Stage Senior 2019 – Livello Medium

Stampato integrale delle lezioni

Autori vari

Indice

ALGEBRA 1 - Medium Senior 2019

Titolo nota 31/12/2011

Polinomi.

$$p(x) = a_n x^n + a_{n-1} x^{n-1} \text{ ---- } + a_1 x + a_0$$

$a_0, \dots, a_n$ sono i coff., con $a_n \neq 0$

n = "grado del polinomio"

Proprietà dei polinomi dipendono da dove prendono i coefficienti, in un anello A.

Def. Anello è un insieme $(A, +, \cdot)$ tale che per "+" esiste l'opposto e per "$\cdot$" esiste l'elemento neutro (1)

$0 \in A$, $1 \in A$, $a \in A \Rightarrow -a \in A$

$1 \cdot a = a$

$A[x]$ = "Insieme di polinomi a coeff. in A"

Fatto. Se A è un anello allora $A[x]$ è un anello

Esempi: $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{C}$ sono tutti anelli

$\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$, $\mathbb{C}[x]$ sono tutti anelli

$\mathbb{Z}/n\mathbb{Z}$ è un anello

Tutto quanto funziona bene se A è un dominio:
cioè se $a, b \in A$ $\quad a \cdot b = 0 \Rightarrow a = 0$ oppure $b = 0$

$\mathbb{Z}/n\mathbb{Z}$ è dominio $\iff$ ($n \mid ab \Rightarrow n \mid a$ o $n \mid b$)
(1)
n è un primo.

Cosa può succedere di male?

Es. $p(x) = (x-3)\cdot(x-4) = x^2 - 7x + 12 \pmod{12}$
$= x^2 - 7x$

3, 4 sono radici di $p(x)$ → 0, 7 sono radici di $p(x)$

$p(x)$ ha come radici (almeno) 0, 3, 4, 7 ma il grado di $p(x)$ è 2.

Th. A è un dominio allora se $p(x)$ ha grado $\le n$, $p(x)$ ha al più n radici.

Lemma (Ruffini) (A dominio) $p(a) = 0$ allora $(x-a) \mid p(x)$, cioè esiste $q(x) \in A[x]$ t.c. $p(x) = (x-a)\,q(x)$.

Pf. $(n=2)$ Supponiamo a_1, a_2, a_3 siano tre radici distinte di $p(x)$. Allora $p(a_1)=0$

$$p(x) = (x-a_1)\, q_1(x)$$

$$0 = p(a_2) = \underbrace{(a_2-a_1)}_{\neq 0}\ \underbrace{q_1(a_2)}_{\neq 0}$$

A è un dominio $\Rightarrow$ $a_2-a_1=0$ NO, oppure $q_1(a_2)=0$ ✓

$$q_1(x) = (x-a_2)\cdot a$$

$$0 = p(a_3) = \underbrace{(a_3-a_1)}_{\neq 0}\ \underbrace{(a_3-a_2)}_{\neq 0}\cdot a \qquad p(x) = a(x-a_1)(x-a_2) \not\equiv 0$$

$\deg(f\cdot g) = \deg(f) + \deg(g)$ ← vero solo per A dominio

$\deg(f\circ g) = \deg(f)\cdot\deg(g)$

$\deg(f+g) \leq \max\{\deg f, \deg g\}$

$$(x^2+1) + (x^3+1) = x^3+x^2+2$$

$$(x+1)^3 - x^3 = 3x^2+3x+1.$$

(Se A è un dominio) Irriducibilità e fatt. unica

$p(x) \in A[x]$ è irriducibile (in $A[x]$) se $\nexists\ q_1, q_2 \in A[x]$ con $\partial q_1 \geq 1$, $\partial q_2 \geq 1$

$$p(x) = q_1(x)\, q_2(x)$$

Th. (fatt. unica) $p(x) = q_1(x)^{\alpha_1} q_2(x)^{\alpha_2} \cdots q_k(x)^{\alpha_k}$ $q_1, \dots, q_k$ sono irriducibili

e la fatt. è unica

Es. pol. irriducibili:

in $\mathbb{C}[x]$ $\{(x-\alpha),\ \alpha \in \mathbb{C}\}$ $\leftrightarrow$ Th. fond. algebra $p(x) \in \mathbb{C}[x]$ $\Rightarrow \exists\ \alpha$ $p(\alpha) = 0$

in $\mathbb{R}[x]$ $\{(x-\alpha),\ \alpha \in \mathbb{R}\} \cup \{(x-\alpha)(x-\bar{\alpha}),\ \alpha \in \mathbb{C}\setminus\mathbb{R}\}$

↓ pol di secondo grado con $\Delta < 0$

Dim. Faccio fatt. su $\mathbb{C}$ e poi uso che $p(x)$ è a coeff. reali per cui $p(\alpha) = 0 \Rightarrow \overline{p(\alpha)} = 0 \Rightarrow p(\bar{\alpha}) = 0$

$$(x-\alpha)(x-\bar{\alpha}) = x^2 - (\alpha+\bar{\alpha})x + \alpha\bar{\alpha} = x^2 - 2\mathrm{Re}\,\alpha \cdot x + |\alpha|^2$$

$$p(x) = (x-r_1)^{d_1} \cdots (x-r_k)^{d_k} \cdot (x-\alpha_1)(x-\bar{\alpha}_1)^{e_1} (x-\alpha_2)(x-\bar{\alpha}_2)^{e_2} \cdots$$

in $\mathbb{Q}$, in $\mathbb{Z}$ $p(x)$ irriducibile può essere di qualsiasi grado.

Lemma di Gauss $p(x) \in \mathbb{Z}[x]$, riducibile in $\mathbb{Q}[x]$, allora è riducibile in $\mathbb{Z}[x]$.

$$p(x) = r_1(x)\, r_2(x) \qquad r_1, r_2 \in \mathbb{Q}_2[x]$$

$\exists\ q \in \mathbb{Q}$ t.c. $\quad q r_1(x) \in \mathbb{Z}[x]$

$\frac{1}{q} r_2(x) \in \mathbb{Z}[x]$

$$p(x) = (q\, r_1(x)) \cdot \left(\tfrac{1}{q} \cdot r_2(x)\right).$$

Derivata di un polinomio

$D(p)(x) \qquad D(p) \in A[x]$

(i) $D(p+q) = D(p) + D(q)$

(ii) $D(p \cdot q) = D(p) \cdot q + D(q) \cdot p$ (derivata formale)

(iii) $D(a \cdot p) = a\, D(p) \qquad a \in A$

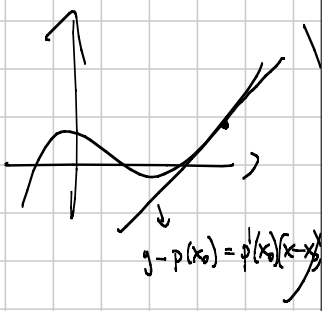
(iv) $D(x) = 1$

Corollario · $D(x^n) = n \cdot x^{n-1}$

$D(a x^n) = a \cdot n\, x^{n-1}$ (per induzione usando (iii) e (ii))

$$D(a_n x^n + \cdots + a_1 x + a_0) = n a_n x^{n-1} + (n-1) \cdot a_{n-1} \cdot x^{n-2} + \cdots + a_1$$

Bonus $D(p)(x) = p'(x) = \lim_{h \to 0} \dfrac{p(x+h) - p(x)}{h}$



Conseguenze per polinomi

(I) Se $x - \alpha \mid p'(x)$ e $x - \alpha \mid p(x)$

$\Rightarrow (x-\alpha)^2 \mid p(x)$.

(II) se $(m \geq 1)$ $(x-\alpha)^m \,||\, p(x) \Rightarrow (x-\alpha)^{m-1} \,||\, p'(x)$

$p(x) = (x-\alpha)^m \cdot q(x) \leftarrow (x-\alpha) \nmid q(x)$, in particolare $q(\alpha) \neq 0$

$p'(x) = \left((x-\alpha)^m\right)' \cdot q(x) + (x-\alpha)^m \cdot q'(x)$

$= m \cdot (x-\alpha)^{m-1} \cdot q(x) + (x-\alpha)^m \cdot q'(x)$

$= (x-\alpha)^{m-1} \left[m \cdot q(x) + (x-\alpha) q'(x) \right]$

↓ valuta in α

$m \cdot q(\alpha) + 0$

$\mathrm{rad}(n) = p_1 p_2 \cdots p_k$

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$\mathrm{rad}(p(x)) = p_1(x) \cdots p_k(x)$ $p_1, \dots, p_k$ sono i fattori irr. DISTINTI di p.

$p(x) = p_1(x)^{\alpha_1} \cdots p_k(x)^{\alpha_k}$

(I) + (II) $\Rightarrow \mathrm{rad}(p(x)) = \dfrac{p(x)}{\mathrm{mcd}(p(x), p'(x))}$

↓ in verità con irriducibile al posto di $(x-\alpha)$.

Esempi:

1) Dimostrare che il numero di radici distinte di $p(x)$ e $p(x)+1$ è ALMENO $\deg p + 1$

1bis) Qual è il numero minimo di radici distinte di $p(x)$, $p(x)+1$, $p(x)+2$, $\dots$, $p(x)+k$?

2) Trovare se esistono soluzioni di $p(x)^3 - q(x)^2 = 1$ p, q non costanti

2bis) Idem con $= 2x+1$

3) (RMM 18) Dire se esistono $p, q \in \mathbb{R}[x]$ non costanti tali che

$$p(x)^{10} + p(x)^9 = q(x)^{21} + q(x)^{20}$$

Come utile: per induzione trovare $D(p(x)^k)$

1. in $\mathbb{R}[x]$ x^n x^n+1

in $\mathbb{C}[x]$ radici distinte 0, $e^{\frac{ik\pi}{n}}$ k dispari $k < 2n$ $k = 1, 3, \dots, 2n-1$

Almeno $\deg p + 1$ radici

(i) $p(x) = (x-\alpha_1)^{d_1} \cdots (x-\alpha_K)^{d_K}$

$p(x)+1 = (x-\beta_1)^{e_1} \cdots (x-\beta_J)^{e_J}$ $\quad K + J \geq \deg p + 1$

$$p'(x) = (x-\alpha_1)^{d_1-1} \cdots (x-\alpha_k)^{d_k-1} \cdot (x-\beta_1)^{e_1-1} \cdots (x-\beta_j)^{e_j-1} \cdot q(x)$$

$$\partial p - 1 = \sum_i (d_i - 1) + \sum_i (e_i - 1) + \partial q$$

$$\geq \left(\sum_i d_i\right) - k + \left(\sum_i e_i\right) - j$$

$$= 2\partial p - k - j$$

$$k + j \geq \partial p + 1 .$$

(ii) $$\operatorname{rad}\left(p(x)(p(x)+1)\right) = \frac{p(x)(p(x)+1)}{MCD\left(p(x)(p(x)+1),\ p'(x)(2p(x)+1)\right)}$$

$$= \frac{p(x)(p(x)+1)}{MCD\left(p(x)(p(x)+1),\ p'(x)\right)}$$

$$\partial \square = 2\partial p - \partial\left(MCD\left(\ ,p'(x)\right)\right)$$

$$\geq 2\partial p - (\partial p - 1) = \partial p + 1$$

1bis) $p(x) = (\ )^{d_1} \cdots (\ )^{\ }$

$p(x)+1 = (\ )^{e_1} \cdots (\ )^{\ }$

$p(x)+k = (\ )^{f_1} \cdots (\ )^{\ }$

$$p'(x) = (\ )^{d_1-1} \cdots (\ )^{e_1-1} (\ )^{f-1} \cdot q(x)$$

$$\partial p - 1 \geq -r_0 + \left[\sum d_i - r_1 + \sum e_i - r_2 + \sum f_i \cdots\right.$$

$\geq -(r_0 + r_1 - - - + r_k) + (k+1)\,\partial p$

$r_0 + r_1 \cdots r_k \geq \underline{k\,\partial p + 1}$

$x^h \quad x^{h+1} \quad x^{h+2} \quad \cdots \quad x^{h+k}$

2) $p(x)^3 - q(x)^2 = 1$ $\quad p, q$ non costanti.

$\partial p = 2d$

$\partial q = 3d$

$3\,p(x)^2\,p'(x) - 2q(x)\,q'(x) = 0$

$3\,p(x)^2\,p'(x) = 2q(x)\,q'(x)$

r irriducibile $\quad r \mid p \Rightarrow r \mid q'$, con molteplicità doppia rispetto a p (poiché $r \nmid q$ dall'eq.)

$\Rightarrow \quad p^2 \mid q' \qquad \partial(p^2) \leq \partial q'$

$4d \leq 3d - 1 \quad \Rightarrow \quad d \leq -1.$

radici distinte di p^3 sono al più $2d$

" " " q^2 " " $3d$

$6d + 1 \leq 5d$

$d \geq -1$

2bis) PreIMO 2018 /p

$p(x)^3 - q(x)^2 = 2x + 1$ $\qquad \partial p = 2d$ $\quad \partial q = 3d$

$3\,p(x)^2\,p'(x) - 2q'(x)\,q(x) = 2$

$$3\,p(x)^3 p'(x) - 2q'(x)q(x)p(x) = 2p(x) \qquad (\text{La uno "mod } q(x)")$$

$$3(2x+1)p'(x) \equiv 2p(x)$$

($p(x)^3 \equiv 2x+1$ dall'equazione)

$$2p(x) - 3(2x+1)p'(x) \equiv 0 \quad (q(x))$$

$$q(x) \mid 2p(x) - 3(2x+1)p'(x)$$

$$\Downarrow$$

$$= 2d$$

$$\partial q = 3d$$

$$2a_n x^n + \cdots - 3(2x+1)\cdot\left(n\cdot a_n x^{n-1} + \cdots\right)$$

$$x^n\left(2a_n - 6n a_n\right) = a_n\cdot(2-6n)x^n \neq 0$$

↯.

3) Rmm'18

$$(p(x)+1)\,p(x)^9 - p(x)^{10} + p(x)^9 \equiv q(x)^{21} + q(x)^{20} = p(x)^{20}(p(x)+1)$$

P, q non costanti. $\in \mathbb{R}[x]$

$$p'(x)\,p(x)^8\left(10p(x)+9\right) = q'(x)\,q(x)^{19}\left(21q(x)+20\right)$$

$\partial q = 10n$

$\partial p = 21n$

$$\left(D(p(x)^k) = k\cdot p(x)^{k-1}\cdot p'(x)\right.$$

$$\left.D(y^k) = k\,y^{k-1}\cdot y' = k\,p(x)^{k-1}\cdot p'(x)\right)$$

$$p'(x)\,p(x)^3\left(10p(x)+y\right) = q'(x)\,q(x)^{19}\cdot p(x)\left(21q(x)+20\right)$$

$$p'(x)\,q^{20}(x)\left(q(x)+1\right)\left(10p(x)+y\right) = q'(x)\,q(x)^{19}\,p(x)\left(p(x)+1\right)\left(21q(x)+20\right)$$

$$p'(x)\,q(x)\left(q(x)+1\right)\left(10p(x)+y\right) = p(x)\left(p(x)+1\right)q'(x)\left(21q(x)+20\right)$$

se faccio il conto dei gradi: a sinistra $2\partial q + 2\partial p - 1$, in entrambi i membri.

$$p(x)\left(p(x)+1\right) \mid q(x)\left(q(x)+1\right)q'(x)$$

$$2\partial p \le 2\partial q + \partial p - 1$$

$$\partial p \le 2\partial q - 1 \quad ?$$

$$21n \le 2\cdot 10n - 1$$

$$20n - 1 \quad ?$$

$$n \le -1. \quad \lightning$$

Theorem (Mason-Stothers, Teorema ABC). $a, b, c \in A[x]$

$$a(x) + b(x) = c(x)$$

$\leftarrow$ a, b, c coprimi

$$\partial\left(\mathrm{rad}(abc)\right) \ge \max\{\partial a, \partial b, \partial c\} + 1$$

APPLICAZIONI!

1) $a(x) = p(x) \qquad b(x) = 1 \qquad c(x) = p(x)+1$

$rad(abc) = rad(p(x)(p(x)+1)) = \#$ rad. dist. di $p(x)$ e $p(x)+1$

$\geq \max(\partial a, \partial b, \partial c) + 1 = \partial p + 1$

2) $a = p^3 \qquad b = -q^2 \qquad c = p^3 - q^2$

Suppongo che $\partial c < \partial a$.

$\partial p = 2d$

$\partial q = 3d$

$\partial c < 6d$

$\partial(rad(abc)) \geq 6d + 1$

$\partial\left(rad\left(p^3(-q^2)\cdot(p^3-q^2)\right)\right) \leq \partial(rad(p)) + \partial\, rad(q) + \partial\, rad(p^3-q^2)$

$\left(\begin{array}{l} rad(ab) \leq rad(a)\cdot rad(b) \\ rad(p^k) = rad\, p \end{array}\right) \leq 2d + 3d + \partial\, rad(p^3q^2)$

$\partial\, rad(p^3-q^2) \geq d+1 \left(= \frac{\partial p}{2} + 1\right) \geq 2$

$\partial(p^3-q^2) \geq d+1 = \left(\frac{\partial p}{2} + 1\right)$

provare a vedere se si riesce ad ottenere la costante $d+1$.

3) $p^{10} + p^{1} = q^{21} + q^{20}$

$c \qquad a \qquad b$

$\partial q = 10d$

$\partial p = 21d$

$rad(abc) \geq \partial a + 1 = 210d + 1$

$rad(q^{21}\cdot q^{20}\cdot p^9\cdot(p+1)) \leq \partial q + 2\partial p = 10d + 42d.$

Attenzione!! bisogna avere a, b, c coprimi.

Fermat per polinomi: $\nexists\ p, q, r \in \mathbb{R}[x]$ t.c. $p(x)^3 + q(x)^3 = r(x)^3$

Dim. (ABC per polinomi)

$W = ac' - ca'$ $\quad \partial a \le d,\ \partial c \le d \Rightarrow \partial W \le 2d-1$ $\quad a+b=c,\ a'+b'=c'$

$r^k \| a \Rightarrow r^{k-1} \mid W$

$r^k \| c \Rightarrow r^{k-1} \mid W$

$r^k \| b \Rightarrow r^{k-1} \mid W$

$ac' - ca' = (c-b)c' - c(c'-b') = -bc' + b'c$

poiché a, b, c sono coprimi

$r^k \| abc \Rightarrow r^{k-1} \mid W \qquad W = \prod r_i^{(k_i-1)} \cdot q$

$$\mathrm{rad}(abc) = \prod r_i = \frac{\prod r_i^{k_i}}{\prod r_i^{k_i-1}} = \frac{abc}{W} \cdot q$$

$$\partial\,\mathrm{rad}(abc) \ge \partial(abc) - \partial W \ge 3\max\{\partial a, \partial b, \partial c\} - (\max\{\partial a, \partial b, \partial c\} - 1) = \max\{\partial a, \partial b, \partial c\} + 1$$

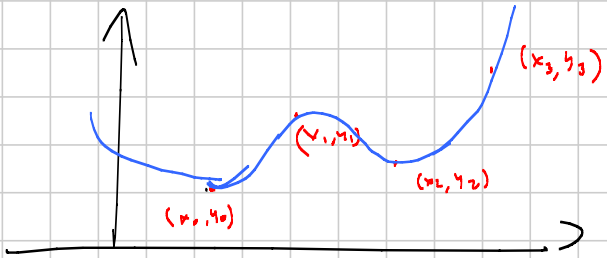
$a+b=c \qquad \frac{a}{c} + \frac{b}{c} = 1 \qquad \frac{a'c - c'a}{c^2} + \frac{b'c - c'b}{c^2} = 0.$

0

Interpolazione:

Domanda: date coppie di punti $(x_0, y_0) \dots (x_n, y_n)$ con x_i distinti ($x_i, y_i \in \mathbb{R}$).

Esiste una funzione polinomiale p che "passa" per questi punti? Quanto "facile" risulta farlo?



Vandermonde

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

$$\begin{cases} p(x_0) = y_0 \\ \vdots \\ p(x_n) = y_n \end{cases} \qquad \begin{cases} a_d x_0^d + \dots + a_1 x_0 + a_0 = y_0 \\ \vdots \\ a_d x_n^d + \dots + a_1 x_n + a_0 = y_n \end{cases}$$

$$V \to \begin{pmatrix} x_0^d & \dots & x_0 & 1 \\ x_1^d & x_1^{d-1} & \dots & x_1 \; 1 \\ & \ddots & & \\ x_n^d & x_n^{d-1} & \dots & x_n \; 1 \end{pmatrix} \begin{pmatrix} a_d \\ a_{d-1} \\ \vdots \\ a_1 \\ a_0 \end{pmatrix} = \begin{pmatrix} y_0 \\ \vdots \\ y_n \end{pmatrix}$$

Se $d+1 \geq n+1$ ci sono chance che il sistema abbia soluzione

Se $d+1 < n+1$ sicuramente non posso risolvere per

QUALSIASI $y_0, \dots, y_n$

IL CASO INTERESSANTE È $d+1 = n+1$

$$V \begin{pmatrix} a_n \\ \vdots \\ a_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow a_n = \dots = a_0 = 0$$

$\downarrow$

$p(x_0) = 0$

$p(x_1) = 0$

$\vdots$

$p(x_n) = 0$

$\Rightarrow p \equiv 0$

II metodo (costruttivo: includete (Lagrange))

$n = 3$ (x_0, y_0) (x_1, y_1) (x_2, y_2)

$$p_0(x) = \frac{(x-x_1)(x-x_2)}{(x_0-x_1)(x_0-x_2)} \qquad p_2(x) = \frac{(x-x_0)(x-x_1)}{(x_2-x_0)(x_2-x_1)}$$

$$p_1(x) = \frac{(x-x_0)(x-x_2)}{(x_1-x_0)(x_1-x_2)}$$

Lemma $p_i(x_j) = 0$ se $i \neq j$ $p_i(x_i) = 1$

$$p(x) = y_0 p_0(x) + y_1 p_1(x) + y_2 p_2(x)$$

$$p(x_0) = y_0 \underbrace{p_0(x_0)}_{1} + y_1 \underbrace{p_1(x_0)}_{0} + y_2 \underbrace{p_2(x_0)}_{0} = y_0$$

$p(x_1) = y_1$

$p(x_2) = y_2$

$$c\frac{(x-a)(x-b)}{(c-a)(c-b)} + b\frac{(x-c)(x-a)}{(b-c)(b-a)} + a\frac{(x-b)(x-c)}{(a-c)(a-b)} = X$$

$$p(x) = 1 \cdot p_c(x) + 1 \cdot p_b(x) + 1 \cdot p_a(x) \equiv 1$$

$\partial\, p(x) \leq n$

$\partial\, \tilde{p}(x) \leq n$

$p(x) - \tilde{p}(x) = 0$ su $x_0, \dots, x_n$

(x_0, y_0) $\quad p(x) = y_0$

(x_1, y_1) $\quad p(x) = y_0 + (x-x_0)\cdot\frac{(y_1-y_0)}{(x_1-x_0)}$

(x_2, y_2) $\quad p(x) = y_0 + (x-x_0)\frac{(y_1-y_0)}{(x_1-x_0)} + (x-x_0)(x-x_1)\cdot q$

$x_0, \dots, x_n = 1, 2, \dots, n+1$

$\partial\, p \leq n$

$p(-1)\ p(0)\ p(1)\ p(2)\ p(3)\ \cdots\ p(n)\ p(n+1)$

1 $\quad p(1)-p(0) \quad p(2)-p(1) \quad \cdots \quad p(n)-p(n-1)$

2 $\quad p(2)-2p(1)+p(0) \quad \cdots$

$\vdots$

n $\quad c_n \cdot n!$

$q(k) = p(k+1) - p(k)$

Dopo k diff. finite $\quad q(n) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} p(n+i)$

se $\quad k > \partial p \quad q \equiv 0$

$k = \partial p \quad q = c_{\partial p} \cdot (\partial p)!$

ALGEBRA 2 - Medium Senior 2019

Titolo nota 08/09/2019

Disuguaglianze.

1) Riarrangiamento $a_1, a_2, a_3, \dots, a_n, b_1, b_2, b_3, \dots, b_n \in \mathbb{R}$

Se $a_1 \geq a_2 \geq \dots \geq a_n$ e $b_1 \geq b_2 \geq \dots \geq b_n$

Allora $\forall \sigma \in S_n$ (gruppo delle permutazioni)

$$a_1 b_1 + a_2 b_2 + \dots + a_n b_n \geq a_1 b_{\sigma(1)} + a_2 b_{\sigma(2)} + \dots + a_n b_{\sigma(n)}$$

$\Rightarrow$ Chebyshev $\dfrac{a_1 b_1 + a_2 b_2 + \dots + a_n b_n}{n} \geq \left(\dfrac{a_1 + a_2 + \dots + a_n}{n}\right) \cdot \left(\dfrac{b_1 + b_2 + \dots + b_n}{n}\right)$

Dim. Somma Riarrang. su tutte le permutazioni σ oppure

Somma su le permutazioni del tipo $\sigma(i) = i + k \pmod n$

con $k = 0, \dots, n-1$

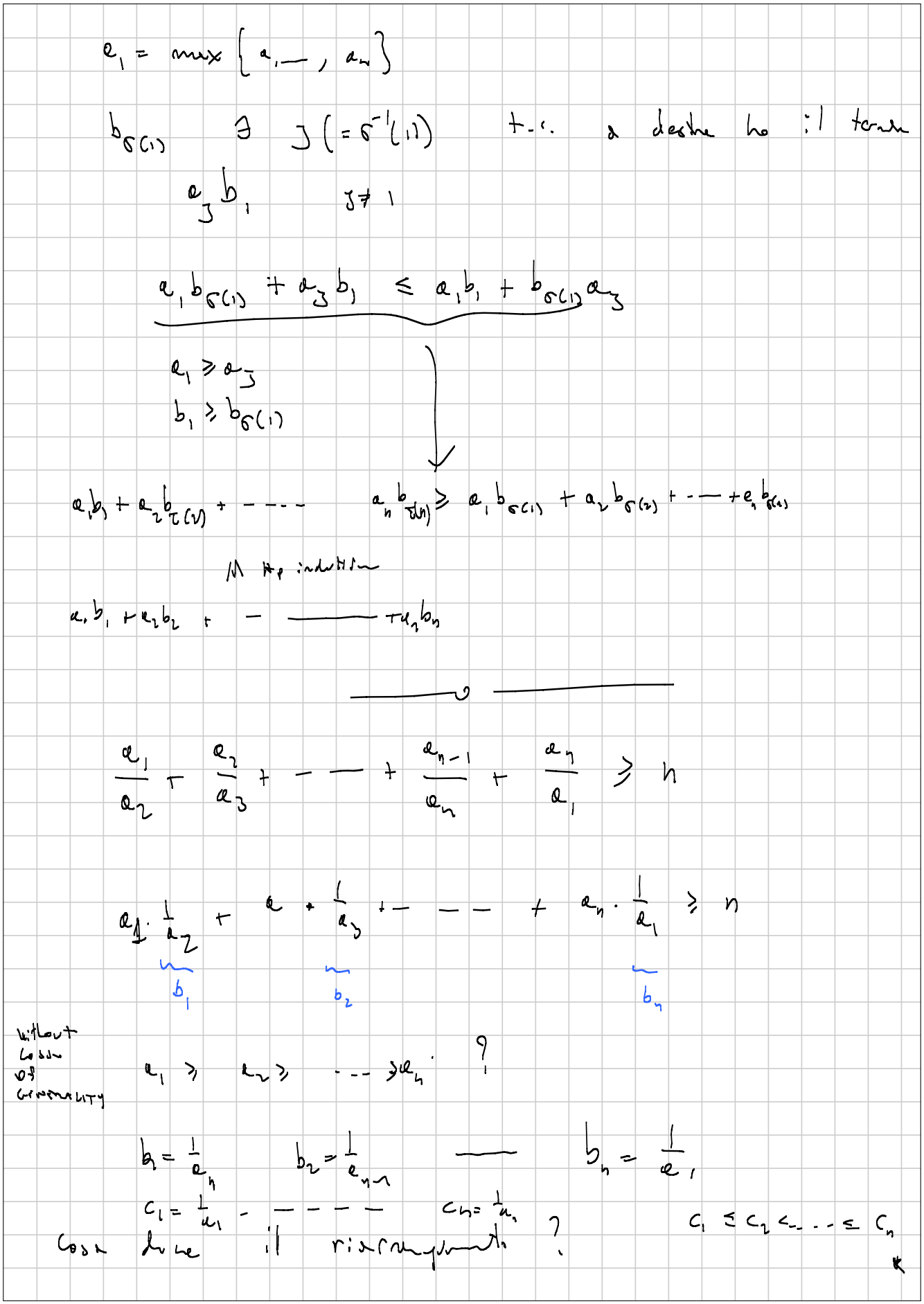
Dim (riarrangiamento) STEP FONDAMENTALE $n = 2$

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

$$a_1 b_1 + a_2 b_2 \geq a_1 b_2 + a_2 b_1$$

$$a_1 (b_1 - b_2) \geq a_2 (b_1 - b_2)$$

$$(a_1 - a_2)(b_1 - b_2) \geq 0 .$$


$a_1 = \max\{a_1, \dots, a_n\}$
$b_{\sigma(1)}$ $\exists$ j $(= \sigma^{-1}(1))$ t.c. a destra ho il termine
$a_j b_1$ $j \neq 1$
$a_1 b_{\sigma(1)} + a_j b_1 \leq a_1 b_1 + b_{\sigma(1)} a_j$
$a_1 \geq a_j$
$b_1 \geq b_{\sigma(1)}$
$a_1 b_1 + a_2 b_{\tau(2)} + \dots$ $a_n b_{\tau(n)} \geq a_1 b_{\sigma(1)} + a_2 b_{\sigma(2)} + \dots + a_n b_{\sigma(n)}$
N° induzione
$a_1 b_1 + a_2 b_2 + \dots + a_n b_n$
$\frac{a_1}{a_2} + \frac{a_2}{a_3} + \dots + \frac{a_{n-1}}{a_n} + \frac{a_n}{a_1} \geq n$
$a_1 \cdot \frac{1}{a_2} + a_2 \cdot \frac{1}{a_3} + \dots + a_n \cdot \frac{1}{a_1} \geq n$
b_1 b_2 b_n
Without Loss of Generality
$a_1 \geq a_2 \geq \dots \geq a_n$?
$b_1 = \frac{1}{a_n}$ $b_2 = \frac{1}{a_{n-1}}$ $b_n = \frac{1}{a_1}$
$c_1 = \frac{1}{a_1}, \dots, c_n = \frac{1}{a_n}$
Cosa dice il riarrangiamento ?
$c_1 \leq c_2 \leq \dots \leq c_n$

$$\frac{a_1}{a_n} + \frac{a_2}{a_{n-1}} + \dots + \frac{a_n}{a_1} \geq \text{numero finito del testo}$$

1b) Se $a_1 \geq a_2 \geq \dots \geq a_n$ e $b_1 \geq \dots \geq b_n$ $\quad c_i = -b_{n-i+1}$

$c_1 \geq \dots \geq c_n$

$$a_1 b_1 + a_2 b_2 + \dots + a_n b_n \leq a_1 b_{\sigma(1)} + \dots + a_n b_{\sigma(n)}$$

$$-a_1 c_1 - a_2 c_2 - \dots - a_n c_n \leq -a_1 c_{\sigma(1)} - \dots$$

$\Rightarrow$ se orientati in modo inverso

$$n = a_1 c_1 + \dots + a_n c_n \leq a_1 c_2 + \dots + a_{n-1} c_n + a_n c_1$$

$\uparrow$

Lts del testo

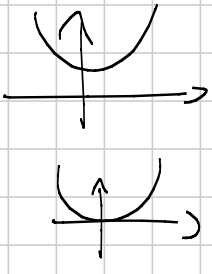
ATTENZIONE a "riordinare le variabili"

---

3) CS

$$(a_1^2 + a_2^2 + \dots + a_n^2)(b_1^2 + \dots + b_n^2) \geq (a_1 b_1 + \dots + a_n b_n)^2$$

I) $P(x) = \sum_{i=1}^{n} (a_i + x b_i)^2 \geq 0$



$\Rightarrow \quad \Delta \leq 0$

$$\frac{\Delta}{4} = \left(\sum a_i b_i\right)^2 - \left(\sum_i a_i^2\right)\left(\sum_i b_i^2\right) \leq 0$$

II) SOS $\left(\sum_i a_i^2\right)\left(\sum_j b_j^2\right) - \left(\sum_i a_i b_i\right)\left(\sum_j a_j b_j\right) =$

$$= \sum_i \sum_j \left(a_i^2 b_j^2 - a_i b_i a_j b_j\right)$$

$$= \sum_i \sum_j' \left(a_j^2 b_i^2 - a_i b_i a_j b_j\right)$$

$$= \sum_i \sum_j \frac{\left(a_i^2 b_j^2 + a_j^2 b_i^2 - 2 a_i b_i a_j b_j\right)}{2} = \sum_{i,j} \left(a_i b_j - a_j b_i\right)^2 \geq 0$$

Importante se uso SOS è che i quadrati che "creo" si bene che si annullino nei casi di uguaglianza conosciuti:

$$\frac{a^2+b^2}{2} \geq ab \quad \leftarrow \text{ha uguaglianza per } a=b$$

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

$\nwarrow \neq 0$ se $a=b$

$f(a,b,c) \geq g(a,b,c)$ = se $a=b=c$

$$f(a,b,c) - g(a,b,c) = f_1(a,b,c)^2 + f_2(a,b,c)^2 + f_3(a,b,c)^2 \geq 0$$

$$0 = f(a,a,a) - g(a,a,a) = f_1(a,0,0)^2 + f_2(a,a,a)^2 + f_3(a,0,a)^2 \geq 0$$

III) OMOGENEIZZAZIONE

Un'espressione $f(a_1, \dots, a_n)$ si dice OMOGENEA di grado d se

$$f(\lambda a_1, \dots, \lambda a_n) = \lambda^d f(a_1, \dots, a_n)$$

$f(x,y) = x^2 + y^2 + xy$ ← $d = 2$

$f(x,y,z) = x^3 + y^3 + z^3 - 3xyz$ ← $d = 3$

$f(x,y,z) = \frac{x}{y} + \frac{y}{z} + \frac{z}{x}$ ← $d = 0$

$f(a_1, \dots, a_n, b_1, \dots, b_n) = \left(\sum_i a_i^2\right)\left(\sum_i b_i^2\right) - \left(\sum_i a_i b_i\right)^2$ ← $d = 4$

$f(a_1, \dots, a_n) = \left(\sum_i a_i^2\right)\left(\sum_i b_i^2\right) - \left(\sum_i a_i b_i\right)^2$ ← o $d = 2$

Posso fissare un vincolo / posso levare un vincolo.

⚠ SOLO SE $d \neq 0$ (grado del vincolo)

f omogenea di grado d

$f(a_1, \dots, a_n) \geq 0 \qquad a_1, \dots, a_n \geq 0$

⇕

$f(b_1, \dots, b_n) \geq 0$ se $b_1 + \dots + b_n = 1 \qquad b_1, \dots, b_n \geq 0$

$a_1 + \dots + a_n = S$

$b_i = \lambda a_i \qquad \sum b_i = \lambda S \qquad \lambda = \frac{1}{S}$

$g(b_1, \dots, b_n) = 1$

$g(\lambda a_1, \dots, \lambda a_n) = \lambda^{\tilde{d}}\, g(a_1, \dots, a_n) = 1$ ← $\tilde{d} \neq 0$

$f(b_1, \dots, b_n) \geq 0$

$\lambda^d f(a_1, \dots, a_n) \geq 0$

$\lambda \neq 0$

$(a_1 b_1 + \dots + a_n b_n)^2 \leq (a_1^2 + \dots + a_n^2)(b_1^2 + \dots + b_n^2)$

$a_1^2 + \dots + a_n^2 = 1$
$b_1^2 + \dots + b_n^2 = 1$
$\Rightarrow \quad a_1 b_1 + \dots + a_n b_n \leq 1$

Equiv. a CS.

