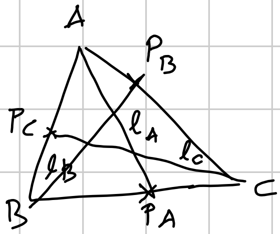


$$\frac{[T_C]}{[T_B]} = \frac{[ABP_A]}{[ACP_A]} = \frac{BP_A}{CP_A}.$$

aree orientate

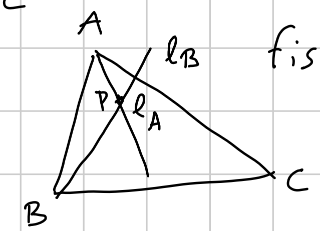
$$\frac{[T_A]}{[T_B]} \cdot \frac{[T_B]}{[T_C]} \cdot \frac{[T_C]}{[T_A]} = 1$$

$$\frac{AP_C}{P_CB} \cdot \frac{BP_A}{P_AC} \cdot \frac{CP_B}{P_BA} = 1.$$



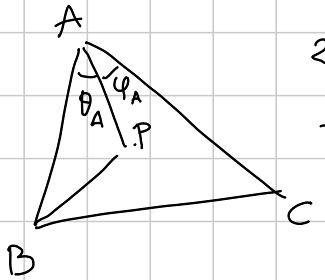
Teorema di Ceva

ℓ_A, ℓ_B, ℓ_C concorrono $\Longleftrightarrow$ $\underbrace{\frac{AP_C}{P_CB} \cdot \frac{BP_A}{P_AC} \cdot \frac{CP_B}{P_BA}}_{\text{lunghezze con segno}} = 1$



fissati $\frac{[APB]}{[APC]}$, $\frac{[APB]}{[BPC]}$

è fissato anche $\frac{[APC]}{[BPC]}$ $\square$

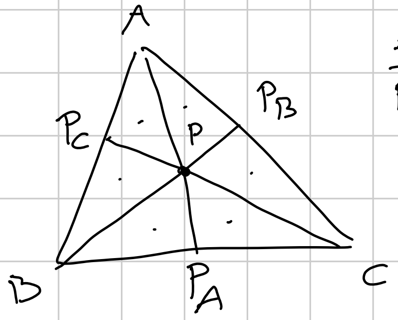


$$2\,[APB] = AP \cdot AB \cdot \sin(\theta_A)$$

Trig Ceva $\quad \sin\theta_A \cdot \sin\theta_B \cdot \sin\theta_C = \sin\varphi_A \sin\varphi_B \sin\varphi_C$

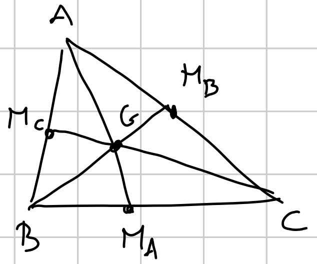
Ceva $\Longleftrightarrow$ Meneleo

Van Obel



$$\frac{AP}{PP_A} = \frac{AP_C}{P_C B} + \frac{AP_B}{P_B C}$$

$$\frac{[ABPC]}{[BPC]} = \frac{[APB]+[APC]}{[BPC]}$$



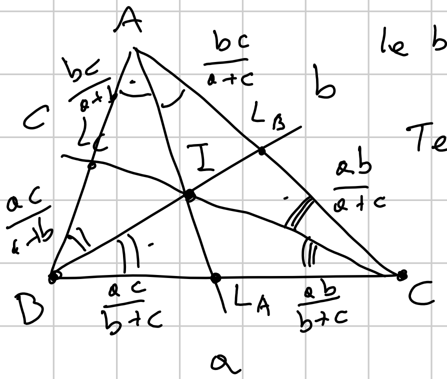
Il baricentro esiste $\longleftrightarrow$ AM_A, BM_B, CM_C concorrono

$\updownarrow$

Ceva vale ovviamente

$$\frac{AG}{GM_A} = \frac{AM_C}{M_C B} + \frac{AM_B}{M_B C} = 1 + 1 = 2$$

G cade a 2/3 di ogni mediane



L'incentro esiste, ossia le bisettric concorrono. $\longleftrightarrow$ trig Ceva

Teorema delle bisettrice

$$\frac{BL_A}{L_A C} = \frac{c}{b} \qquad \frac{2[ABL_A]}{2[ACL_A]} = \frac{AB \cdot \cancel{AL_A} \cdot \cancel{\sin\frac{A}{2}}}{AC \cdot \cancel{AL_A} \cdot \cancel{\sin\frac{A}{2}}}$$

$$\frac{2[ABL_A]}{2[ACL_A]} = \frac{BL_A}{CL_A}$$

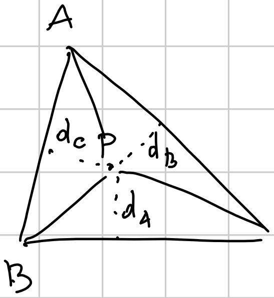
$$BL_A = \frac{c}{b+c} \cdot a \qquad CL_A = \frac{b}{b+c} \cdot a$$

$$\frac{AI}{IL_A} = \frac{AL_C}{L_C B} + \frac{AL_B}{L_B C} = \frac{b}{a} + \frac{c}{a} = \frac{b+c}{a}$$

$$AI = \frac{b+c}{b+c+a} \cdot AL_A$$

$\longrightarrow$ si trova con Stewart

$\nearrow$ teorema del coseno



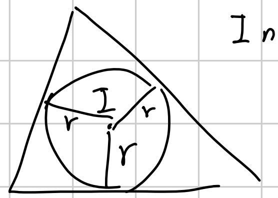
$$2[APB] = AB \cdot d_C$$

Ceva $\iff \dfrac{d_A}{d_B} \cdot \dfrac{d_B}{d_C} \cdot \dfrac{d_C}{d_A} = 1$

$[d_A ; d_B ; d_C]$ coordinate trilineari esatte di P

$[\gamma d_A ; \gamma d_B ; \gamma d_C] \quad \forall \gamma \neq 0$

la terna $[d_A ; d_B ; d_C]$, definita a meno di moltiplicaz. per costanti non nulle, ci permette di identificare univocamente il punto P. <u>coordinate triliN.</u>

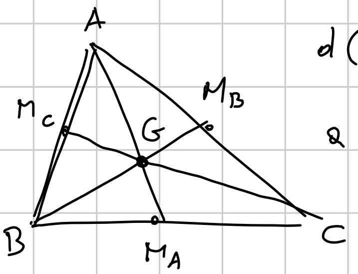


Incentro coordinate tril. esatte $[r ; r ; r]$

coord tril. $[1 ; 1 ; 1]$ $\cdot \lambda$

$$a d_A + b d_B + c d_C = 2[ABC]$$
$$ar + br + cr = 2[ABC]$$

$$\lambda = \frac{2[ABC]}{a+b+c}.$$



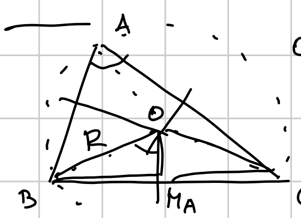
$d(G, BC) = \dfrac{1}{3} \cdot \dfrac{2\Delta}{a}$ $\quad d(G, AB) = \dfrac{2\Delta}{3c}$

$a \cdot h_A = 2\Delta$ $\quad d(G, AC) = \dfrac{2\Delta}{3b}$

$h_A = \dfrac{2\Delta}{a}$

$G\left[\dfrac{2\Delta}{3a} ; \dfrac{2\Delta}{3b} ; \dfrac{2\Delta}{3c}\right]$ tril. esatte

$G\left[\dfrac{1}{a} ; \dfrac{1}{b} ; \dfrac{1}{c}\right]$ trilineari



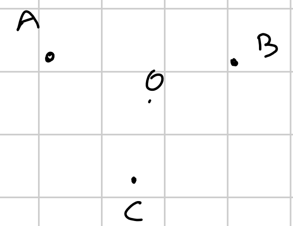
$OA = OB = OC = R$

$\widehat{BOC} = 2\widehat{A}$ $\quad \widehat{BOM_A} = \widehat{A}$ $\quad OM_A = R\cos A$

$O \quad [R\cos A, R\cos B, R\cos C]$ tril. esatte

$[\cos A, \cos B, \cos C]$ tril

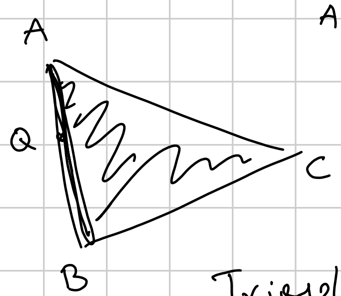
$$\cos A = \frac{b^2+c^2-a^2}{2bc} \qquad \| \qquad [\underbrace{a(b^2+c^2-a^2)}_{\text{triangle center function } (\alpha)}; \dots; \dots]$$



Coordinate di $A, B, C \in \mathbb{R}^3$

$\downarrow$

Coordinate di O



$A, B, C \in \mathbb{R}^n$

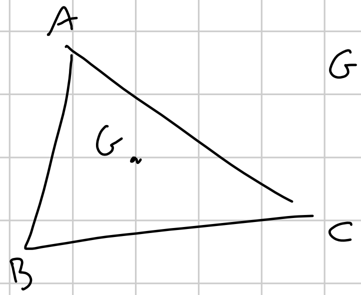
$$\forall Q \in AB \quad \exists \lambda \in [0,1] : Q = \underbrace{\lambda A + (1-\lambda) B}_{\text{comb. convesse di } A \text{ e } B}$$

$$\text{Triangolo } ABC \equiv \left\{ xA + yB + zC : \begin{array}{l} x+y+z=1 \\ x,y,z \in [0,1] \end{array} \right\}$$

inviluppo convesso di A, B, C (convex hull) più piccolo (rispetto a $\subseteq$) insieme convesso che contiene A, B e C.

$[X; Y; Z]$ coordinate baricentriche esatte

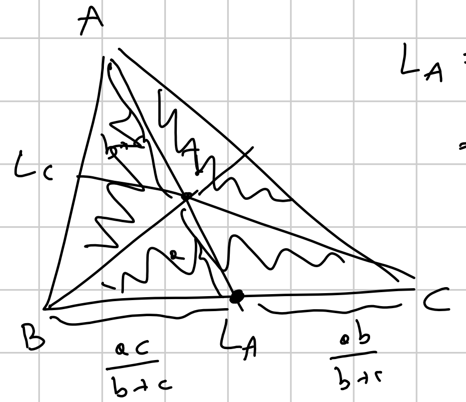
$[x; y; z]$ coordinate baricentriche (a meno di moltiplic. per scalari non nulli)



$$G = \frac{A+B+C}{3}$$

coord baricentriche di $G = [1 ; 1 ; 1]$

Coord baricentriche dell'incentro



$$L_A = B + (C-B)\cdot\frac{ac}{a}\cdot\frac{1}{b+c}$$

$$= B + (C-B)\frac{c}{b+c} = \frac{b}{b+c}\cdot B + \frac{c}{b+c}\,C$$

$$I = \frac{aA + bB + cC}{a+b+c}$$

$I = [a, b, c]$ baricentriche

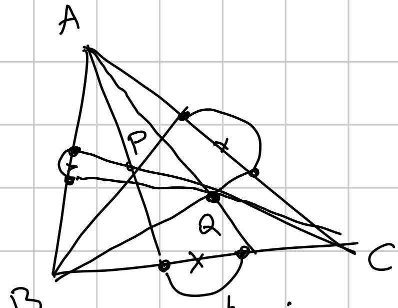
Conversione tra trilineari e baricentriche

$[\alpha, \beta, \gamma]$ trilineari $\longrightarrow$ $[a\alpha, b\beta, c\gamma]$ baricentriche

---

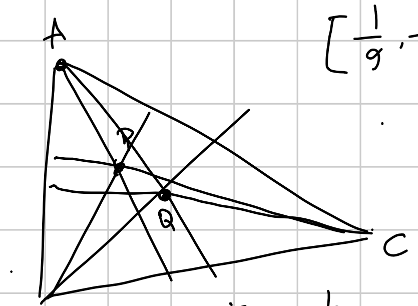
Ceva $\longrightarrow$ conj. isotomico

Trig Ceva $\longrightarrow$ conj. isogonale



conj isotomico

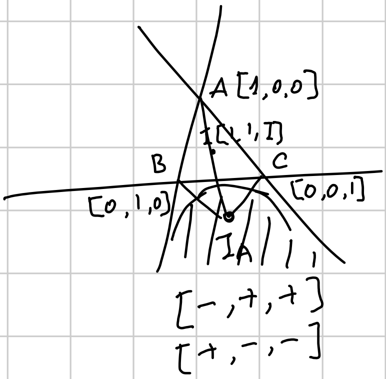
vengono reciprocate le coord. baricentriche



conj isogonale

$\left[\frac{1}{\alpha}, \frac{1}{\beta}, \frac{1}{\gamma}\right]$ coord tril. del conj. isogon. di P

$[\alpha, \beta, \gamma]$ coord. tril di P coord. tril. esatte $[\alpha, \beta, \gamma]$



baricentriche $[1;1;-2]$

$$\frac{A+B-2C}{1+1-2}$$

$$\mathbb{R}^2 \subseteq \mathbb{P}^2(\mathbb{R})$$

i punti con coord baricentriche $[\alpha, \beta, \gamma]$ con $\alpha+\beta+\gamma=0$ appartengono alla retta all'infinito di $\mathbb{P}^2(\mathbb{R})$

In coordin tril (o bar) le rette si scrivono come oggetti del tipo $u\alpha + v\beta + w\gamma = 0$

$\hookrightarrow [u, v, w]$ coord tril (duali) della retta

dualità proiettiva rette <—> punti

Retta OH in trilineari.

$O = [\cos A, \cos B, \cos C]$ tril

coniug. iso

$H = \left[\frac{1}{\cos A}, \frac{1}{\cos B}, \frac{1}{\cos C}\right]$ tril

$\downarrow$

$[u; v; w]$

$$\begin{cases} u\cos A + v\cos B + w\cos C = 0 \\ \dfrac{u}{\cos A} + \dfrac{v}{\cos B} + \dfrac{w}{\cos C} = 0 \end{cases}$$

$$\det \begin{vmatrix} \cos A & \cos B & \cos C \\ \frac{1}{\cos A} & \frac{1}{\cos B} & \frac{1}{\cos C} \\ u & v & w \end{vmatrix}$$

$$u = \frac{\cos B}{\cos C} - \frac{\cos C}{\cos B} = \frac{\cos^2 B - \cos^2 C}{\cos B \cos C} = \frac{\sin^2 C - \sin^2 B}{\cos B \cos C}$$

Retta di Eulero $\quad O, G, H$ sono allineati

$$\det \begin{vmatrix} \cos A & \cos B & \cos C \\ \frac{1}{\cos A} & \frac{1}{\cos B} & \frac{1}{\cos C} \\ \frac{1}{\sin A} & \frac{1}{\sin B} & \frac{1}{\sin C} \end{vmatrix} = 0$$

$$a = 2R \sin A$$
$$2bc \cos A = b^2 + c^2 - a^2$$

$$\det \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = aei + bfg + cdh - gec - hfa - dbi$$

Regola di Sarrus

$$\det \begin{vmatrix} a & \\ b & \\ c & M_a \\ d & \end{vmatrix} = a \det(M_a) - b \cdot \det(M_b) + c \cdot \det(M_c) - d \det(M_d)$$

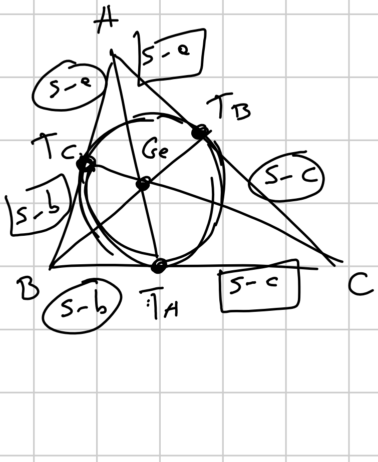
sviluppo di Laplace

$$M = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1N} \\ \vdots & & & \\ a_{N1} & \dots & \dots & a_{NN} \end{pmatrix} \qquad \det M = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \prod_{k=1}^{n} a_{k,\sigma(k)}$$

volume orientato della "scatola" generata dai vettori riga

Esercizio: I, G, Na, Sp sono allineati $\quad$ (O, G, H sono allin.)

I ↑ incentro, G ↑ baricentro, Na ↑ Nagel, Sp ↑ Spieker $\qquad$ Ge Gergonne

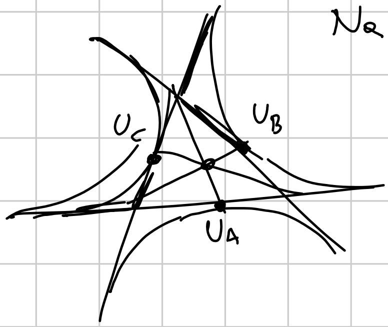


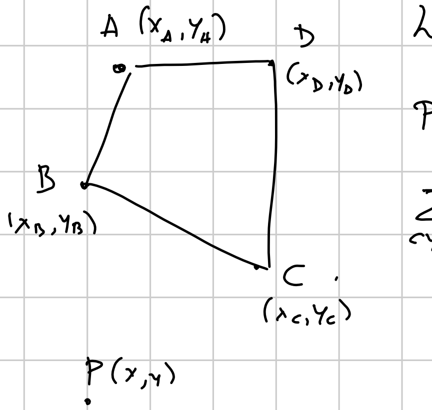
Baricentriche di Ge

$$T_A = B + (C - B) \cdot \frac{s-b}{a}$$

$$\frac{A\,Ge}{Ge\,T_A} = \frac{s-a}{s-b} + \frac{s-a}{s-c}$$

N_a è coniug. isotomico di Gergonne





Luogo di punti P per cui

$$PA^2 + PB^2 + PC^2 + PD^2 = 1000000$$

$$\sum_{cyc} (x - x_A)^2 + (y - y_A)^2 = 1'000'000$$

$$x^2 + y^2 = -3$$

$$x^2 + y^2 = 0$$

$$f(P) = PA^2 + PB^2 + PC^2 + PD^2$$

dove si trova il minimo di f?

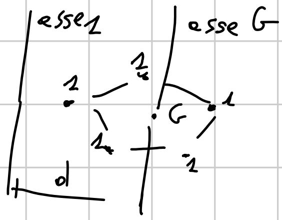
$$f(x) = x^2 - \underline{17}x + 8$$

$$f(x,y) = 4x^2 + 4y^2 - 2x\sum_{cyc} x_A + \sum_{cyc} x_A^2 - 2y\sum_{cyc} y_A + \sum_{cyc} y_A^2$$

$$\arg\min f = \left(\frac{\sum_{cyc} x_A}{4}, \frac{\sum_{cyc} y_A}{4}\right) = G$$

si scrive in soli termini di PG^2

Huygens-Steiner: il momento di inerzia rispetto a $asse_1$ è pari al momento di inerzia rispetto a $asse_G + d^2 \cdot$ (massa del sistema).



Distanza IG.

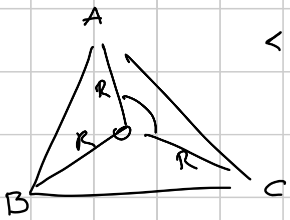
$$I = \frac{aA + bB + cC}{a+b+c} \qquad G = \frac{A+B+C}{3}$$

$$I - G = x_A A + x_B B + x_C C$$

$$IG = \|I - G\|$$

$$IG^2 = \langle I-G, I-G \rangle$$

In un sistema di rif centrato nel circocentro



$$\langle A, C \rangle = R^2 \cos(2B)$$

OH^2 si scrive solo in termini di R^2 e $(a^2+b^2+c^2)$.

Utilizzo di $\mathbb{C}$ in geometria. $\mathbb{R}^2 \subseteq \mathbb{P}^2(\mathbb{R})$, $\mathbb{R}^2 \cong \mathbb{C}$

Teo fond Algebra : $\mathbb{C}$ è algebricamente chiuso, ossia

$\forall p(x) \in \mathbb{C}[x]$, $\deg p \geq 1$

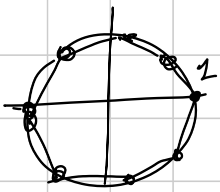
$\exists \xi \in \mathbb{C} : p(\xi) = 0$.

(+ Ruffini) Ogni $p(x) \in \mathbb{C}[x]$ con $\deg p \geq 1$ ha tante radici complesse (contate con molt.) quante il suo grado.

Gli zeri di $z^n - 1$ sono detti radici n-esime dell'unità.

$z^n = 1$ $\quad |z|^n = 1$ $\quad |z| = \sqrt{z \cdot \bar{z}}$

$|z| = 1$ $\quad \overline{a+bi} = a - bi$



ξ radice primitiva n-esima dell'unità se è radice n-esima ma non è radice d-esima per un qualche $d \mid n$, $d < n$.

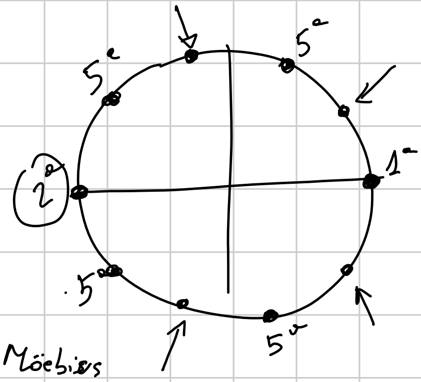
Quante sono le radici primitive n-esime? $\varphi(n)$

Sono tutte radici di $\Phi_n(x)$, n-esimo polinomio ciclotomico

$\Phi_3(x) = \frac{x^3-1}{x-1} = x^2+x+1 \in \mathbb{Z}[x]$ ed è monico

$\Phi_{10}(x) = \frac{x^{10}-1}{x^5-1} \cdot \frac{x^2-1}{x-1}$

$\varphi(10) = (2-1)(5-1)$



$\Phi_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)}$ μ f.d. Möebius

Se ζ è radice di $z^n - 1$, vale $\zeta = \exp\left(\frac{2\pi i}{n} \cdot k\right)$

$= \cos\left(\frac{2\pi}{n} k\right) + i \sin\left(\frac{2\pi}{n} k\right)$

$e^x = \sum_{n \geq 0} \frac{x^n}{n!}$

$\Big\downarrow$ Bin. Newton

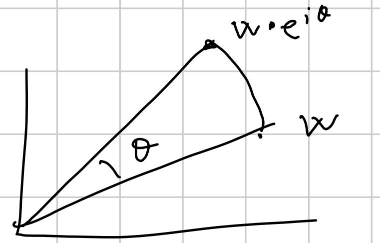
$e^\alpha \cdot e^\beta = e^{\alpha + \beta}$

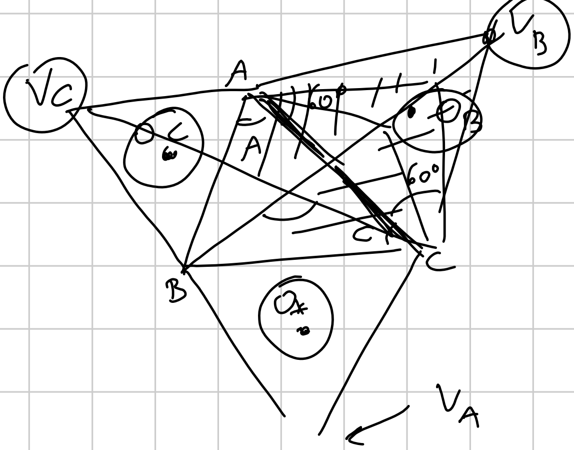
$$\left.\begin{aligned} e^z &\doteq \sum_{n \geq 0} \frac{z^n}{n!} \\ \sin z &= \sum_{n \geq 0} \frac{(-1)^n z^{2n+1}}{(2n+1)!} \\ \cos z &= \sum_{n \geq 0} \frac{(-1)^n z^{2n}}{(2n)!} \end{aligned}\right\} \quad e^{iz} = \cos z + i \sin z$$

$$\boxed{e^{i\pi} + 1 = 0}$$

$\forall z \in \mathbb{C}$, $|z| = 1$, $z = \exp(i\theta)$ per $\theta \in \mathbb{R}$

$w \longmapsto w \cdot \exp(i\theta) = w(\cos\theta + i \sin\theta)$





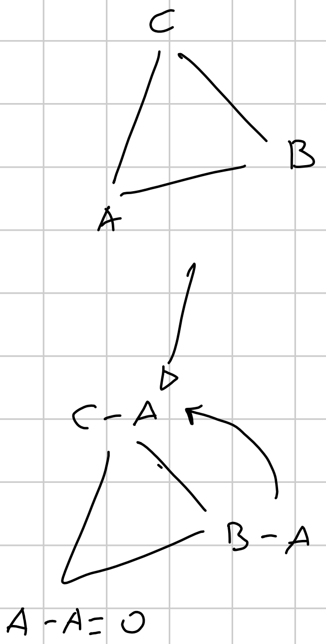
Ex 1. AV_A etc concorrono

$$\frac{[ABV_B]}{[BCV_B]} = \frac{c}{b} \cdot \frac{\sin(A + 60^\circ)}{\sin(C + 60^\circ)}$$

($\exists$ Iperbole di Kiepert)

