Stage Senior 2014 – Livello Medium

Stampato integrale delle lezioni

Autori vari

Indice

Senior 2014 A1 Medium Simone

Titolo nota 02/09/2014

Se $p(x)$, che ha grado al più n, ha $n+1$ radici, allora $p(x) = 0$.

Supponiamo $\lambda_1, \dots, \lambda_n$ radici distinte, allora applicando Ruffini più volte ottengo

$$p(x) = c(x-\lambda_1)\dots(x-\lambda_n)$$

sia $\alpha \neq \lambda_i$ $\quad p(\alpha) = 0$

$$0 = c\cdot(\alpha-\lambda_1)\cdot\dots\cdot(\alpha-\lambda_n)$$

($\alpha-\lambda_1 \neq 0$, $\alpha-\lambda_n \neq 0$)

quindi $c = 0$ (legge di annullamento del prodotto*)

* infatti su $\mathbb{Z}/6\mathbb{Z}$ questo non è vero: es.

$(x-2)(x-3)$

$x^2 - 5x$ "$\|$" (6).

Per la dimostrazione, oltre alla legge di an. del prodotto, abbiamo usato Ruffini.

Di cosa è figlio Ruffini?

Per la divisione con resto: se $P(x)$ e $Q(x)$ sono due polinomi allora esistono (e unici) due polinomi $q(x)$ e $r(x)$ tali che $\deg(r) < \deg(Q)$

$$P(x) = q(x) \cdot Q(x) + r(x)$$

Sempre vera SE Q è MONICO

$$a_n x^n + \dots + a_1 x + a_0 \;\Big|\; x^3 + \dots + \;\Big|\; a_n x^{n-3}$$

Se Q non è monico non è detto che io lo possa fare, ma vale sempre se A è un campo $(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \dots)$.

Oss. Quando vale la divisione con resto, vale anche Bezout (stessa dimo. che in $\mathbb{Z}$) $(P(x), Q(x)) = 1$ allora esistono $a(x)$ e $b(x)$ $\deg(a) < \deg(q)$, $\deg(b) < \deg(P)$

$$a(x) \cdot p(x) + b(x) Q(x) = 1.$$

Questa cosa ci dice nel caso $\mathbb{Z}[x]$

$p(x), q(x) \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ $\quad a, b \in \mathbb{Q}[x]$

$$a(x) \cdot p(x) + b(x) \cdot q(x) = 1$$

$$a(x) = \frac{\bar{a}(x)}{m} \qquad b(x) = \frac{\bar{b}(x)}{m}$$

$$\bar{a}(x) p(x) + \bar{b}(x) q(x) = d \in \mathbb{Z}$$

$$\text{mcd}\{p(n), q(n)\} \mid d$$

es. $p(x) = x^{2014} + x^{1000} - 2$

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

$$p(x) = q(x) \cdot Q(x) + a \cdot x + b$$

$$p(i) = \cancel{q(i)}^{\,0} \cdot Q(i) + a \cdot i + b$$

$$p(-i) = \cancel{q(-i)}^{\,0} \cdot Q(-i) - a \cdot i + b$$

$$\begin{cases} p(i) = ai + b \\ p(-i) = -ai + b \end{cases}$$

$p(i) = -1 + 1 - 2 = -2$

$p(-i) = -2$

$$p(x) - q(x) \cdot Q(x) = -2$$

$$MCD\left(n^{2014} + n^{1000} - 2,\ n^2 + 1\right) \mid 2$$

$$x^{2014} + x^{1000} - 2 \equiv \pmod{x^2+1}$$

$$\equiv (-1)^{1007} + (-1)^{500} - 2 = -2$$

$$x^2 + 1 \equiv 0$$

$$x^2 \equiv -1$$

$$\frac{\mathbb{Q}[x]}{(x^2+1)} = \{ ax + b \}$$

$$(ax+b)(cx+d) = ac \cdot x^2 + (bc+ad) \cdot x + bd$$

$$\equiv (bc+ad) \cdot x + (bd - ac)$$

Fatto: Se $p(x)$ è irriducibile, allora $\frac{\mathbb{Q}[x]}{(p(x))}$ è un campo.

---

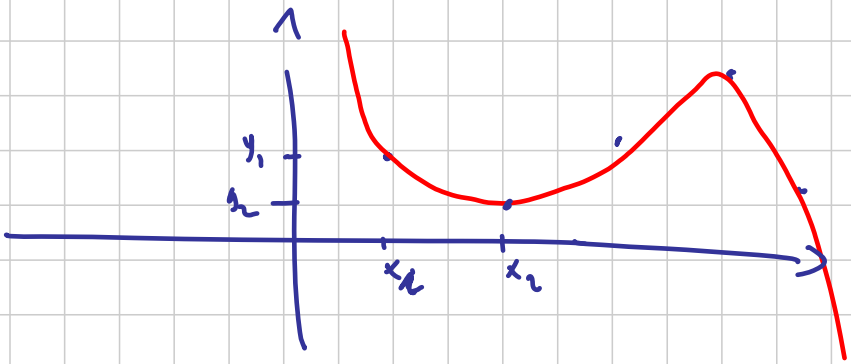
o

Voglio trovare un polinomio "che passi dove voglio", ovvero "che ha dei valori assegnati".

Ho $x_1, \dots, x_n, x_{n+1} \in A$ distinti e $y_1, \dots, y_{n+1} \in A$ non necessariamente distinti.

Q: Esiste un polinomio $p(x) \in A[x]$ tale che

$$p(x_i) = y_i \quad \forall\, i = 1, \dots, n+1$$



A: Sì, ma solo se A è un campo.

(A campo) $L_i(x) = \dfrac{(x-x_1)(x-x_2)\cdots\widehat{(x-x_i)}\cdots(x-x_{n+1})}{(x_i-x_1)(x_i-x_2)\cdots\widehat{(x_i-x_i)}\cdots(x_i-x_{n+1})}$

.

L_i è un polinomio di grado n

tale che $L_i(x_j) = 0 \quad \forall j \neq i \qquad L_i(x_i) = 1$

$$p(x) = \sum_{i=1}^{n+1} y_i L_i(x) \qquad \deg(p) \leq n$$

$$p(x_j) = \sum_{i=1}^{n+1} y_i L_i(x_j) = y_j \underbrace{L_j(x_j)}_{=1} = y_j$$

Dim. 2

$$\begin{cases} a_n \cdot x_1^n + a_{n-1} \cdot x_1^{n-1} + \dots + a_1 \cdot x_1 + a_0 = y_1 \\ a_n \cdot x_2^n + \dots \qquad\qquad a_1 \cdot x_2 + a_0 = y_2 \\ \vdots \qquad\qquad\qquad\qquad \vdots \\ a_n \cdot x_{n+1}^n + \dots \qquad\qquad + a_1 \cdot x_{n+1} + a_0 = y_{n+1} \end{cases}$$

(n colonne, m righe)

$$\begin{pmatrix} x_1^n & x_1^{n-1} & \dots & x_1 & 1 \\ x_2^n & & & x_2 & 1 \\ \vdots & & & \vdots & \vdots \\ x_{n+1}^n & x_{n+1}^{n-1} & \dots & x_{n+1} & 1 \end{pmatrix} \cdot \begin{pmatrix} a_n \\ \vdots \\ a_0 \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_{n+1} \end{pmatrix}$$

Fatto (mistico) se ho un sistema $m \times n$ con $m \leq n$ allora ho almeno una soluzione (in genere)

Fatto 2 (esistenza) se ho un sistema mxn allora il sistema ha una soluzione se $\det(M) \neq 0$.

$$\det\left(V\right) = \prod_{i<j}(x_i - x_j) \neq 0.$$

$\mathbb{Z}[x]$ $\quad p(2)=0$, $\quad p(0)=1$?

Non esiste perché $p(0)=1 \Rightarrow a_0 = 1$

ma allora $p(2)$ è dispari

$$\underbrace{a_n \cdot 2^n + \dots + a_1 \cdot 2}_{\text{roba}} + a_0 = \text{dispari}$$

se $p(x) \in \mathbb{Z}[x]$ $\quad a-b \mid p(a)-p(b)$

$$p(a)-p(b) = a_n\cdot(a^n-b^n) + a_{n-1}\cdot(a^{n-1}-b^{n-1}) - \dots$$

$$\dots + a_1(a-b)$$

$a-b \mid a^m-b^m$ $\forall m$ $\Rightarrow$ $a-b \mid p(a)-p(b)$.

Ricordatevi l'esercizio.

Es. Sia $P(x) \in \mathbb{Z}[x]$. dimostrare che

(i) Sia $Q(x) = \overbrace{P(P(\dots(P(x))}^{k}) - x$. Se $Q(n) = 0$ allora $P(P(n)) = n$ $(n \in \mathbb{N})$

(ii) IMO 2006/5

Dim. $a - b \mid P(a) - P(b)$

(prendo $b = P(a)$)

$a - P(a) \mid P(a) - P(P(a))$

$P(a) - P(P(a)) \mid P(P(a)) - P(P(P(a)))$

$a - P(a) \mid P(a) - P(P(a)) \mid P(P(a)) - P(P(P(a))) \mid P^{(3)}(a) - P^{(4)}(a)$

$\dots \mid P^{(k)}(a) - P^{(k+1)}(a)$

Se $Q(a) = 0 \iff P^{(k)}(a) = a$ $\quad = P(P^{(k)}(a))$

$a - P(a) \mid P(a) - P(P(a)) \mid \dots\dots \mid a - P(a)$

sono uguali

$|a - P(a)| \in |P(a) - P(P(a))| \leq \dots\dots \leq |a - P(a)|$

Quindi $a - P(a) = \pm (P(a) - P(P(a)))$

Caso 1 $a - P(a) = -P(a) + P(P(a)) \Rightarrow P(P(a)) = a$ ok.

Caso 2 $a - P(a) = P(a) - P(P(a))$

$P(a) - P(P(a)) = \pm (P(P(a)) - P(P(P(a))))$

Caso 2.1 $P(a) - P(P(a)) = -P(P(a)) + P(P(P(a)))$

$P(P(a)) = P(P(P(P(a))))$

$\overbrace{P \dots P}^{k}(P(a)) = P(\overbrace{P \dots P}^{k+2}(P(a)))$

$a = P(P(a))$

Caso 2.2. $P(a) - P(P(a)) = P(P(a)) - P(P(P(a)))$

Caso 2.2.2 $\dots$ 1. $P^{(r)}(a) = P^{(r+2)}(a)$

applico P $k-r$ volte ad ambo i membri e ottengo $P^{(k)}(a) = P^{(k+2)}(a)$

cioè $a = P(P(P^{(a)}(a))) = P(P(a))$

Caso II se non ci sono cambi di segno

$P(a) - a = P(P(a)) - P(a) = P(P(P(a)) - P(P(a)) = \dots = P(a) - a$

ma allora $P^{(r)}(a) = a_r$ a_r è prog. aritmetica

$a_k = a_0 \Rightarrow a_r \equiv a_0 = a \Rightarrow a_1 - a_0 = 0$

$P(a) - a = 0$

$P(a) = a \Rightarrow P(P(a)) = a.$

Parte (ii) $Q_k(x) = P^{(k)}(x) - x$ (con k fissato).

Dimostrare che $Q(x)$ ha al più n radici intere, dove $n = \deg(P)$

(i) ci dice che $Q_k(n) = 0 \Rightarrow Q_2(n) = 0$

in particolare n° radici di Q_k è numero di radici di Q_2.

Siano $a_1, a_2, a_3 - - -, a_{n+1}$ radici distinte di $Q_2(x)$

$a_1 - a_2 \mid P(a_1) - P(a_2) \mid P(P(a_1)) - P(P(a_2))$

Supponiamo che $P(P(a_1)) = a_1$ e $P(P(a_2)) = a_2$

$a_1 - a_2 \mid P(a_1) - P(a_2) \mid a_1 - a_2$

Quindi, di nuovo $a_1 - a_2 = \pm (P(a_1) - P(a_2))$

$\exists \quad a_1 - a_2 = P(a_1) - P(a_2) \rightsquigarrow a_1 - P(a_1) = a_2 - P(a_2)$

$\nexists \quad a_1 - a_2 = P(a_2) - P(a_1) \rightsquigarrow a_1 + P(a_1) = a_2 + P(a_2)$

Consideriamo $h(x) = x - P(x)$ $(n. > 0)$

e $g(x) = x + P(x)$

Presi $a_i, a_j \Rightarrow h(a_1) = h(a_j)$ oppure

$g(a_1) = g(a_j)$.

$h(a_j) - h(a_1) = 0 \qquad a_j = a_1$

$g(a_j) - g(a_1) = 0 \qquad h(x) - h(a_1)$

Vuol dire $h(a_2) \neq h(a_1)$

ma allora $g(a_2) = g(a_1)$.

$\forall a_i \quad g(a_i) = g(a_2)$

oppure $h(a_i) = h(a_2)$

$\exists \; j$ t.c. $h(a_j) = h(a_2)$ e $g(a_j) \neq g(a_2)$

$h(a_j) = h(a_2) \neq h(a_1)$

$$g(a_1) \neq g(a_2) = g(a_1)$$

$\Rightarrow$

$P(P(x))$ ha grado n^2 !! ATTENZIONE !

Fattorizzazioni

1- radici razionali
2- Eisenstein
3- Lemma di Gauss
4- modulo p

$P(x) \in \mathbb{Z}[x]$

Radici razionali

$$P(x) = a_n x^n + \dots + a_1 x + a_0$$

Se $r = \frac{p}{q}$ $\quad (p,q)=1$ è radice di $P(x)$, allora $p \mid a_0$ e $q \mid a_n$.

$$0 = P(r) = a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \dots + a_1 \frac{p}{q} + a_0$$

$$0 = a_n p^n + a_{n-1} p^{n-1} \cdot q + \dots + a_1 p \cdot q^{n-1} + a_0 q^n$$

mod q $\quad 0 = a_n \cdot p^n + 0$ $\quad q \mid a_n \cdot p^n$ $\quad q \mid a_n$

mod p $\quad 0 = a_0 \cdot q^n$ $\quad p \mid a_0 \cdot q^n$ $\quad p \mid a_0$

Guardo il polinomio mod p

$$A(x) = P(x) - Q(x)$$

$$\overline{A}(x) = \overline{P}(x) - \overline{Q}(x)$$

Se $\overline{A}$ è irriducibile, anche A lo è

Crit. Eisenstein sia $q(x) \in \mathbb{Z}[x]$ $\deg(q) = n$ tale che $p \nmid a_n$, $p \mid a_i$ $\forall\, 0 \le i \le n-1$ $p^2 \nmid a_0$

$\Rightarrow$ $q(x)$ è irriducibile.

Dim. ($\mathbb{F}_p$) $\quad \overline{q}(x) = a_0 \cdot x^n$

supp che $q(x) = a(x) \cdot b(x)$

$$a_0 x^n = \overline{q}(x) = \overline{a}(x)\,\overline{b}(x)$$

!! fatt. unica

$$\overline{a}(x) = \alpha x^k \qquad \overline{b}(x) = \beta x^{n-k} \qquad (\alpha\beta = a_0)$$

$$a(x) = \tilde{\alpha} x^k + \dots + \alpha_1 x + \alpha_0$$

$$b(x) = \tilde{\beta} x^{n-k} + \dots + \beta_1 x + \beta_0$$

$p \mid \alpha_0$ e $p \mid \beta_0$

$$a(x) \cdot b(x) = x^n \cdot \tilde{\alpha}\tilde{\beta} + \dots + (\alpha_1\beta_0 + \alpha_0\beta_1)x + \alpha_0\beta_0$$

$p^2 \mid a_0 = \alpha_0 \beta_0$ Assurdo!

Dim (continua) $a(x)\, b(x) = p(x)$

$a(x) = \alpha_k x^k + \alpha_{k-1} x^{k-1} + \dots + \alpha_0$

$b(x) = \beta_{n-k} \dots + \beta_0$

$a_0 = \alpha_0 \beta_0$ $\quad p \mid a_0$ ma $p^2 \nmid a_0 \Rightarrow$ wlog $p \mid \alpha_0$, $p \nmid \beta_0$

$a_1 = \alpha_0 \beta_1 + \beta_0 \alpha_1 \rightsquigarrow p \mid \alpha_1$ ($p \mid a_1$, $p \mid \alpha_0$)

$a_2 = \alpha_0 \beta_2 + \alpha_1 \beta_1 + \alpha_2 \beta_0$ $\quad p \mid \alpha_2$

$a_3 = \alpha_0 \beta_3 + \dots + \alpha_3 \beta_0$ $\quad (p \mid \alpha_n)$

$a_k = \alpha_0 \beta_k + \dots + \alpha_{k-1} \beta_1 + \alpha_k \beta_0$

$a_{n-1} = \alpha_{k-1} \beta_{n-k} + \alpha_k \beta_{n-k-1}$

$a_n = \alpha_k \beta_{n-k}$

ma $p \nmid a_n \Rightarrow$ assurdo!

Teorema plus Se $p \mid a_i \ \forall\, i \le k$ e $p^2 \nmid a_0$ allora $p(x)$ ha un fattore irriducibile di grado almeno $k+1$.

Dim. $\overline{p}(x) = \overline{a}_n x^n + \dots + \overline{a}_{k+1} x^{k+1} = x^{k+1} r(x)$

$\overline{p}(x) = \overline{a}_1(x) \cdot \overline{a}_2(x) \cdot \dots \cdot \overline{a}_s(x)$

devo distribuire i fattori di x^{k+1} tra tutti gli $\overline{a}_i$. Supp. per assurdo che $\deg(\overline{a}_i) \le k$

$\Rightarrow$ wlog $x \mid \bar{a}_1(x)$, $x \mid \bar{a}_2(x)$

$\Rightarrow$ termine noto di a_1 e di a_2 e' divisibile per p $\Rightarrow$ ASSURDO perché altrimenti $p^2 \mid a_0$.

IMO 1993-1 $x^n + 5x^{n-1} + 3$ e' irriducibile per $n > 1$.

Eisenstein.pls con $p = 3$ $k = n-2$

$\Rightarrow$ c'e' un fattore irrid di grado almeno $n-1$

ma allora $\begin{cases} x^n + 5x^{n-1} + 3 \text{ e' irrid.} & \text{(ok)} \\ x^n + 5x^{n-1} + 3 = (x - \xi)(\cdot^{n-1}) \end{cases}$

Per il criterio della radice razionale $\xi \mid 3$

$\xi = \pm 1$ $\xi = \pm 3$ ma $p(\xi)$ e' dispari

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

(A) V non divide il polinomio $x^{2014} - x^{1997} + 2$

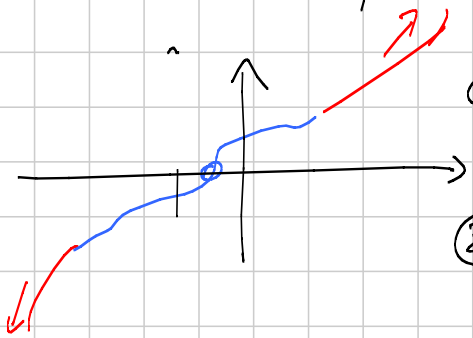
(B) V Ha due radici comp. con. con $Re > 0$

(C) F Ha una radice con $Im > 3/2$ $|\xi_1| < \sqrt{2}$

(D) V Tutte le sue radici (ev. complesse) hanno mod > 1

(E) V Ha un'unica radice reale.

Sv. reali qualsiasi polinom di grado dispr (a coeff. reali) si annulla almeno una volta.



(I) Se deg $p(x)$ ha almeno una radice reale.

(II) tutti i coeff. positivi $\Rightarrow p(x) > 0$ se $x > 0$ (non ha radici positive)

(III) $p(x) = (x+1)(x^2+1) + 1$

$p(-1) = 1$ $\quad p\left(-\frac{3}{2}\right) = \left(-\frac{1}{2}\right)\left(\frac{9}{4}+1\right) + 1 < 0$

ho una radice $r \in \left(-\frac{3}{2}, -1\right)$

Se $x < y < -1$ $\quad x+1 < y+1 < 0$

$x^2 > y^2$

$(x+1)(x^2+1) < (y+1)(x^2+1) < (y+1)(y^2+1)$

$p(x)$ è crescente per $x \le -1$. -1 ha un'unica radice reale

$D(x^n) = n x^{n-1}$

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

Lemma: $p'(x) \geq 0$ in $[0,6] \iff p(x)$ è crescente in $[0,+\infty)$

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

$$p'(x) = 3x^2 + 2x + 1 = (x+1)^2 + 2x^2 > 0 \text{ sempre}$$

$\Rightarrow p(x)$ è crescente sempre.

Lemma ($p(x)$ ha radici doppie $\iff (p(x), p'(x)) \neq 1$)

$$D(p \cdot q)(x) = D(p)(x) \cdot q(x) + p(x) D(q)(x).$$

$p(x)$ ha un'unica radice reale $r \in \left(-\frac{3}{2}, -1\right)$.

ξ_1, ξ_2 le radici complesse $\xi_1 = \overline{\xi}_2$

$r, \xi_1, \overline{\xi_1}$

relazioni di Viète (rel. coeff)

$$(x-r)(x-\xi_1)(x-\overline{\xi_1}) = x^3 + x^2 + x + 2$$

$$r + \xi_1 + \overline{\xi_1} = -1$$

$$2 \operatorname{Re} \xi_1 = -1 - r \in \left(0, \frac{1}{2}\right)$$

$$\operatorname{Re} \xi_1 \in \left(0, \frac{1}{4}\right)$$

$r\xi_1\overline{\xi_1} = -2 \qquad |\xi_1|^2 = -\frac{2}{r} \in \left(\frac{4}{3}, 2\right)$

$|\xi_2| = |\xi_1| \in \left(\sqrt{\frac{4}{3}}, \sqrt{2}\right)$

$q(x) = x^{2014} - x^{1997} + 2 =$

$= (x^{17} - 1)(x^{1997}) + 2 > 4$

$-\frac{3}{2} < r < -1 \qquad r^{17} < -1$

$r^{1997} < -1$

$x^{17} - 1 < -2$

$x^{1997} < -1$

$(x^{17} - 1)\, x^{1997} > 2$

$q(x) > 0 \quad$ per $\quad x < 0$

se $x \geq 1 \qquad x^{2014} > x^{1997} \Rightarrow q(x) > 2$

se $x < 1 \qquad x^{1997} < 1$

$x^{2014} - x^{1997} + 2 > 0 - 1 + 2 > 1.$

Polinomi ciclotomici

Radici dell'unità sono numeri complessi tali che $z^n = 1$ per qualche n.

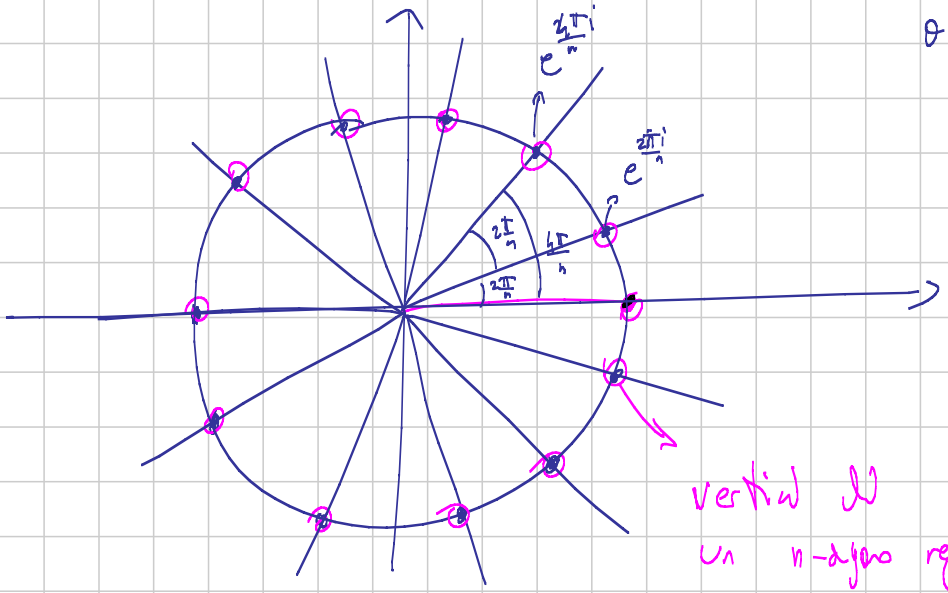
$$z = \rho \cdot e^{i\theta}$$

$$z^n = \rho^n \cdot e^{in\theta} = 1 \qquad \rho = 1$$

$$e^{in\theta} = 1 \iff n\theta = 2\pi k$$

$$\theta = \frac{2\pi k}{n}$$

$k = 1, \dots, n$



vertici di un n-agono regolare

$$\xi_1, \dots, \xi_n \qquad \xi_k = e^{\frac{2k\pi i}{n}}$$

$$x^n = 1 \qquad p(x) = x^n - 1 = (x - \xi_1)(x - \xi_2) \cdots (x - \xi_n)$$

$n = 6$ $\qquad \xi_1 = e^{i\frac{2\pi}{6}} = e^{i\frac{\pi}{3}} = \cos\frac{\pi}{3} + i\,\sin\frac{\pi}{3} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$

$\wedge 2 \quad \wedge 3 \quad \wedge 4 \quad \wedge 5 \quad \wedge 6$

ξ_1	ξ_2	ξ_3	ξ_4	ξ_5	1
ξ_2	ξ_4	1	ξ_2	ξ_4	1
ξ_3	1	ξ_3	1	ξ_3	1
ξ_4	ξ_2	1	ξ_4	ξ_2	1
ξ_5	ξ_4	ξ_3	ξ_2	ξ_1	1

è anche radice 3_a

è anche radice 2_a

$\xi_5 = (\xi_1)^{-1} = \overline{\xi_1}$

è anche radice 3_a

$$(\xi_i)^3 = (\xi_1^i)^3 = \xi_1^{i\cdot 3} = \xi_1^{(i\cdot 3)_6} = \xi_{(i\cdot 3)_6}$$

Se $(k,n) = 1$ allora $\xi_k, \xi_k^2, \dots \to \xi_k^n$ sono tutti distinti e sono tutte le radici n-esime dell'unità

$$\xi_k^j = e^{\frac{2\pi i j k}{n}} = 1$$

$$\frac{2\pi j k}{n} = 2\pi s$$

$$jk = ns$$

$$n \mid jk \Rightarrow n \mid j$$

$$\Rightarrow j \geq n$$

Se $(k,n) = 1 \Rightarrow \operatorname{ord}(\xi_k) = n$

Se $(k,n)=1 \Rightarrow \operatorname{ord}(\zeta_n) = n \Rightarrow$ rad. primitive sono $\phi(n)$

Se $(k,n)=d \Rightarrow \operatorname{ord}(\zeta_k) = \frac{n}{d} \Rightarrow$ rad. con ordine $\frac{n}{d}$ $\varphi(\frac{n}{d})$

$\frac{2\pi j k}{n} = 2\pi s \qquad jk = ns \qquad \frac{n}{d} \mid j \cdot \frac{k}{d}$

$\Downarrow$

$\frac{n}{d} \mid j$

$(k,n)=d \qquad dk' \text{ t.c. } (k', \frac{n}{d}) = 1 \qquad \varphi(\frac{n}{d})$

$\Downarrow$

$(k', \frac{n}{d}) = 1$

radici n-esime $= n = \sum_{d \mid n} \underbrace{\text{radici } n\text{-esime che hanno ordine } \frac{n}{d}}_{=\varphi(d)} = \sum_{d \mid n} \varphi(d)$

$$\Phi_n(x) = \prod_{(k,n)=1} \left(x - e^{\frac{2\pi i k}{n}}\right)$$

$$\deg(\Phi_n) = \varphi(n)$$

$$x^n - 1 = \prod_{k=1}^{n} \left(x - e^{\frac{2\pi i k}{n}}\right) = \prod_{d \mid n} \prod_{(k',\frac{n}{d})=1} \left(x - e^{\frac{2\pi i k'}{n/d}}\right)$$

$$= \prod_{d \mid n} \Phi_{\frac{n}{d}}(x)$$

$$\Phi_1(x) = x - 1$$

$$\Phi_2(x) = x + 1$$

$$\Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1$$

$$\Phi_4(x) = x^2 + 1$$

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1 = \frac{x^5 - 1}{x - 1}$$

$$\Phi_6(x) = x^2 - x + 1.$$

$$(x^3+1)(x^3-1) = x^6 - 1 = \Phi_1(x)\,\Phi_2(x)\,\Phi_3(x)\,\Phi_6(x)$$

$$= (x-1)(x+1)(x^2+x+1)\,\Phi_6(x)$$

$$= (x^3 - 1)(x+1)\,\Phi_6(x)$$

$$\Phi_6(x) = \frac{x^3 + 1}{x + 1} = x^2 - x + 1$$

$$\Phi_{15}(x) = \frac{x^{15} - 1}{\Phi_1(x)\,\Phi_3(x)\,\Phi_5(x)} = \frac{x^{15} - 1}{(x^5 - 1)(x^2 + x + 1)} =$$

$$= \frac{x^{10} + x^5 + 1}{x^2 + x + 1} \stackrel{?}{=}$$

$$X^n - 1 = \prod_{d|n} \Phi_d(x)$$

$$\Phi_n(x) = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})}$$

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n \text{ non è sq.free} \\ (-1)^k & \text{se } n = p_1 p_2 \cdots p_k \end{cases}$$

$$\left(\text{se } h(n) = \sum_{d|n} g(d) \iff g(n) = \sum_{d|n} h(d)\mu\left(\frac{n}{d}\right) \right)$$

Es. Fissato n, esistono infiniti primi $p \equiv 1 \ (n)$

Dim. Sia $a > 1$ a multiplo di n, considero $p \mid \Phi_n(a)$ $p \nmid n$

$$\Phi_n(a) \equiv 0 \ (p)$$

$$a^n - 1 \equiv 0 \ (p)$$

$$a^n \equiv 1 \ (p) \qquad \operatorname{ord}_p(a) \mid n$$

supponi $\operatorname{ord}_p(a) = d$

$$a^d \equiv 1 \quad \text{con } d < n$$

$$\frac{a^n - 1}{a^d - 1} = (a^d)^{\frac{n}{d}-1} + (a^d)^{(\frac{n}{d}-2)} + \cdots + (a^d) + 1$$

$$\equiv \frac{n}{d} \ (p)$$

assurdo se $p \nmid n$

$$\Phi_n(a) \cdot (a^d - 1) \mid a^n - 1 \qquad p \mid \Phi_n(a) \mid \frac{a^n - 1}{a^d - 1}$$

$\mathrm{ord}_p(a) = n$ $\quad \mathrm{ord}_p(a) \mid p-1$ $\quad n \mid p-1$

$p \equiv 1 \pmod{n}$.