$a_1 b_1 \leq \frac{a_1^2 + b_1^2}{2} \qquad \sum a_i b_i \leq \frac{\sum a_i^2 + \sum b_i^2}{2} = 1$

$A_i = \frac{a_i}{\sqrt{\sum a_i^2}} \qquad B_i = \frac{b_i}{\sqrt{\sum b_i^2}}$

$A_i B_i \le \frac{A_i^2 + B_i^2}{2}$

$\frac{a_i b_i}{\sqrt{\sum_i a_i^2}\sqrt{\sum_i b_i^2}} \le \frac{\frac{a_i^2}{\sum_i a_i^2} + \frac{b_i^2}{\sum_i b_i^2}}{2}$

$\frac{\sum_i a_i b_i}{\sqrt{\sum_i a_i^2}\sqrt{\sum_i b_i^2}} \le \frac{\frac{\sum_i a_i^2}{\sum_i a_i^2} + \frac{\sum_i b_i^2}{\sum_i b_i^2}}{2} = 1$

$a_i b_i c_i \le \frac{a_i^3 + b_i^3 + c_i^3}{3}$ $\qquad \sum_i a_i^3 = 1 \quad \sum_i b_i^3 = 1 \quad \sum_i c_i^3 = 1$

$\sum_i a_i b_i c_i \le \frac{\sum a^3 + \sum_i b_i^3 + \sum_i c_i^3}{3} = 1$

$= \left(\sum_i a_i^3\right)^{1/3} \left(\sum_i b_i^3\right)^{1/3} \left(\sum_i c_i^3\right)^{1/3}$ $\quad *$

Ho dimostrato $*$ sotto il vincolo

$\sum_i a_i^3 = 1$

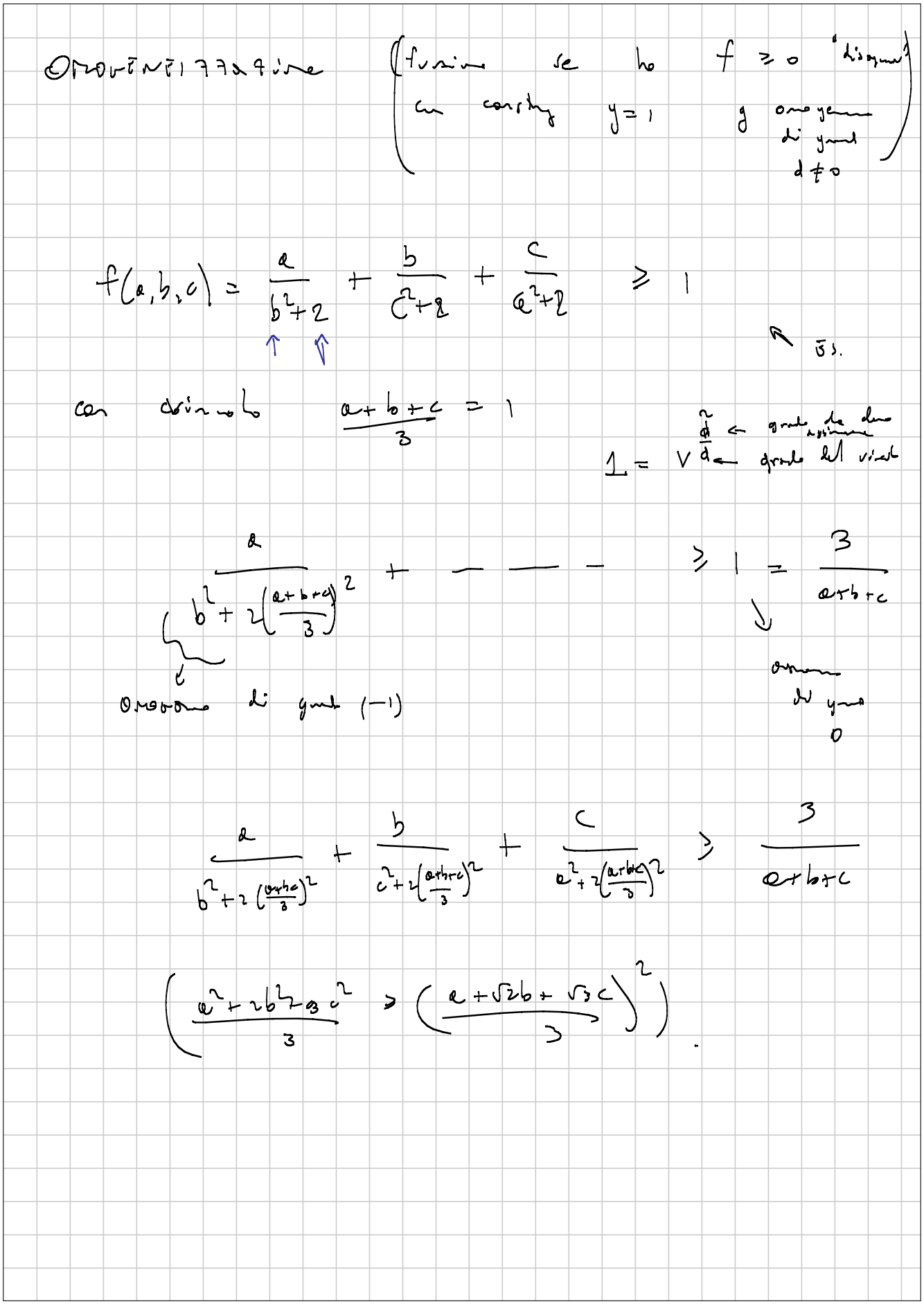
Ma poiché $\sum_i a_i b_i c_i - \left(\sum_i a_i^3\right)^{1/3}\left(\sum_i b_i^3\right)^{1/3}\left(\sum_i c_i^3\right)^{1/3} = f(a_i, b_i, c_i)$

f è 1-omogenea rispetto a (a_i)

$\sum_i a_i^3 = \lambda^3$ $\qquad \tilde{a}_i = \frac{a_i}{\lambda}$ $\qquad \sum_i \left(\frac{a_i}{\lambda}\right)^3 = 1$

omogeneità

$\frac{1}{\lambda} f(a_i, b_i, c_i) \ge \sum_i \frac{a_i}{\lambda} b_i c_i - \left(\sum_i \left(\frac{a_i}{\lambda}\right)^3\right)^{1/3} \le \ldots \ge 0$


Disuguaglianze
(funzioni se ho $f \geq 0$ "disuguaglianza"
con costante $y=1$ omogenee di grado $d \neq 0$)
$f(a,b,c) = \frac{a}{b^2+2} + \frac{b}{c^2+2} + \frac{c}{a^2+2} \geq 1$
C.S.
con dominio $\frac{a+b+c}{3} = 1$
$1 = \sqrt[2]{\frac{a}{a}}$ ← grado della disuguaglianza
grado dell'insieme
$\frac{a}{b^2+2\left(\frac{a+b+c}{3}\right)^2} + \dots \geq 1 = \frac{3}{a+b+c}$
omogeneo di grado (−1)
omogeneo di grado 0
$\frac{a}{b^2+2\left(\frac{a+b+c}{3}\right)^2} + \frac{b}{c^2+2\left(\frac{a+b+c}{3}\right)^2} + \frac{c}{a^2+2\left(\frac{a+b+c}{3}\right)^2} \geq \frac{3}{a+b+c}$
$\left(\frac{a^2+2b^2+3c^2}{3} \geq \left(\frac{a+\sqrt{2}b+\sqrt{3}c}{3}\right)^2\right)$.

Hölder, Hilbert e p-$\mathcal{V}$ spazi

$$a_1 b_1 \le \frac{a_1^2 + b_1^2}{2} \quad \to \quad CS$$

$$a_1 b_1 c_1 \le \frac{a_1^3 + b_1^3 + c_1^3}{3} \quad \to \quad \text{Holder} \quad \tfrac{1}{3}\ \tfrac{1}{3}\ \tfrac{1}{3}$$

$$a_1 b_1 \le \frac{a_1^p}{p} + \frac{b_1^q}{q} \qquad \left(\frac{1}{p} + \frac{1}{q} = 1\right) \qquad \left(\sum_i a_i^p\right) = 1 \quad \left(\sum_i b_i^q\right) = 1$$

$$\sum_i a_i b_i \le 1 = \left(\sum_i a_i^p\right)^{\frac{1}{p}} \left(\sum_i b_i^q\right)^{\frac{1}{q}}$$

AM-GM

$$\frac{na + mb + kc}{n + m + k} \ge \left(a^n b^m c^k\right)^{\frac{1}{n+m+k}} \qquad \underbrace{a, a, \dots}_{n}, \underbrace{b, \dots, b}_{m}, \underbrace{c, \dots}_{k}$$

$$w_a a + w_b b + w_c c \ge a^{w_a} b^{w_b} c^{w_c}$$

↑ AM-GM pesata

$$0 \le w_a \le 1 \qquad \boxed{w_a + w_b + w_c = 1}$$

$$w_a = \frac{1}{p_a} \qquad w_b = \frac{1}{p_b} \qquad w_c = \frac{1}{p_c}$$

$$a \to A^{p_a}$$

$$\frac{1}{p_a} A_i^{p_a} + \frac{1}{p_b} B_i^{p_b} + \frac{1}{p_c} C_i^{p_c} \ge ABC \qquad \frac{1}{p_a} + \frac{1}{p_b} + \frac{1}{p_c} = 1$$

$$\sum_i A_i B_i C_i \le \left(\sum_i A_i^{p_a}\right)^{\frac{1}{p_a}} \left(\sum_i B_i^{p_b}\right)^{\frac{1}{p_b}} \left(\sum_i C_i^{p_c}\right)^{\frac{1}{p_c}}$$

$$\left(\sum_i A_i\right)^{\alpha_1}\left(\sum_i B_i\right)^{\alpha_2}\left(\sum_i C_i\right)^{\alpha_3} =$$

$$= \left[\left(\sum_i A_i\right)^{\frac{\alpha_1}{\alpha_1+\alpha_2+\alpha_3}}\left(\sum_i B_i\right)^{\frac{\alpha_2}{\alpha_1+\alpha_2+\alpha_3}}\left(\sum_i C_i\right)^{\frac{\alpha_3}{\alpha_1+\alpha_2+\alpha_3}}\right]^{\alpha_1+\alpha_2+\alpha_3}$$

$$\geq \left[\sum A_i^{\frac{\alpha_1}{\alpha_1+\alpha_2+\alpha_3}} B_i^{\frac{\alpha_2}{\alpha_1+\alpha_2+\alpha_3}} C_i^{\frac{\alpha_3}{\alpha_1+\alpha_2+\alpha_3}}\right]^{\alpha_1+\alpha_2+\alpha_3}$$

$$\prod\left(a_i^2+b_i^2\right) \geq \left(\left(\prod a_i\right)^{\frac{2}{n}}+\left(\prod b_i\right)^{\frac{2}{n}}\right)^n.$$

ITA 10/01/2

$$\sum_{cyc} \frac{a}{\sqrt{a^2+8bc}} \geq 1$$

(1) MAGIA! $\frac{a}{\sqrt{a^2+8bc}} \geq \frac{a^\lambda}{a^\lambda+b^\lambda+c^\lambda}$ λ per cui sia vera

$\lambda = \frac{4}{3}$

$$a\left(a^{\frac{4}{3}}+b^{\frac{4}{3}}+c^{\frac{4}{3}}\right) \geq a^{\frac{1}{3}}\sqrt{a^2+8bc}$$

$$a+\frac{b^{4/3}+c^{4/3}}{a^{1/3}} \geq \sqrt{a^2+8bc}$$

$$a^2+2a^{2/3}\left(b^{4/3}+c^{4/3}\right)+\frac{\left(b^{4/3}+c^{4/3}\right)^2}{a^{2/3}} \geq a^2+8bc$$

$$\left(b^{4/3}+c^{4/3}\right)\left(2a^{4/3}+b^{4/3}+c^{4/3}\right) \geq 8bca^{2/3}$$

↑ AM-GM

② $\left(\sum \frac{a}{\sqrt{a^2+8bc}}\right)\left(\sum \frac{a}{\sqrt{a^2+8bc}}\right)\left(\sum (a^2+8bc)a\right) \geq \left(\sum a\right)^3$

$T^2 \geq \frac{(\sum a)^3}{(\sum a^3 + 24abc)} \overset{?}{\geq} 1$

$(\sum a)^3 = a^3+b^3+c^3 + \underline{\quad\quad} - -$ sicuramente vero $\geq a^3+b^3+c^3+24abc$

③ + Iran da Re

$\left(\sum \frac{a}{\sqrt{a^2+8bc}}\right)\left(\sum a\sqrt{a^2+8bc}\right) \geq \left(\sum a\right)^2$

$\left(\sum a\right)^2 \geq \sum a\sqrt{a^2+8bc}$

↓ LAVORO DA FARE

↓ $2bc \leq b^2+c^2$ --- etc

IMO 05/3 $x,y,z>0$ se $xyz \geq 1$ allora

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

$\sum \frac{(x^5-x^2) - x^3 - y^2 - z^2}{x^5+y^2+z^2} \geq -3$

$$\sum_{cyc} \frac{x^2+y^2+z^2}{x^5+y^2+z^2} \leq 3 \quad \Big\} \text{ o.s.}$$

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

$xyz \geq 1$

$xyz > 1$

posso porre $x \to \lambda x$, $\lambda \leq 1$

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

$$\frac{x^2+y^2+z^2}{x^5+y^2+z^2} \leq \frac{\frac{1}{x}+y^2+z^2}{x^2+y^2+z^2} \leq \frac{yz+y^2+z^2}{x^2+y^2+z^2}$$

$$\sum \quad xy+yz+zx \leq x^2+y^2+z^2 \qquad \vee$$

(AM-RM) (Riarrangiamento) (CS)

$$(x^2+y^2+z^2)\left(y^2+z^2+x^2\right) \geq (xy+yz+zx)^2$$

o

$$\frac{a}{b^2+2}+\frac{b}{c^2+2}+\frac{c}{a^2+2} \overset{?}{\geq} 1 \qquad a+b+c=3$$

CS $\quad \left((b^2+2)a+(c^2+2)b+(a^2+2)c\right) \top \geq (a+b+c)^2$

$$\frac{1}{3}(a+b+c)^3 \geq ab^2+bc^2+ca^2+\frac{2}{9}(a+b+c)^3$$

$$\frac{(a+b+c)^3}{9} \geq ab^2+bc^2+ca^2 \quad ?$$

$$a^3+b^3+c^3+3\sum_{sym} ab^2+6abc \geq 9\sum_{cyc} ab^2$$

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

SHUR → $a(a-b)(a-c)+b(b-c)(b-a)+c(c-a)(c-b)\geq 0$

VORNICU-SHUR $x(a-b)(a-c)+y(\quad -\quad \quad (\quad , \quad --)\geq 0$

se x,y,z e a,b,c sono ordinati nello stesso modo

$$\left(a^3+b^3+c^3+3abc-\sum_{sym}\right)+3abc+4\sum_{sym}-9\sum_{cyc}\geq 0$$

SHUR $\quad +\left(4\sum_{sym}-1\sum_{cyc}\right)+3abc\sum_{sym}$

$a^2b+b^2c+c^2a-ab^2-bc^2-ca^2$

$a(a-b)(a-c)+b(b-c)(b-a)+c(c-a)(c-b)+(a-b)(b-a)(c-a)+3abc-a^2b-b^2c-c^2a\overset{?}{\geq}0$

$a=0 \quad b=c$ $\qquad -b^3$

$$\frac{a}{b^2+2}+\frac{b}{c^2+2}+\frac{c}{a^2+2}\geq 1 \qquad a+b+c=3$$

$a\geq b \qquad a-\varepsilon,\ b+\varepsilon,\ c$

$$\frac{a-\varepsilon}{(b+\varepsilon)^2+2}+\frac{b+\varepsilon}{c^2+2}+\frac{c}{(a-\varepsilon)^2+2}$$

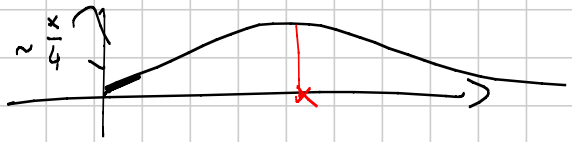
$$-\underbrace{\frac{\varepsilon}{b^2+2}}_{①} - \frac{\varepsilon \cdot a}{(b^2+2)^2}\cdot 2b \quad ② \qquad + \underbrace{\frac{\varepsilon}{c^2+2}}_{1b} + \frac{\varepsilon c a}{(a^2+2)} \quad 2b$$

$$\frac{2\cancel{b}}{(b^2+2)^2} \geq \frac{2\cancel{c}}{(c^2+2)^2} \qquad ① \leq 1b \quad \text{se } b \leq c$$

$$\frac{\cancel{2}b}{(b^2+2)^2} \geq \frac{\cancel{c}}{(a^2+2)^2} \leq \frac{c}{(c^2+2)^2} \leq \frac{b}{(b^2+1)} \qquad ② \leq 2b \quad \text{se } \begin{matrix} c \geq a \\ \sqrt{\frac{2}{3}} \leq b \leq c \end{matrix}$$

$$\sim \frac{1}{x^3}$$

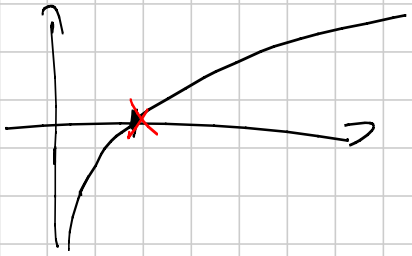
$$f(x) = \frac{x}{(x^2+2)^2} \sim \frac{1}{x^3}$$



$$f(x) = \frac{1}{\left(\frac{x^2+2}{\sqrt{x}}\right)^2} \qquad g(x) = x^{3/2} + \frac{2}{\sqrt{x}}$$

$$(x^\alpha)' = \alpha x^{\alpha-1}$$

$$g'(x) = \frac{3}{2}x^{1/2} - \frac{1}{x^{3/2}} < 0$$



$$\frac{3}{2}x^{1/2} = \frac{1}{x^{3/2}}$$

$$x^2 = \frac{2}{3}$$

$$x = \sqrt{\frac{2}{3}}$$

$a, b, c \in (0, 3)$ "tipicamente" ~ 1

FUNZIONI CONVESSE, MASSIMI E MINIMI

f convessa in I intervallo se

$\forall\ x, y \in I$ e $\forall\ \lambda \in (0,1)$ si verifica

$$f(\lambda x + (1-\lambda) y) \leq \lambda f(x) + (1-\lambda) f(y)$$

- vera sse $\lambda = \frac{1}{2}$ $\forall\ x, y \in I$ $\Leftarrow$

(i) $f(\sum \lambda_i x_i) \leq \sum \lambda_i f(x_i)$ (induzione)

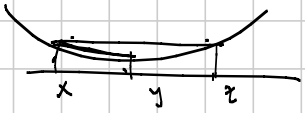
$\sum \lambda_i = 1$, $\lambda_i \in (0,1)$, $x_i \in I$

(ii) massimo si trova ai bordi dell'intervallo

esiste un unico minimo all'interno ($f'(x) = 0$)

Def. equivalenti

① Rapporti incrementali crescenti



$x \leq y \leq z$

$$\frac{\Delta f}{\Delta x}(y,x) \leq \frac{\Delta f}{\Delta x}(z,x) \leq \frac{\Delta f}{\Delta x}(z,y)$$

$$\frac{\Delta f}{\Delta x}(a,b) = \frac{f(b) - f(a)}{b - a}$$

② se $\exists\ f'$ allora f' è crescente

③ se $\exists\ f''$ allora $f'' \geq 0$.

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

0 - omogenea

$a+b+c=1$

$$\frac{a}{1-a} + \frac{b}{1-b} + \frac{c}{1-c} \geq \frac{3}{2}$$

$$f(x) = \frac{x}{1-x} \qquad f \text{ convessa}$$

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

$f+\lambda$	è conv.
$f(x-x_0)$	è conv.
$f(g(x))$	g conv. f conv. e crescente

$\frac{1}{x^\alpha} \quad \forall \alpha > 0$

x^α convessa $\alpha \geq 1$

x^2 concava se $\alpha < 1$

Es. cos x max e min $\sin\alpha + \sin\beta + \sin\gamma$ α, β, γ angoli di un triangolo

$\cos\alpha + \cos\beta + \cos\gamma$

$\sin(x)' = \cos(x)$

$\cos(x)' = -\sin(x)$

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

$$f(a) + f(b) + f(c) \geq 3 f\left(\frac{1}{3}\right) = 3 \frac{\frac{1}{3}}{1-\frac{1}{3}} = \frac{3}{2}$$

SL 2015 / A3 $-1 \leq x_i \leq 1$ trovare il minimo di $i = 1, \dots, 2n$

$$\sum_{1 \leq r < s \leq 2n} (s-r-n)\, x_r x_s$$

$(s-r-n) \in [-3n+1, n-1]$

1) ridurre $x_i \in \{\pm 1\}$ ←1

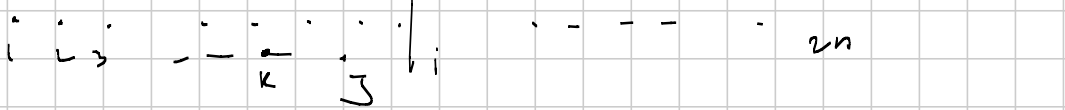
2) $y_i = \sum_{j \leq i} x_j - \sum_{j > i} x_j$ somma di $2n$ numeri ± 1

$$y_i^2 = \sum_i x_k^2 + 2\sum_{k<j\leq i} x_k x_j + 2\sum_{i<k<j} x_k x_j - 2\sum_{k\leq i<j} x_j x_k$$

$\sum_i x_k^2 = 2n$

$$\sum_i y_i^2 = 4n^2 + 2\sum_{k<j} x_k x_j \left(2n - 2\#\text{ quanti: negativi } j \to k\right)$$

$$4n^2 + 2 \sum_{k<j} x_k x_j (2n - 2(j-k))$$



$$\sum_i y_i^2 = 4n^2 + 4 \sum_{k<j} x_k x_j (n - j + k)$$

$$= 4n^2 - 4T$$

$$4T = 4n^2 - \sum_i y_i^2 \qquad \text{massimizzare}$$

Massimo di T è in modo di

$$\frac{\sum_i y_i^2}{4} - n^2$$

y_i è pari e $y_i - y_{i+1} = 2x_i \in \{\pm 2\}$

$$(y_1, y_2 = \text{——}, y_{2n}) = (0, 2, 0, 2, 0, 2 \text{ ——})$$

$$\min \overset{?}{=} \frac{4n}{4} - n^2 = n - n^2$$

$$\rightsquigarrow \max T = n^2 - n$$

$x_i = (-1)^i$.

$\sum_i x_i - \sum_{i,j} x_i x_j$ $\qquad a,b,c \in (-1,1)$

$a+b+c - ab - bc - ca$

Teo. Weierstrass

$f(x_1, \dots, x_n)$ $\quad f$ CONTINUA

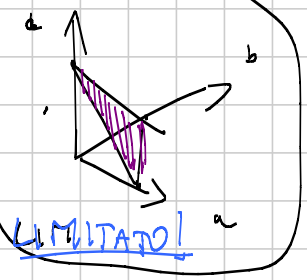
$(x_1, \dots, x_n) \in U$ $\quad U$ CHIUSO $\to$ approssimazione di cui sono $= 0 \leq$

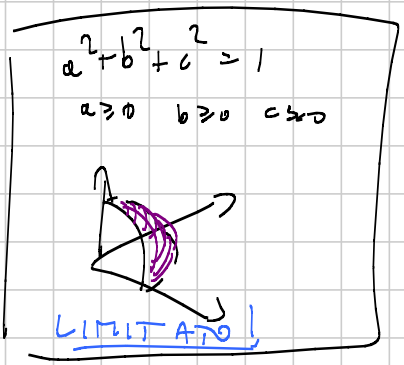
LIMITATO

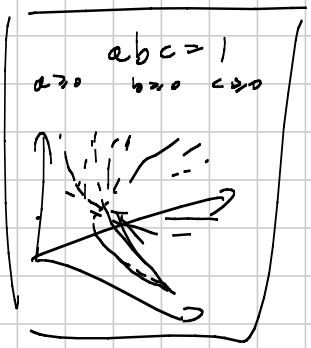
ALLORA $\exists\ (\overline{x}_1, \dots, \overline{x}_n) \in U$ di MASSIMO della funzione

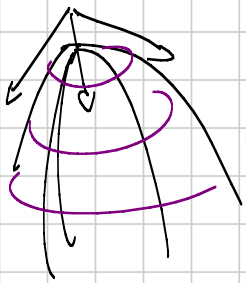
---

$a+b+c=1$ $\quad a \geq 0 \quad b \geq 0 \quad c \geq 0$









← ILLIMITATO!

• U limitato se $\exists M > 0$ t.c. $|x_i| \le M$ $\forall (x_1, \dots, x_n) \in U$

$a+b+c=1$ $\quad 0 \le a \le 1$

$a \ge 0$ $b \ge 0$ $c \ge 0$

$a^2+b^2+c^2=1$ $\quad |a| \le 1$

$abc=1$ $\quad M>0$ $\quad a = n+1$ $\quad b = \frac{1}{n+1}$ $\quad c=1$

non limitato!

$$1 \le \frac{a^3+b^3+c^3}{3} \qquad abc=1$$

$U = \{abc=1\}$

$B = \begin{cases} a \le 10 \\ b \le 10 \\ c \le 10 \end{cases}$ $\quad f(a,b,c) = \frac{a^3+b^3+c^3}{3}$ ha un minimo $\le \frac{1^3+1^3+(\frac{1}{1})^3}{3}$

come stimo $f(a,b,c)$ fuori da B?

$U \setminus B$ $\quad a \ge 10$ o $b \ge 10$ o $c \ge 10$

Ma almeno $f(a,b,c) \ge \frac{10^3}{3} \ge \frac{1^3+1^3+(\frac{1}{1})^3}{3}$

① Esiste il minimo in $abc=1$ di $f(a,b,c)$

② Questo minimo sta in $B \cap U$

Serve a giustificare l'esistenza e come ci comportano con i min: (tipo, c'è un min./max. stretto in un certo modo).

$$\frac{a}{\sqrt{a^2+8bc}} \geq \frac{a^\lambda}{a^\lambda+b^\lambda+c^\lambda}$$ come individuare λ:

c'è sicuramente uguaglianza in $a=b=c=1$

$b=c=1$

$$\frac{a}{\sqrt{a^2+8}} \geq \frac{a^\lambda}{a^\lambda+2}$$ per quali λ è vera

$$= 1-\frac{2}{a^\lambda+2}$$

$$f_\lambda(a) = \left(\frac{a}{\sqrt{a^2+8}} - \frac{a^\lambda}{a^\lambda+2}\right) \geq 0 \qquad = 0 \text{ in } 1=a \quad \forall \lambda$$

$$f_\lambda'(a) = 0$$

$$\frac{1}{\sqrt{a^2+8}} - \frac{a^2}{(a^2+8)^{3/2}} - \frac{\lambda 2a^{\lambda-1}}{(a^\lambda+2)^2} = 0$$

$$\frac{1}{3} - \frac{4}{27} - \frac{2\lambda}{9} = 0$$

$$\frac{9}{27} - \frac{1}{27} - \frac{6\lambda}{27} = 0 \qquad \lambda = \frac{8}{6} = \frac{4}{3}.$$

A3 Medium pol

Titolo nota 10/09/2019

Successioni + equazioni funzionali

(1) $a_{n+1} = \alpha a_n + \beta a_{n-1} + \gamma a_{n-2} + \dots$

$\hat{a} := $ tutta la successione $(a_1, a_2, a_3, a_4, \dots)$

$z\hat{a} := (a_2, a_3, a_4, a_5, \dots)$

$z^2\hat{a} := (a_3, a_4, a_5, \dots)$

(1) diventa $z^2\hat{a} = \alpha z\hat{a} + \beta\hat{a}$

$(z^2 - \alpha z - \beta)\hat{a} = 0$ o di grado più alto

$q(z)$

Il polinomio avrà due soluzioni, λ_1, λ_2

$$0 = (z-\lambda_1)(z-\lambda_2)\hat{a} = (z-\lambda_2)(z-\lambda_1)\hat{a}$$

Due successioni particolari che verificano (1) sono quelle che verificano $(z-\lambda_2)\hat{a} = 0$, $(z-\lambda_1)\hat{a} = 0$,

cioè rispettivamente $a_n = \lambda_1^n$, $b_n = \lambda_2^n$

La soluzione generale di (1) è

(soluzione generale) $a_n = c\lambda_1^n + d\lambda_2^n$ al variare di $c, d \in \mathbb{C}$

Se mi viene data (1) + condizioni iniziali $a_1 = \square$, $a_2 = \bigstar$

basta risolvere il sistema $\begin{cases} \square = a_1 = c\lambda_1^1 + d\lambda_2^1 \\ \bigstar = a_2 = c\lambda_1^2 + d\lambda_2^2 \end{cases}$

per trovare i valori di c, d che soddisfano (1) + cond. iniziali

(soluzione particolare)

Se le soluzioni di $z^2 - \alpha z - \beta = 0$ sono complesse, ho potenze complesse, che posso scrivere anche come seni/coseni;

se α, β reali, le sol. sono complesse coniugate

$$\lambda_{1,2} = \rho \cdot (\cos\vartheta \pm i \sin\vartheta)$$

sol. generale è $a_n = c\rho^n(\cos n\vartheta + i\sin n\vartheta) + d\rho^n(\cos n\vartheta - i\sin n\vartheta)$

$$= (c+d)\ \rho^n \cos(n\vartheta) + i(c-d) \cdot \rho^n \sin(n\vartheta)$$

Se l'equazione $z^2 - \alpha z - \beta$ (o il suo equivalente di grado superiore) ha soluzioni multiple, si riescono comunque a trovare soluzioni particolari che generano tutte le soluzioni:

se c'è un fattore di grado k, le soluzioni di

$$(z-\lambda)^k \hat{a} = 0$$

sono $a_n = \lambda^n$, $b_n = n\lambda^n$, $c_n = n^2\lambda^n$, ... fino ad avere k distinte

e le loro comb. lineari, cioè, la sol. generale è

$$a_n = p(n)\lambda^n$$, dove p è un polinomio di grado $< k$.

Per dimostrare che sono soluzioni, serve criterio della derivata:

se λ è una radice doppia di $q(z) = z^2 - \alpha z - \beta$, allora è anche radice di $q'(z)$. Se è radice tripla, è anche radice di $q''(z)$, e così via

(dietro a questa notazione con le z ci sono serie di potenze: se definite $\hat{a} := a_1 + a_2 z^{-1} + a_3 z^{-2} + a_4 z^{-3} + \dots$, allora $z\hat{a}$ vuol dire moltiplicare $\hat{a}$ per z (a meno di un valore iniziale).

Generalizzazione: successioni "non omogenee": ad esempio,

(2) $a_{n+1} = \alpha a_n + \beta a_{n-1} + f(n)$ (ad esempio $f(n) = 2^n$)

(1) si dice "successione omogenea",
(2) si dice "successione non omogenea"

Se sapete trovare una soluzione particolare della (2) (con condizioni iniziali a nostra scelta), allora c'è un teorema che ve le produce tutte:

Teo: se p_n è una soluz. particolare di (2), allora tutte e sole le soluz. della (2) si ottengono sommando la sol. generale della (1) e la p_n:

$$a_n = \underbrace{c\lambda_1^n + d\lambda_2^n}_{\text{sol. generale della (1)}} + p_n$$

Dim: se a_n soddisfa (2) e p_n soddisfa la (2) allora $a_n - p_n$ soddisfa (1), per differenza:

$$a_{n+1} = \alpha a_n + \beta a_{n-1} + f(n)$$
$$p_{n+1} = \alpha p_n + \beta p_{n-1} + f(n)$$
$$a_{n+1} - p_{n+1} = \alpha(a_n - p_n) + \beta(a_{n-1} - p_{n-1})$$

quindi $a_n - p_n = \underbrace{c\lambda_1^n + d\lambda_2^n}_{\text{sol. generale della (1)}}$ (per qualche c, d)

R1 per trovare p_n, se $f(n)$ è della forma μ^n, allora cercate una p_n della forma $p_n = c \cdot \mu^n$

Es: cerchiamo le soluzioni di (3) $a_{n+1} = a_n + a_{n-1} + 2^n \quad \forall n > 1$:

(1) cerco p_n della forma $p_n = c \cdot 2^n$:

(3): $c \cdot 2^{n+1} \overset{!}{=} c \cdot 2^n + c \cdot 2^{n-1} + 2^n \quad \forall n$

$\iff 2^{n-1} \cdot 4c = 2^{n-1}(2c + c + 2) \quad \forall n$

$\iff 4c = 3c + 2 \iff c = 2$

$\Rightarrow p_n = 2 \cdot 2^n = 2^{n+1}$ è una sol. particolare di (3).

Per il teorema, tutte le sol. di (3) sono della forma

$$a_n = c \cdot \phi_1^n + d\,\phi_2^n + 2^{n+1} \qquad \left(\phi_{1,2} = \frac{1 \pm \sqrt{5}}{2}\right)$$

Questo trucco fallisce se μ è una soluzione di $z^2 - \alpha z - \beta = q(z)$.

R2: In questo caso, provare con $p_n = (a + bn) \cdot \mu^n$

$p_n = (a + bn + cn^2) \cdot \mu^n$

$\vdots$

R3: se $f(n)$ è della forma $(r_0 + r_1 n + \dots + r_d n^d)\,\mu^n$, allora cercate p_n della stessa forma (polinomio di grado d moltiplicato per μ^n.

Se μ è radice di $q(z)$, dovrete alzare il grado

Cosa c'è dietro: $q(z)\,\hat{a} = 0$ per una succ. omogenea

$q(z)\,\hat{a} = f(n)$, per esempio $q(z)\,\hat{a} = 2^n$

Posso applicare un "operatore con la z" che mi elimina il 2^n:

$$(z - 2)\,q(z)\,\hat{a} = 0$$

Cioè, in altra notazione: parto da $a_{n+1} = \alpha a_n + \beta a_{n-1} + 2^n$

sottraggo $a_{n+2} = \alpha a_{n+1} + \beta a_n + 2^{n+1}$

e $2a_{n+1} = 2\alpha a_n + 2\beta a_{n-1} + 2\cdot 2^n$

$(a_{n+2} - 2a_{n+1}) = \alpha(a_{n+1} - 2a_n) + \beta(a_n - 2a_{n-1})$

$\Rightarrow a_{n+1} - 2a_n$ è una succ. per ricorrenza omogenea con polinomio associato $q(z)$

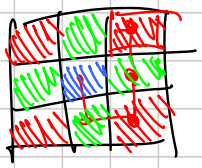
e quindi a_n è una succ. per ric. omogenea con pol. associato $q(z)\cdot(z-2)$

---

n^2 è $n^2 \cdot 1^n$ (conta 3 radici 1)

$\cos(n\theta) = \frac{e^{in\theta} + e^{-in\theta}}{2}$ (conta radici $e^{i\theta}$ e $e^{-i\theta}$)

Saltano spesso fuori in problemi di contare sequenze:

Es:  su una scacchiera 3×3, quanti sono i percorsi lunghi n che partono dalla casella centrale, e finiscono in una casella d'angolo

Idea: definisco

$A_n = \#\{$percorsi lunghi n da centro a centro$\}$

$B_n = \#\{$ " " " da centro a edge$\}$

$C_n = \#\{$ " " " da centro ad angolo$\}$

(una a scelta delle caselle, dato per simmetria sono tutti uguali)

Posso scrivere una ricorrenza combinata:

$$\begin{cases} A_{n+1} = 4B_n & \text{(i)} \\ B_{n+1} = A_n + 2C_n & \text{(ii)} \\ C_{n+1} = 2B_n & \text{(iii)} \end{cases} \xrightarrow{\text{(iii)}} \begin{cases} A_{n+1} = 2C_{n+1} \\ \frac{1}{2}C_{n+2} = A_n + 2C_n \end{cases}$$

$$\rightarrow \begin{cases} \vdots \\ \frac{1}{2} C_{n+2} = 4 C_n \\ \vdots \end{cases} \qquad \text{pol. associato } \frac{1}{2} z^2 - 4$$

$$\begin{aligned} z\hat{A} &= 4\hat{B} \\ z\hat{B} &= \hat{A} + 2\hat{C} \\ z\hat{C} &= 2\hat{B} \end{aligned} \qquad \begin{bmatrix} -z & 4 & 0 \\ 1 & -z & 2 \\ 0 & 2 & -z \end{bmatrix} \cdot \begin{bmatrix} \hat{A} \\ \hat{B} \\ \hat{C} \end{bmatrix} = 0$$

$$\Leftrightarrow \det \begin{bmatrix} -z & 4 & 0 \\ 1 & -z & 2 \\ 0 & 2 & -z \end{bmatrix} = 0 \quad \text{che è il } q(z) \text{ di queste successioni}$$

ES: Quante sono le successioni di 0 e 1 lunghe n che non hanno tre zeri di fila, oppure quattro uni di fila?

$A_n = \#\{$ succ. lunghe n che finiscono con $10\}$

$B_n = \#\{$ " $100\}$

$C_n = \#\{$ " $01\}$

$D_n = \#\{$ " $011\}$

$E_n = \#\{$ " $0111\}$

$$C_{n+1} = A_n + B_n$$

FUNZIONALI

$$(*) \quad f(x+y) = f(x) + f(y) \qquad \forall x, y \in \mathbb{Q}, \mathbb{R}, \dots$$

Varianti...

es. $f(x+y) = f(x) + f(y) \quad \forall x, y \geq 0$

1) $f(ny) = nf(y) \quad \forall n \in \mathbb{N}, y \geq 0$

2) $f\left(\frac{n}{m} y\right) = \frac{n}{m} f(y) \quad \forall n, m \in \mathbb{N}, m>0, y \geq 0$

3) $P(-y, y) : 0 = f(0) = f(-y) + f(y) \quad \forall y \geq 0$

$P(0,0) : f(0) = 0$

$\Rightarrow f(-y) = -f(y) \quad \forall y \geq 0 \Rightarrow$ dispari

---

$f(x+y+1) = f(x) + f(y) + f(1) \quad \forall x, y \in \mathbb{Q}$ (+g(1), +f(1))

Sostituzioni!