$\boxed{O_A O_B O_C \text{ è equilatero.}}$

$AV_A \cap BV_B =$ punto di Fermat-Torricelli



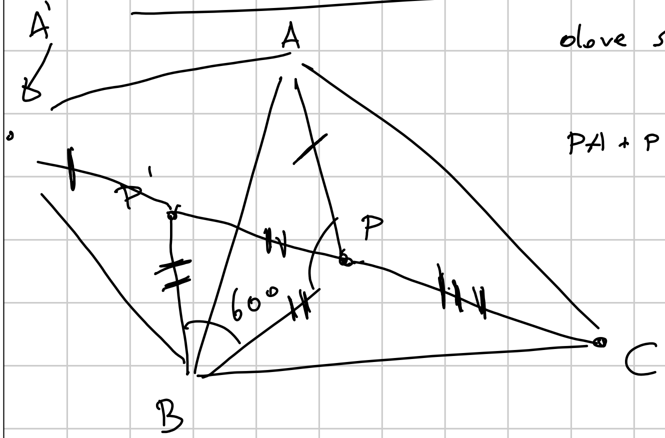
è equilatero se e solo se una rotazione di 60° attorno ad A porta B in C

$$\omega = \exp\left(\frac{i\pi}{3}\right) = \cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right) = \frac{1+i\sqrt{3}}{2}$$

$$(B-A)\omega = (C-A)$$

$$B\omega - A\omega + A - C = 0$$

$$A + \omega B + \omega^2 C = 0$$



dove si trova P che minimizza $PA + PB + PC$

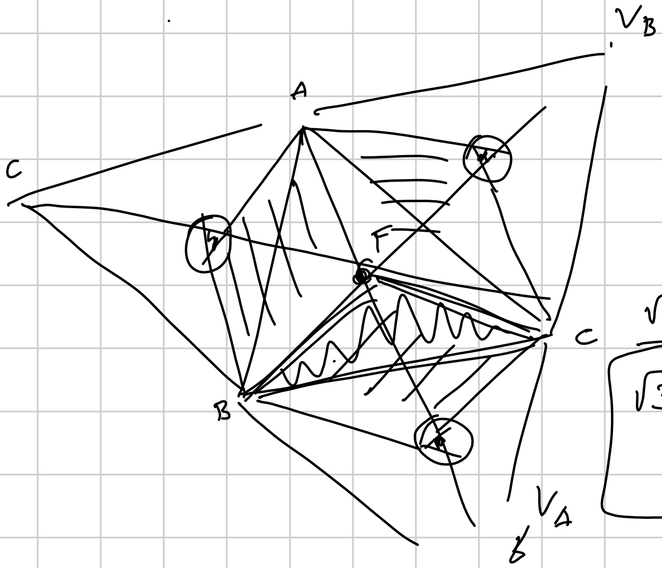
$$PA + PB + PC = CP + PP' + P'A' \geq CA'$$

$$\widehat{BPC} = \widehat{APB} = \widehat{CPA} = 120°$$

si può dimostrare anche minimizzando $PA + PB + PC$ via Moltiplicatori di Lagrange

---

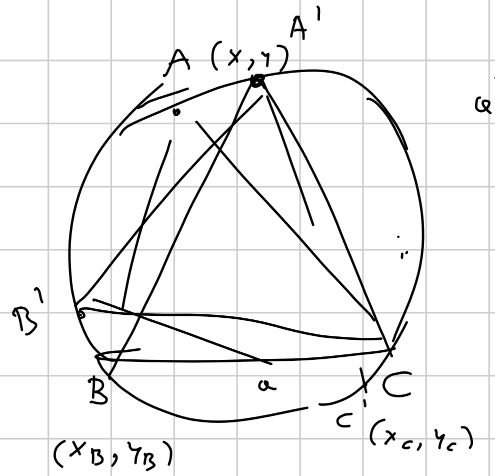
Disug di Weitzenbock



$$\Delta + \frac{\sqrt{3}}{4}(a^2+b^2+c^2) \geq 4\Delta$$

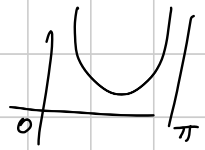
$$\sqrt{3}(a^2+b^2+c^2) \geq 12\Delta$$

$$\boxed{\sqrt{3}(ab+ac+bc) \geq 12\Delta \quad \text{(Roland)}}$$



$$a^2 + (x-x_B)^2 + (y-y_B)^2 + (x-x_C)^2 + (y-y_C)^2 = k$$

$$abc = 4R\Delta$$



$\frac{1}{\sin\theta}$ è $\underbrace{\text{convessa}}$ su $(0, \pi)$

vale la disug di Jensen.

www.oliforum.it

www.matemate.it ⟶ Appunti & Mat. Did.

math.stackexchange.com

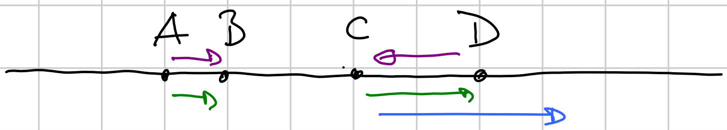
www.cut-the-knot.org

□

G2 medium - Proiettive - Sam

Titolo nota 05/09/2018

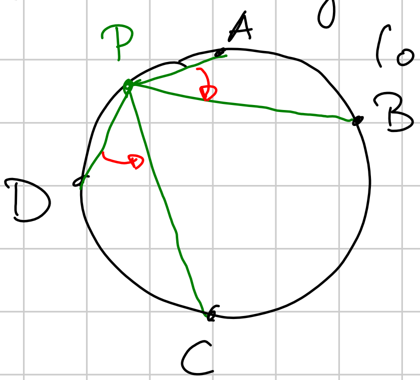
0) Segmenti e archi orientati



$AB > 0 \qquad BA < 0$

$$\frac{AB}{CD} > 0 \qquad \frac{DC}{AB} < 0$$

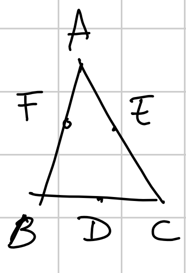
Stessa cosa con gli archi di circonferenza (o le corde)



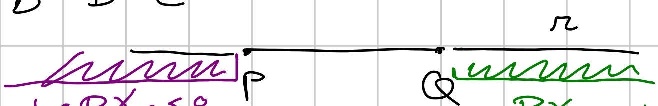
$$\frac{AB}{DC} < 0 \qquad \frac{DB}{BC} > 0$$

$AB \sim A\hat{P}B < 0$

$DC \sim D\hat{P}C > 0$



$$\frac{\overline{BD}}{DC}\cdot\frac{CE}{EA}\cdot\frac{\overline{AF}}{FB} = \begin{cases} 1 & \text{se } AD, BE, CF \text{ concorrono} \\ -1 & \text{se } D, E, F \text{ sono allineati} \end{cases}$$



$-1 < \frac{PX}{XQ} < 0 \qquad \frac{PX}{XQ} < -1$

$X \in r$

$$\frac{PX}{XQ} \text{ è } \begin{cases} > 0 & \text{se } X \text{ sta sul seg. } PQ \\ < 0 & \text{se } X \text{ sta fuori} \end{cases}$$

$$\frac{PX}{XQ} = 0 \iff X \equiv P$$

1) non fa mai -1

2) in $X = Q$ non è definita

Risolviamo 2) dicendo che $\frac{PX}{XQ} = \infty$ quando $X=Q$.

Risolviamo 1) aggiungendo un punto in più alla retta, detto punto all'infinito, cioè l'unico punto X_∞ t.c. $\frac{PX_\infty}{X_\infty Q} = -1$.

Tutte le rette parallele a r passano per X_∞.

— . —

1) Birapporti

Dati A, B, C, D su una retta r, il birapporto è
$$(A,B;C,D) = \frac{AC}{CB} \cdot \frac{BD}{DA}$$
$$\shortparallel$$
$$\frac{AC}{CB} \Big/ \frac{AD}{DB}$$

Oss: 1) $(A,B;C,D) = 1 \iff C \equiv D$ o $A \equiv B$

2) $\left.\begin{matrix}(B,A;D,C)\\(C,D;A,B)\\(D,C;B,A)\end{matrix}\right\}$ sono tutti uguali a $(A,B;C,D) = \lambda$

$(B,A;C,D) = \frac{1}{\lambda}$ $\qquad (C,B;A,D) = \frac{\lambda}{1-\lambda}$

$(D,B;C,A) = 1-\lambda$

$$\boxed{\lambda, \frac{1}{\lambda}, \frac{\lambda}{1-\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{1-\lambda}{\lambda}}$$

3) r (con anche il pt all'∞) $\longrightarrow \mathbb{R} \cup \{\infty\}$

$D \longmapsto (A,B;C,D)$

fisso A,B,C su r

questa funzione è bigettiva.

$A \longmapsto \infty$

$B \longmapsto 0$

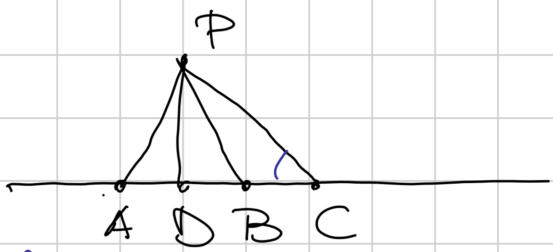
$C \longmapsto 1$

$X_\infty \longmapsto -\dfrac{AC}{CB}$

Lemma 1 $A,B,C,D \in r$

$P \notin r$

Allora $(A,B;C,D)$ si scrive in termini degli angoli in P.



dim: $A\hat{P}C = \alpha$ $\quad A\hat{P}D = \gamma$

$C\hat{P}B = \beta$ $\quad D\hat{P}B = \delta$

Teo dei seni in $\overset{\triangle}{APC}$: $\dfrac{AC}{\sin\alpha} = \dfrac{AP}{\sin A\hat{C}P}$

" " " " $\overset{\triangle}{BPC}$: $\dfrac{CB}{\sin\beta} = \dfrac{BP}{\sin B\hat{C}P}$

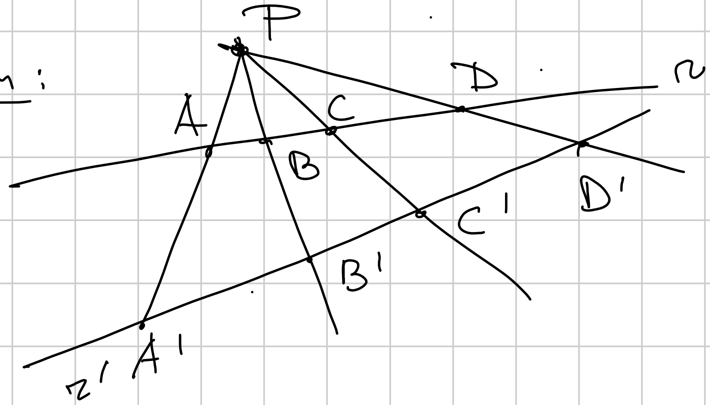
" " " $\overset{\triangle}{BPD}$: $\dfrac{BD}{\sin\delta} = \dfrac{BP}{\sin B\hat{D}P}$

" " " $\overset{\triangle}{DPA}$: $\dfrac{DA}{\sin\gamma} = \dfrac{AP}{\sin A\hat{D}P}$

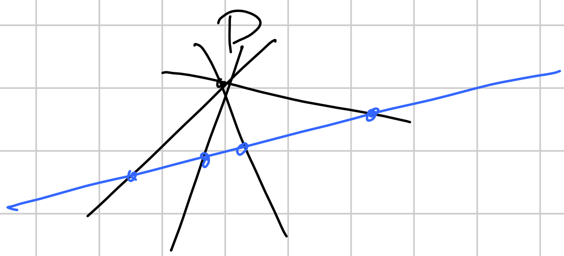
$$\frac{AC}{CB}\cdot\frac{BD}{DA} = \frac{\sin\alpha}{\sin\beta}\cdot\frac{\sin\delta}{\sin\gamma}.$$

Cor 1: Se $A, B, C, D \in r$ e AA', BB', CC', DD' concorrono,
$A', B', C', D' \in r'$
allora $(A, B; C, D) = (A', B'; C', D')$.

dim:



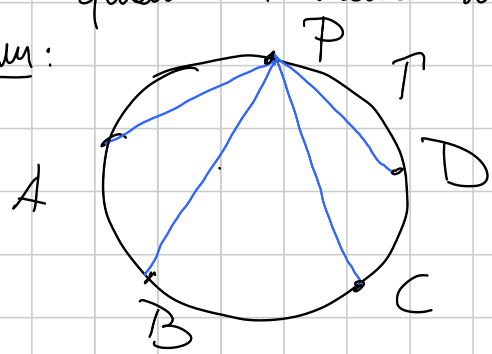
Def: Date 4 rette r_1, r_2, r_3, r_4 concorrenti in un punto P,
$(r_1, r_2; r_3, r_4) = (A, B; C, D)$
con $A = r_1 \cap r$, $B = r_2 \cap r$, $C = r_3 \cap r$, $D = r_4 \cap r$
per una retta r che NON PASSA per P



Notazione: $(A, B; C, D)_P =$
$= (PA, PB; PC, PD)$

Cor 2: Se A, B, C, D sono conciclici su Γ,
allora $(A, B; C, D)_P$ ha lo stesso valore
quando P varia su Γ.

dim:



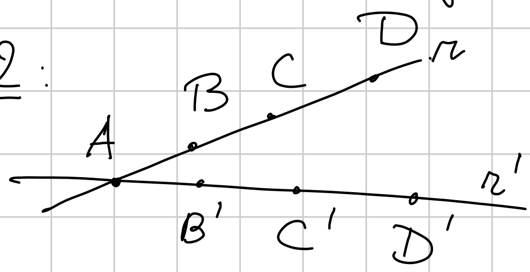
$$\frac{\sin A\hat{P}C}{\sin C\hat{P}B} \cdot \frac{\sin B\hat{P}D}{\sin D\hat{P}A} = \overbrace{\frac{AC}{CB} \cdot \frac{BD}{DA}}^{\text{corde orientate}}$$

teo delle corde

Def: A,B,C,D su Γ $\quad (A,B;C,D)_\Gamma = (A,B;C,D)_P$
per un qualsiasi $P \in \Gamma$.

Nota: $P = A$
Cosa vuol dire $(AA, AB; AC, AD)$??
AA è la retta tangente a Γ in A.

Prop 2:



BB', CC', DD' concorrono se e solo se $(A,B;C,D) =$
$= (A,B';C',D')$

dim: ($\Leftarrow$) $\quad P = BB' \cap CC'$

$$(A,B';C',D') = (A,B;C,D) = (PA,PB;PC,PD) \overset{\text{interseco con } r'}{=} (A,B';C',X)$$

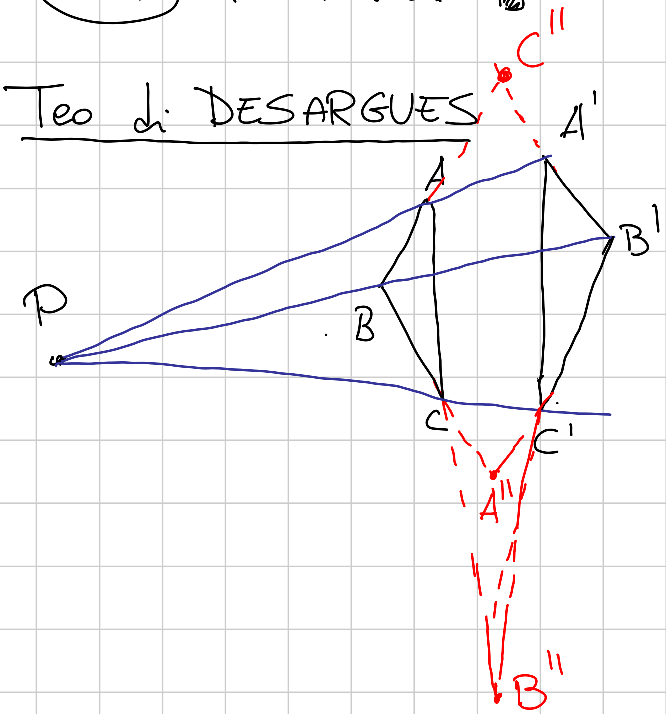
$X = PD \cap r'$

per l'iniettività del birapporto $X = D'$.

$\Rightarrow$ concorrono.

($\Rightarrow$) x esercizio. ∎

Teo di DESARGUES

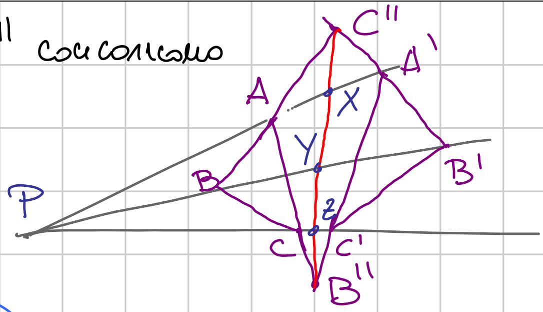


AA', BB', CC' concorrono

$\Downarrow$

$AB \cap A'B' = C''$
$AC \cap A'C' = B''$
$BC \cap B'C' = A''$
sono allineati

dim: Voglio dim che BC, $B'C'$, $B''C''$ concorrono



Chiamo $X = AA' \cap B''C''$
$Y = BB' \cap B''C''$
$Z = CC' \cap B''C''$

$$(P, A; X, A') \underset{\text{da } C''}{=} (P, B; Y, B').$$

da B'' $\rightarrow$ $\|$

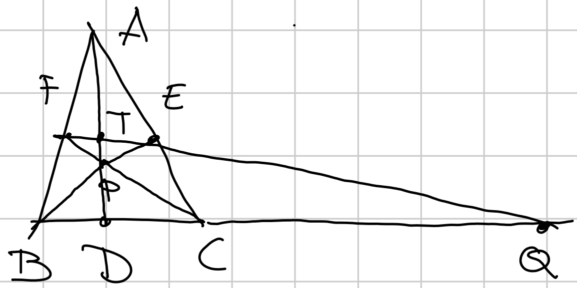
$$(P, C; Z, C')$$

$\Rightarrow$ BC, YZ, $B'C'$ concorrono per la Prop 2.

Es: Se A'', B'', C'' sono allineati, allora AA', BB', CC' concorrono.

Esempi di birapporti

(1)



$$(B, C; D, Q) \underset{\substack{\text{proiez da } A\\ \text{su } EF}}{=} (F, E; T, Q) \underset{\substack{\text{proiez da } P\\ \text{su } BC}}{=} (C, B; D, Q)$$

$$\Rightarrow (B, C; D, Q) = \frac{1}{(B, C; D, Q)}$$

non può fare 1 $\Rightarrow (B, C; D, Q) = -1$

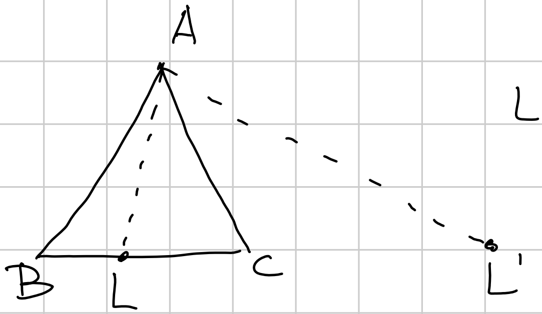
Oppure

Per menelao E, F, Q allineati $\Rightarrow \dfrac{BF}{FA} \cdot \dfrac{AE}{EC} \cdot \dfrac{CQ}{QB} = 1$

Per Ceva, AD, BE, CF concorrenti $\Rightarrow \frac{AE}{EC}\cdot\frac{CD}{DB}\cdot\frac{BE}{FA} = 1$

$\Rightarrow$ Facendo il rapporto $\boxed{\frac{BD}{DC}\cdot\frac{CQ}{QB} = -1}$.

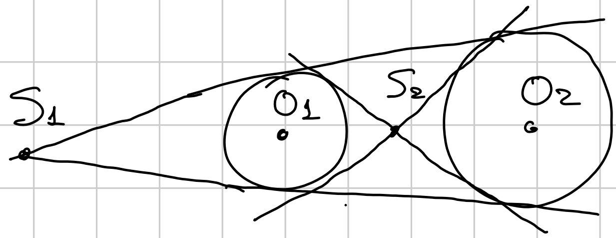
(2)



L, L' piedi di bisettrice interna e esterna

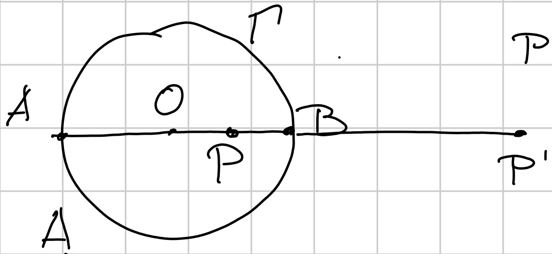
$(B, C; L, L') = ?$

(3)



$(O_1, O_2; S_1, S_2) = ?$

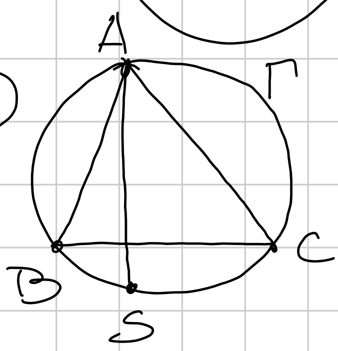
(4)



P' inverso di P in Γ

$(A, B; P, P') = ?$

(5)



AS simmediana

$(A, S; B, C) = ?$

Soluzioni

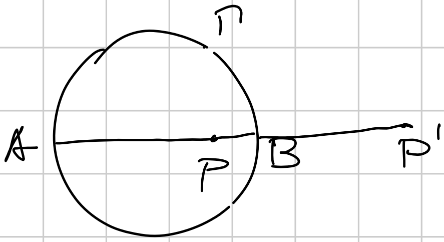
(2) Teo delle bisettrice: $\frac{BL}{LC} = \frac{BA}{AC}$ $\quad \frac{BL'}{L'C} = -\frac{BA}{AC}$

$\Rightarrow (B, C; L, L') = -1$

(3) S_1, S_2 centri di similitudine

$$\Longrightarrow \quad \frac{O_1S_1}{S_1O_2} = -\frac{R_1}{R_2} \qquad \frac{O_1S_2}{S_2O_2} = \frac{R_1}{R_2} \quad \Longrightarrow (O_1,O_2;S_1,S_2) = -1$$

4



a) faccio i conti

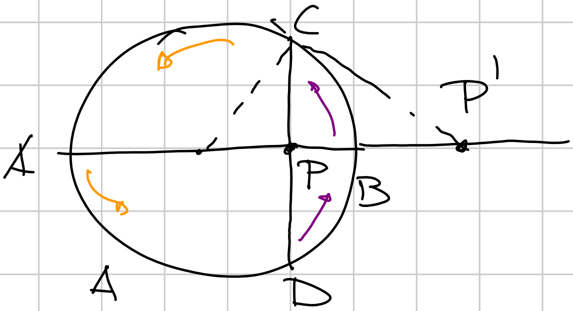
$$X,Y \xrightarrow[\text{inversione}]{} X',Y'$$

$$X'Y' = R^2 \frac{XY}{OX \cdot OY}$$

$$BP' = \frac{BP}{\cancel{OB}\cdot OP}\cdot R^{\cancel{2}}$$

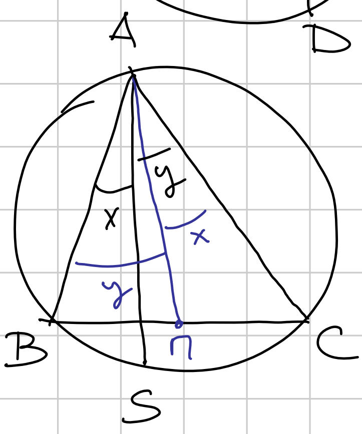
$$AP' = \frac{AP}{\cancel{OA}\cdot OP}\cdot R^{\cancel{2}} \qquad \Longrightarrow (A,B;P,P') = -1$$

b)



$$(A,B;P,P') = (CA,CB;CP,CP') = (A,B;D,C)_\Gamma = \frac{AD}{DB}\frac{BC}{CA} = -1$$

5



$$(A,S;B,C)$$

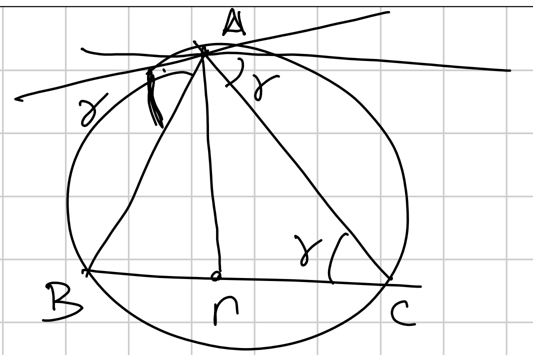
a)

$$\frac{\Gamma C}{\sin x} = \frac{AC}{\sin A\hat{\Gamma}C} \qquad \frac{\Gamma B}{\sin y} = \frac{AB}{\sin A\hat{\Gamma}B} \qquad \Longrightarrow \frac{\sin x}{\sin y} = \frac{AB}{AC}$$

$$\frac{BS}{SC} = \frac{\sin x}{\sin y} = \frac{AB}{AC} \quad \Longrightarrow (A,S;B,C) = -1$$

b) - $(A,S;B,C)_\Gamma = (AA,AS;AB,AC) \overset{\text{simmetria risp. alla bisett. di } B\hat{A}C}{=}$

$= (r, A\Gamma; AC, AB) \underset{\text{interseco con BC}}{=} (X_\infty, \Gamma; C, B) = -1$



r è la $//$ a BC per A

X_∞ = pt all'∞ di r

<u>Lemma 3</u>: I birapporti si conservano sotto inversione

<u>dim</u>: $A,B,C,D \longrightarrow A',B',C',D'$

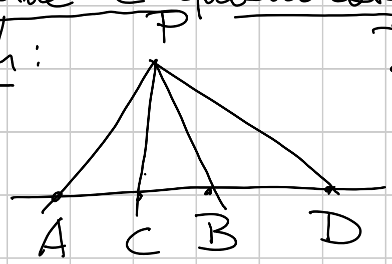
$$\left|\frac{A'C'}{C'B'}\right| = \left|\cancel{R^2}\frac{AC}{OA\cdot\cancel{OC}}\cdot\frac{\cancel{OC}\cdot OB}{BC\cdot\cancel{R^2}}\right| = \left|\frac{AC}{BC}\right|\cdot\left|\frac{OB}{OA}\right|$$

$$\left|\frac{B'D'}{D'A'}\right| = \left|\frac{BD}{DA}\right|\cdot\left|\frac{OA}{OB}\right|$$

e l'inversione mantiene l'ordine tra i punti. $\square$

2) <u>Quaterne e quadrilateri armonici</u>

<u>Lemma 4</u>:



Due delle seguenti implicano la terza:

(i) $(A,B;C,D) = -1$

(ii) PC biseca $\widehat{APB}$

(iii) $PC \perp PD$

(i) + (ii) $\Rightarrow$ PD bisett. esterna $\Rightarrow PD \perp PC$

(ii) + (iii) $\Rightarrow$ PD bisett. esterna $\Rightarrow (A,B;C,D) = -1$

(i) + (iii) $\Rightarrow$ $\widehat{APD} = \widehat{APC} + \frac{\pi}{2}$

$\widehat{BPD} = \widehat{BPC} + \frac{\pi}{2}$

$$\frac{\sin\widehat{APC}}{\sin\widehat{CPB}} = -\frac{\sin(\widehat{APD})}{\sin(\widehat{DPB})} = \frac{\cos(\widehat{APC})}{\cos(\widehat{CPB})} \Rightarrow \operatorname{tg}\widehat{APC} = = \operatorname{tg}\widehat{CPB}$$

$\Rightarrow \widehat{APC} = \widehat{CPB} \Rightarrow PC$ bisettrice.