$q \mid \Phi_n(p^n)$ $\quad \Phi_n(q p^n)$.

Considero $q \mid \Phi_n(p^n)$ $\quad \mathrm{ord}_q(p^n) = n$

a multiplo di $n \Rightarrow p \neq n$.

$p \mid \Phi_n(a)$.

Algebra 2 - Medium [Tess]

Approccio contoso

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

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

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

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

Ho vinto per bunching

- Polinomi
- Grado omogeneo
- sommatorie simmetriche

Th: $\sum_{sym} a_1^{t_1} a_2^{t_2} \cdot \ldots \cdot a_n^{t_n} \geq \sum_{sym} a_1^{u_1} \cdots a_n^{u_n}$ è vera se

$a_i \geq 0 \quad \forall i$

(wlog $t_1 \geq t_2 \geq \ldots \geq t_n$, $u_1 \geq \ldots \geq u_n$)

- $t_1 \geq u_1$
- $t_1 + t_2 \geq u_1 + u_2$
- $\vdots$
- $t_1 + \ldots + t_n = u_1 + \ldots + u_n$

$\Big\} >$

Vettori non confrontabili per bunching

$(3,3,0) \qquad (4,1,1)$

$\Rightarrow$ non è sempre vero che $\sum_{sym} a^3b^3 \geq \sum_{sym} a^4bc$

ne $\sum_{sym} a^3b^3 \leq \sum_{sym} a^4bc$

Esempio

$a,b,c > 0 \quad a+b+c = 3$

$$\sum_c \frac{1}{a^2} \geq \sum_c a^2$$

$$\sum_c a^2b^2 \geq \sum_c a^4b^2c^2$$

$$\sum_c a^2b^2(\sum a)^4 \geq 81 \sum_c a^4b^2c^2$$

$$\sum_c a^2b^2 \cdot \left(\sum a^2 + 2\sum ab\right)^2 \geq 81 \sum_c a^4b^2c^2$$

$$\sum_c a^2b^2 \cdot \left((\sum a^2)^2 + 4\sum a^2 \sum ab + 4(\sum ab)^2\right) \geq 81 \sum_c a^4b^2c^2$$

$$\sum a^4 + 2\sum a^2b^2 + 4\sum(a^3b + a^2bc + a^3c)$$
$$+ 4\left(\sum a^2b^2 + 2\sum a^2bc\right)$$
$$\left(\sum_c a^4 + 6\sum a^2b^2 + 4\sum_s a^3b + 12\sum a^2bc\right)$$

$$\sum_s a^6b^2 + \sum_c a^4b^2c^2 + 6\sum a^4b^4 + 12\sum a^4b^2c^2$$
$$4\sum_s a^5b^3 + 4\sum_s a^3b^3c^2 + 4\sum_s a^5b^2c$$
$$12\sum_s a^4b^3c + 12\sum a^3b^3c^2$$
$$\geq 81 \sum_c a^4b^2c^2$$

Bunching da solo non basta !!

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

forte + scarso $\geq$ 2 medio

è equivalente a Schur :

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

Data la simmetria posso supporre

$a \geq b \geq c$

$$\sum_{} \; \geq \; a(a-b)(a-c) + b(b-a)(b-c) =$$

($a-b \geq 0$, $a-c \geq 0$, $b-a \leq 0$, $b-c \geq 0$)

$$= (a-b)\left[a^2 - ac - b^2 + bc \right]$$

$$= (a-b)^2 (a+b-c)$$

($(a-b)^2 \geq 0$, $a+b-c \geq 0$)

Lo stesso risultato si ha per

$$\sum_{c} a^m (a^n - b^n)(a^n - c^n) \geq 0$$

$m, n \geq 0$

altre varianti si ottengono ponendo al posto di a, b, c, ab, bc, ca.

Esempio asimmetrico

$$\sum_c a^4 b \geq \sum_c a^2 b^2 c$$

$$a^4 b + b^4 c + c^4 a \geq a^2 b^2 c + a^2 b c^2 + a b^2 c^2$$

→ si fa con AM-GM pesata

$$\frac{X a^4 b + Y b^4 c + Z c^4 a}{X+Y+Z} \geq \sqrt[X+Y+Z]{(a^4 b)^X (b^4 c)^Y (c^4 a)^Z}$$

sommo le cicliche di questa disug. e ottengo la tesi

voglio capire chi sono X, Y, Z

Se scelgo X, Y, Z $\quad a^2 b^2 c$

chi ottengo sotto la radice?

a) $\frac{4X+Z}{X+Y+Z} = 2$

b) $X + 4Y = 2(X+Y+Z)$

c) - - - - - omogeneo

$2X = 2Y + Z$ $\qquad 2X = X + 2Z + Z$

$2Y = X + 2Z$ $\qquad X = 3Z$

$2Y = 5Z$

Una scelta è $Z=2 \quad Y=5 \quad X=6$

Ho trovato dei pesi positivi, e sono felice :)

Disuguaglianze con frazioni

Esempio 1

$$\sum_{c} \frac{a}{b+2c+d} \geq 1$$

C-S: $\left(\sum_i a_i^2\right)\left(\sum_i b_i^2\right) \geq \left(\sum_i a_i b_i\right)^2$

$$\left(\sum_i a_i^2\right) \geq \frac{\left(\sum a_i b_i\right)^2}{\sum_i b_i^2}$$

$a_i = \frac{c_i}{b_i} \Rightarrow$

$$\sum_i \frac{c_i^2}{b_i^2} \geq \frac{\left(\sum c_i\right)^2}{\sum b_i^2}$$

$d_i = \sqrt{b_i}$

$$\sum_i \frac{c_i^2}{d_i} \geq \frac{\left(\sum c_i\right)^2}{\sum d_i}$$

← Lemma di Titu vale per $d_i > 0$

$$\sum_c \frac{a}{b+2c+d} \geq \frac{\left(\sum_c \sqrt{a}\right)^2}{4\sum_c a} \geq 1$$

$c_i = \sqrt{a}$

$d_i = b+2c+d$

hope!

Però le nostre sono vane speranze

Proviamo così:

$$\sum_c \frac{a^2}{(b+2c+d)a} \geq \frac{(\sum a)^2}{\frac{1}{2}\sum_s ab + 2ac + 2bd} \geq 1$$

$c_i = a$, $d_i = den$ — hope

$$(\sum a)^2 = \sum a^2 + \frac{1}{2}\sum_s ab \geq \frac{1}{2}\sum_s ab + 2ac + 2bd$$

$\Leftrightarrow$

→ ora sono felice: $(a-c)^2 + (b-d)^2 \geq 0$

Esempio 2

$xyz = 3(x+y+z)$

$$\sum_c \frac{1}{x^2(y+1)} \geq \frac{3}{4(x+y+z)}$$

non è omogeneo!

piccola sostituzione

$x \to \frac{1}{a}$ e cyc

la cond. è $1 = 3\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right)abc$

$$\frac{1}{3} = ab+bc+ca$$

la dis. è

$$\sum_{cyc} \frac{a^2b}{b+1} \geq \frac{3abc}{4(ab+bc+ca)}$$

$$\sum_{cyc} \frac{a^2b}{b+1} = \sum_{cyc} \frac{a^2}{\left(\frac{b+1}{b}\right)} \geq \frac{\left(\sum a\right)^2}{3+\sum \frac{1}{a}}$$

T.: t_0

hope:

$$\left(\sum a\right)^2 + \sum ab \geq 9abc + 3\sum ab$$

$$\left(\sum a\right)^2 \frac{4}{3} \geq 9abc + 3\sum ab$$

$$\frac{4}{3}\sum a^2 + \frac{8}{3}\sum ab \geq 9abc + \frac{9}{3}\sum ab$$

$$4\sum a^2 \geq 27abc + \sum ab$$

$$\sum a^2 \geq \sum ab \qquad \sum a^2 \geq 9abc$$

hope

$$\sum a^2 \geq \sum ab = \frac{1}{3}$$

$$\frac{1}{3} \geq 9abc \Rightarrow \left(\sum ab\right)^2 \cdot 3 \geq 81a^2b^2c^2$$

per AM-GM su tutti i termini

Esempio 3

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

variante di C-S

$$\left(\sum a_i^3\right)\left(\sum b_i^3\right)\left(\sum c_i^3\right) \geq \left(\sum a_i b_i c_i\right)^3$$

$$\Updownarrow$$

$$\left(\sum a_i\right)\left(\sum b_i\right)\left(\sum c_i\right) \geq \left(\sum \sqrt[3]{a_i b_i c_i}\right)^3$$

l'idea per applicarla è far sparire le $\sqrt[3]{}$

$$a_1 = \frac{a}{\sqrt{a^2+8bc}}$$

come scelgo b_1 e c_1?

potrei fare $b_1 = \sqrt{a^2+8bc}$ e $c_1 = a^2$

invece

potrei fare $b_1 = \frac{a}{\sqrt{a^2+8bc}}$ $\quad c_1 = a(a^2+8bc)$

cosa ottengo

$$\left(\sum \text{testo}\right)^2 \left(\sum_{cic} (a^3+8abc)\right) \geq \left(\sum a\right)^3$$

hope:

$$\left(\sum a\right)^3 \geq \sum_{cic} (a^3+8abc)$$

$$\sum \cancel{a^3} + 3\sum_{sym} a^2 b + 6abc \geq \sum \cancel{a^3} + 24abc$$

(IMO 2001, 2)

Esempio 4 (SL A7, 2009 o 2010)

$a^2+b^2+c^2=3$; $a+b,\ b+c,\ c+a > \sqrt{2}$

$$\Rightarrow \sum_c \frac{a}{(b+c-a)^2} \geq \frac{3}{(abc)^2}$$

con C-S (T1 TV)

$$\sum \frac{a^2}{a(b+c-a)^2} \geq \frac{(\sum a)^2}{\sum a(b+c-a)^2} \overset{\text{hope}}{\geq} \frac{3}{(abc)^2}$$

$a+b > \sqrt{2}$

$a^2+b^2 \geq \frac{(a+b)^2}{2} > 1$

$\Rightarrow c^2 = 3-a^2-b^2 < 2$

$c < \sqrt{2} < a+b$

$$\left(\sum_c \frac{a}{(b+c-a)^2}\right)\left(\sum (b+c-a)a\right)\left(\sum (b+c-a)a\right) \geq \left(\sum a\right)^3$$

↑ C-S a 3

uno adesso cambia un poco le terne

$$\sum \frac{a}{(b+c-a)^2} \cdot \sum (b+c-a)a^2 \cdot \sum (b+c-a)a^3 \geq \left(\sum a^2\right)^3$$

$$\frac{27}{9}(abc)^2 \geq \sum (b+c-a)a^2 \cdot \sum (b+c-a)a^3$$

($a=b=c=1$ è l'=; ↑ 3 term; ↑ 3 term.)

vorrei ?

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

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

⊛ è schur ! ☺

⊛ $\sum a^4 - \sum_S a^3 b + 3abc \overset{?}{\geq} 0$

schur con $m=2, n=1$ è

$$\sum a^4 - \sum_S a^3 b + \sum_S a^2 bc \geq 0$$

$\sum a \overset{?}{\leq} 3$ vera per AM-QM .

Esempio 5

$$\sum_c \frac{1}{a^3+b^3+abc} \leq \frac{1}{abc}$$

(viene con bunching)

idea per risparmiare i conti:

lavoro sulla singola frazione

vorrei $X(a,b,c) \leq a^3+b^3+abc$

$ab(a+b+c) = a^2b + ab^2 + abc \leq a^3+b^3+abc$

allora mi rimane $\sum_c \frac{1}{ab(a+b+c)} \leq \frac{1}{abc}$

questa è un = !!!

Esempio 6

$abc=1$ $\qquad \sum_{cyc} \frac{1}{a+b^{20}+c^{12}} \leq 1$

$\frac{1}{a+b^{20}+c^{12}} \leq ?$

C-S !

$(\sum a_i)(\sum b_i) \geq (\sum \sqrt{a_i b_i})^2$

$(a+b^{20}+c^{12})\left(a^{2t-1}+b^{2t-20}+c^{2t-12}\right) \geq (a^t+b^t+c^t)^2$

(t reale generico)

mi rimane

$$\sum_{cyc} \frac{a^{2t-1}+b^{2t-20}+c^{2t-12}}{(a^t+b^t+c^t)^2} \leq 1$$

$$\sum_{cyc} a^{2t-1} + \sum_{cyc} a^{2t-20} + \sum_{cyc} a^{2t-12} \leq \sum_{cyc} a^{2t} + 2\sum_{cyc} a^t b^t$$

$a^{2t-1} \geq (abc)^{\frac{1}{3}}$, $a^{2t-20} \geq (abc)^{\frac{20}{3}}$

- $\left(2t-20+\frac{20}{3}, \frac{20}{3}, \frac{20}{3}\right) \leq (t,t,0)$

  basta che $t > \frac{20}{3}$ e $t \leq 20-\frac{20}{3}=\frac{40}{3}$

- $(2t-12+4, 4, 4) \leq (t,t,0)$

basta $t \geq 4$; $t \leq 8$

basta che $t = 7$ va bene!

Disuguaglianze con Radici

Tecniche

1) tra RHS e LHS ∃ 1 numero

2) fondere le radici con tecniche tipo AM-QM, C-S

3) ridurre la disuguaglianza termine a termine

Esempio 1

$a+b+c = 1$

$$\sum_c \sqrt{1-a} \leq \sqrt{2}\left(\sqrt{\sum_c ab} + 2\sqrt{\sum a^2}\right)$$

① ∃ un numero? SÌ

$$\sum_c \sqrt{1-a} \leq \sqrt{6}$$

$\sqrt{A}+\sqrt{B}+\sqrt{C} \leq \sqrt{3}\sqrt{A+B+C}$

② : $LHS \leq \sqrt{3}\sqrt{3-(a+b+c)} = \sqrt{6}$

mi manca $\sqrt{6} \leq \sqrt{2}\left(\sqrt{\sum_c ab} + 2\sqrt{\sum_c a^2}\right)$

al quadrato ...

$$3 \leq \sum_c ab + 4\sum_c a^2 + 4\sqrt{\sum ab \sum a^2}$$

$$3\left(\sum a\right)^2 \leq \quad ,,$$

$$3\sum a^2 + 6\sum ab \leq \sum ab + 4\sum_c a^2 + 4\sqrt{\sum ab}\sum a^2$$

$$\sum a^2 \geq \sum ab \qquad \geq 3\sum_c a^2 + \sum ab \qquad \geq 4\sqrt{\sum ab \sum ab}$$

Esempio 2

$$\sum_c \frac{2}{\sqrt{a+b}\sqrt{a+c}} \leq \frac{3}{2}$$

$$\sum_c 2\sqrt{b+c} \leq \frac{3}{2}\left((a+b)(b+c)(c+a)\right)^{\frac{1}{2}}$$

2 modi:

- Jensen sulla $f(x) = \sqrt{x}$ (concava)
  sui termini $b+c,\ c+a,\ a+b$
  e con pesi $\frac{a}{\sum a},\ \frac{b}{\sum b},\ \frac{c}{\sum c}$

- C-S

  $2\sqrt{b+c} = A_1 B_1$

  se $A_1 = 2 \quad B_1 = \sqrt{b+c}$

  otterrei $\sum 2\sqrt{b+c} \leq \sqrt{a^2+b^2+c^2}\sqrt{2(a+b+c)}$

  invece, $A_1 = \sqrt{a} \quad , B_1 = \sqrt{ab+ac}$

Ora rimane $\sqrt{\sum a} \cdot \sqrt{2\sum ab} \leq \frac{3}{2}(\ ,,\ )^{\frac{1}{2}}$

$$8 \sum a \sum ab \le 9(a+b)(b+c)(c+a)$$

$$8\left(\sum_s a^2b + 3abc\right) \le 9\left(\sum_s a^2b + 2abc\right)$$

AM - GM

Esempio 3

$$ab+bc+ca \le 3abc$$

$$\sum_c \sqrt{\frac{a^2+b^2}{a+b}} + 3 \le \sqrt{2} \sum_c \sqrt{a+b}$$

① NO! per omogeneità

② NO! per problemi con le radici a DX

③ Term. a term.:

$$\sqrt{2}\sqrt{a+b} \overset{?}{\ge} \sqrt{\frac{a^2+b^2}{a+b}} + ?$$

$\sqrt{2}\sqrt{A+B} \ge \sqrt{A}+\sqrt{B}$

$$\sqrt{2}\sqrt{\frac{(a+b)^2}{a+b}} = \sqrt{2}\sqrt{\frac{a^2+b^2}{a+b} + \frac{2ab}{a+b}} \ge \sqrt{\frac{a^2+b^2}{a+b}} + \sqrt{\frac{2ab}{a+b}}$$

mi rimane

$$\sum_c \sqrt{\frac{2ab}{a+b}} \ge 3 \qquad \left(ab+bc+ca \le 3abc\right)$$

$$\sum_c \sqrt{\frac{2}{\frac{1}{a}+\frac{1}{b}}} \ge 3 \qquad \left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c} \le 3\right)$$

sostituisco $x = \frac{1}{a}$ e cyc

$\sum_c \sqrt{\frac{z}{x+y}} \geq 3 \qquad x+y+z \leq 3$

$\sqrt{2} \sum_c \sqrt{x+y}\sqrt{x+z} \geq 3\sqrt{x+y}\sqrt{y+z}\sqrt{z+x}$

al quadrato

$2\left(\sum_c x^2 + 3\sum xy\right) + 4\sqrt{x+y}\sqrt{x+z}\sqrt{y+z}\sum\sqrt{x+y} \geq 9(x+y)(y+z)(z+x)$

omogeneizzo molt. sopra per $\frac{x+y+z}{3}$

Separatamente

$2\sum x^2\sum x + 6\sum xy\sum x \geq 9\left(\sum_s x^2y + 2xyz\right)$

$2\sum x^3 + 2\sum_s x^2y + 6\sum_s x^2y + 6\sum xyz \geq 9\sum_s x^3y + 18xyz$

$2\sum x^3 \geq \sum_s x^2y$ ✓ Bunching

$4\sum\sqrt{x+y}\sum x \geq 18\left(\sum_s x^2y + 2xyz\right)^{\frac{1}{2}}$

elev. al ^{2} viene ....

EX per casa

$\sum_c \sqrt{a^4+a^2b^2+b^4} \geq \sum_c 2\sqrt{2a^2+bc}$

$(a,b,c \geq 0)$

A3 – MEDIUM SCAMBRET

Titolo nota 05/09/2014

$a_{n+2} = \alpha a_{n+1} + \beta a_n + \text{Mostro}(n)$ (*)

a_n e $\overline{a_n}$ che risolvono (*)

$a_n - \overline{a_n}$

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

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

$a_n = \underbrace{(a_n - \overline{a_n})}_{\text{SOLUZIONE GENERALE DI (*) SENZA MOSTRO}} + \underbrace{\overline{a_n}}_{\text{SOLUZIONE SPECIALE DI (*) CON MOSTRO}}$

$a_n - \overline{a_n} = a_n^*$

Esempio 1: $a_{n+1} = c a_n + d$ $(c \neq 1)$

1) $a_1 = c a_0 + d$

$a_2 = c^2 a_0 + cd + d$

$a_3 = c^3 a_0 + c^2 d + cd + d$

$a_n = c^n a_0 + d(c^{n-1} + c^{n-2} + \dots + 1)$

$= c^n a_0 + d \frac{c^n - 1}{c - 1}$

2) $a_{n+1} = ca_n + d$

$a_{n+1}^* = ca_n^* \rightarrow a_n^* = c^n \cdot \alpha$

$\overline{a_{n+1}} = c\overline{a_n} + d$

Euristica: se mostro (n) è un polinomio di grado q, allora $\overline{a_n}$ un polinomio di grado q
- se mostro (n) è b^n, $\overline{a_n} = \phi \cdot b^n$

$\overline{a_n} = \ell$

$\ell = c\ell + d \rightarrow \ell = -\frac{d}{c-1}$

$a_n = c^n \alpha - \frac{d}{c-1}$

Esempio 2 $a_{n+1} = 5a_n - 4n \qquad a_0 = b$

$a_n^* = 5^n \cdot \alpha$

$\overline{a_n} = cn + d$

$c(n+1) + d = 5(cn + d) - 4n$

$cn + c + d = 5cn + 5d - 4n$

$c = 1 \quad d = \frac{1}{4}$

$a_n = 5^n \cdot \alpha + n + \frac{1}{4}$

Esempio 3 $a_{n+2} = 6a_{n+1} - 8a_n + 4^n$

$a_n^* = \lambda_1 \cdot 2^n + \lambda_2 \cdot 4^n$

$\overline{a_n} = \phi \cdot 4^n$

$\phi \cdot 4^{n+2} = 6\phi \cdot 4^{n+1} - 8\phi 4^n + 4^n$

$16\phi = 24\phi - 8\phi + 1$

$\rightsquigarrow 0 \cdot \phi = 1$

Euristica: se $\text{resto}(n) = b^n$, ma b è soluzione dell'equazione associata della ricorrenza senza resto (con molteplicità m)

$\overline{a_n} = \phi \cdot n^m \cdot b^n$

Esempio (n+1) $a_{n+2} = 4a_{n+1} - 4a_n + 2^n$

$\overline{a_n} = \phi \cdot n^2 \cdot b^n$

Euristica: se $\text{resto}(n) = f(n) + g(n)$ produce $\overline{a_n} = \overline{f_n} + \overline{g_n}$

Esempio (n+2): $a_{n+2} = 5a_{n+1} - 6a_n + n^2 \cdot 3^n$

BMO 2004/1 $\quad a_n \in \mathbb{N}$

$$\begin{cases} a_{m+n} + a_{m-n} - m + n - 1 = \frac{1}{2}(a_{2m} + a_{2n}) \quad m \geq n \geq 0 \\ a_1 = 3 \end{cases}$$

$a_{2004} = ?$

$n=0 \quad 2a_m - m - 1 = \frac{1}{2}(a_{2m} + a_0)$

$m=0 \quad a_0 = 1$

$$4a_m - 2m - 3 = a_{2m}$$

$n=1 \quad a_{m+1} + a_{m-1} - m = \frac{1}{2}(4a_m - 2m - 3 + 2)$

$$(**) \quad \boxed{a_{m+1} = 2a_m - a_{m-1} + 2} \quad \forall m \geq 1$$

$a_0 = 1, \; a_1 = 3$

$a_m^* = \lambda_1 \cdot 1^n + \lambda_2 \, n \cdot 1^n = \lambda_1 + \lambda_2 n$

$\overline{a_m} = am^2 + bm + c$

$a = 1$

$a_m = m^2 + \lambda_2 m + \lambda_1$

$a_m = m^2 + m + 1$

BMO '03/3 $\quad f : \mathbb{Q} \to \mathbb{R}$

i) $f(1) > -1$

ii) $f(x+y) - xf(y) - yf(x) + x + y - xy - f(x)f(y)$ $\quad = 0$

iii) $f(x) - 2f(x+1) - x - 2 = 0$

(i) $x=y=0 \rightarrow f(0) \in \{0,1\}$

(iii) $x=0 \rightarrow f(1) \in \{-1, -\frac{1}{2}\}$

$f(1)=-\frac{1}{2} \quad f(0)=1$

(ii) $x=n \quad f(n)=2f(n+1)+n+2$

$f(n)=a_n$

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

$a_n^* = \alpha \cdot \frac{1}{2^n}$

$\overline{a_n} = cn+d$

$$cn+c+d=\frac{cn+d-n-2}{2}$$

$c=-1 \quad d=0$

$a_n = f(n) = \frac{\alpha}{2^n} - n$

$1 = a_0 = f(0) = \frac{\alpha}{1} - 0 \rightarrow \alpha = 1$.