$g(x) := f(x) + f(1) \qquad g(x+y+1) = g(x) + g(y)$

$h(x) := g(x-1)$

$h(x+1) = g(x)$

$h(x+y+2) = h(x+1) + h(y+1) \quad \forall x, y \in \mathbb{Q}$

poniamo $z := x+1$, $w := y+1$ $\qquad h(z+w) = h(z) + h(w)$

(*) $f(xy) = f(x) \cdot f(y) \qquad f: \mathbb{R}^+ \to \mathbb{R}^+ \qquad x, y \in \mathbb{R}^+ \quad (= \{x \in \mathbb{R}, x > 0\})$

$g(x) := \log f(x) \qquad \log(*): \quad \log f(xy) = \log f(x) + \log f(y)$

(**) $g(xy) = g(x) + g(y) \quad \forall x, y \in \mathbb{R}^+$

$x = e^z, \ y = e^w$

(**) $g(e^{z+w}) = g(e^z) + g(e^w) \qquad z, w \in \mathbb{R}$

$h(x) := g(e^x) \qquad h(z+w) = h(z) + h(w) \qquad z, w \in \mathbb{R}$

$h(\log(x)) = g(x)$

Es (per casa): trovare tutte le funzioni t.c. $f:\mathbb{Q}\to\mathbb{Q}$.

$$f\left(\frac{x+y}{2}\right)=\frac{f(x)+f(y)}{2} \qquad x,y\in\mathbb{Q}$$

$f:\mathbb{Q}\to\mathbb{Q}$

trovare tutte le funzioni t.c. $f(a)+f(d)=f(b)+f(c)$

per ogni $a<b<c<d$ in progr. aritmetica

$f:\mathbb{Q}\to\mathbb{Q}$ t.c. $f(x+y)=f(x)+f(y)$ $\forall x,y$

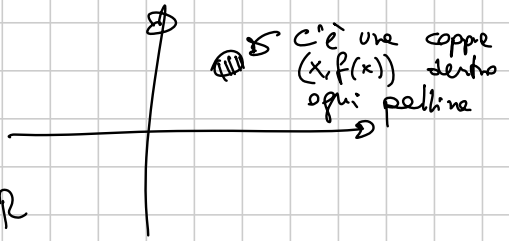
ha come soluzioni solo le rette

$f:\mathbb{R}\to\mathbb{R}$ t.c. $f(x+y)=f(x)+f(y)$

ha anche altre soluzioni.

Queste soluzioni "wild" hanno tutte grafico denso in $\mathbb{R}^2$

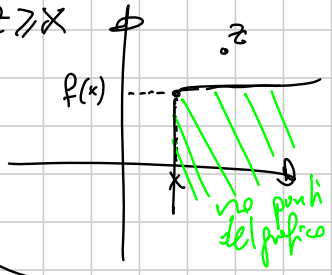
Per escludere soluzioni wild, si cercano proprietà di "parti vuote del piano":



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

ogni numero $z>x$ si scrive come $x+y^2$ per un qualche y,

e (*) ci dice che $f(z)\geq f(x)$ per ogni $z\geq x$



Equazioni con soluzioni "wild"

$$f(f(x))=x \qquad \forall x\in\mathbb{R}$$

Posso costruire sol. wild in questo modo: divido tutti i reali in coppie, ad es. $\{1,2\}$, $\{\pi,-\pi\}$, $\{\sqrt{2},\sqrt{3}\}$ + singoletti: $\{e\}$

e definisco la f che "scambia" i numeri di queste coppie

$f(1)=2$ $\quad f(\pi)=-\pi$ $\quad f(e)=e$

$f(2)=1$ $\quad f(-\pi)=\pi$

ES:

(*) $[f(x)]^2 = x^2$ soluzioni: non solo $f(x)=x$ e $f(x)=-x$

ma anche $f(x)=\begin{cases} x & x\in S \\ -x & x\notin S \end{cases}$ per ogni $S\subseteq\mathbb{R}$

Data una soluzione f di (*), definiamo $S:=\{x : f(x)=x\}$

Bisogna far vedere che per $x\notin S$, $f(x)=-x$

$(f(x)+x)(f(x)-x)=0$ se non è uguale a 0 :| secondo fattore, dev'essere il primo

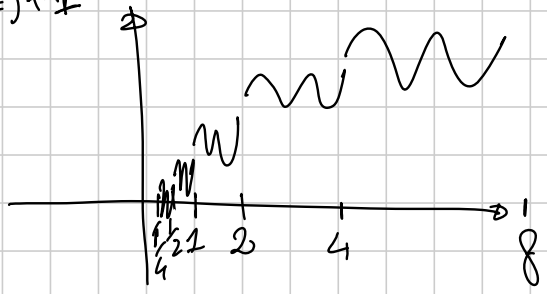
---

$f:(1,\infty)\to\mathbb{R}$: $f(x^2)-f(x)=1$ $\forall x\in$ dominio

Scriviamo $x=e^z$ $z\in(0,\infty)$

$f(e^{2z})-f(e^z)=1$ definisco $g(z):=f(e^z)$

(**) $g(2z)=g(z)+1$ $\quad g:(0,\infty)\to\mathbb{R}$



Posso definire arbitrariamente la g in $[1,2)$.

A questo punto, la relazione (**) mi dice quanto vale la funzione in $[2,4)$, $[4,8)$, ecc. $[\frac{1}{2},1)$, $[\frac{1}{4},\frac{1}{2})$, ecc.

Costruzione delle soluzioni brutte dell'equazione di Cauchy.

Idea: prendo un insieme di reali "libero da relazioni razionali"

per es. $\{1, \sqrt{2}, \sqrt{3}\}$: non esistono $a, b, c \in \mathbb{Q}$

tali che $1 \cdot a + \sqrt{2} \cdot b + \sqrt{3} \cdot c = 0$ (a perde $a=b=c=0$)

e consideriamo l'insieme

$$S = \{x : x = 1 \cdot a + \sqrt{2} \cdot b + \sqrt{3} \cdot c : a, b, c \in \mathbb{Q}\}$$

sono tutti distinti : se $1a_1 + \sqrt{2} b_1 + \sqrt{3} c_1 = 1 \cdot a_2 + \sqrt{2} \cdot b_2 + \sqrt{3} \cdot c_2$

allora faccio la differenza...

Sono in grado di costruire una soluzione di

$$(C) \quad f(x+y) = f(x) + f(y) \qquad x, y \in S \qquad f : S \to \mathbb{R}$$

che non sia una retta: scelgo in modo arbitrario

$f(1)$, $f(\sqrt{2})$, $f(\sqrt{3})$, e definisco $\forall x \in S$

$$f(x) = f(1 \cdot a + \sqrt{2} \cdot b + \sqrt{3} \cdot c) = a \cdot f(1) + b \cdot f(\sqrt{2}) + c \cdot f(\sqrt{3}).$$

Per ogni $x, y \in S$, se $x = a_1 \cdot 1 + b_1 \cdot \sqrt{2} + c_1 \sqrt{3}$

$y = a_2 \cdot 1 + b_2 \cdot \sqrt{2} + c_2 \cdot \sqrt{3}$

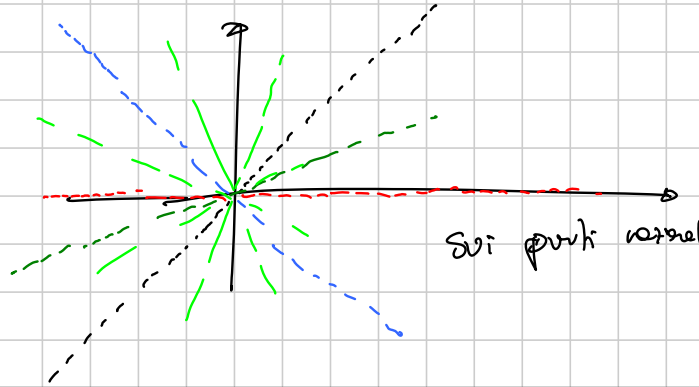
allora $RHS = (a_1 + a_2) f(1) + (b_1 + b_2) f(\sqrt{2}) + (c_1 + c_2) f(\sqrt{3})$

$$LHS = f(x+y) = f((a_1+a_2) \cdot 1 + (b_1+b_2)\sqrt{2} + (c_1+c_2)\sqrt{3}) = (a_1+a_2) \cdot f(1) + (b_1+b_2) f(\sqrt{2}) + (c_1+c_2) \cdot f(\sqrt{3})$$

$f(1) = 1$

$f(\sqrt{2}) = 0$

$f(\sqrt{3}) = -1$



sui punti razionali: $q = q \cdot 1 + 0 \cdot \sqrt{2} + 0 \cdot \sqrt{3}$

$$f(q) = q \cdot f(1) = q$$

sui punti della forma $q\cdot\sqrt{2}$: $f(q\sqrt{2})=0$

sui punti della forma $q\cdot(1+\sqrt{2})$, $q\in\mathbb{Q}$

$$f\left(q\left(1+\sqrt{2}\right)\right)=q\cdot f(1)+q\cdot f(\sqrt{2})=q$$

per ogni $\alpha,\beta\in\mathbb{Z}$, i punti della forma $q(\alpha+\beta\sqrt{2})$, $q\in\mathbb{Q}$, hanno una retta con coeff. ang. $\frac{\alpha}{\alpha+\beta\sqrt{2}}$

Posso ingrandire sempre questo insieme: es,

$$\{1,\sqrt{2},\sqrt{3}\}\to\{1,\sqrt{2},\sqrt{3},\sqrt{5}-1\}\to\{1,\sqrt{2},\sqrt{3},\sqrt{5}-1,\pi\}$$

Si riesce a costruire un insieme di "generatori" di questo tipo per tutto $\mathbb{R}$, si chiama <u>base di HAMEL</u>

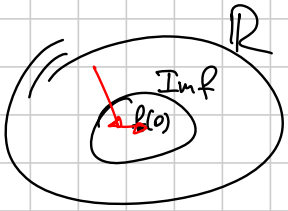
TI: esistono soluzioni non costanti di

$$f(xy+f(x))=f(7xy)\qquad\forall x,y\in\mathbb{R}\ ?$$

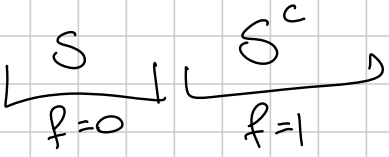
$P(x,0)$: $f(f(x))=f(0)$

$P(1,y)$: $f(y+f(1))=f(7y)$

$a=f(1)$ $7y$ e $a+y$ hanno la stessa immagine



$P(2,y)$: $f(2y+f(2))=f(14y)$



BMO07 $f:\mathbb{R}\to\mathbb{R}$

$$f(f(x)+y)=f(f(x)-y)+4yf(x)\qquad P(x,y)$$

$P(x, f(x))$: $f(2f(x)) = f(0) + 4[f(x)]^2$

⚠ NO! Pongo $2f(x) = z$ e ottengo $f(z) = f(0) + z^2$

Idea cruciale:

$\mathbb{R} = \mathrm{Im}\, f - \mathrm{Im}\, f$: ogni $z \in \mathbb{R}$ si scrive come $f(\text{roba}) - f(\text{roba})$

Dim:

$P\left(b, \frac{a}{4f(b)}\right)$: $f(\text{roba}) = f(\text{roba}) - a$ (se $f(b) \neq 0$)

$\star$ $f(f(x)+y) = f(f(x)-y) + 4yf(x)$

Sostituzione truccosa: $P(x, 2f(z) - f(x))$

$f(2f(z)) = f(2f(x) - 2f(z)) + 4 \cdot (2f(z) - f(x)) \cdot f(x)$ Max

$P(x, f(y))$: $f(f(x)+f(y)) = f(f(x)-f(y)) + 4f(y)f(x)$

$= f(f(y)+f(x)) = f(f(y)-f(x)) + 4f(x)f(y)$

Grazie al lemma $\Rightarrow$ $f(\underbrace{f(x)-f(y)}_{a}) = f(\underbrace{f(y)-f(x)}_{-a})$ $\forall a \in \mathbb{R}$

$P(a, f(b)+f(c))$: $P(a, f(b)+w)$

$f(f(a)+f(b)+f(c)) = f(f(a)-f(b)-f(c)) + 4f(a)f(b) + 4f(a)f(c)$

$P(b, f(a)+f(c))$: $P(b, f(a)+w)$

$f(f(b)+f(a)+f(c)) = f(f(b)-f(a)-f(c)) + 4f(b)f(a) + 4f(b)f(c)$

$\Rightarrow f(f(a)-f(b)-f(c)) + 4f(a)f(c) = f(f(b)-f(a)-f(c)) + 4f(b)f(c)$

$f(f(a)-f(b)-f(c)) + 4(f(a)-f(b))f(c) = f(f(b)-f(a)-f(c))$

$\forall a, b, c \in \mathbb{R}$

LENTA

$f(z-f(c))+4zf(c)=f(+z+f(c))$ Ripeto con w al posto di $f(c)$

$f(z-w)+4zw=f(z+w)$ facile concludere (poni $z=w$)

SL2005 $f:\mathbb{R}^+\to\mathbb{R}^+$

$$f(x)f(y)=2f\left(x+yf(x)\right) \qquad \forall x,y\in\mathbb{R}^+$$

Riesco a porre $y=x+yf(x)$?

Sì, se scelgo $y=\frac{x}{1-f(x)}$ (e se $f(x)<1$)

Dato x t.c. $f(x)<1$, scrivo $P\left(x,\frac{x}{1-f(x)}\right)$

$$f(x)\,f(y)=2f(y) \Rightarrow f(x)=2 \text{, assurdo ?!}$$

$\Rightarrow f(x)$ non è mai minore di 1.

Se $a,b\in \mathrm{Im}\,f$, allora $\frac{ab}{2}\in \mathrm{Im}\,f$ (dalla P)

e anche $\frac{a}{2}\cdot\frac{ab}{2}$, e anche $\frac{a}{2}\cdot\frac{a}{2}\cdot\frac{ab}{2}$, ... $\left(\frac{a}{2}\right)^n\cdot b$

Se avessi $a<2$, allora per un n abbastanza grande

$\left(\frac{a}{2}\right)^n b$ sta nell'immagine ed è minore di 1. $\Rightarrow$ assurdo

$\Rightarrow \mathrm{Im}\,f\subseteq[2,\infty)$.

Supponiamo per ora $\mathrm{Im}\,f\subseteq(2,\infty)$

TESTO: $2f(x)<f(x)f(y)=2f\left(x+yf(x)\right)$

$\Rightarrow f(x)<f\left(x+yf(x)\right)$

Per ogni $z>x$, posso scrivere

$P\left(x,\frac{z-x}{f(x)}\right)$: $2f(x)<f(x)f\left(\frac{z-x}{f(x)}\right)=2f(z)$ $\Rightarrow f(x)<f(z)$

$$2f\big(y+xf(y)\big) = f(x)f(y) = 2f\big(x+yf(x)\big)$$

strett. crescente $\Rightarrow$ iniettive

uguali

$$y+xf(y) = x+yf(x)$$

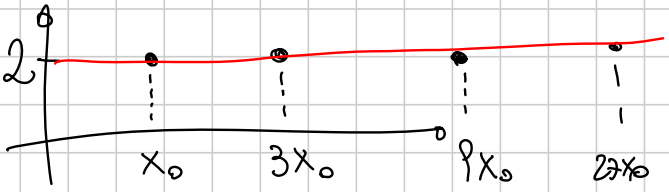
e da qui si finisce facilmente

- se $2 \in \operatorname{Im} f$,

Dato x_0 tale che $f(x_0)=2$, ho

$P(x_0, x_0)$: $2^2 = 2 \cdot f\big(x_0 + x_0 f(x_0)\big)$

$\Rightarrow$ anche $f(3x_0) = 2 \cdot 2$



Crescente (debole in questo caso) $\Rightarrow$ soluzione.

Induttivamente, $f(3^k x_0) = 2 \quad \forall\, k \in \mathbb{N}$

Analogamente a sopra, si dimostra che f è (debolmente) crescente

$\forall\, y \in \mathbb{R}$, esisterà k tale che $y < 3^k x_0$

$$\Rightarrow \quad 2 \leq f(y) \leq f(3^{k+1} x_0) = 2. \quad \square$$

per i lemmi di sopra sui valori nell'immagine

SL01: $f : \mathbb{R} \to \mathbb{R}$ t.c.

$$f(xy)\big(f(x)-f(y)\big) = (x-y) f(x) f(y)$$

$P(x,1)$: $f(x)\big[f(x)-f(1)\big] = (x-1) f(x) f(1)$

$\Rightarrow$ $f(x) \cdot f(x) = x \cdot f(x) \cdot f(1)$ $\qquad a := f(1)$

$$f(x) = \begin{cases} 0 & x \notin S \\ a \cdot x & x \in S \end{cases}$$

(suppongo $a = f(1) \neq 0$, altrimenti f è banalmente costante)

Chiamiamo S l'insieme t.c. $f(x) \neq 0$ $\quad 0 \notin S$

Se $x \neq y$, $x, y \in S$, allora $xy \in S$.

Se $x \in S$, allora $x^{-1} \in S$

Dato qualunque S che è un sottogruppo moltiplicativo di $\mathbb{R}$,

$f(x) = \begin{cases} 0 & x \notin S \\ ax & x \in S \end{cases}$ è soluzione (verificare!).

C1 Medium [Tess]

Titolo nota 29/12/2011

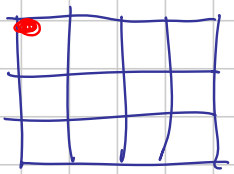
Contare oggetti geometrici

Iran TST 2013 3.14

Sono disegnati n rettangoli distinti

Dimostrare che il numero di angoli retti distinti sono almeno $\lceil 4\sqrt{n} \rceil$

Euristica Random



quanti rettangoli ce l'hanno come angolo?

R: basta scegliere l'angolo opposto

i rettangoli potrebbero essere non paralleli (sono contento)

Formalmente: raggruppo i rettangoli per classe di parallelismo

n_1 , n_2 , n_3 - - - -

supponiamo di aver risolto quando i rettangoli sono tutti //

$\Rightarrow$

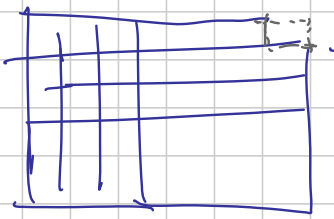
$$\#\text{angoli distinti} \begin{cases} \_1 \geq \lceil 4\sqrt{n_1} \rceil \\ \_2 \geq \lceil 4\sqrt{n_2} \rceil \\ \_3 \geq \text{- - -} \\ \vdots \end{cases}$$

Σ : totale angoli $\geq 4\left(\sum \sqrt{n_i}\right) \geq 4\sqrt{n}$

Mi posso dimenticare di $\lceil \ \rceil$, perché gli angoli sono in quant. intera

Ora contiamo le coppie di angoli: A B

la griglia parziale la estendo



ci sono a_1 angoli di tipo A

" a_2 "

ci sono b_2 angoli di tipo B

ogni rettango identifica univocamente una coppia (A, B)

$$\Rightarrow \quad \#\text{rett} \leq \sum_{\text{righe}} a_{\text{riga minore}} \cdot \left(\sum_{\text{righe}} b_{\text{riga maggiore}} \right)$$

$$= \sum_{i<j} a_i b_j$$

$$n \leq \sum_{i<j} a_i b_j$$

$$a_i b_j \leq \left(\frac{a_i + b_j}{2} \right)^2$$

$$\leq \frac{\left(\sum a_i + \sum b_i \right)^2}{2}$$

$\sqrt{2n} \leq$ numero di angol. di tipo A e B

l'altra stima su tipo C e D conclude

× casa: i dettagli

IMO 2014 6

n rette generiche sul piano ne coloro k di blu

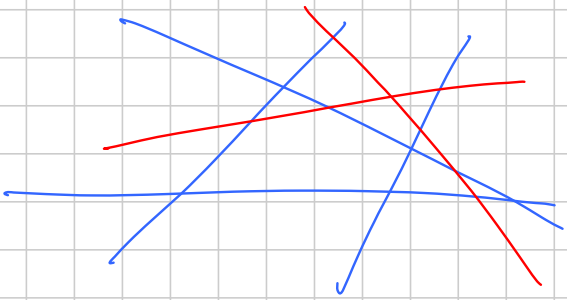
succede che nessuna regione limitata è completam. circondata di blu. Quanto può essere grande k?

MS: 1 pt $k \geq C n^{\alpha}$ $\alpha > 0$

2 pt $k \geq C n^{\frac{1}{2}}$

4 pt $k \geq \sqrt{\frac{n}{2}}$

7 pt $k \geq \sqrt{n}$



$$X = \{ (C, R) : C \text{ è config. di rette blu e } R \text{ è una regione blu di } C \}$$

$$|X| = \sum_C \text{numero di regioni blu in } C$$

$$\geq \sum_C 1 = |\text{insieme delle } C| = \binom{n}{k}$$

$$|X| = \sum_R \text{numero di config. che rendono blu } R$$

$$= \sum_R \binom{n - b(R)}{k - b(R)}$$

$$\leq \sum_R \binom{n-3}{k-3} = \binom{n-3}{k-3} \cdot \#\text{regioni limitate}$$

$$\leq \frac{(n-1)(n-2)}{2}$$

x caso

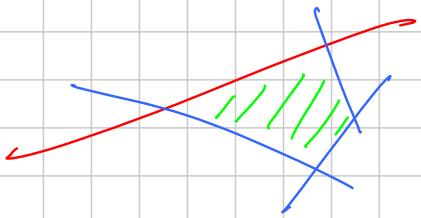
$$\binom{n}{k} \leq |X| \leq \binom{n-3}{k-3} \frac{(n-1)(n-2)}{2}$$

semplificando $\quad n \leq k\frac{(k-1)(k-2)}{2} \quad C \leq C' k^3$

$$k \geq \alpha n^{1/3}$$

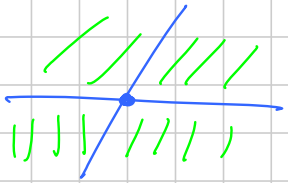
Idea: scegliere una configurazione massimale di rette blu.

Se C è massimale



Contiamo le $= n-k$

ad ogni regione verde associo un'inters. blu



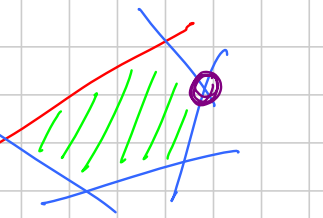
ogni $\cap$ è scelta al massimo 4 volte

$$\#\{(\text{regione } ///, \cap)\} \leq 4 \#\cap = 4\binom{k}{2}$$

$$n-k \leq 2k(k-2)$$

$k \geq \sqrt{\frac{n}{2}}$

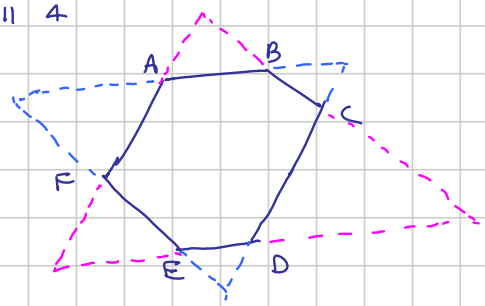
Per migliorare scegliamo meglio la mappa



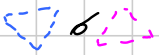
x casa: fate la stima con la nuova scelta di: $\cap$

BMO 2011 4

Es:



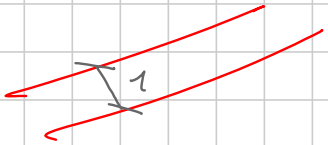
 ha area 1

Th:  ha area $\geq \frac{3}{2}$

Scegliere oggetti estremali

BMO 2010 3

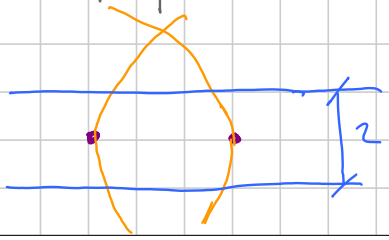
Finiti punti nel piano. Ogni terna di punti è contenuta in una striscia larga 1.



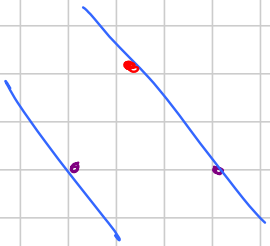
Th: dimostrare che tutti i punti stanno in una striscia larga 2.

Idea fondamentale: prendere la coppia con distanza massima

ora scelgo



per ogni altro punto voglio sperare che rientri in questa



il rosso sta dentro la nostra fascia?

per massimalità l'altezza , corrisp. alla base massima è la minima del triangolo e dunque l'altezza ↑

IMO 2013 2

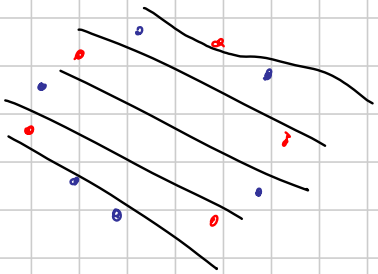
Ci sono 2013 pt e 2014 pt. Vi vengono date k rette da disegnare senza passare per i punti colorati. (a 3 a 3 NON allineati)

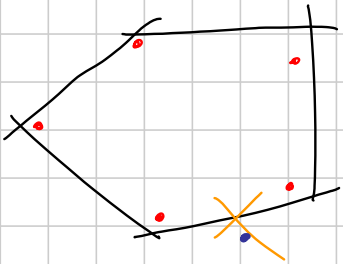
Quante ve ne servono per suddividere tutte le coppie di punti di colori diversi?

Idea fondamentale: inviluppo convesso

spesso i punti sul bordo dell'inviluppo convesso sono interessanti

Esempio:

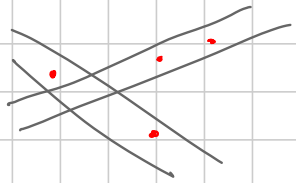




abbiamo $k \geq 2013$

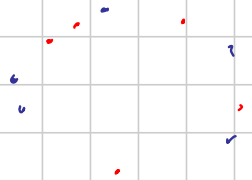
possiamo usare 2 rette (parallele alla congiung.) per separare 2 punti dagli altri;

perché? perché ho solo finiti punti e non sono allineati



Già ora abbiamo sempre una costr. con $k \geq 2 \lfloor \frac{n}{2} \rfloor$

Migliora la costruzione all'inizio:



qui separare 1 rosso costa 1 retta

altrimenti il convex hull è tutto •, ne separo 2 e lavoro sui blu.

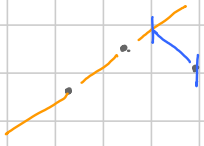
Thm di Sylvester

L'insieme di punti $A \subseteq$ piano è finito e gode della seg.

$\forall\ p_1, p_2 \in A$, $\exists\ p_3 \in A$ allineato con p_1, p_2

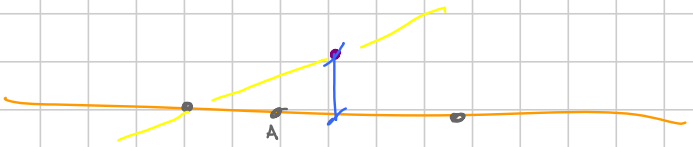
Th: allora $A \subseteq$ retta.

Idea: considerare una distanza minima



fra le finite coppie (retta r, punto p) dove retta fra 2 pt. in A, punto $\in A$

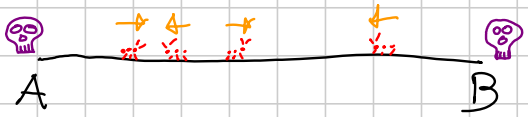
prendiamo quella che minimizza la dist. fra p e r.



violazione della minimalità di $(\_\_, \cdot)$
perché $(\_\_, A)$

Invarianti

Folklore



le formiche che toccano A, B muoiono
formiche che si scontrano si girano istantaneamente

Quanto tempo impiegano prima di morire tutte?

Invariante: i semini vanno dritti perché si scambiano a contatto
il tempo è facilmente controllabile dal cammino dei semini

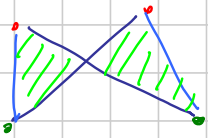
IMOSL 2014 7

n punti sul piano a 3 a 3 non allineati
ci sono n segmenti che li congiungono in modo che ogni punto è estremo di esattamente 2 segmenti

Domanda: il processo termina?

Vera domanda: dimostrare che termina in $\leq \frac{n^3}{4}$ mosse.

Domanda 1: classico



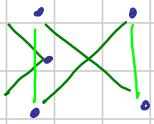
solo finite possibilità per le lunghezze di segmenti (in tot)

Oss: questo invariante dà troppa poca informazione per il bound $\frac{n^3}{4}$

abbiamo un bound $> (n-1)!$

Idea discretizzare l'invariante

idea 1: contare tutte le intersezioni fra segmenti



niente da fare

idea 2: guardare le intersezioni con i prolungamenti

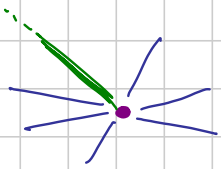
considerazione 1: i segmenti cambiano, quindi anche le rette su cui stanno

considerazione 2: devo tener conto dei segmenti

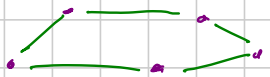
Q = numero di |inters.| fra segmenti tracciati e le (*)

rette fra qualsiasi coppie di punti.

considerazione 3



vorrei contarle O

()

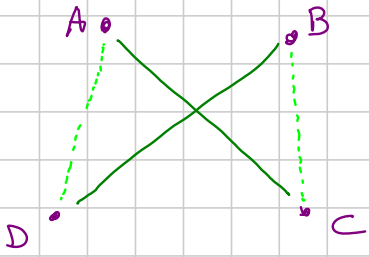
(*) non agli estremi del segmento

i) quanto fa al massimo Q

ii) far vedere che scende abbastanza in fretta

i) $Q \leq$ #rette · #segm. $\leq \binom{n}{2} n < \frac{n^3}{2}$

ii) Hope: ad ogni mossa Q scende di almeno 2



n_{xy} = numero di inters. fra le rette e il segm. xy

$n_{AC} + n_{BD} \geq 2 + n_{AD} + n_{BC}$

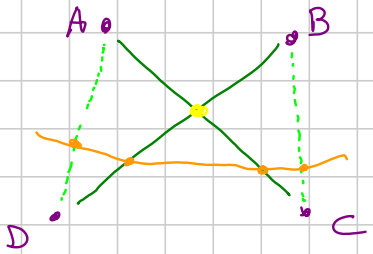
N_{xy} = l'insieme delle rette che toccano xy (al suo interno)

$n_{xy} = |N_{xy}|$

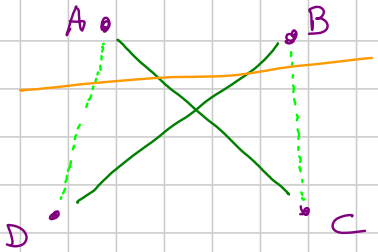
A) $|N_{AC} \cup N_{BD}| \geq 2 + |N_{AD} \cup N_{BC}|$

B) $|N_{AC} \cap N_{BD}| \geq |N_{AD} \cap N_{BC}|$

A)

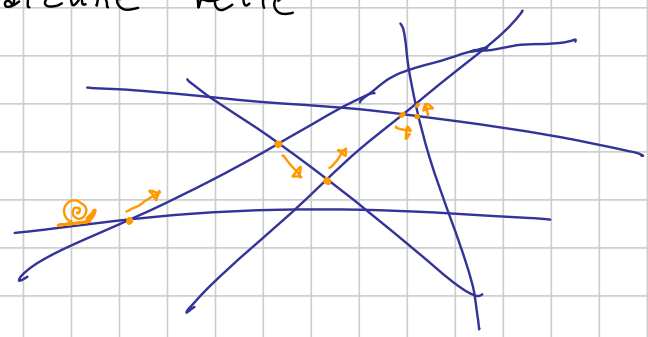


B)



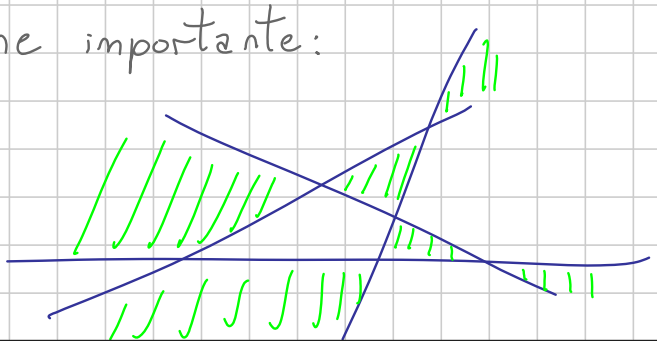
EGMO 2017 3

La chiocciola "Turbo" cammina alla sua massima velocità su alcune rette



Th: dimostrare che non può percorrere uno segmento in entrambe le direzioni.

Colorazione importante:



costruiamola induttivamente !

P.B. tutto bianco!

P.I. per ip. ind., se tolgo una retta ho una colorazione che va bene per k-1 rette

aggiungo l'ultima retta e inverto i colori su una delle 2 metà
⇒ ∀ segmento che esisteva già prima la condizione di colori diversi è mantenuta
∀ segmento della nuova retta ho invertito solo una delle 2 regioni

Altro modo: geometria analitica

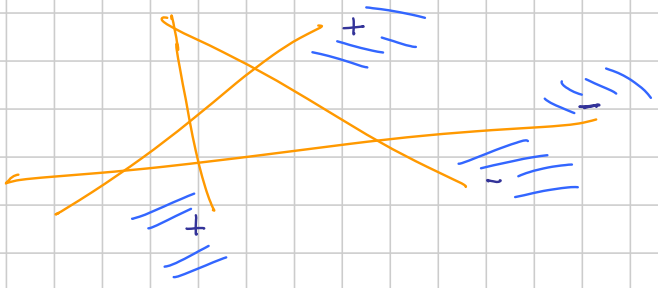
ogni retta è identificata da un'equazione cartesiana $E(x,y) = 0$

e i 2 semipiani individuati corrisp. a $E(x,y) > 0$, $E(x,y) < 0$

tante rette corr. a tante equaz.

$E_1(x,y)$
$E_2(x,y)$
⋮
$E_k(x,y)$

le regioni sono identificate dall'intersez. di alcuni semipiani (uno per ogni retta)



(alcune scelte danno $\cap = \emptyset$)

il colore di ogni regione lo assegno con la parità dei segni

autom. funziona!

Oss: la stessa colorazione funziona con anche altri tipi di equazione

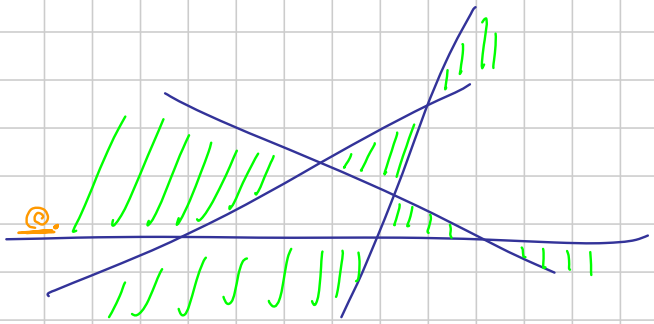
l'unica condizione è che il segno di F cambi da una parte all'altra

Oss: il teorema dei 4 colori ha bisogno di 4 colori!

Continuiamo l'EGMO

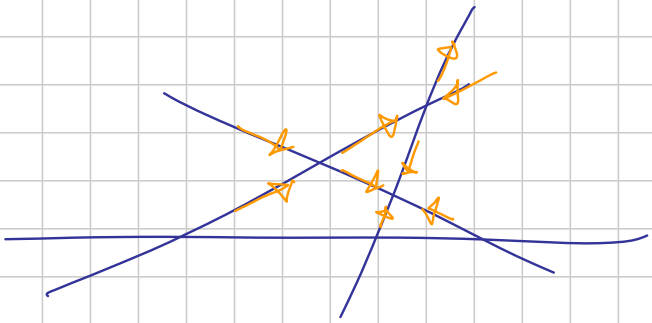
L'invariante è

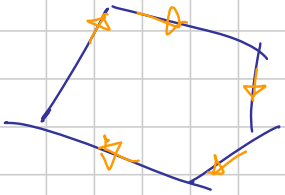
avere il /// a sinistra



Altro approccio

direzionare le porzioni di retta in modo che tutti gli incroci siano "a sella"





ho tutte selle $\Rightarrow$ bordo percorribile

se ho tutti i bordi percorribili $\Rightarrow$ regioni adiacenti si percorrono nell'altro senso

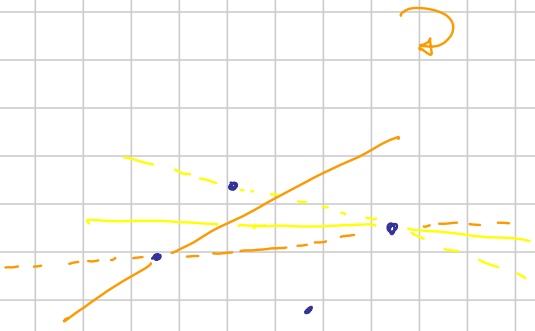
posso colorare le regioni dei colori "orario" e "antior."

Se parto da una colorazione alternante, ritrovo i punti di sella!