Def: $(A,B;C,D) = -1$ si dicono quaterna armonica

D quarto armonico

Lemma 5: O pt. medio di AB, allora le seguenti sono equivalenti

(i) $(A,B;C,D) = -1$

(ii) $\dfrac{2}{AB} = \dfrac{1}{AC} + \dfrac{1}{AD}$ (iv) $OC \cdot OD = OA^2$

(iii) $CA \cdot CB = CO \cdot CD$ (v) $\dfrac{OC}{OD} = \left(\dfrac{AC}{AD}\right)^2 = \left(\dfrac{BC}{BD}\right)^2$

Def: A, B, C, D su Γ con $(A,B;C,D)_\Gamma = -1$ si dicono quadrilatero armonico.

Prop 6: A, B, C, D su Γ, allora le seguenti sono equivalenti

(i) $AB \cdot CD = BC \cdot AD$

(ii) BD simmediana di $\overset{\triangle}{ABC}$

(iii) le tangenti a Γ in A e C si incontrano su BD

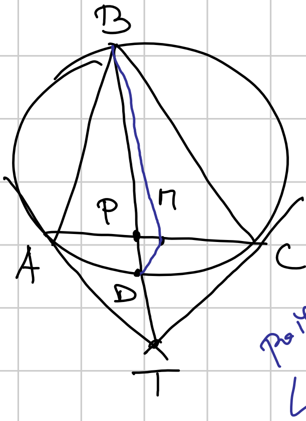
(iv) $(A, C; B, D)_\Gamma = -1$

(v) M pt. medio di AC, allora MB, MD simmetriche rispetto ad AC.

(vi) la bisettrice di $\widehat{ABC}$ e quella di $\widehat{ADC}$ si intersecano su AC

(vii) $\dfrac{AB^2}{AD^2} = \dfrac{MB}{MD}$.

(v)



AC bisett. di $B\hat{M}D$

$$\Updownarrow$$

$(B,D;P,T)=-1$

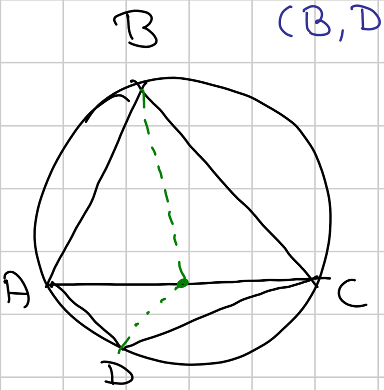
e

$P\hat{M}T=\frac{\pi}{2}$ ✓ ovvio

polare di C

$(B,D;A,C)_\Gamma=-1 \iff BD$ simmediana

(vi)



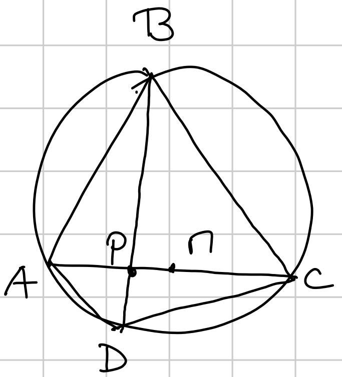
bisett. di $A\hat{B}C = BL$ $\qquad L, L' \in AC$

bisett di $A\hat{D}C = BL'$

$$\frac{AL}{LC}=\frac{AB}{BC} \qquad \frac{AL'}{L'C}=\frac{AD}{DC}$$

$$L=L' \iff \frac{AB}{BC}=\frac{AD}{DC} \iff \underbrace{(A,C;B,D)}_{=-1}$$

(vii)



$$\frac{BP}{PD}=\frac{AP}{\sin A\hat{B}D}\cdot \sin B\hat{A}P\left(\frac{1}{AP}\,\frac{\sin A\hat{D}B}{\sin P\hat{A}D}\right)$$

$$=\frac{\sin B\hat{A}C}{\sin A\hat{B}D}\cdot\frac{\sin A\hat{D}B}{\sin C\hat{A}D}=$$

$$=\frac{BC}{AD}\,\frac{AB}{CD}$$

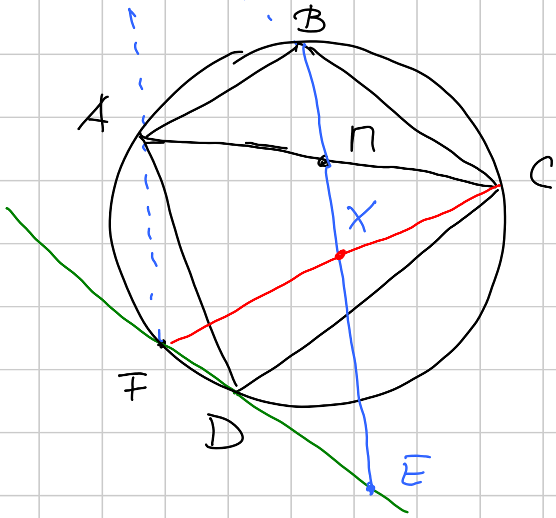
$$AB\cdot CD=BC\cdot AD \iff \frac{AB}{AD}=\frac{BC}{CD} \iff \frac{BP}{PD}=\left(\frac{AB}{AD}\right)^2$$

$$\Updownarrow$$

$$MP \text{ bisett. di } B\hat{M}D \iff \frac{BP}{PD}=\frac{BM}{MD}$$

$$AB\cdot CD=BC\cdot AD \implies \frac{BM}{MD}=\left(\frac{AB}{AD}\right)^2.$$

Es: $ABCD$ ciclico, bisettrici di $A\hat{B}C$ e $A\hat{D}C$ si intersecano su AC. Sia M pt. medio di AC.
La retta parallela a BC per D incontra BM in E e la cfr. circoscritta ad $ABCD$ in $F \neq D$.
Dim. che $BCEF$ è un parallelogramma



dim: $ABCD$ armonico

$(B, D; A, C) = -1$

$BE \cap CF = X$

$AF \cap BC = Y$

$(FB, FD; FY, FC) = -1$

interseco con BC

$(B, X_\infty; Y, C) = -1$

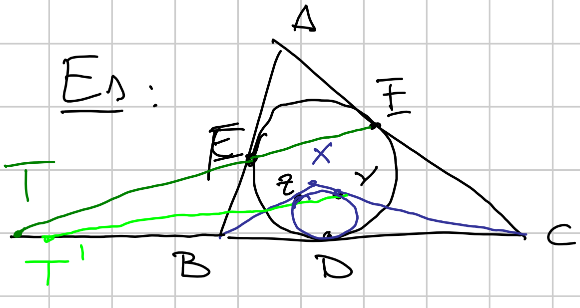
X_∞ pt all'∞ di BC

$YB = BC$

$\Downarrow$

$FY \parallel BM \Rightarrow FX = XC$ ∎

Es:



X t.c. l'inscritta in $X\hat{B}C$ tange BC in D. Allora $EFZY$ è ciclico.

Hope: $FE \cap ZY$ sta su BC.

$FE \cap BC = T$ $\quad (B, C; D, T) = -1$
perché AD, BE, CF concorrono

$ZY \cap BC = T'$ $\quad (B, C; D, T') = -1$
perché XD, BY, CZ concorrono.

$\Rightarrow T = T'$

$TD^2 = TY \cdot TZ$

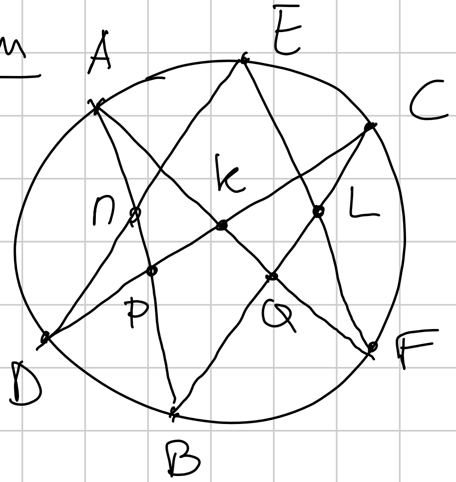
$TD^2 = TE \cdot TF$ $\Rightarrow TE \cdot TF = TY \cdot TZ \Rightarrow$ ciclico.

Teo (Pascal)

Γ cf. A, B, C, D, E, F su Γ

$\Rightarrow AB \cap DE = M$
$BC \cap EF = L$ sono allineati
$CD \cap FA = K$

dim



$(C, L; Q, B) \overset{\text{da } F \text{ su } \Gamma}{=} (C, E; A, B)_\Gamma \overset{\text{da } D \text{ su } AB}{=}$

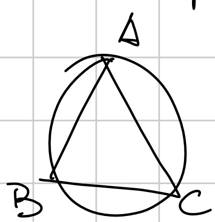
$= (P, M; A, B) \overset{\text{da } K \text{ su } CB}{=}$

$= (C, MK \cap BC; Q, B)$

$MK \cap BC = L \Rightarrow M, K, L$ allineati. $\boxtimes$

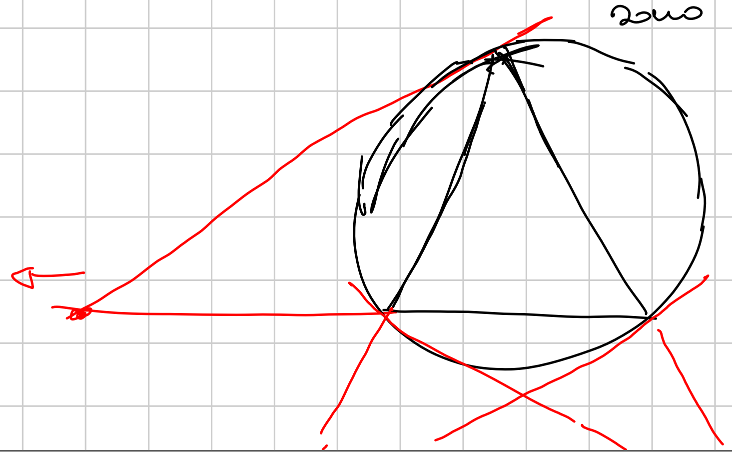
Oss: Se due punti coincidono, si usa la tangente

Es:



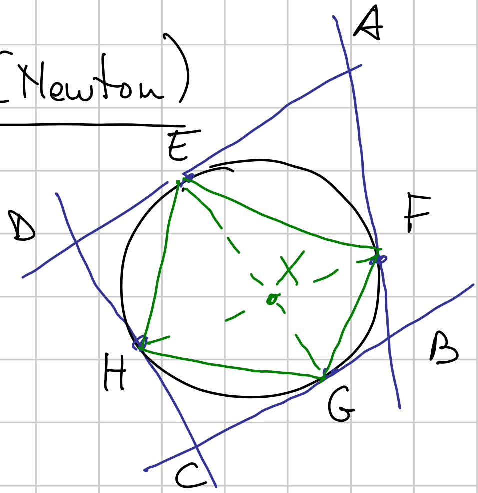
$AABBCC$

$AA \cap BC$, $AB \cap CC$, $BB \cap CA$ sono allineati.



questa retta si chiama asse di Lemoine

Teo (Newton)



Allora AC, BD, EG, FH concorrono

dim: $EG \cap FH = X \qquad EH \cap FG = Y$

Pascal su $EGGFHH$

$EG \cap F\cancel{H}H = X$
$GG \cap HH = C$
$GF \cap EH = Y$

sono allineati

Pascal su $EEHFFG$

$EE \cap FF = A$
$EH \cap FG = Y$
$HF \cap GE = X$

sono allineati

A, C, X, Y sono allineati

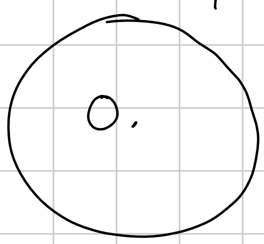
Definisco $Z = EF \cap HG$ e dimostro che B, D, X, Z sono allineati ancora con 2 pascal. $\square$

Cor: A, C, X, Y
B, D, X, Z allineati.

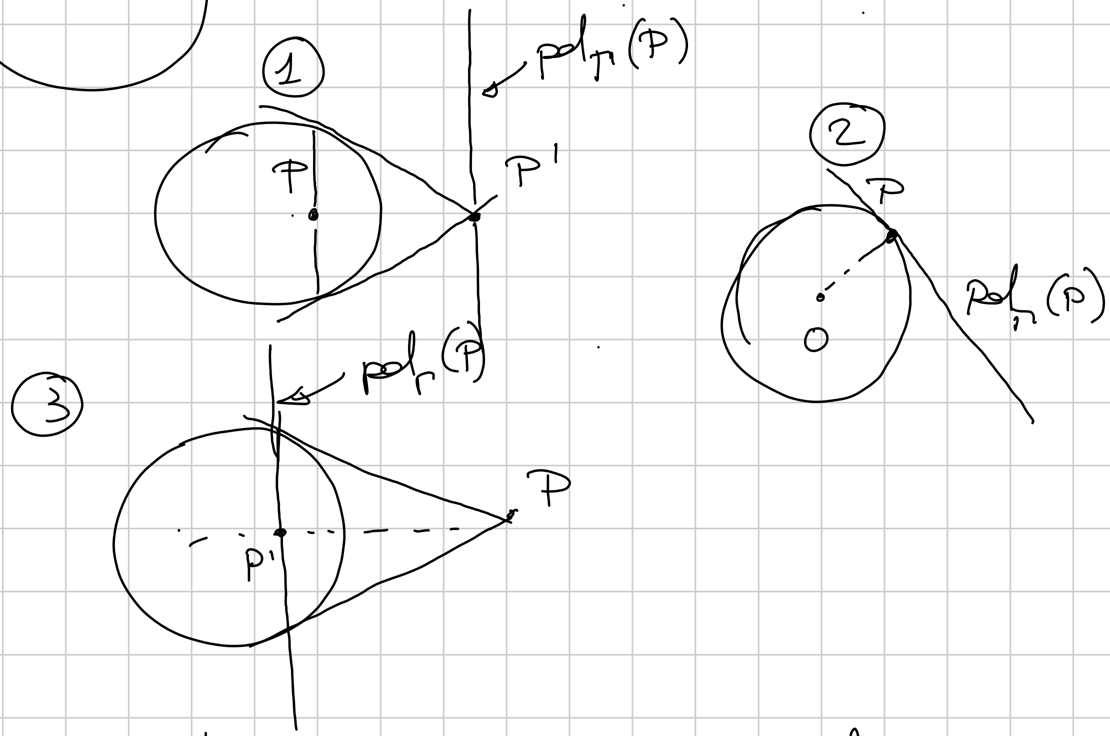
Teo (Brianchon): $ABCDEF$ circoscritto a Γ allora AD, BE, CF concorrono.

3) Poli e polari

Γ



La polare rispetto a Γ di un punto P è la retta $\perp$ a OP che passa per l'inverso di P.

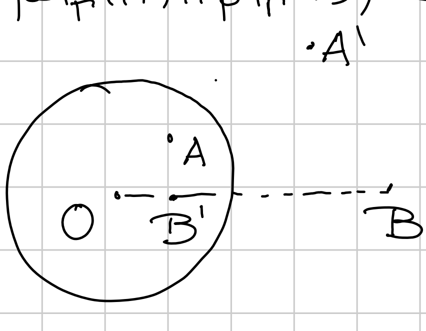


Γ cfr. r retta $\quad P = \mathrm{pol}_\Gamma(r) \iff r = \mathrm{pol}_\Gamma(P)$

Proprietà

1. $A \in \mathrm{pol}_\Gamma(B) \iff B \in \mathrm{pol}_\Gamma(A)$
2. $\mathrm{pol}_\Gamma(r \cap s) =$ retta per $\mathrm{pol}_\Gamma(r)$ e $\mathrm{pol}_\Gamma(s)$
3. $\mathrm{pol}_\Gamma(A) \cap \mathrm{pol}_\Gamma(B) = \mathrm{pol}_\Gamma(AB)$

Dim: (1)

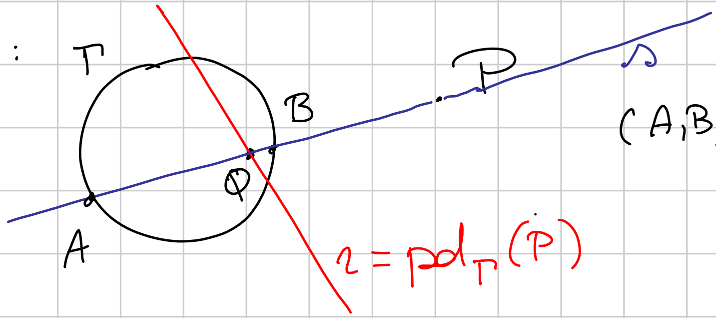


$$A \in \mathrm{pol}_\Gamma(B)$$
$$\Updownarrow$$
$$A\hat{B'}O = \frac{\pi}{2}$$
$$\Updownarrow$$
$$B \in \mathrm{pol}_\Gamma(A) \iff B\hat{A'}O = \frac{\pi}{2}$$

(2), (3) esercizio

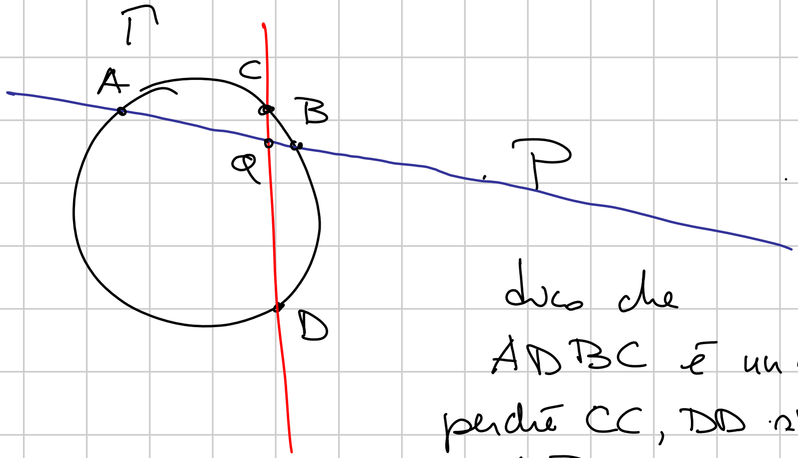
Oss: $\mathrm{pol}_\Gamma(P) = \{\mathrm{pol}_\Gamma(r) \mid P \in r\}$

Prop:



$(A,B;Q,P) = -1$

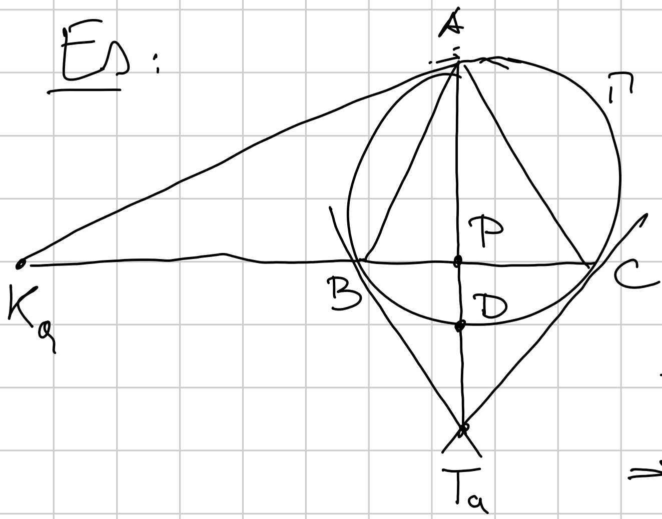
dim:



dico che $ADBC$ è un quad. armonico perché CC, DD si intersecano in P

$$\Rightarrow (A,B;C,D) = -1$$
$$\| $$
$$(A,B;Q,P).$$

Es:



$BC = \mathrm{pol}_\Gamma(T_a)$

$K_a \in \mathrm{pol}_\Gamma(T_a)$

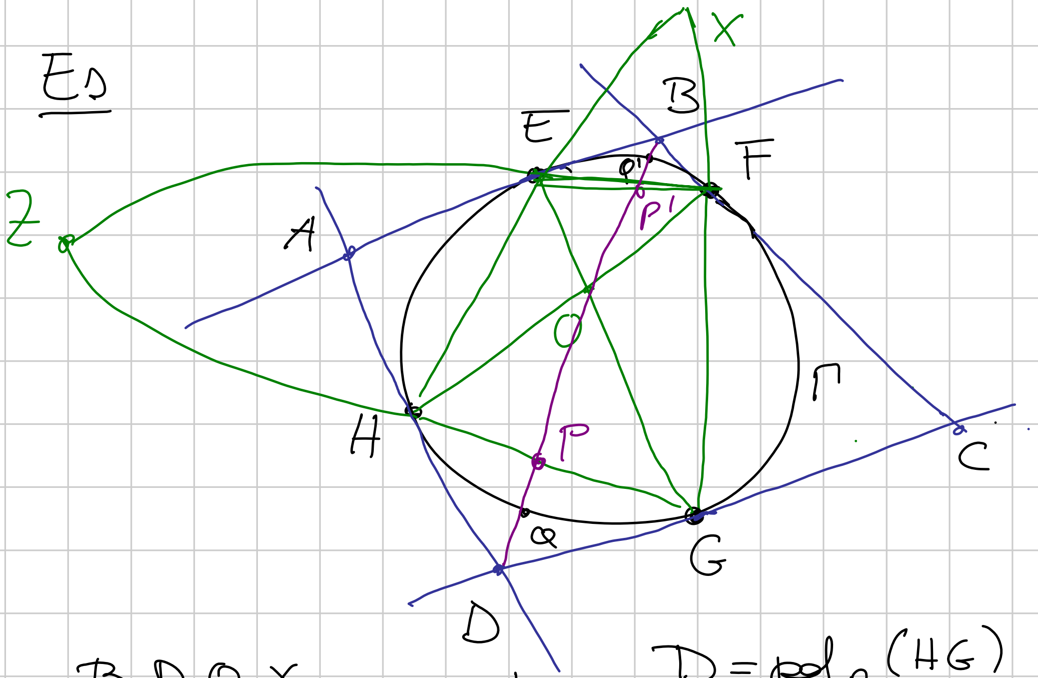
$\Rightarrow T_a \in \mathrm{pol}_\Gamma(K_a)$

e $A \in \mathrm{pol}_\Gamma(K_a)$

$\Rightarrow T_aA = \mathrm{pol}_\Gamma(K_a)$

$\Rightarrow (B,C;P,K_a) = -1$

Es



B, D, O, X
Z, A, O, C allineati

$D = \mathrm{pol}_\Gamma(HG)$
$B = \mathrm{pol}_\Gamma(EF)$

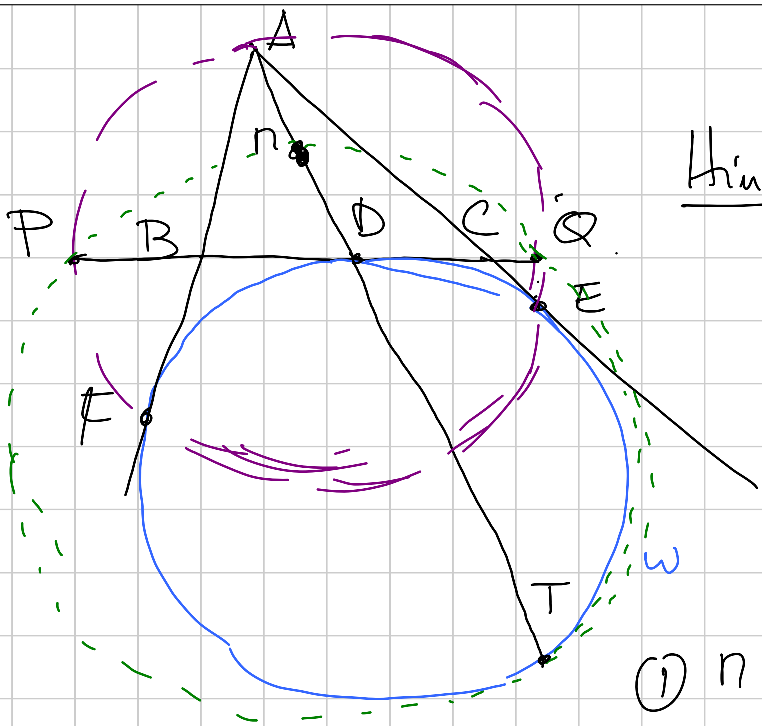
$\Longrightarrow Z = \mathrm{pol}_\Gamma(BD)$

$P = BD \cap HG \quad P' = BD \cap EF$

$$(H, G; P, Z) = -1$$
$$(E, F; P', Z) = -1$$

Romanian TST 2018

ABC triangolo, ω excerchio opposto ad A
D, E, F tangenze di ω con BC, CA, AB
La circonf per EAF interseca BC in P e Q.
M pt. medio di AD
Dim che la circoscritta a MPQ è tangente a ω.