$f(n) = \frac{1}{2^n} - n \quad \forall n \in \mathbb{N}$

$g(x) = f(x) + x$

(ii) $g(x+y) = g(x)g(y)$ ←

(iii) $g(x) = 2g(x+1)$

Algebra 3 (Medium) – Alberto Alfarano

IMO SL 1992 A2

$a, b \in \mathbb{R}^+ \quad f: \mathbb{R}^+ \to \mathbb{R}^+$

$$f(f(x)) + af(x) = b(a+b)x \quad \forall x \in \mathbb{R}^+$$

Eustrea: $f(f(x)), f(x), x \to$ successioni

$x_0 \in \mathbb{R}^+ \qquad x_{n+1} = f(x_n)$

$x = x_n \qquad x_{n+2} + ax_{n+1} = b(a+b)x_n \quad \forall n$

$$x^2 + ax - b(a+b) = 0$$

$R_1 = b \qquad R_2 = -(a+b)$

$$x_n = \lambda_1 \cdot b^n + \lambda_2 (-a-b)^n$$

$a + b > b$

Se $\lambda_2 \neq 0 \quad |\lambda_2 (-a-b)^n| > |\lambda_1 b^n|$

$\to \exists M: x_M < 0$

$\lambda_2 = 0 \to x_n = \lambda_1 \cdot b^n$

$x_0 = \lambda_1 \cdot b^0 = \lambda_1$

$\to x_n = x_0 \cdot b^n$

$x_1 = f(x_0) = x_0 \cdot b$

$\to f(x) = bx \quad \forall x > 0$

BMO 2002/4

$f: \mathbb{N}^+ \to \mathbb{N}^+$ $\quad 2n+2001 \le f(f(n)) + f(n) \le 2n+2002$

BMO 2009/4 $\qquad f: \mathbb{N}^+ \to \mathbb{N}^+$

$$f\left(f^2(m) + 2f^2(n)\right) = m^2 + 2n^2$$

$n = 2014$ $\quad f\left(f^2(m) + 2f^2(2014)\right) = m^2 + 2 \cdot 2014^2$

$$m^2 = m_1^2 \to m = \pm m_1$$

Se $\quad a^2 + 2b^2 = c^2 + 2d^2 \ (*) \Longrightarrow$

$$\Rightarrow f\left(f^2(a) + 2f^2(b)\right) = f\left(f^2(c) + 2f^2(d)\right)$$

$a = x+p$
$b = x+q$
$c = x+r$
$d = x+s$

$$\begin{cases} p^2 + 2q^2 = r^2 + 2s^2 \\ p + 2q = r + 2s \end{cases}$$

$p = 0$

$$\begin{cases} 2q^2 = r^2 + 2s^2 \\ 2q = r + 2s \end{cases}$$

$r = 2\alpha$

$q = \alpha + s$
$q^2 = 2\alpha^2 + s^2$
$\alpha^2 + 2\alpha s + s^2 = 2\alpha^2 + s^2$

$(p, q, r, s) = (0, 3, 5, 1)$

$$f^2(x) + 2f^2(x+3) = f^2(x+5) + 2f^2(x+1)$$

$f^2(x) = 4x$

$\sum_{k=0}^{n} k x^k$ $\qquad 1^4 + 2^4 + \dots + m^4$

C1 – 2009 M
(TEPPIC)

$f: \mathbb{R} \to \mathbb{R}$ $\qquad f(x+y) = f(x) + f(y)$ ←

$f(x) = \lambda x \quad \forall x \in \mathbb{Q}$

- f è continua
- f è monotona
- f è limitata (almeno in un intervallo)
- $\exists$ un pallino nel piano in cui non passa il grafico di f.

BST 2012/4

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

$$f(x + f(y + f(z))) = y + f(x+z) \qquad \forall x,y,z \in \mathbb{Q}$$

E: 1° passaggio → mai azzerare le variabili senza f

$x = z = 0$ $\qquad f(f(y + f(0))) = y + f(0)$

$f(f(w)) = w \quad \forall w \in \mathbb{Q}$

f è biunivoca

E: f è iniettiva $f(M) = f(N) \Rightarrow M = N$

f è surgettiva

① $\exists \alpha : f(\alpha) =$ quello che volete voi

② $f(y) = z$

$f(f(x)) = 2f(x)$

$f(z) = 2z$

E : se RHS è simmetrico nelle variabili x e z → LHS è simmetrico.

$$f(x+f(y+f(z))) = y+f(x+z) = f(z+f(y+f(x)))$$

$$x+f(y+f(z)) = z+f(y+f(x)) \quad (*)$$

$x = f(a)$, $z = f(c)$ $\quad y = b$

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

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

$c = 0$ $\quad f(a)+f(b) = f(a+b)+f(0)$

$-f(0) \quad -f(0) \quad -f(0) \quad -f(0)$

$$(f(a)-f(0))+(f(b)-f(0)) = (f(a+b)-f(0))$$

$g(x) = f(x) - f(0)$

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

2° PRA | BMO 2007/2

$\forall x, y \in \mathbb{R}$

$f: \mathbb{R} \to \mathbb{R} \quad f(f(x)+y) = f(f(x)-y) + 4f(x)y$

E.: azzerare f, cioè $f(\Pi)$ porre $\Pi = 0$

oppure $f(\ q_1\ ) = f(\ q_A\ ) + \dots$

$\Rightarrow q_1 = q_A$

~~$f(x)+y = f(x)-y$~~ $\to y = 0$

$y = f(x) \quad f(2f(x)) = 4f(x)^2 + f(0)$

$= [2f(x)]^2 + f(0)$

$\to f(z) = z^2 + f(0) \quad z \in 2\,\mathrm{Im}(f)$

$y = f(x) - m$

$f(2f(x) - m) = f(m) + 4f(x)^2 - 4f(x)\,m$

$m = 2f(z) \quad f(2f(x) - 2f(z)) = 4f(z)^2 + f(0) + 4f(x)^2 - 8f(x)f(z)$

$f(2f(x) - 2f(z)) = [2f(x) - 2f(z)]^2 + f(0)$

$f(\omega) = \omega^2 + f(0) \quad \omega \in 2(\mathrm{Im}\, f_1 - \mathrm{Im}\, f_1)$

$2f(f(x)+y) - 2f(f(x)-y) = 8f(x)y$

- se $\forall x \ f(x) \equiv 0$
- se $\exists x_0 : f(x_0) \neq 0$

$LHS = 2(f(\ ) - f(\ )) = 8f(x_0)y$

$y = \frac{r}{8f(x_0)}$ $\quad f(x) = x^2 + f(0)$

IMO 1999/6 (x case)

— o — o —

TST 2008/6

$f: \mathbb{R}^+ \to \mathbb{R}^+$ $\quad f(x+y) \geq yf(f(x)) + f(x) \to \not\exists f$

$f(x+y) \geq yf(f(x))$

$\frac{f(x+y)}{y} \geq f(f(x))$

$y=1$ $\quad f(x+1) \geq f(f(x))$

$x=1$ $\quad f(y+1) \geq yf(f(1))$

$\lim_{x \to +\infty} f(x) = +\infty$

se sapessi che $f(f(x_0)) \geq n$

$f(x_0+y) \geq yn$

$f(y) \geq ny - nx_0 > (n-1)y \quad \forall y > nx_0$

$f(x+y)$

$x+y = f(z)$

$x=1$

$y = f(z)-1$

$f(f(z)) \geq (f(z)-1) f(f(1))$

$\to \lim_{x \to +\infty} f(f(x)) = +\infty$

$$f(x+y) \geq y f(f(x))$$

$x + y = f(x)$

$\begin{cases} x = z \\ y = f(z) - z \end{cases}$

per ogni z abbastanza grandi $(z > 2^{x_0})$

$f(f(z)) \geq (f(z) - z) f(f(z))$

$1 \geq f(z) - z$

$f(z) \leq z + 1$

$f(z) > nz$ ↯

IMO 2013/5 $f: \mathbb{Q}_{>0} \to \mathbb{R}$

i) $f(x)f(y) \geq f(xy) \quad \forall x, y \in \mathbb{Q}_{>0}$

ii) $f(x+y) \geq f(x)+f(y) \quad \forall x, y \in \mathbb{Q}_{>0}$

iii) $\exists\, a \in \mathbb{Q}_{>1} : f(a)=a$

$\Longrightarrow f(x)=x \quad \forall x \in \mathbb{Q}_{>0}$

$f(x+y+z) \geq f(x)+f(y+z) \geq f(x)+f(y)+f(z)$

① $f(nx) \geq n f(x) \quad \forall x \in \mathbb{Q}_{>0} \quad \forall n \in \mathbb{N}$

$f(x)f(y)f(z) \geq f(x)f(yz) \geq f(xyz)$

② $(f(x))^n \geq f(x^n) \quad \forall x \in \mathbb{Q}_{>0} \quad \forall n \in \mathbb{N}$

③ $x=a \quad y=1 \qquad f(a)f(y) \geq f(ay) \qquad f(1) \geq 1$

$f(n) \geq n \quad \forall n \in \mathbb{N}$

④ $x=\frac{p}{q} \quad y=q$

$f\left(\frac{p}{q}\right) \geq \frac{f(p)}{f(q)} > 0 \quad \forall \frac{p}{q}$

⑤ $\to f(x) > 0 \quad \forall x \in \mathbb{Q}_{>0}$

$f(x+y) \geq f(x)+f(y) > f(x)$

⑥ $\to f$ è crescente

↓

⑥ $a^n \geq f(a^n)$

$b_n = \lfloor e^n \rfloor$

$b_n \le f(b_n) = f(\lfloor e^n \rfloor)$

$\le f(e^n) \le e^n < b_n + 1$

$b_n \le f(b_n) < b_n + 1$

(7) Se esistesse un c : $f(c) \ge c+1$

$f(c+1) \ge f(c) + f(1) \ge c+2$

$f(y) \ge y+1 \quad \forall y \ge c$

per un qualche b_n : $b_n \ge c$

$\rightarrow f(b_n) \ge b_n + 1$ ↯

$\rightarrow f(n) < n+1$

(8) Suppongo che $f(c) \ge c + \frac{1}{m}$ con $c \in \mathbb{N}$, $m \in \mathbb{N}$

(1) $f(nx) \ge n f(x)$

$n = m, x = c \quad f(mc) \ge m f(c)$

$\ge mc + m \cdot \frac{1}{m}$

$= mc + 1$

$\rightarrow f(n) = n \quad \forall n \in \mathbb{N}$

$f\left(\frac{p}{q}\right) f(q) \geq f(p) \qquad p, q \in \mathbb{N}$

$f\left(\frac{p}{q}\right) \geq \frac{p}{q} \qquad (*)$

① $f(nx) \geq n f(x)$

$n = q, \; x = \frac{p}{q} \qquad f(p) \geq q f\left(\frac{p}{q}\right)$

$f\left(\frac{p}{q}\right) \leq \frac{p}{q} \; (*)$

TST USA SL 2004 $f: \mathbb{R}_{\geq 1} \to \mathbb{R}_{\geq 1}$

i) $f(x) \leq 2(x+1)$

ii) $xf(x+1) = f(x)^2 - 1$

(1) $f(x) = \sqrt{xf(x+1)+1}$

$\leq \sqrt{x \cdot 2 \cdot (x+2)+1}$

$= \sqrt{2x^2+2x+1}$

$< \sqrt{2}(x+1)$

(2) $f(x)^2 = xf(x+1)+1$

$< x\sqrt{2}(x+2)+1$

$< \sqrt{2}(x+1)^2$

$f(x) < 2^{\frac{1}{2}}(x+1)$

(3) $\to f(x) \leq 2^{\frac{1}{2^k}}(x+1) \quad \forall k \in \mathbb{N}$

$\nexists x \in \mathbb{R}_{\geq 1} : f(x) > x+1$

$2^{\frac{1}{2^k}}(x_0+1) \geq f(x_0) = x_0 + 1 + \varepsilon$

$\to f(x) \leq x+1 \quad \forall x \in \mathbb{R}_{\geq 1}$

$f(x) \geq 1 \quad \forall x \in \mathbb{R}_{\geq 1}$

(4) $f(x)^2 = xf(x+1)+1 \geq x+1$

$\to f(x) \geq \sqrt{x+1} > \sqrt{x}$

⑤ $f(x)^2 = xf(x+1)+1 \geq x\sqrt{x+1}+1$

$> x\sqrt{x}$

$f(x) \geq x^{3/5}$

$f(x) \geq x^{1-\frac{1}{2^k}}$

$\rightarrow \nexists x : f(x) < x$ ( )

$\rightarrow f(x) \geq x$

⑦ $f(x)^2 = xf(x+1)+1 \geq x(x+1)+1$

$= x^2+x+1$

$= (x+\frac{1}{2})^2 + \frac{3}{5}$

$> (x+\frac{1}{2})^2$

$\rightarrow f(x) > x+\frac{1}{2}$

⑧ $f(x)^2 = xf(x+1)+1 > x(x+\frac{3}{2})+1$

$= (x+\frac{3}{5})^2 + \text{scarto}$

$> (x+\frac{3}{5})^2$

$\rightarrow f(x) > x+\frac{3}{5}$

$f(x) \geq x+1-\frac{1}{2^k}$

$\rightarrow \nexists x : f(x) < x+1$

$\rightarrow f(x) \geq x+1 \quad \forall x \geq 1$

— o — o —

3° ORA

TST VIETNAM 2003

Siz A l'insieme delle $f: \mathbb{R}^+ \to \mathbb{R}^+$ t.c.

$$f(3x) \geq f(f(2x)) + x \quad \forall x \in \mathbb{R}^+$$

Trovare max α : $\forall f \in A \quad f(x) \geq \alpha x$

$f(x) = cx$

$3cx \geq 2c^2 x + x$

$3c \geq 2c^2 + 1$

$\to \frac{1}{2} \leq c \leq 1 \qquad \alpha \leq \frac{1}{2}$

$f(x) \geq a_n x$

$f(3x) \geq 2a_n^2 x + x = \frac{2a_n^2+1}{3} \cdot 3x$

$a_{n+1} = \frac{2a_n^2+1}{3}$

TST 2006/3 $f: \mathbb{Z} \to \mathbb{Z}$

$$f(m-n+f(n)) = f(m)+f(n) \quad \forall m,n \in \mathbb{Z}$$

E: se $a, b \in \mathrm{Im}(f)$
avrete m_0 e n_0 : $f(m_0)=a$, $f(n_0)=b$

$$f(\quad) = a+b$$

$\to a+b \in \mathrm{Im}(f)$

- $0 \in \mathrm{Im}(f) \to |\mathrm{Im}(f)| = 1$
- $a \neq 0 \in \mathrm{Im}(f) \quad na \in \mathrm{Im}(f) \to |\mathrm{Im}(f)| = \infty$

$m=n$ $\quad f(f(n)) = 2f(n) \quad \forall n \in \mathbb{Z}$

$f(n) = 2n \quad \forall n \in \mathrm{Im}(f)$

$$f(m-n+f(n)) = f(n-m+f(m))$$

Se f è inietiva $\quad m-n+f(n) = n-m+f(m)$

$$f(n)-2n = f(m)-2m$$

Se {espressione x} = {espressione in y}
$\to$ {espressione x} $= k$

$$f(n) = 2n+k$$

f non è iniettiva $\Longleftrightarrow \exists\, a<b : f(a)=f(b)$

$n=a \quad f(m-a+f(a)) = f(m)+f(a)$

$n=b \quad f(m-b+f(b)) = f(m)+f(b)$

$$f(m-a+f(a)) = f(m-b+f(b))$$

$m = k+a-f(a)$

$$f(k) = f(k+a-f(a)-b+f(b))$$

$$f(k) = f(k+(a-b))$$

$\rightarrow f$ è periodica

$\rightarrow |\mathrm{Im}(f)| = 1$

$\rightarrow f(n)=0 \quad \forall n \in \mathbb{N}$

IMO SL A2 2005 $f:\mathbb{R}^+ \to \mathbb{R}^+$

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

① $f(x)=c \to c^2 = 2c \to c=2$

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

$\frac{f(x)f(y)}{2}$

Supponiamo f iniettiva

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

$x=1 \quad 1+yf(1) = y+f(y)$

$f(y) = cy+1$ NO

$x = x+yf(x) \to yf(x) = 0$ no

$y = x+yf(x) \to y_f = \frac{x}{1-f(x)}$

Se $f(x) < 1 \rightsquigarrow y_f > 0$

$\to f(x)f(y) = 2f(\quad)$

$f(x) = 2$

$\to f(x) \geq 1 \quad \forall x > 0$

Se $f(x)f(y) = 2f(\quad) \geq 2f(x)$

$f(y) \geq 2$

Claim: $f(x) \geq 2$

$$\frac{f(x)}{2}\frac{f(y)}{2} = 2f\left(\frac{\quad}{2}\right)$$

$a, b \in \mathrm{Im}(f) \to \frac{ab}{2}$

$$\left(\frac{f(x)}{2}\right)\left(\frac{f(y)}{2}\right) = \frac{f(\quad)}{2}$$

$$g(x)g(y) = g(\quad)$$

se $a, b \in \mathrm{Im}(g) \to ab \in \mathrm{Im}(g)$

$\to a^k \in \mathrm{Im}(g)$

$g(x) \geq \frac{1}{2}$ Supponiamo che esiste α: $g(\alpha) < 1$

$\beta < 1$ e $\beta \in \mathrm{Im}(g)$

$\to \beta^k \in \mathrm{Im}(g)$

ma $\beta^k \geq \frac{1}{2}$ $\forall k$ ↯

$\to g(x) \geq 1 \to f(x) \geq 2$

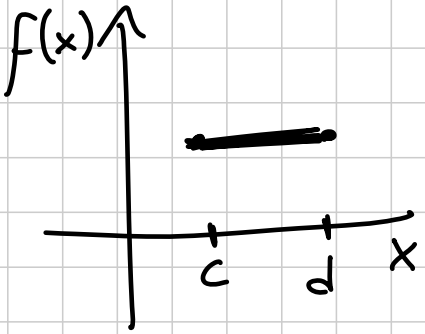
$2f(x) \leq f(x)f(y) = 2f(x+y)$

$\to f$ è monotona

$\exists\ c, d$: $f(c) = f(d)$ e $c < d$

$x = c$

$f(c)f(y) = 2f(c + yf(c))$



Se $c + yf(c) \le d$

$f(c)f(y) = 2f(\quad)$

$0 < y \le \frac{d-c}{f(c)}$

Se $f(\alpha) = 2$

$x = y = \alpha$

$4 = 2f(\alpha + \alpha) \to f(3\alpha) = 2$

$f(3^k\alpha) = 2$

$x \in (0, \alpha) : f(x) = 2$

$\to x \in (0, 3^k\alpha) : f(x) = 2$ □

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

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

MEMO 2012/1 $f:\mathbb{R}^+\to\mathbb{R}^+$

$$f(x+f(y))=yf(xy+1)$$

$$xf(x+f(y))=yf(y+f(x)) \quad \xleftarrow{\text{SIM}} \quad (\text{NO})$$

$x=\frac{1}{y}$ (NO)

$x+f(y)=xy+1$ (FORSE)

$x=\frac{f(y)-1}{y-1}$ $(y\neq 1)$

$y=1$

$\frac{f(y)-1}{y-1}\leq 0$ $\rightleftarrows$ $y>1 \to f(y)\leq 1$, $y<1 \to f(y)\geq 1$

E: se avete $f(\text{Mostro})=f(x)$

$xy+1=x \to y=\frac{x-1}{x}=1-\frac{1}{x}$ $(x>1)$

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

$f(x+f(1-\frac{1}{x}))=(1-\frac{1}{x})f(x)$ no

$xy+1=y \longrightarrow x=1-\frac{1}{y}$ $(y>1)$

$f(1-\frac{1}{y}+f(y))=yf(y)$

Se $\exists\, y_0 : f(y_0) > \frac{1}{y_0}$

$f(y_0) - \frac{1}{y_0} + 1 > 1 \rightarrow f(\quad) \leq 1$

$1 = y_0 \cdot \frac{1}{y_0} < y_0 f(y_0) \leq 1$ ↯

Se $\nexists\, y_0 : f(y_0) < \frac{1}{y_0}$ ↯

$\rightarrow f(y) = \frac{1}{y} \quad \forall y > 1$

$f(x + f(y)) = \frac{y}{xy+1} \qquad \forall x, y \in \mathbb{R}^+$

se $y > 1$

$f(x + \frac{1}{y}) = \frac{y}{xy+1} \qquad \forall x \in \mathbb{R}^+ \quad \forall y > 1$

$\frac{1}{y} = a \quad (\text{con } a < 1)$

$f(x+a) = \frac{\frac{1}{a}}{\frac{x}{a}+1} = \frac{1}{x+a}$

Claim : $f(z) = \frac{1}{z}$

$x + a = z \quad \text{con} \quad z < 1$

$x = z - a$

$\rightarrow f(x) = \frac{1}{x} \qquad \forall x \in \mathbb{R}^+$

ARGENTINA TST 2010/3

$f : \mathbb{R} \rightarrow \mathbb{R} \qquad f(x + xy + f(y)) = \left(f(x) + \frac{1}{2}\right)\left(f(y) + \frac{1}{2}\right)$

IMO SL 2002 A1

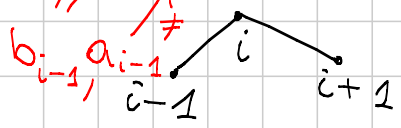
FINE

Combinatoria 1 MEDIUM

Titolo nota 04/09/2014

RUSS '07/5 100 è pari – agono regolare

in ogni vertice ho 2 # a_i, b_i $a_i \neq b_i$



Esiste un modo di scegliere $c_i \in \{a_i, b_i\}$ per ogni vertice in modo che vertici adiacenti abbiano $c_i \neq$.

gli zeri

COMBINATORIAL NULLSTELLENSATZ

campo $\mathbb{R}, \mathbb{Q}, \mathbb{Z}/p\mathbb{Z}$

Fatto "ovvio". $p \in F[x]$ $\deg p = n$

$A \subseteq F$ $|A| \geq n+1$ $\exists a \in A$ $p(a) \neq 0$.

CN $p \in F[x_1 \dots x_n]$ $x_1^{t_1} \dots x_n^{t_n}$ che compare con coeff. $\neq 0$ ed è di grado max in p.

$A_1, \dots, A_n \subseteq F$ $|A_1| \geq t_1 + 1$ $\dots$ $|A_n| \geq t_n + 1$, allora

$\exists\, a\ (a_1, \dots, a_n) \in A_1 \times \dots \times A_n$

tc $p(a_1 \dots a_n) \neq 0$.

Sol di RUS '07. $p \in \mathbb{R}[x_1, \dots, x_{100}]$

$A_i = \{a_i, b_i\} \mid i = 1, \dots, 100$

$$p(x_1, \dots, x_n) = \prod_{cyc} (x_{i+1} - x_i) = (x_2 - x_1) \cdots (x_n - x_{n-1})(x_1 - x_n)$$

$c_1 \dots c_n \in A_1 \times \dots \times A_n$

$p(c_1, \dots, c_n) = 0 \iff \exists\ i, i+1$ (c_{n+1} inteso come c_1) $\mid\ c_i = c_{i+1}$

ie coeff. di $x_1 \cdots x_n = 2$.

$\rightarrow$ per ie CN $\exists\ \underline{c}\ p(\underline{c}) \neq 0$.

Dimostrazione del CN.

Per induzione su $\deg p$.

Se $\deg p = 1$ è chiaro.

wlog $c_1 x_1 + r(x_2, \dots, x_n)$ [...]

$x_1^{t_1} \cdots x_n^{t_n}$ mon. di $\deg = \deg p$.

wlog $t_1 \geq 1$.

$A_1, \dots, A_n$. Sia $a \in A_1$.

Divido p per $x_1 - a_1$.

$$p(\underline{x}) = (x_1 - a_1)\, q(\underline{x}) + r(\underline{x})$$

$\deg_{x_1} r = 0$ $\qquad r(x_2, x_3, \dots, x_n)$

Supp per ass. $\forall (a_1, \dots a_n) =: \underline{a} \in A_1 \times \dots \times A_n$ $p(\underline{a}) = 0$.

Su $\{a_1\} \times A_2 \times \dots \times A_n$ r fa 0.

$\rightarrow$ ma allora $r = 0$ su $A_1 \times \dots \times A_n$

→ q si annulla su $A_1 \setminus \{a_1\} \times A_2 \dots \times A_n$

t_1 t_2+1 t_n+1

che coeff. ha $x_1^{t_1-1} \dots x_n^{t_n}$ in q?
Sicuramente $\neq 0$! $\in \deg q = \deg p - 1$

Contraddice hp induttiva !

[Cauchy - Davenport] □

$A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ (non vuoti)
considero
$A+B = \{a+b \mid a \in A, b \in B\} \subseteq \mathbb{Z}/p\mathbb{Z}$
$|A+B| \geq \min(p, |A|+|B|-1)$.

dim.

Se $|A|+|B| \geq p+1$; voglio dim che $A+B = \mathbb{Z}/p\mathbb{Z}$.

Prendo $x \in \mathbb{Z}/p\mathbb{Z}$. $x-B = \{x-b \mid b \in B\}$ ha $|B|$ elementi.
Ma allora (pigeonhole) interseca A. $a \in A \cap x-B$ allora $a = x-b$ per qualche $b \in B \to x = a+b$.
($a \in A$, $b \in B$)

Manca :
→ $|A|+|B| \leq p$. $|A+B| \leq |A|+|B|-2$

$\in \mathbb{Z}/p\mathbb{Z}[x,y]$ $C \supseteq A+B$ $|C| = |A|+|B|-2$

$$p = \prod_{c_i \in C} (x+y-c_i)$$

$\deg p = |A| + |B| - 2$

monomio $x^{|A|-1} y^{|B|-1}$ in p ha coeff. $\binom{|A|+|B|-2}{|A|-1}$

ma questo $(|A| + |B| - 2)!$
e $|A| + |B| - 2 \leq p - 1$
$\rightarrow$ non è 0.

Ma allora $\exists a \in A,\ b \in B \mid p(a,b) \neq 0$
MA È ASSURDO!

IMO '07. 6 $\{0, 1, \dots, n\}^3$

Quanti piani sono necessari per coprire tutti i pti TRANNE $(0,0,0)$ (e $(0,0,0)$ DEVE rimanere scoperto.

Posso farlo con $3n$. $x = 1, \dots, n$
$y = 1, \dots, n$
$z = 1, \dots, n$

AIM: non si fa con meno di $3n$.

p pol. in $\mathbb{R}[x,y,z]$. Suppongo bastino meno di $3n$ piani.

$$q(x,y,z) = \prod_{i=1}^{\#\text{piani}} (a_i x + b_i y + c_i z + d_i)$$

si deve annullare su $= \{0, \dots, n\}^3 \setminus (0,0,0)$

$$r(x,y,z) = \prod_{i=1}^{n} (x-i)(y-i)(z-i)$$

r si annulla su $\in$
MA non su $(0,0,0)$

$$p(x,y,z) = q(x,y,z) - \frac{q(0,0,0)}{r(0,0,0)} r(x,y,z)$$

$\deg p = 3n \quad (\deg q < 3n)$

$x^n y^n z^n$ COMPARE (con coeff $-\frac{q(0,0,0)}{r(0,0,0)}$)

→ CONTRADDICE CN.

[Chevalley – Warning] Sistema

$$\begin{cases} p_1(x_1 \dots x_n) = 0 \\ \dots \\ p_k(x_1 \dots x_n) = 0 \end{cases}$$

di k polinomi in $\mathbb{Z}/p\mathbb{Z}[x_1 \dots x_n]$ tc. $\sum_{i=1}^{k} \deg p_i < n$

Se c'è una soluzione, allora ce n'è un'altra.