IMO 2011 2

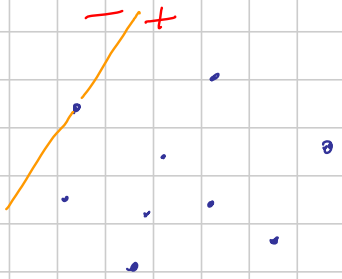
$n \geq 2$ punti sul piano

c'è una retta che si chiama "mulino a vento"



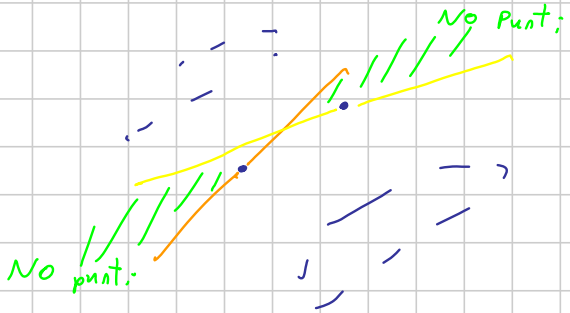
Th: dimostrare che esiste una config. iniziale a partire dalla quale la retta tocca tutti i punti

Cerchiamo invarianti e config. che non toccano tutti i punti



l'invariante qui è che tutti i punt. stanno dallo stesso lato

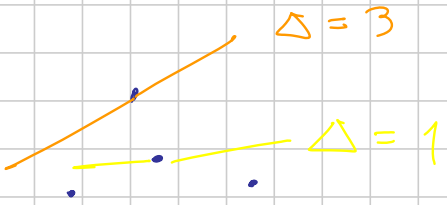
in generale



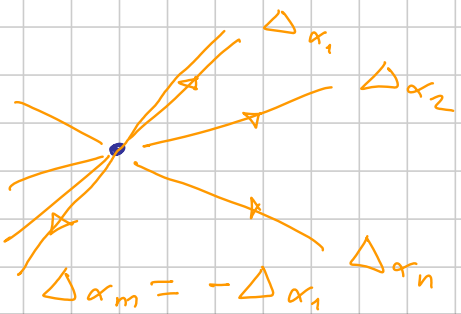
l'invariante è la diff. Δ di punt. tra lato + e −

Quindi non vanno bene le conf. in cui

la Δ iniziale non viene mai presa per almeno un punto



Vorrei iniziare con $\Delta = 0$ n dispari (Δ minimo)
$= \pm 1$ n pari

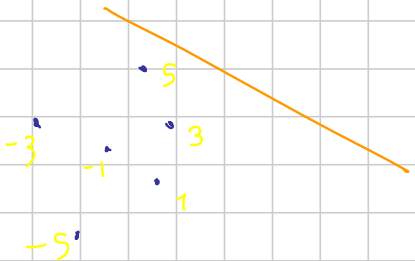


fra l'angolo α_1 e α_m, la quant. Δ si è avvicinata di molto allo 0

(- caso continuo: tocco lo 0
- $|\Delta_{min}| \leq 1$)

Ora si conclude facilmente perché

- la retta visita tutte le angolazioni,
- $\forall$ angolazione ho 1 vertice che ha Δ_{min}



- $\forall$ vertice $\exists$ 1 angolazione buona

C2 Medium [Tess]

Titolo nota 07/09/2019

Pigeonhole

1 Dimostrare che esiste $N \in \mathbb{Z}_{>0}$ t.c. N si può scrivere come somma di 2015 potenze 2014-esime in ≥ 2016 modi diversi.

2 In un paese ci sono solo 2 lettere A, M e le parole hanno ≤ 2019 lettere la concatenazione di 2 parole non è mai una parola. Quante parole al max?

3 In un altro paese ci sono 2^N bandiere che sono formate da $1 \times N$ quadretti ciascuno colorato di giallo o blu. $(N \geq 4)$ Quante ne devo prendere a caso affinché ne possa prelevare N tali che trovo la diagonale monocromatica?

1 ITAMO 2014 5

posso scegliere 2015 interi distinti come basi $(\leq K)$

e calcolarne la somma delle potenze 2014

è una mappa $f: A \longrightarrow B$

$|A| = \binom{K}{2015}$ $\quad |B| \leq 2015 \cdot K^{2014}$

2 TF 2014

Chiaramente posso scegliere solo parole con lungh. $> \frac{L}{2}$

è un insieme buono e sto escludendo $2^{\lfloor \frac{L}{2} \rfloor + 1} - 2$

Se ho una parola più piccola P

X , $P+X$ (concatenazione) non posso averle entrambe

$\forall X$ t.c. $\ell(X+P) \le L$

$\ell(X) \le L - \ell(P)$

Quanti vincoli esclusivi? Sono $2^{L-\ell(P)+1} - 2$

Il punto è che tutti i vincoli $(X, P+X)$ sono disgiunti

3 IMOSL 2010 2

A mano, per $N=4$, $K=5$

Non può essere $K \le 2^{N-2}$ perché se scelgo 2 colonne una gialla, l'altra blu non ho diag. monocr.

lower bound

Vorrei $K = 2^{N-2}+1$

Voglio costruire la bandiera $\square$ con diag. per induzione

quindi brucio una colonna e mi tengo solo le righe che hanno wlog blu (se sono almeno $2^{N-3}+1$ pigeonhole)

Ora l'ip. induttiva mi garantisce un quadrato con diagonale grande $N-1$

(se la diag. è gialla, mi occorreva almeno un punto giallo)

Lemma dei matrimoni (Hall):

Boys GIRLS

ciascun ragazzo ha delle preferenze $r_i \to G_i \subseteq G$

vogliamo un accoppiamento che comprenda tutto B.

La condizione affinché ne esista uno è

$$\forall\ S \subseteq B \qquad \left| \bigcup_{i \in S} G_i \right| \geq |S|$$

Dim:

Necessità: ovvia (condizione verificata per un accoppiamento)

Sufficienza: induzione estesa su $|B|$

caso 1 - $\exists$ una "$=$" nella condizione $\forall$, nel sottoins. S, allora per ip. ind. su S e B/S ho gli accoppiamenti per entrambi

caso 2 - $\nexists$ $=$.
scelgo 1 coppia a caso e valuto la condizione su $B \setminus \{b\}$

3 nuovo approccio:

devo accoppiare righe e colonne

1 situazione (1 poss. acc.) collego le colonne alle righe se nell'inters. c'è il blu

2 " (2° poss. acc.) " giallo

Ora controlliamo le ipotesi di Hall. Se non riesco ad acc.
$\exists$ $C_g \subseteq$ colonne e $C_b \subseteq$ colonne t.c.

$$|P(C_g)| < |C_g| \quad \text{e} \quad |P(C_b)| < |C_b|$$

se $\exists$ $c \in C_g \cap C_b$

tutte le righe si collegano a c, dall'altra

$$\text{n° righe} \leq 1 \cup | \leq |P(C_g)| + |P(C_b)| \leq |C_g| + |C_b| - 2 \leq 2N - 2$$

4 $S \subseteq \mathbb{Z}$, $|S| = 2019$ allora $\exists$ $T \subseteq S$, $T \neq \emptyset$ t.c.
$2019 \mid \sum_{t \in T} t$

5 $A \subseteq \{1, \dots, n\}$ fissato. Una A-partizione di n in k parti è
$n = p_1 + \dots + p_k$ con $p_i \in A$ dove $k = |\{p_i\}|$
È ottimale se k è il minimo possibile.
Dimostrare che $k \leq \sqrt[3]{6n}$ per A-partizioni ottimali

6 Una catena di sottoinsiemi di A è $S_1 \subseteq \dots \subseteq S_h$.
Quante catene occorrono per ricoprire $\mathcal{P}(A)$, con $|A| = n$?

4 Grande classico

Prendo una catena $\{a_1\} \subseteq \dots \subseteq S$

è lunga $|S|$, o ho già trovato un sottoins. con somma $\equiv 0$ oppure 2 hanno la stessa classe mod $|S|$

Quindi la differenza va bene!

5 IMOSL 13 C4

Consideriamo una partizione ottimale

Posso assumere $A = |\{p_i\}|$

allora l'ottimalità significa che non posso "raccogliere" termini

$$\sum_{i \in I} p_i = \sum_{j \in J} p_j \quad \text{con } |I| < |J|$$

l'idea di come applicare pigeonhole è prendere

$\forall$ cardinalità di $|I|$ voglio tanti sottoinsiemi con somme diverse ⊛

tutte queste somme sono $\leq n$

$$f : \mathcal{P}(A) \to \{1, \dots, n\}$$

$Y = \bigcup \{\text{insiemi scelti ⊛}\}$

il bound che trovo sarà $|Y| \leq n$

$g(|A|) = g(k)$

vorrei che $g(k) \geq \frac{k^3}{6}$

Come trovo molti sottoinsiemi con cardinalità fissata $= s$ e somme diverse?

$a_1 < a_2 \dots < a_k$

somma minore con s

poi gli altri sottoinsiemi con somma via via crescente li prendo alzando il + grande disponibile

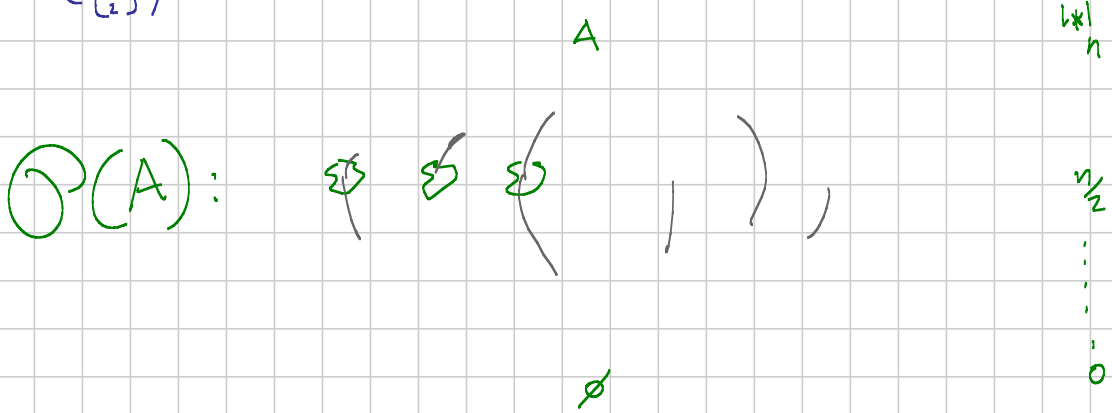
6 teorema noto

La risposta si indovina facilmente: $\binom{n}{\lfloor \frac{n}{2} \rfloor}$

$\geq \binom{n}{\lfloor \frac{n}{2} \rfloor}$ perché nessuna catena coinvolge + di un insieme con la stessa card.

e $\binom{n}{\lfloor \frac{n}{2} \rfloor} = \max_i \binom{n}{i}$

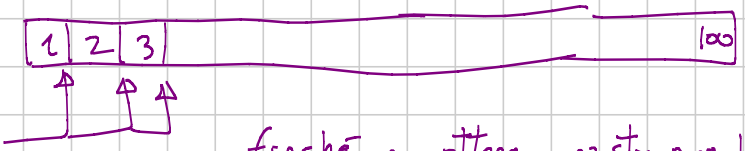
$\leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$ Per costruire le catene vrene in aiuto Hall



l'accoppiamento è fatto fra card. $k < \lfloor \frac{n}{2} \rfloor$ e $k+1$

devo valutare $\forall$ scelta di sottoins. con card. $=k$
ne devono esistere almeno altrettanti che contengono almeno 1
e di card $= k+1$

Double - Counting

7 Una striscia: 

viene piegata finché non ottengo una str. preg. larga 1
Ora scriviamo i numeri nell'ordine dall'alto al basso.
Dimostrare che $2^{100} \leq$ # permut. ottenibili $\leq 4^{100}$

8 Selezioniamo un sottografo G della maglia infinita 
con $E(G) = e$
dimostrare che $\frac{e}{2} \leq \min\left(V(G) - CC(G)\right) \leq \frac{e}{2} + \sqrt{\frac{e}{2}} + 1$

IRAN TST 2017 1.6

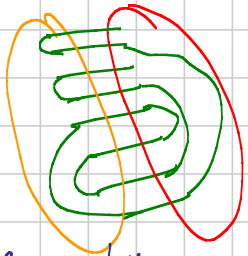
7 Piego in ordine dalla fine e ho sempre almeno 2 possibilità

2^{99} modi

Piego solo il 100 in 2 modi
incollo il 99 e il 100 e questi modi mi garantiscono sempre 2 possibilità per estendere una perm. ott. con 99 in una da 100
$\Rightarrow$ per induzione ho # ottenibili$(100) \geq 2^k \cdot$ #ottenibili$(100-k)$

il P.B. funziona con 5

Per l'upper bound

la conf. finale: 

posso stimare con catalan a sx e a dx

.... il numero di ottenibili $\leq C_{50} \cdot C_{48} \cdot \binom{50}{2}$
Hope! $\leq 4^{100}$

8 IRAN TST 2015 1.5

Lavoriamo su una componente connessa.

$$\frac{e}{2} \le \min(VC_G) - 1 \le \frac{e}{2} + \sqrt{\frac{e}{2}} + 1$$

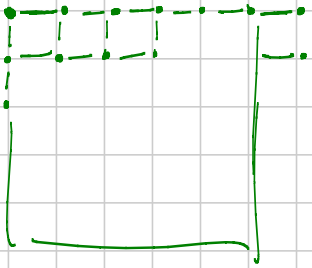
$|\#\text{colonne occupate} + \#\text{lati}| \le \text{vertici}$ (come somma per ogni colonna)

$\#\text{righe} + \#\text{lati} - \le \text{vertici}$ (" riga)

$$c + r + e \le 2v$$

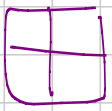
$$\frac{c+r}{2} + \frac{e}{2} \le v$$

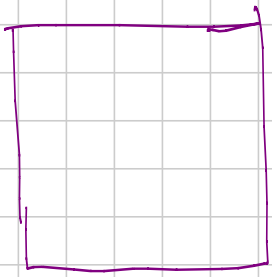
Per l'esempio che minimizza scelgo 1 grafo connesso il più vicino possibile al □



x casa: $\frac{e}{2} + \sqrt{\frac{e}{2}} \le VC_G)$

9 Inseriamo i numeri $1, \dots, 25$ in:





e contiamo le somme nei

e prendiamo la massima

Quanto vale al minimo?

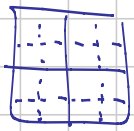
10

$$\begin{array}{ccccccc} & & & 4 & & & \\ & & 2 & & 6 & & \\ & 5 & & 7 & & 1 & \\ 8 & & 3 & & 10 & & 9 \end{array}$$

Si riesce a costruire un triangolo con 2019 righe?

9 ITATST 2019 6

Problema graticolo: se avessi avuto una tabella 4×4

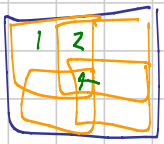


somma i 4 2×2 agli angoli $= C = 1 + \dots + 16$

$\Rightarrow$ almeno 1 ha $\geq \left\lceil \frac{C}{4} \right\rceil$

$1 + \dots + 16 = C \leq 4 \cdot M$

2 Problema graticolo: nel 3×3



$1 \cdot (\dots) + 2(\dots) + 4 \dots = S \leq 4 \cdot M$

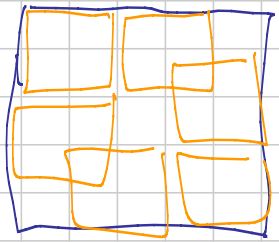
$= \sum_{i=1}^{16} p_i n_i = \sum p_i \cdot i$

per riarrang. $\geq 1 \cdot (9 + 8 + \dots) + 2(\dots) + 4 \cdot 1$

Problema vero:

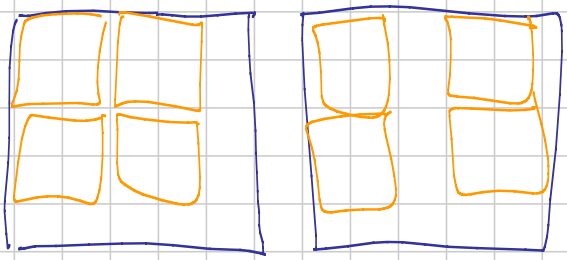
1° tentativo: sommo tutti i 2×2 e ottengo $M \geq 41$

2° tentativo: prendo meno $\square$

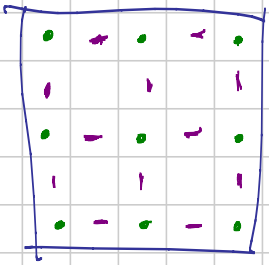


$M \geq 43$

3° tentativo:



scelgo sempre riga e colonna diverse



viene $M \geq 45$

(10) IMO 2018 3 (C4 shortlist)

4
2 6
5 7 1
8 3 10 9

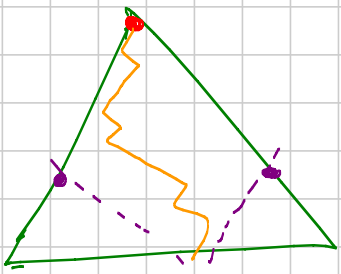
osserviamo il max deve stare sulla riga in fondo

ogni volta che prendo un numero non in fondo deve avere un numero più grosso di lui sotto

se parto dall'alto e scendo così ottengo questa stima

$1 + 2 + \dots + n \leq$ cima $+ \sum_{\text{strade scartate}} = F \leq \binom{n+1}{2}$

I numeri + piccoli $(1, 2, \dots, n)$ sono vincolati a indicare la strada verso il più grande



l'assurdo è già al secondo passo

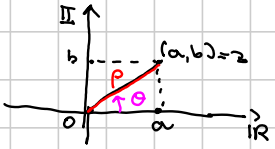
GM1 - Complessi e baricentriche

Titolo nota 30/12/2011

Complessi

Def.

Ripasso ① $z = a + bi$ $\quad a, b \in \mathbb{R}$ a p. IReale, b p. Immag.



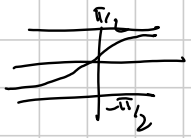
i un simbolo che soddisfa $i^2 = -1$.

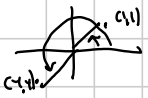
② $z = \rho e^{i\theta}$ $\quad \rho \in \mathbb{R}_{>0}$, $\theta \in [0, 2\pi)$

$\rho \to$ modulo $\to$ distanza (sul p.d. Gauss di z dall'origine)

$\theta \to$ argomento $\to$ angolo (in senso antiorario) fra semiasse positivo IR e la retta oz.

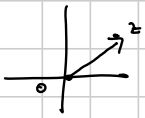
Passare da uno all'altro: $\begin{cases} a = \rho\cos\theta \\ b = \rho\sin\theta \end{cases}$ - $\begin{cases} \rho = \sqrt{a^2+b^2} \\ \theta = \tan^{-1}\frac{b}{a} \end{cases}$





Oss. "Numeri complessi $\overset{\text{identificheremo}}{\equiv}$ punti sul piano $\equiv$ vettori"

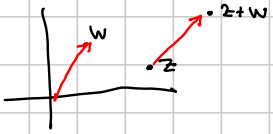
$z \longleftrightarrow (a,b) \longleftrightarrow \vec{oz}$



Operazioni:

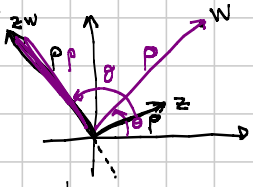
Fisso w numero complesso, $w = \rho e^{i\theta}$

Ⓐ $z \mapsto z + w$ è una traslazione di vettore w.



Ⓑ $z \mapsto zw$ è una rotomotetia di angolo θ (in senso antiorario, e ragione ρ) di centro l'origine,

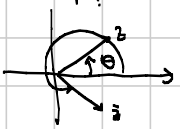
Oss. Moltiplicare per i = rotazione attorno all'origine di $\frac{\pi}{2}$ in senso antiorario.



Ⓒ $z \mapsto \bar{z}$ Riflessione rispetto all'asse reale

$z = a + bi = \rho e^{i\theta}$

$\bar{z} = a - bi = \rho e^{-i\theta}$



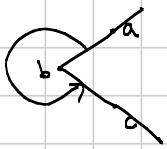
Ⓓ $z \mapsto z^{-1}$ Inversione di centro o e raggio 1

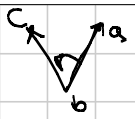
Es. Scrivere la riflessione attorno a II.

Angoli e similitudini

Oss. Ⓐ $g(z) = \frac{z}{w}$. Se $z = \rho e^{i\theta}$ $\quad g(z) = e^{a \cdot i\theta}$

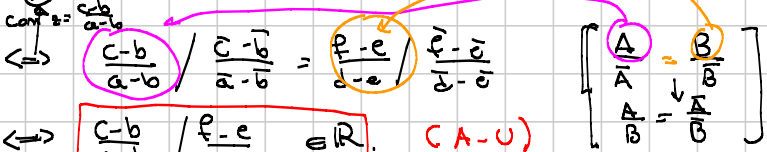
Ⓑ $\angle abc$ = l'angolo di cui devo ruotare la retta ab attorno a b (in senso antiorario) per perdere coincidenza con la retta bc.





Eq. angolo: $\boxed{c-b = (a-b)\,e^{i\angle abc}\cdot\rho} \to$ dove $\rho = \frac{|\vec{cb}|}{|\vec{ab}|}$ $\Rightarrow \frac{c-b}{a-b} = \rho e^{i\angle abc}$

Cons. 1. $\theta = \angle abc$, $e^{2i\theta} = \frac{c-b}{a-b} \Big/ \frac{\bar{c}-\bar{b}}{\bar{a}-\bar{b}}$



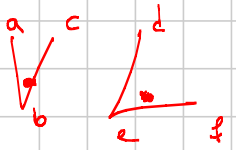
$\angle abc = \angle def \iff \frac{c-b}{a-b} \Big/ \frac{\bar{c}-\bar{b}}{\bar{a}-\bar{b}} = \frac{f-e}{d-e} \Big/ \frac{\bar{f}-\bar{e}}{\bar{d}-\bar{e}}$

$\iff \boxed{\frac{c-b}{a-b} \Big/ \frac{f-e}{d-e} \in \mathbb{R}}$. (A-U)

Oss. $e^{2i\theta} = e^{2i\theta'} \iff \theta - \theta' = k\pi \quad k \in \mathbb{Z}$

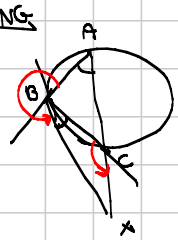
C'è l'ambiguità "$\theta - \theta' = \pi$". Però dati a, b, c $\angle abc$ o $\angle cba$ è convenzione secondo la quale intendiamo, in base al problema facendo, di scegliere i versi in modo che l'angolo sia $< \pi$ altrimenti non c'è più ambiguità.

Cons. 2. Eq. angolo $\begin{matrix} abc \\ def \end{matrix}$ $\begin{matrix} abc \to \frac{c-b}{a-b} = \frac{|\vec{cb}|}{|\vec{ab}|} e^{i\angle abc} \\ def \to \frac{f-e}{d-e} = \frac{|\vec{fe}|}{|\vec{de}|} e^{i\angle def} \end{matrix}$



Quindi per il I Crit. sim. $abc \underset{\text{diretti}}{\sim} def \iff \boxed{\frac{c-b}{a-b} = \frac{f-e}{d-e}}$ (D-S)

ATTENZIONE



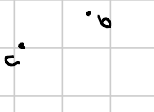
$A\hat{B}x \sim B\hat{C}x \quad \angle abx \neq \angle bcx$

Per i triangoli simili basta aggiungere un – a uno dei due termini.

Parallelismi e Perpendicolarità

(1) abc allineati $\iff \angle abc = \pi \overset{\text{Eq. angolo}}{\iff} \frac{c-b}{a-b} \Big/ \frac{\bar{c}-\bar{b}}{\bar{a}-\bar{b}} = -1 \iff \frac{c-b}{a-b} = \frac{\bar{c}-\bar{b}}{\bar{a}-\bar{b}}$

$\iff \frac{c-b}{a-b} \in \mathbb{R}$.



(Es.) $ab \parallel cd \iff \frac{d-c}{b-a} = \frac{\bar{d}-\bar{c}}{\bar{b}-\bar{a}} \quad \left[\iff \frac{d-c}{b-a} \in \mathbb{R}\right]$

(2) $ab \perp bc \overset{\text{Eq. ang.}}{\iff} -1 = \frac{c-b}{a-b} \Big/ \frac{\bar{c}-\bar{b}}{\bar{a}-\bar{b}} \iff \frac{c-b}{a-b} = -\frac{\bar{c}-\bar{b}}{\bar{a}-\bar{b}}$

$\iff \frac{c-b}{a-b} \in i\mathbb{R}$ [$\mathbb{R}i$]

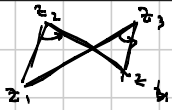
(Es.) $ab \perp cd \iff \frac{d-c}{b-a} = -\frac{\bar{d}-\bar{c}}{\bar{b}-\bar{a}}$

Birapporti e circonferenze

Def. $[z_1, z_2, z_3, z_4] \overset{\text{def}}{=} \frac{z_1 - z_2}{z_3 - z_2} \cdot \frac{z_3 - z_4}{z_1 - z_4}$

Lemma z_1, z_2, z_3, z_4 cocicl. $\iff [z_1, z_2, z_3, z_4] \in \mathbb{R}$.

Segue da $\angle abc = \angle def \iff \frac{c-b}{a-b} \Big/ \frac{f-e}{d-e}$ è reale.



$z_1 z_2 z_3 z_4$ ciclico $\iff \angle z_1 z_2 z_4 = \angle z_1 z_3 z_4 \iff [z_1, z_2, z_3, z_4] \in \mathbb{R}$.

Circonferenza unitaria e scelta delle coordinate

Circonf. unitaria $z\bar{z} = 1$ ($|z|^2$) $\quad [z\bar{z} = a^2+b^2]$

Molto spesso Cfr circoscritta = Cfr unitaria o circocentro → origine.

Domanda: Chi è h?

Da "Retta di Eulero" $h + 2O = 3G$, $\boxed{G = \frac{a+b+c}{3}}$ e quindi

$h + O = a+b+c \rightsquigarrow h = a+b+c$ (NIENTE)

Es l'incentro proclo remind. in vettori $\vec{I} = \frac{a\vec{A}+b\vec{B}+c\vec{C}}{a+b+c}$ a,b,c sono le lunghezze dei lati

Notazione u,v,w. p

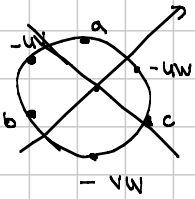
Lemma Dato abc triangolo [a,b,c sono i C che identificano i vertici] o circocentro è l'origine.

$\exists\, u,v,w$ complessi t.c. $\begin{cases} a = u^2 \\ b = v^2 \\ c = w^2 \\ i = -(uv+vw+uw) \end{cases}$

Oss. i punti medi degli archi sono $\pm uv, \pm vw, \pm uw$

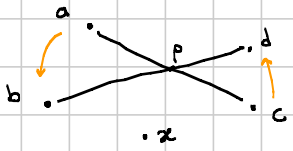
Es. Scriv. i tre excentri

Idea di dim.



Cercato u,v,w C cfr unitaria in modo che $-uv$ sia p.to medio di $\overset{\frown}{ab}$ che non contiene c e analogo usando l'info simmetrica che l'incentro è l'ortocentro dei punti medi: $-uv, -vw, -uw$.

Es 1



$abcd$ no par.

- Mostrare che $\exists!$ rotomotetia che manda $a \to b$, $c \to d$
- Il centro di questa rotomotetia è

$$x = \frac{ad-bc}{a+d-b-c}$$

e il n. C che ha come modulo la ragione di questa rotomotetia e come argomento l'angolo di rotazione è

$$\alpha = \frac{b-d}{a-c}$$

$p = ac \cap bd$

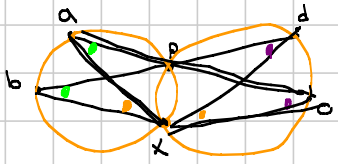
- x è l'intersezione di $\odot abp \cap \odot cpd$.

Sol: $\begin{cases} b-x = (a-x)\alpha \\ d-x = (c-x)\alpha \end{cases} \Rightarrow \frac{b-x}{a-x} = \frac{d-x}{c-x} \Rightarrow bc-(b+c)x+x^2 = ad-(a+d)x+x^2$

$\Rightarrow x(a+d-b-c) = ad-bc$

$\Rightarrow x = \frac{ad-bc}{a+d-b-c}$

Facendo i conti si ottiene $\alpha = \frac{b-d}{a-c}$

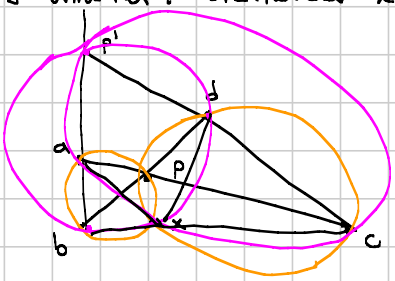


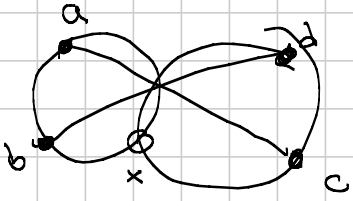
$$\left[\begin{array}{l} a \to b \\ c \to d \end{array} \middle| \begin{array}{l} x = \frac{ad-bc}{a+d-b-c} \\ \alpha = \frac{b-d}{a-c} \end{array} \right] \quad \left| \begin{array}{l} a \to c \\ b \to d \end{array} \right. \left[x = \frac{ad-bc}{a+d-b-c} \right] \quad \left| \begin{array}{l} \\ \alpha = \frac{c-d}{a-b} \end{array} \right.$$

Vedete gli altri

Mostro $X\hat{A}C \sim X\hat{B}D$. Infatti $\angle XAC = \angle XAP = \angle XBP = \angle XBD$ e anal. $\angle XCA = \angle XDB$.

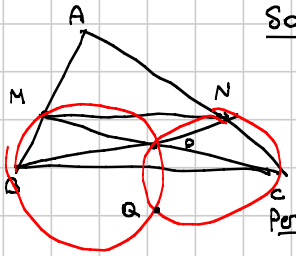
Quindi $\exists$ una rot. che manda $\widehat{XAC} \rightsquigarrow \widehat{XBD}$ e quindi manda $A \to B$, $C \to D$.





Cosa salvare?
Se so $a,b,c,d \to x = \dfrac{ad-bc}{a+d-b-c}$

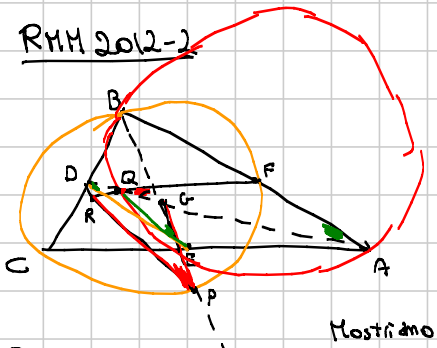
BMO 2009-2 Mostre $\angle BAQ = \angle PAC$, Hp. $MN \parallel BC$, $P = MC \cap BN$, $Q = \odot BMP \cap \odot CNP$.



Sol! Complessi:
a = origine $= 0$
b, c
$\exists \lambda \in \mathbb{R}$ $m = \lambda b$, $n = \lambda c$ poiché $MN \parallel BC$
Per primo $q = \dfrac{mn-bc}{m+n-b-c} = \dfrac{\lambda^2 bc - bc}{\lambda b + \lambda c - b - c} = \dfrac{(\lambda^2-1)bc}{(\lambda-1)(b+c)} = \dfrac{(\lambda+1)bc}{b+c}$

$p = ?$ p è l'intersezione di mc con bn $\begin{cases} p \in mc \\ p \in bn \end{cases}$
Siccome dobbiamo mostrare $\angle BAQ = \angle PAC$, possiamo anche sostituire P con un punto p' su AP e mostrare $\angle BAQ = \angle p'AC$. Però AP è mediana C per $ceva$ e quindi prendo $p' = 2M_{BC} = b+c$
$\angle BAQ = \angle PAC \iff \dfrac{q-a}{b-a} \Big/ \dfrac{c-a}{p-a} \in \mathbb{R} \iff \dfrac{\frac{(\lambda+1)bc}{b+c}}{b} \Big/ \dfrac{c}{b+c} \in \mathbb{R}$ ✓
$(\lambda+1)\dfrac{bc}{b+c} \cdot \dfrac{1}{b} \cdot \dfrac{1}{c}(b+c)$

RMM 2012-2



D, E, F p.ti medi
$P = BE \cap \odot BCF$, $Q = \odot ABE \cap AD$
$R = FQ \cap DP$
Mostra che G sta su $\odot DQR$.

Sol!
Mostriamo che $\angle GPD = \angle GQF$. Come troviamo P e Q?
[Provate a imporre $Q \in AD + Q BAE$ ciclico.]
Può anche prendere un'altra strada ... G, Q, D allineati. e D lo so!
Magari le riesco a dire qualcosa su $|GQ|$ ... Il fatto è che
$G \hat{D} E \sim G \hat{E} Q$! Perché $\begin{cases} \angle GDE = \angle GAB = \angle QEG \\ \hat{G} \text{ in comune.} \end{cases}$ ($DE \parallel AB$)
Questo suggerisce di mettere l'origine in g! $g = 0$ origine

Geometria 1 (Medium) – Gioacchino Antonelli

d, e, f i p.ti medi $\quad \boxed{d+e+f=0}$.

$G\hat{D}E \sim G\hat{E}Q \Rightarrow GQ \cdot GD = GE^2 \Rightarrow q = \frac{d}{|d|}\frac{|GB|^2}{|GD|} = \frac{1}{|d|}\cdot\frac{|e|^2}{|d|} = \frac{d\cdot e\bar{e}}{d\bar{d}} = e\frac{\bar{e}}{\bar{d}}$

Analogamente $p = f\frac{\bar{f}}{\bar{e}}$

Vogliamo $\angle GPD = \angle GQF \iff \frac{d-p}{g-p} \Big/ \frac{f-q}{g-q} \in \mathbb{R} \iff \frac{d-f\frac{\bar{f}}{\bar{e}}}{-f\frac{\bar{f}}{\bar{e}}} \Big/ \frac{f-e\frac{\bar{e}}{\bar{d}}}{-e\frac{\bar{e}}{\bar{d}}} \in \mathbb{R}$

$\iff \frac{d\bar{e}-f\bar{f}}{-f\bar{f}} \Big/ \frac{df-e\bar{e}}{-e\bar{e}} \in \mathbb{R} \iff \frac{e\bar{e}(d\bar{e}-f\bar{f})}{f\bar{f}(df-e\bar{e})} \in \mathbb{R} \iff \frac{d\bar{e}-f\bar{f}}{df-e\bar{e}} \in \mathbb{R}$

$d = -e-f$ poiché $d+e+f=0$. $\quad \overset{\text{II}}{\underset{\text{I}}{\cdot}}$

$\frac{(-e-f)\bar{e}-f\bar{f}}{(-\bar{e}-\bar{f})f-e\bar{e}} \in \mathbb{R} \iff \frac{-e\bar{e}-f\bar{e}-f\bar{f}}{-\bar{e}f-f\bar{f}-e\bar{e}} \in \mathbb{R}$ ✓

Oss. Perché $d+e+f=0$? In generale $g = \frac{a+b+c}{3}$, $d = \frac{b+c}{2}$, $e = \frac{a+c}{2}$, $f = \frac{a+b}{2}$

Quindi $d+e+f = a+b+c$. Se $g=0$, allora $\frac{a+b+c}{3} = 0 \to a+b+c = 0$

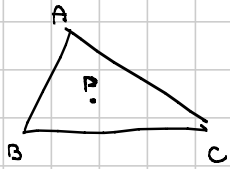
e quindi se $g=0$, $d+e+f=0$.

Coordinate baricentriche

Def. ① $[u:v:w]$ terna omogenea, tre numeri reali non tutti nulli.

$[a:b:c] = [u:v:w]$ se $\exists k \in \mathbb{R}\setminus\{0\}$ t.c. $u=ka$, $v=kb$, $w=kc$

Def.



$P \in$ piano di ABC

② $|BCP|$ indica l'area (con segno) del triangolo $B\hat{C}P$. Il segno è + se B, C, P sono ordinati come A, B, C, - altrimenti.