Hint: DETF armonico

$\Downarrow$

BC

EF

tang a ω in T

concorrono in R

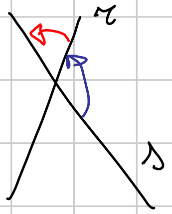
(1) ΠPTQ ciclico

(2) Tangenza in T calcolando le potenze da R

G3 medium - Metodo Sintetico - Som

Titolo nota 06/09/2018

1) Angoli orientati modulo π



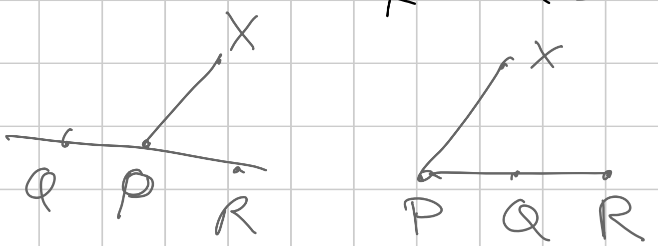
- $\measuredangle(r,s)$ = angolo per portare r su s in senso antiorario
- $\measuredangle(s,r)$ = angolo per portare s su r in senso antiorario

$$\measuredangle(r,s) + \measuredangle(s,r) = 0 \quad (\text{mod } \pi)$$

$$\measuredangle APB = \measuredangle(AP, PB)$$

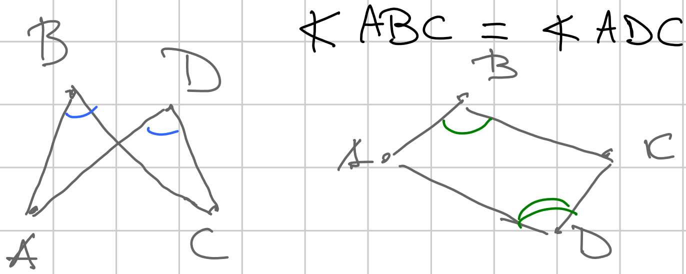
Es 1: Per dimostrare P, Q, R allineati basta dimostrare che esiste X t.c.

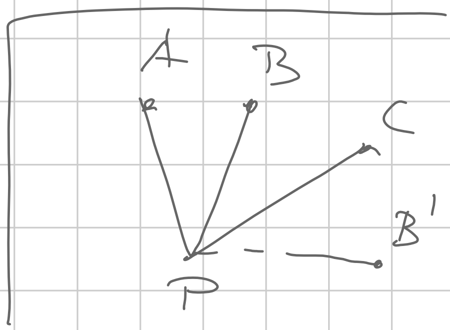
$$\measuredangle XPQ = \measuredangle XPR$$



Es 2: Per dimostrare che $ABCD$ è ciclico mi basta dimostrare che

$$\measuredangle ABC = \measuredangle ADC$$



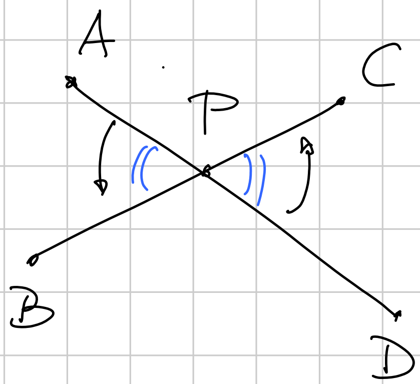


Altre proprietà: i) $\measuredangle ABC = -\measuredangle CBA$

ii) $\measuredangle APB + \measuredangle BPC = \measuredangle APC$

iii) $\measuredangle ABC + \measuredangle BCA + \measuredangle CAB = 0$

Es:



$\measuredangle APB = \measuredangle DPC$

Es: Se so che $\measuredangle ABC = \measuredangle DEF$

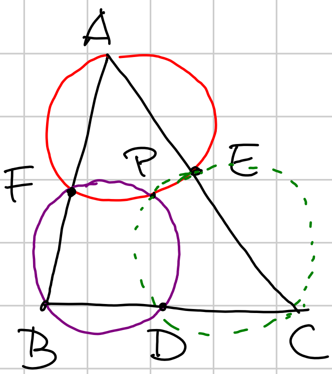
$\measuredangle BCA = \measuredangle EFD$

posso dire che $ABC \sim DEF$? Certo! Perché ci convince.

2) Configurazioni di Miquel

(I) ABC triangolo D, E, F sulle rette BC, CA, AB risp.
Allora (AEF), (BDF), $C(DE)$ concorrono.

(XYZ) la circonf per X, Y, Z



Dim: Sia P l'altra intersezione di (AEF) e (BFD) oltre ad F.
Voglio dim $PECD$ ciclico.

$\iff \measuredangle PEC \overset{?}{=} \measuredangle PDC$

$\measuredangle PEC = \measuredangle PEA$ (perché A, E, C allineati)

$\measuredangle PEA = \measuredangle PFA = \measuredangle PFB = \measuredangle PDB = \measuredangle PDC$

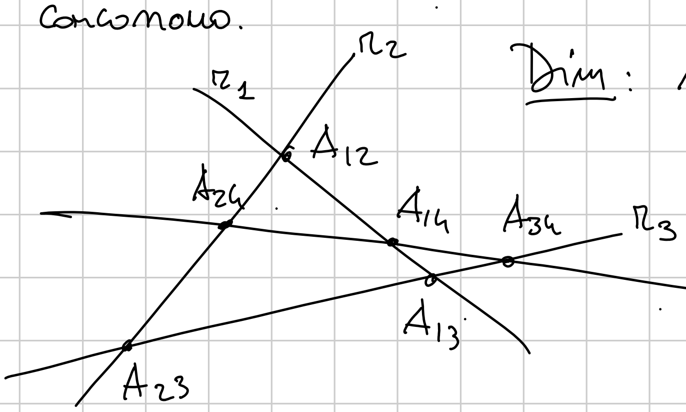
ciclicità F, A, B allineati   ciclicità B, D, C allineati.

$\boxtimes$

P si dice punto di Miquel di D, E, F in $\overset{\triangle}{ABC}$.

Es: P a caso, D, E, F proiez. sui lati di P
$\Rightarrow$ P pt. di Miquel di D, E, F in ABC.

(II) r_1, r_2, r_3, r_4 rette in posizione generale
cioè non ve ne sono due parallele o 3 concorrenti
Sia $A_{ij} = r_i \cap r_j$. Allora
$(A_{12}A_{23}A_{13})$, $(A_{13}A_{34}A_{14})$, $(A_{12}A_{24}A_{14})$, $(A_{23}A_{34}A_{24})$
concorrono.



Dim: Applico I al triangolo $A_{12}A_{13}A_{23}$ con punti A_{24}, A_{34}, A_{14}

$\Downarrow$

$\boxed{(A_{12}A_{24}A_{14})}$
$(A_{13}A_{34}A_{14})$
$\boxed{(A_{23}A_{34}A_{24})}$

concorrono in M

Applico I al triangolo $A_{13}A_{34}A_{14}$ con i punti A_{12}, A_{24}, A_{23}

$\Downarrow$

$(A_{13}A_{23}A_{12})$
$\boxed{(A_{34}A_{24}A_{23})}$
$\boxed{(A_{14}A_{24}A_{12})}$

concorrono in M'.

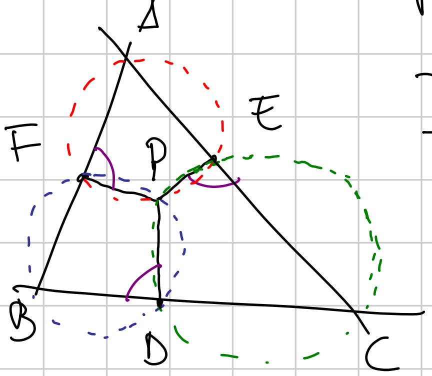
$\Rightarrow M' = M$
oppure
$\cancel{M' = A_{24}}$ impossibile

$\Rightarrow$ le circonf. concorrono in M.

Es: I circocentri O_1, O_2, O_3, O_4 sono conciclici su una circonferenza che passa per M.

Es2: Gli ortocentri H_1, H_2, H_3, H_4 stanno su una sola retta detta retta di STEINER–MIQUEL.

Oss: ABC triangolo, D,E,F sulle rette BC, CA, AB.
P t.c. $\sphericalangle PDB = \sphericalangle PEC = \sphericalangle PFA$
Allora P è il pt. di Miquel di D,E,F in ABC



Dim: $\sphericalangle PEC = \sphericalangle PDB = \sphericalangle PDC$
$\Rightarrow$ $CDPE$ ciclico.
Così si fanno gli altri due. $\square$

Oss2: P pt. di Miquel di D,E,F in ABC
$P \in (ABC) \iff D,E,F$ allineati.

Dim: $\Leftarrow$ è il Teo di Miquel II.

$\Rightarrow$ So che $\sphericalangle APB = \sphericalangle ACB$ (ciclicità di $APBC$)
Se dim che $\sphericalangle PFE = \sphericalangle PFD$ ho finito!

$$\sphericalangle PFE = \sphericalangle PFA - \underbrace{\sphericalangle EFA}_{} = \sphericalangle PFA - \underbrace{\sphericalangle EPA}_{} = \sphericalangle PFA + \underbrace{\sphericalangle APE}_{}$$
ciclicità di $EPFA$

$$\sphericalangle PFD = \sphericalangle PFB - \underbrace{\sphericalangle DFB}_{} = \sphericalangle PFB - \underbrace{\sphericalangle BPB}_{} = \underbrace{\sphericalangle PFB}_{} + \sphericalangle BPD$$
ciclicità di $DPFB$

$\parallel \to A,F,B$ allineati

$$\sphericalangle APE + \sphericalangle EPD + \sphericalangle DPB + \sphericalangle BPA = 0 \Rightarrow \sphericalangle APE = \sphericalangle BPD$$

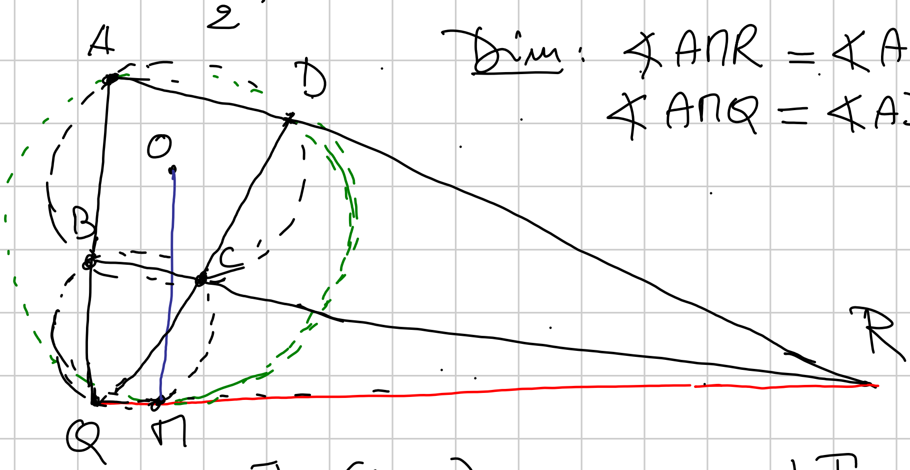
ciclicità di $EPCD$ $\to$ $\sphericalangle EPD = \sphericalangle ECD = \sphericalangle ACB = \sphericalangle APB$

$$\Rightarrow \sphericalangle PFE = \sphericalangle PFD. \ \blacksquare$$

Corollario (RETTA DI SIMSON) Se proietto $P \in (ABC)$ sui lati, ottengo 3 punti allineati.

Lemma: $ABCD$ ciclico, $P = AC \cap BD$, $Q = AB \cap CD$, $R = AD \cap BC$

M pt. di Miquel di AB, BC, CD, DA. Allora $M \in QR$ e, detto O il centro di $(ABCD)$, si ha $O\hat{M}R = \frac{\pi}{2}$.



Dim: $\sphericalangle AMR = \sphericalangle ABR = \sphericalangle ABC$

$\sphericalangle AMQ = \sphericalangle ADQ = \sphericalangle A\hat{D}C$

perché $ABCD$ ciclico.

$\Gamma = (ABCD)$ $\quad r =$ raggio di Γ

$$pow_\Gamma(R) = RO^2 - r^2 = RA \cdot RD = RC \cdot RB = RQ \cdot RM$$

$$pow_\Gamma(Q) = QO^2 - r^2 = QB \cdot QA = QC \cdot QD = QM \cdot QR$$

$$\boxed{RO^2 - QO^2} = QR(RM - QM) = \boxed{RM^2 - QM^2}$$

$\Downarrow$ + Q, M, R allineati

$OM \perp QR$

Altre proprietà

(i) $MOAC$, $MODB$ ciclici

(ii) MO biseca $A\hat{M}C$ e $B\hat{M}D$

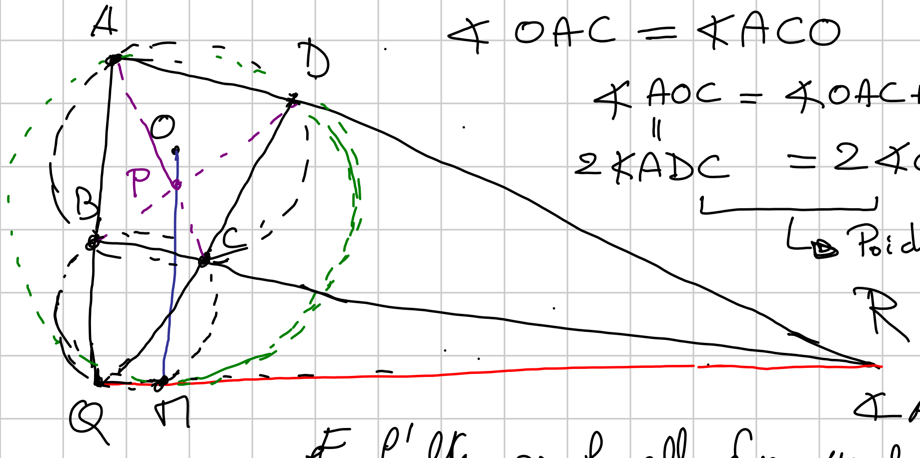
(iii) OM, AC, BD concorrono (in P)

(iv) P, M inversi risp. a Γ

(v) O ortocentro di PQR.

Dim: (i) $\quad \sphericalangle OMC = \sphericalangle OAC$

$$\sphericalangle OMR + \sphericalangle RMC = \frac{\pi}{2} + \sphericalangle RDC = \frac{\pi}{2} + \sphericalangle ADC$$



$\sphericalangle OAC = \sphericalangle ACO$

$\sphericalangle AOC = \sphericalangle OAC + \sphericalangle ACO =$
$\overset{\shortparallel}{2\sphericalangle A\hat{D}C} = 2\sphericalangle OAC$

$\hookrightarrow$ Poiché $A\hat{D}C$ deve essere $\geq O\hat{A}C$ si deve avere $\sphericalangle ADC = \frac{\pi}{2} + \sphericalangle OAC$

E l'altro si fa allo stesso modo.

(ii) MO biseca $A\hat{M}C$

$\left.\begin{array}{l}\sphericalangle AMO = \sphericalangle ACO \\ \sphericalangle OMC = \sphericalangle OAC\end{array}\right\}$ perché O è il centro di Γ

Idem l'altro

(iii) Assi radicali

(iv) P, M inversi in Γ: sappiamo che $P = pol_\Gamma(QR)$

$\Rightarrow$ inv di $P \in pol_\Gamma(P) \cap OP = M$

$\Rightarrow$ inv di P è M.

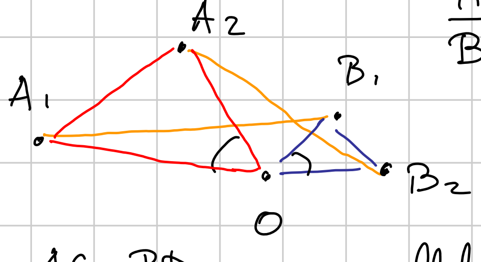
(v) Posso permutare A, B, C, D scambiando tra loro P, Q, R e so che (in ogni configurazione) $OP \perp QR$

$\Rightarrow$ O ortocentro di PQR.

3) Rotomotetie (Spiral similarities)

$\shortparallel$

[rotazione + omotetia]



$\frac{A_1O}{B_1O} = \frac{A_2O}{B_2O}$

$A_1\hat{O}B_1 \overset{\shortparallel}{} A_2\hat{O}B_2$

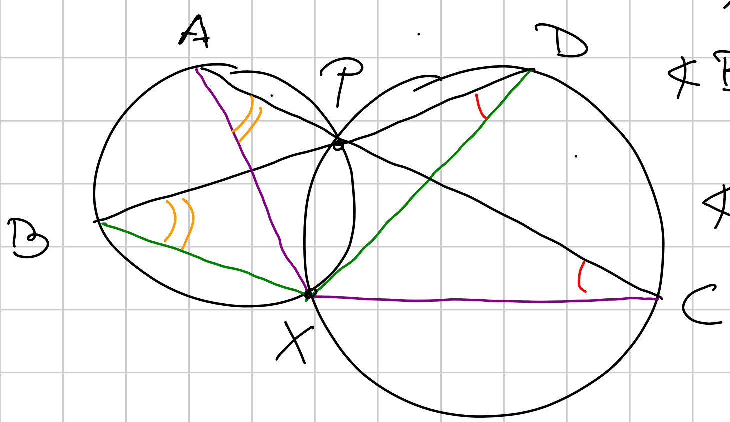
Lemma: A, B, C, D con AC e BD non parallele

Allora esiste una rotomotetia che manda A in C e B in D

Dim: $P = AC \cap BD$ X pt. di Miquel di AB, CD, AC, BD

$X = (ABP) \cap (CDP)$ e non è P.

Se dim ACX e BDX sono simili, ho finito



$\sphericalangle BDX = \sphericalangle PDX = \sphericalangle PCX$
$= \sphericalangle ACX$

$\sphericalangle DBX = \sphericalangle PBX = \sphericalangle PAX$
$= \sphericalangle CAX$

$\Rightarrow$ simili ■

Lemma: X è il centro anche di una rotomotetia che manda A in B e C in D

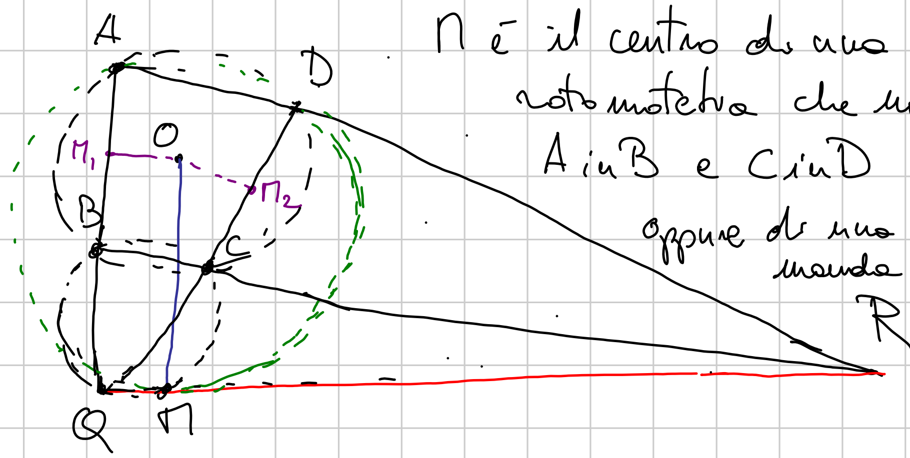
Dim: So che $\sphericalangle AXB = \sphericalangle CXD$

$$\frac{XC}{XA} = \frac{XD}{XB} \Rightarrow \frac{XB}{XA} = \frac{XD}{XC}$$

$\Rightarrow$ tri $B\hat{X}A$ e $D\hat{X}C$ simili $\Rightarrow$ ho finito. ■

Es: Si può dim $OM \perp QR$ anche con le rotomotetie.

Dim:



M è il centro di una rotomotetia che manda A in B e C in D

oppure di una che manda A in D e B in C

La rotomotetia che manda A in D e B in C, manda M_1 in M_2

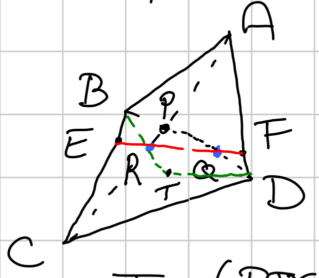
$\Rightarrow M$ è il centro di una rotomotetia che manda A in M_1 e D in M_2

$\Rightarrow \Pi, \Pi_1, \Pi_2, Q$ conciclici. Inoltre $O\Pi_1\Pi_2 Q$ conciclici

$\Rightarrow O\Pi, \Pi_1, \Pi_2, Q$ conciclici

OQ è diametro $\Rightarrow \widehat{O\Pi Q} = \frac{\pi}{2}$. ▨

IMO 2005 – 5 $ABCD$ convesso, $BC = DA$ ma non parallele
E su BC, F su DA t.c. $BE = DF$.
$AC \cap BD = P$ $BD \cap EF = Q$, $EF \cap AC = R$
Dim che (PQR) passa per un punto fisso al variare di E, F come detto.



Claim: Il punto fisso è T ($\neq P$) centro della rotomotetia che manda AC in BD

$T = (BPC) \cap (APD)$ e diverso da P

T è anche centro della rotomotetia che manda CB in AD

Voglio dim $TPRQ$ ciclico!

$\sphericalangle TAD = \sphericalangle TCB$
$\sphericalangle TDA = \sphericalangle TBC$

$BC = AD$
$\Downarrow$
(BPC) e (APD) sono congruenti

$\Rightarrow$ la rotomotetia che manda BC in AD è una rotazione!!