[+FORTE: il #soluzioni è $\equiv 0 (p)$]

dim. $(c_1, \dots, c_n)$ è sol.; supponiamo (per ass.) sia unica.

$$\prod_{j=1}^{k} \left(1 - p_j(x_1, \dots, x_n)^{p-1}\right) = q(x_1 \dots x_n)$$

$\to$ si annulla sse $(x_1, \dots, x_n) \neq (c_1, \dots, c_n)$

$$\to \deg q = \sum_{j=1}^{k} (p-1) \deg p_j < (p-1)n.$$

$$r(x_1 \dots x_n) = \prod_{i=1}^{n} \prod_{j \neq c_i} (x_i - j)$$

$\to$ si annulla sse $(x_1 \dots x_n) \neq (c_1 \dots c_n)$

$\to \deg r = n(p-1)$
($x_1^{p-1} \dots x_n^{p-1}$ ha c. 1)

Ora prendo $p(x_1 \dots x_n) = q(x_1 \dots x_n) - \dfrac{q(c_1 \dots c_n)\, r(x_1 \dots x_n)}{r(c_1 \dots c_n)}$

$\to$ p si annulla su $(\mathbb{Z}/p\mathbb{Z})^n$
ha deg $(p-1)n$ e termine $x_1^{p-1} \dots x_n^{p-1}$

$\to$ CONTRADDICE CN!

[EGZ] Ho $2n-1$ interi; posso sempre sceglierne n t.c. n divida la loro somma.

LEMMA 1. Se so EGZ(a) e EGZ(b) allora so EGZ(ab).

$2ab-1$ interi; posso prenderne a | la Σ è div. per a

li chiamo $x_1 \dots x_a$

li tolgo; rimangono $2ab-a-1$

$a(2b-1)-1$

ripeto! ne tolgo a

li chiamo $x_{a+1} \dots x_{2a}$

...

quante volte posso ripetere?

Posso farlo $2b-1$ volte.

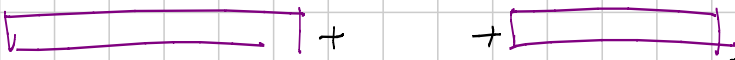
Ho $\frac{1}{a}(x_1 + \dots + x_a)$

$\frac{1}{a}(x_{a+1} + \dots + x_{2a})$

...

$\frac{1}{a}(x_{a(2b-2)+1} + \dots + x_{a(2b-1)})$

Sono $2b-1$ interi;
ne scelgo b la cui somma sia multipla di b.

$\frac{1}{a}$() $= kb$

b blocchi

$\rightarrow ab$ el. sommano a

un multiplo di ab

→ EGZ (ab)

→ wlog n è un primo!

$$p(x_1 \dots x_p) = 1 - (x_1 + \dots + x_p)^{p-1}$$

→ si annulla se $x_1 + \dots + x_p \not\equiv 0 \ (p)$

→ ha deg $p-1$.

$x_1 \dots x_{p-1}$ c'è $((p-1)! \neq 0)$

$A_1 \times \dots \times A_{p-1} \times A_p$

2 2 1

i miei $2p-1$ el. erano $a_1 a_2 a_3 a_4 \dots a_{2p-1}$

ATTENZIONE! Detto così non è chiaro che $|A_i| = 2$ per $i < p$.

MA se ho p el. della stessa classe mod p li prendo e ho finito; altrimenti ordino gli el. secondo la loro classe:

$a_1 \dots a_k \dots a_{2p-1}$

0 0 0 0 1 1 ... p-1 ...

e raggruppo in A_i a_i, a_{i+p}

$A_p = \{a_p\}$

Dim con CAUCHY-DAVENPORT

supp wlog che non ci siano p interi $\equiv$ fra loro mod p (altrimenti finito)

$A_1 \quad \dots \quad A_p \subseteq \mathbb{Z}/p\mathbb{Z}$

$A_1 = \{a_1, a_1+a\}$ diversi mod p ; $A_p = \{a_p, a_p+a, \dots, a_p+(p-1)a\}$; $\{a_p\}$

$$|A_p + A_{p-1}| \geq |A_p| + |A_{p-1}| - 1$$
$$\geq 2$$

$$|(A_p + A_{p-1}) + A_{p-2}| \geq 2 + |A_{p-2}| - 1$$
$$= 3$$

$\dots$

$$|A_1 + \dots + A_p| \geq p$$

ho vinto!

Dim. con Chev. War.

pol. in $\mathbb{Z}/p\mathbb{Z}$

$$\begin{cases} x_1^{p-1} + \dots + x_{2p-1}^{p-1} = 0 \\ \sum a_i x_i^{p-1} = 0 \end{cases}$$

a_i i miei interi mod p

$a_1 \dots a_{2p-1}$ sono gli interi dell'insieme

$c_1 \dots c_{2p-1}$ è sol $\iff$ ci sono es. p $c_i \neq 0$ e $\sum a_i \equiv 0$

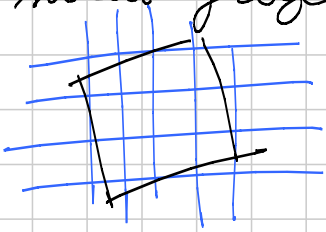
$c_1 \dots c_n = 0 \dots 0$

$i \mid c_i \neq 0$

$\sum \deg = p-1+p-1 = 2p-2 < 2p-1$

→ Per CW siccome ho $0, \dots, 0$ ho anche una sol "non banale" che mi dice quali a_i prendere.

RUS '13? Ho un tovagliolo 100×100, e la griglia intera infinita. Trovare il min n t.c. COMUNQUE SIA APPOGGIATO il tov. sulla griglia si possano coprire tutti i punti della griglia sul tovagliolo (anche sul bordo) con n rette.



$\sum$ coeff. di un pol. $p = p(1)$

$\sum$ coeff. dei termini di deg pari $= \dfrac{p(1)+p(-1)}{2}$

$\sum$ coeff dei termini multipli di n in $p =$

$$\frac{1}{n}\sum_{i=0}^{n-1} p(\zeta^i)$$

ζ radice n-esima primitiva

$d \mid n \mid k$ $\quad \frac{c_k}{n} \sum_{i=0}^{n-1} (\zeta^i)^k = c_k$

$d \quad n \nmid k$ $\quad \frac{c_k}{n} \sum_{i=0}^{n-1} (\zeta^i)^k \to 1$

$= \frac{c_k}{n} \frac{(\zeta^k)^n - 1}{\zeta^k - 1}$

ROOT OF UNITY FILTER

Quanti sono i # di 4 cifre che contengano solo cifre 3, 7, 8, 9 e siano multipli di 3?

IDEA! $p(x) = (x^3 + x^7 + x^8 + x^9)^4$

$p(1) = 4^4$ = # di naturali di 4 cifre con cifre 3, 7, 8, 9

La risposta è la $\sum$ dei coeff. dei termini di deg mult. di 3.

sia ζ a rad. 3 dell'unità

$\frac{1}{3}(p(1) + p(\zeta) + p(\zeta^2))$

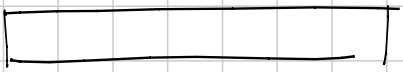
4^4 $\quad (1+\zeta+\zeta^2+1)^4$ $\quad \to 1$

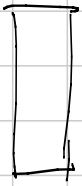
ζ^n

1

Abbiamo un rettangolo che sappiamo tassellare con rettangolini

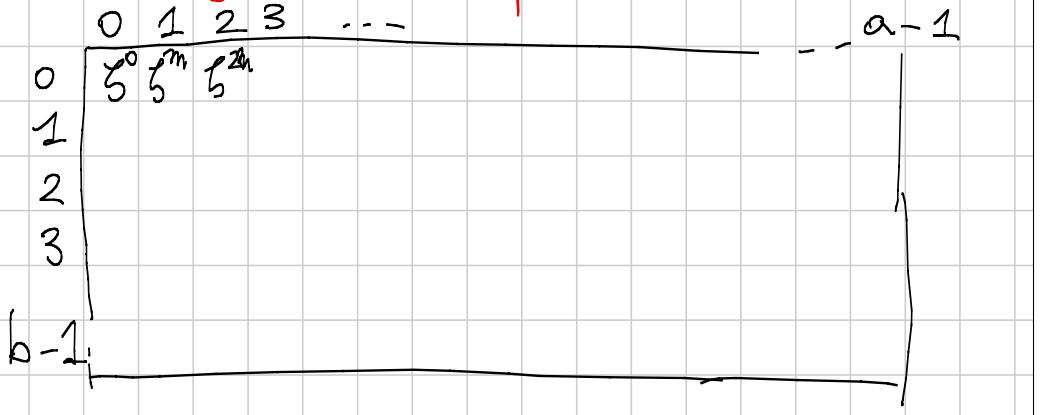
$1 \times n$ $\qquad$ $m \times 1$





Allora sappiamo tassellarla anche con rettangoli di un solo tipo!

Sia ζ una rad. prim. nm-esima



nel quadrato (i,j) $\quad \zeta^{mi+nj}$

$1 \times n$ i rett. hanno somma 0.

$$\zeta^{nj} \sum_{i=0}^{n-1} \zeta^{mi} = \frac{\zeta^{nj}(\zeta^{mn}-1)}{\zeta^m - 1}$$

($\zeta^{mn} = 1$)

$m \times 1$ è uguale!

$\sum$ tutti i quadretti è 0

ma quanto vale?

0

$$\sum_{\substack{0 \le i \le a-1 \\ 0 \le j \le b-1}} \zeta^{mi+nj} =$$

$$= \left(1 + \zeta^{m} + \zeta^{2m} + \dots + \zeta^{(a-1)m}\right)$$
$$\left(1 + \zeta^{n} + \dots + \zeta^{(b-1)n}\right) =$$
$$= \frac{\zeta^{am} - 1}{\zeta^{m} - 1} \cdot \frac{\zeta^{bn} - 1}{\zeta^{n} - 1}$$

MA uno dei due fattori deve annullarsi.

wlog am mult. di nm
$\rightarrow$ a è mult. n
$\rightarrow$ si tassella con gli $1 \times n$!

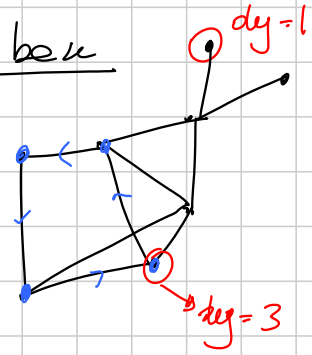
□

C2 – GRAFI

ma_go

Titolo nota 05/09/2014

Definizioni di base

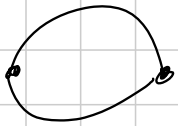


Un grafo è (V, E) dove $E \subseteq \{\{v, w\} : v \neq w, v, w \in V\}$

V: insieme di vertici; E: archi

Il grado di un vertice è il numero di archi incidenti (il numero di archi che escono da lui)

Un ciclo è una successione di vertici $v_1, \dots, v_\ell \equiv v_1$ t.c. v_i collegato a v_{i+1} $\forall i$. La lunghezza del ciclo

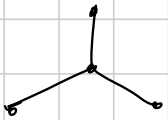


← non è un grafo!

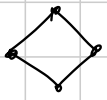
$v, w \Rightarrow \{v, w\} \in E$ → si può stare o non stare un arco è i suoi estremi

← non è un grafo.

es • Alberi; • un grafo senza cicli connesso.
• connesso minimale (= tolgo un arco e si disconnette)
• aciclico massimale (= aggiungo un arco e ci sono cicli)

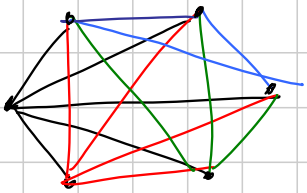


✓



✗

- Completo (K_n)



Lemma $\deg(v)$ ← grado di v

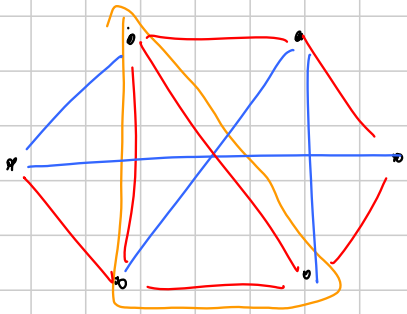
$$\sum_{v \in V} \deg(v) = 2|E|. \qquad \square$$

es IMO 64/4 | 17 scienziati che collaborano su 3 argomenti. Dimostrare che ce ne sono 3 che collaborano su uno stesso argomento

Proviamo a fare qualcosa se ci sono 2 argomenti: cosa?

Idea 1 Associamo a questa cosa un grafo!

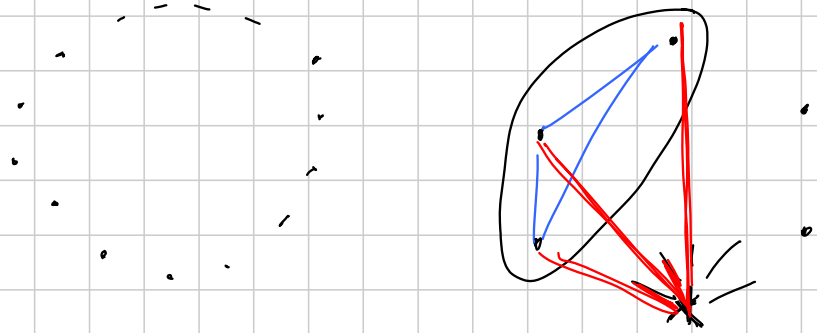
Idea 2 Le persone sono 6 persone e 2 argomenti, siamo contenti.



TDN

ALG

Colorazioni (di archi) Dato un certo grafo Γ, colorato con k colori, $\exists$ un triangolo monocromatico in Γ?



idea: $n=6$, $k=2$; consetti sui lati uscenti V_0:
$\rightsquigarrow$ c'è un colore (rosso) con almeno 3 archi $\rightsquigarrow V_1, V_2, V_3$

- o $V_1 V_2 V_3$ è tutto blu ✓
- o $V_1 V_2$ è rosso ✓ $V_0 V_1 V_2$ è rosso.

Ricado l'idea: $V_0 \rightsquigarrow$ 16 archi $16 = 3 \cdot 5 + 1 \Rightarrow$ consetti
($3 = k$, $5 = (6-1)$)

$\exists$ 

← 6 elem. Win.

$6 = R(3,3) \rightsquigarrow$ numero di Ramsey.

$$R(m,n) = \min\{N \mid \text{ogni colore } K_N \text{ con 2 colori (blu, rosso) o esiste un sottografo } K_m \text{ tutto blu o un } K_n \text{ tutto rosso}\}$$

$17 \geq R(3,3,3)$

Abbiamo colorato archi: in realtà nessuno ci vieta di colorare i vertici.

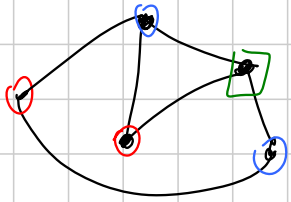
Una colorazione di un grafo Γ con k colori è

una funzione $f: V \longrightarrow \{1, \dots, k\}$ t.c.

se $V \leftrightsquigarrow W$ allora $f(V) \neq f(W)$.

Dato un certo grafo Γ, ci serve un min. k t.c. esiste una k-colorazione. $k = \chi(\Gamma)$ → numero cromatico

es



⇒ non ho 1-col.
non ho 2-col.
con 3 colori sì

oss Se Γ ha n vertici: $\chi(\Gamma) \leq n$.

Se Γ è un albero? $\chi(\Gamma) = 2$ a meno che Γ non sia un punto.

$\chi(K_n) = n$. (ho bisogno di tutti i colori possibili)

$\chi(\Gamma) = 1$? Quando è totalmente disconnesso ($E = \emptyset$).

$\Gamma' \subset \Gamma \Rightarrow \chi(\Gamma') \leq \chi(\Gamma)$

$V' \subset V$
$E' \subset E$

problema $\chi(\mathbb{R}^2)$?

$\mathbb{R}^2$ lo vedo come grafo, dove collego P, Q se $\overline{PQ} = 1$.

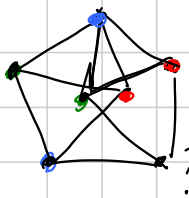
mi servono almeno 3 colori.

è un sottografo di $\mathbb{R}^2$.

è un problema aperto!

Si vede abbastanza facilmente che $\chi(\mathbb{R}^2) \leq 7$ (?)

$$\chi(\mathbb{R}^2) \geq 4$$



$\subset \mathbb{R}^2$ (sottografo)

def Un grafo Γ si dice **bipartito** se $\chi(\Gamma) \leq 2$.

(ovvero se ammette una 2-colorazione).

teo (Teorema di Turán)

Se Γ è un grafo senza triangoli, allora

$$|E| \leq \left\lfloor \frac{n^2}{4} \right\rfloor.$$ parte intera.

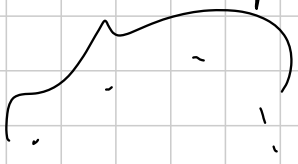
[**oss** Γ ha n vertici $\Rightarrow$ $0 \leq |E| \leq \binom{n}{2}$.]

dim Prendiamo $u, v, t \in V$; se ~~tra~~ in Γ non ci sono triangoli, allora ci sono al più 2 archi tra questi 3 vertici.

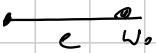
Prendiamo tutte le possibili terne e sommiamo:

$\binom{n}{3} \cdot 2$ $\quad$ $n-2$ volte per ogni.

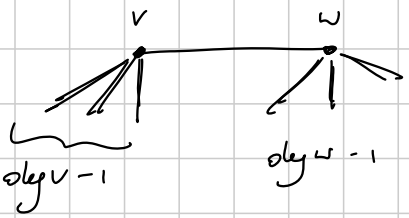
$(n-2)\cdot|E| \to$ perdo!



$(n-2)\cdot E \le \frac{n(n-1)(n-2)}{3} = \frac{n(n-1)}{3}$.



non è abbastanza.



$\deg(v)' + \deg(w)' \le n-2$

$\deg v + \deg w \le n$.

$$\sum_{\{v,w\}\in E}{}' \deg v + \deg w \le n\cdot|E|.$$

$$\frac{1}{2}\left(\sum_{\{v,w\}\in E}{}' \deg v + \sum_{\{v,w\}\in E}{}' \deg w\right) = \sum_{v\in V}{}' \deg^2(v)$$

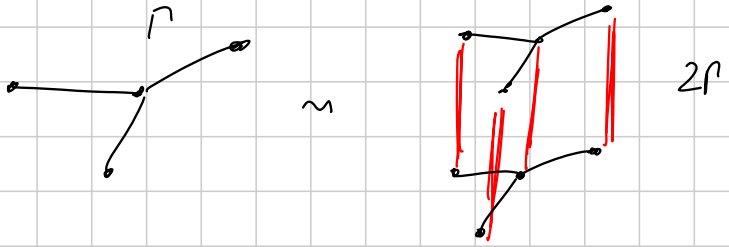
$$\sum_{v}{}' \deg^2 v \le n\cdot|E|.$$

v AM-QM

$$\frac{\left(\sum' \deg v\right)^2}{n} = \frac{(2|E|)^2}{n} \Rightarrow 4|E| \le n^2 \Rightarrow |E| \le \left\lfloor \frac{n^2}{4} \right\rfloor$$

IMO SL 2013/C3 $\quad$ Γ grafo: posso fare le seguenti op.:

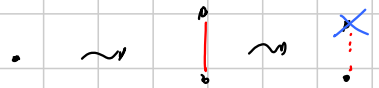
- tolgo un vertice di grado dispari
- "raddoppio" il grafo. $\Gamma \to 2\Gamma$



Partendo da Γ qualunque, posso ottenere a Γ compl. disc.

oss 1 La seconda mossa cambia la parità di tutti i vertici

oss 2 Se ho già isolato un vertice, raddoppiarlo non mi crea problemi:



oss 2' Posso considerare Γ connesso.

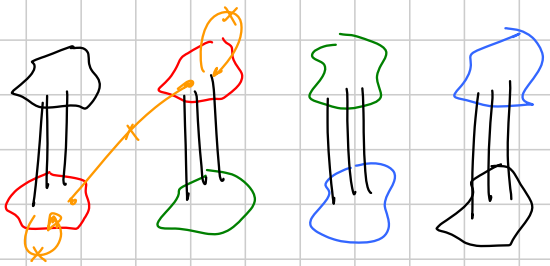
oss 3 Γ è compl. disc. $\Rightarrow \chi(\Gamma) = 1$.

oss 3 accende una speranza: $\Gamma \rightsquigarrow \Gamma'$ con $\chi(\Gamma') < \chi(\Gamma)$!

$\chi = \chi(\Gamma) =$ min di colori per colorare Γ

Supp. che Γ sia χ-colorato.

oss 4 $\chi(2\Gamma) \leq \chi$.



vorremmo tanto eliminare un colore.
Lo possiamo fare se tutti i nodi hanno grado dispari.

oss 5 Usando solo le prime mosse, possiamo ottenere Γ_{pari} t.c. tutti i vertici hanno valenza pari!

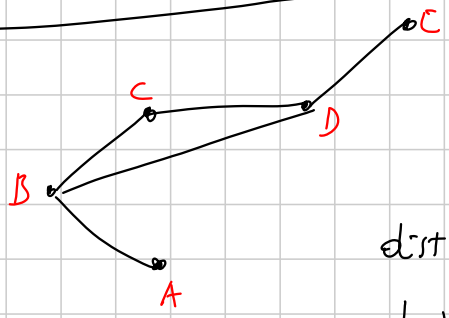
idea: $\Gamma \rightsquigarrow \Gamma_{pari} \rightsquigarrow 2\Gamma_{pari} \rightsquigarrow$ elimino un colore Γ'

tc. $\chi(\Gamma') < \chi(\Gamma)$. $\Longrightarrow$ ripetendo, Win!

IMOSL 2013/C6 Provare che un certo numero di città, per ognuna delle quali il numero di città a dist. = 3 da essa è al più 100.

Dim. che il num. di città a dist. 4 da una città qualunque è ≤ 2550.

es/dist

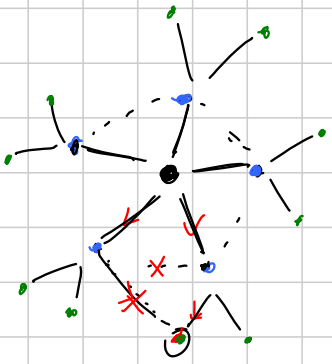


$dist(A,E) = 3$

$dist(A,D) = 2$

oss -1 è un problema di grafi.

Provare e contare il # di città a dist 4 da V_0.



- $S_1(v) = \{$dist = 1 da $v\}$
- $S_2(v)$
  $S_k(v) = \{$dist k da $v\}$

$|S_1(v)| = \deg v$.

$S_1(v) \cap S_2(v) = \phi$

$$|S_2(v)| \leq \sum_{w \in S_1(v)} \deg(w) - 1$$

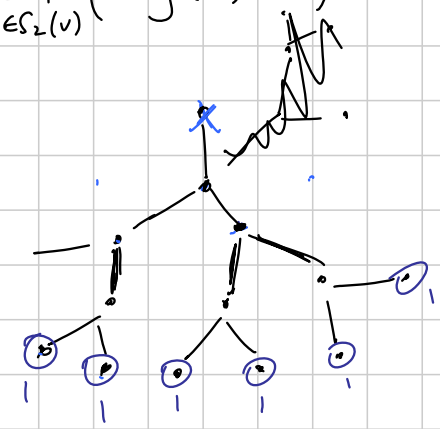
mossa utile: Semplifico Γ! elimino i cicli, mantenendo le distanze da v_0!

Con questa semplificazione, $|S_2(v)| = \sum_{w \in S_1(v)} \deg(w) - 1$

$100 \overset{hp}{\geq} |S_3(v)| = ?$ $\quad \Rightarrow \quad |S_2(v)| = \sum_{w \in \Gamma_1(v)} \deg w - \deg v$

notare che l'ipotesi su Γ resta valida.

$$|S_3(w)| = \sum_{w \in S_2(v)} \left(\deg(w) - 1 \right)$$



$$|S_3(v)| \approx \sum_{w \in S_1(v)} |S_2(w) \setminus ?|$$

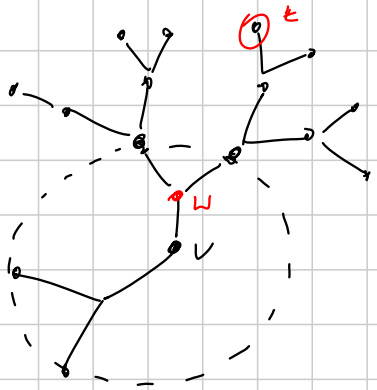
$$|S_4(v)| \approx \sum_{w \in S_1(v)} |S_3(w) \setminus \dots|$$

$$\boxed{|100 \geq |S_3(v)|| = \sum_{w \in S_1(v)} |S_2(w)| - (\deg v - 1) \deg v}$$

vale $\forall$ vertice!

$$|S_2(w)| = \sum_{w' \in S_1(w)} (\deg w' - 1)$$

$$\text{però} \geq |S_4(v)| = \sum_{w \in S_1(v)} |S_3(w)| - \sum_{w \in S_1(v)} |S_2(v)| + |S_1(w)| = 0$$



$t \in S_3(w)$

$$= \sum_{w \in S_1(v)} |S_3(w)| - S_2(v) \cdot \deg v + \sum_{w \in S_1} \deg w - \deg v$$

$\wedge\wedge$
100

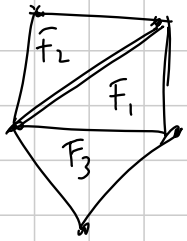
$$= 99 \cdot \deg v - |S_2(v)| \cdot \deg v + \sum_{w \in S_1(v)} \deg w$$

$$= 99 \cdot \deg v - |S_2(v)| \cdot \deg v + |S_2(v)| + \deg v$$

$$\leq 100x - x^2 \quad \text{per un qualche par. } x.$$

(in sospeso)

Folklore: Un **grafo planare**: un grafo che si può immergere nel piano ($V \to$ punti nel piano, $E \to$ curve che uniscono) in modo che archi non si intersechino fuori dei vertici (tranne quando sono incidenti).



$|V|$, $|E|$

thm (utile) Formula di Eulero:

$$|V| - |E| + |F| = 2 \quad \forall \text{ grafo planare.}$$

Per induzione.

cor Un poliedro convesso soddisfa la stessa formula.

thm Ci sono al più 5 solidi platonici.

- in ogni vertice concorrono $d \geq 3$ facce ($\sigma = 0$ d lati)
- tutte le facce sono ℓ-agoni regolari.

f, e, v: $\quad e = \frac{f \cdot \ell}{2}$ $\quad d \geq 3$

$v = \frac{f \cdot \ell}{d}$

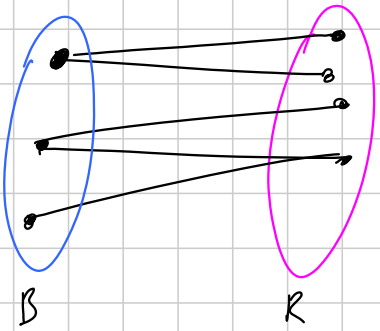
$$f \cdot \left(1 - \frac{\ell}{2} + \frac{\ell}{d}\right) = 2 \qquad \ell \geq 3 \Rightarrow d < 6.$$

$\ell > 0$, siccome $d \geq 3$, è negativo. Ultimo un # finito di casi

finita per conto vostro

Teorema di Hall / Lemma dei matrimoni.