③ **C-B:** Le coord. bar. di P sono $[|BCP| : |CAP| : |APB|]$

④ Not. Conway $\quad S_A = \frac{b^2+c^2-a^2}{2} = \left[\frac{b^2+c^2-a^2}{2bc}\right]\cdot bc = bc\cos\alpha$

$S_B = \frac{a^2+c^2-b^2}{2}$

$S_C = \frac{a^2+b^2-c^2}{2}$

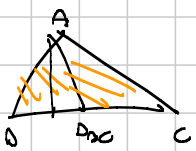
Es. $S_AS_B + S_AS_C + S_BS_C = 4\,\mathrm{Area}^2_{ABC}$

⑤ α, β, γ sono gli angoli $\hat{A}, \hat{B}, \hat{C}$

a, b, c sono (le lunghezze dei) lati BC, CA, AB

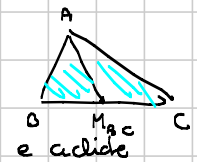
Alcuni punti

- $A = [1:0:0]$, $B = [0:1:0]$, $C = [0:0:1]$
- $M_{BC} = [0:1:1]$ e ciclidi

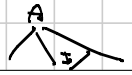


- D_{BC} piede bar.: $= [0 : |CD_{BC}A| : |AD_{BC}B|]$

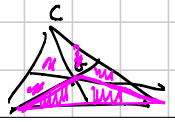
$\frac{|CD_{BC}A|}{|AD_{BC}B|} = \frac{CD_{BC}}{D_{BC}D} = \frac{b}{c}$ $\quad = [0:b:c]$ e ciclidi



- $G = [1:1:1]$



- $I = [|BC| : |CA| : |AB|]$



raggio inscritto

$= \left[\frac{BC\cdot r}{2} : \frac{CA\cdot r}{2} : \frac{AB\cdot r}{2}\right] = [a:b:c]$

- $H = [|BCH| : \text{circ.}] = \left[\frac{BC\cdot HH_A}{2} : \text{circ.}\right] = \left[\frac{ac\cos\beta\cos\gamma}{2\sin\gamma} : \text{circ.}\right]$

$= [aR\cos\beta\cos\gamma : \text{circ.}] = [a\cos\beta\cos\gamma : \text{circ.}] =$

$\frac{HH_A}{\cos\gamma} = \frac{BH_A}{\sin\gamma} \Rightarrow HH_A = BH_A\frac{\cos\gamma}{\sin\gamma} = \frac{AB\cos\beta\cos\gamma}{\sin\gamma} = \frac{c\cos\beta\cos\gamma}{\sin\gamma}$

$= \left[\frac{a}{\cos\alpha} : \frac{b}{\cos\beta} : \frac{c}{\cos\gamma}\right] = \left[\frac{2R\sin A}{\cos\alpha} : \frac{2R\sin B}{\cos\beta} : \frac{2R\sin\gamma}{\cos\gamma}\right] =$

$\left[\frac{a}{\frac{S_A}{bc}} : \frac{b}{\frac{S_B}{ac}} : \frac{c}{\frac{S_C}{ab}}\right] = [\tan\alpha : \tan\beta : \tan\gamma]$

$\left[\frac{abc}{S_A} : \frac{abc}{S_B} : \frac{abc}{S_C}\right] = \left[\frac{1}{S_A} : \frac{1}{S_B} : \frac{1}{S_C}\right] = [S_BS_C : S_AS_C : S_AS_B]$

Somme Convesse quando usiamo le coordinate erealte

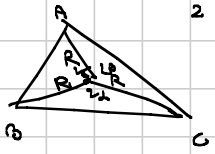
$16S^2 = (p(p-a)(p-b)(p-c) = \frac{1}{16}(-a^4-b^4-c^4+2a^2b^2+2b^2c^2+2a^2c^2) = S_AS_B+S_BS_C+S_CS_A$

$(a+b+c)(a+b-c)(a-b+c)(-a+b+c)$
$[(a+b)^2-c^2][c^2-(a-b)^2]$
$(a^2+b^2-c^2+2ab)(c^2-a^2-b^2+2ab)$
$4a^2b^2-(a^2+b^2-c^2)^2$

$O = \left[\frac{R^2\sin 2\alpha}{2} : \frac{R^2\sin 2\beta}{2} : \frac{R^2\sin 2\gamma}{2}\right] = [\sin 2\alpha : \sin 2\beta : \sin 2\gamma] =$

$= [\sin\alpha\cos\alpha : \text{circ.}] = \left[\sin\alpha\frac{S_A}{bc} : \text{circ.}\right] = [a\sin\alpha S_A : \text{circ.}] =$

$= \left[\frac{a^2}{2A}S_A : \text{circ.}\right] = [a^2S_A : b^2S_B : c^2S_C]$

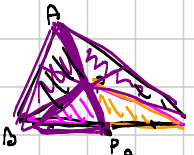


Oss. $a^2S_A+b^2S_B+c^2S_C = \sum_{ciclica} a^2\left(\frac{b^2+c^2-a^2}{2}\right) =$

$= -\frac{a^4}{2}-\frac{b^4}{2}-\frac{c^4}{2}+a^2b^2+b^2c^2+a^2c^2 = 8S^2$ ← area

Oss. / Def. $P = [x:y:z]$ si dicono coordinate erealte di P se $x+y+z=1$

Oss. P ha coord. erealte $[x:y:z]$ $\quad \vec{P} = x\vec{A}+y\vec{B}+z\vec{C}$ [Esercizio]



Oss. Per fare i punti medi vale che $\frac{\text{somma coordinate}}{2}$ a patto che le coordinate abbiano la stessa somma.

N = p.to medio ob

$O = \left[\frac{a^2S_A}{8S^2} : \text{circ.}\right]$

$H = \left[\frac{S_BS_C}{4S^2} : \text{circ.}\right]$

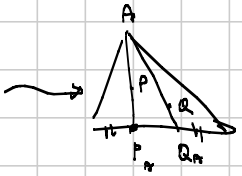
$N = \left[\frac{a^2S_A}{8S^2}+\frac{S_BS_C}{4S^2} : \text{circ.}\right] = \left[a^2S_A+2S_BS_C : \text{circ.}\right] = \left[a^2(b^2+c^2-a^2)+(a^2+c^2-b^2)(a^2+b^2-c^2) : \text{circ.}\right]$

$= [a^2b^2+a^2c^2-a^4+a^4+a^2b^2-a^2c^2+a^2c^2+b^2c^2-c^4 = a^2b^2-b^4+b^2c^2 : \text{c.c.}]$

$= [-c^4-b^4+2b^2c^2+a^2b^2+a^2c^2 : \text{c.c.}]$ q.e.

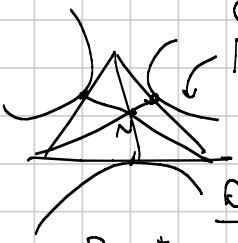
↳ Oss. $P=[x:y:z] \longrightarrow$ $AP\cap BC=[0:y:z]$
$BP\cap AC=[x:0:z]$
$CP\cap AB=[x:y:0]$

Es. 1 $[x:y:z]$ ortogonale $\left[\frac{a^2}{x}:\frac{b^2}{y}:\frac{c^2}{z}\right]$
isot. $\left[\frac{1}{x}:\frac{1}{y}:\frac{1}{z}\right]$



Es. 2 $I_A=[-a:b:c]$ e ciclici
$L=[a^2:b^2:c^2]$
$Ge=\left[\frac{1}{p-a}:\frac{1}{p-b}:\frac{1}{p-c}\right]=[(p-b)(p-c):\text{ciclici}]$
$Na=[p-a:p-b:p-c]$

Lemoine? → imt. simmediane



Oss. $[1:-1:0]$ chi è?

Pensate a come abbiamo definito le coord. baricentriche
$P \longrightarrow [|PBC|:|CAP|:|ABP|]$.
Quanto vale $|BCP|+|CAP|+|ABP|=S\neq 0$. Se faccio così si vede non posso invece avere $[x:y:z]$ t.c. $x+y+z=0$.
Diciamo che i p.ti t.c. $x+y+z=0$ sono p.ti all'∞.

Esercizio: Vicenza data $[x:y:z]$ $x+y+z\neq 0$ $\exists!$ P t.c. $[|PBC|:|CAP|:|ABP|]=[x:y:z]$

Thread: Eurotile 6
Evan Chen

Rette
- Una generica retta ha equazione $[lx+my+nz=0]$ $l,m,n\in\mathbb{R}$
- P.to all'∞ di $lx+my+nz=0$ è $[m-n:n-l:l-m]$
- Intersezione $\begin{cases} lx+my+nz=0 \\ l'x+m'y+n'z=0 \end{cases}$ e non sono una multipla dell'altra
$\begin{pmatrix} m & n \\ m' & n' \end{pmatrix}$ $-\begin{pmatrix} l & n \\ l' & n' \end{pmatrix}$ $\begin{pmatrix} l & m \\ l' & m' \end{pmatrix}$
si intersecano nel punto $[n'm-nm':nl'-n'l:lm'-l'm]$

Oss. se ho 2 rette parallele ! è all'∞
(A) Come vedere che 2 rette sono $\parallel$? Hanno lo stesso p.to all'∞

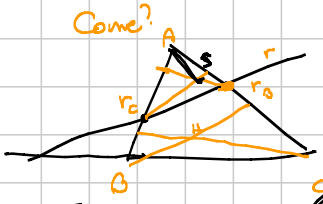
- Retta per 2 punti: $[a:b:c]$, $[a':b':c']$
$$\left[\det\begin{pmatrix} a & b & c \\ a' & b' & c' \\ x & y & z \end{pmatrix}=0\right]$$
e quindi 3 p.ti sono allineati se il det della matrice che ha per righe le coord. mate dei punti fa zero
- Retta parallela a $lx+my+nz=0$ passante per $[a:b:c]$
$$\det\begin{pmatrix} m-n & n-l & l-m \\ a & b & c \\ x & y & z \end{pmatrix}=0$$

(Esercizio) $r: px+qy+rz=0 \to$ p.to all'∞ è $[f:g:h]=[q-r:r-p:p-q]$

Allora il p.to all'∞ di una retta perpendicolare a r è

$[S_B g - S_C h : S_C h - S_A f : S_A f - S_B g]$.

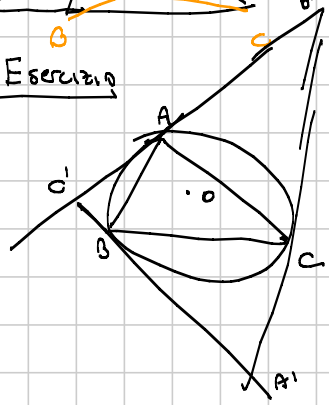
Come?



retta $\perp$ CH passante per r_B ∩ retta $\perp$ BH passante per r_C = S

p.to all'∞ della perp di r è p.to all'∞ di AS.

Esercizio



Trovare A', B', C' vertici del triangolo tangenziale

Sol. Scriviamo l'eq. della tg in A

Troviamo ∞_{OA} e $\infty_{\perp,OA}$ e poi fare retta per A, $\infty_{\perp,OA}$.

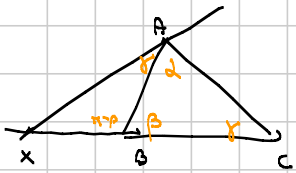
$O=[a^2S_A : b^2S_B : c^2S_C]$

$OA: \quad c^2S_C\, y - b^2S_B\, z = 0 \qquad l=0,\ m=c^2S_C,\ n=-b^2S_B$

$\infty_{OA}=[c^2S_C+b^2S_B : -b^2S_B : -c^2S_C]$

$\infty_{\perp,OA}=[-b^2S_B^2+c^2S_C^2 : \dots]$

È un po' contorto.



$\frac{BX}{\sin\gamma}=\frac{AX}{\sin\beta}$

$\frac{CX}{\sin(\alpha+\gamma)}=\frac{AX}{\sin\gamma}$

$X=[|BXC|:|CXA|:|AXB|]=$

$=[0:-CX:XB]$

$=[0:-AX\frac{\sin\beta}{\sin\gamma}:AX\frac{\sin\gamma}{\sin\beta}]$

$=[0:-\sin^2\beta:\sin^2\gamma]=$

$=[0:-b^2:c^2]$

$AX \to$

$1,0,0 \quad 0,-b^2,c^2$

$c^2y+b^2z=0$

le altre sono

$c^2x+a^2z=0$

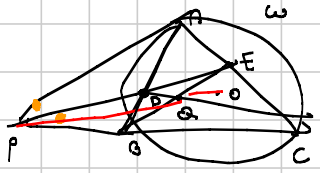
$b^2x+a^2y=0$

e i vertici sono $[a^2:b^2:-c^2]$, $[a^2:-b^2:c^2]$, $[-a^2:b^2:c^2]$

$[a^2:b^2:c^2]$

$[\ :\ 0:0]$

MOP 2006



PA tg. ω

bis. $\angle APB$ interseca AB, AC in P, E risp.

P, D, E allineati, $D\in AB$, $E\in AC$, PDE bisettrice

$Q=BE\cap PC$

PQ, O allineati

Sol. Thesi: Calcolare $\angle BAC$.

P è, come prima, $[0:b^2:-c^2]$

D si trova con il th bisettrice in APB. $\frac{AD}{DB}=\frac{AP}{PB}=\frac{\sin\beta}{\sin\gamma}=\frac{b}{c}$

quindi $D=[c:b:0]$. Analogamente $E=[b:0:c]$.

$[bc:b^2:0]$ $\qquad [bc:0:c^2]$

Quindi $Q=[bc:b^2:c^2]$

P.Q.D. $\Leftrightarrow \begin{pmatrix} 0 & b^2 & -c^2 \\ bc & b^2 & c^2 \\ a^2 S_A & b^2 S_B & c^2 S_C \end{pmatrix} = 0 \iff \begin{pmatrix} 0 & 1 & -1 \\ bc & 1 & 1 \\ a^2 S_A & S_B & S_C \end{pmatrix} = 0$

$\Leftrightarrow 2a^2 S_A - bc S_B - bc S_C = 0 \Leftrightarrow$

$\Leftrightarrow 2a^2 S_A - a^2 bc = 0 \Leftrightarrow$ ($S_A + S_C = a^2$)

$\Leftrightarrow 2S_A = bc \Leftrightarrow$

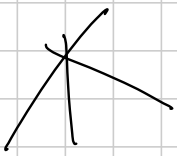
$\Leftrightarrow \frac{S_A}{bc} = \frac{1}{2} \Leftrightarrow \cos\alpha = \frac{1}{2} \Leftrightarrow$

$\Leftrightarrow \alpha = 60°.$ □

G2 - MEDIUM PROIETTIVA

Titolo nota 09/09/2019

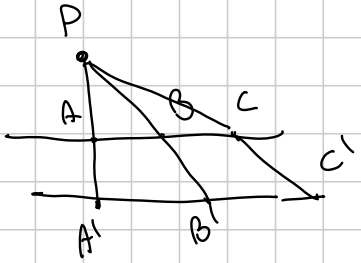
• r, s, t concorrono oppure r, s, t parallele



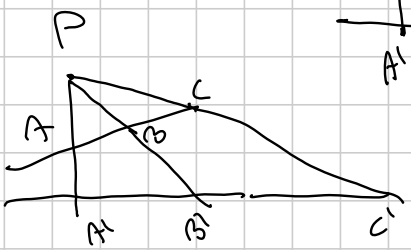
rette proiettive = rette ∪ {punto all'infinito}

piano proiettivo = piano ∪ retta all'infinito

• Omotetie



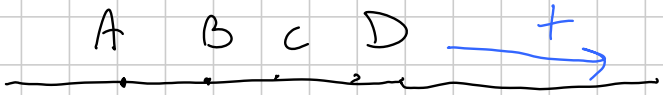
$AB \parallel A'B'$ $\quad \frac{AB}{A'B'} = \frac{BC}{B'C'}$



$AB = BC$

$\times$ $A'B' = B'C'$ NO!

Birapporto



$$(A, B; C, D) = \frac{\frac{AC}{AD}}{\frac{BC}{BD}} = \frac{AC \cdot BD}{BC \cdot AD}$$

I segmenti vanno presi con segno!

$AB > 0 \quad AB = -BA$

$BA < 0$

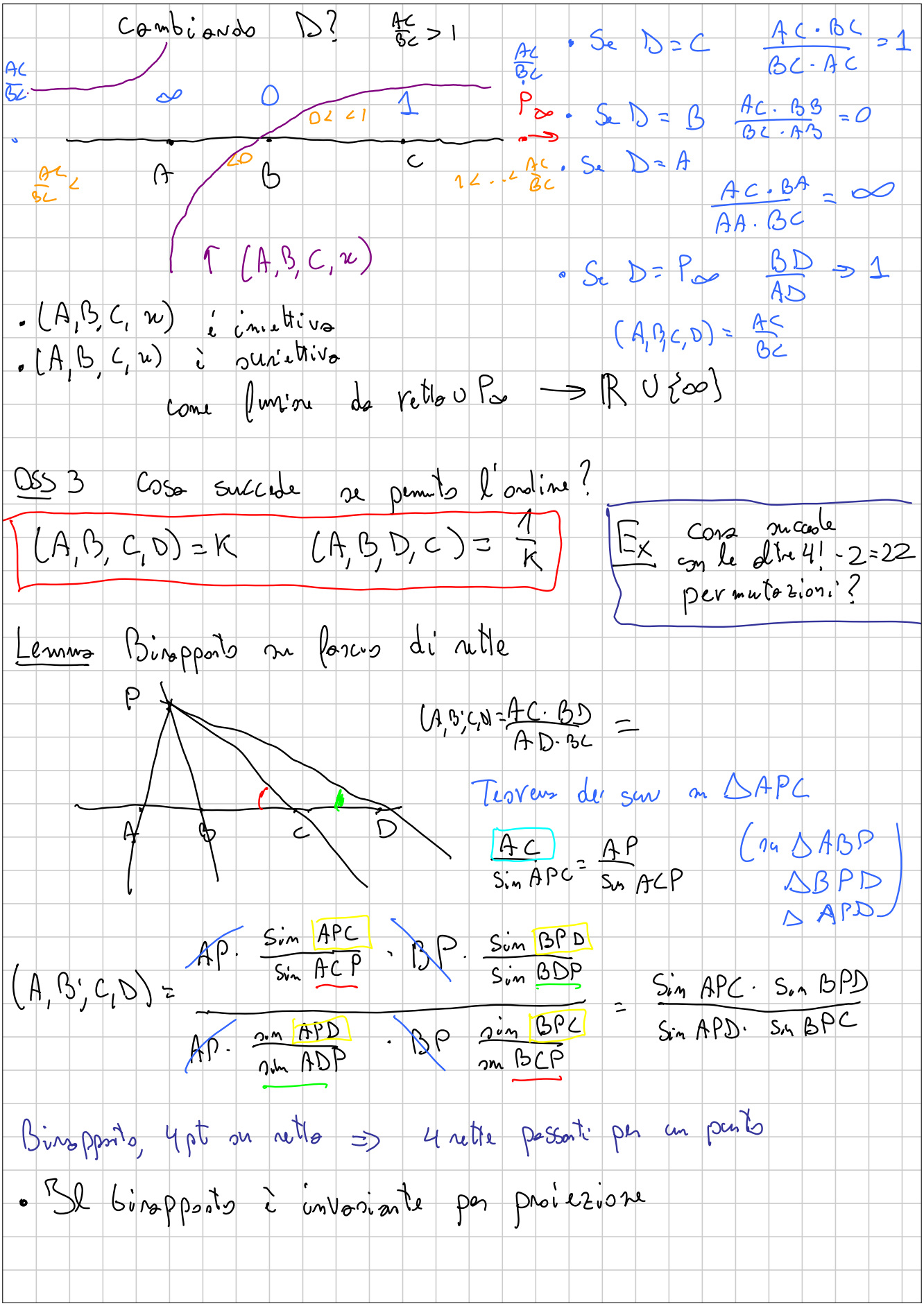
($\forall A, B, C \quad AB + BC = AC$ con segm. orientati)

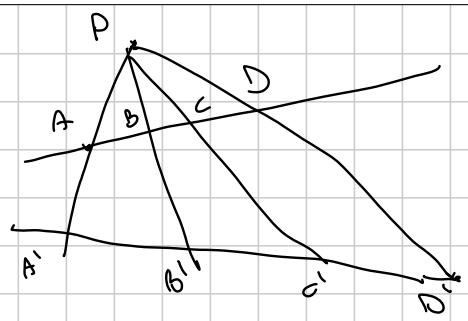
1° oss A, B, C, D_1 e D_2 su una retta $(A, B; C, D_1) = (A, B; C, D_2)$

$\iff D_1 = D_2$

Dim $\frac{AC \cdot BD_1}{BC \cdot AD_1} = \frac{AC \cdot BD_2}{BC \cdot AD_2} \Rightarrow \frac{BD_1}{AD_1} = \frac{BD_2}{AD_2}$ → si verifica se $D_1 = D_2$

2° oss fisso A, B, C su una retta. Come varia $(A, B; C, D)$


Cambiando D?
AC/BC > 1
AC/BC
∞
0
1
A
B
C
0 < 1
1 < AC/BC < ∞
P∞
(A,B,C,x)
• Se D = C AC·BC / BC·AC = 1
• Se D = B AC·BB / BC·AB = 0
• Se D = A AC·BA / AA·BC = ∞
• Se D = P∞ BD/AD → 1
(A,B,C,D) = AC/BC
• (A,B,C,x) è iniettiva
• (A,B,C,x) è suriettiva
come funzione da retta ∪ P∞ → ℝ ∪ {∞}
Oss 3 Cosa succede se permuto l'ordine?
(A,B,C,D) = K (A,B,D,C) = 1/K
Ex Cosa succede con le altre 4! - 2 = 22 permutazioni?
Lemma Birapporto su fascio di rette
P
A
B
C
D
(A,B,C,D) = AC·BD / AD·BC =
Teorema dei sen su △APC
AC / sin APC = AP / sin ACP
(su △ABP △BPD △APD)
(A,B,C,D) = AP · sin APC / sin ACP · BP · sin BPD / sin BDP / AP · sin APD / sin ADP · BP · sin BPC / sin BCP = sin APC · sin BPD / sin APD · sin BPC
Birapporto, 4 pt su retta ⇒ 4 rette passanti per un punto
• Il birapporto è invariante per proiezione



$$(A,B;C,D) = \frac{\sin APC \cdot \sin BPD}{\sin APD \cdot \sin BPC}$$

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

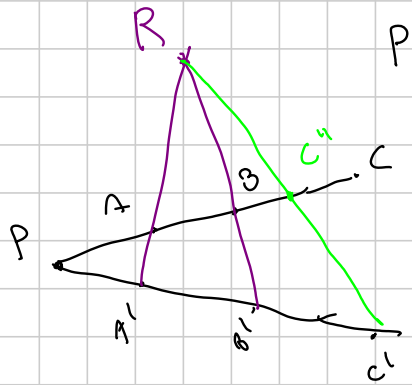
Lemma converso P,A,B,C su r, P,A',B',C' su s

$$(P,A,B,C) = (P,A',B',C') \iff AA', BB', CC' \text{ concorrono}$$

$\Uparrow$ già fatta

$\Downarrow$ $R = AA' \cap BB'$, $C'' = RC' \cap r$

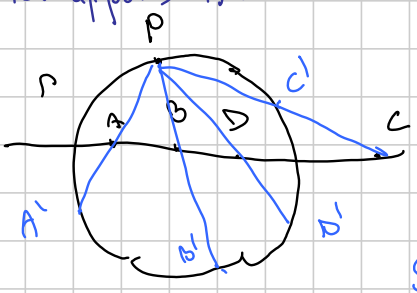
$$(P,A,B,C'') \overset{R}{=} (P,A',B',C') \underset{\text{hp}}{=} (P,A,B,C) \Rightarrow C = C''$$



Birapporto su cerchio $A',B',C',D' \in \Gamma$, $P \in \Gamma$ def $(A',B',C',D') =$ Birapporto delle rette passanti per P

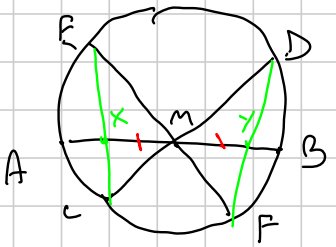
$$= (A,B;C,D) = \frac{\sin \hat{APC'} \cdot \sin \hat{BPD}}{\sin \hat{BPC'} \cdot \sin \hat{APD'}}$$

Se P varia su Γ gli angoli non fanno stima



⚠ P deve stare su Γ

Ex: teorema della farfalla:



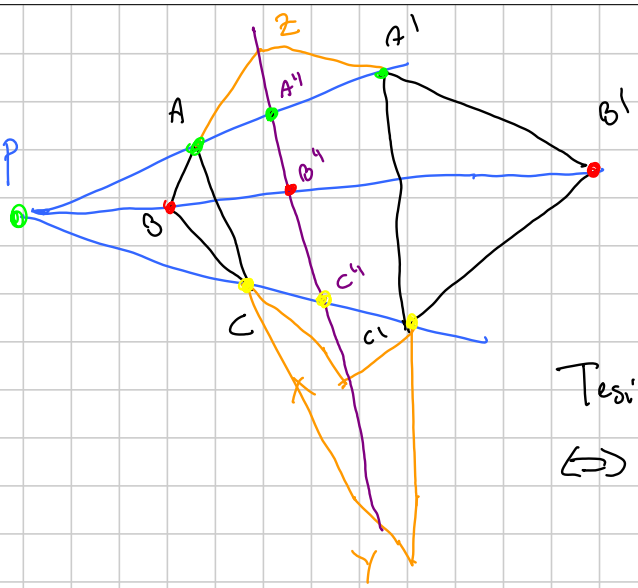
$AM = MB$

$X = BC \cap AB$

$Y = DF \cap AB$

Tesi: $MX = MY$

Teorema di Desargues



ABC $A'B'C'$ triangoli.

$Z = AB \cap A'B'$

$X = BC \cap B'C'$

$Y = AC \cap A'C'$

Tesi: AA', BB', CC' concorrono in P $\Leftrightarrow$ XYZ allineati

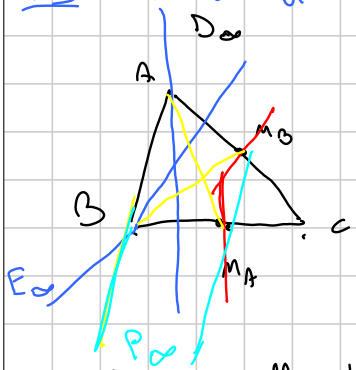
Dim: $l = XZ$ $\quad A'' = l \cap AA'$ è ciò che cerco

$X \in l \Leftrightarrow l, AC, A'C'$ concorrono $\quad AC, A'C', A''C''$ concorrono

$(P, A, A', A'') \overset{Z}{=} (P, B, B', B'') \overset{X}{=} (P, C, C', C'')$

per il lemma, $AC, A'C', A''C''$ concorrono.

Es: Retta di Eulero



D_∞ = pt all'infinito di AH

E_∞ = pt all'infinito di BH

$\triangle A M_A D_\infty$, $\triangle B M_B E_\infty$

$AD_\infty \cap BE_\infty = H$ $\quad M_A D_\infty \cap M_B E_\infty = O$

$AM_A \cap BM_B = G$

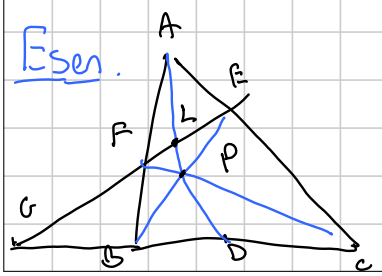
G, H, O allineati $\Leftrightarrow$ AB, $M_A M_B$, $D_\infty E_\infty$ concorrono

Desargues — AB e $M_A M_B$ sono parallele

$AB \cap M_A M_B = P_\infty$

$P_\infty, D_\infty, E_\infty$ sono allineati sulla retta all'∞

Esen.



D, E, F sui lati

$G = EF \cap BC$

Tesi: $(B, C, D, G) = -1$

$\Leftrightarrow$ AD, BE, CF concorrono

1) Ceva + Menelao (facili!)

2) AD, BE, CF concorrono in P $\quad L = AD \cap EF$

$(B, C; D, G) \overset{P}{=} (E, F; L, G) \overset{A}{=} (C, B; D, G)$ $\quad k = \frac{1}{k}$, $k^2 = 1$

$k = \frac{1}{k}$

$k = 1$ solo se il birapporto è degen ($C = D$)

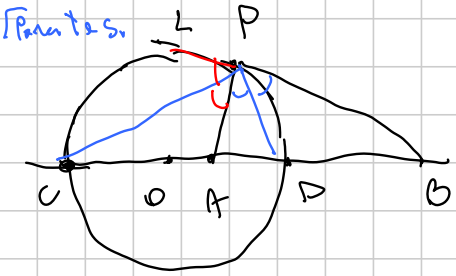
$k = -1 = (B, C; D, G)$

Oss: $(A, B; C, D) = (B, A; C, D) \iff \boxed{(A, B; C, D) = -1}$

Quaterna armonica.

$\frac{AC \cdot BD}{BC \cdot AD} = -1$ $\quad \left|\frac{AC}{BC}\right| = \left|\frac{AD}{BD}\right|$ Circonferenza di Apollonio

Potenza di P



$\left|\frac{AP}{PB}\right| = k$ costante?

È cerchio di luogo centro su AB

$\left|\frac{AP}{PB}\right| = \left|\frac{AC}{CB}\right| = \left|\frac{AD}{DB}\right| \Rightarrow C, D$ piedi delle Bisett. di $\triangle APB$

$\Rightarrow \angle CPD = \frac{1}{2} \cdot \angle BPA = 90°$

Es: A, B, C, D su retta, P punto fuori, due cose implicano la 3ª:

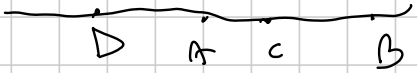
1) $(A, B; C, D) = -1$

2) PC bisect $\widehat{APB}$ ($\circ$ PD bisect $\widehat{APB}$)

3) $\angle CPD = 90°$

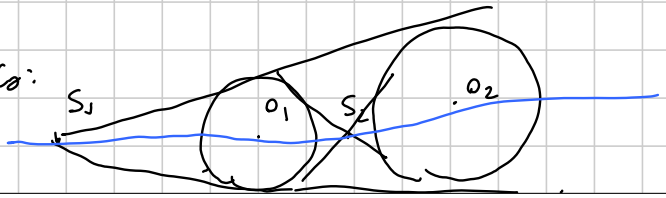
1+2 $\Rightarrow$ 3

$\frac{AC}{CB} = \frac{AD}{DB} \Rightarrow \left|\frac{AC \cdot BD}{AD \cdot BC}\right| = 1$ $\quad \overset{+}{\cdot}$ $\overset{-}{\cdot}$ $\quad$ $-$ $-$ $\searrow$ Segno $-$



Altri esempi di quaterna armonica:

Es: $(O_1, O_2, S_1, S_2) = -1$

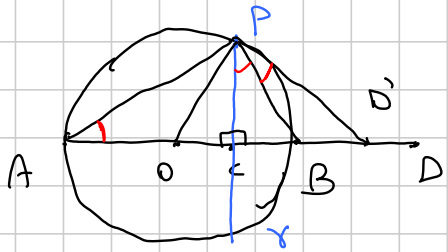


hint: S_1 e S_2 sono centri di simm. rotazione

• $(A,B,C,D) = -1$, O pt medio di AB, N pt medio di CD

① $OC \cdot OD = OA^2$

C e D sono inversi rispetto alla circonf. di diametro AB, γ



$\angle PCA = 90°$

tangente in P a γ in D'

$OC \cdot OD' = r^2 = OP^2$

$\angle D'PB = \angle PAB$ → $\triangle APD'$ e $\triangle BPD'$ simili

$\parallel$

$\angle CPB$ perché $\triangle APB$ è retto

⇒ PB è bisettrice ⇒ $(A,B;C,D')$ è armonico ⇒ $D' = D$

e $OC \cdot OD = r^2$

② $DC \cdot DO = DB \cdot DA$ =

$\parallel$ DP^2 per Euclide su $\triangle OPD$

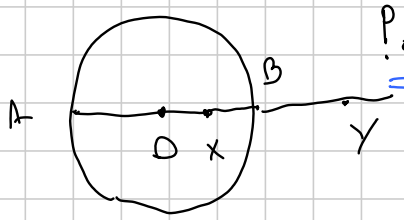
$DP^2 = DB \cdot DA$ per potenza di D rispetto a γ

③ $\frac{OC}{OD} = \frac{AC^2}{AD^2} = \frac{BC^2}{BD^2}$

④ $AB^2 + CD^2 = 4ON^2$ (N pt medio CD)

} × Esercizio

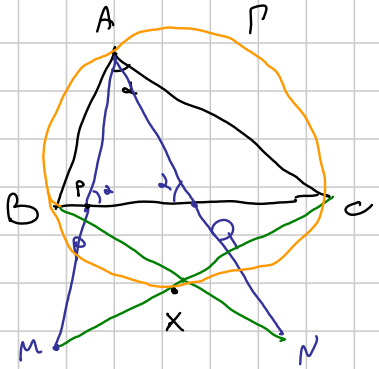
⑤ $\frac{2}{AB} = \frac{1}{AC} + \frac{1}{AD}$



P_∞ X e Y sono inversi

⇒ $(A,B,O,P_\infty) = -1$

IMO 2014-4



P, Q su BC

$\angle AQB = \angle APC = \alpha$

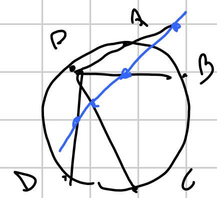
$MP = PA$ $NQ = QA$

Tesi: MCNB ciclico sulla circonf. circoscritta ad ABC

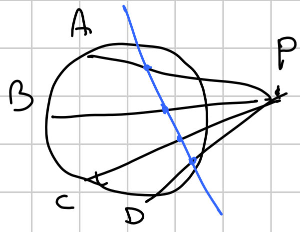
$X = MC \cap \Gamma$ Vorrei dimostrare che $X \in BN$ $\qquad Y = BN \cap \Gamma$

Nope: $(A, X, B, C) \overset{?}{=} (A, Y, B, C)$

$(A, X; B, C)$

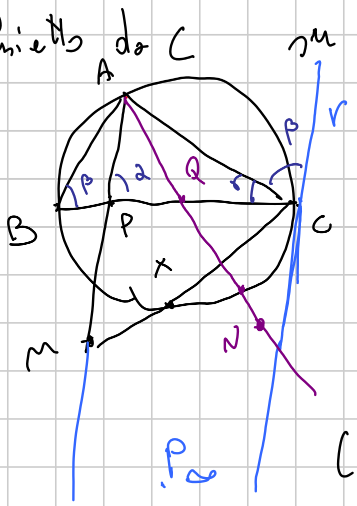


ok! :)



NO! non funziona.