$TB = TD$
$TA = TC$

$BE = DF$

$\Rightarrow \triangle TBE \cong \triangle TDF$
$\Downarrow$
$TE = TF$
$\sphericalangle BTE = \sphericalangle DTF$

$\Rightarrow$ rotomotetia di centro T che manda D in F e B in E

$\Rightarrow T$ pt. di Miquel di DF, BE, EF, BD

$\Rightarrow B, T, Q, E$ conciclici

$\Rightarrow T \in (BQE)$

$T \in (BPC)$

Considero le rette BP, PR, RE, EB

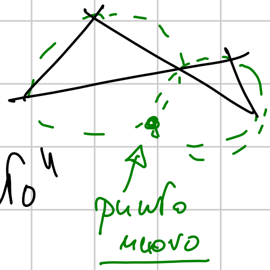
$BP \cap RE = Q$

$PR \cap EB = C$

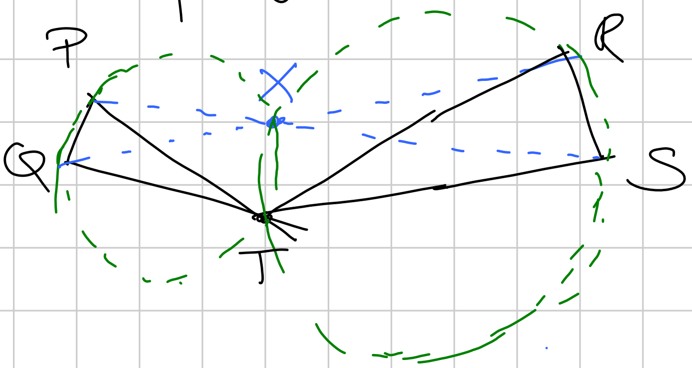
$\Rightarrow T$ pt di Miquel

$\Rightarrow T \in (PQR)$. ■

Idea 1: Usare Miquel / centro di SS per "produrre un nuovo punto"

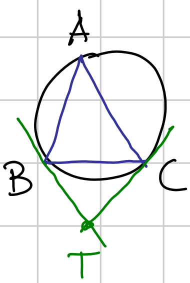


Idea 2: Trovare "cose rotomotetiche" per dimostrare ciclicità



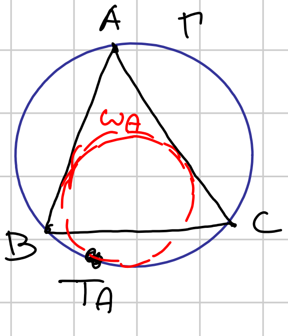
Inversione + simmetria

Es 1:



Dim che AT è simmediana

Es 2:



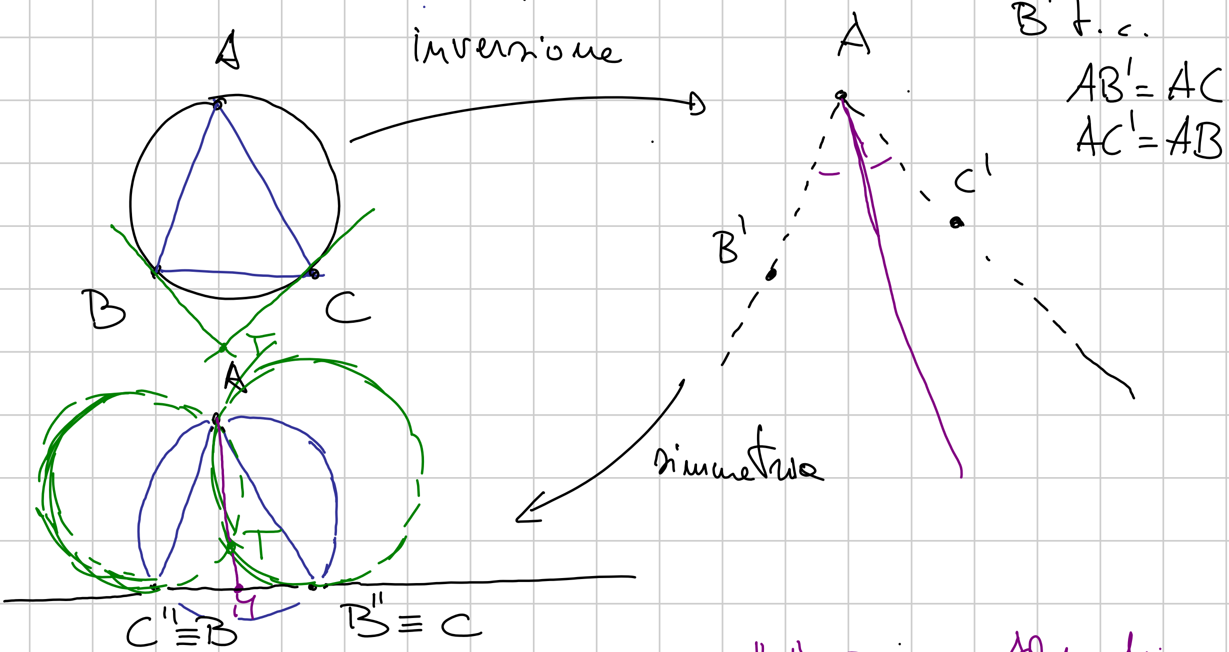
ω_A tangente a AC, AB, Γ (internamente)

ω_B, ω_C simili

⇒ AT_A, BT_B, CT_C concorrono nel coniugato isogonale del punto di Nagel.

Tecnica: Inversione in A di raggio $\sqrt{AB \cdot AC}$ + simmetria rispetto alla bisettrice.

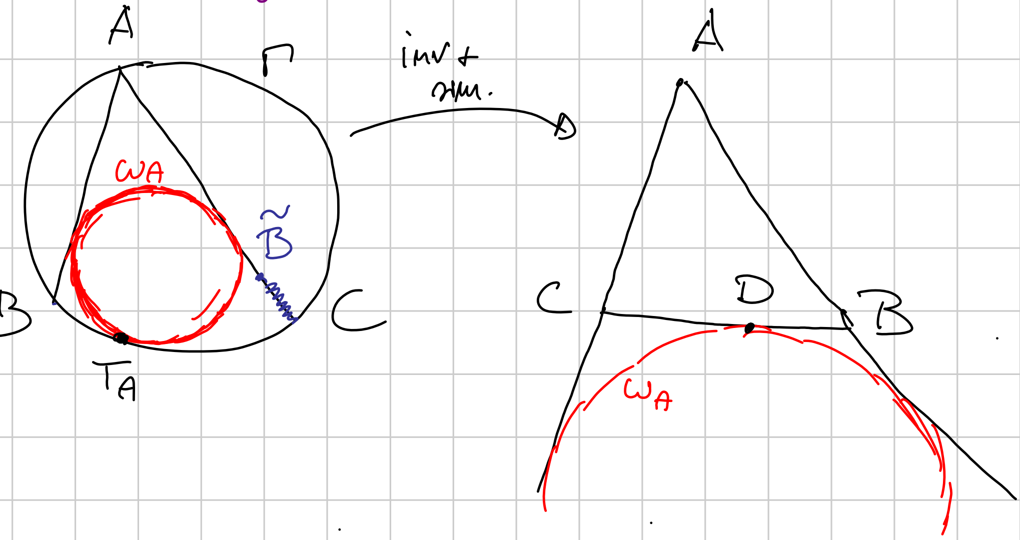
(I) Applico la trasformazione



AT'' asse radicale ⇒ biseca $B''C'' = BC$ ⇒ AT'' mediana

è l'immagine di AT ⇒ sono simmetriche nella bisettrice.

(II)



$\Longrightarrow$ AT_A è simmetrica di AD risp. alla bisettrice in A

$\Longrightarrow$ AT_A, BT_B, CT_C si intersecano nel coniug. isog. del pt. di Nagel.

inscritta

<u>Oss</u>: A = centro di simil. esterno tra ω e ω_A

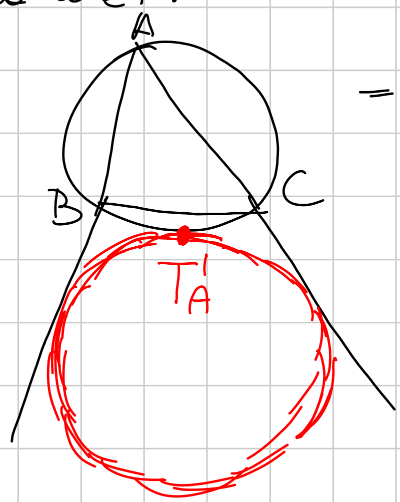
T_A = " " " esterno tra ω_A e Γ

$\Downarrow$

AT_A contiene il centro di simil. esterno tra ω e Γ

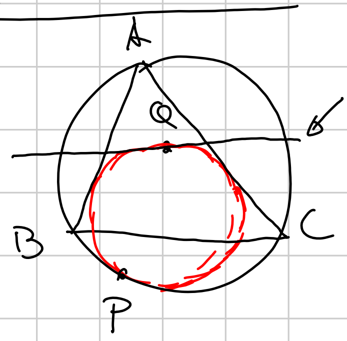
$\Longrightarrow$ AT_A, BT_B, CT_C concorrono nel centro di simil. esterno tra ω e Γ.

<u>Per casa</u>:



$\Longrightarrow$ AT'_A BT'_B CT'_C concorrono nel centro di simil interno tra ω e Γ, coniugato isogonale del punto di Gergonne.

<u>EGMO 2013 - 5</u>



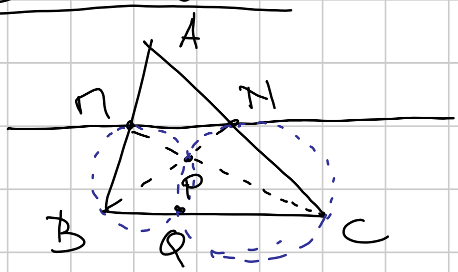
parallela a BC

$\Longrightarrow$ $B\hat{A}P = Q\hat{A}C$

<u>Dim</u>: AP è simm. di AD con D tangenza dell'exscritto opposto ad A.

Per omotetia in A, A, Q, D allineati. ∎

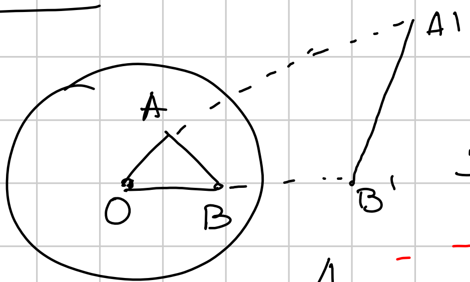
BMO 2009 – 2



$\Rightarrow \widehat{BAQ} = \widehat{CAP}$

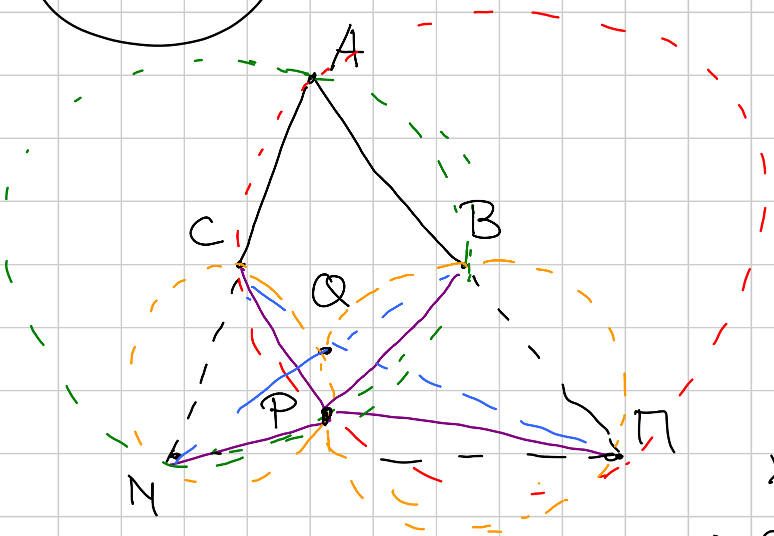
Sol 1: $Q \in (ABN)$
$Q \in (AMC)$ etc...

Sol 2: inv $\sqrt{bc}$ + simmetria



$OAB \sim OB'A'$

+ simmetria $\Rightarrow OAB \sim OA'B'$



P = seconda intersez tra (ABN) e (ACM)

$\Rightarrow$ è il pt di Miquel di BM, CN, BN, CM

$X = BN \cap CM$

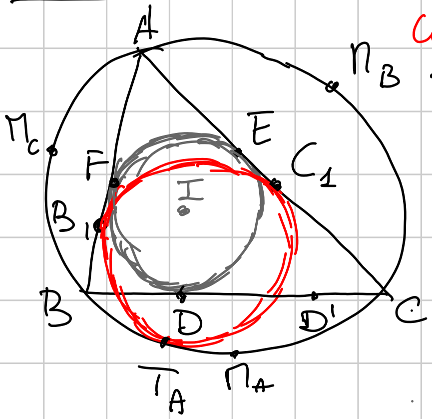
$\Rightarrow P \in (BXM)$
$P \in (CXN)$

$\Rightarrow X = (BPM) \cap (CPN)$ oltre P

$\Rightarrow$ AP e AQ simmetriche.
(la config. finale e quella iniziale sono omotetiche)

Alternativa: AP è mediana (Ceva)
$\Rightarrow$ devo dim che AQ è simmediana

Roba Mistilinea



ω_A - incerchio mistilineo opposto A
Γ - circoscritta
ω - inscritta
I - incentro

AT_A, AD' simmetriche in AM_A

0) T_A, B_1, M_C allineati. ✓
T_A, C_1, M_B allineati

1) B_1, I, C_1 sono allineati

$B_1 = AB \cap M_C T_A$
$C_1 = AC \cap M_B T_A$
$I = BM_B \cap CM_C$

Pascal su
$T_A M_B B A C M_C$ (inscritto in Γ)
$\Downarrow$
B_1, I, C_1 allineati.

2) $B_1 I = I C_1$ (AB_1C_1 isoscele $\Rightarrow$ bisettrice = mediana)

3) raggio di ω_A (ci basta calcolare AB_1)

inversione + simmetria manda B_1 nel punto in cui la A-exinscritta tocca AB (sia B_2)
AB_2 è noto
$$\Rightarrow \quad AB_1 = \frac{AB \cdot AC}{AB_2}$$

$$r_A = \frac{r}{\cos^2 \frac{\alpha}{2}}$$

4) $T_A I$ biseca $\widehat{BT_AC}$ (per casa)

5) BC, B_1C_1, $T_A M_A$ concorrono.

Pascal su $BCM_CT_AM_AA \Rightarrow BC \cap T_AM_A$, $\overbrace{CM_C \cap M_AA}^{I}$, $\overbrace{M_CT_A \cap AB}^{B_1}$

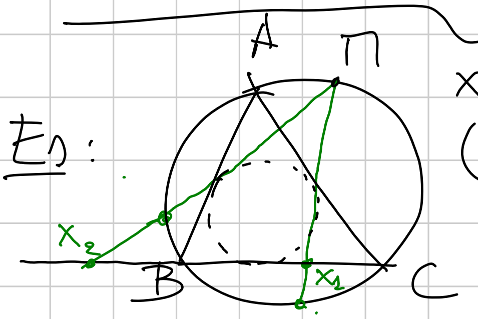
$\Rightarrow$ ok.

6) BB_1IT_A, CC_1IT_A ciclici

7) T_AA simmediana in $T_AB_1C_1 \Rightarrow T_AI \cap \Gamma = \{T_A, M_A\}$

M_A = diam. opposto a Π_A

Es:



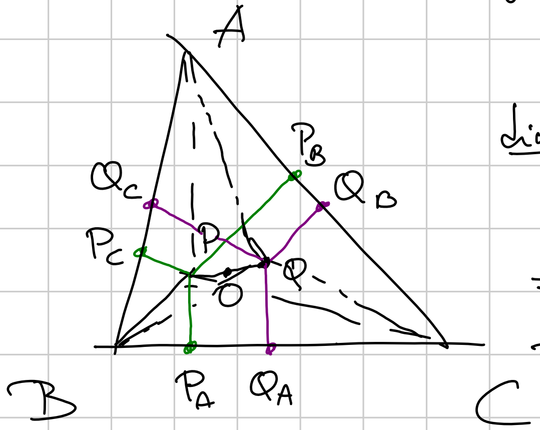
X_1, X_2 = intersez. delle tg da Π a ω con BC

(ΠX_1X_2) incontra Γ in Π e T

$\Rightarrow T$ è T_A

(TST Taiwan 2014)

Extra: P, Q coniugati isogonali $\Rightarrow$ i tri. pedali di P e Q hanno la stessa circoscritta.



dim

$$BP_C \cdot BQ_C = BP \cdot \cos P\hat{B}P_C \cdot BQ \cdot \cos Q\hat{B}Q_C = BP \cdot \cos Q\hat{B}Q_A \cdot BQ \cdot \cos P\hat{B}P_A = BP_A \cdot BQ_A$$

e così $P_AP_CQ_AQ_C$ conciclici.

Asse rad tra $(P_AP_CQ_AQ_C)$ e $(P_AP_BQ_AQ_B)$ è BC e gli altri due sono AC e BA. Assurdo, a meno che le 3 circonf. non coincidano.

N1 medium

Jack, DarkCrystal

Titolo nota 04/09/2018

- Somme di 2 e 4 quadrati
- Problema del cerchio di Gauss
- Ciclotomia, φ, esistenza $g: \langle g \rangle = G$
- $\left(\frac{\cdot}{p}\right)$ e casi elementari di $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$

Cauchy-Schwarz $\quad (a^2+b^2)(c^2+d^2) \geq (ac+bd)^2$

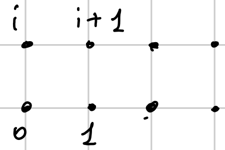
Id. Lagrange $\quad (a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2$

$\mathbb{Z}[i]$ anello degli interi di Gauss

$N(a+bi) = (a+bi)(a-bi) = a^2+b^2 \qquad a+bi = z$

$N(z) = z \cdot \bar{z}$

$\mathbb{Z}[i] = \{(a+bi) : a, b \in \mathbb{Z}\}$



$z = a+bi \qquad w = c-di \qquad N(z \cdot w) = N(z) \cdot N(w)$

$z \cdot w = (ac+bd) - i(ad-bc)$

Id. Lagrange in più variabili

$$\sum_{k=1}^{n} a_k^2 \cdot \sum_{k=1}^{n} b_k^2 = \underbrace{\left(\sum_{k=1}^{n} a_k b_k\right)^2}_{\langle \cdot, \cdot \rangle^2} + \overbrace{\underbrace{\sum_{1 \leq j < k \leq n} (a_j b_k - a_k b_j)^2}_{|v \times w|^2}}^{CS \longleftrightarrow \geq 0}$$

$A = \{\square + \square\}$ è un semigruppo : $a \in A,\ b \in A \longrightarrow ab \in A$

Quali interi si scrivono come a^2+b^2 ?

– se $n \equiv 3\ (4)$, $n \notin \{\square+\square\}$ $\qquad m^2 \pmod 4 \in \{0,1\}$

– $n = 21 = 0^2 + \sqrt{21}^2$

$1^2 + \sqrt{20}^2$

$2^2 + \sqrt{17}^2$

$3^2 + \sqrt{12}^2$

Quali primi si scrivono come a^2+b^2 ?

di certo non quelli della forma $4k+3$,

2 sì, $2 = 1^2+1^2$ e

(Conj) $\forall p \equiv 1\ (4)\ \exists a,b : p = a^2+b^2$

[(Atto di fede) $\forall p \equiv 1\ (4)$ -1 è residuo quadratico (mod p),

ossia $\exists m \in \mathbb{Z} : m^2+1 \equiv 0 \pmod p$]

Metodo di discesa di Fermat

$p = 101 = 10^2+1^2$

$a^2+b^2 = kp \iff a^2+b^2 \equiv 0 \pmod p$ $\qquad$ atto di fede

$0 < a,b < \frac{p}{2}$ $\quad \underline{k < \frac{p}{2}}$ $\qquad \Updownarrow$

$(ab^{-1})^2 + 1 \equiv 0 \pmod p$

$x^2 \equiv (-x)^2 \mod p$

riduciamo a e b (mod k) ottenendo a_1 e b_1

$a_1^2 + b_1^2 = kq$

$$(\underbrace{aa_1+bb_1}_{\equiv 0\,(k)})^2 + (\underbrace{ab_1-ba_1}_{\equiv 0\,(k)})^2 = k^2pq$$

$$\left(\frac{aa_1+bb_1}{k}\right)^2 + \left(\frac{ab_1-ba_1}{k}\right)^2 = pq \qquad q<k$$

reiterando l'argomento, $p \in A$.

$p \equiv 1\ (4) \longrightarrow p = a^2 + b^2$ rappresentazione "unica"

a meno di $a \longleftrightarrow b$

$a \longleftrightarrow -a$

$b \longleftrightarrow -b$

Se tutti i primi $p \mid n$ sono della forma $4k+1$,

$n \in A$

$r_2(n) = \left| \left\{ (a,b) \in \mathbb{Z}^2 : a^2 + b^2 = n \right\} \right|$

$$r_2(n) = 4 \cdot \underset{\tau(n)}{d(n)}$$

$25 = 5 \cdot 5$ $\quad 5 = 1^2 + 2^2$ $\quad 5 = 1^2 + 2^2$ $\quad 25 =$

$0^2 + 5^2$

$5^2 + 0^2$

$3^2 + 4^2$ $\quad (-3)^2 + 4^2$ $\quad - - \quad + -$

$4^2 + 3^2$ $\quad (-4)^2 + (3)^2$ $\quad - - \quad + -$

$0^2 + (-5)^2$

$(-5)^2 + 0^2$

Se $p \equiv 3\ (4)$ divide n con molteplicità dispari

$\nu_p(n) \equiv 1\ (2)$

$\nu_p(n) = \max \{ m \in \mathbb{N} : p^m \mid n \}$

allora $n \notin A$

Se $p \equiv 3\ (4)$ divide n con molteplicità pari

e tutti gli altri divisori primi di n

sono $\equiv 1\ (4)$, allora $n \in A$

$\forall\ n = a^2 + b^2, \quad a, b \equiv 0 \pmod p$

$n \in A \longrightarrow 2n \in A$ $\qquad \underset{n \equiv 0\ (2)}{n \in A} \longrightarrow \frac{n}{2} \in A$

$$(a-b)^2 + (a+b)^2 = 2(a^2 + b^2)$$

Gli elementi di A sono tutti e soli gli interi per cui $p \equiv 3\,(4),\ p \mid n \longrightarrow \nu_p(n) \equiv 0\,(2)$

$$r_2(n) = 4\,(\chi_4 * 1)(n) = 4 \sum_{d \mid n} \chi_4(d)$$

convoluzione di Dirichlet

$$\chi_4(m) \begin{cases} 1 & m \equiv 1\,(4) \\ -1 & m \equiv -1\,(4) \\ 0 & m \text{ pari} \end{cases}$$

$r_2(n)$ è <u>un multiplo di una funzione moltiplicativa</u>.

$\mathbb{Z}[i]$ è euclideo $\longrightarrow$ $\mathbb{Z}[i]$ è UFD

$$n = (a+bi)(a-bi)$$

---

in $\mathbb{Z}[i]$ i primi sono i primi di $\mathbb{Z}$ della forma $4k+3$ e gli elementi $\pm a \pm bi$ dove $a^2+b^2 = p \equiv 1\,(4)$

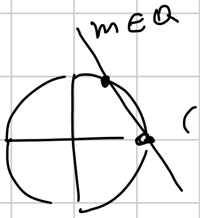
$1, -1, i, -i$

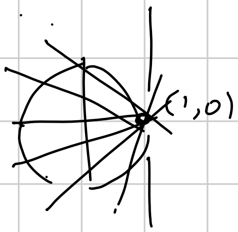
$B = \{\square + 2\cdot\square\}$ investigazione lasciata al lettore.

Formule parametriche $\longleftrightarrow$ Struttura delle terne pitagoriche primitive

$a^2+b^2 = c^2 \qquad \gcd(a,b)=1$

$\left(\frac{a}{c}\right)^2+\left(\frac{b}{c}\right)^2 = 1$





$$\begin{cases} y = m(x-1) \\ x^2 + y^2 = 1 \end{cases} \qquad m \in \mathbb{Q}$$

$x^2 + m^2(x-1)^2 = 1$

$x = 1$ è sicuramente sol di

$\forall (x,y) \in S^1$ (⇑ $\mathbb{Q}^2$) $\qquad \underbrace{x = \frac{1-t^2}{1+t^2} \quad y = \frac{2t}{1+t^2}}$ per $t \in \mathbb{Q}$

se $a^2 + b^2 = c^2$ e $\gcd(a,b) = 1$ allora

$a = 2pq \quad b = p^2 - q^2 \quad c = p^2 + q^2$ → caso $n=4$ FLT

$\gcd(p,q) = 1$, $p + q \equiv 1\ (2)$

$$\bar{d}(A) = \limsup_{n \to +\infty} \frac{|[1,n] \cap A|}{n}$$

$$|A \cap [1,n]| \leq \frac{C_0 n}{\sqrt{\log n}}$$

$A \quad A$ densità 0

$A + A$ densità 1

$B = \{ \square + \square + \square + \square \}$

oss. 1 è un semigruppo per la norma su $\mathbb{H}$

$\mathbb{C} = \mathbb{R}[x]/(x^2+1)$

$1 \quad i \quad j \quad k$

$a + bi + cj + dk$

$(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2) = \square + \square + \square + \square$

$B = \mathbb{N}$ $\qquad r_4(n) = |\{(a,b,c,d) \in \mathbb{Z}^4 : a^2+b^2+c^2+d^2 = n\}|$

$$r_4(n) = 8 \sum_{\substack{d \mid n \\ d \not\equiv 0\,(4)}} d$$

$\exists\, u, v : \quad u^2+v^2 \equiv -1 \ (p)$ (Chevalley)

$$(a+ib)-(c+id)(u+iv)$$

con $a^2+b^2+c^2+d^2 \leq R^2$

$$a = a_1 - a_2 \qquad b = b_1 - b_2$$

Teorema di Minkowski per i corpi convessi e simmetrici.

Prodotto triplo di Jacobi $\xrightarrow{\partial/\partial x}$ serie di Lambert

$$\underbrace{\sum_{n\in\mathbb{Z}} z^{n^2}}_{\Theta(z)} = \prod_{m\geq 1} (\quad)(\quad)(\quad)$$

$$r_2(n) = [z^n]\ \Theta(z)^2 \qquad r_4(n) = [z^n]\ \Theta(z)^4$$

Serie di Lambert

$$\sum_{m\geq 1} \frac{x^m}{1-x^m} = \sum_{m\geq 1}\sum_{k\geq 1} x^{mk}$$

$$= \sum_{n\geq 1} x^n\, d(n)$$

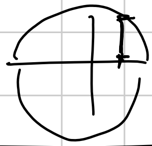
$$\sum_{n\geq 0} \frac{(-1)^n\, d(2n+1)}{2n+1} = \frac{\pi^2}{16}$$ Esercizio

Hint: cos'è $\chi_4 * \chi_4(n) = \sum_{d|n} \chi_4(d)\,\chi_4\!\left(\frac{n}{d}\right)$?