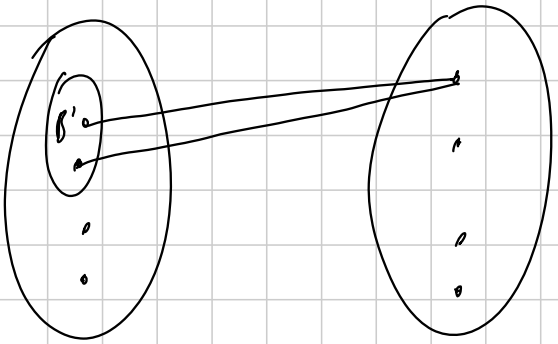
Supponiamo di aver un grafo **bipartito**



Quando posso avere $f: B \to R$ iniettiva t.c. $\{f(b), b\} \in E \ \forall b$?

ostruzione ovvia: $|R| \geq |B|$.

ostruzione semi-ovvia deve valere $\forall$ sotto $B' \subset B$.



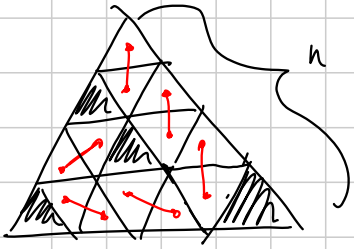
$B' \subset B$, dove $\Gamma(B')$ = l'insieme degli elementi in R che sono collegati a un B'.

C'è speranza solo se $|\Gamma(B')| \geq |B'| \ \forall B' \subset B$.

Thm (Hall) Vale il viceversa! $\exists f$ come sopra sse $\forall B' \subset B \quad |\Gamma(B')| \geq |B'|$.

dim Per induzione.

IMO SL 06/C6



n colori n

Dimostrare che posso tassellare quello che rimane

usando k colori k a k per ogni sottotriangolo

ho colorato al più k triangolini.

$B = \{\nabla\}$ $\quad R = \{\Delta\}$ o viceversa.

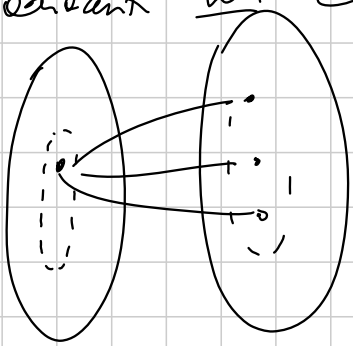
hp dico che in ogni Δ che ha punta ∇ ci sono almeno tanti Δ

Grafo?

Collego ∇ con quelli adiacenti non colorati.

OSS

$\Rightarrow$



$d := \deg v.$

$$|S_4(v)| = \sum_1^d \left(\underbrace{|S_3(w)|}_{\leq 100} - |S_2(v)| + |S_1(w)| - 1 \right) \qquad S = \sum_2 d_2$$

$$\leq 100 \cdot d - d \cdot |S_2(v)| + \sum_{w \in S_1(v)} \deg w - d$$

$$= 100d - d \cdot (S - d) - d \neq S =$$

$= 100d - (d-1)\cdot S + d^2 - d$

oss $S = \sum_i \deg w \geq 2d$

$\deg w \geq 2$ $\forall w$

$\leq 100d - 2(d-1)d + (d-1)d =$

$\leq 101d - d^2$

$\max(101d - d^2) = 101 \cdot 50 - 50^2 = 2550.$

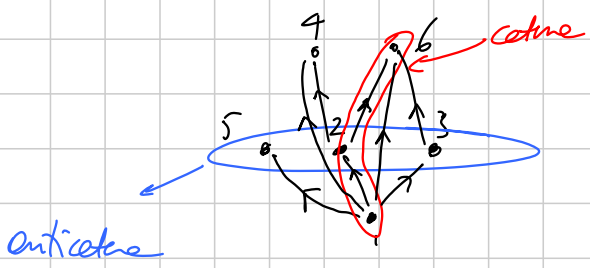
Un ordine parziale su un insieme P è una relazione $<, \leq$ $x \leq y$, t.c. $x<y, y<z \Rightarrow x<z$

non riflessiva $x \not< x$.

es $<$, $\subset$ (sottoinsiemi), $|$ (divisibilità)

$\subseteq$ $\quad$ $\leq$

Se anche un $(P, <)$ finito, potete allocarci un grafo.



$\Gamma_{(P,<)}$ è orientato, aciclico.

~~$\{v,w\}$~~ $(v,w) \in V \times V$.

Possiamo parlare di percorsi orientati:

$1 \to 2 \to 4$ è un percorso orientato.

Una <u>catena</u> in $(P, <)$ è un percorso orientato in $\Gamma_{(P,<)}$.

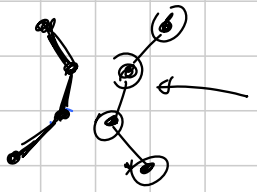
Un'<u>anticatena</u> in $(P, <)$ è un insieme tot. sconnesso.

(P finito)

<u>Thm</u> (Dilworth) Se $\Gamma_{(P,<)}$ ha un'anticatena di lunghezza ℓ (ma non una di lungh. $\ell+1$), allora P è unione di ℓ catene.

2. Se P è unione di ℓ catene (ma non di $\ell-1$), allora c'è un'anticatena di cardinalità ℓ.

<u>dim</u> 1. Se ci fossero $\ell-1$ catene $\Rightarrow$ almeno 2 elem. dell'anticatena stanno nella stessa catena. Assurdo.

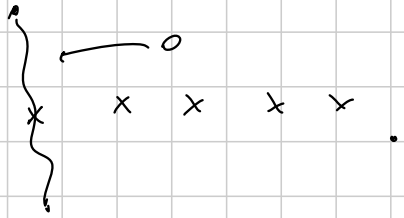


almeno una di queste catene è disgiunta dall'anticatena.

Un'altra idea: prendere una catena massimale e via induzione su ℓ.

Unica cosa a cui non abbiamo accesso è che

$P \setminus C_{max}$ non ha un'anticatena con ℓ elementi.



l'ordine è il contenimento

Teo (Sperner) $A \subset \mathcal{P}(X)$ anticatena ($\subset$). Allora $|A| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$ elementi.

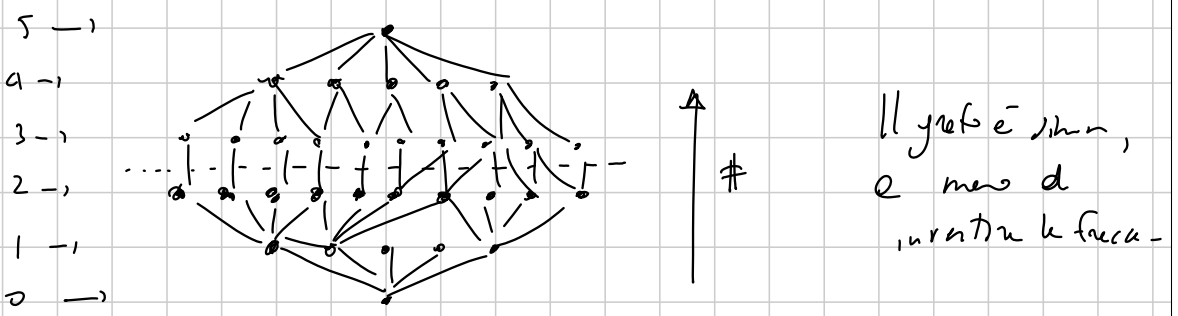
Oss Chiaramente, un'anticatena con $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ è tale che:

$\binom{n}{\lfloor \frac{n}{2} \rfloor}$ = # insiemi con $\lfloor \frac{n}{2} \rfloor$ elementi

$\Downarrow$

anticatena.

dim Ci basta dimostrare che $\mathcal{P}(X)$ è unione di N catene!

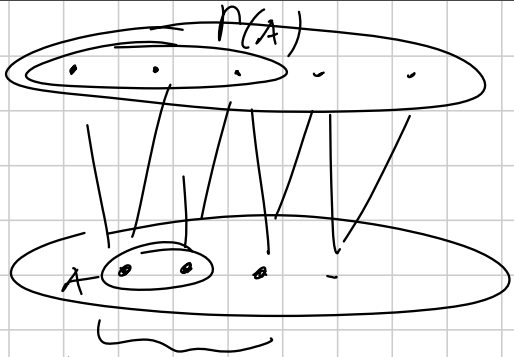


Il grafo è simmetrico, e mano a mano aumentano le frecce.

Basta scrivere questo grafo come unione di N catene

Vogliamo arrivare ad un sottoinsieme di X con k elementi. Un sott. con $k+1$ elementi che lo contiene.

Proviamo ad applicare il lemma dei matrimoni!?



$k+1$ elem

k elem.

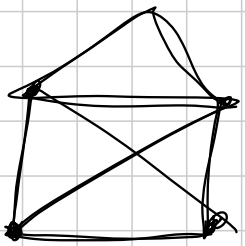
M elem quanti ce ne stanno sopra

Dim per induzione su M che $|\Gamma(A)| \geq |A|$

se $k+1 \leq n/2$. ES.

---

folklore Percorso Euleriano su un grafo Γ



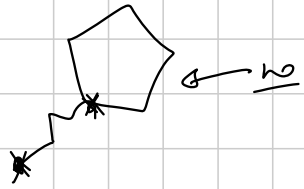
percorso Euleriano passa per tutti gli archi di Γ una ed una sola volta.

dom Per quali grafi esiste un percorso Euleriano?

Grafi Connessi Euleriani:

Ci sono dei grafi per cui, andando a caso, fate un percorso Euleriano? Con tutti vertici pari.

Sì, i cicli.

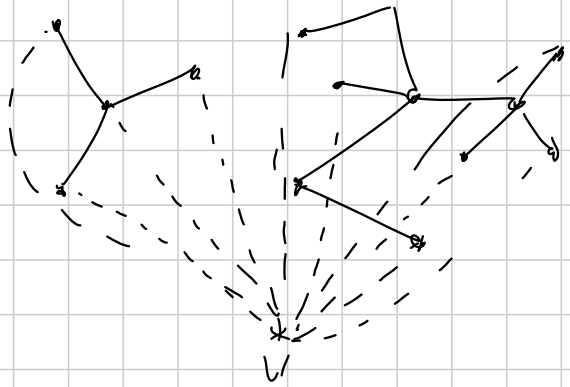


Criterio Γ è C.E. $\Leftrightarrow \exists v$ t.c. tutti i cicli di Γ passano per E. (partendo da v)

~~Formal~~

dim Per induzione: sul grado di v o sul # cicli.

es



fatti Un albero su n vertici ha $n-1$ archi.

dom Quanti alberi numerati ci sono su n vertici?

Sol n^{n-2}. L'idea è che ad un albero numerato $\rightarrow$ successione di $n-2$ interi in $\{1, \dots, n\}$ (e viceversa)

G1 - Medium (Sam)

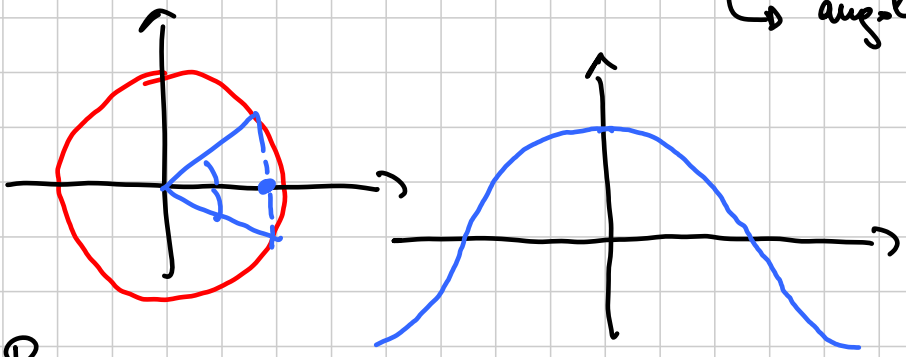
Titolo nota 02/09/2014

- Vettori
- Coordinate
- Complessi

Vettori

$$\vec{A}\cdot\vec{B} = \|\vec{A}\|\cdot\|\vec{B}\|\cdot\cos\widehat{AB}$$

↳ angolo tra i vettori



Piano ⇓ in 2 coord $\vec{A} = (a_1, a_2)$ $\vec{B} = (b_1, b_2)$

$$\vec{A}\cdot\vec{B} = a_1b_1 + a_2b_2$$

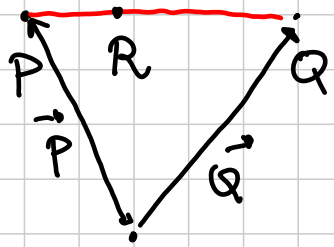
si può fare in n coordinate

Es: IF I = incentro F = centro della cfr. di Feuerbach

Fissata qualunque origine

$$|F|^2 = \|\vec{I}-\vec{F}\|^2 = (\vec{I}-\vec{F})\cdot(\vec{I}-\vec{F})$$

$$\vec{I} = \frac{a\vec{A}+b\vec{B}+c\vec{C}}{a+b+c}$$

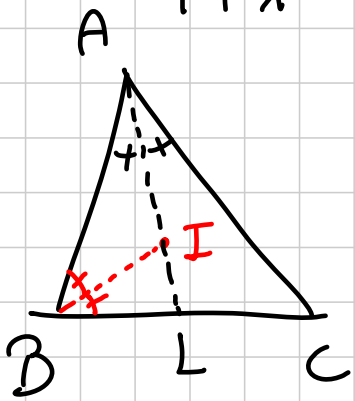


$$\frac{PR}{RQ} = \frac{\lambda}{1}$$

punti materiali $P_1, \dots, P_N$
con masse $m_1, \dots, m_N$

$$\frac{m_1\vec{P_1} + \dots + m_N\vec{P_N}}{m_1 + \dots + m_N}$$

$$\vec{R} = \frac{\vec{P} + \lambda\vec{Q}}{1+\lambda}$$



$$\frac{BL}{LC} = \frac{c}{b} \qquad \vec{L} = \frac{c\vec{C} + b\vec{B}}{b+c}$$

$$\frac{LI}{IA} = \frac{BL}{c}$$

$$I = \frac{a\vec{A} + b\vec{B} + c\vec{C}}{a+b+c}$$

$\vec{F} = ?$ F pt. medio di OH (O circocentro H ortocentro)

se metto l'origine in O

$$\vec{H} = \vec{A} + \vec{B} + \vec{C}$$

$$\vec{F} = \frac{1}{2}(\vec{O} + \vec{H}) = \frac{\vec{A} + \vec{B} + \vec{C}}{2}$$

$$\|\vec{I}-\vec{F}\|^2 = \left\| \frac{aA+bB+cC}{a+b+c} - \frac{A}{2} - \frac{B}{2} - \frac{C}{2} \right\|^2 =$$

$$= \left\| \frac{A(a-b-c) + B(b-a-c) + C(c-a-b)}{2(a+b+c)} \right\|^2 =$$

$$= \frac{1}{4(a+b+c)^2} \left[\sum_{cyc} AA\,(a-b-c)^2 + 2 \sum_{cyc} A\cdot B\,(a-b-c)(b-a-c) \right]$$

$$= \frac{1}{4p^2} \left[\sum_{cyc} R^2 (a-b-c)^2 + \sum_{cyc} (2R^2 - c^2)(c^2 - a^2 - b^2 + 2ab) \right],$$

$\vec{A}\cdot\vec{A} = R^2$ $\qquad 2\vec{A}\cdot\vec{B} = 2R^2 - c^2$

origine in O

$$= \frac{1}{4p^2} \left[\sum_{cyc} R^2 (a^2+b^2+c^2-2ab-2ac+2bc) + \sum_{cyc} \cdots \right] =$$

$$= \frac{1}{4p^2} \left[R^2 \left(3\sum_{cyc} a^2 - 2\sum_{cyc} a^2 + 2\sum_{cyc} ab \right) - \left(\sum_{cyc} a^4 - 2\sum_{cyc} a^2 b^2 \right) - 2\sum_{cyc} a^2 bc \right] =$$

$$= \frac{1}{4p^2} R^2 \underbrace{\left(\sum_{cyc} a^2 + 2\sum_{cyc} ab \right)}_{11p^2} + \frac{1}{4p^2} 165^2 - \frac{2abc\cdot p}{4p^2} =$$

$$= \frac{1}{4}R^2 + \frac{4S^2}{p^2} - \frac{abc}{2p} = \frac{R^2}{4} + r^2 - 2\frac{R}{2}\cdot r =$$

$$= \left(\frac{R}{2} - r\right)^2 \qquad IF = \frac{R}{2} - r$$

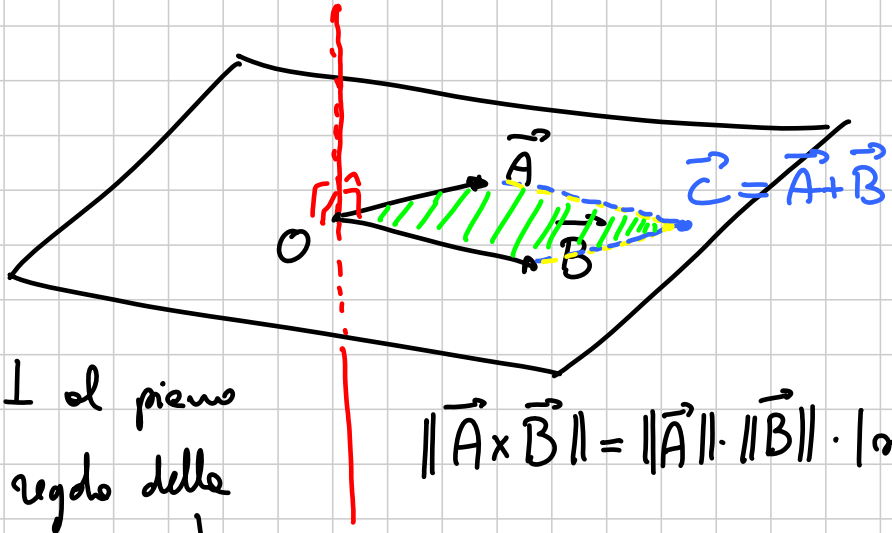
$OH = ?$ $GH = ?$ $GO = ?$ $GI = ?$ $IH = ?$

ΔGIH è ottusangolo.

Oss: $\vec{P}\cdot\vec{Q} = 0 \iff \vec{P} = \vec{0}$ oppure $\vec{Q} = \vec{0}$ (O origine)

$PO \perp QO$

Prodotto vettore: $\vec{A}, \vec{B} \longrightarrow \vec{A}\times\vec{B}$ in 3 dim.



dir = $\perp$ al piano

verso = regola della mano dx.

$\|\vec{A}\times\vec{B}\| = \|\vec{A}\|\cdot\|\vec{B}\|\cdot|\sin A\hat{O}B|$

$\Rightarrow \vec{A}\times\vec{B} = -\vec{B}\times\vec{A}$

A, O, B allineati: $\iff \vec{A}\times\vec{B} = \vec{0}$

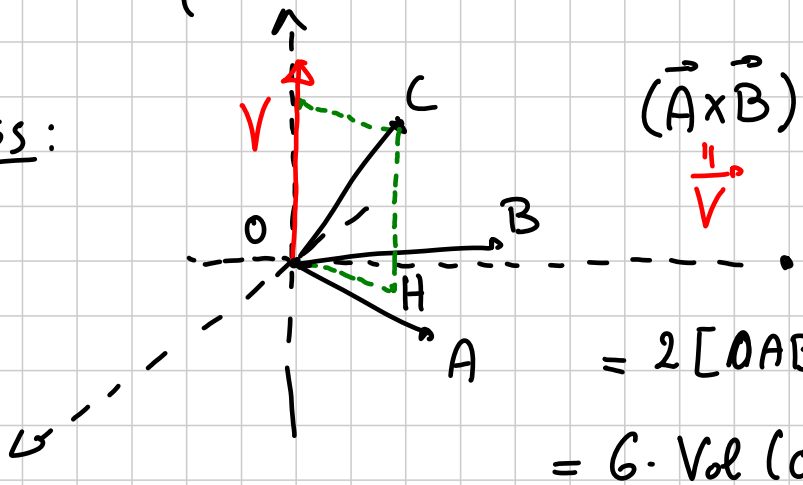
$$\|A \times B\| = 2[AOB]$$

ED per casa: $\vec{A} = (a_1, a_2, a_3)$

$\vec{B} = (b_1, b_2, b_3)$

$$\vec{A} \times \vec{B} = (a_2 b_3 - b_2 a_3,\ b_1 a_3 - a_1 b_3,\ a_1 b_2 - b_1 a_2)$$

Oss:



$$(\vec{A} \times \vec{B}) \cdot \vec{C} =$$

$$\|\vec{V}\|$$

$$= 2[OAB] \cdot CH =$$

$$= 6 \cdot \mathrm{Vol}(OABC)$$

$A = (a_1, a_2, a_3)$

$B = (b_1, b_2, b_3)$

$C = (c_1, c_2, c_3)$

$$(A \times B) \cdot C =$$

$$= c_1 a_2 b_3 - c_1 b_2 a_3 + c_2 b_1 a_3 - c_2 a_1 b_3 + c_3 a_1 b_2 - c_3 b_1 a_2 =$$

$$= \det \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix}$$

$A+B$
B
C

$C = D + E$

$$((A+B) \times B) \cdot C =$$

$$= (A \times B) \cdot C + (B \times B) \cdot C$$
$$\hat{\imath} \quad 0$$

Coordinate baricentriche

ABC triangolo P punto del piano

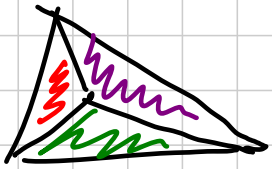
$\rightarrow \exists!\ \alpha, \beta, \gamma$ reali t.c.

(i) $\alpha+\beta+\gamma = 1$

(ii) $\alpha\vec{A} + \beta\vec{B} + \gamma\vec{C} = \vec{P}$

$[XYZ] > 0$ se X, Y, Z sono in senso antiorario

$$\gamma = \frac{[PAB]}{[ABC]}, \dots,$$



$P = \alpha A + \beta B + \gamma C \qquad Q = \rho A + \sigma B + \tau C$

pt. medio $\frac{\alpha+\rho}{2} A + \frac{\beta+\sigma}{2} B + \frac{\gamma+\tau}{2} C$

Coord. baricentriche di $P = [p : q : r]$

t.c. $\vec{P} = \dfrac{p\vec{A} + q\vec{B} + r\cdot\vec{C}}{p+q+r}$

se $p+q+r = 1$ si dicono normalizzate

$\underline{E\Lambda}$: $\{lx + my + nz = 0\}$ l, m, n reali

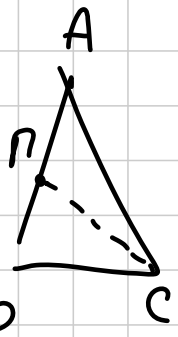
Λ_0 è una retta

$x + y = 0$ $\quad x = 0, y = 0, z = 0$ lati

$\underline{E\Lambda}$: $A = [1:0:0]$ $\quad B = [0:1:0]$ $\quad C = [0:0:1]$

Π = pt medio di $AB = [\frac{1}{2} : \frac{1}{2} : 0] = [1:1:0]$

↑ normalizzato ↑ generico



$C\Pi$ → della forma $lx + my + nz = 0$

passare per C $\quad l \cdot 0 + m \cdot 0 + n \cdot 1 = 0$

// // Π $\quad l \cdot 1 + m \cdot 1 + n \cdot 0 = 0$

$$\begin{cases} n = 0 \\ l + m = 0 \end{cases} \qquad x - y = 0$$

$\underline{\text{Un po' di punti}}$: $G = [1:1:1]$

$I = [a:b:c]$ → eccentri a coppie uno a uno

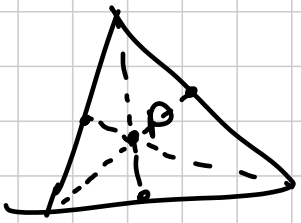
$\Pi_a = [0:1:1]$ $\quad \Pi_b = [1:0:1]$

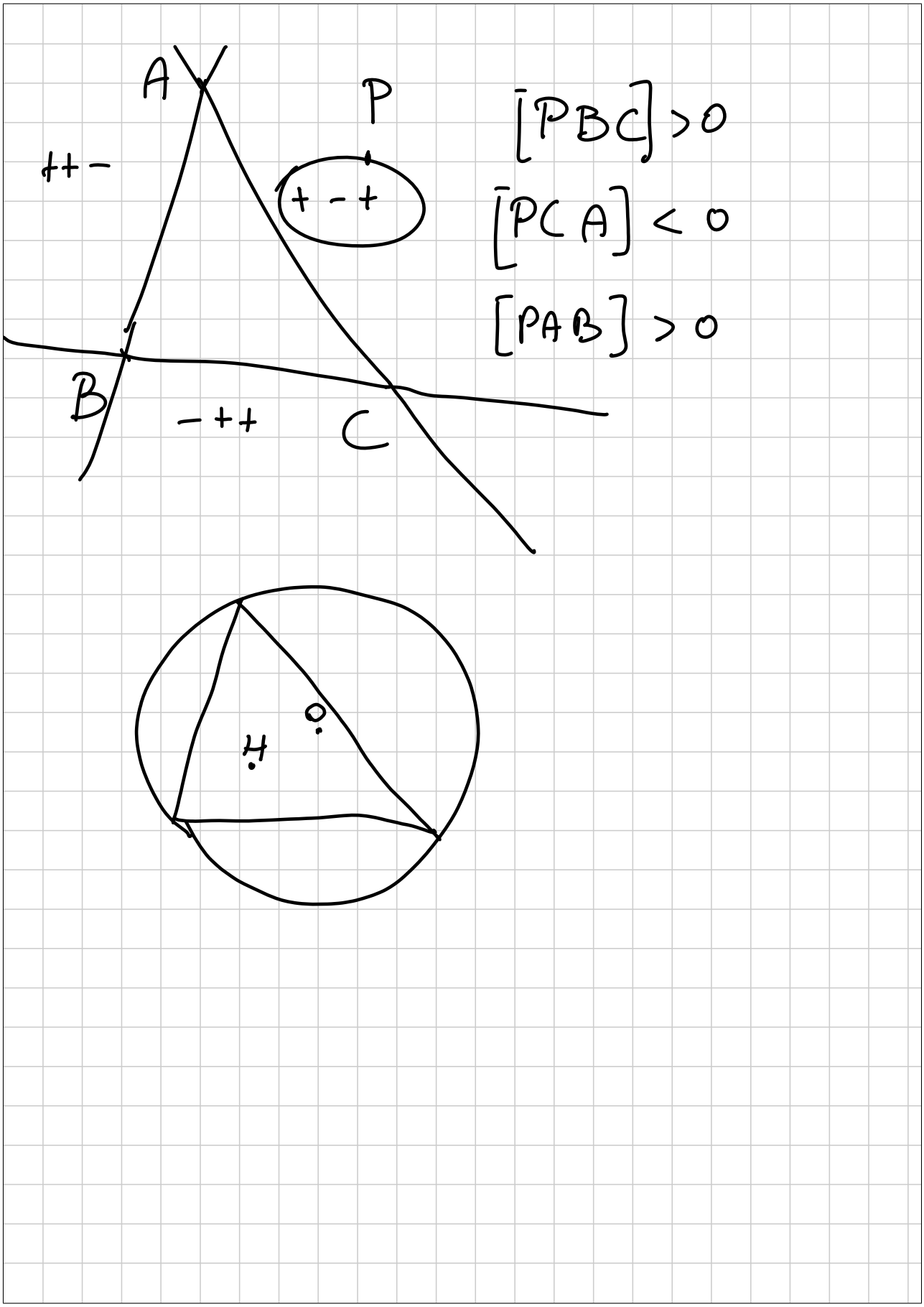
$\Pi_c = [1:1:0]$

piedi delle bisett: $L_a = [0:b:c]$

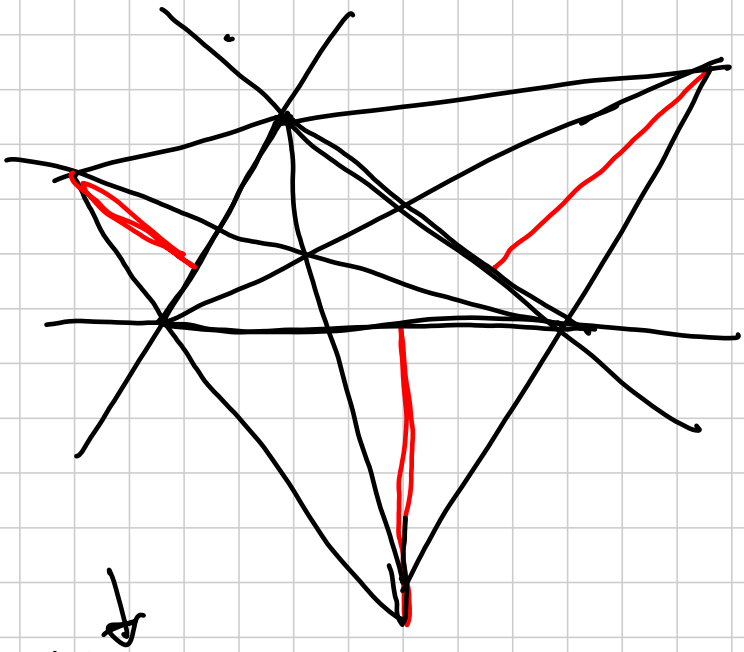
$O = \ldots$

$H = \ldots$

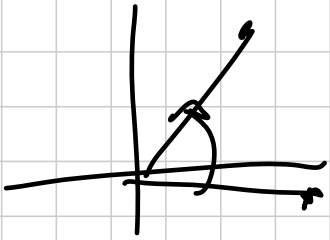




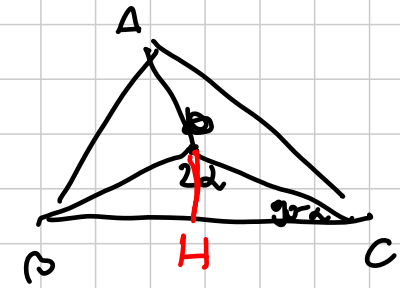
Geometria 1 (Medium) – Samuele Mongodi – Gioacchino Antonelli



$\mathbb{R}^3$



- Y1U: Introduction to Triangle Geometry
- I. to the geometry of Complex Numbers



$[\Delta OBC : \Delta OCA : \Delta OAB]$

$\left[\frac{BC \cdot OH}{2} : \dots\right]$

$\left[\frac{2R \sin\alpha R\cos\alpha}{2} : \dots\right]$

$\frac{a}{\sin\alpha} = \frac{b}{\sin\beta} = \frac{c}{\sin\gamma} = 2R$

$[\sin\alpha\cos\alpha : \sin\beta\cos\beta : \sin\gamma\cos\gamma]$ 1.)