Proietto da C su AM



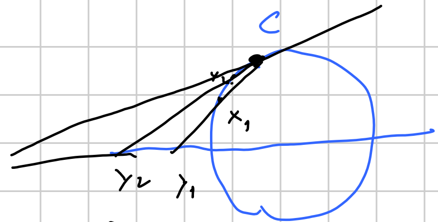
$A \to A$

$B \to P$

$X \to M$

$C \to r \cap AM$

$C \to P_\infty$ di AM



proiezione C da C $= AM \cap$ tangente in C

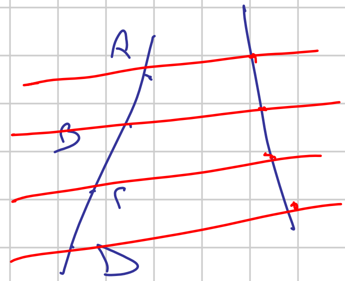
tg in C // AM

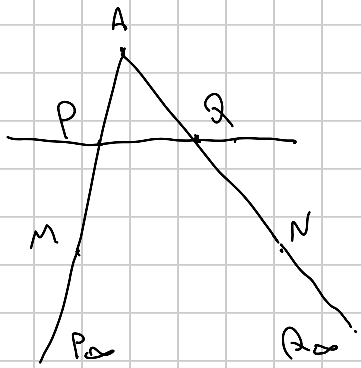
r // AM $\quad r$

$(A, X; B, C) = (A, M, P, P_\infty) = -1$

(sym; pt medio AM)

Proietto (A, M, P, P_∞) da Punto all'infinito di BC





Proietto da $R_\infty \in BC$

R_∞ $\quad A \to A$

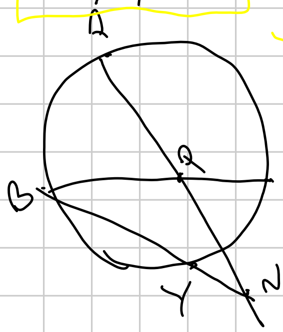
$P \to Q \qquad PQ // MN$

$M \to N$

$P_\infty \to Q_\infty$

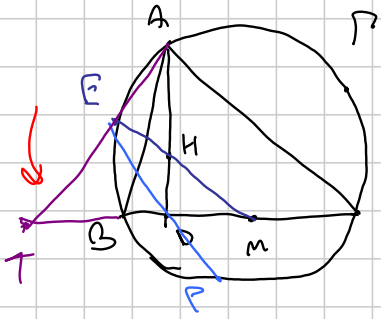
$$(A, X, B, C) = (A, M, P, P_\infty) = (A, N, Q, Q_\infty) = (A, Y, C, B) = -1$$

$$= (A, Y, B, C)$$



$X = Y$

APMO 2012-4 (WC 2013)



AD altezza. M pt mid BC

$MH \cap \Gamma = E$

$ED \cap \Gamma = F$ Tesi: $\frac{BF}{FC} : \frac{AB}{AC}$

$\left|\frac{BF \cdot AC}{FC \cdot AB}\right| = 1$ ↑ Segmenti Veri

$(A,F;B,C) \overset{?}{=} \frac{\sin APB \cdot \sin RPC}{\sin RPB \cdot \sin APC} = \frac{\frac{AB}{2R} \cdot \frac{FC}{2R}}{\frac{FB}{2R} \cdot \frac{AC}{2R}}$

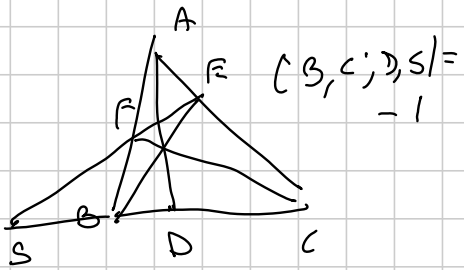
$|\sin APB| = \left|\frac{AB}{2R}\right|$ Ricordo i segni e l'ordine dei punti

$= \frac{+AB \cdot FC}{FB \cdot AC} = -1$ (− +) ↑ Segmenti orientati

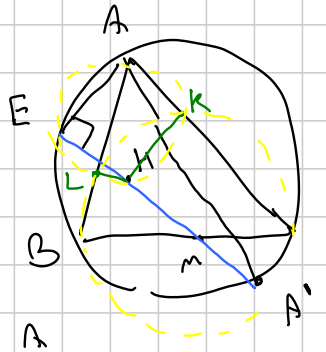
Tesi $\Leftrightarrow (A,F;B,C) = -1$ • proietto da E

$(A,F;B,C) \overset{E}{=} (T,D;B,C) \overset{?}{=} -1$

Classe: T sta sulla retta per i piedi delle altezze



$(B,C;D,S) = -1$

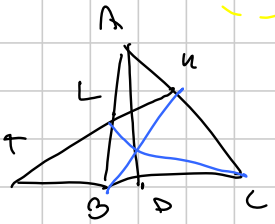


A' diam oppos di A

A'H ⊥ E dunque $\Rightarrow \angle AEH = 90°$

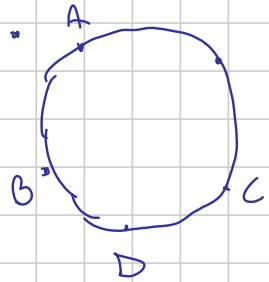
- AKHL E' ciclo di diam AH
- BCKL è ciclo

AE, LK, BC sono gli assi radicali $\Rightarrow$ concorrono in T



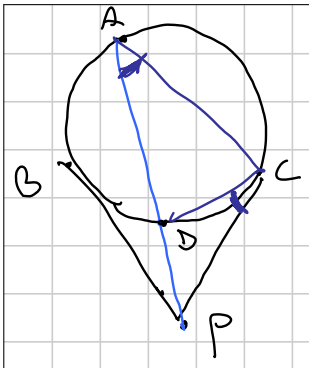
$\Rightarrow$ per il lemma $(B,C,D,T) = -1 \Leftrightarrow$ AD, BK, CL concorrono

□



$(A,B,C,D) = -1 \Leftrightarrow \frac{AC}{AB} = \frac{DC}{BD} \Leftrightarrow AC \cdot BD = AB \cdot CD$

A, B, C, D sono un quadrilatero ARMONICO



Simmediana P = $\cap$ tangenti da B e C

$D = AP \cap \Gamma$ Tesi: A,D,B,C è armonico

- $\triangle CDP \sim \triangle ACP$

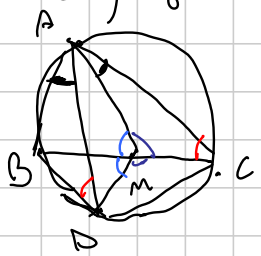
$\frac{AC}{AP} = \frac{DC}{CP}$ $\quad \frac{AC}{DC} = \frac{AP}{CP} \overset{BP,CP\ tg}{=} \frac{AP}{BP} = \frac{AB}{BD}$ ($\triangle ABP \sim \triangle BDP$)

$AC \cdot BD = AB \cdot DC$

- AP è simmediana in quanto ottenuta (Inv + simm di $\widehat{AB}\,\widehat{BC}$ in A)
- A,D,B,C su Γ quadrilatero armonico
- $(A,D,B,C) = -1$
- $AC \cdot BD = AB \cdot DC$
- AD è simmediana di $\triangle ABC$

  DA è " di $\triangle DBC$

  CB è " di $\triangle CAD$
- AD, tg in B, tg in C concorrono
- BC, tg in A, tg in D concorrono



M pt medio $BC \Rightarrow \angle AMB = \angle BMD$

$\angle AMC = \angle CMD$

$\angle BAD = \angle MAC$ per AD simmediana

$\Rightarrow \triangle ABD, \triangle AMC$ simili

$\triangle ABD, \triangle DMC$ simili

Teorema di Pascal

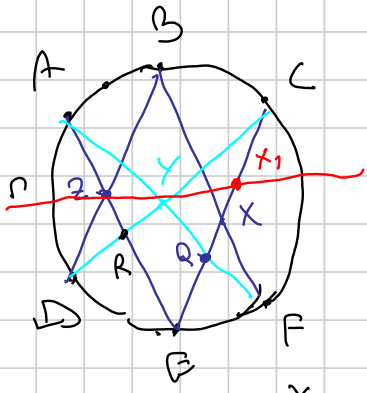
A,B,C,D,E,F su Γ

$AB \cap DE = Z$

$BF \cap CE = X$

$AF \cap CD = Y$

$\Big\}$ XYZ sono allineati



DIM: $YZ \cap CE = X_1$

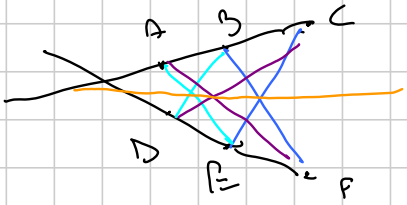
CE, pentola $C, X_1, E, Q = AF \cap CE$

$R = CD \cap AB$

$(C,X_1,E,Q) \overset{Y}{=}_{m\,AE} (R,Z,E,A) \overset{D}{=}_{m\,\Gamma} (C,B,E,A) \overset{F}{=}_{m\,CE} (C,X,E,Q)$

$\Rightarrow X_1 = X$

Es: Teorema di Pappo: come sopra, ma A, B, C, D, E, F sono on due rette



La dimostrazione è identica!

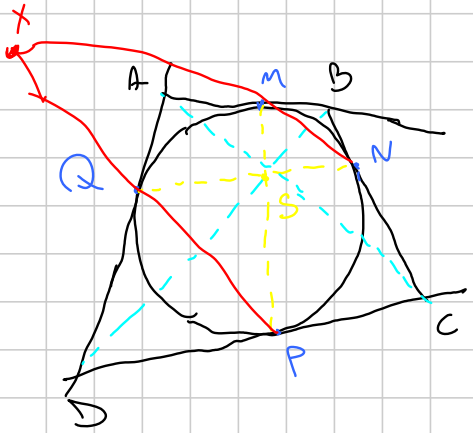
Teo Pascal ++ $A, B, C, D, E, F \to XYZ$ intersecando

allora X, Y, Z sono allineati $\Leftrightarrow$ A, B, C, D, E, F stanno su una CONICA

Errore comune è: $ABCDEF$ è ciclico. $\to XYZ$, dimostro che sono allineati

$\Rightarrow$ NO, non sono vicino che $ABCDEF$ sono su un cerchio, sono su una CONICA

• **Es.** teorema di Newton:



γ inscritta in $ABCD$

M, N, P, Q pt tangenza.

Tesi: BD, AC, MP, NQ concorrono

• Pascal su $\begin{matrix} M & Q & N \\ Q & M & P \end{matrix}$

$t_{g \text{ in } M}$ $t_{g \text{ in } Q}$

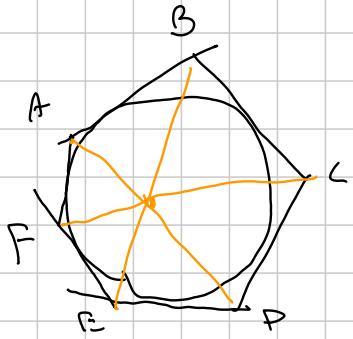
$MM \cap QQ = A$ $\quad$ $Q P \cap NM = X$

$MP \cap NQ = S$ $\Rightarrow$ A, S, X allineati

Pascal su $\begin{matrix} N & P & Q \\ P & N & M \end{matrix}$ $\to$ S, X, C allineati

$\to$ AC, QN, PM concorrono

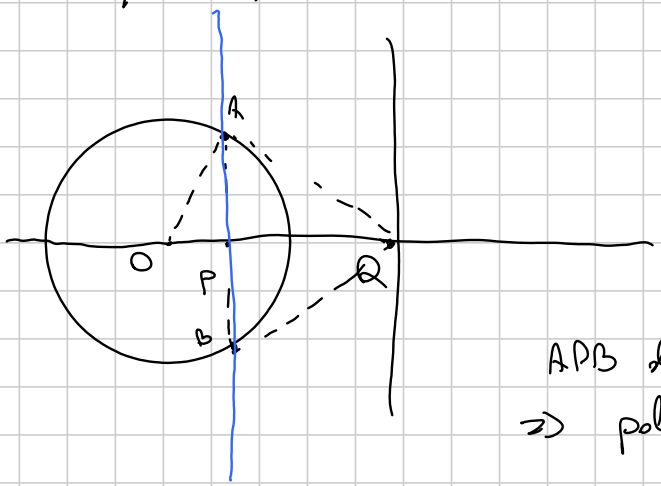
Es (con Pascal) Teorema di Brianchon



γ circoscritta a $ABCDEF$

$\Rightarrow$ AD, BE, CF concorrono

- **Poli, Polari, Dualità**



polare di P = $pol(P)$

Q inverso di P rispetto Γ

$pol(P) \perp PQ$ e passa per Q

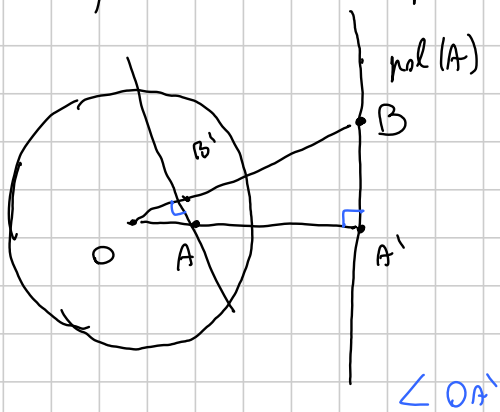
$pol(Q)$ = retta per $P \perp PQ$

APB allineati, $AB \perp PQ$

$\Rightarrow pol(Q) = AB$

- **Teorema di La Hire**

Ho Γ, A, B. $A \in pol(B) \iff B \in pol(A)$



$B \in pol(A)$

A, A' e BB' inversi rispetto Γ

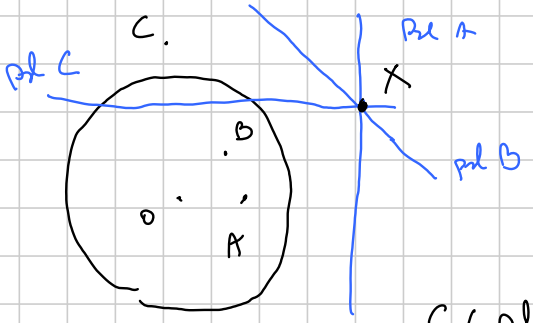
- L'inversione manda $\triangle OAB' \to \triangle OA'B$

$\triangle OAB' \sim \triangle OBA'$ $\left(OB' = \frac{R^2}{OB} \text{ etc.}\right)$

$\angle OA'B = 90° \Rightarrow \angle OB'A = 90°$

$\Rightarrow B'A \perp OB \Rightarrow B'A = pol(B)$

Corollario: A, B, C allineati $\iff pol(A), pol(B), pol(C)$ concorrono



$X = pol\,A \cap pol\,B$

$X \in pol\,A \Rightarrow A \in pol\,X$

$X \in pol\,B \Rightarrow B \in pol\,X$

$\Rightarrow pol(X) = AB$

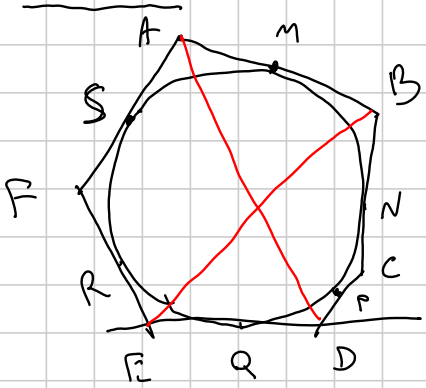
$C \in pol(X) \Rightarrow X \in pol\,C$ → polari concorrono

- Prendo tutti i punti e tutte le rette

$P \to r$ $\quad r = pol(P)$ e P è il polo della retta $P = Pol(r)$

- $P \in r \iff pol(P) \ni Pol(r)$
- $pol(P) \cap pol(Q) = Pol(PQ)$
- $pol(r \cap s) = Pol(r)\, Pol(s)$

Es. Brianchon:



$M, N \dots S$ ms $\mathcal{P}$

$pol(M) = AB$

$A = AB \cap AF$

$pol(A) = MS$ $\quad pol(B) = MN$

$pol(C) = NP$ $\quad pol(D) = PQ$

$pol(E) = RQ$ $\quad pol(F) = RS$

$X = AD \cap BE \xrightarrow{pol} pol(X) = \overline{Pol(AD)\, Pol(BE)}$

CF

$Pol(AD) = Pol(A) \cap Pol(D) = MS \cap QP$

$Pol(BE) = MN \cap RQ$

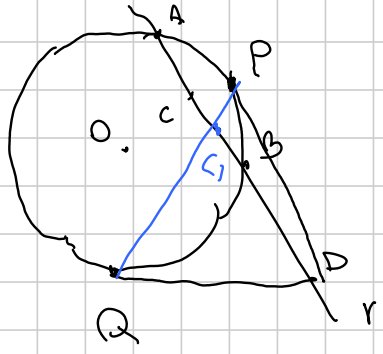
$pol(CF) = NP \cap SR$

$X \in AD, BE, CF \iff pol(X) \ni MS \cap QP,\ MN \cap RQ,\ NP \cap SR$

Pascal m M P R Q S N

Es: che teorema otteng facendo il duale di Newton?

- Lemma della polare.



r retta con A, B, C, D

$(A, B; C, D) = -1 \iff C \in pol(D)$

$(D \in pol(C))$

$Pol(D) = PQ$

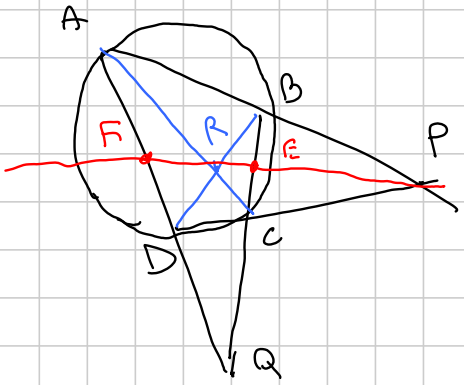
$C_1 = PQ \cap AB$

$AB, tg\,P, tg\,Q$ concorrono in $D \Rightarrow ABPQ$ è quadrilatero armonico

$(A, B; P, Q) = -1$ Proietto da P $(A, B, D, C_1) = (A, B, C_1, D) = (A, B, C, D)$ $C = C_1$

$\Rightarrow C, P, Q$ allineati $\Rightarrow C \in$ pol D

- Teorema di Brokard



A, B, C, D su Γ

$AB \cap DC = P$

$AD \cap BC = Q$

$AC \cap BD = R$.

Tesi: pol Q = PR
pol P = QR
pol R = PQ

$(A, D; F, Q) \overset{P}{=} (B, C; E, Q)$

$R \parallel$

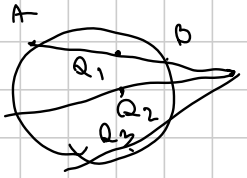
$(C, B; E, Q)$

$\Rightarrow x^2 = 1 \Rightarrow x = -1$

$\searrow (B, C; E, Q) = -1$

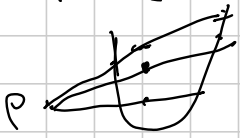
$BC \cap RQ$, $AD \cap FQ$ sono armonici.

Per lemma polare, pol (Q) passa per F passa per E $\Rightarrow$ pol $Q = EF = PR$ $\square$



Q_1 t.c. $(A, B, Q_1, P) = -1$

pol (P) = luogo di Q al variare di AB



$\Rightarrow$ pol (P) per una scelta generica

GM3 - Medium Metodi Sintetici

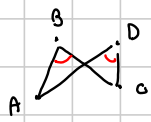
Titolo nota 10/09/2019

Angoli orientati : "Servono a evitare i problemi di configurazione"

Per esempio "ABCD ciclico sse $\angle ABC = \angle ADC$" ←

È vero? Dipende. Ci sono 2 casi.

CASO I



✓

CASO II

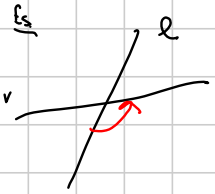
×

Qui bisognerebbe mostrare $\angle ABD + \angle ACD = \pi$.

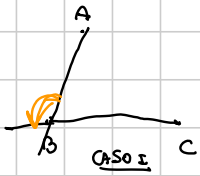
Def. $\angle(l,r)$ è l'angolo di cui devo ruotare l in senso antiorario perché coincida con r.

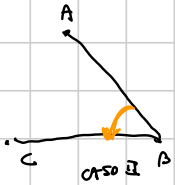
$\angle ABC = \angle(AB, BC)$

Es.



Es.





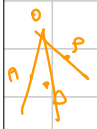
Oss. CASO I → $\angle ABC = \pi - \hat{ABC}$, CASO II → $\angle ABC = \hat{ABC}$

Proprietà 1) $\angle(l,m) + \angle(m,l) = \pi$

2) $\angle ABC + \angle BCA + \angle CAB \equiv 0 \mod \pi$

Oss. Molto spesso può succedere $\angle \cdot = \angle \cdot \overset{\mod \pi}{=} \angle \cdot + \angle \cdot = \dots = \angle \cdot$

Consideriamo le uguaglianze mod π



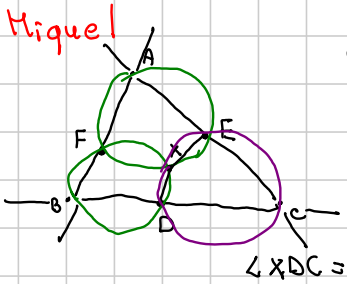
[3) $\angle AOP + \angle POB \equiv \angle AOB$] mod π

4) A, B, C allineati sse $\exists X$ t.c. $\angle XBC = \angle XBA$

[5) A, B, X, Y ciclico sse $\angle AXB = \angle AYB$]

Teorema di Miquel

- Triangolare



⊙AFE, ⊙BFD, ⊙CDE concorrono.

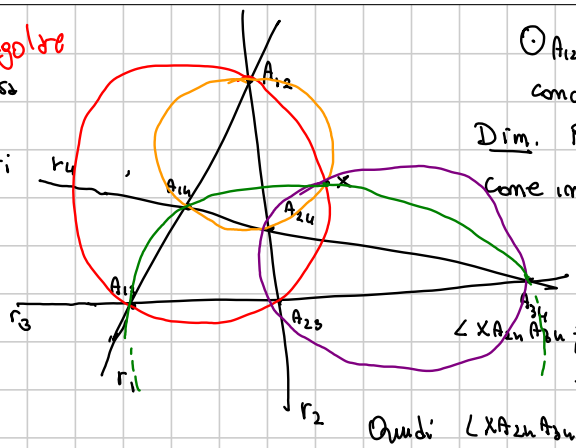
Dim. Sia X l'altra intersezione di ⊙AFE e ⊙BFD. Voglio mostrare XDCE ciclico. Infatti:

$\angle XDC = \angle XDB \overset{4}{=} \angle XFB \overset{5}{=} \angle XFA \overset{4}{=} \angle XEA \overset{5}{=} \angle XEC$

e quindi $\angle XDC = \angle XEC$ e per la 5, concludo.

Quadrangolare

Es. Capite cosa succede nei casi degenri



$\odot A_{12}A_{23}A_{13}$, $\odot A_{13}A_{34}A_{14}$, $\odot A_{12}A_{24}A_{14}$, $\odot A_{23}A_{34}A_{24}$ concorrono.

Dim. Prendiamo $X = \odot A_{12}A_{23}A_{13} \cap \odot A_{12}A_{24}A_{14}$ come in figura. Mostriamo che $XA_{24}A_{23}A_{34}$ e $XA_{14}A_{13}A_{34}$ ciclici.

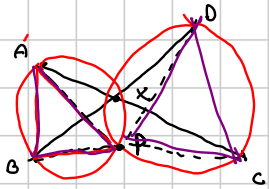
Facciamo solo la prima ciclicità. Ho che

$\angle XA_{24}A_{34} \overset{4}{=} \angle XA_{24}A_{14} = \angle XA_{12}A_{14} \overset{4}{=} \angle XA_{12}A_{13} = \angle XA_{23}A_{13} \overset{4}{=} \angle XA_{23}A_{34}$

Quindi $\angle XA_{24}A_{34} = \angle XA_{23}A_{34}$ e per 5 allora $XA_{24}A_{23}A_{34}$ ciclico.

X si dice punto di Miquel del quadrangolo (r_1, r_2, r_3, r_4)

Rotomotetie



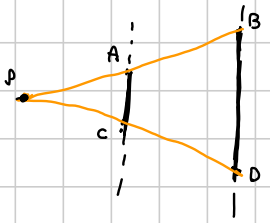
A, B, C, D punti distinti sul piano

GM1 / 2019 $\rightarrow \exists!$ centro di rotomotetia $\begin{matrix} A \to B \\ C \to D \end{matrix}$ sse $ABCD$ non è parall.

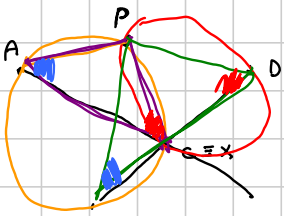
Sia $X = AC \cap BD$, $P = \odot AXB \cap \odot CXD$.

Oss. È anche il centro dell'! rotometia che manda $\begin{matrix} A \to C \\ B \to D \end{matrix}$ perché $P\hat{B}A \sim P\hat{D}C$

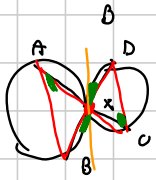
CASI DEGENERI



① Se $AC \parallel BD$? Esiste un'omotetia che manda $A \to B$, $C \to D$ di centro $AD \cap CD$.

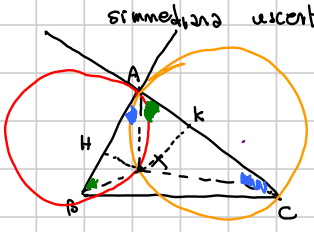


② Se X coincide con un elemento di $\{A, B, C, D\}$ una delle due circonferenze di retta "tangente".



③ $P \equiv X$, X sarà il centro dell'omotetia.

Es. Mostrare che il centro dell'! rotomotetia che manda $\begin{matrix} B \to A \\ A \to C \end{matrix}$ sta sulla simmediana uscente da A del $\triangle ABC$.



Sol. Prendo $\odot BAA$ la cfr tangente ad AC in A, passante per B

$\odot CAA$ analoga.

$X = \odot BAA \cap \odot CAA$.

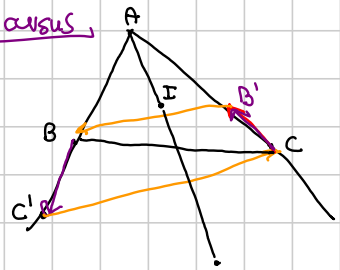
Osservo che $X\hat{B}A \sim X\hat{A}C$ poiché per tangente $\angle XBA = \angle XAC$, $\angle XAB = \angle XCA$. e quindi X è il centro dell'!

rotom che manda $B \to A$, $A \to C$.

X è simmediana poiché XH, XK pari ai lati, $\frac{XH}{XK} \overset{\text{sim}}{=} \frac{AB}{AC} = \frac{c}{b}$ e noi sappiamo che la retta d.c. di punto di cui X fa $\frac{X(X_{1c})}{X(X_{1b})} = \frac{c}{b}$ è la simmediana.

sol. Inversione centro A, raggio $\sqrt{AB\cdot AC}$, + simmetria ort. alla bissettrice uscente da A

Ex cursus



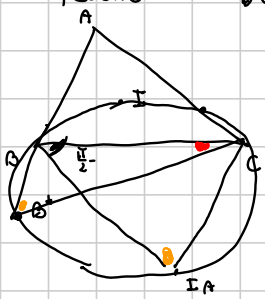
$B \to C$, $C \to B$, $\odot ABC \to BC$

$I \to I'$ t.c. $AI\cdot AI' = AB\cdot AC$ è $I' = I_A$.

Incentro.

Perché $BCII_A$ ciclico. Basta vedere che

$B^* \overset{def}{=} \odot BCII_A \cap AB$, $AB^* = AC$.



$\bullet = \pi - (I_A\hat{B}O + I_A\hat{C}B) =$

$= \pi - \left(\frac{\pi}{2} - \frac{\beta}{2} + \frac{\pi}{2} - \frac{\gamma}{2}\right) = \frac{\beta}{2} + \frac{\gamma}{2} = \frac{\pi}{2} - \frac{\alpha}{2}$

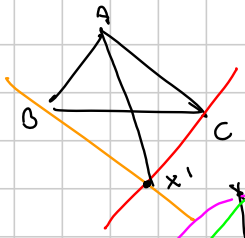
e quindi $A\hat{C}B^* = \pi - \bullet - \alpha = \frac{\pi}{2} - \frac{\alpha}{2}$

e quindi AB^*C è isoscele.

$AI\cdot AI_A = AB\cdot AB^* = AB\cdot AC$

Nell'esercizio $\odot BAA$ va nella retta passante per C e $\parallel AB$

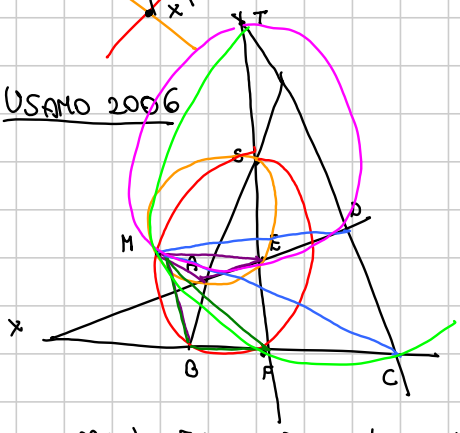
$\odot CAA$ " B $\parallel AC$



$X \to X'$, AX' è mediana. Perché per costruzione $ABX'C$ parallelogramma.

Quindi AX era simmediana.

USAMO 2006



E, F su AD, BC t.c. $\frac{AE}{ED} = \frac{BF}{FC}$.

Dim. che $\odot SAE, \odot SBF, \odot TCF, \odot TDE$ concorrono.

Sol. Sia $M = \odot SAE \cap \odot SBF$

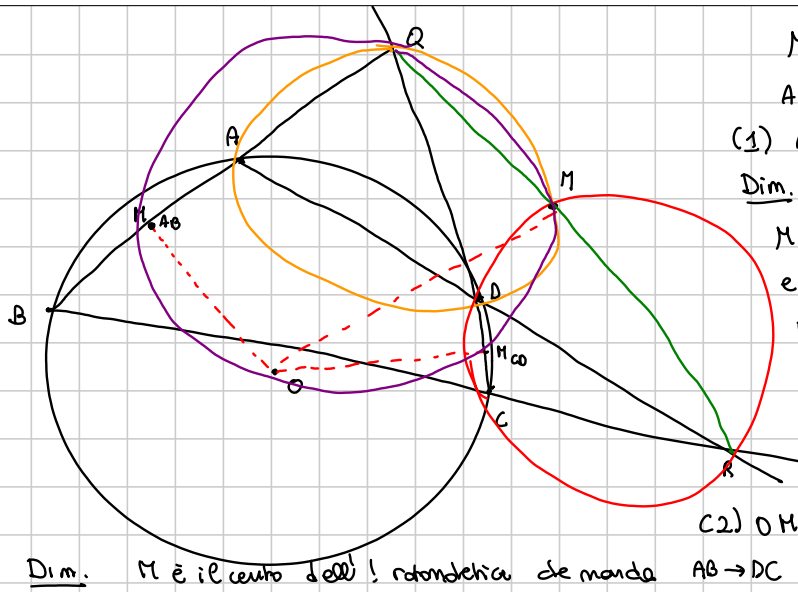
Per quello visto prima $\exists$ rotomotetia di centro M che manda $AE \to BF$.

Voglio mostrare che $\exists$ rotomotetia di centro M che manda ED in FC. Innanzitutto $\angle MED = \angle MFC$ che viene dalla similitudine $M\hat{A}E \sim M\hat{B}F$. In più per ipotesi $\frac{ED}{FC} = \frac{AE}{BF} = \frac{ME}{MF}$ e quindi $M\hat{E}D \sim M\hat{F}C$

per il I cr. di similitudine.

Quindi per quanto detto sulle rotomotetie M deve essere anche l'intersezione di $\odot EDT$ e $\odot FCT$. Quindi tutte e 4 le cfr. concorrono in M.

Conf. di Miquel nel caso ciclico.



M punto di Miquel del q.c. $ABCDQR$, quindi $M = \odot QAD \cap \odot DCR$.

(1) $ABCD$ ciclico $\Leftrightarrow M \in QR$

Dim. $M \in QR \overset{4}{\Leftrightarrow} \angle DMQ = \angle DMR$.

Ma $\angle DMQ \overset{5}{=} \angle DAQ \overset{4}{=} \angle DAB$

e $\angle DMR \overset{3}{=} \angle DCR \overset{4}{=} \angle DCB$.

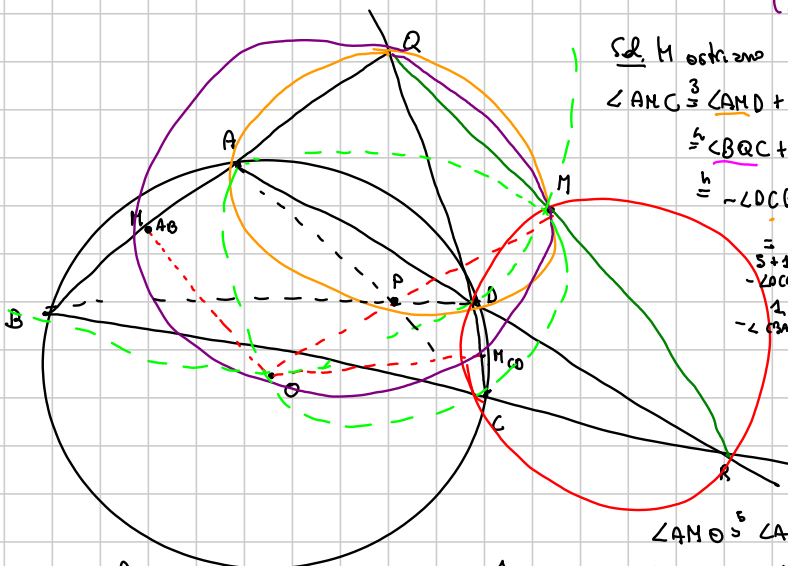
Dunque $M \in QR \overset{4}{\Leftrightarrow} \angle DAB = \angle DCB \overset{3}{\Leftrightarrow} ABCD$ ciclico.

D'ora in poi assumiamo $ABCD$ ciclico e O centro $\odot ABCD$.

(2) $OM \perp QR$

Dim. M è il centro dell'! rotomotetia che manda $AB \to DC$. Prendo M_{AB}, M_{CD} punt. med. di AB e CD. Questa rotomotetia manda anche AM_{AB} in DM_{CD}. E M quindi è anche il centro dell'! rotom. che manda AD in $M_{AB}M_{CD}$. Quindi per come si costruisce il centro di questa rotom., $M \in \odot Q M_{AB} M_{CD}$. Però $O \in \odot Q M_{AB} M_{CD}$ poiché $Q\hat{M}_{AB}O = Q\hat{M}_{CD}O = \pi/2$.

Dunque $Q M_{AB} O M_{CD} M$ ciclico e $O\hat{M}Q = O\hat{M}_{CD}Q = \pi/2$.



(3) $MAOC$, $BODM$ ciclici.

Sol. Mostriamo $MAOC$ ciclico - $BODM$ analogamente.

$\angle AMC \overset{3}{=} \angle AMD + \angle DMC \overset{5}{=} \angle AQD + \angle DRC \overset{4}{=}$

$\overset{4}{=} \angle BQC + \angle ARB \overset{5}{=} -\angle QCB - \angle CBQ - \angle RBA - \angle BAR$

$\overset{4}{=} -\angle DCB - \angle BAD - 2\angle CBA$

$= 2\angle ABC = \angle AOC$.

$\overset{5+1}{-\angle OCB - \angle BAD = 0}$

$\overset{1}{-\angle CBA = \angle ABC}$

↑ angolo al centro sopra lo stesso arco

e dunque $\angle AMC = \angle AOC$ e quindi ok.

(4) MO bisseca AMC, BMD

Sol. Usando (3) di prima $\angle AMO \overset{5}{=} \angle ACO$, $\angle OMC \overset{5}{=} \angle OAC$.

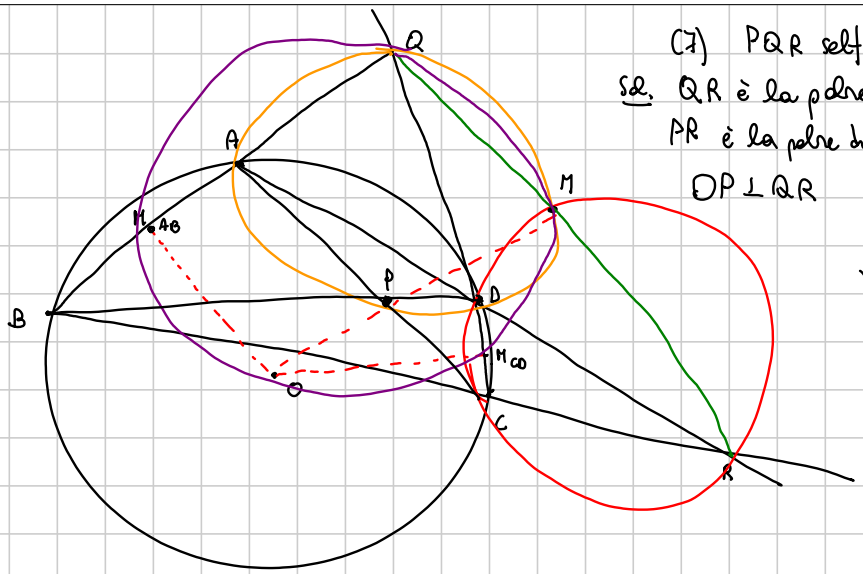
Però $\angle ACO = \angle OAC$ perché $A\hat{O}C$ è isoscele. MO bisseca AMC e analog. BMD.

(5) $P = AC \cap BD \Rightarrow O, M, P$ allineati.

Sol. $MAOC$, $BODM$, $ABCD$ ciclici. I lati sono radicali sono OM, AC, BD e concorrono.

(6) P, M sono uno l'inverso dell'altro wrt. circonferenza $ABCD$.

In quest'inverso $AC \to \odot AOC$. $BD \to \odot BOD$, $AC \cap BD = P \to \odot AOC \cap \odot BOD \overset{(3)}{=} M$



(7) PQR self-pol. $\Rightarrow$ O ortocentro di PQR

Sol. QR è la polare di P, PQ è la polare di R, PR è la polare di Q (Lemma della polare + dualità)

$OP \perp QR$ e ciclicità (Centro-polo $\perp$ polare).

Yufei Zhao

Circonferenze Mistilinee.

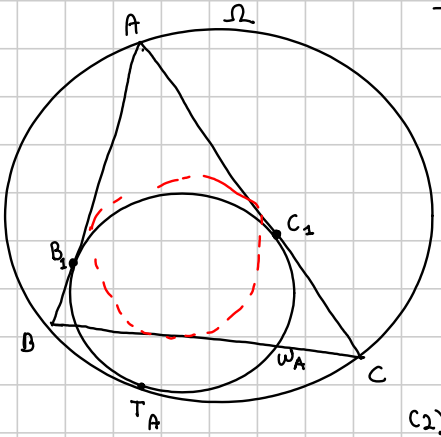
(1) AT_A è la ceviana isogonale di Nagel.

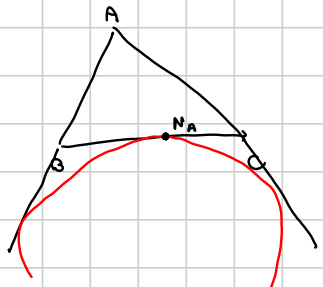
Sol. Inversione $\sqrt{AB \cdot AC}$ + simmetria rispetto bisettrice d_2 A

$B \to C$, $C \to B$, $\Omega \to BC$

$\omega_A \to$ excircle rispetto A

$T_A \to N_A$





Quindi dopo inv. + simmetria $AT_A \to$ ceviana di Nagel AN_A.