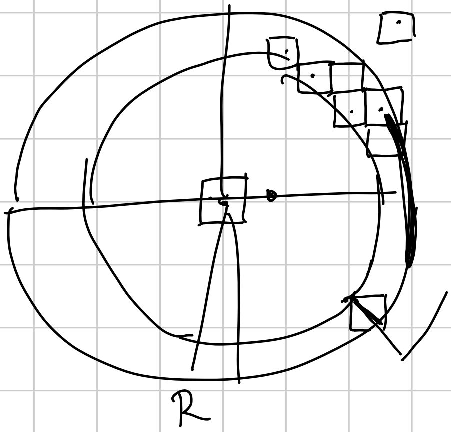
Cosa ci dice l'algebra delle serie di Dirichlet ?

Quanti elementi di $\mathbb{Z}\times\mathbb{Z}$ soddisfano $x^2+y^2 \leq R^2$?

$$2\sum_{z=-R}^{R} \left\lfloor \sqrt{R^2-z^2} \right\rfloor + 2R-1$$



$$1 + \sum_{m=1}^{R^2} r_2(m)$$



$$\pi(R-\sqrt{2})^2 \leq \ldots \leq \pi(R+\sqrt{2})^2$$

$$\pi R^2 + E(r)$$

$$|E(r)| \leq k \cdot r$$

Teorema del cerchio di Gauss

l'ordine medio di r_2 è π

Voronoi $\quad \pi R^2 + E(r)$

$$|E(r)| \leq k \cdot r^{2/3}$$

Struttura delle f. di Bessel

$$\lim_{x\to 1^-} \sqrt{1-x} \sum_{n=0}^{+\infty} x^{n^2} = \frac{\sqrt{\pi}}{2}$$

$$\frac{\theta(x)-1}{2} \sim \frac{1}{2}\sqrt{\frac{\pi}{1-x}} \quad \text{per } x \to 1^-$$

formula di sommazione di Poisson

$$\left(\sum_{n\geq 0} x^{n^k}\right)^k \sim \frac{\Gamma\left(1+\frac{1}{k}\right)^k}{1-x} \quad \text{per } x \to 1^-$$

(Hardy 192x)

Ciclotomia: $\Phi_n(x)$ è il poly. min. su $\mathbb{Q}$ di $\exp\left(\frac{2\pi i}{n}\right)$

$\Phi_n(x)$ è monico e a coeff. interi.

$\deg \Phi_n = \varphi(n)$

φ è moltiplicativa e $\varphi(p^k) = (p-1)\,p^{k-1}$

$\varphi(n) = \left|\mathbb{Z}/_{n\mathbb{Z}}^{*}\right|$ $\qquad \left.\begin{array}{c}\mathbb{Z}/_{n\mathbb{Z}}^{*} \times \mathbb{Z}/_{m\mathbb{Z}}^{*} \simeq \mathbb{Z}/_{nm\mathbb{Z}}^{*} \\ \gcd(n,m)=1\end{array}\right\}$ TC R

$$\varphi(n) \cdot \varphi(m) = \varphi(nm)$$

$$\left|\mathbb{Z}/_{p^k\mathbb{Z}}^{*}\right| = p^k - p^{k-1} = p^{k-1}(p-1)$$

$\mathbb{Z}/_{p\mathbb{Z}}^{*}$ è ciclico, ossia $\exists\, g \in \mathbb{Z}/_{p\mathbb{Z}}^{*} : \langle g \rangle = \mathbb{Z}/_{p\mathbb{Z}}^{*}$

$p=7 \quad \mathbb{Z}/_{7\mathbb{Z}}^{*} = \{\overset{NO}{1}, \overset{NO}{2}, 3, \overset{NO}{4}, 5, \overset{NO}{6}\}$ $\qquad |\langle g \rangle| = o(g)$ è un divisore di $|G|$

$\langle 1 \rangle = \{1\}$

$\langle 2 \rangle = \{1,2,4\}$

$\langle 3 \rangle = \{1,3,2,6,4,5\}$

$\langle 4 \rangle = \{1,4,2\}$ $\qquad \langle 5 \rangle = \{1,5,4,6,3,2\}$

$$\langle g \rangle = G \iff \langle g^{-1} \rangle = G$$

se $|G|$ è pari e $h = g^2$ allora $\langle h \rangle \neq G$

Preso $m = p-1 = \left|\mathbb{Z}/_{p\mathbb{Z}}^{*}\right| = q_1^{\alpha_1} \cdot \ldots \cdot q_k^{\alpha_k}$

$g \in \mathbb{Z}/_{p\mathbb{Z}}^{*}$ è generatore se e solo se

$$g^{\frac{p-1}{q_j}} \not\equiv 1 \pmod p \quad \forall j \in [1,k]$$

In $\mathbb{Z}/_{p\mathbb{Z}}^{*}$ ci sono $\varphi(\varphi(p)) = \varphi(p-1)$ generatori

$(\mathbb{Z}/p\mathbb{Z}, +)$ $\quad (\mathbb{Z}/p\mathbb{Z}^*, \cdot)$ $\quad \mathbb{F}_p$ campo finito con p elementi

$x^m - 1$ ha $\leq m$ radici in $\mathbb{F}_p$

$x^2 - 1$ ha ≤ 2 radici in $\mathbb{F}_p$

$x^3 - 1$ ha ≤ 3 radici in $\mathbb{F}_p$

$x^{p-1} - 1$ = prodotto di poly ciclotomici

$\deg \Phi_m = \varphi(m)$

$\Phi * 1 = \mathrm{Id}$ $\qquad \underbrace{\sum_{d|n} \varphi(d)}_{\text{f. molt.}} = n$

$$\sum_{d|p^k} \varphi(d) = \sum_{j=0}^{k} \varphi(p^j) = 1 + \underbrace{\sum_{j=1}^{k} (p-1)p^{j-1}}_{\text{telescopica}} = p^k$$

$\mathbb{Z}/p\mathbb{Z}^*$ c'è un generatore $\longrightarrow$ $\mathbb{Z}/p^k\mathbb{Z}^*$ c'è un generatore

p dispari

$\mathbb{Z}/2\mathbb{Z}^*$ $\quad \mathbb{Z}/4\mathbb{Z}^*$

$\mathbb{Z}/2^m\mathbb{Z}^* \overset{m \geq 3}{=} \{\pm 5^a\}$

Sollevamento henseliano.

---

www.matemate.it $\longrightarrow$ Appunti

$\downarrow$

Tarento

- dispense Jack
- dispense Pete Clark

COMPLEMENTI SUI RESIDUI QUADRATICI

Simbolo di Legendre modulo p primo

n e' residuo quadratico mod p

$\iff$ $x^2 \equiv n$ mod p si risolve

Def
$$\left(\frac{n}{p}\right) = \begin{cases} +1 & \text{se } n \text{ e' R.Q. mod } p \\ -1 & \text{se non lo e'} \\ 0 & \text{se } p \mid n \end{cases}$$

$$\#\left\{\text{quadrati} \neq 0 \ (p)\right\} = \frac{p-1}{2}$$

$$x \longmapsto x^2$$

e' 2-a-1 da $\left(\mathbb{Z}/p\mathbb{Z}\right)^* \longrightarrow \left(\mathbb{Z}/p\mathbb{Z}\right)^*$

$$p-1 \longmapsto \frac{p-1}{2}$$

Criterio di Eulero

$$\left(\frac{n}{p}\right) = +1 \iff n^{\frac{p-1}{2}} \equiv 1 \mod p$$

$$\left(\frac{n}{p}\right) \equiv \underbrace{n^{\frac{p-1}{2}}}_{} \pmod p$$

Sempre ± 1 : il suo quadrato
e' $n^{p-1} \equiv 1 \pmod p$

Se n è un quadrato, $n \equiv a^2 \bmod p$,

$$n^{\frac{p-1}{2}} \equiv (a^2)^{\frac{p-1}{2}} \equiv a^{p-1} \equiv 1 \ (p)$$

L'equazione $X^{\frac{p-1}{2}} \equiv 1 \bmod p$

ha $\leq \frac{p-1}{2}$ soluzioni (grado)

$\geq \frac{p-1}{2}$ soluzioni ($\square$)

Se prendo n non RQ, $n^{\frac{p-1}{2}}$ non

può fare 1 (altrimenti avrei

$> \frac{p-1}{2}$ soluzioni di $X^{\frac{p-1}{2}} \equiv 1$),

e quindi è $\equiv -1 \pmod p$

Cor -1 è RQ mod $p \iff p \equiv 1 \ (4)$
(o $p = 2$)

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & p \equiv 1 \ (4) \\ -1 & p \equiv 3 \ (4) \end{cases}$$

Cor. 2 $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

$$(ab)^{\frac{p-1}{2}} \equiv (a)^{\frac{p-1}{2}} (b)^{\frac{p-1}{2}} \mod p$$

Conseguenza $(x^2-2)(x^2-3)(x^2-6) \equiv 0 \ (p)$

ha soluzione $\forall p$

Se $\left(\frac{2}{p}\right) = +1$ OK

Se $\left(\frac{3}{p}\right) = +1$ OK

Altrimenti $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1$, e quindi

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)(-1) = +1$$

Simile x^4+1 si fattorizza modulo ogni primo

è riducibile

Reciprocità quadratica

$$\left(\frac{28}{32003}\right) = \left(\frac{2}{32003}\right)\left(\frac{14}{32003}\right).$$

$$= \left(\frac{2}{32003}\right)^2 \left(\frac{7}{32003}\right)$$

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \qquad p, q \text{ dispari}$$

$$= \begin{cases} \left(\frac{q}{p}\right) & \text{se } p \equiv 1\ (4) \text{ o } q \equiv 1\ (4) \\ -\left(\frac{q}{p}\right) & \text{se } p \equiv q \equiv 3\ (4) \end{cases}$$

Es $\left(\frac{7}{32003}\right) = -1 \cdot \left(\frac{32003}{7}\right)$

$$= (-1) \cdot \left(\frac{-1}{7}\right) = +1$$

E $p = 2$? $\qquad \left(\frac{2}{p}\right) = +1 \iff p \equiv \pm 1\ (8)$

Caso speciale

$$\left(\frac{-3}{p}\right) = +1 \iff \left(\frac{p}{3}\right) = +1$$

$$\Updownarrow$$

$$p \equiv 1 \ (3)$$

L'equazione $x^3 \equiv 1 \pmod p$ ha

$$\begin{cases} \text{① } 1 \quad \text{soluzione} \quad \text{se } p \equiv 2 \ (3) \\ \text{② } 3 \quad \text{soluzioni} \quad \text{se } p \equiv 1 \ (3) \end{cases}$$

① $x^3 \equiv 1 \ (p)$ $\quad \operatorname{ord}_p(x) = 1$ ~~o 3~~

$\operatorname{ord}_p(x) \mid p-1$

② Le tre soluzioni sono $x \equiv 1$, $x \equiv g^{\frac{p-1}{3}}$, $x \equiv g^{\frac{p-1}{3}\cdot 2}$ con g generatore

$$x^3 - 1 = (x-1)\underbrace{(x^2+x+1)}_{\text{0 o 2 radici}}$$

$p \equiv 2$ o $p \equiv 1 \ (3)$

$$x \equiv \frac{-1 \pm \sqrt{-3}}{2} \pmod{p}$$

$x^2 + x + 1 \equiv 0 \mod p$ ha delle soluzioni

$$\Longleftrightarrow \quad \left(\frac{-3}{p}\right) = +1 \quad \Longleftrightarrow \quad p \equiv 1 \ (3)$$

$$\left(\frac{2}{p}\right) \qquad (1+i)^2 = 2i$$

$$\Rightarrow \quad 2 = \frac{(1+i)^2}{i}$$

$$\left(\frac{2}{p}\right) \equiv \left(\frac{(1+i)^2}{i}\right)^{\frac{p-1}{2}} \equiv \frac{(1+i)^{p-1}}{i^{\frac{p-1}{2}}}$$

$$\equiv \frac{(1+i)^p}{(1+i)\, i^{\frac{p-1}{2}}} \equiv \frac{1 + i^p}{(1+i)\, i^{\frac{p-1}{2}}} \pmod{p}$$

ESERCIZI

① Contare il numero di soluzioni di

$$x^2 + y^2 \equiv 1 \pmod p$$

Supponiamo $p \equiv 1 \mod 4$ e sia (con notazione ovvia) $i \in \mathbb{Z}$ t.c. $i^2 \equiv -1 \ (p)$

$$(x+iy)(x-iy) \equiv 1 \mod p$$

L'eqz $u \cdot v \equiv 1 \mod p$ ha $p-1$ soluzioni; quella sopra anche: $\begin{cases} x+iy = u \\ x-iy = v \end{cases}$ $\begin{cases} x = \frac{u+v}{2} \\ y = \frac{u-v}{2i} \end{cases}$

Supponiamo invece $p \equiv 3 \mod 4$.

$$x^2 + y^2 \equiv 1 \pmod p$$

$y \equiv 0 \longrightarrow 2$ soluzioni

$y \not\equiv 0 \ (p)$ $\left(\frac{x}{y}\right)^2 + 1 \equiv \left(\frac{1}{y}\right)^2 \mod p$

$$1 \equiv \left(1/y\right)^2 - \left(x/y\right)^2 \mod p$$

$$\equiv u^2 - v^2 \equiv (u+v)(u-v)$$

$$\equiv A \cdot B \ (p)$$

$p-1$ soluzioni

CONCLUSIONE: se $p \equiv 3\ (4)$ ci sono $p+1$ soluz.

soluzioni di $x^2 \equiv n \mod p$ è

$$1 + \left(\frac{n}{p}\right)$$

Soluz di $x^2+y^2 \equiv 1 \ (\mathrm{mod}\ p)$

$$= \sum_{x=0}^{p-1} \left(\#\ \text{soluz di } y^2 \equiv 1-x^2\ (p)\right)$$

$$= \sum_{x=0}^{p-1} \left(1 + \left(\frac{1-x^2}{p}\right)\right)$$

$$\equiv \sum_{x=0}^{p-1} \left(1 + (1-x^2)^{\frac{p-1}{2}}\right) \mod p$$

$$\equiv \sum_{x=0}^{p-1} \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} (-x^2)^j \mod p$$

PARENTESI: SOMME DI POLINOMI MOD p

$$\sum_{x=0}^{p-1} x \equiv 0 \quad (p) \qquad p>2$$

$$\sum_{x=0}^{p-1} x^2 \equiv \frac{(p-1)p(2p-1)}{6} \equiv 0 \, (p) \qquad p>3$$

$$\sum_{x=0}^{p-1} x^{p-1} \equiv -1 \quad (p)$$

LEMMA IMPORTANTE Sia $f(x)$ un polinomio di grado d. Se $p-1>d$, allora
$$\sum_{x=0}^{p-1} f(x) \equiv 0 \pmod p$$

DIM Basta farlo per i monomi, $f(x) = a \cdot x^d$, anzi, $f(x) = x^d$

$$\sum_{x=0}^{p-1} x^d \equiv \sum_{x=1}^{p-1} x^d$$

$d>0$

$$\equiv \sum_{k=0}^{p-2} \left(g^k\right)^d$$

$d<p-1$
$(p-1 \nmid d)$

$$\equiv \frac{\left(g^d\right)^{p-1}-1}{g^d-1} \equiv 0 \ (p)$$

$\square$

$$\equiv \sum_{x=0}^{p-1} \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} (-x^2)^j \mod p$$

$$\equiv \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} \underbrace{\left(\sum_{x=0}^{p-1} (-x^2)^j \right)}_{\text{di grado } < p-1 \text{ tranne che per } j = \frac{p-1}{2}}$$

$$\equiv \binom{(p-1)/2}{(p-1)/2} \cdot (-1)^{\frac{p-1}{2}} \sum_{x=0}^{p-1} x^{p-1}$$

$$\equiv (-1)^{\frac{p-1}{2}} \cdot (-1) \pmod{p}$$

$$\# \text{ Soluzioni } \begin{cases} \equiv -(-1)^{\frac{p-1}{2}} \ (p) \\ 0 < \cdot < 2p \end{cases}$$

$\#$ Soluz : $\cancel{1}$, $p-1$, $p+1$, $\cancel{2p-1}$

$\#$ Soluz è pari : se c'è (x,y) c'è $(-x,-y)$

$$\# \text{ soluz } = p - \left(\frac{-1}{p}\right)$$

Cor (del conto) $\#$ Soluz di

$$x^2 + y^2 \equiv a \pmod{p}$$

è sempre $p - \left(\frac{-1}{p}\right)$ (se $a \neq 0$)

IMO SL 2010 N3

Trovare il minimo n per cui esistono polinomi a coefficienti razionali $f_1(x), \dots, f_n(x)$ t.c.

$$f_1(x)^2 + \dots + f_n(x)^2 = x^2+7$$

$\boxed{n=8}$ $f_1(x) = x$, $f_i(x) = 1$ $i = 2, \dots, 8$

$\boxed{n=5}$ $(x)^2 + (2)^2 + (1)^2 + (1)^2 + (1)^2$

$\deg f_i(x) \leq 1$

$f_i(x) = a_i x + b_i$ $\quad a_i, b_i \in \mathbb{Q}$

$$(a_1 x + b_1)^2 + \dots + (a_4 x + b_4)^2 = x^2 + 7$$

$$\begin{cases} a_1^2 + a_2^2 + a_3^2 + a_4^2 = 1 & \|a\|^2 = 1 \\ a_1 b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4 = 0 & a \perp b \\ b_1^2 + \dots + b_4^2 = 7 & \|b\|^2 = 7 \end{cases}$$

MIRACOLO

$$7 = (a_1^2 + \dots + a_4^2)(b_1^2 + \dots + b_4^2) =$$

$$= (a_1 b_1 + a_2 b_2 + \dots + a_4 b_4)^2 + (\quad)^2 + (\quad)^2 + (\quad)^2$$

$$= \frac{A^2}{D^2} + \frac{B^2}{D^2} + \frac{C^2}{D^2} \qquad A, B, C, D \text{ interi}$$

$A^2 + B^2 + C^2 = 7D^2$: la guardo mod 8.

Se D e' dispari trovo $A^2 + B^2 + C^2 \equiv 7\ (8)$, che non si risolve. Quindi D e' pari.

$\Rightarrow A^2 + B^2 + C^2 \equiv 0 \mod 4$

$\Rightarrow A, B, C$ tutti pari

Per discesa infinita non ci sono soluzioni (tranne $A = B = C = D = 0$, che pero' non da' soluzioni del problema iniziale).

Esercizio

Determinare tutti i k interi positivi tali che

$$k+1 \mid 2^k + 1$$

2^k+1 è dispari! Quindi k è pari

$k = 2k_1 \qquad 2k_1+1 \mid 2^{2k_1}+1$

Tutti i fattori primi di $2^{2k_1}+1$ sono $\equiv 1 \ (4)$:

se $p \equiv 3 \ (4)$ dividesse $2^{2k_1}+1$, si avrebbe

$$-1 \equiv (2^{k_1})^2 \mod p, \text{ assurdo}$$

Quindi $2k_1+1 \equiv 1 \ (4) \Rightarrow k_1 = 2k_2$

$$4k_2+1 \mid 2^{4k_2}+1.$$

Sia p un divisore primo di $2^{4k_2}+1$.

$$2^{4k_2} \equiv -1 \ (p) \Rightarrow 2^{8k_2} \equiv 1 \ (p)$$

$$\mathrm{ord}_p(2) \mid p-1$$

$$\mathrm{ord}_p(2) \mid 8k_2 \qquad \mathrm{ord}_p(2) \nmid 4k_2$$

q^h : se $q \neq 2$ OK per entrambe

le divisibilità

$$\Longrightarrow \ 8 \mid \mathrm{ord}_p(2) \mid p-1 \ \Longrightarrow \ p \equiv 1 \ (8)$$

E ora per induzione: $k = 2^r \cdot k_r$

$$2^r k_r + 1 \ \Big| \ 2^{2^r k_r} + 1$$

Voglio dim che k_r è pari $\Longleftrightarrow$ $2^r k_r + 1 \equiv 1$ mod 2^{r+1}. Basta vedere che tutti i divisori primi di $2^{2^r k_r} + 1$ sono $\equiv 1$ mod 2^{r+1}

$$2^{2^r k_r} \equiv -1 \ (p) \quad \& \quad 2^{2^{r+1} k_r} \equiv 1 \ (p)$$

$$\Longrightarrow \ \mathrm{ord}_p(2) \equiv 0 \ \text{mod } 2^{r+1}, \text{ fine.}$$

Stage Senior 2018 N2 Medium

Titolo nota 06/09/2018

- Ballo

ARGOMENTI:

- VALUTAZIONI p-ADICHE E LTE;
- DISCESA INFINITA E VIÉTA JUMPING;
- APPROSSIMAZIONE DIOFANTEA ED EQUAZIONI DI PELL;
- (SE C'È TEMPO...) STIME.

VALUTAZIONI p-ADICHE

SE $n \in \mathbb{Z}$, $n \neq 0$ ESISTE UN UNICO MODO DI SCRIVERE n COME PRODOTTO DI PRIMI, A MENO DEL SEGNO:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \cdot (-1)^{\delta} \qquad \delta \in \{0, 1\}$$

GLI p_i E α_i SONO UNIVOCAMENTE DETERMINATI.

LA $v_p(n)$ (VALUTAZIONE p-ADICA DI n) È L'ESPONENTE CON CUI p COMPARE NELLA FATTORIZZAZIONE DI n.

$v_{p_1}(n) = \alpha_1$, $v_{p_2}(n) = \alpha_2, \ldots$

$v_3(18) = 2$ PERCHÉ $18 = 2 \cdot 3^2$.

COME CALCOLARE $v_p(n!)$?

$1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$

1: QUANTI MULTIPLI DI p CI SONO TRA 1 ED n?

$$\left\lfloor \frac{n}{p} \right\rfloor$$

2: QUANTI MULTIPLI DI p^2 CI SONO TRA 1 ED n?

$$\left\lfloor \frac{n}{p^2} \right\rfloor$$

...

I MULTIPLI DI p CONTRIBUISCONO DI UN FATTORE 1.

I MULTIPLI DI p^2 CONTRIBUISCONO DI UN FATTORE 2.

$$v_p(n!) = \cancel{\sum_{i=1}^{+\infty} i \cdot \left\lfloor \frac{n}{p^i} \right\rfloor}$$

No!

$p = 2 \qquad n = 5 \qquad v_2(120) = 3$

$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$

$2^1 \quad 2 \quad 4 \to 1 \cdot 2$

$2^2 \quad 4 \to 2 \cdot 1$

$$\boxed{v_p(n!) = \sum_{i=1}^{+\infty} \left\lfloor \frac{n}{p^i} \right\rfloor} \quad \checkmark$$

PERCHÉ QUANDO CONSIDERO I MULTIPLI DI p^2 (CHE VALGONO 2) LI HO GIÀ CONSIDERATI UNA VOLTA TRA I MULTIPLI DI p.