$[\sin 2\alpha : \sin 2\beta : \sin 2\gamma]$

2) $[2R\sin\alpha\cos\alpha \cdot \dots]$

$[a\cos\alpha : b\cos\beta . - c\cos\gamma]$

$\left[a\left(\frac{b^2+c^2-a^2}{2bc}\right) : \dots\right]$

$[a^2(b^2+c^2-a^2) : \dots]$ 2)

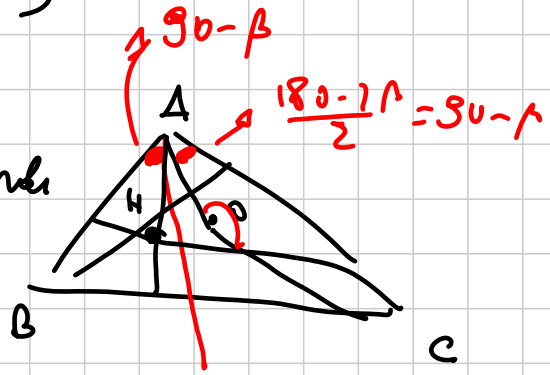
CONWAY $\quad S_A = 2S \cdot \frac{1}{4}\cot\alpha = \frac{b^2+c^2-a^2}{2}$

$2 \cdot \frac{bc\sin\alpha}{2} \cdot \frac{\cos\alpha}{\sin\alpha}$ // cormot

$S_B = \dots$

$S_C = \dots$

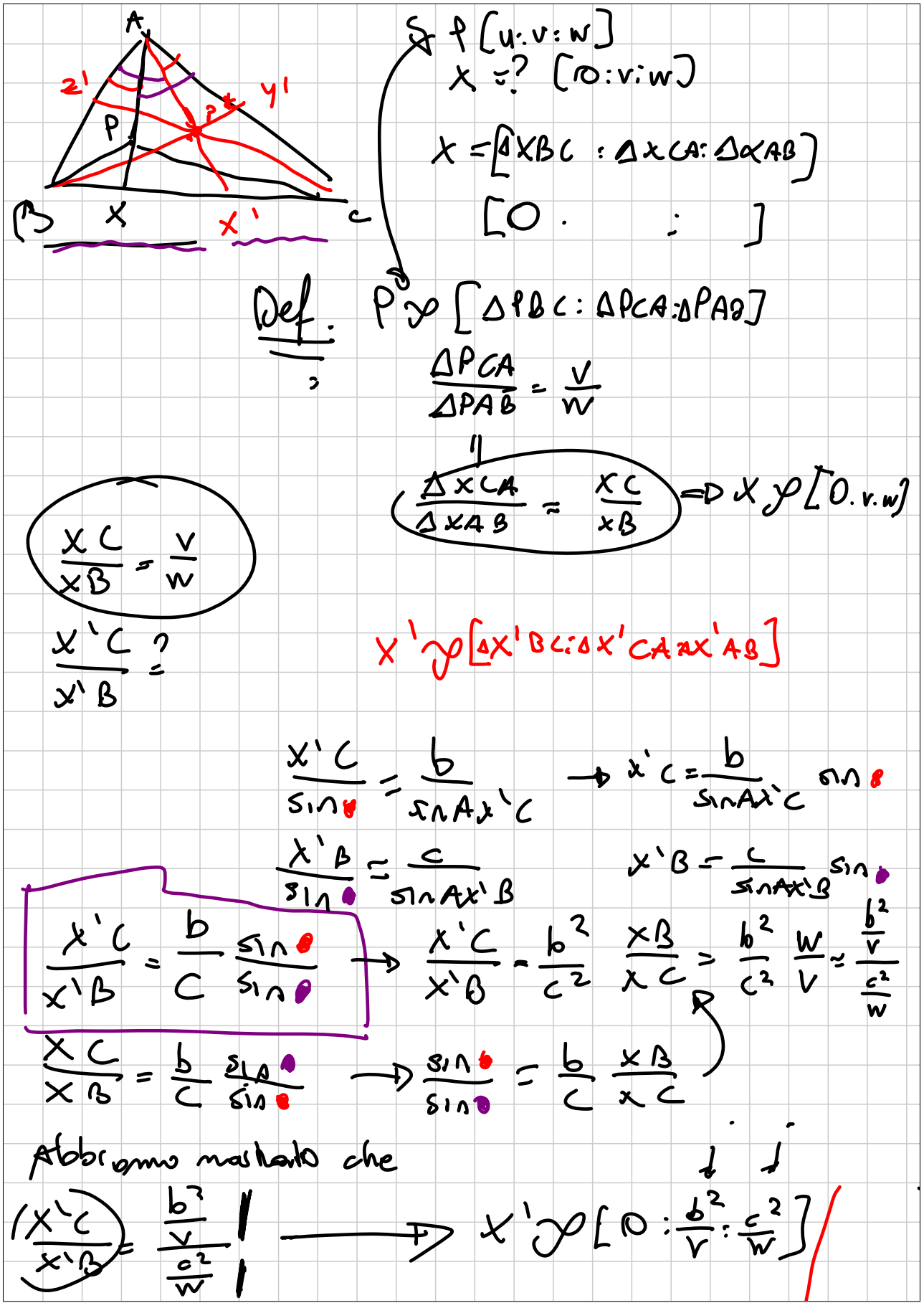
3) $[Q^2 S_A : \dots]$



H, O coniugati isogonali

$P[u:v:w]$

$P^C : ?$


A
B
C
X
X'
P
Def:
Abbiamo mostrato che

$Y' \in \left[\frac{a^2}{u} : 0 : \frac{c^2}{w}\right]$

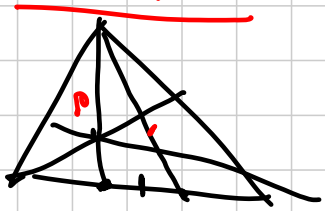
$Z' \in \left[\frac{a^2}{u} : \frac{b^2}{v} : 0\right]$

$P'\left[\frac{a^2}{u} : \frac{b^2}{v} : \frac{c^2}{w}\right]$

$H\left[\frac{a^2}{a^2 S_A} \cdot \dots\right] = H\left[\frac{1}{S_A} : \dots\right]$

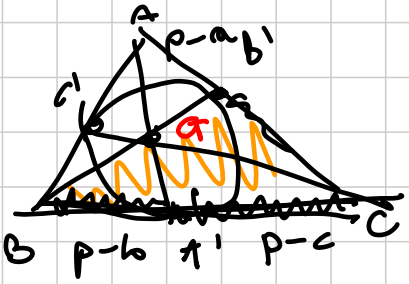
ISOTOMICO

$H[\text{tana} : \dots]$



$P[u:v:w] \to P'\left[\frac{1}{u} : \frac{1}{v} : \frac{1}{w}\right]$

G



GF

$A'[0 : p-c : p-b]$

$B'[p-c : 0 : p-a]$

$C'[p-b : p-a : 0]$

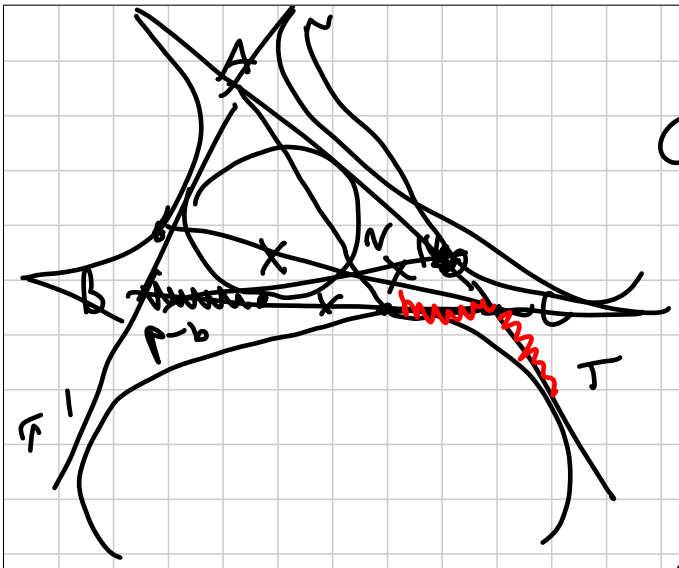
$A'\left[0 : \frac{1}{p-b} : \frac{1}{p-c}\right]$

$B'\left[\frac{1}{p-a} : 0 : \frac{1}{p-c}\right]$

$C'\left[\frac{1}{p-a} \cdot \frac{1}{p-b} : 0\right]$

$\to G\left[\frac{1}{p-a} \cdot \frac{1}{p-b} : \frac{1}{p-c}\right]$

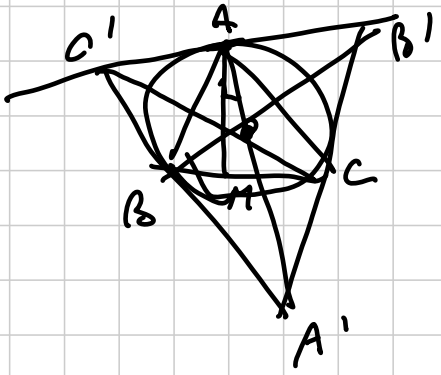
$M[p-a : p-b : p-c]$



$CT = AT - AC = p - b$

$AT' + AT = Ab + BT' + AC + Cx' = Ab + BX + AC + Cx' = \text{Perimetro}$

$G[1:1:1]$ $\quad L[a^2 : b^2 : c^2]$



$O[a^2 S_A : b^2 S_B : c^2 S_C]$

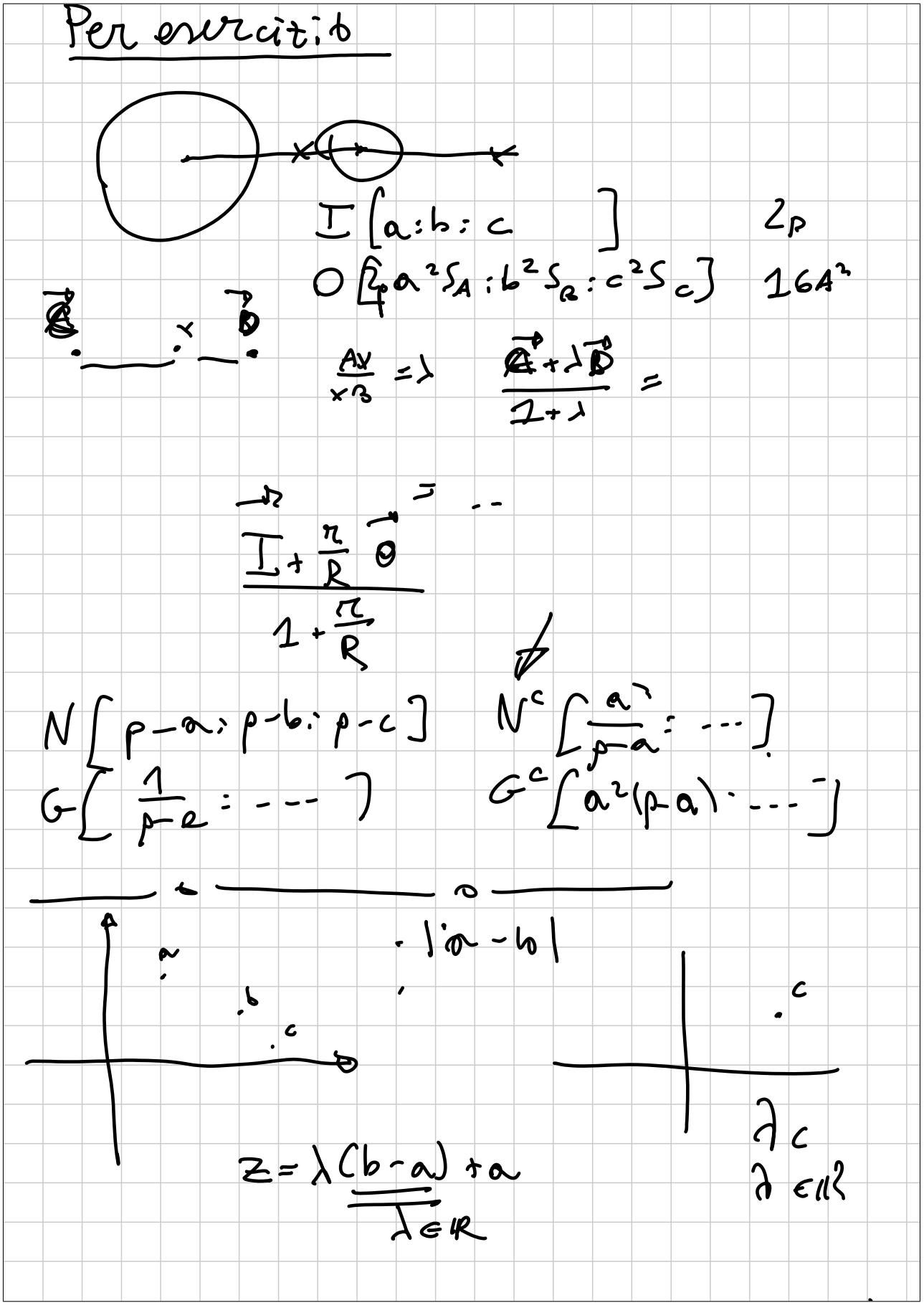
$a^2 S_A + b^2 S_B + c^2 S_C = 16 A^2$ (*) Eulero

$H[S_B S_C : S_A S_C : S_A S_B]$

$S_B S_C + S_A S_C + S_A S_B = 4A^2$ Dimostra!

$= a^4 + b^4 + c^4 + a^2 b^2 + b^2 c^2 + a^2 c^2$

$F : \left[\frac{a^2 S_A + 4 S_B S_C}{2} : \right]$


Per esercizio
I [a : b : c]
O [a²S_A : b²S_B : c²S_C]
2p
16A²
N [p−a : p−b : p−c]
G [1/(p−a) : ...]
N^c [a²/(p−a) : ...]
G^c [a²(p−a) · ...]
|a − b|
a
b
c
c
z = λ(b − a) + a
λ ∈ ℝ
∂c
λ ∈ ℝ

$\exists \lambda \quad c = \lambda(b-a) + a \qquad \lambda \in \mathbb{R}$

$\frac{c-a}{b-a} \in \mathbb{R} \iff \boxed{\frac{c-a}{b-a} = \frac{\bar{c}-\bar{a}}{\bar{b}-\bar{a}}}$ ALT.

$\frac{z-a}{b-a} \in \mathbb{R} \iff \frac{z-a}{b-a} = \frac{\bar{z}-\bar{a}}{\bar{b}-\bar{a}}$

$(b\bar{z}) - (\bar{b}z)$

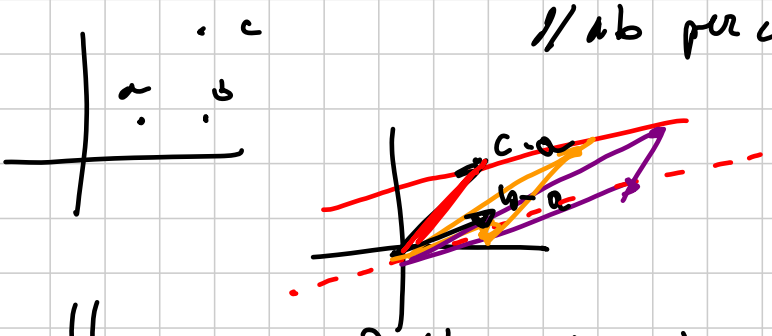
1) $(\bar{b}-\bar{a})z + (a-b)\bar{z} + \boxed{b\bar{a} - a\bar{b}} = 0$

$\underbrace{i(\bar{b}-\bar{a})}_{A} z + \underbrace{i(a-b)}_{\bar{A}}\bar{z} + \underbrace{i(b\bar{a}-a\bar{b})}_{B} = 0$

2) $Az + \bar{A}\bar{z} + B = 0 \qquad B \in \mathbb{R}.$

Raddoppio

// ab per c



$z = c - a + \lambda(b-a) \quad \lambda \in \mathbb{R}$

$z = c - \cancel{a} + \lambda(b-a) + \cancel{a}$

$z = c + \lambda(b-a)$

$\exists \lambda$ t.c. $d = c + \lambda(b-a) \qquad \lambda \in \mathbb{R}$

$\frac{d-c}{b-a} \in \mathbb{R} \iff \boxed{\frac{d-c}{b-a} = \frac{\bar{d}-\bar{c}}{\bar{b}-\bar{a}}}$

$\frac{z-c}{b-a} = \frac{\bar{z}-\bar{c}}{\bar{b}-\bar{a}} \longrightarrow (\bar{b}-\bar{a})z + (a-b)\bar{z} + c\bar{a} - a\bar{c} + \bar{c}b - \bar{b}c = 0$

Perpendicolare

$z = c - a + \lambda i (b-a) \quad \lambda \in \mathbb{R}$

$z = c + \lambda i (b-a) \quad \lambda \in \mathbb{R}$

$ab \perp cd$

$\exists \lambda$ t.c. $d = c + \lambda i (b-a)$

$\frac{d-c}{b-a} \in Im \iff \boxed{\frac{d-c}{b-a} = -\frac{\bar{d}-\bar{c}}{\bar{b}-\bar{a}}}$

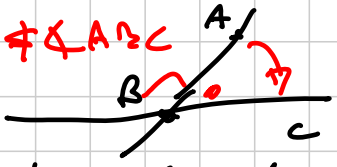
Retta

$\frac{z-c}{b-a} = -\frac{\bar{z}-\bar{c}}{\bar{b}-\bar{a}} \longrightarrow (\bar{b}-\bar{a})z + (b-a)\bar{z} + c\bar{a} + a\bar{c} - c\bar{b} - \bar{c}b = 0$

Angoli ORIENTATI

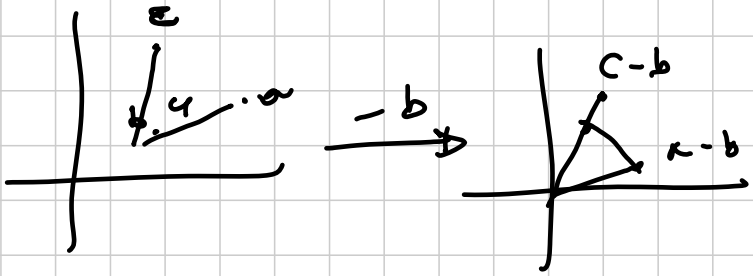
$\sphericalangle(r_1, r_2)$ misura α_1 IM per cui ruotando r_1 per come. con r_2.

$\sphericalangle ABC \neq \sphericalangle CBA$



Att può non essere l'angolo classico

$A\hat{B}C$ = a meno di $k\pi$ $k \in \mathbb{Z}$.



$$c-b = (a-b)\,e^{i\,\sphericalangle abc}\cdot\frac{|c-b|}{|a-b|}$$

EQ. ANGOLO $\dfrac{c-b}{a-b} = e^{i\varphi}\dfrac{|c-b|}{|a-b|}$ $\qquad \varphi = \sphericalangle abc$

Supponiamo di voler misurare $\sphericalangle ABC = \sphericalangle xyz$

$$\frac{c-b}{a-b} = e^{i\varphi}\frac{|c-b|}{|a-b|} \quad (1)$$

$$\frac{z-y}{x-y} = e^{i\theta}\frac{|z-y|}{|x-y|} \quad (2)$$

$\varphi = \theta$

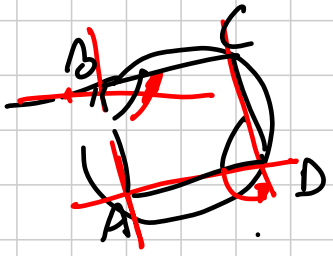
$$\frac{c-b}{a-b}\cdot\frac{x-y}{z-y} = e^{i(\varphi-\theta)}\frac{|c-b|}{|a-b|}\frac{|x-y|}{|z-y|} \in \mathbb{R}$$

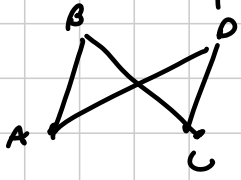
$$\frac{c-b}{a-b}\,\frac{x-y}{z-y} \in \mathbb{R} \iff \frac{c-b}{a-b}\,\frac{x-y}{z-y} = \frac{\bar{c}-\bar{b}}{\bar{a}-\bar{b}}\,\frac{\bar{x}-\bar{y}}{\bar{z}-\bar{y}}$$

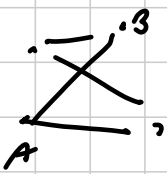
Ciclicità

b

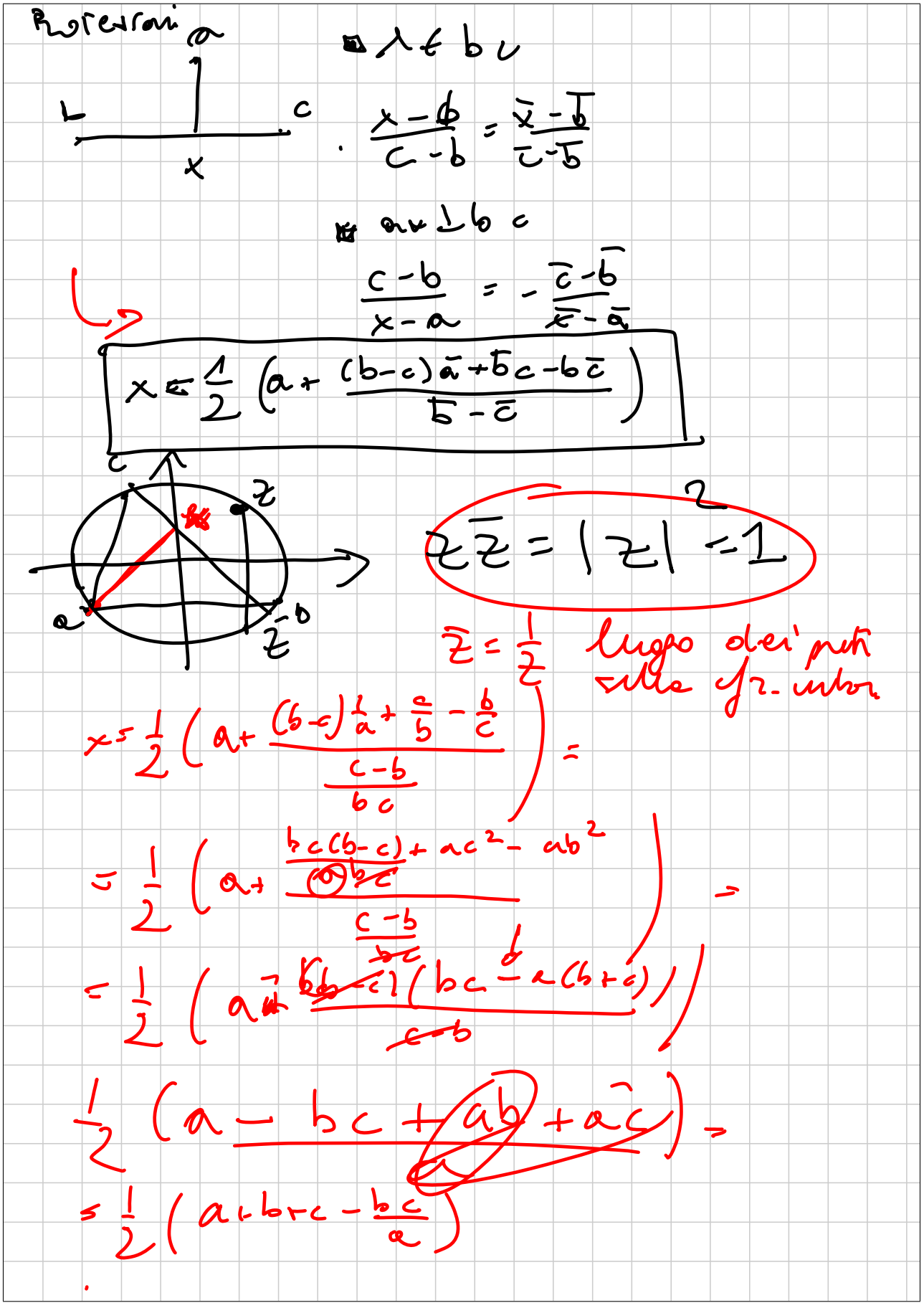
$\sphericalangle ABC = \sphericalangle AOC$