Dunque AT_A è la ceviana isog. di Nagel

(2) AT_A, BT_B, CT_C concorrono nel coniugato isogonale di Nagel

(3) Il coniugato isog. di nagel esterno fra ω (Cfr incircle ad ABC) e Ω

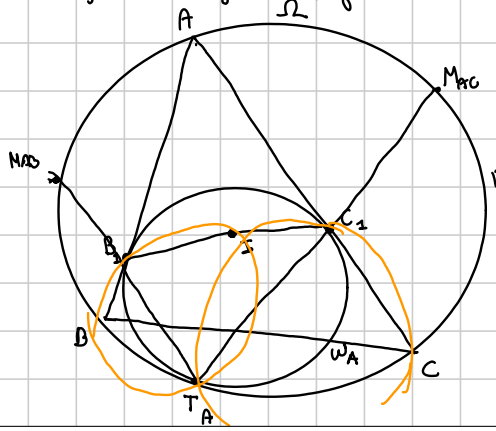
Dim. A centro di sim. esterno fra ω e ω_A

T_A centro di sim. esterno fra Ω e ω_A

Quindi per Monge centro di sim. esterno fra ω e Ω è AT_A.

Questo vale ciclicamente per BT_B, CT_C Quindi la loro intersezione, che era il con. isog. di Nagel, è il centro di sim. esterno fra ω e Ω.

(4) Il coniugato isogonale di Gergonne è il centro di sim. interno fra ω e Ω



(5) I è pto medio di B_1C_1.

(5a) TB_1 e TC_1 intersecano $\widehat{AB}$, $\widehat{AC}$ nei loro punti medi.

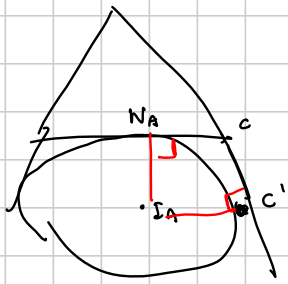
Dim. Immaginiamo I $\in B_1C_1$. Dalla carcol su $M_{AB}T_AM_{AC}$ BAC. Infatti $M_{AB}T_A \cap BA = B_1$, $T_AM_{AC} \cap AC = C_1$, $M_{AC}B \cap CM_{AB} = I$ (bicentrici)

e dunque I, B_1, C_1 allineati.

Impiliè AB_1C_1 isoscele, AI bisettrice, allora è anche mediana e quindi I è pto medio di B_1C_1.

(6) $B_1 I T_A B$, $C_1 I T_A C$ ciclici

Dim. Inversione + simmetria $T_A \to N_A$, $I \to I_A$, $B \to C$, $B_1 \to C'$



$B_1 I T_A B$ ciclico $\iff$ $C' I_A N_A C$ ciclico

Ma $C' I_A N_A C$ ciclico perché $I_A \hat{N}_A C = I_A \hat{C}' C = \pi/2$.

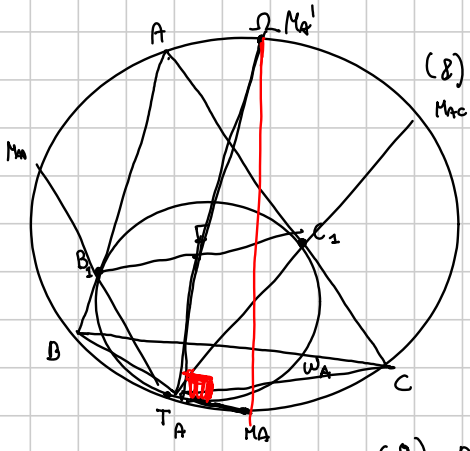
Analog. $C_1 I T_A C$ ciclico.

Oss. $I_A \in \odot AB'C'$ sotto inv. + simm. diviene $I \in B_2C_1$. Quindi è una dim. alternativa di $I \in B_1C_1$.

(7) $T_A I$ biseca $B\hat{T}_A C$.

Dim. $\angle BT_A I \overset{5}{=} \angle BB_1 I \overset{4}{=} \angle AB_1 I$ e $\angle CT_A I \overset{5}{=} \angle CC_1 I \overset{4}{=} \angle AC_1 I$

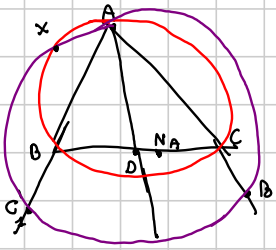
Ma $\angle AB_1 I = \angle AC_1 I$ perché AB_1C_1 isoscele e quindi $\angle BT_A I = \angle CT_A I$.



(8) M_A pto medio $\overset{\frown}{BC}$. $M_A T_A$, BC, B_1C_1 concorrono.

Sol ① sotto inversione $M_A \to D$ piede della bisettrice

Rimane da mostrare $X = \odot ABC \cap \odot AB_1'C_1' I_A$ allora AXD_1N_A ciclici. ... Dicembre: si può fare?



② Poncel su $BCM_{AB}T_AM_AA$

$BC \cap T_AM_A$

$CM_{AB} \cap M_AA = I$

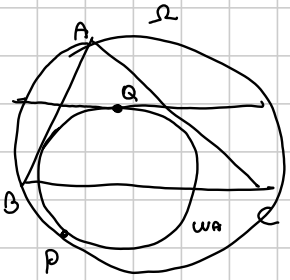
$M_{AB}T_A \cap AB = B_1$

$I, C_1, BC \cap T_AM_A$ allineati ma $I \in B_1C_1$ ✓

(9) Da (7) T_AI biseca $B\hat{T}_AC \Rightarrow M_A\hat{T}_AI = \pi/2$ e duale T_AI intercetta Ω nel diam. opposto di M_A.

[EGMO 2013 - 5]

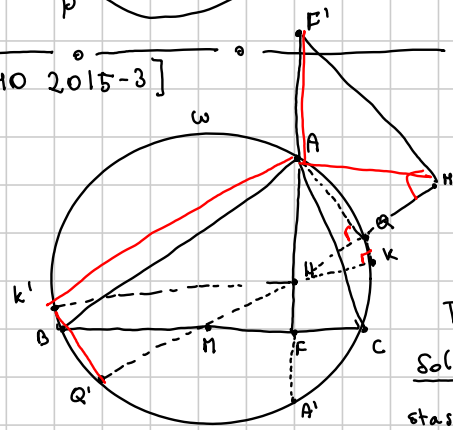
Mostra che $\angle BAP = \angle QAC$



Sol. Omotetia centro in A che $\omega_A \to$ circonscritta ci dice che AQ è la ceviana di Nagel

AP è l'isogonale della ceviana di Nagel per (1) e quindi fine.

[IMO 2015-3]



H ortocentro

$HF \perp BC$, $F \in BC$

M medio di BC

$Q \in \omega$ t.c. $H\hat{Q}A = \pi/2$

$K \in \omega$ t.c. $H\hat{K}Q = \pi/2$

A B C K Q su ω in quest'ordine (come in figura)

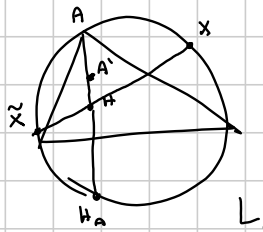
Th. $\odot KQH$, $\odot FKM$ sono tangenti.

Sol. $Q \in MH$. Fatto noto: il simmetrico di H wrt M sta sulla circonscritta ed è il diam. opposto di A.

Oss. Esiste una unif. inversione $\circ$ simmetia centrale in H che mantiene fissa la circonf.

Inversione di centro H e raggio $\sqrt{\text{Pow}_{\Gamma'}(H)}$ + simmetia centrale in H, $A \to H_A$

Con questa trasformazione $X \to XH \cap \omega = \tilde{X}$



Sotto questa trasformazione $Q \to Q' = HQ \cap \omega$ che è la simmetrica di H wrt M, $A \to A'$ simmetrico di H wrt F. $F \to F'$ simmetrico di H wrt A, $M \to M'$ simmetrico di H wrt Q. $k \to k' = Hk \cap \omega$.

$\odot kQH \to$ retta $k'Q'$ $\quad \odot FkM \to F'k'M'$

La tesi diventa $k'Q'$ tange $\odot F'k'M'$

Oss. 1 $H\hat{k}Q = \pi/2 + A\hat{Q}Q' = \pi/2 \Rightarrow AQQ'k'$ rettangolo

Euristica: Se la tesi è vera Ak' deve essere l'one di $F'M'$.

Oss. 11 Ak' one di $F'M'$.

Infatti $M'F' \parallel AQ$ e $Ak' \perp AQ$ per oss. I. Dunque $Ak' \perp F'M'$. Inoltre nel triangolo rettangolo $F'M'H$, $M'A = AF'$ perché $M'A$ mediana rel. all'ipotenusa è metà dell'ipotenusa stessa. Dunque Ak' one di $F'M'$.

Fine: Dunque poiché $Ak' \perp k'Q'$ per Oss. 1 allora $k'Q'$ è la tangente in k' alla cfr $k'F'M'$, che è la Tesi

— ∘ —

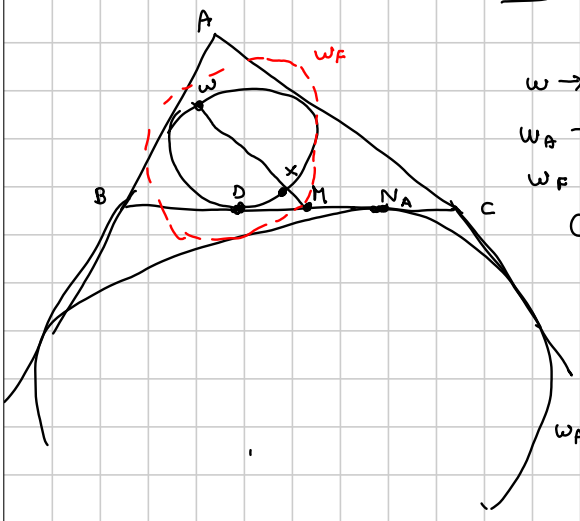
Th. Feuerbach La cfr. inscritta e le exinscritte tangono la cfr di Feuerbach

Dim Inversione in M punto medio di BC con raggio $MD = MN_A$ (Ricordo $MD = MN_A$).

$\omega \to \omega$ (l'immagine di X è $MX \cap \omega$).

$\omega_A \to \omega_A$ (l'immagine di X è $MX \cap \omega_A$)

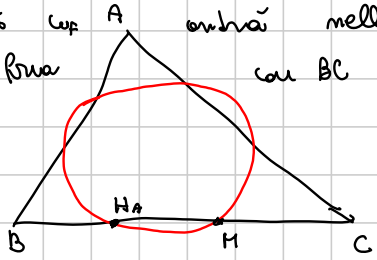
$\omega_F \to$ retta!



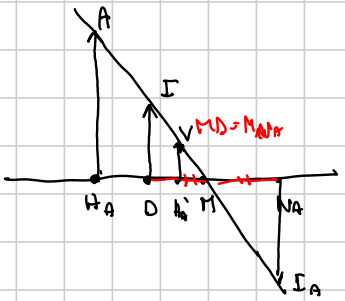
Come capire quale retta? Capisco 2 cose:

1) dove va H_A? 2) che angolo forma ω_F con BC

A quel punto ω_F coincide nella retta per H_A che forma con BC l'angolo uguale in 2).



$H_A \to H_A'$ t.c. $M_{H_A} \cdot M H_A' = MD^2$

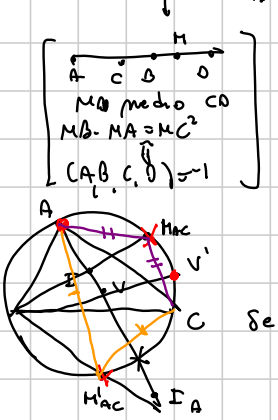


$MH_A \cdot MH_A' = MD^2 \iff (H_A H_A', D, N_A) = -1 \iff$

$\iff$ proiettando dalla bis. $(A, V, I, I_A) = -1$

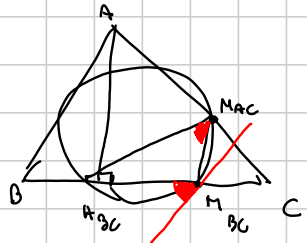
$\iff$ proiett. su ω $(A, V', M_{AC}, M'_{AC}) = -1$

da B $\iff \left| \frac{AM_{AC}}{M_{AC}V'} \cdot \frac{V'M'_{AC}}{M'_{AC}A} \right| = 1$

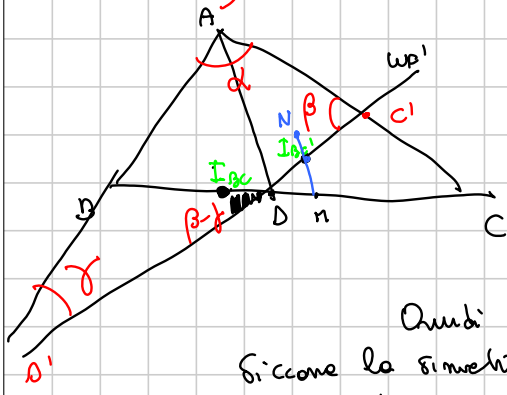


Se $V' \equiv C$ $\frac{AM_{AC}}{M_{AC}V'} = 1$ e $\frac{V'M'_{AC}}{M'_{AC}A} = 1$

Quindi il punto $V' \in \omega$ t.c. $(A, V', M_{AC}, M'_{AC}) = -1$ è C. Dunque il punto V sulla bisettrice t.c. $(A, V, I, D_A) = -1$ è il piede della bisettrice. Dunque W' è il piede della bisettrice!



• angolo fra ω_F e BC $= \angle BM_{AC}C - \angle MM_{AC}C =$
$= \pi - 2\gamma - \alpha = \beta - \gamma$
$AH_{BC}C$ rettangolo, $M_{BC}M_{AC} \parallel A_3$



$\omega_F \to$ retta per D piede della bisettrice che forma un angolo $\beta - \gamma$ con BC
Quanto vale $A\hat{B}'C$ = ?
$A\hat{B}'C = \pi - B'\hat{B}C - B'\hat{D}B =$
$= \pi - (\pi - \beta) - (\beta - \gamma) = \gamma$
Quindi $A\hat{C}'B' = \beta$.

Quindi $B'C'$ è la simm. di BC rispetto alla bisettrice in A.
Siccome la simmetria rispetto alla bisettrice lascia ω e ω_A invariate, allora ω' tange ω_A e ω. ✓ ∎

Teoria dei Numeri - 1

Titolo nota 30/12/2011

POLINOMI CICLOTOMICI

Def: $z \in \mathbb{C}$ è detta radice n-esima dell'unità se per $n \in \mathbb{N}$ $z^n = 1$

Def: una radice n-esime è detta primitiva se

$$z^n = 1 \quad \text{e} \quad \forall k < n \quad z^k \neq 1$$

OSS: $e^{\frac{2\pi i k}{n}}$ sono le radici n-esime dell'unità.

... PARTE ALLA LAVAGNA ...

GENERATORI MOD p^n

$\forall p$ primo $\exists g$ generatore mod p, ovvero $\exists g$ t.c $\text{ord}_p(g) = p-1$.

DIM: Sappiamo che $\forall a \quad \text{ord}_p(a) \mid p-1$

$$\Rightarrow \mathbb{F}_p \setminus \{0\} = \bigcup_{d \mid p-1} \{a \in \mathbb{F}_p \mid \text{ord}_p(a) = d\}$$

è un'unione disgiunta!

$$G_d = |\{a \in \mathbb{F}_p \mid \text{ord}_p(a) = d\}| \qquad p-1 = \sum_{d \mid p-1} G_d$$

Se $\text{ord}_p(a) = d \Rightarrow a^d - 1 \equiv 0 \ (p) \Rightarrow$

$\Rightarrow$ ϑ è radice di $x^d - 1$, ma $x^d - 1$ ha al più d radici in $\mathbb{F}_p$. Voglio dire che ϑ è radice di $\Phi_d(x)$; questo è vero perché $x^d - 1 = \Phi_d(x) \cdot \prod_{\substack{c \mid d \\ c<d}} \Phi_c(x)$, quindi se ϑ non fosse radice di $\Phi_d(x)$ $\exists\, c<d$ t.c. $\Phi_c(\vartheta) \equiv 0 \Rightarrow \vartheta^c - 1 \equiv 0 \Rightarrow$ assurdo perché d è l'ordine. $\Rightarrow$ ogni ϑ di ordine d è radice (in $\mathbb{F}_p$) di $\Phi_d(x)$.

$\Rightarrow$ $G_d \leq \varphi(d)$

(G_d: elementi di ord d; $\varphi(d)$: radici di Φ_d)

$\Rightarrow$ $p-1 = \sum_{d \mid p-1} G_d \leq \sum_{d \mid p-1} \varphi(d) = p-1$

$\Rightarrow$ $G_d = \varphi(d)$ $\forall d$!!! $\Rightarrow$

$\Rightarrow$ in particolare $G_{p-1} = \varphi(p-1) > 0$

$\Rightarrow \exists$ g generatore.

DIGRESSIONE: In $\mathbb{F}_p$ bisogna fare attenzione alla differenza fra funzione polinomiale e polinomio:

$f: \mathbb{F}_p \to \mathbb{F}_p$ t.c. $f(x) = x^p - x$ $\rightsquigarrow$

$\rightsquigarrow$ $f \equiv 0$ questa È la funzione 0.

tuttavia il polinomio $x^p - x$ NON è il polinomio nullo.

LEMMA: dato p primo

$$(1+kp)^{p^s} \equiv 1 + kp^{s+1} \ (p^{s+2})$$

DIM: PER INDUZIONE

PASSO BASE: $s=0$ $\quad 1+kp \equiv 1+kp \ (p^2)$

PASSO INDUTTIVO: $(1+kp)^{p^{s+1}} \equiv 1+kp^{s+2} \ (p^{s+3})$

$$(1+kp)^{p^{s+1}} = \left((1+kp)^{p^s}\right)^p \equiv (1+kp^{s+1}+hp^{s+2})^p \ (p^{s+3})$$

$$\equiv (1+p^{s+1}(k+hp))^p \equiv 1+kp^{s+2} \ (p^{s+3})$$

perché ho $\sum_{i=0}^{p} \binom{p}{i} p^{(s+1)i} (k+hp)^i \equiv \uparrow$ □

TEOREMA: Dato p primo $\forall n \in \mathbb{N}$ $\exists g$ t.c.

$$\mathrm{ord}_{p^n}(g) = \varphi(p^n) \quad \text{(generatore)}$$

DIM: Se g è un generatore mod p allora

$p-1 \mid \mathrm{ord}_{p^n}(g) \mid (p-1)p^{n-1}$, ci basta trovare un g tale che $g^{(p-1)p^{n-2}} \not\equiv 1 \ (p^n)$.

Sappiamo che $g^{p-1} \equiv 1 \ (p) \Rightarrow g^{p-1} \equiv 1+kp \ (p^2)$

se $p \nmid k$ g è un generatore mod p^2

se invece $p \mid k$ prendo $g+p$, il suo ordine

è ancora multiplo di $p-1$.

$$(g+p)^{p-1} = \sum_{k=0}^{p-1} \binom{p-1}{k} p^k g^{p-1-k} \equiv g^{p-1} + (p-1)p\,g^{p-2} \equiv$$

$$\equiv 1 + (p-1)g^{p-2}p \pmod{p^2}, \text{ ma } p \nmid g^{p-2}(p-1)$$

$\Longrightarrow$ $g+p$ è un generatore.

Abbiamo trovato che mod p^2 esiste sempre un generatore. Per il lemma, se $\exists$ un generatore mod p^2 allora $g^{p-1} \equiv 1 + kp \pmod{p^2}$

$\Longrightarrow \forall n \quad g^{(p-1)p^{n-2}} \equiv (1+kp)^{p^{n-2}} \overset{\text{LEMMA}}{\equiv} 1 + kp^{n-1} \pmod{p^n}$,

ma $p \nmid k$ (g è gen.) $\Longrightarrow$ g è generatore mod p^n. □

"OSS": Gli unici n per cui $\exists$ un generatore mod n sono $2, 4, p^k, 2p^k$ (p dispari primo).

LTE — LIFTING THE EXPONENT

TEOREMA: Sia p primo $v_p(n)$ il più grande k per cui $p^k \mid n$ (si scrive $p^k \| n$), allora dati $x, y \not\equiv 0 \pmod p$, $p \mid x-y$, $p \neq 2$ vale

$$v_p(x^n - y^n) = v_p(x-y) + v_p(n)$$

DIM: $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \dots + y^{n-1})$

Ci basta dimostrare che $v_p(n) = v_p(x^{n-1} + \dots + y^{n-1})$

Possiamo assumere che $n = q$ primo, perché mi basta scomporre in primi e iterare il ragionamento.

Abbiamo 2 casi:

$q \neq p$ $\quad x \equiv y \ (p) \Rightarrow x^{q-1} + \dots + y^{q-1} \equiv$

$\equiv x^{q-1} + x^{q-1} + \dots + x^{q-1} \equiv q x^{q-1} \not\equiv 0 \ (p)$

$\Rightarrow v_p\left(\frac{x^q - y^q}{x-y}\right) = v_p(q) = 0$ è ok!

$q = p$ $\quad$ Vorrei che $v_p(p) = 1 = v_p(x^{p-1} + \dots + y^{p-1})$

Sicuramente $v_p(x^{p-1} + \dots) \geq 1$ perché

$x^{p-1} + \dots + y^{p-1} \equiv p x^{p-1} \ (p) \equiv 0$

$y = x + kp \qquad y^i = \sum_{j=0}^{i} x^j \cdot k^{i-j} p^{i-j} \binom{i}{j} \equiv x^i + x^{i-1} \cdot i \cdot kp \pmod{p^2}$

(fa 0 se $i = p-1$)

$x^{p-1} + \dots + y^{p-1} \equiv \sum_{i=0}^{p-1} x^i \left(x^{p-1-i} + kpi\, x^{p-2-i}\right) \equiv$

$\equiv p \cdot x^{p-1} + x^{p-2} \cdot kp \cdot \sum_{i=0}^{p-1} i \equiv p x^{p-1} + x^{p-2} \cdot k \cdot p \cdot \frac{p(p-1)}{2}$

$\equiv p x^{p-1} \ (p^2)$ $\quad \square$

OSS: $p = 2$ non funziona per via di lui

PROP: Se n è dispari e $p \mid x+y \quad p \nmid x$

$v_p(x^n + y^n) = v_p(x+y) + v_p(n)$

DIM: $x^n+y^n = x^n-(-y)^n$ ... come prima.

PROP:
- Se $4 \mid x-y$ allora
$$v_2(x^n-y^n) = v_2(x-y)+v_2(n)$$
- Se $2 \parallel x-y$ e $2 \mid n$ allora
$$v_2(x^n-y^n) = v_2(x-y)+v_2(x+y)+v_2(n)-1$$
- Se n è dispari: $v_2(x^n-y^n) = v_2(x-y)$

ESERCIZIO 1 Sia $a \in \mathbb{N}$ $a \neq 0$ $a_n = 1+a+\dots+a^{n-1}$, siano s,t interi t.c. $\forall p \mid s-t$ primo $p \mid a-1$. Mostrare che $\frac{a_s-a_t}{s-t}$ è intero.

SOL: $a_s = \frac{a^s-1}{a-1}$, $a_t = \frac{a^t-1}{a-1}$, quindi
$$\frac{a_s-a_t}{s-t} = \frac{a^s-1-a^t+1}{(s-t)(a-1)} = \frac{a^t\cdot(a^{s-t}-1)}{(s-t)(a-1)}$$

mi basta che $\forall p \mid s-t$
$$v_p(s-t)+v_p(a-1) \leq v_p(a^{s-t}-1)$$
$=$ ← LTE □

ESERCIZIO: Determinare il più grande $k \in \mathbb{Z}$ tale che $2017^k \mid 2016^{2017^{2018}} + 2018^{2017^{2016}} + 2017^{2016^{2015}}$

SOL: Se le ipotesi fossero rispettate

$$v_{2017}\left(2016^{2017^{2018}} + 2018^{2017^{2016}}\right) =$$

$$v_{2017}\left(2016^{2017^2} + 2018\right) + 2016$$

Le ipotesi sono rispettate se $2017 \mid 2016^{2017^2} + 2018 \equiv$

$\equiv (-1)^{2017^2} + 1 \equiv 0 \ (2017)$ OK.

$2017 = p$

$2016 = p - 1 \longrightarrow -2016^{p^2} = -(1-p)^{p^2}$ ma

$1 - p \equiv 1 \ (p) \Longrightarrow (1-p)^{p^2} \equiv 1 \ (p^2) \Longrightarrow$

$\Longrightarrow 2016^{2017^2} + 2018 \equiv -1 + 2018 \equiv 2017 \ (2017^2)$

$\Longrightarrow k = 2016 + 1 = 2017$.

LEMMA DEL GUADAGNO DI UN PRIMO:

$x, y \in \mathbb{N}$ $x > y$ $n > 1$ $(x, y) = 1$ allora

$x^n - y^n$ ha un primo che non divide $x - y$

tranne: casi in cui $n = 2$ $x + y = 2^k$.

DIM: Posso assumere che $n = q$ sia primo.

Se la tesi fosse falsa avrei, per $q \neq 2$,

$$v_p(x^q - y^q) = v_p(x - y) + v_p(q)$$

$v_p(q) = \begin{cases} 0 & q \neq p \\ 1 & q = p \end{cases}$, quindi se $q \nmid x - y$

$x^q - y^q = x - y$ assurdo per $q \neq 1$.

se $q \mid x - y$ allora $x^q - y^q = q(x - y)$

$q = x^{q-1} + x^{q-2}y + \dots + y^{q-1} > q \cdot y^{q-1} \geq q$

assurdo.

Se $q = 2$ $\quad x^2 - y^2 = (x-y)(x+y)$

$(x+y, x-y) \mid 2y$ e $\mid 2x \Rightarrow (x+y, x-y) \mid 2$.

$\Rightarrow$ se in $x+y$ non ci sono primi "nuovi" allora

$x+y = 2^k$.

Se $n = 2^\alpha$ $\alpha > 1$ allora $x^n - y^n = (x^2)^{2^{\alpha-1}} - (y^2)^{2^{\alpha-1}}$

in questo caso $4 \mid x^2 - y^2$, quindi

$v_2(x^{2^\alpha} - y^{2^\alpha}) = v_2(2^{\alpha-1}) + v_2(x^2 - y^2)$

Sono nel caso q dispari! (o quasi)

(ripercorro lo stesso ragionamento di prima).

TEOREMA DI ZSIGMONDY:

$x, y \in \mathbb{N}$ $\quad x > y$ $\quad n > 1$, allora $x^n - y^n$ contiene un primo che non è contenuto in tutti i $x^k - y^k$ per $k < n$ .....

Tranne nei seguenti casi:

- $n = 2$, $x = 3$, $y = 1$
- $x + y = 2^k$

LEMMA DI HENSEL

LEMMA: Dato un polinomio $f(x) \in \mathbb{Z}[x]$ detto S_ℓ il numero di soluzioni di $f(x)$ modulo p^ℓ (per p primo), se $\forall$ soluzione mod p z, $f'(z) \not\equiv 0 \ (p)$, ho che

$$S_\ell = S_1 \quad \forall \ell \in \mathbb{N}$$

DIM: Mostriamo prima che data una soluzione mod p questa si può "sollevare" ad una soluzione mod p^n

PASSO BASE: $f(z) \equiv 0 \ (p)$

PASSO INDUTTIVO: So che $\exists z \in \mathbb{Z}/p^n\mathbb{Z}$ t.c. $f(z) \equiv 0 \ (p^n)$

$\Rightarrow$ sia $\tilde{z}$ un "sollevamento di z in $\mathbb{Z}/p^{n+1}\mathbb{Z}$", ovvero tale che $\tilde{z} = z$ (proiezione su $\mathbb{Z}/p^n\mathbb{Z}$), allora $f(\tilde{z}) \equiv kp^n \ (p^{n+1})$. Se $p \mid k$ allora $\tilde{z}$ è una soluzione mod p^{n+1}, altrimenti prendo $\tilde{z} + \alpha p^n$, allora $f(\tilde{z} + \alpha p^n)$ cos'è?

$$(\tilde{z} + \alpha p^n)^i \equiv \tilde{z}^i + i\tilde{z}^{i-1} \cdot \alpha p^n \ (p^{n+1}) \quad \Rightarrow$$

$$\Rightarrow \quad f(\tilde{z} + \alpha p^n) = \sum_{i=0}^{\deg f} a_i (\tilde{z}^i + i\tilde{z}^{i-1} \cdot \alpha p^n) \equiv$$

(coefficienti; ① ②)

$\equiv \underbrace{k p^n}_{\equiv 0} + \underbrace{\alpha p^n \cdot f'(\tilde{z})}_{\equiv 0} = p^n (k + \alpha f'(\tilde{z}))$

α lo posso scegliere, prendo $\alpha \equiv -\frac{k}{f'(z)} \ (p)$

e posso farlo perché $f'(z) \not\equiv 0 (p)$.

Inoltre, per come scelgo α data z radice mod p^n $\exists!$ $\tilde{z}$ tale che $f(\tilde{z}) \equiv 0 (p^{n+1})$ e $\tilde{z} = z$.

pensati come insiemi

Definisco una funzione $\psi_n : S_n \to S_{n+1}$ t.c. $z \mapsto \tilde{z}$ (è ben definita per unicità di α)

se mostro che ψ_n è biiettiva ho la tesi.

se $z_1 \neq z_2$ allora $\tilde{z}_1 \neq \tilde{z}_2$ perché $\overline{\tilde{z}_1} = z_1 \neq z_2 = \overline{\tilde{z}_2}$,

$\Rightarrow$ è iniettiva. Inoltre $\forall$ w radice mod p^{n+1} $\overline{w}$ è radice mod $p^n \Rightarrow w = \tilde{\overline{w}} \Rightarrow \psi_n$ è suriettiva $\square$

COSA CI DICE HENSEL?

Le equazioni polinomio = potenza

NON si possono risolvere con le congruenze

ES: $3^n = x^2 + 5$ x^2+5 ha una radice mod 3 che è 1 e $2x$ in 1 non fa 0 mod 3,

$\Rightarrow$ ha sol. mod 3^n $\forall n$

SOL: mod 8 $\quad 3^n \equiv \begin{cases} 1 \\ 3 \end{cases} \qquad x^2+5 \equiv \begin{cases} 5 \\ 1 \\ 6 \end{cases}$

$\Rightarrow$ n pari $\Rightarrow$ $3^n - x^2 = 5$ - - - -

e si finisce.

ESERCIZIO) Mostrare che $\forall n \in \mathbb{N}$ $\exists m \in \mathbb{N}$ t.c. $7^n \mid 5^m + 3^m - 1$

TEORIA DEI NUMERI 2 – MEDIUM

Titolo nota 08/09/2019

Estensioni quadratiche

d intero, non quadrato

$\mathbb{Z}[\sqrt{d}] = \{a+b\sqrt{d} \text{ con } a,b \text{ interi}\} \subseteq \mathbb{C}$

$\mathbb{Q}(\sqrt{d}) = \{a+b\sqrt{d} \text{ con } a,b \text{ razionali}\} \subseteq \mathbb{C}$

Se d non è quadrato mod p,

$\mathbb{F}_p[\sqrt{d}] = \{a+b\sqrt{d} \text{ con } a,b \in \mathbb{F}_p\}$

$\mathbb{F}_p \hookrightarrow \mathbb{Z}/p\mathbb{Z}$

$$(a_1+b_1\sqrt{d})(a_2+b_2\sqrt{d}) = a_1a_2 + \sqrt{d}(a_1b_2+b_1a_2) + db_1b_2$$

Pell $x^2 - dy^2 = 1$, d intero fissato $\neq \square$, $d>0$

$x^2 - dy^2 = (x-\sqrt{d}y)(x+\sqrt{d}y)$

Norma: dato $z = a+\sqrt{d}b$ (con a,b razionali), la sua NORMA è $N(z) = a^2 - db^2 = (a+b\sqrt{d})(a-b\sqrt{d})$

Oss $N(z_1 \cdot z_2) = N(z_1)\cdot N(z_2)$ [ci fidiamo]

Pell: $N(x+\sqrt{d}y) = 1$

$$N\left(\frac{1}{z}\right)\cdot N(z) = N(1) = 1$$

$$\Rightarrow N(1/z) = 1/N(z)$$

$$N\left(z_1/z_2\right) = N(z_1 \cdot 1/z_2) = N(z_1)\cdot N(1/z_2)$$

$$= N(z_1)/N(z_2)$$

$$z = a + b\sqrt{d} \qquad \frac{1}{z} = \frac{1}{a+b\sqrt{d}} = \frac{a-b\sqrt{d}}{a^2-db^2}$$

$\neq 0$ perché $d \neq \square$

Idea: se voglio $N(z)=1$, mi basta trovare z_1, z_2 con $N(z_1)=N(z_2)$ e poi prendere $z = z_1/z_2$

Idea 2: $x^2 - dy^2 = 1 \Rightarrow \left(\frac{x}{y}\right)^2 - d = \frac{1}{y^2}$

$$\Rightarrow \left|\frac{x}{y} - \sqrt{d}\right| \cdot \left|\frac{x}{y} + \sqrt{d}\right| = 1/y^2$$

Soluzioni della Pell = approssimazioni razionali molto precise di $\sqrt{d}$

Esempio: BMO 2015/4

Dati 20 interi consecutivi (positivi), ce n'è uno — chiamiamolo d — t.c.

$$n\sqrt{d}\left\{n\sqrt{d}\right\} > 5/2$$

per ogni n.

Soluzione Scriviamo $\{n\sqrt{d}\} = n\sqrt{d} - m > 0$

$$2n\sqrt{d} \cdot \left(n\sqrt{d} - m\right) > 5$$

$$\left(n\sqrt{d} + m\right)$$

$$d n^2 - m^2$$

$$\left(2n\sqrt{d}\right) > \left(n\sqrt{d} - m\right) \cdot \left(n\sqrt{d} + m\right) = dn^2 - m^2 \overset{?}{\geq} 5$$

$$\left(n\sqrt{d} - m\right)$$

Siamo tristi se $dn^2 - m^2 = 1, 2, 3, 4$

Obiettivo: scegliere d in modo che queste equaz. non abbiano soluzione

Congruenze, e il testo suggerisce mod 4 / 5

Se $5 \mid d$: $\quad -m^2 \equiv 1, \cancel{2}, \cancel{3}, 4 \ (5)$

Resta da fare una congr. mod 4 per vietare $1, 4$.

Vogliamo escludere: -1 è un R.Q. mod d.

Sarebbe bello: d è un primo $\equiv 3 \ (4)$

Basta: d è divisibile per $p \equiv 3 \ (4)$

" : $d \equiv 3 \ (4)$

" : $d \equiv 15 \ (20)$ □

Teo Se $d>0$, $d \neq \square$, l'equazione

$$x^2 - dy^2 = 1$$

ha sempre soluz. (intera) $\neq (\pm 1, 0)$

Dim. Per pigeonhole, dato $\sqrt{d}$ (che è irraz.) so trovare ∞ coppie (x_n, y_n) di interi t.c.

$$\left| \frac{x_n}{y_n} - \sqrt{d} \right| < \frac{1}{y_n^2}$$

$$\left| x_n^2 - d y_n^2 \right| = y_n^2 \left| \left(\frac{x_n}{y_n}\right)^2 - d \right|$$

$$= y_n^2 \cdot \left| \frac{x_n}{y_n} - \sqrt{d} \right| \cdot \left| \frac{x_n}{y_n} + \sqrt{d} \right| < \left| \frac{x_n}{y_n} + \sqrt{d} \right|$$

$$\leq 2\sqrt{d} + 1$$

Per pigeonhole trovo ∞ coppie x_n, y_n per cui $x_n^2 - d y_n^2$ assume lo stesso valore N

$$N \left(x_n + \sqrt{d}\, y_n \right)$$

Scegliamo due tali coppie, (x_0, y_0) e (x_1, y_1) con $N(x_i + \sqrt{d}\, y_i) = 1$.

$$N\left(\frac{x_0 + \sqrt{d}\, y_0}{x_1 + \sqrt{d}\, y_1} \right) = \frac{N(x_0 + \sqrt{d}\, y_0)}{N(x_1 + \sqrt{d}\, y_1)} = \frac{N}{N} = 1$$

$a + b\sqrt{d}$ MA A PRIORI a, b razionali

$$\frac{(X_0+\sqrt{d}\,Y_0)(X_1-\sqrt{d}\,Y_1)}{(X_1+\sqrt{d}\,Y_1)(X_1-\sqrt{d}\,Y_1)} = \frac{(X_0X_1-dY_0Y_1)+\sqrt{d}\,(X_1Y_0-X_0Y_1)}{N}$$

Vogliamo fare in modo che $\begin{cases} X_1Y_0 \equiv X_0Y_1 \ (N) \\ X_0X_1 \equiv dY_0Y_1 \ (N) \end{cases}$

Per esempio andrebbe bene se $(*)\begin{cases} X_0 \equiv X_1 \ (N) \\ Y_0 \equiv Y_1 \ (N) \end{cases}$:

allora $X_1Y_0 \equiv X_0Y_1$ è ovvio e

$$X_0X_1 - dY_0Y_1 \equiv X_0^2 - dY_0^2 \equiv N \equiv 0 \ (N)$$

Per piccionhole di nuovo, trovo due coppie con la stessa norma N e tale che $(*)$ valga ☒

Verso l'infinito e oltre

$$X^2 - 2Y^2 = 1 \qquad 3^2 - 2\cdot 2^2 = 1$$

$$N(3+2\sqrt{2})$$

$$\Rightarrow N\left((3+2\sqrt{2})^2\right) = N(3+2\sqrt{2})^2 = 1$$

$$N(17+12\sqrt{2})$$

Trovo ∞ soluz. considerando $(3+2\sqrt{2})^n$: ∞ soluz sono date da

$$X_n = \frac{1}{2}\left[(3+2\sqrt{2})^n + (3-2\sqrt{2})^n\right]$$

$$Y_n = \frac{1}{2\sqrt{2}}\left[(3+2\sqrt{2})^n - (3-2\sqrt{2})^n\right]$$

Teo Sia $x_0 + \sqrt{d}\, y_0 = f$ la più piccola soluzione di $x^2 - dy^2 = 1$ $\boxed{x_0 > 0,\ y_0 > 0}$ (└ minimo $x > 1$)

Allora ogni soluzione di $x^2 - dy^2$ è della forma $\pm f^k$ per un certo $k \in \mathbb{Z}$.