FACCIAMO UNA STIMA!

$$v_p(n!) < C_{p,n}$$

$$\sum_{i=1}^{+\infty} \left\lfloor \frac{n}{p^i} \right\rfloor < C_{p,n}$$

STIMA BRUTALE: $\lfloor x \rfloor \leq x$ (PER DEFINIZIONE)

$$\sum_{i=1}^{+\infty} \left\lfloor \frac{n}{p^i} \right\rfloor \leq \sum_{i=1}^{+\infty} \frac{n}{p^i} = n \sum_{i=1}^{+\infty} \frac{1}{p^i}$$

$$\sum_{i=0}^{+\infty} \frac{1}{p^i} = \frac{p}{p-1} \qquad \left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots = \frac{1}{1-\frac{1}{p}} \right)$$

SPENDIAMOCI UNA PAROLA:

$$1 + x + x^2 + x^3 + \ldots = L$$

$$xL = x + x^2 + x^3 + x^4 + \ldots$$

$$L - xL = 1 \rightarrow L = \frac{1}{1-x}$$

IN REALTÀ CI SONO DEI PROBLEMI DI CONVERGENZA

SE $x = 2$

$$1 + 2 + 2^2 + 2^3 + \ldots = \frac{1}{1-2} = -1 \quad ?????$$

PERÒ SE $-1 < x < 1$ TUTTO FILA LISCIO

$$n\sum_{i=1}^{+\infty}\frac{1}{p^i}=n\left(\sum_{i=0}^{+\infty}\frac{1}{p^i}\cdot p^{-1}\right)=\frac{n}{p-1}$$

$$\sum_{i=0}^{+\infty}\frac{1}{p^i}\to\frac{p}{p-1}$$

ABBIAMO

$$v_p(n!)\leq\frac{n}{p-1}$$

$$\leq\;\sum_{i=1}^{+\infty}\left\lfloor\frac{n}{p^i}\right\rfloor\leq\sum_{i=1}^{+\infty}\frac{n}{p^i}$$

VA BENE IL $<$

PERCHÉ SE $p^i>n$: $\left\lfloor\frac{n}{p^i}\right\rfloor=0$

MA $\frac{n}{p^i}>0$ E VISTO CHE DI $p^i>n$

NE HO (E NE HO PURE TANTI), POTEVAMO

METTERE IL $<$

$$v_p(n!) = \sum_{i=1}^{+\infty} \left\lfloor \frac{n}{p^i} \right\rfloor < \frac{n}{p-1}$$

ESERCIZIO PER CASA

TROVARE GLI n E I p t.c.

$$v_p(n!) = \frac{n-1}{p-1}$$

LTE

LIFTING THE EXPONENT

SIA n UN INTERO POSITIVO >1 E SIANO a E b INTERI TALI CHE $a > |b| > 0$. SIA p UN NUMERO PRIMO TALE CHE:

- $p \mid a-b$, $p \nmid a$, $p \nmid b$;
- SE $p=2$, $4 \mid a-b$ (SE $p=2$, $n \geq 2$)

($a > 0$, MA b PUÒ ANCHE ESSERE NEGATIVO)

Th. $v_p(a^n - b^n) = v_p(n) + v_p(a-b)$

DIM.: CHIAMIAMO $\alpha = v_p(a-b)$

$a = b + K \cdot p^{\alpha}$ CON $(K,p)=1$

(I.E. SE $p | K \Rightarrow v_p(a-b) > \alpha$)

$v_p(a^n - b^n)$: $a^n - b^n =$

$(b + Kp^{\alpha})^n - b^n =$

$\sum_{i=0}^{n} (Kp^{\alpha})^i \cdot b^{n-i} \cdot \binom{n}{i} - b^n =$

LEVA $i=0$

$= \sum_{i=1}^{n} (Kp^{\alpha})^i \cdot b^{n-i} \binom{n}{i} =$

ISOLIAMO $i = n$ E $i = 1$

$$= (Kp^w)^n + \sum_{i=2}^{n-1} (Kp^w)^i \cdot b^{n-i} \cdot \binom{n}{i} +$$

$$Kp^w \cdot b^{n-1} \cdot n$$

$v_p > v_p$

$v_p(a) > v_p(b)$

$\to v_p(a+b) = v_p(b)$

GUARDIAMO LA v_p:

- $i=1$: $v_p(\cancel{K} \cdot p^w \cdot \cancel{b^{n-1}} \cdot n) =$

$$w + v_p(n)$$

- $i=n$: $v_p((\cancel{K}p^w)^n) = nw$

CI VERREBBE DA DIRE CHE:

$$nw > w + v_p(n)$$

$$\Updownarrow$$

$$(n-1)w > v_p(n)$$

SE USASSIMO SOLO $v_p(n) < n$, ALLORA CON $w=1$ È $v_p(n) = n-1$ SAREMMO FREGATI.

$$\boxed{v_p(n) \leq \log_p n}$$

$$\log_p n = \log_p J + v_p(n)$$

$$n = J \cdot p^{v_p(n)}$$

VORREMO:

$$(n-1)k > \log_p n$$

$$\Updownarrow$$

$$p^{(n-1)\cdot k} > n$$

- $p=2$: $\boxed{p^{(n-1)k} \geq 2^{(n-1)k}}$ $\boxed{2^b \geq b+1}$

$$2^{(n-1)k} \overset{?}{>} n$$

$(1+1)^b = 1+b+\cancel{\binom{b}{2}}+\dots$

$$2^{(n-1)k} \geq 1+(n-1)k \overset{?}{>} n$$

$$\Updownarrow$$

$$k>1$$

(VEDI HP. $4 \mid (a-b)$)

- $p \geq 3$: $p^{(n-1)k} \geq 3^{(n-1)k}$

$$3^{(n-1)k} \overset{?}{>} n$$

$$\text{IV}$$

$$3^{n-1} > n \quad \forall n \geq 2$$

n	3^{n-1}
2	3
3	9
4	27
...	

QUINDI:

- $i=1$: $\quad v_p = k + v_p(n)$

$$\wedge$$

- $i=n$: $\quad v_p = kn$

- $2 \le i \le n-1$: $\quad v_p\left(\binom{n}{i} \cdot (\cancel{1} \cdot p^k)^i \cdot \cancel{1}^{n-i}\right) =$

$$v_p(p^{ki}) + v_p\left(\binom{n}{i}\right) = ik + v_p\left(\binom{n}{i}\right)$$

COME STIMARE DAL BASSO $v_p\left(\binom{n}{i}\right)$?

IO VORREI DIMOSTRARE CHE:

$$ik + v_p\left(\binom{n}{i}\right) > k + v_p(n)$$

$$\binom{n}{i} = \frac{n!}{(n-i)!} \cdot \frac{1}{i!} \qquad 2 \le i \le n-1$$

$$v_p\left(\frac{n!}{(n-i)!}\right) = v_p(n \cdot (n-1) \cdot \ldots \cdot (n-i+1))$$

$$\ge v_p(n)$$

$$v_p\left(\frac{n!}{(n-i)!}\right) \geq v_p(n)$$

$$v_p\left(\frac{1}{i!}\right) > \text{TOT}$$

$$\Updownarrow$$

$$v_p(i!) < \text{TOT}_2$$

MA CE L'ABBIAMO!

$$v_p(i!) < \frac{i}{p-1}$$

$$v_p\left(\binom{n}{i}\right) = v_p\left(\frac{n!}{(n-i)!}\right) + v_p\left(\frac{1}{i!}\right) =$$

$$= v_p\left(\frac{n!}{(n-i)!}\right) - v_p(i!) > v_p(n) - \frac{i}{p-1}$$

È IMPLICATA DA:

$$iw + v_p\left(\binom{n}{i}\right) > iw + \cancel{v_p}(n) - \frac{i}{p-1} \overset{?}{\geq} w + \cancel{v_p}(n)$$

CI RESTA:

$$w(i-1) \geq \frac{i}{p-1}$$

$$k(p-1)(i-1) \geq i \qquad \forall\, n-1 \geq i \geq 2$$

$$\Updownarrow$$

$$k(p-1) \geq \frac{i}{i-1}$$

- $2 \geq \dfrac{i}{i-1}$ PERCHÉ $i \geq 2$
- $k(p-1) \geq 2$ — $p=2 \rightarrow k \geq 2$ (CFR. $4 \mid a-b$); $p \geq 3$ ✓

$$v_p(a^n - b^n) = v_p\left(\ \right) = v_p = k + v_p(n)$$

$$= v_p(a-b) + v_p(n)$$

$\square$

LEMMA DEL GUADAGNO DI UN PRIMO

SIA a, b INTERI COPRIMI t.c.
$a > |b| > 0$ E n UN INTERO POSITIVO DISPARI > 1
$\exists\, p$ PRIMO t.c. $p \mid a^n - b^n$ MA
$p \nmid a - b$
(A PARTE UN'ECCEZIONE...)

$$\begin{cases} a = 2 \\ b = -1 \\ n = 3 \\ a - b = 3 \\ a^3 - b^3 = 9 \end{cases}$$

SUPPONIAMO PER ASSURDO CHE $\forall p$ t.c.
$p \mid a^n - b^n \rightarrow p \mid a - b$

- $p = 2$: a E b SONO ENTRAMBI DISPARI

$$v_2(a^n - b^n) = v_2(a - b)$$

$$\underbrace{\frac{a^n - b^n}{a - b}}_{\text{DISPARI}} = \overbrace{a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + ab^{n-2} + b^{n-1}}^{n \text{ ADDENDI DISPARI}}$$

$\longrightarrow$ DISPARI

• $p \geq 3$: $\quad v_p(a^n - b^n) = v_p(n) + v_p(a-b)$

$| a^n - b^n$

QUINDI $\forall p$ ABBIAMO:

$$v_p(a^n - b^n) = v_p(n) + v_p(a-b)$$

• $p \mid a-b$, $p \nmid a^n - b^n$ IMPOSSIBILE PERCHÉ $a-b \mid a^n - b^n$

• $p \mid a-b$, $p \mid a^n - b^n$ VERO PER LTE E PER $p=2$ VERO PER

• $p \nmid a-b$, $p \mid a^n - b^n$ È LA TESI (QUINDI CONTRO L'IPOTESI DI ASSURDO)

PER OGNI $p \mid a^n - b^n$ ABBIAMO

$$v_p(a^n - b^n) = v_p(n) + v_p(a-b) = v_p(n(a-b))$$

VORREMMO $a^n - b^n = n(a-b)$, MA NON È DETTO! PERCHÉ POTREBBE ESISTERE q PRIMO t.c. $q \nmid a-b$, $q \nmid a^n - b^n$ ma $q \mid n$. È PER QUESTO CHE HO SALTATO $\bullet$ $p \nmid a-b$, $p \nmid a^n - b^n$

(I.E.: $a=2$, $b=1$, $n=3$,

$a^3 - b^3 = 7$, $a-b=1$ ma $v_3(7) \neq v_3(3) + v_3(1)$)

Se ho x, y t.c. $\forall p \mid x$

$v_p(x) \leq v_p(y) \longleftrightarrow x \mid y$

$$a^n - b^n \mid n(a-b)$$

$$\Downarrow$$

$$a^n - b^n \leq n(a-b)$$

$$\Downarrow$$

$$\frac{a^n - b^n}{a-b} \leq n \qquad n = 2k+1, \quad k \geq 1$$

$$\frac{a^{2k+1} - b^{2k+1}}{a-b} \overset{?}{\leq} 2k+1$$

$$a^{2k} + a^{2k-1}b + \ldots + ab^{2k-1} + b^{2k} \overset{?}{\leq} 2k+1$$

(COSA VORREMMO FARE:

$a^{2k} \geq 1$, $\cancel{a^{2k-1}b \geq 1}$, ..., $b^{2k} \geq 1$ HO $2k+1$ TERMINI, QUINDI DEVONO ESSERE TUTTI 1)

b PUÒ ESSERE NEGATIVO!

$$(a+b) \cdot a \cdot (\underbrace{a^{2k-2}}_{\geq 1} + \underbrace{a^{2k-4}b^2}_{\geq 1} + \ldots + \underbrace{a^2b^{2k-4}}_{\geq 1} + \underbrace{b^{2k-2}}_{\geq 1}) + b^{2k} \overset{?}{\leq} 2k+1$$

$b^{2k} \geq 1$

$(a+b) \geq 1$

$a \geq 2$

$a^{2k-2} + \ldots + b^{2k-2} \geq k$

DEVONO ESSERE UGUAGLIANZE

$$2k+1 \geq \underbrace{(a+b)}_{\geq 1} \cdot \underbrace{a}_{\geq 2} \underbrace{(a^{2k} + \ldots + b^{2k})}_{\geq k} + \underbrace{b^{2k}}_{\geq 1} \geq 2k+1$$

$a = 2$

$a+b = 1$

$\Rightarrow a = 2, \; b = -1$

$$2^{2k-2} + \ldots + 1 = k$$

$$\sum_{i=0}^{k-1} 4^i = k \longrightarrow 4+1+\sum_{i=2}^{k-1} 4^i \to \geq k+3$$

$$\geq k-2 \quad \text{SE } k \geq 2$$

$k=1 \to n = 2k+1 = 3$

$$(2,-1,3)$$

$2-(-1)=3 \qquad 2^3-(-1)^3=9 \quad \checkmark$

ECCEZIONE!

ESERCIZIO

ESISTONO INFINITI INTERI POSITIVI n t.c.

$$n^2 \mid 3^n + 2^n$$

$n=1$ FUNZIONA $\quad 1^2 \mid 3^1+2^1 = 5$

$n=5$ FUNZIONA $\quad 5^2 \mid 3^5+2^5 = 275 = 11 \cdot 5^2$

PROVIAMO $n = 275$ $\quad$ LTE: $a=3$, $b=-2$

$$v_5(3^{275}+2^{275}) = v_5(3+2)+v_5(275) = 3$$

MA $v_5(275^2) = 4$!

$$v_{11}\left(3^{275}+2^{275}\right) = v_{11}\left(\left(3^5\right)^{55} - \left(-2^5\right)^{55}\right) =$$

$a = 3^5$ $\quad b = -2^5$

$n = 55$

$$= v_{11}\left(3^5+2^5\right) + v_{11}(55) = 2$$

$v_5(55^2) = 2$

$v_{11}(55^2) = 2$

VEDIAMO CON $n=55$:

$$v_5\left(2^{55}+3^{55}\right) = v_5(5) + v_5(55) = 2 \quad ✓$$

$$v_{11}\left(3^{55}+2^{55}\right) = v_{11}\left(3^5+2^5\right) + v_{11}(11) = 2 \quad ✓$$

$n = 1 \quad \rightarrow \quad 2^1 + 3^1 = 5$

$n = 5 \quad \rightarrow \quad 2^5 + 3^5 = 5^2 \cdot 11$

$n = 5 \cdot 11 \quad \rightarrow \quad 2^{55} + 3^{55} = \ldots$ BOH

COSTRUIAMO UNA SUCCESSIONE $(a_n)_{n\geq 0}$ DI INTERI POSITIVI T.C. $a_0 = 1$ E DI NUMERI PRIMI $(p_n)_{n\geq 1}$ T.C.:

- $a_n^2 \mid 3^{a_n} + 2^{a_n}$;
- $p_n \mid 3^{a_{n-1}} + 2^{a_{n-1}}$;
- $a_n = p_n \cdot a_{n-1}$;
- VORREMMO $p_n \nmid a_{n-1}$;

$\oplus$ $\left(a_n \mid 3^{a_{n-1}} + 2^{a_{n-1}} \right)$ CONDIZIONE PIÙ FORTE

PASSO BASE: $\underset{n=0}{1^2 \mid 3^1 + 2^1}$, $\underset{n=1}{5^2 \mid 3^5 + 2^5}$

PASSO INDUTTIVO: ABBIAMO LA SEQUENZA CHE RISPETTA LE IPOTESI FINO A n

$a_0, \dots, a_n$ E $p_1, \dots, p_n$

VOGLIAMO p_{n+1} CHE:

1 — $p_{n+1} \nmid a_n$;

2 — $p_{n+1} \mid 3^{a_n} + 2^{a_n}$;

— $a_{n+1} = p_{n+1} \cdot a_n$ (DEFINIZIONE DI a_{n+1});

3 — $a_{n+1}^2 \mid 3^{a_{n+1}} + 2^{a_{n+1}}$.

LA 1 E LA 2 CI DEFINISCONO p_{n+1} (SE ESISTE)

IO VOGLIO UN PRIMO CHE DIVIDA $3^{a_n} + 2^{a_n}$, MA NON DIVIDA a_n.

VORREMMO CHE $a_n \mid 3^{a_{n-1}} + 2^{a_{n-1}}$.

SE $a_n \mid 3^{a_{n-1}} + 2^{a_{n-1}}$, HO AUTOMATICAMENTE UN PRIMO $p_{n+1} \mid 3^{a_n} + 2^{a_n}$ MA NON $3^{a_{n-1}} + 2^{a_{n-1}}$ (LEMMA DEL GUADAGNO DI UN PRIMO, POICHÉ $a_{n-1} \mid a_n$, $a_{n-1} < a_n$) E

QUINDI $p_{n+1} \nmid a_n \mid 3^{a_{n-1}} + 2^{a_{n-1}}$

LE NOSTRE IPOTESI SONO:

1. $a_{n+1} = p_{n+1} a_n$;
2. $a_{n+1}^2 \mid 3^{a_{n+1}} + 2^{a_{n+1}}$;
3. $a_{n+1} \mid 3^{a_n} + 2^{a_n}$; (PER IP. INDUTTIVA) $\rightarrow p_{n+1} \nmid a_n$
4. $p_{n+1} \mid 3^{a_n} + 2^{a_n}$;
5. $p_{n+1} \nmid 3^{a_{n-1}} + 2^{a_{n-1}}$.

LA SEQUENZA ESISTE FINO AD a_n E p_n.

SCELGO p_{n+1} (5) $\nmid 3^{a_{n-1}} + 2^{a_{n-1}}$ MA

DIVIDA 3^{a_n} (4) $+ 2^{a_n}$ PER IL LEMMA SEC

GUADAGNO DI UN PRIMO E PONGO

$a_{n+1} = p_{n+1} a_n$. (1)

RESTANO (2) E (3):

$a_{n+1} \mid 3^{a_n} + 2^{a_n}$

$\Updownarrow$

POICHÉ $p_{n+1} \nmid a_n$:

$a_n \mid 3^{a_n} + 2^{a_n}$ E $p_{n+1} \mid 3^{a_n} + 2^{a_n}$ ✓ (3) ✓

PERCHÉ $a_n \mid 3^{a_{n-1}} + 2^{a_{n-1}} \mid 3^{a_n} + 2^{a_n}$

$$a_{n+1}^2 \mid 3^{a_{n+1}} + 2^{a_{n+1}}$$

(2) ✓

$$\Updownarrow$$

$a_n^2 \mid 3^{a_{n+1}} + 2^{a_{n+1}}$ VERO PERCHÉ

E $\qquad a_n^2 \mid 3^{a_n} + 2^{a_n} \mid 3^{a_{n+1}} + 2^{a_{n+1}}$

$$p_{n+1}^2 \mid 3^{a_{n+1}} + 2^{a_{n+1}}$$

$$v_{p_{n+1}}\left(3^{a_{n+1}} + 2^{a_{n+1}}\right) = \underbrace{v_{p_{n+1}}\left(3^{a_n} + 2^{a_n}\right)}_{\geq 1} + \underbrace{v_{p_{n+1}}(p_{n+1})}_{= 1}$$

PERCHÉ $p_{n+1} \mid 3^{a_n} + 2^{a_n}$

DISCESA INFINITA

O, VOLGARMENTE, IL PRINCIPIO DEL MINIMO.

RISOLVERE NEGLI INTERI

$$x^3+3y^3=9z^3$$

i) $3 \mid x \to x=3\tilde{x}$

$$27\tilde{x}^3+3y^3=9z^3$$

$$\downarrow$$

$$9\tilde{x}^3+y^3=3z^3$$

ii) $3 \mid y \to y=3\tilde{y}$

$$9\tilde{x}^3+27\tilde{y}^3=3z^3$$

$$\downarrow$$

$$3\tilde{x}^3+9\tilde{y}^3=z^3$$

iii) $3 \mid z \to z=3\tilde{z}$

$$3\tilde{x}^3+9\tilde{y}^3=27\tilde{z}^3$$

$$\downarrow$$

$$\tilde{x}^3+3\tilde{y}^3=9\tilde{z}^3$$

CON
$x=3\tilde{x}$
$y=3\tilde{y}$
$z=3\tilde{z}$

QUALSIASI TERNA PUÒ ESSERE DIVISA PER 3 INFINITE VOLTE. L'UNICA SOLUZIONE È $(0,0,0)$.

USANDO IL PRINCIPIO DEL MINIMO: SIA (a,b,c) UNA SOLUZIONE TALE $(a,b,c) \neq (0,0,0)$ E $a^2+b^2+c^2$ MINIMO (PRINCIPIO DEL MINIMO: OGNI SOTTOINSIEME DI $\mathbb{N}$ HA UN MINIMO).

(a,b,c) SOLUZIONE $\Rightarrow$ $(\tilde{a}, \tilde{b}, \tilde{c})$ SOLUZIONE

CON $\tilde{a}^2+\tilde{b}^2+\tilde{c}^2 = \frac{1}{9}(a^2+b^2+c^2) < a^2+b^2+c^2$

SE $a^2+b^2+c^2 \neq 0$

VIÉTA JUMPING

PROBLEM

DETERMINARE I POSSIBILI VALORI INTERI DI

$$\frac{a^2+b^2+1}{ab}$$

CON a, b INTERI POSITIVI

SOLUZIONE

(a, b, k) LE TERNE DI INTERI POSITIVI t.c.

$$a^2 + b^2 + 1 = kab$$

$$a^2 - (kb)a + b^2 + 1$$

$$p(x) = x^2 - kbx + b^2 + 1$$

RADICI: x_1, x_2 t.c.

$$x_1 + x_2 = kb$$

$$x_1 \cdot x_2 = b^2 + 1$$

a È GIÀ UNA RADICE DI $p(x)$

(x_1, b, k) È SOLUZIONE

$\downarrow$

(x_2, b, k) È SOLUZIONE

$x_1 = a$

$\downarrow$

$x_2 = kb - a$

$\hookrightarrow$ INTERO!!!!!

(a, b, k) SOLUZIONE

$\downarrow$

$(bk - a, b, k)$ SOLUZIONE

(a, b, k) SOLUZIONE $\rightarrow (b, a, k)$ SOLUZIONE

$a > b$: (a, b, k) SOLUZIONE $\quad \dfrac{a^2+b^2+1}{ab} = k$

$(bk-a, b, k)$ SOLUZIONE: LO È PER COME ABBIAMO SCELTO $bk-a$

(SE NON VI FIDATE, FATE IL CONTO)

$$\boxed{\underset{>0}{a}\,(\underset{>0}{bk-a}) = \underset{>0}{b^2+1}}$$

- $bk - a > 0$:

$$\cancel{b} \cdot \frac{a^2+b^2+1}{a\cancel{b}} - a > 0$$
$$\Updownarrow$$
$$b^2+1 > 0 \quad \checkmark$$

- $bk - a < b$: ☺

$$\cancel{b} \cdot \frac{a^2+b^2+1}{a\cancel{b}} < a + b$$
$$\Updownarrow$$
$$a^2+b^2+1 < a^2+ab$$
$$\Updownarrow$$
$$b^2+1 < ab$$

$$\Updownarrow$$

$$1 \times (a-b)\cdot b \qquad a>b>0$$

$$\Updownarrow$$

(LA NEGAZIONE DI $a=2, b=1$) $b \neq 1 \vee a > b+1$

$(a, b, k) \qquad a > b > 0$

$$\downarrow$$

$(b, bk-a, k) \qquad b > bk-a > 0$

A MENO CHE $a=2, b=1$.

CASI RESTANTI:

$\star_1$ $a=b$: $\dfrac{a^2+b^2+1}{ab} = \dfrac{2a^2+1}{a^2} = 2+\dfrac{1}{a^2} \to a=1, b=1, k=3$

$\star_2$ $b=1$: $\dfrac{a^2+2}{a} = a+\dfrac{2}{a} \to a=1, b=1, k=3$; $a=2, b=1, k=3$

VOGLIAMO TROVARE TUTTI I VALORI DI k.

SUPPONIAMO CHE (a, b, k) SIA SOLUZIONE.

SE $a=b \to K=3$. $☆_1$

SE $a \neq b$, POICHÉ (a,b,K) SOL. $\to (b,a,K)$ SOL.

SUPPONIAMO $a>b$.

FISSATO UN CERTO K, SIA $(\tilde{a},\tilde{b},K)$ LA SOLUZIONE CON $\tilde{a}>\tilde{b}>0$ CON $\tilde{a}+\tilde{b}$ MINIMO.

DAL RAGIONAMENTO DI PRIMA:

- $\tilde{b}=1 \to K=3$ $☆_2$
- $\tilde{b}>1 \to (\tilde{b}, K\tilde{b}-\tilde{a}, K)$ È SOLUZIONE

CON $\tilde{b}>K\tilde{b}-\tilde{a}>0$ E CON

$$\tilde{b}+(K\tilde{b}-\tilde{a})<\tilde{a}+\tilde{b}$$

PERCHÉ $\tilde{b}<\tilde{a}$, $K\tilde{b}-\tilde{a}<\tilde{b}$ PER QUANTO VISTO PRIMA.

QUINDI $(\tilde{a},\tilde{b},K)$ <u>NON</u> ERA LA SOLUZIONE CON $\tilde{a}+\tilde{b}$ MINIMALE.

PERCIÒ $K=3$ SEMPRE.

I.E.: $(a,b)=1$ FUNZIONA

$(a_n, a_{n-1}, 3)$ $\qquad a_n > a_{n-1} > 0$

$\downarrow$

$(a_{n-1}, \overbrace{3a_{n-1} - a_n}^{a_{n-2}}, 3)$

$\downarrow$

$(a_{n-2}, \overbrace{3a_{n-2} - a_{n-1}}^{a_{n-3}}, 3)$

$\downarrow \ldots$

$\downarrow$

$(a_1, \underbrace{a_0}_{1}, 3)$

$\downarrow$

2 o 1

(ω) CI DICE CHE (a,b,k) NON PRODUCE $(b, kb-a, k)$ CON $b = kb - a$ A MENO CHE $b=1$; QUINDI PRIMA SI ARRIVA A 1.

$a_{n+2} = 3a_{n+1} - a_n$

$a_0 = 1 \qquad a_1 = 1 \longrightarrow a_2 = 2 \to a_3 = 5$

$a_0 = 1 \qquad a_1 = 2 \longrightarrow a_2 = 5$

IN REALTÀ È UNA SOLA SHIFTATA

$a_0 = 1, \; a_1 = 1, \; a_{n+2} = 3a_{n+1} - a_n$

$$x^2 - 3x + 1 = 0 \rightarrow x_1, x_2 = \frac{3 \pm \sqrt{5}}{2} = \left(\frac{1 \pm \sqrt{5}}{2}\right)^2 = (\varphi_1, \varphi_2)^2$$

MORALE DELLA FAVOLA! LE SOLUZIONI SONO TUTTE E SOLO DELLA FORMA

$$(F_{2n+1}, F_{2n-1}, 3) \text{ CON } n \in \mathbb{N}$$

E F_i L'i-ESIMO NUMERO DI FIBONACCI.

PELL IN PILLS

LE EQUAZIONI DI PELL SONO EQUAZIONI DEL TIPO

$$x^2 - dy^2 = 1$$

CON d FISSATO E NON UN QUADRATO.

(SE $d = t^2 \rightarrow x^2 - t^2y^2 = 1 \Rightarrow$

$(x - ty)(x + ty) = 1 \rightarrow x = 1, y = 0$
$x = -1, y = 0$)

IN GENERALE $x^2 - dy^2 = 1$ SE $d \neq \square$ HA INFINITE SOLUZIONI.

LEMMA DI DIRICHLET

SIA $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ IRRAZIONALE > 0. ALLORA ESISTONO INFINITI INTERI POSITIVI COPRIMI (p, q) t.c.