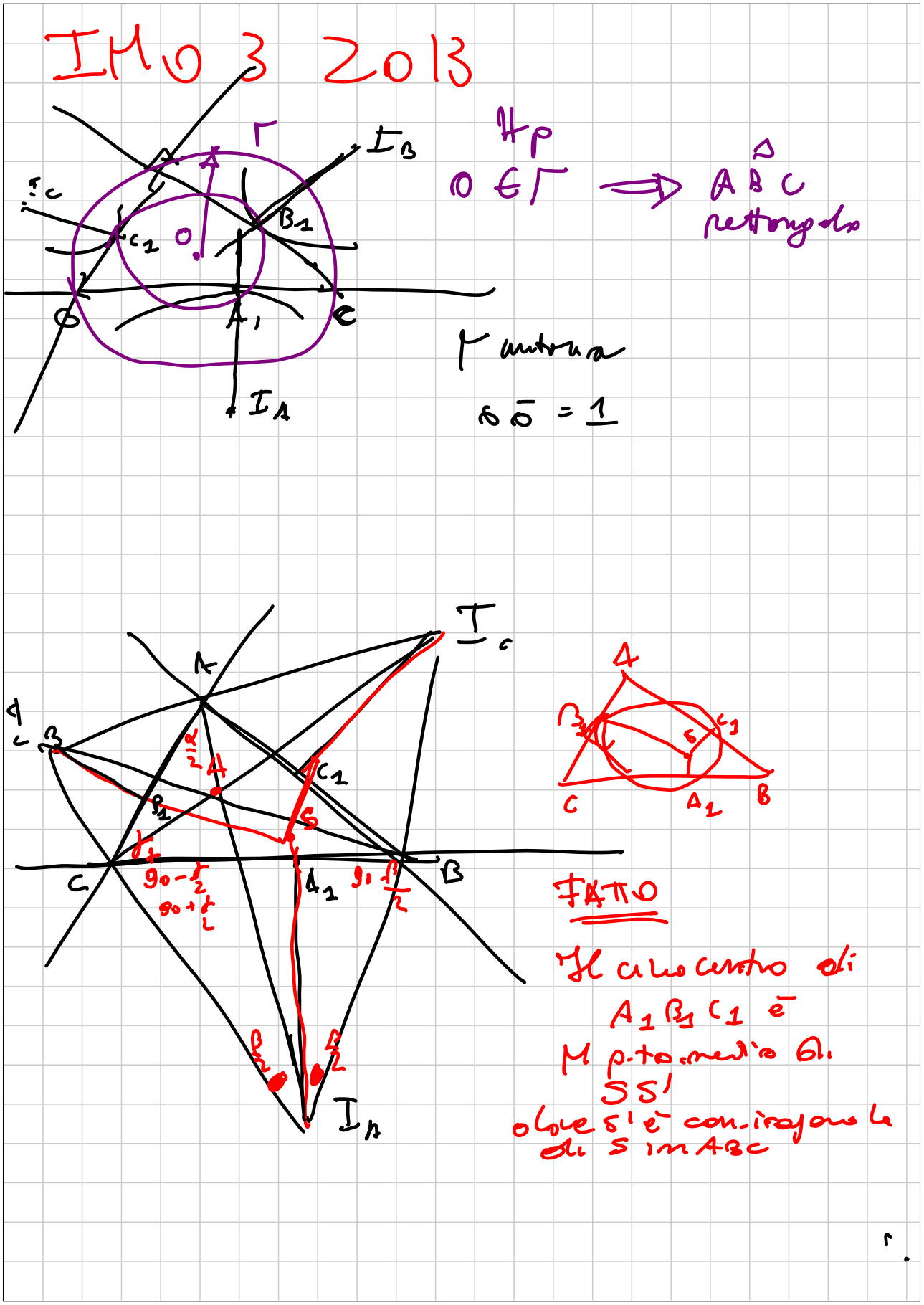


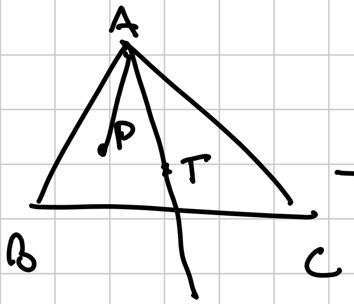




$$\frac{c-b}{a-b}\,\frac{a-d}{c-d} = \frac{\bar{c}-\bar{b}}{\bar{a}-\bar{b}}\,\frac{\bar{a}-\bar{d}}{\bar{c}-\bar{d}}$$

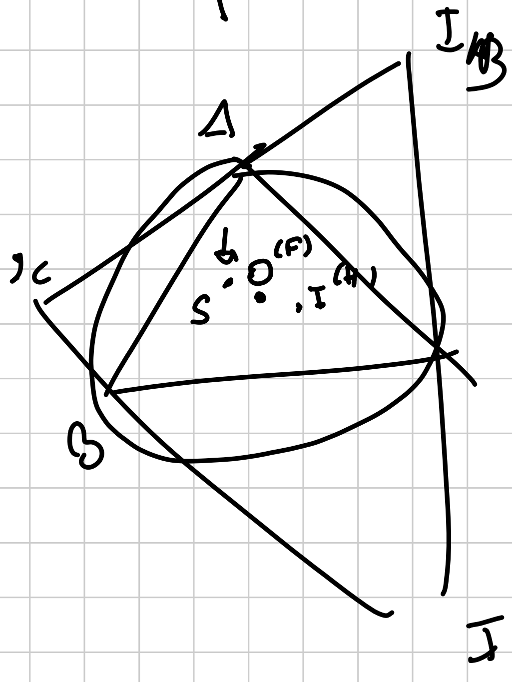

Proviamo
a
b
c
x
$\frac{x-b}{c-b} = \frac{\bar{x}-\bar{b}}{\bar{c}-\bar{b}}$
$\frac{c-b}{x-a} = -\frac{\bar{c}-\bar{b}}{\bar{x}-\bar{a}}$
$x = \frac{1}{2}\left(a + \frac{(b-c)\bar{a}+bc-b\bar{c}}{b-\bar{c}}\right)$
$z\bar{z} = |z|^2 = 1$
$\bar{z} = \frac{1}{z}$ luogo dei punti sulla circonf. unit.
$x = \frac{1}{2}\left(a + \frac{(b-c)\frac{1}{a}+\frac{c}{b}-\frac{b}{c}}{\frac{c-b}{bc}}\right) =$
$= \frac{1}{2}\left(a + \frac{bc(b-c)+ac^2-ab^2}{\frac{c-b}{bc}}\right) =$
$= \frac{1}{2}\left(a + \frac{(b-c)(bc-a(b+c))}{c-b}\right)$
$\frac{1}{2}(a - bc + ab + ac) =$
$= \frac{1}{2}\left(a+b+c-\frac{bc}{a}\right)$


IMO 3 2013
Γ
I_B
I_C
A
B
C
B_1
C_1
O
A_1
I_A
Hp
O ∈ Γ ⟹ ABC rettangolo
Γ circonferenza
OO = 1
I_C
A
B
C
C_1
A_1
B_1
S
I_B
FATTO
Il circocentro di $A_1B_1C_1$ è M punto medio di SS'
dove S' è coniugato di S in ABC



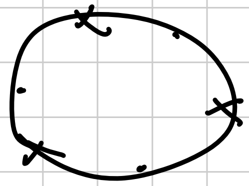
$\measuredangle BAP = \measuredangle TAC$ [illegible]

$\rightarrow t = \dfrac{-p + a + b + c - \bar{p}(ab + bc + ca) + \bar{p}^2 abc}{1 - p\bar{p}}$



b	F	H
[illegible]	[illegible]	[illegible]

C S è il simmetrico dell'incentro rispetto al circuito



TRUCCO a, b, c

$a = u^2$, $b = v^2$, $c = w^2$ → Punti $-uv, -vw, -uw$ i punti medi degli archi

$i = -(uv + vw + uw)$

$s = uv + vw + uw$ u^2, v^2, w^2

$O = \dfrac{s + s^c}{2} = \ldots$

$\begin{cases} u+v+w = A \\ uv+vw+uw = B \\ uvw = C \end{cases}$ $\bar{A} = \dfrac{B}{C}$, $\bar{B} = \dfrac{A}{C}$, $\bar{C} = \dfrac{1}{C}$

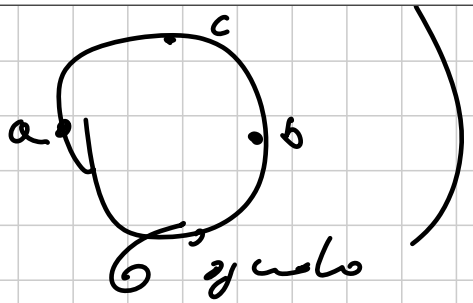
$O\bar{O} = 1 \longrightarrow \ldots$ 9° grado $\neq 0$

ABC ortocentro

$\Updownarrow$

$(a+b)(b+c)(c+a)=0$

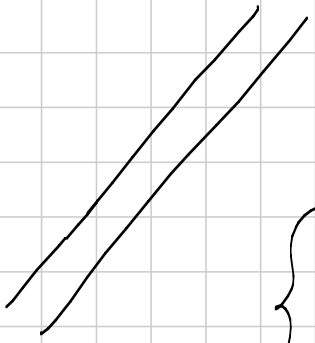
$u^2 \quad v^2 \quad v^2 \quad w^2 \quad w^2+u^2$



G2-MEDIUM [KFP]

Titolo nota 03/09/2014

COSA CAMBIA? LE RETTE PARALLELE SI INCONTRANO



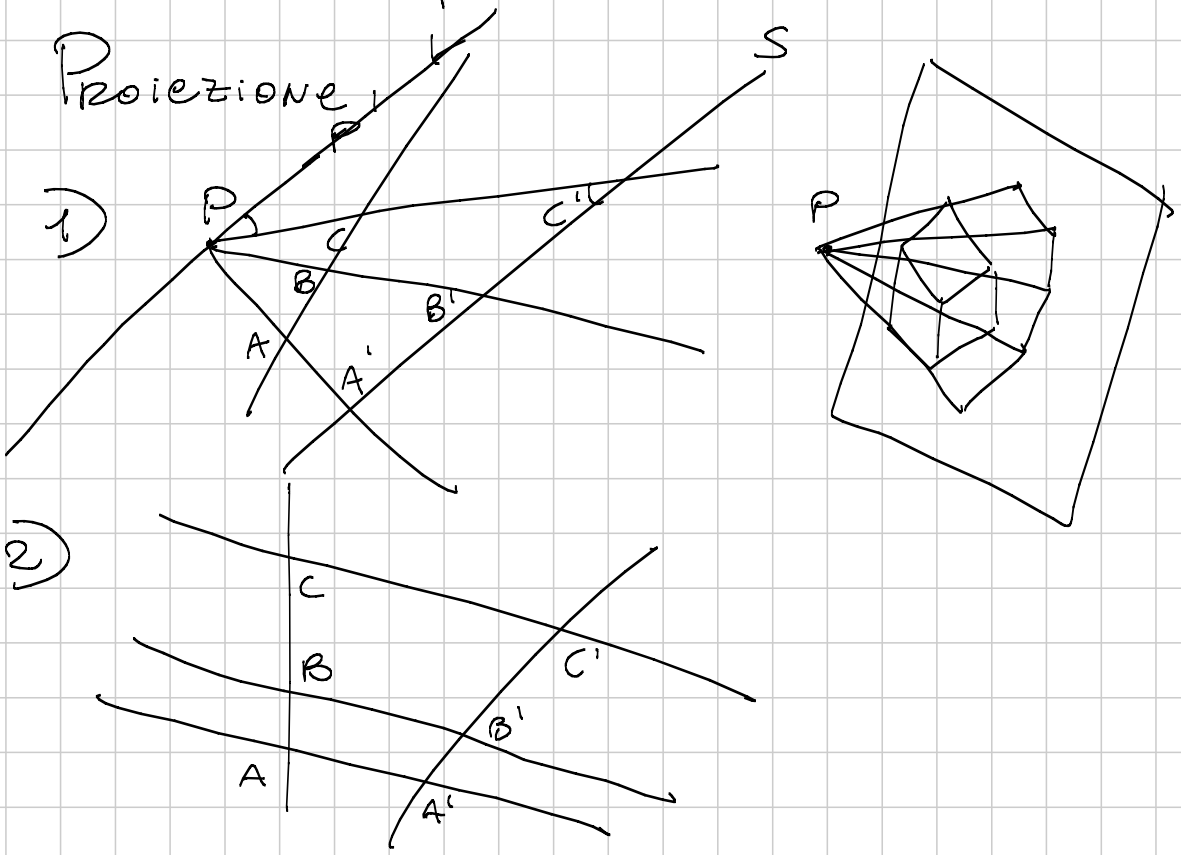
PIANO PROIETTIVO

=

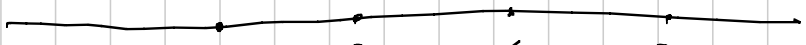
{PIANO EUCLIDEO} ∪ {Retta all'∞}

Ogni coppia di rette si incontra in uno e un solo punto.

PROIEZIONE

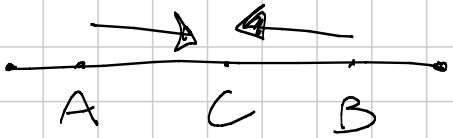


Birapporto



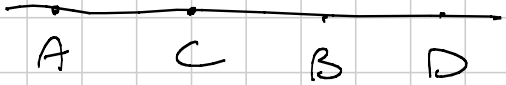
$$(A,B;C,D) = \frac{\frac{AC}{BC}}{\frac{AD}{BD}} = \frac{AC \cdot BD}{AD \cdot BC}$$

$(A,C;B,D)$



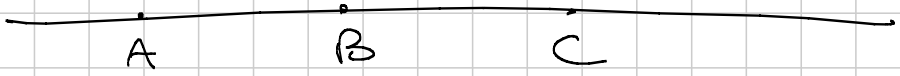
$\frac{AC}{BC}$

☆

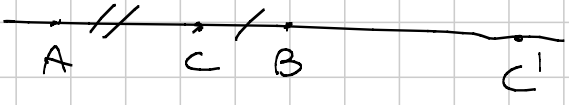


$(A,B;C,D) < 0$

$|(A,B;C,X)| = \lambda$



$$\frac{AC \cdot BX}{BC \cdot AX}$$



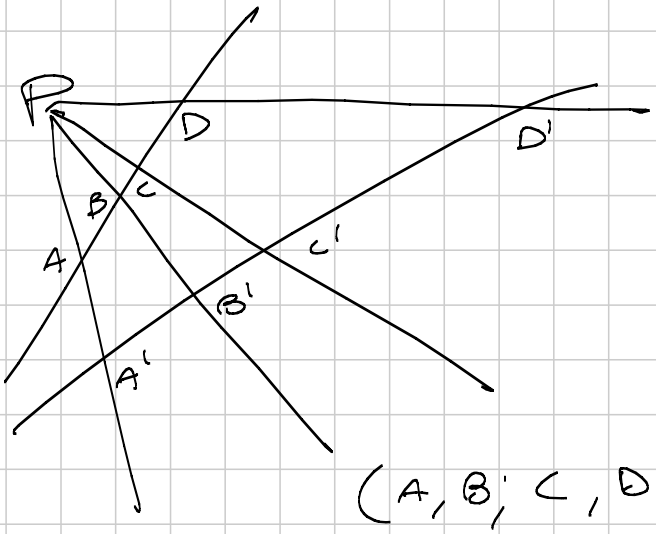
$f(X) = (A, B; C, X)$

$\{\text{retta proiettivo}\} \to \{\text{reali} + \infty\}$

$(A, B; C, X) = \dfrac{AC}{BC}$

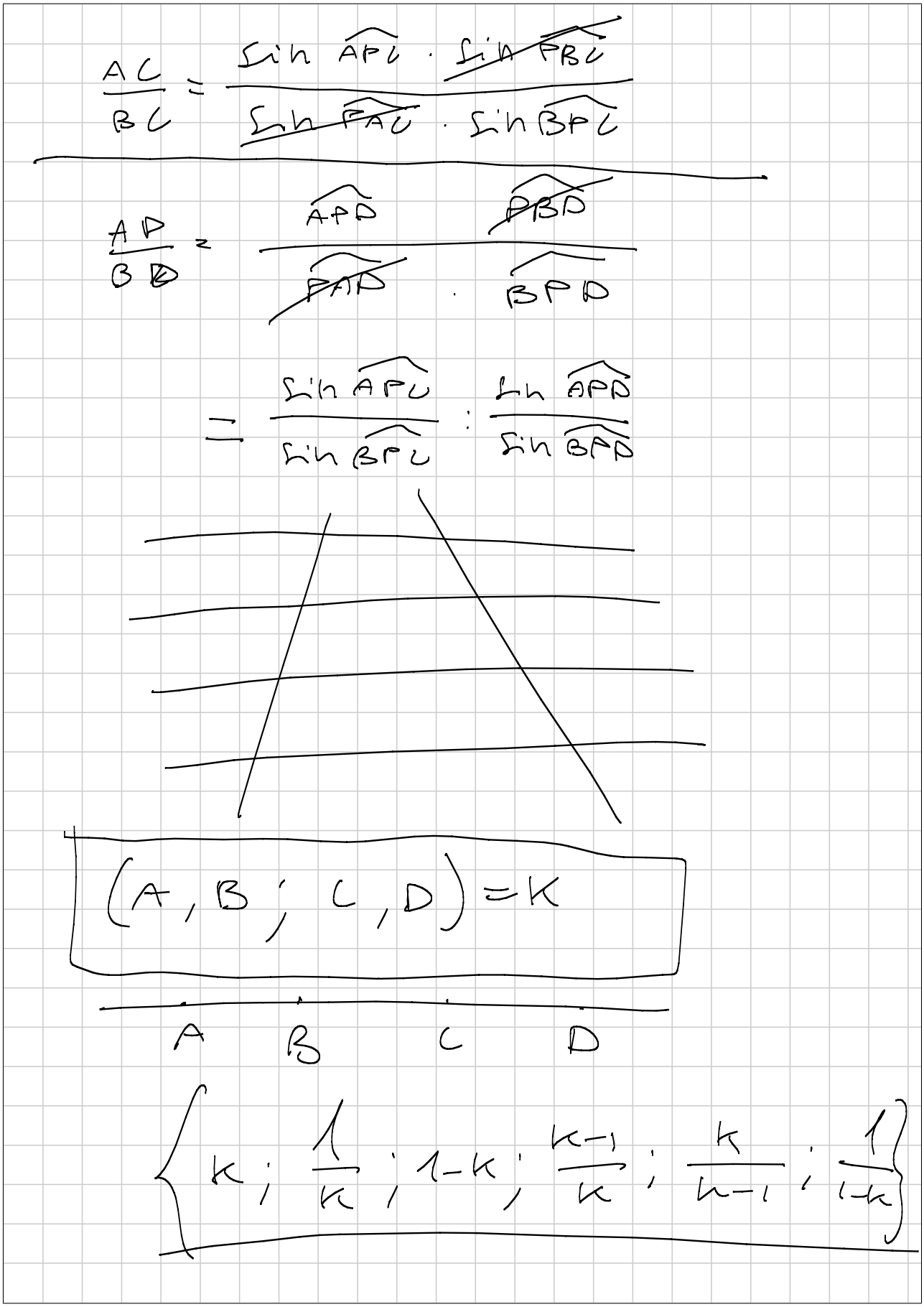
$(A, B; C, \infty) = \dfrac{AC \cdot \cancel{B\infty}}{BC \cdot \cancel{A\infty}}$

INVARIANZA PER PROIEZIONE



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

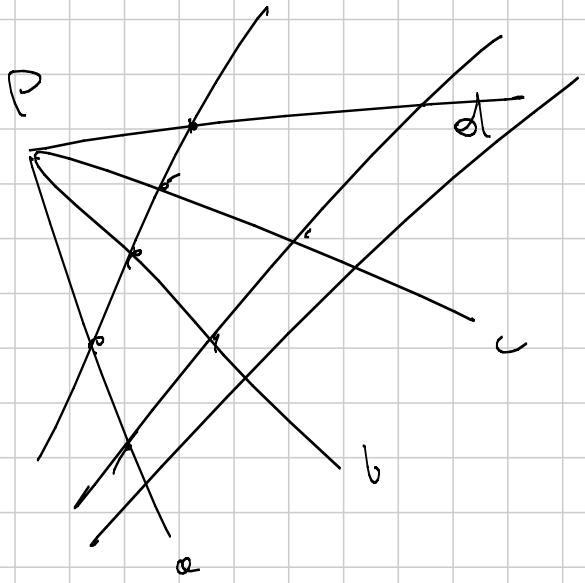
$AC = CP \dfrac{\sin \widehat{APC}}{\sin \widehat{PAC}} \qquad BC = CP \dfrac{\sin \widehat{BPC}}{\sin \widehat{PBC}}$


$\frac{AC}{BC} = \frac{\sin \widehat{APC} \cdot \sin \widehat{PBC}}{\sin \widehat{PAC} \cdot \sin \widehat{BPC}}$
$\frac{AD}{BD} = \frac{\widehat{APD}}{\widehat{PAD}} \cdot \frac{\widehat{PBD}}{\widehat{BPD}}$
$= \frac{\sin \widehat{APC}}{\sin \widehat{BPC}} : \frac{\sin \widehat{APD}}{\sin \widehat{BPD}}$
$(A, B; C, D) = k$
A
B
C
D
$\left\{ k; \frac{1}{k}; 1-k; \frac{k-1}{k}; \frac{k}{k-1}; \frac{1}{1-k} \right\}$

$$(A, B; C, D) = k$$

$$(B, A; C, D) = \frac{1}{k}$$

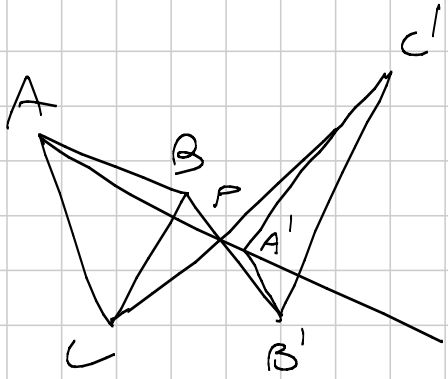
$$(A, B; D, C)$$



$$(a, b; c, d)$$

Il birapporto di 4 rette è il birapporto che si ottiene intersecando una retta qualunque con queste 4.

Teorema di Desargues

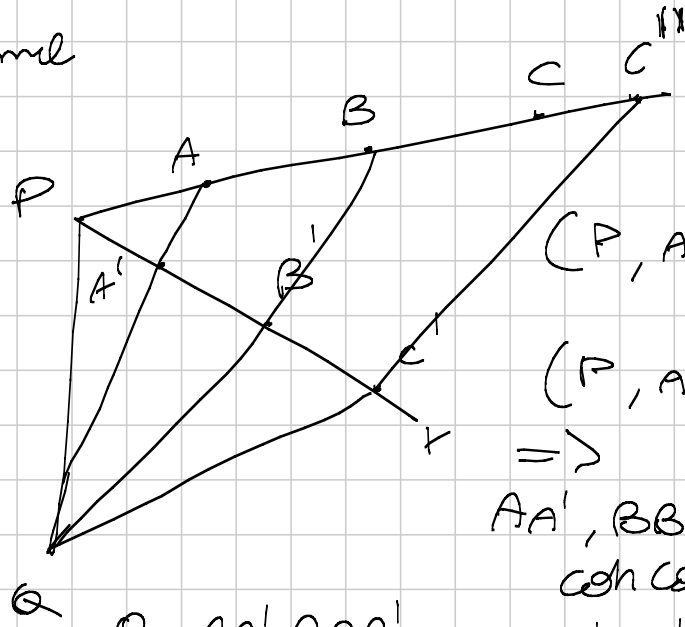


AA', BB', CC' concorrono in P

$\Longleftrightarrow$

$AB \cap A'B', \; BC \cap B'C', \; CA \cap C'A'$ sono allineati.