Dim Sia (u, v) una soluzione, sia $g = u + \sqrt{d}\, v$

Posso supporre wlog $g > 0$, e voglio dim $g = f^k$.

Osservo che $f^{-1} = x_0 - \sqrt{d}\, y_0$ $\quad (N(f) = 1)$

Scegliamo k in modo che

$$f^k \le g < f^{k+1} \qquad (f > 1)$$

$$\Downarrow$$

$$1 \le \underbrace{f^{-k} g}_{\in \mathbb{Z}[\sqrt{d}],\ N(f^{-k}g) = 1} < f$$

cioè $f^{-k} g$ è una soluz. della Pell. Siccome f era la più piccola soluzione > 1, questo vuol dire che $f^{-k} g = 1$ □

Oss f è detta la SOLUZIONE FONDAMENTALE

ALGORITMO PER TROVARE LA SOLUZ. FONDAM.

$x^2 - 7y^2 = 1$

$$\frac{2}{1} < \sqrt{7} < \frac{3}{1}$$

$$\frac{5}{2} = \frac{2+3}{1+1}$$

$5^2 - 7\cdot 2^2 = -3$ NO

$\frac{5}{2} < \sqrt{7} < \frac{3}{1}$

$\frac{5+3}{2+1} = \frac{8}{3}$

$8^2 - 7\cdot 3^2 = 1$: la fondam. è $(8,3)$, o in modo equivalente $8 + 3\sqrt{7}$

Esempio: $p \equiv 1 \ (4)$. L'eqz $x^2 - py^2 = -1$ ha ∞ soluzioni

Infinite soluz sono gratis a partire da una: se (u,v) è soluz e $g = u + v\sqrt{p}$, allora g^{2k+1} è ancora soluz.

$$N\left(g^{2k+1}\right) = N(g)^{2k+1} = (-1)^{2k+1} = -1$$

Ma anche $g \cdot f^k$ sono soluzioni ... ispirazione: magari $g = \sqrt{f}$

(e in effetti è l'unica speranza: $N(g) = -1$

$\Rightarrow N(g^2) = 1 \Rightarrow g^2 = f^n$, e n deve essere dispari ...)

Sia $f = a + b\sqrt{p}$, $g = c + d\sqrt{p}$: sto cercando di risolvere $\begin{cases} c^2 + pd^2 = a \\ 2cd = b \end{cases}$, e so $a^2 - pb^2 = 1$

$(a+1)(a-1) = pb^2$

$4 \quad pe^2$

Oss: $1 = a^2 - pb^2 \equiv a^2 - b^2 \pmod 4$

$\Rightarrow a$ dispari, b pari $= 2e$

$$\left(\frac{a+1}{2}\right)\left(\frac{a-1}{2}\right) = p \cdot e^2$$

$$\begin{cases} \frac{a \pm 1}{2} = \ell^2 \\ \frac{a \mp 1}{2} = p m^2 \end{cases} \Rightarrow \quad a = \ell^2 + p m^2 \qquad b = 2e$$

Siamo riusciti a far vedere che $\sqrt{f} \in \mathbb{Z}[\sqrt{p}]$, e ci siamo. □

Oss Se $x^2 - dy^2 = a$ ha una soluz, allora ne ha ∞: se c'è soluzione (u, v), allora $N(\underbrace{u + v\sqrt{d}}_{g}) = a$, e quindi $N(g \cdot f^k) = a \ \forall k$.

Esempio: $y^2 - 5183x^2 = 2$

Vorremmo far vedere che non ne esistono.

Sia (u, v) una soluz, $g = u + v\sqrt{5183}$

e f una soluz. fondam.

$$5183 = 72^2 - 1$$

La fondam. è quindi $f = 72 + \sqrt{5183} \approx 144$

$$f^{-1} = 72 - \sqrt{5183}$$

Morale: vorrei aggiustare g con potenze di f per avere informaz. su quanto è grande x.

$$y = \frac{g \cdot f^k + 2g^{-1} f^{-k}}{2} \qquad \text{(No, ma quasi)}$$

$$g \cdot f^k = a + b\sqrt{5183}$$

$$a - b\sqrt{5183} = \frac{2}{a + b\sqrt{5183}}$$

Per ottimizzare vorrei che $g \cdot f^k$ e $2g^{-1}f^{-k}$ fossero "dello stesso ordine di grandezza"

$$x f^k \in \left[\frac{\sqrt{a}}{\sqrt{f}}, \sqrt{a}\sqrt{f}\right]$$

$$x \cdot f^k + \frac{a}{x \cdot f^k} \leq \max\left\{\frac{\sqrt{a}}{\sqrt{f}} + \frac{a\sqrt{f}}{\sqrt{a}}, \sqrt{af} + \frac{\sqrt{a}}{\sqrt{f}}\right\}$$

$$= \sqrt{a} \cdot \left(\sqrt{f} + \frac{1}{\sqrt{f}}\right)$$

Nel nostro caso particolare: se c'è una soluz, ce n'è una con $|y| \leq \frac{1}{2}\sqrt{2}\left(\sqrt{f} + \frac{1}{\sqrt{f}}\right)$

$$\leq \frac{\sqrt{2}}{2}\left(12 + 1\right) < 13$$

$y^2 - 5183x^2 = 2$ il membro sinistro sarebbe negativo!

Oss OVVIAMENTE il primo tentativo DOVEVA essere modulo $71 \cdot 73 = 5183$ (ma non funziona)

Lemma Se $x^2 - dy^2 = a$ ha una soluzione, ne ha una con $|x| \leq \frac{1}{2}\sqrt{a}\left(\sqrt{f} + 1/\sqrt{f}\right)$

Esempio: IMO SL 2016/N5

Sia $a>0$ intero, $a \neq \square$, e consideriamo, per $K>0$, l'equazione $K = \dfrac{x^2-a}{x^2-y^2}$. Siano

$A = \{ K \mid$ c'è una soluz con $x > \sqrt{a} \}$

$B = \{ K \mid$ ——————— $0 \le x < \sqrt{a} \}$

Dim. che $A = B$

Soluzione $K(x^2-y^2) = x^2-a$

$(K-1)x^2 - Ky^2 = -a$

$\Rightarrow \quad \big((K-1)x\big)^2 - K(K-1)y^2 = -a(K-1)$

$w^2 - K(K-1)y^2 = -a(K-1)$

$B \subseteq A$ Idea di base: prendere una soluz "piccola" e moltiplicarla per una potenza della fondamentale

Parto da $\left(w_0 + y_0\sqrt{K(K-1)}\right)$ e moltiplico per la fondam. $\left(u + v\sqrt{K(K-1)}\right) = f$

$$= \left(\underbrace{w_0 u}_{\equiv 0 (K-1)} + y_0 v K(K-1) + \sqrt{K(K-1)}\,(w_0 v + u y_0) \right)$$

Moltiplicando per f^n con n grande trovo una soluz. grande (con $\dfrac{w}{K-1}$ intero)

$y^2 - 2x^2 = 1$ $\qquad$ $3+2\sqrt{2} = f$

$3-2\sqrt{2} = f^{-1}$

$17-8\sqrt{2} = f^{-2}$

$\vdots$

i coefficienti crescono!

A ⊆ B Bisogna davvero capire chi è la fondamentale

Cerchiamo davvero f: $y^2 - k(k-1)x^2 = 1$

Una soluzione è $(2k-1, 2)$. È la fondam.

perché $x=1$ non è soluz $\left(k^2 - k + 1 = \square \dots\right)$

$(k-1)y^2 - kx^2 = 1$: con -1 la so fare,

e la soluz. è $(1,1)$ "$\rightsquigarrow$" $\sqrt{k-1} + \sqrt{k}$

$\square$

$\rightsquigarrow 2k-1+2\sqrt{k(k-1)}$

Applichiamo il macchinario: la Pell

$$w^2 - k(k-1)x^2 = -a(k-1),$$

che per hp ha una soluz, ne ha anche una con

$$|w| \leq \frac{1}{2}\sqrt{a(k-1)} \cdot \left(\sqrt{f} + \frac{1}{\sqrt{f}}\right)$$

$|w| = |(k-1)x|$

$$\Rightarrow |x| \leq \frac{1}{2}\sqrt{a}\,\frac{1}{\sqrt{k-1}}\left(\sqrt{f} + \frac{1}{\sqrt{f}}\right) \overset{?}{\leq} \sqrt{a}$$

$$\iff \sqrt{f} + \frac{1}{\sqrt{f}} \leq 2\sqrt{k-1}$$

$$\iff \quad f + \frac{1}{f} + 2 \leq 4(k-1)$$

$4k - 2 + 2 \leq 4k - 4$ che è un po' falsa..

Riproviamo: $\boxed{A \subseteq B}$

Riscriviamo in termini di x, y la trasformazione "soluz $\longrightarrow$ soluz $\times$ fondam^{-1}" che abbiamo nelle var. (w, y)

$$\left(w + \sqrt{k(k-1)}\, y\right) \cdot \left((2k-1) - 2\sqrt{k(k-1)}\right) =$$

$$= \left((2k-1)w - 2k(k-1)y + \sqrt{k(k-1)}\left(-2w + (2k-1)y\right)\right)$$

Siccome $w = (k-1)x$ abbiamo che se (x, y) è soluz, anche $\begin{cases} x' = (2k-1)x - 2ky \\ y' = 2(k-1)x - (2k-1)y \end{cases}$ è soluz.

Sia (x, y) la soluz MINIMA con $x > \sqrt{a}$, wlog $y > 0$

Se $|x'| < x$, allora (x', y') deve risp. $|x'| < \sqrt{a}$

- $x' < x$: $\quad (2k-1)x - 2ky < x$

$$\frac{k-1}{k}x < y \iff \left(\frac{k-1}{k}\right)^2 x^2 < y^2$$

testo $\rightarrow$ $= \dfrac{(k-1)x^2 + a}{k}$

$$\iff (k-1)^2 x^2 < k(k-1)x^2 + ka, \text{ vera perché } k, a > 0$$

- $x' > -x$ $\quad (2k-1)x - 2ky > -x$

$$\iff 2kx > 2ky \iff x^2 > y^2$$

$$0 < k = \frac{x^2 - a > 0}{x^2 - y^2 > 0}$$

∎

Diamo un senso alle congruenze mod p con $\sqrt{d}$

Esempio $F_0 = 0$, $F_1 = 1$, ..., $F_{n+1} = F_n + F_{n-1}$.

Dim che $F_* \equiv 0 \ (p)$ per ogni p primo, $p \neq 5$

↳ una qualche funzione semplice di p

$$F_n = \frac{1}{\sqrt{5}} \left[\varphi^n - \left(-\frac{1}{\varphi}\right)^n \right] \qquad \varphi = \frac{1+\sqrt{5}}{2}$$

$$-1/\varphi = \frac{1-\sqrt{5}}{2}$$

$$F_n \equiv 0 \ (p) \iff \boxed{\varphi^n \equiv (-1/\varphi)^n \mod p}$$

Caso 1: $p \neq 2$ e 5 è un quadrato mod p

Scelgo $a \in \mathbb{Z}$ con $a^2 \equiv 5 \mod p$

$$\left(\frac{a+1}{2}\right)^n \equiv \left(\frac{1-a}{2}\right)^n \mod p$$

è verificata per $n \equiv 0 \ (p-1)$

Caso 2: $p \neq 2$ e 5 NON è un quadrato mod p

Diamo alla congruenza mod p il seguente significato:

$a + b\sqrt{5} \equiv c + d\sqrt{5} \mod p$ (con $a, b, c, d \in \mathbb{Z}$)

se e solo se $a \equiv c$, $b \equiv d \mod p$

Oss Se 5 fosse $\equiv n^2 \bmod p$, le due espressioni

$$n + 0\sqrt{5} \quad \text{e} \quad 0 + 1\sqrt{5}$$

"avrebbero voglia" di essere congrue mod p, ma è difficile formalizzarlo.

$$F_n \equiv 0 \ (p) \iff 2^n F_n \equiv 0 \ (p)$$

$$\iff (1+\sqrt{5})^n \equiv (1-\sqrt{5})^n \bmod p$$

$$\iff (1+\sqrt{5})^{2n} \equiv (1-5)^n \bmod p$$

Se $a_1 + b_1\sqrt{5} \equiv a_2 + b_2\sqrt{5}$ (p) e

$c_1 + d_1\sqrt{5} \equiv c_2 + d_2\sqrt{5}$ (p)

allora $(a_1 + b_1\sqrt{5})(c_1 + d_1\sqrt{5}) \equiv (a_2 + b_2\sqrt{5})(c_2 + d_2\sqrt{5})$ (p)

La dim è scrivere $a_2 = a_1 + k p_1$ etc e sviluppare ∎

Il piccolo teo di Fermat "fallisce":

$$X = 1 + \sqrt{5} \bmod 3$$

$$X^2 = 6 + 2\sqrt{5} \equiv -\sqrt{5} \bmod 3$$

Teo (Fermat ++) $(a + b\sqrt{d})^{p^2-1} \equiv 1 \bmod p$, $p > 2$

Dim. Basta far vedere che $(a+b\sqrt{d})^{p+1} \equiv c + 0\sqrt{d}$ (p)

Calcoliamo $(a + b\sqrt{d})^p \equiv a^p + \binom{p}{1} a^{p-1} b\sqrt{d} + \dots$

$$+ \binom{p}{p-1} a (b\sqrt{d})^{p-1} + b^p \sqrt{d}^{\,p-1} \cdot \sqrt{d}$$

$$\equiv a^p + b^p d^{\frac{p-1}{2}} \sqrt{d} \equiv a + b d^{\frac{p-1}{2}} \sqrt{d} \quad (p)$$

piccolo di Fermat

Per Eulero, $d^{\frac{p-1}{2}} \equiv -1 \ (p)$, quindi

$$(a+b\sqrt{d})^p \equiv a - b\sqrt{d} \mod p$$

$$\Rightarrow (a+b\sqrt{d})^{p+1} \equiv a^2 - db^2 \mod p$$

$$\Rightarrow (a+b\sqrt{d})^{p^2-1} = (\underbrace{a^2-db^2}_{\neq 0})^{p-1} \equiv 1 \mod p$$

FLT

□

Esempio $(1+\sqrt{2})^k \mod 3$

$k=2$: $3+2\sqrt{2} \equiv -\sqrt{2} \mod 3$

$k=4$: $2 = (1+\sqrt{2})(1-\sqrt{2}) \equiv 1-2 \equiv 2 \ (3)$

$k=8$: 1

$(1+\sqrt{5})^n \equiv (1-\sqrt{5})^n \mod p$: sicuramente vera per $n = p^2-1$, perché entrambi i membri sono $\equiv 1 \mod p$, ma è vera anche per $n = p+1$ perché allora sono entrambi congrui a $N(1+\sqrt{5}) \equiv N(1-\sqrt{5}) \equiv -4 \ (p)$

Esempio $a_0 = 2$, $a_{n+1} = 2a_n^2 - 1$. Sia p un primo che divide a_n $(n>0)$. Allora

$$p \equiv \pm 1 \mod 2^{n+2}$$

Soluzione $\cos(2\theta) = 2\cos^2\theta - 1$

Se per caso $a_0 = \cos(\theta_0)$, $a_1 = 2\cos^2(\theta_0) - 1 = \cos(2\theta_0)$,

..., $a_n = \cos\left(2^n \theta_0\right)$

Ma $\cos\theta_0 = \dfrac{e^{i\theta_0} + e^{-i\theta_0}}{2}$ e

$$a_n = \cos\left(2^n\theta_0\right) = \frac{\left(e^{i\theta_0}\right)^{2^n} + \left(e^{-i\theta_0}\right)^{2^n}}{2} = \frac{A^{2^n} + A^{-2^n}}{2}$$

Scritta bene: se $a_n = \frac{1}{2}\left(A^{2^n} + A^{-2^n}\right)$, allora

$$a_{n+1} = 2a_n^2 - 1 = 2\frac{1}{4}\left(A^{2^{n+1}} + A^{-2^{n+1}} + 2\right) - 1.$$

Basta quindi scegliere A in modo t.c.

$$A + A^{-1} = 4 \qquad (a_0 = 2)$$

$$A^2 - 4A + 1 = 0 \iff A = 2 \pm \sqrt{3}$$

$$2a_n = \left(2+\sqrt{3}\right)^{2^n} + \left(2-\sqrt{3}\right)^{2^n} \overset{?}{\equiv} 0 \ (p)$$

$$\left(2+\sqrt{3}\right)^{2^n} \equiv -\left(2-\sqrt{3}\right)^{2^n} \pmod p$$

$$\left(2+\sqrt{3}\right)^{2^{n+1}} \equiv -1 \pmod p$$

$$\Rightarrow \operatorname{ord}_p\left(2+\sqrt{3}\right) = 2^{n+2}$$

- Se 3 è un residuo quad. mod p, allora posso applicare il piccolo Teo Fermat "usuale" per ottenere $2^{n+2} \mid \varphi(p) = p-1$
- Se 3 NON è res. quad. mod p, il FLT "potenziato" dà $2^{n+2} \mid p^2 - 1 = (p-1)(p+1)$, che fornisce solo $p \equiv \pm 1 \ (2^{n+1})$

MA possiamo osservare che $(2+\sqrt{3})^{p+1} \equiv (2+\sqrt{3})(2-\sqrt{3})$

$\equiv 1 \pmod{p} \implies 2^{n+2} \mid p+1$ □

Combiniamo tutto!

Sia $n>0$. Dim. che esistono a,b interi >1 t.c.

$a^2+1 = 2b^2$ e $a \equiv b \pmod{n}$

Soluzione $a^2 - 2b^2 = -1$ ha come soluzioni

- $(1,1)$ è soluz $\rightsquigarrow$ $g = 1+\sqrt{2}$
- Infinite soluzioni: $(1+\sqrt{2})(3+2\sqrt{2})^k = (1+\sqrt{2})^{2k+1}$

$$a_k = \frac{1}{2}\left[(1+\sqrt{2})^{2k+1} + (1-\sqrt{2})^{2k+1}\right]$$

$$b_k = \frac{1}{2\sqrt{2}}\left[(1+\sqrt{2})^{2k+1} - (1-\sqrt{2})^{2k+1}\right]$$

Cerchiamo di imporre $a_k \equiv b_k \mod n$

$$\iff \frac{1}{2}\left[(1+\sqrt{2})^{2k+1} + (1-\sqrt{2})^{2k+1}\right] \equiv \frac{1}{2\sqrt{2}}\left[(1+\sqrt{2})^{2k+1} - (1-\sqrt{2})^{2k+1}\right] \mod n$$

Idea chiave: la congruenza è vera per $k=0$ e i due membri sono periodici.

Come si dimostra la periodicità?

$x^0, x^1, x^2, \dots, x^t \mod n$

Ce ne sono 2 congrue, diciamo $x^r \equiv x^s \mod n$ con $r<s$. SICCOME x è INVERTIBILE

MOD n, LA PRIMA CHE SI RIPETE È 1

La cosa funziona anche qui, perché $1+\sqrt{2}$ è invertibile mod n, visto che l'inverso è $\sqrt{2}-1$

TEORIA DEI NUMERI 3 MEDIUM

Titolo nota 09/09/2019

VARI PROBLEMI

- $\frac{a^2+b^2}{1+ab} = k$ intero $\Rightarrow$ k è un $\square$ (IMO 88/6)
  a, b interi >0
- $\frac{a^2+b^2+1}{ab} = k \in \mathbb{Z} \Rightarrow k=3$ $(a,b>0)$
- $a^m b^n = (a+b)^2+1$ con $m, n, a, b > 0$
- Trova min n per cui esistono infiniti razionali $a_1, \dots, a_n$ con
  $a_1 + \dots + a_n$ intero, $\frac{1}{a_1} + \dots + \frac{1}{a_n}$ intero

RECIPROCITÀ QUADRATICA

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & a \text{ quadrato mod } p \\ -1 & a \text{ non è quadrato mod } p \\ 0 & p \mid a \end{cases}$$

Teo Siano p, q primi dispari, $p \neq q$. Allora

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Ovvero • Se almeno uno fra p e q è $\equiv 1 (4)$, allora $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

• Se $p \equiv q \equiv 3 (4)$ $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

Oss Funziona anche con p, q primi negativi, ad esempio $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$, e quindi

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1 (3) \\ -1, & \text{se } p \equiv 2 (3) \end{cases}$$

$$\left(\frac{1002}{13}\right) = \left(\frac{2 \cdot 501}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{501}{13}\right)$$

$$= \left(\frac{2}{13}\right) \cdot \left(\frac{167}{13}\right) \cdot \left(\frac{3}{13}\right)$$

$$\left(\frac{2}{13}\right) \cdot \left(\frac{-2}{13}\right) \cdot \left(\frac{13}{3}\right)$$

$$= \left(\frac{-1}{13}\right)\cdot\left(\frac{2}{13}\right)^2\cdot\left(\frac{1}{3}\right) = +1$$

Lemma $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv \pm 1 \ (8) \\ -1, & p \equiv \pm 3 \ (8) \end{cases}$

Dim elementare $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \quad (p)$

$$1 = (-1)(-1)$$
$$2 = 2\cdot(-1)^2$$
$$3 = (-3)(-1)^3$$
$$\vdots$$
$$\frac{p-1}{2} = \pm\left(\frac{p-1}{2}\right)(-1)^{\frac{p-1}{2}}$$

moltiplico tutto — $1+2+\cdots+\frac{p-1}{2}$

$$\left(\frac{p-1}{2}\right)! \equiv 2\cdot 4\cdot\cdots\cdot(p-1)\cdot(-1)^{\left(\frac{p-1}{2}\cdot\frac{p+1}{2}\right)\cdot\frac{1}{2}} \pmod p$$
$$\equiv 2^{\frac{p-1}{2}}\cdot\left(\frac{p-1}{2}\right)!\,(-1)^{\frac{p^2-1}{8}} \mod p$$

$$\Rightarrow 2^{\frac{p-1}{2}}\cdot(-1)^{\frac{p^2-1}{8}} \equiv 1 \ (p)$$

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \ (p) \Rightarrow \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \quad \square$$

Dim meno elementare $2^{\frac{p-1}{2}}$, ma

$2 = -(1+i)^2 i$, e quindi

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-i)^{\frac{p-1}{2}}\cdot(1+i)^{p-1} \quad (p)$$
$$\equiv (-i)^{\frac{p-1}{2}}\,\frac{(1+i)^p}{1+i} \quad (p)$$

$$\equiv (-i)^{\frac{p-1}{2}} \frac{1+i^p}{1+i} \mod p$$

Basta controllare i casi per $p \bmod 8$ ∎

Oss $\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 (4) \\ -1, & p \equiv 3 (4) \end{cases}$

Dimostriamo un altro caso speciale

$$\left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 (3)$$

Supponiamo che $\left(\frac{-3}{p}\right) = 1$. Allora la quantità

$$\zeta_3 = \frac{-1+\sqrt{-3}}{2}$$ ha senso modulo p

↳ fissiamo $a \in \mathbb{Z}$ t.c. $a^2 \equiv -3 (p)$ e definiamo $\zeta_3 := 2^{-1} \cdot (-1+a)$

$$\zeta_3^2 + \zeta_3 + 1 \equiv 0 \quad (p)$$

$\Rightarrow$ l'equazione $X^2+X+1 \equiv 0 (p)$ ha 2 sol. mod p

$\Rightarrow$ ——— $X^3 - 1 \equiv 0 (p)$ ha 3 ———

$\Rightarrow p \equiv 1 (3)$ $\quad \operatorname{ord}_p(\zeta_3) = 3 \mid p-1$

↑ Il n° di soluz di $x^k \equiv 1 (p)$ è $(p-1, k)$ ⌟

Viceversa: $p \equiv 1 (3) \Rightarrow X^3 \equiv 1 (p)$ ha 3 soluz.

↳ $g^0, g^{\frac{p-1}{3}}, g^{\frac{p-1}{3} \cdot 2}$

dove g = gen. mod p

$\hookrightarrow (x-1)(x^2+x+1) \equiv 0 \ (p)$ ha 3 soluz. mod p

$\hookrightarrow x = \frac{-1 \pm \sqrt{-3}}{2}$ esistono mod p, cioè

$-3 = \square \mod p$

Sia b una soluz. di $x^2+x+1 \equiv 0 \ (p)$

Sia $a = 2b+1$. Allora $a^2 \equiv 4b^2+4b+1$

$\equiv 4(-b-1)+4b+1 \equiv -3 \ (p)$

Esempio

(RMM 2013) $p_1 = 2^{\overset{q_1}{a}} - 1$, $2^{\overset{q_2}{2a+1}} - 1$, $2^{\overset{q_3}{4a+3}} - 1$ non sono tutti e 3 numeri primi

$\| p_2 \qquad \| p_3$

p_3 primo $\Rightarrow q_3$ primo

$1 \equiv \left(\frac{2}{q_3}\right) \equiv 2^{\frac{q_3-1}{2}} \equiv 2^{q_2} \mod q_3$

└ basta conoscere $q_3 \equiv 4 \cdot 1 + 3 \ (8)$

$\Rightarrow q_3 \mid 2^{q_2} - 1 = p_2 = 2^{2a+1} - 1$

$\|$

$4a+3$

ci deve essere uguaglianza perché sono primi, ma è assurdo $\square$

TST TAIWAN

$(m,n)=1$. Allora $\phi(5^m-1) \neq 5^n-1$

- $m=1$ non funziona
- m pari: n dispari, quindi $v_2(5^n-1)=2$ (il n° di fattori 2 nella fattorizz.)

  ma $8 \mid 5^m-1$, $3 \mid 5^m-1 \Rightarrow 24 \mid 5^m-1$

  $\Rightarrow \phi(24)=4\cdot 2=8 \mid \phi(5^m-1)$, assurdo
- m dispari, $A=5^m-1$.

Se $p^2 \mid A$, allora $p \mid \phi(A)=5^n-1$

$p \mid A = 5^m-1$

$\Rightarrow p \mid (5^n-1, 5^m-1) = 5^{(m,n)}-1 = 4$

(Quindi p dispari $\Rightarrow p^2 \nmid A$)

$A = 4\cdot p_1 \cdots p_k = 5^m-1$

$\phi(A) = 2\cdot(p_1-1)\cdots(p_k-1) = 5^n-1$

Mod p_i ho $5^m \equiv 1 \ (p_i) \Rightarrow 5^{m+1} \equiv 5 \ (p_i)$

$\Rightarrow \left(\frac{5}{p_i}\right) = +1$

$\Rightarrow \left(\frac{p_i}{5}\right) = +1 \Rightarrow p_i \equiv \pm 1 \ (5)$

Siccome $p_i-1 \mid 5^n-1$, $p_i \neq 1 \ (5)$, quindi

$p_i \equiv -1 \pmod 5$

Guardando mod 5: $\prod 4\cdot(-1)^k \equiv -1 \ (5)$

$$\begin{cases} 2\cdot(-2)^k \equiv -1 \ (5) \\ (-1)^k \equiv 1 \ (5) \Rightarrow k \text{ pari}, \ k = 2t \\ 2\cdot(-1)^t \equiv -1 \ (5), \text{ assurdo.} \end{cases}$$ □

Teorema Se a è un intero NON QUADRATO, esistono infiniti primi p per cui $\left(\frac{a}{p}\right) = -1$

Esercizio $a_1, \dots, a_{2019}$ interi ≥ 0

Supponiamo che per ogni $n > 0$ si abbia

$$a_1^n + \dots + a_{2019}^n = \square$$

Quanti sono come minimo gli $a_i = 0$?

Soluz. Sicuramente "so fare" il caso in cui

$$a_1 = \dots = a_k = 1, \quad a_{k+1} = \dots = a_{2019} = 0,$$

con k = più grande quadrato < 2019, cioè 1936

Prendiamo $n = p-1$, $p > \max\{a_i\}$. Allora (se t = n° degli $a_i \neq 0$) ottengo

$$\square \equiv a_1^{p-1} + \dots + a_{2019}^{p-1} \equiv t \pmod p$$

$\xRightarrow{\text{teorema}}$ t è un quadrato $\Rightarrow t \leq 1936$. □

TST di qualche posto

$$2^m - 1 \mid 3^n - 1 \Rightarrow n \text{ pari}$$

$m, n \geq 2$

Soluzione Sia p un primo che divide $2^m - 1$

[Oss gratis: m è dispari]

$p \mid 2^m - 1 \mid 3^m - 1$, e se (per assurdo) n fosse dispari avrei $3^{n+1} \equiv 3 \ (p) \Rightarrow \left(\frac{3}{p}\right) = +1$

* Se $p \equiv 1 \ (4)$, la RQ dice che anche $\left(\frac{p}{3}\right) = \left(\frac{3}{p}\right) = +1$

$\Rightarrow p \equiv 1 \ (3) \Rightarrow p \equiv 1 \ (12)$

* Se $p \equiv -1 \ (4)$, la RQ dà $\left(\frac{p}{3}\right) = -1 \left(\frac{3}{p}\right) = -1$

$\Rightarrow p \equiv -1 \ (3) \Rightarrow p \equiv -1 \ (12)$

Deduciamo che $2^m - 1 \equiv \pm 1 \ (12)$, che è assurdo con entrambi i possibili segni. $\square$

Tanti fattori primi $\equiv 3 \ (8)$

$\forall n > 0$, $2^{3^n} + 1$ ha $\geq n$ divisori primi $\equiv 3 \ (8)$

Idee • $2^9 + 1 = (2^3)^3 + 1 = (2^3 + 1)(2^{3 \cdot 2} - 2^3 + 1)$

$2^{27} + 1 = \underbrace{(2^9 + 1)}(2^{9 \cdot 2} - 2^9 + 1)$

$= (2^3 + 1)(2^{3 \cdot 2} - 2^3 + 1)(2^{9 \cdot 2} - 2^9 + 1)$

• (simile) Sia p un fattore di $2^n + 1$. Allora $p \not\equiv -1 \ (8)$, e se n è dispari non è nemmeno $\equiv 5 \ (8)$

Oss livello basic: $p \mid 2^n+1$ con n pari $\Rightarrow p \equiv 1 (4)$,

quindi posso supporre n dispari

$$2^n+1 \equiv 0 \ (p) \Rightarrow 2^{n+1} \equiv -2 \ (p)$$

$$\Rightarrow \left(\frac{-2}{p}\right) = 1,$$

ma $$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1 \ (8) \\ 1 & p \equiv 3 \ (8) \\ -1 & p \equiv 5 \ (8) \\ -1 & p \equiv 7 \ (8) \end{cases}$$

LEMMA DI THUE

Fissiamo n intero positivo, K mod n.

La congruenza $y \equiv Kx \pmod n$ ha una soluz. intera (x_0, y_0) con $|x_0|, |y_0| \leq \sqrt{n}$

Dim. Prendiamo tutte le coppie (x, y) con

$$0 \leq x \leq \sqrt{n}, \quad 0 \leq y \leq \sqrt{n}$$

Quante sono? $(\lfloor \sqrt{n} \rfloor + 1)\cdot(\lfloor \sqrt{n} \rfloor + 1) > n$ (anche se n è □)

Per ogni coppia calcolo $y - Kx \mod n$.

Per pigeonhole ci sono 2

coppie <u>distinte</u> (x_1, y_1) e (x_2, y_2) t.c.

$$y_1 - Kx_1 \equiv y_2 - Kx_2 \ (p)$$

$$\Leftrightarrow y_1 - y_2 \equiv K(x_1 - x_2) \ (p)$$

$\Rightarrow (x_1 - x_2, y_1 - y_2)$ è soluz, e $|x_1 - x_2| \leq \sqrt{n}$, $|y_1 - y_2| \leq \sqrt{n}$ ∎

Lemma Se $p \equiv 1 \ (4)$ esistono a, b interi t.c.

$$p = a^2 + b^2$$

Dim. Se $p = a^2+b^2 \Rightarrow a^2+b^2 \equiv 0 \ (p)$

$$\Rightarrow (a \cdot b^{-1})^2 \equiv -1 \ (p)$$

(Questo motiva la condiz. $p \equiv 1 \ (4)$). Sia $m \in \mathbb{Z}$ t.c. $m^2 \equiv -1 \ (p)$. Cerco di risolvere $a \cdot b^{-1} \equiv m \ (p)$

$\hookrightarrow$ $a \equiv mb \pmod p$

Thue $\Rightarrow$ c'è soluz $\neq (0,0)$ con $|a|, |b| < \sqrt{p}$.

Allora $0 < a^2+b^2 < 2p$, ed inoltre

$$a^2+b^2 \equiv (mb)^2+b^2$$
$$\equiv b^2(m^2+1) \equiv 0 \ (p)$$

$\Rightarrow a^2+b^2 = p$. ∎

Esercizio Sia p primo t.c. $\left(\frac{7}{p}\right) = +1$. Allora uno fra $\pm p$ si scrive come $y^2 - 7x^2$.

Soluz. Prendo m t.c. $m^2 \equiv 7 \pmod p$, e uso Thue su $y \equiv mx \pmod p \longrightarrow$ soluz $\neq (0,0)$ con $|x|, |y| < \sqrt{p}$.

$$y^2 - 7x^2 \equiv m^2x^2 - 7x^2 \equiv 0 \ (p)$$

$$|y^2 - 7x^2| < 7p$$

$y^2 - 7x^2 = \pm p, \pm 2p, \pm 3p, \pm 4p, \pm 5p, \pm 6p$

ok

in modo analogo a $2p$

mod 4 scopro che $x \equiv y \equiv 0 \ (2)$

$\Rightarrow \left(\frac{y}{2}\right)^2 - 7\left(\frac{x}{2}\right)^2 = \pm p$

$* \quad y^2 - 7x^2 = \pm 5p \quad \Rightarrow \quad y^2 \equiv 7x^2 \ (5)$

$x \not\equiv 0 (5)$: $(y/x)^2 \equiv 2 (5)$ assurdo

$x \equiv 0$: $y \equiv 0 \Rightarrow x^2 - 7y^2 \equiv 0 (25)$, assurdo

$*$ Se $y^2 - 7x^2 = \pm 2p$, x e y sono dispari

$$\left(\frac{3a-7b}{2}\right)^2 - 7\left(\frac{3b-a}{2}\right)^2 =$$

$$= \frac{1}{4}\left[9a^2 + 49b^2 - 42ab - 63b^2 - 7a^2 + 42ab\right]$$

$$= \frac{1}{4}\left[2a^2 - 14b^2\right] = \frac{1}{2}(a^2 - 7b^2) = \pm p$$

(MAGIA!)

Dietro le quinte: $N(y + \sqrt{7}x) = \pm 2p$

Risolviamo $c^2 - 7d^2 = \pm 2 \rightsquigarrow$ e.g. $3 + \sqrt{7}$

$$N\left(\frac{y+\sqrt{7}x}{3+\sqrt{7}}\right) = \frac{N(y+\sqrt{7}x)}{N(3+\sqrt{7})} = \frac{\pm 2p}{2} = \pm p$$

$$\frac{1}{2}\Big(\overset{\shortparallel}{(y+\sqrt{7}x)(3-\sqrt{7})}\Big) = \frac{1}{2}\left(3y - 7x + \sqrt{7}(3x - y)\right)$$

Teo Un intero positivo n è somma di 2 quadrati se e solo se, scrivendo $n = 2^a \cdot p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_\ell^{f_\ell}$

primi $\equiv 1(4)$ primi $\equiv 3(4)$

tutti gli f_i sono pari.

Sketch di dim

$$\underbrace{(a^2+b^2)}_{N(a+bi)}\underbrace{(c^2+d^2)}_{N(c+di)} = \underbrace{(ac-bd)^2+(ad+bc)^2}_{N((a+bi)(c+di))}$$ parte sufficiente

Parte nec: $p \equiv 3(4)$, $p \mid x^2+y^2$

Se per assurdo $p \nmid y$ $\quad \left(\frac{x}{y}\right)^2 + 1 \equiv 0 \ (p)$

$\Rightarrow \left(\frac{-1}{p}\right) = 1$, assurdo

$\Rightarrow p \mid y \Rightarrow p \mid x \Rightarrow p^2 \mid x^2+y^2$ □

Può venire la tentazione di pensare che

$y^2 - ax^2 = \pm p$ ha soluz $\Leftrightarrow \left(\frac{a}{p}\right) = 1$

Controesempio: $y^2 + 5x^2 = 7$ non ha soluzione,

ma $\left(\frac{-5}{7}\right) = +1$