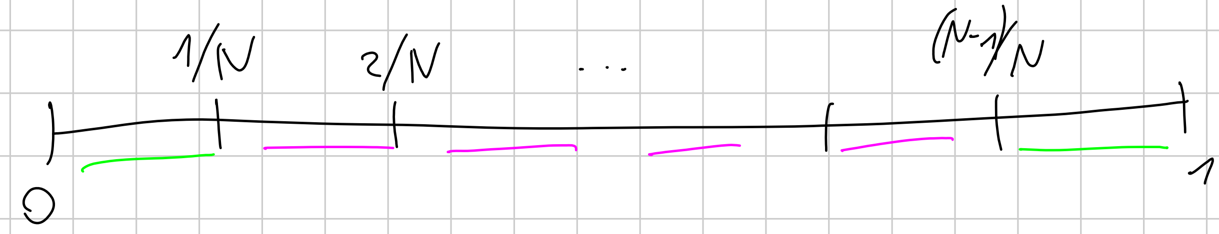
$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}$$

(È UN $\Longleftrightarrow$: SE α È RAZIONALE NE ESISTONO UN NUMERO FINITO).

FISSIAMO UN INTERO POSITIVO N E PRENDIAMO I NUMERI $\alpha, 2\alpha, 3\alpha, \ldots, N\alpha$. PRENDIAMO LE LORO PARTI FRAZIONARIE.

$(\{\pi\} = 0{,}14\ldots)$

LE N PARTI FRAZIONARIE $\{\alpha\}, \{2\alpha\}, \dots, \{N\alpha\}$
SONO IN $(0,1)$



DUE POSSIBILITÀ:

- SE $\exists\, m \le N$ t.c. $\{m\alpha\} \in (0, 1/N)$ o $\in ((N-1)/N, 1)$ $\to \exists\, n$ t.c.
$$|m\alpha - n| < \frac{1}{N}$$
- SE $\nexists\, m \le N$ CON QUELLA PROPRIETÀ, HO N NUMERI $(\{\alpha\}, \dots, \{N\alpha\})$ DISTRIBUITI IN $N-2$ INTERVALLI $\left(\left(\frac{1}{N}, \frac{2}{N}\right), \left(\frac{2}{N}, \frac{3}{N}\right), \dots, \left(\frac{N-2}{N}, \frac{N-1}{N}\right) \right)$

PER PIGEON HOLE $\exists\, a < b \le N$ t.c.
$\{a\alpha\}, \{b\alpha\}$ STANNO NELLO STESSO INTERVALLO.

$$\to \left| \{b\alpha\} - \{a\alpha\} \right| < \frac{1}{N} \to$$

$$\Big| \underbrace{(b-a)}_{\text{INTERO POSITIVO}}\alpha - \left(\lfloor b\alpha \rfloor - \lfloor a\alpha \rfloor \right) \Big| < \frac{1}{N}$$

$\rightarrow \exists \overset{b-a}{\overset{\shortparallel}{c}} \leq N$ d intero t.c. $|ca - d| < \frac{1}{N}$

Unendo i due punti:

$\forall \alpha \in \mathbb{R} \setminus \mathbb{Q}$, $N > 0$, esistono m, n con $m \leq N$ t.c.

$$|m\alpha - n| < \frac{1}{N}$$

- Divido per m: $\left|\alpha - \frac{n}{m}\right| < \frac{1}{Nm} \leq \frac{1}{m^2}$ ✓ Una soluzione

- Per averne infinite, suppongo esistano un numero finito di p_i, q_i funzionanti e prendo N t.c. $\frac{1}{N} < \min |\alpha p_i - q_i|$

Sto facendo il minimo di un # finito di cose > 0 (α è irrazionale)

$\exists\ n, m$ t.c.

$$|m\alpha - n| < \frac{1}{N} < \min |\alpha p_i - q_i|$$

Anche m, n sono funzionanti: Assurdo! $\square$

$$x^2 - dy^2 = 1$$

APPLICHIAMO IL LEMMA DI DIRICHLET
A $\sqrt{d}$

$\exists \infty$ p, q COPRIMI t.c.

$$\boxed{\left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{q^2}}$$

$$(p - \sqrt{d}\cdot q)\,(p + \sqrt{d}\cdot q) = p^2 - d\cdot q^2$$

$\cdot q$

$$|\quad| < \frac{1}{q} \qquad\qquad < \frac{1}{q} + 2\sqrt{d}\cdot q$$

$$p + q\sqrt{d} = (p - q\sqrt{d}) + 2q\sqrt{d} < \frac{1}{q} + 2q\sqrt{d}$$

$\exists \infty$ p, q COPRIMI t.c.

$$|p^2 - q^2 d| < \frac{1}{q}\left(\frac{1}{q} + 2q\sqrt{d}\right) < 2\sqrt{d} + 1$$

$\forall d \neq \square \to \exists \infty$ p, q t.c. $|p^2 - dq^2| < 2\sqrt{d} + 1$

Teoria dei Numeri 2 (Medium) – Francesco Ballini

P - MEDIUM

Titolo nota 02/09/2018

kuzminkirill.math@gmail.com.

Kirill

In un grafo ad albero

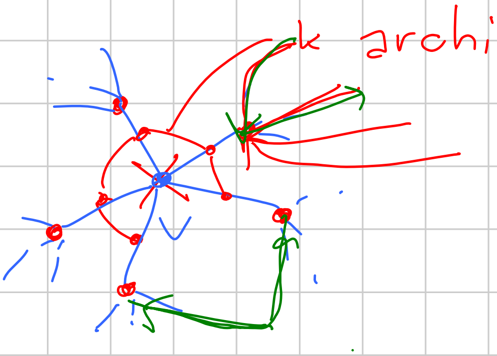
$V = e + 1$

edges

"numero di vertici": quantità su cui indurre

No: partire da struttura piccola ed "accrescere".

Si: partire dal caso "grande" che volete dimostrare, togliere per ricondursi al caso minore per il quale vale l'ipotesi induttiva



No cicli: ok

connessi: ok

disgiunti: ok

k sottografi: sono alberi

Loro: k vertici in più rispetto agli archi

Inoltre avevo: k archi + 1 vertice tolto

Alla fine: 1 vertice in più rispetto agli archi

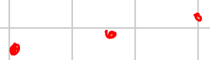
Sylvester – Gallai

Insieme finito con almeno 3 punti nel piano tale che:

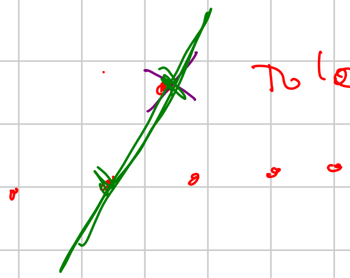
Ogni retta passante per due dei punti passa per il terzo *

Allora sono allineati

Dimostrazione ERRATA:



3 pti: ok



Tolgo un punto cattivo

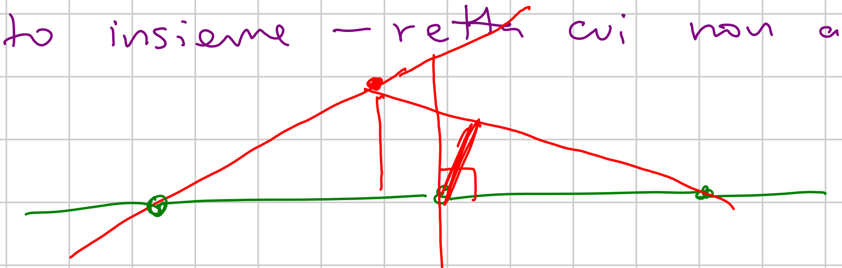
altri allineati per ip induttiva

ERRORE * vale per tutti i punti e non è detto che valga per i sottoinsiemi

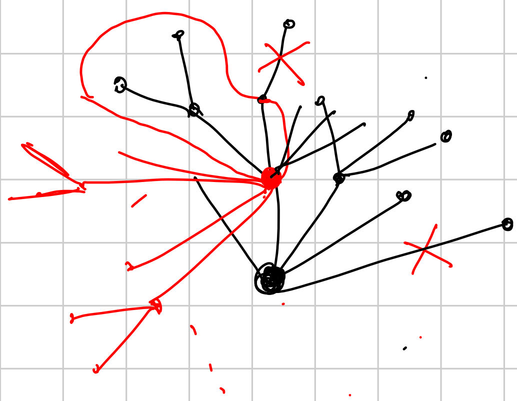
Idea giusta

Prendo le (finite) rette passanti per coppie di punti dell'insieme

Prendo il minimo delle distanze p.to insieme – retta cui non appartiene



Trovata una distanza più piccola; assurdo



Dimostrare che Ercole riesce a battere l'idra in un numero finito di passi;

Sia A un insieme totalmente ordinato

A si dice ben ordinato

se ogni sottoinsieme non vuoto ha minimo

$(\mathbb{N}, <)$ è ben ordinato

$(\mathbb{N}, <)$	Insiemi ben ordinati "generici"
Ogni sottoinsieme non vuoto ha minimo	

Discesa infinita
(non esistono successioni infinite strettamente decrescenti)

Se $P(0)$ e $\forall n$ riuscite, usando come ipotesi $\forall i<n\ P(i)$, a dimostrare $P(n)$, allora P vale per ogni naturale	Se $P(\min A)$ e $\forall a\in A$ riuscite, usando come ipotesi $\forall b<a\ P(b)$, a dimostrare $P(a)$, allora P vale per ogni elemento di A
Induzione classica	Induzione transfinita (NON LA FAREMO)

Esempi: $(\mathbb{N}, <)$ ω

$n = \{0 < 1 < \ldots < n-1\}$

$0 = \emptyset$

A e B ordinati sono isomorfi se $\exists f: A \to B$ biiezione tale che $a_1 < a_2$ se e solo se $f(a_1) < f(a_2)$

A e B insiemi ordinati

$A + B$ è $A \sqcup B$ ← unione disgiunta

Ogni elemento di A è più piccolo di ogni elemento di B

All'interno di A e B preserviamo l'ordine precedente

$A \cdot B$ $\quad A \times B$

(a_1, b_1) $\quad (a_2, b_2)$

se $b_1 < b_2$ allora $(a_1, b_1) < (a_2, b_2)$

se $b_1 > b_2$ ——— $(a_1, b_1) > (a_2, b_2)$

Se $b_1 = b_2$, confronto a_1 con a_2

„antilessicografico"

Associatività: SÌ

$$A + (B + C) = (A + B) + C$$

Commutatività: NO

Se partite da insiemi ben ordinati, ottenete insiemi ben ordinati

$(a_i, b_i)_{i \in I}$ elementi di $\underset{\text{ben ordinati}}{A \cdot B}$

Siccome B è ben ordinato, esiste b_0 minimo tra i possibili b_i

$(a_j, b_0)_{j \in J}$ Siccome A è ben ordinato, $\exists\, a_0$ minimo degli a_j

Quindi (a_0, b_0) è il minimo

$$1 + \omega \neq \omega + 1$$

$$\underbrace{\bullet}_{1} < \underbrace{\bullet < \bullet < \bullet < \bullet < \bullet < \dots}_{\omega} \qquad \underbrace{\bullet < \bullet < \bullet < \dots < \bullet <}_{\omega} < \underbrace{\boxed{\bullet}}_{1}$$

$1 + \omega = \omega$ ha massimo (l'1)

e quindi non è ω

$$A + A = A \cdot 2 \qquad 2 = \{0 < 1\}$$

$$\underbrace{\_0\ \_0\ \_0\ \_0}_{A} \Big| \underbrace{\_1\ \_1\ \_1\ \_1}_{A}$$

$$(a, 0) < (a, 1) \qquad a \in A$$

$$(a, 0) < (b, 1)$$

$$\omega \cdot 2 = \omega + \omega \neq 2 \cdot \omega$$

$$\underbrace{0 < 1 < 2 < \ldots}_{\omega} \Big| \underbrace{0 < 1 < \ldots}_{+\ \omega}$$

$$2 \cdot \omega = \{(0, n), (1, m)\} = \omega$$

$$0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5$$

$$0,0 < 1,0 < 0,1 < 1,1 < 0,2 < 1,2 < 0,3 < 1,3$$

$$(0, n) \longmapsto 2n$$

$$(1, m) \longmapsto 2m + 1$$

$$\omega \cdot 2 = \omega + \omega \neq 2 \cdot \omega = \omega$$

$\omega + \omega$: 0 ha infiniti elementi più piccoli di lui

ω: qui gli elementi più piccoli di un fissato

$\omega \neq \omega+1 \leftarrow$ ha max

$\neq$

$\omega+\omega \leftarrow$ non ha max

Sono sempre finiti

$$A^n = \underbrace{A\cdot A\cdot \ldots A}_{n \text{ volte}}$$

$$1^2+2^2+3^2+\dots+n^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\frac{n(n+1)}{2}\cdot\boxed{\frac{2n+1}{3}}$$

$$\begin{array}{l} 1 \\ 2\ 2 \\ 3\ 3\ 3 \\ \vdots \\ \underbrace{n\ n\ \ldots\ n}_{n} \end{array}$$

$+1$ $\quad$ 0

$$\begin{array}{llll} n & & & \\ \vdots & & & \\ 3 & & & \\ 2 & 3 & & \\ 1 & 2 & 3 & \ldots\ n \end{array} \qquad \begin{array}{llll} & & & n \\ & & & \vdots \\ & & & 3 \\ & & 3 & 2 \\ n\ \ldots & 3 & 2 & 1 \end{array}$$

-1 $\quad$ $+1$ $\quad$ 0 $\quad$ -1

(r,c) $\quad \boxed{c\le r\le n}$

Con ordine lessicografico (confronto partendo da sx)

$\omega\cdot\omega$

Un sottoinsieme di un ben ordinato è ben ordinato

Vogliamo dimostrare, per induzione estesa, P che $\forall (r, c)$ la somma nel posto (r, c) è $2n+1$

$P(1,1)$ è vera $(1+n+n)$

(r, c). Se $c \geq 2$, andiamo a sx $(r, c-1)$

$(r, c-1) < (r, c)$

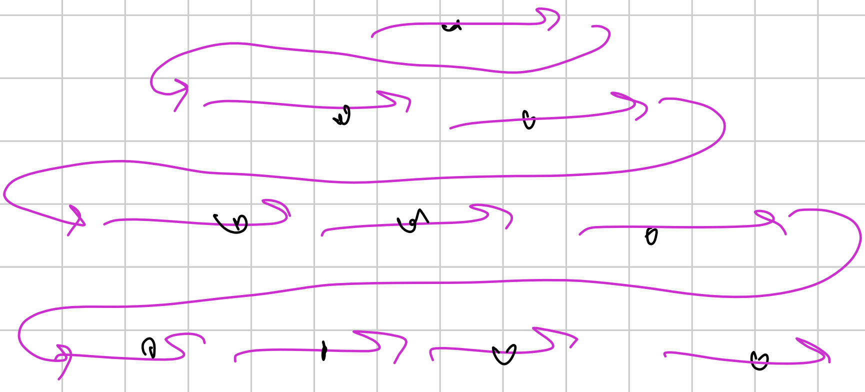
Per ipotesi induttiva, nel posto $(r, c-1)$ la somma è $2n+1$

La variazione della somma passando da $(r, c-1)$ a (r, c) è $0+1-1=0$

Se $c=1$ $(r, 1) > (r-1, 1)$

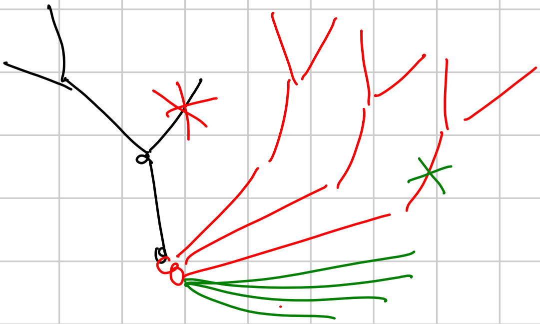
Si conclude analogamente

In realtà questo insieme era $\frac{n(n+1)}{2}$



Idea per l'idra: usare la discesa infinita

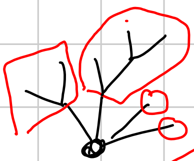
Cosa ci serve: un ordine totale su tutte le possibili idre che sia un buon ordine e tale che un'azione di taglio + ricrescita produca un'idra strettamente più piccola



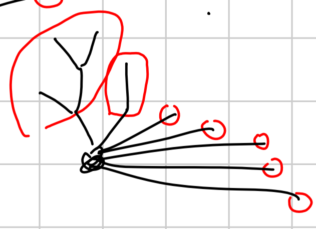
Proviamo a Definire l'ordine per ricorsione

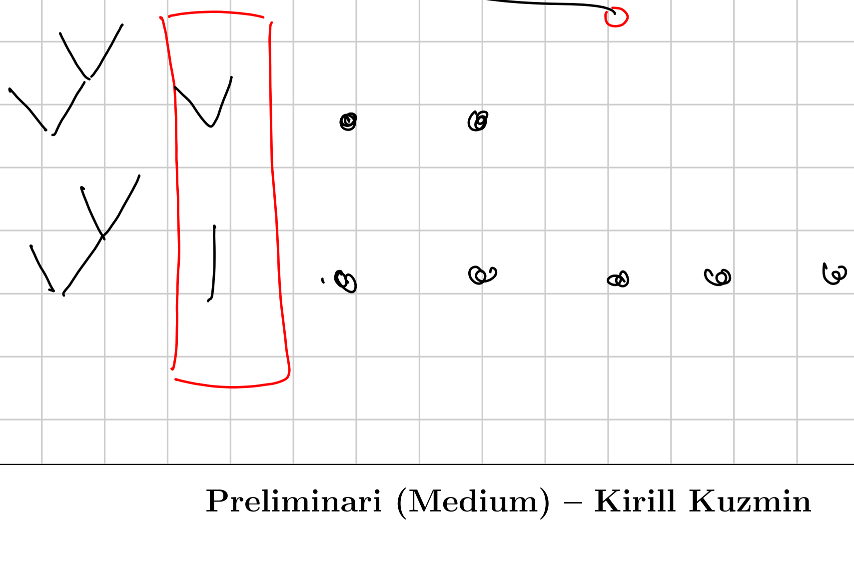
$\emptyset < \bullet <$ Qualunque altra idra

Idra 1



Idra 2





Ordiniamo le sottoidre in maniera decrescente

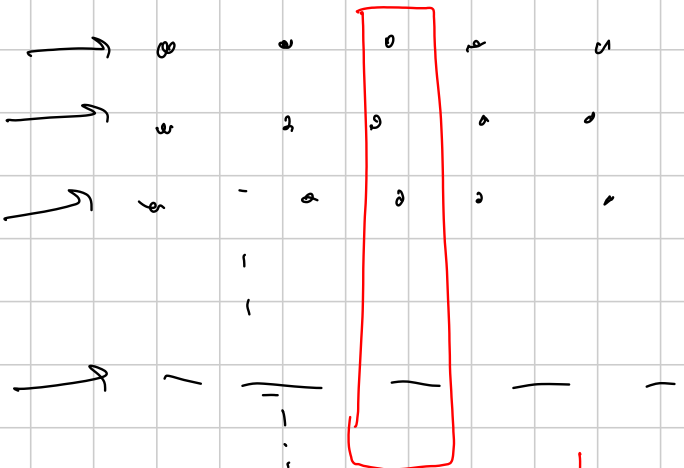
Andiamo a vedere il primo posto in cui le due successioni differiscono

L'idra maggiore è quella che ha la sottoidra maggiore nel primo posto in cui le successioni di sottoidre differiscono (sappiamo confrontare le sottoidre perché sono più basse)

È un ordine: Esercizio

(Attenzione: Definizione ricorsiva, le dimostrazioni vanno fatte per induzione)

È un buon ordine



Difficoltà: le altezze potrebbero non essere limitate. Idea per superarla:

Un'idra più alta è sempre maggiore di un'idra più bassa

Per induzione sull'altezza dell'idra più alta

$\ldots < \bigcirc$ ok

$\bigcirc < 1$ $\quad \emptyset < \bullet <$ Altra idra

ok

Idra 1 Idra 2

$m < n$

Per ipotesi induttiva, la sottoidra più alta della prima ha altezza $m-1$

Idra 1 $* \; \vdots \Big\}\, m-1$

Idra 2 $** \; \vdots \Big\}\, n-1$

Siccome $m-1<n-1<n$

Allora $* < **$

Attenzione: non potevamo fare induzione sull'altezza dell'idra più bassa!

$\bullet <$ Altra Idra

Idra 1 Idra 2

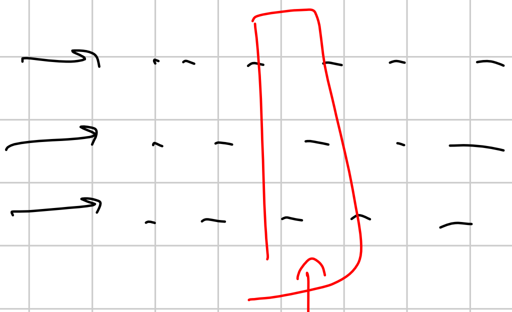
$n < m$

la sottoidra maggiore è alta $n-1$

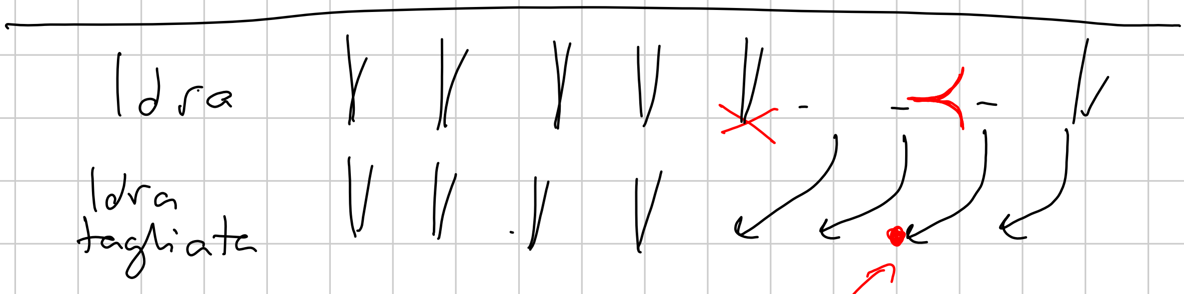
NON SAPPIAMO DIRE L'ALTEZZA DELLA SOTTOIDRA PIÙ ALTA!

Adesso possiamo completare la dim del buon ordine, perché sappiamo che l'idra minore va cercata tra quelle di altezza minima.

La cosa precisa da mostrare è: $P(n)$ ogni insieme di idre alte $\leq n$ ha minimo



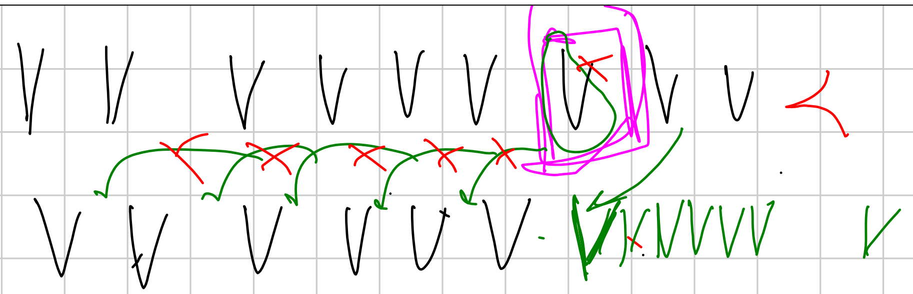
sono tutte di alt $\leq n-1$
Quindi sappiamo che ce n'è una minima per ip induttiva



OK in questo posto (il primo in cui ho stretto tra sottoidre) faccio il confronto

Idra

Idra tagliata e ricresciuta

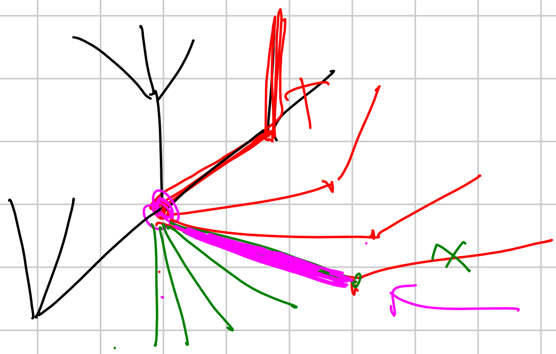


Si crea almeno una sottoidra corrispondente al taglio + ricrescita della sottoidra

Per ip induttiva, la struttura che si crea è $\leq$ originale, quindi va a finire dopo, nella successione delle sottoidre

Esercizio: formalizzare.

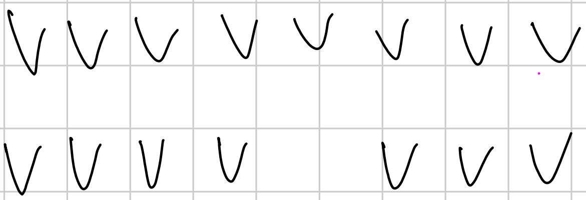
La tesi segue per discesa infinita.



Ricrescono copie della sottoidra rimanente (una sola)

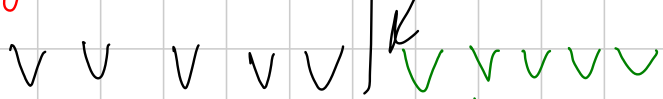
Idra

Idra tagliata



Taglio ad alt ≥ 3: cambio sotto idra

Taglio alt 2: cambio e moltiplica



questa è orig per ip induttiva