Lemma



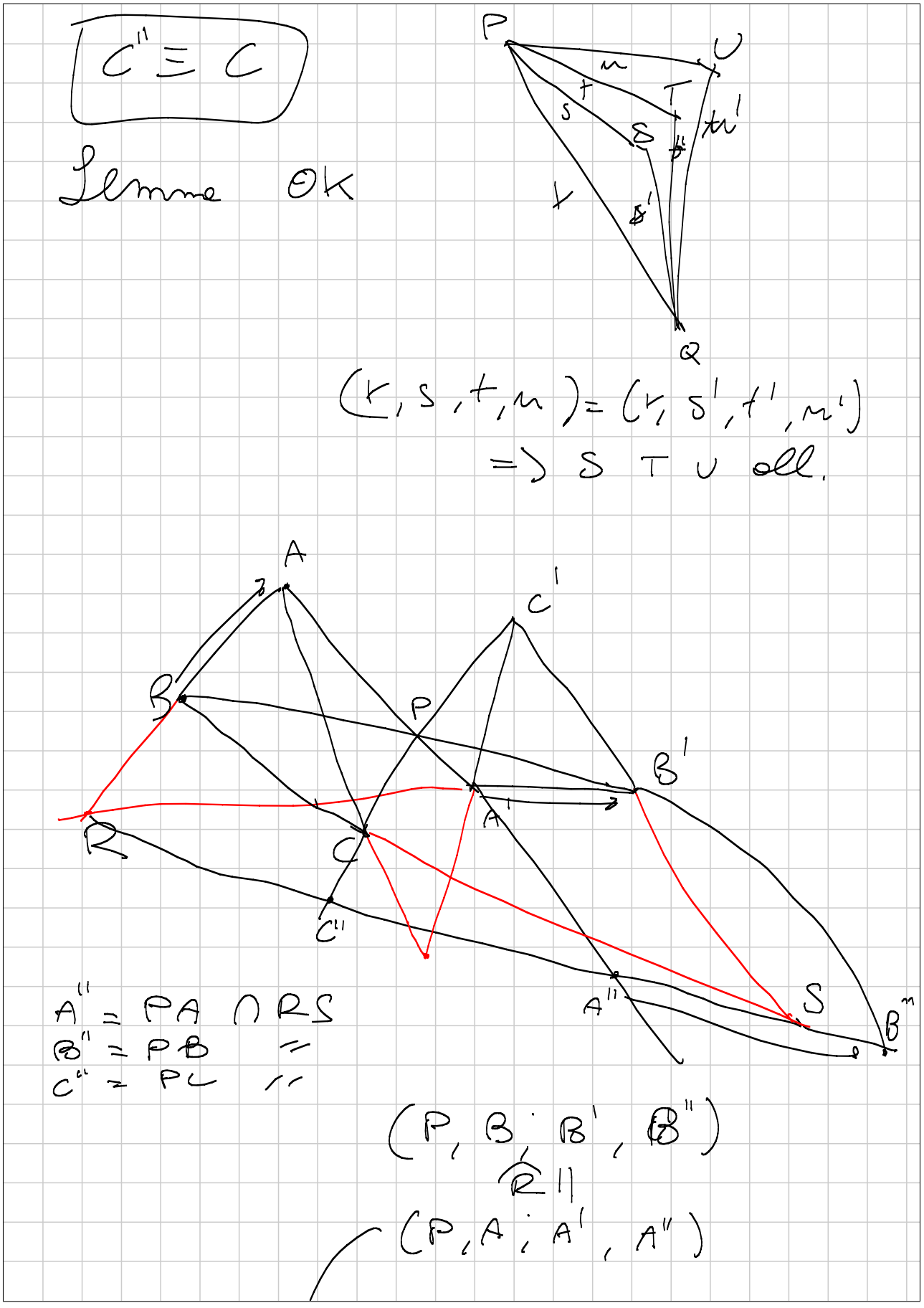
$(P, A', B, C) = (P, A', B', C')$

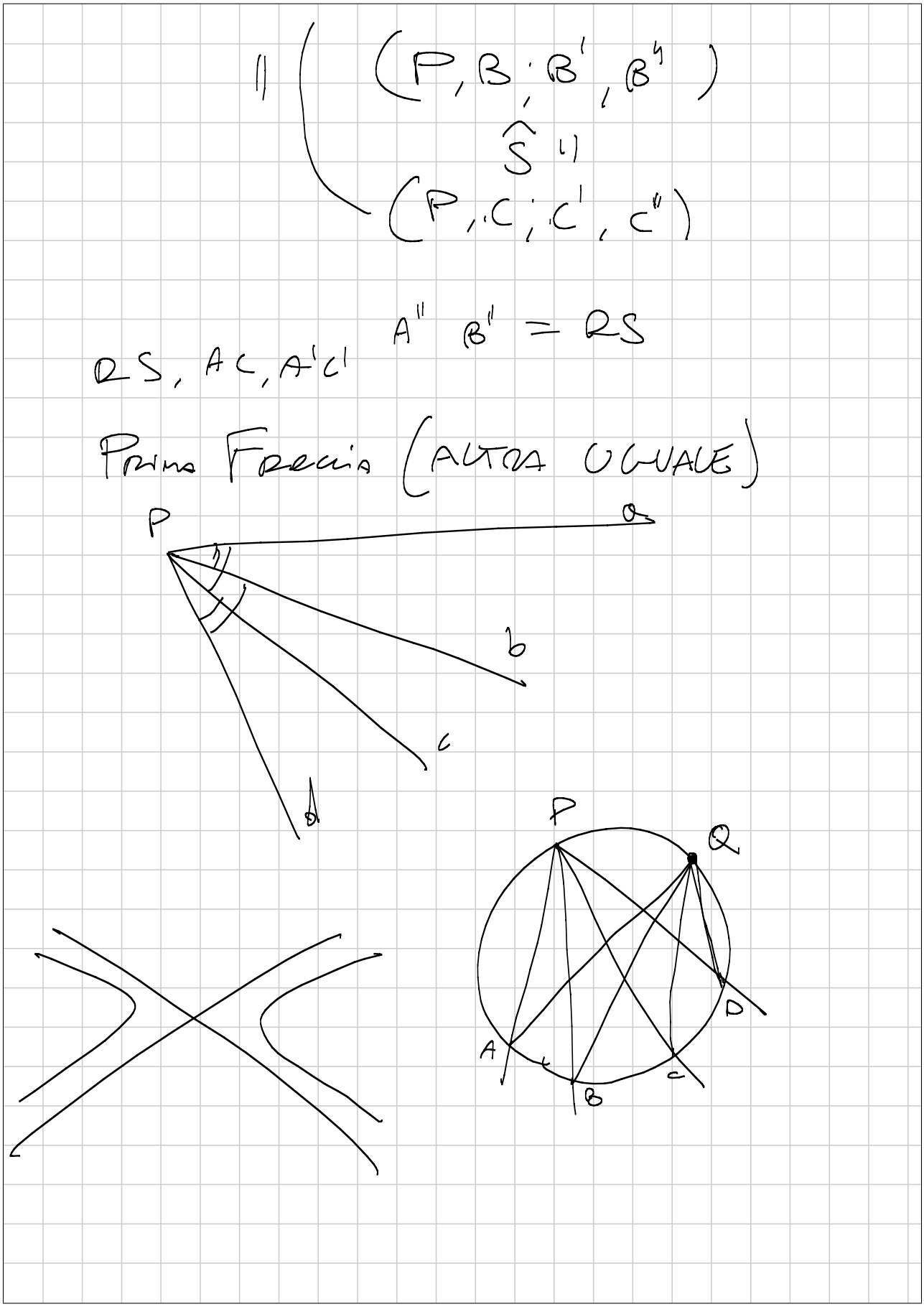
$\Rightarrow$

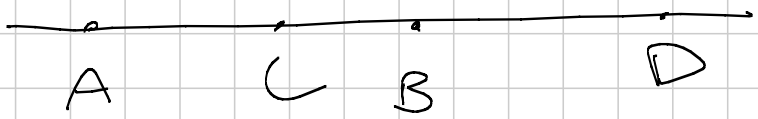
AA', BB', CC' concorrono

$Q = AA' \cap BB'$

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

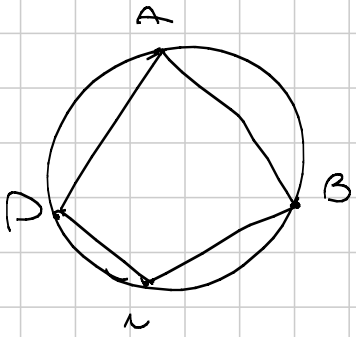

C'' ≡ C
Lemma OK
P
U
T
Q
(r, s, t, u) = (r, s', t', u')
⇒ S T U all.
A
B
C
C'
P
A'
B'
R
C''
A''
S
B''
A'' = PA ∩ RS
B'' = PB ∩
C'' = PC ∩
(P, B, B', B'')
R
(P, A, A', A'')


(P, B; B', B'')
Ŝ
(P, C; C', C'')
RS, AC, A'C'
A'' B'' = RS
PRIMA FREGIA (ALTRA UGUALE)
P
a
b
c
d
P
Q
A
B
C
D



$(A, B; C, D) = -1$

Quando la quaterna è su una circonferenza, il quadrilatero si dice armonico.

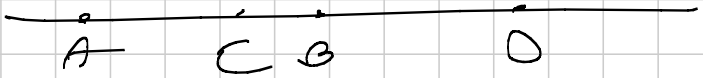


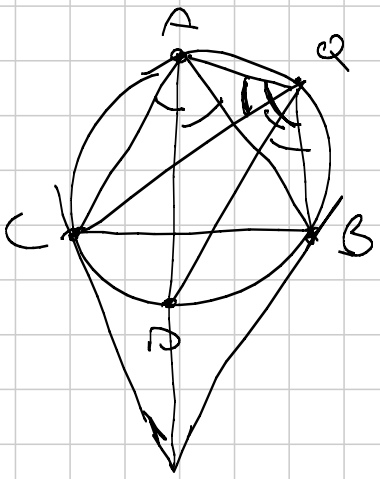
ABCD armonico

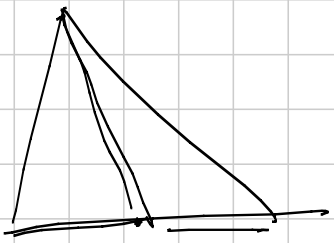
$\Leftrightarrow$

$AB \cdot CD = AD \cdot BC$

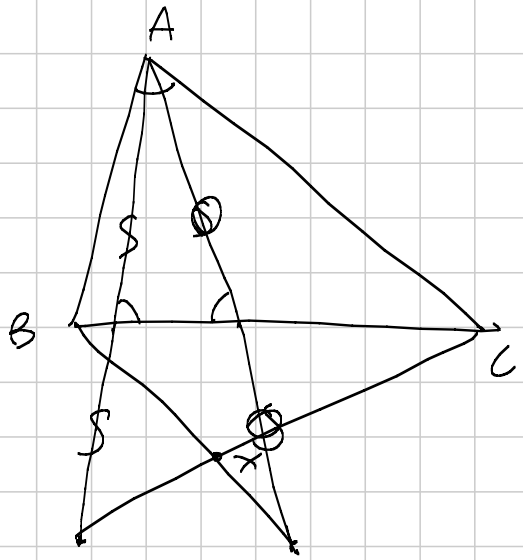
$(A, C; B, D) = \dfrac{AB \cdot CD}{CB \cdot AD} = -1$

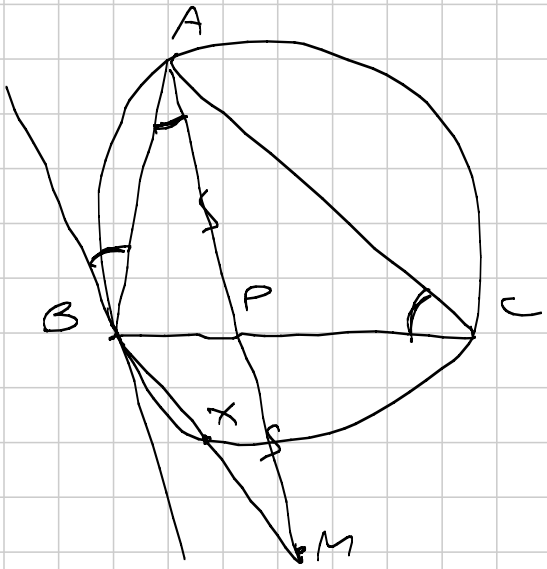






IMO-4 2014





$$(A, M; P, \infty) = \frac{AP \cdot M\infty}{MP \cdot A\infty} = -1$$

$\downarrow B$

$$(A, X; C, B) = -1$$

BM posso per sim ∩ ciclico

CN

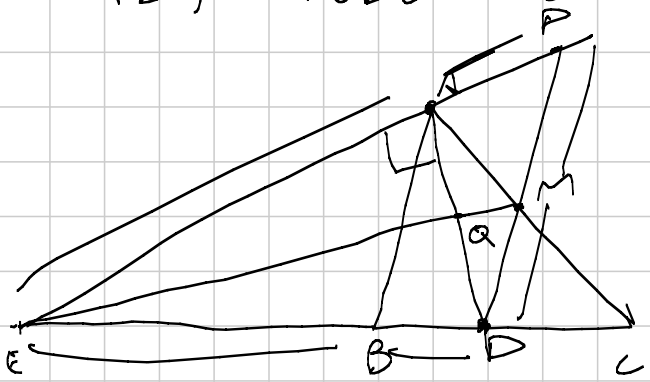
FINE

11

$(A\ M\ B\ \infty) = -1$

e limm.

TST TURCHIA 2009 – 1



PQ PASSA PER UN PUNTO FISSATO AL VARIARE DI P.

Teor. di Menelao in $\widehat{PED}$ a AC

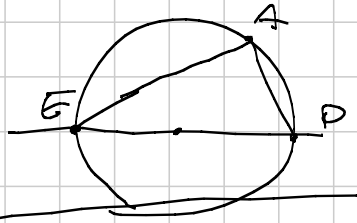
$$\frac{PA}{AE} \cdot \frac{EC}{CD} \cdot \frac{DM}{MP} = 1$$

$(C, B; D, E) = -1$

$$\frac{DB}{DC} = \frac{AB}{AC} \qquad \frac{AB}{AC} = \frac{AB}{AC} \qquad \frac{EB}{EC} = \frac{AB}{AC}$$

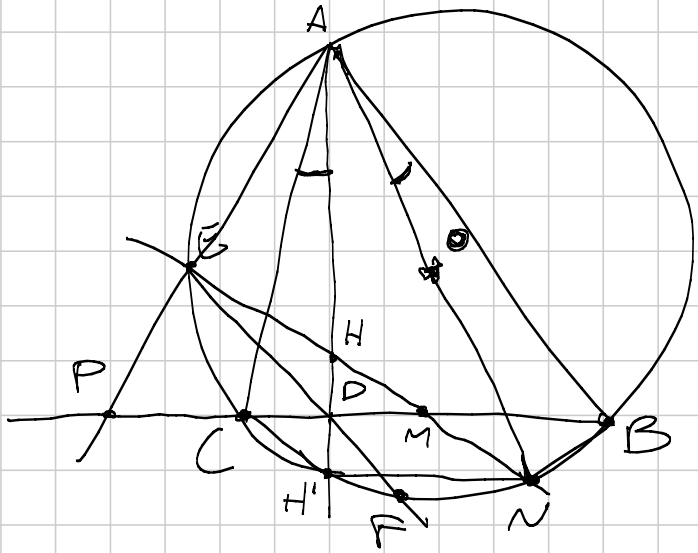
$$\frac{EC}{EB} = \frac{AC}{AB}$$

$$\frac{CD}{CE} = \frac{BD}{BE}$$



$$\frac{PA}{AE} \cdot \frac{BE}{BD} \cdot \frac{DM}{MP} = 1$$

P, Q, B allineati



$\frac{BF}{FC} = \frac{AB}{AC}$

$H'N \parallel BC$

$(NH', NM, NB, NC) = -1$

$\infty \quad M \quad B \quad C$

$\downarrow \hat{N}$

(H', E, B, C)

$\downarrow \hat{A}$

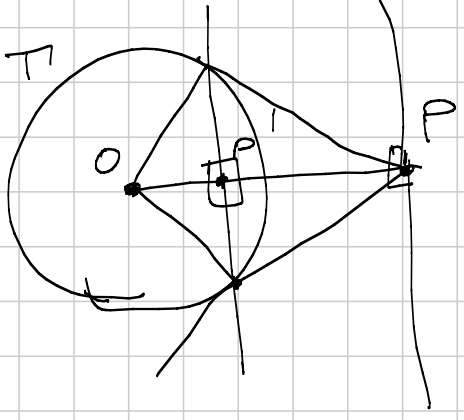
(D, P, B, C)

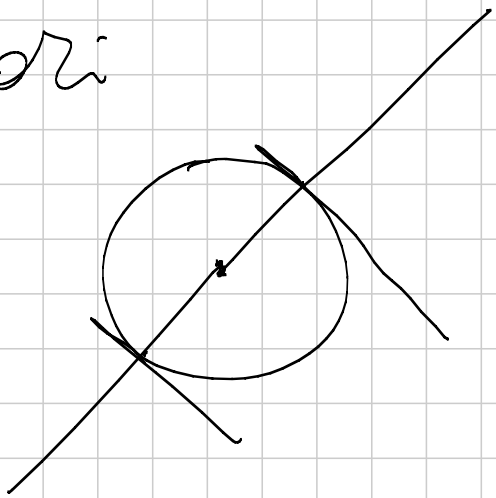
$\downarrow \hat{E}$

$(F, A, B, C) = -1$

FINE!

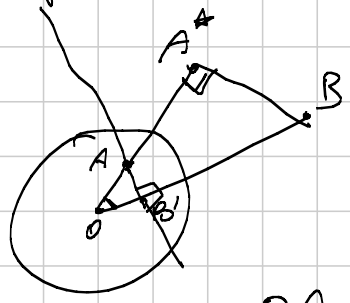
Poli e Polari





Teorema di La Hire

$A \in pol(B) \iff B \in pol(A)$

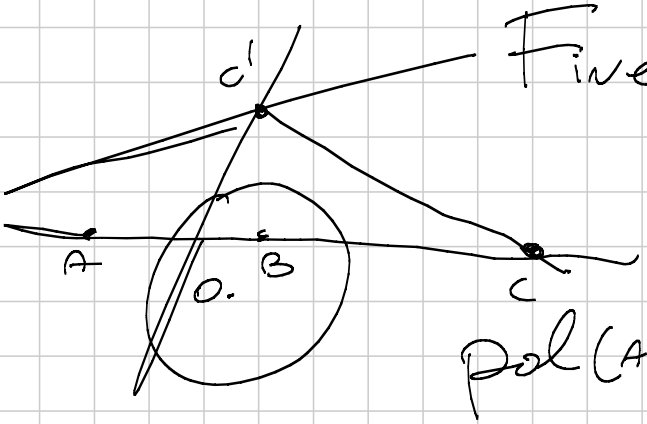


$OB'A$

OA^*BB

$OA \cdot OA^* = OB' \cdot OB$

Fine

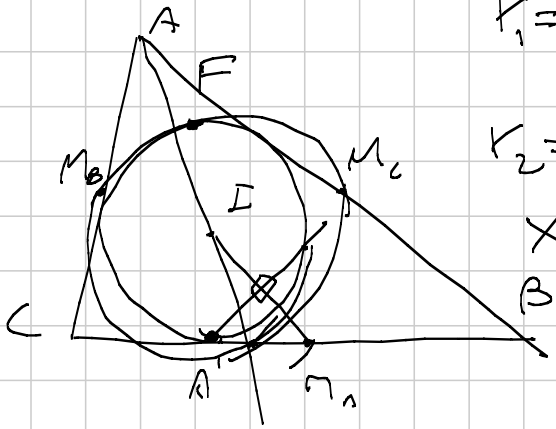


$c' = pol(A) \cap pol(B)$

$pol(A) \cap pol(B) = pol(AB)$

3 punti: all $\iff$ polari concorrono

WC-2010 6



r_1 = sim di BC rispetto ad AI

r_2 = $\perp$ da A_1 a M_AI

$X_A = r_1 \cap r_2$

X_B X_C

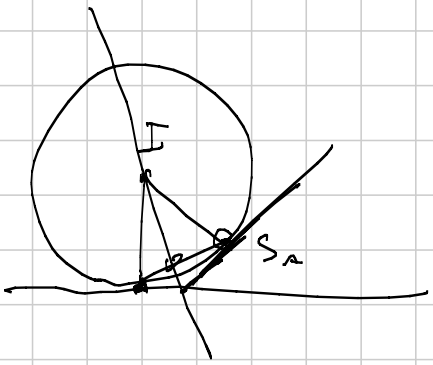
Ts: X_A, X_B, X_L allineati

Tesi + forte: allineati su cerchio tang. all'inscritta.

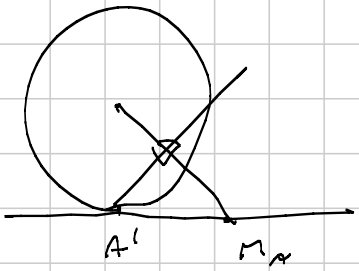
$\Leftrightarrow$ pol(X_2) ...
concorrono sull'inscritta

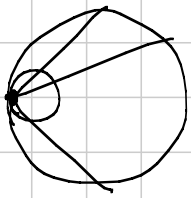
$X_A = \Gamma_1 \cap \Gamma_2$

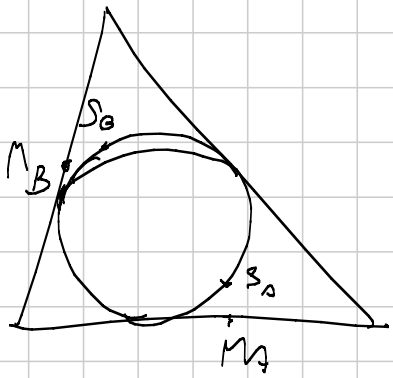
$pol(X_A) = \overline{pol(\Gamma_1) + pol(\Gamma_2)}$



$M_A S_A$ concorrono sull'INSCR.







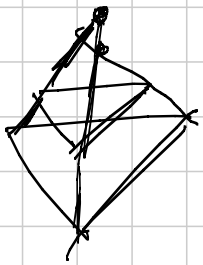
$M_A M_B M_C$

$S_A S_B S_C$

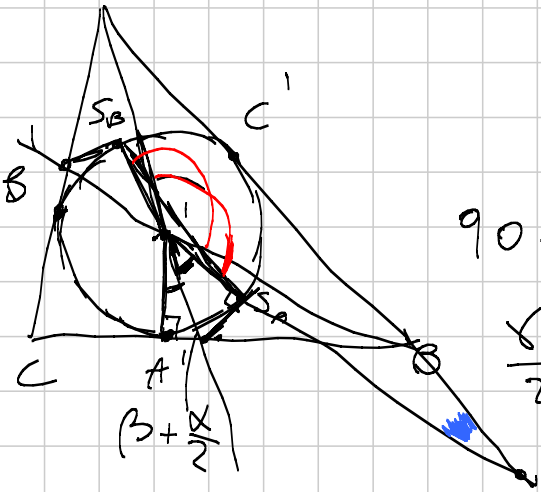
ABC $A_1B_1C_1$

AA_1 BB_1 CC_1

$S_A S_B // M_A M_B // AB$



A



$90 - \beta - \frac{\alpha}{2}$

$\frac{\gamma}{2} = \frac{\beta}{2}$

$K\hat{I}A = \pi + \pi + \frac{\alpha}{2} = \pi$ $\pi - \frac{\gamma}{2} + \frac{\beta}{2}$

$+$

$\cancel{\pi} - \frac{\gamma}{2} + \frac{\alpha}{2}$

$+$

$\cancel{\pi} + \frac{\beta}{2} + \frac{\alpha}{2}$

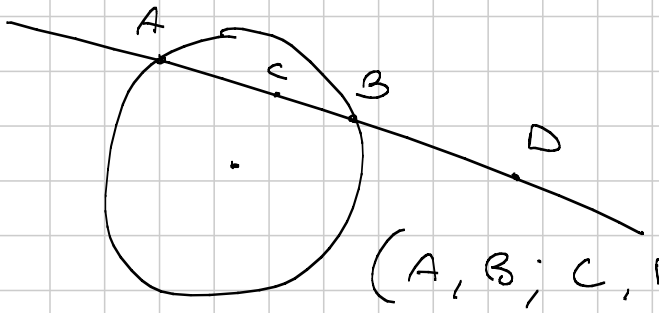
$\pi - \gamma + \alpha + \beta$

$2 \quad 2 \quad 2$

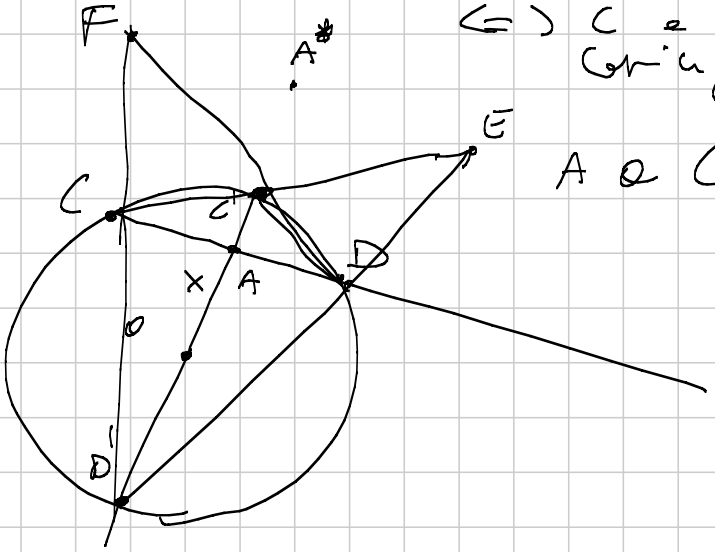
$\frac{\pi - 2\alpha - 2\beta}{2}$

$\frac{\pi}{2} - \alpha - \beta$

Lemma della Polare



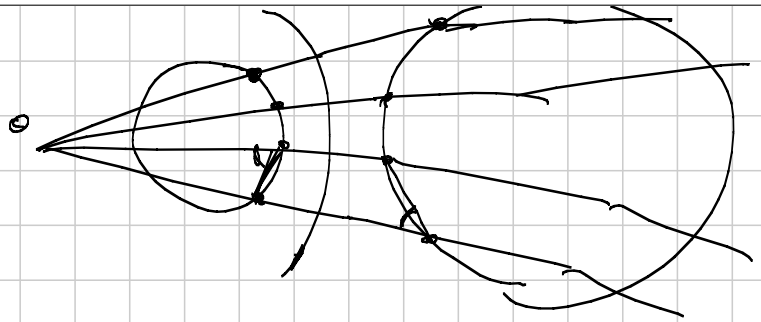
$(A, B; C, D) \Leftrightarrow C$ e D coniugati



A CASO

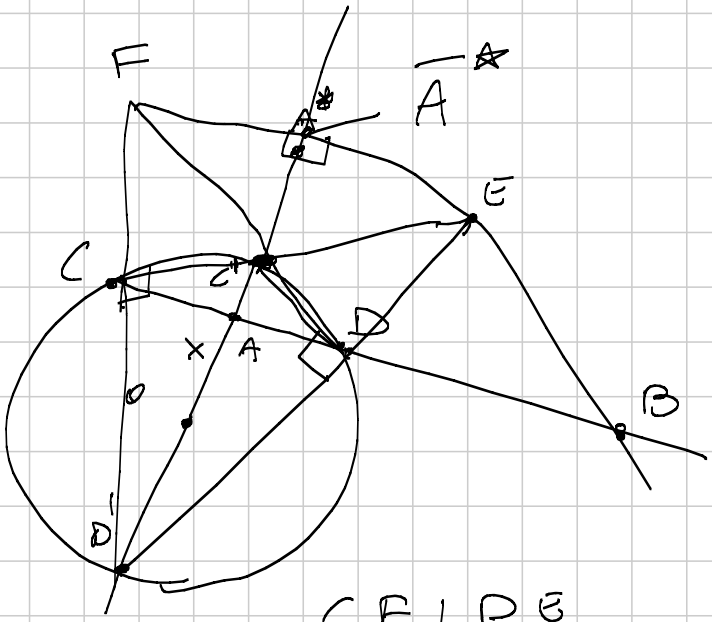
$(C', D'; A, A^*) = -1$

$OA^* = \frac{R'^2}{OA}$ $\quad C'D' = 2R$



$$(C_1, D_1; A, A^*) = k = -1$$

$$= (C_1, D_1; A^*, A) = \frac{1}{k}$$



$$C_1F \perp D_1E$$

$$B = EF \cap CD$$

$$(C_1, D_1, A, \overline{A}^*) \overset{E}{=} (C, D; A, B) \overset{F}{=} (D_1, C_1, A, \overline{A}^*)$$

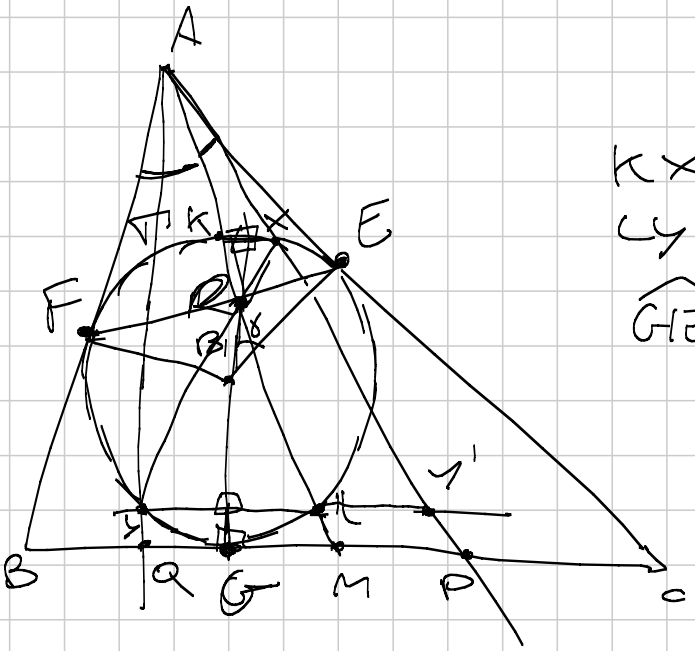
$(C_1, D_1, A, \bar{A}^{\star}) = -1$

$(C_1, D_1, A, A^{\star}) = -1$

$\bar{A}^{\star} \equiv A^{\star}$ $(C, D; A, B) = -1$

FINE

G6 – 2005



$KX \parallel BC$

$LY \parallel BC$

$\widehat{GE} = \overline{\Pi - \gamma}$

$BQ = CP$ $(BM = MC)$

$QM = MP$

$YL = LY'$

$\frac{LY}{KX} = \frac{RL}{RK}$

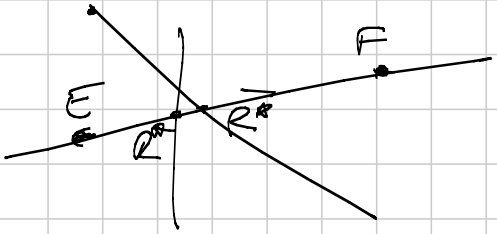
$\frac{LY'}{KX} = \frac{AL}{AK}$

$\frac{RL}{RK} = \frac{AL}{AK} \Leftrightarrow (A, R; K, L) = -1$

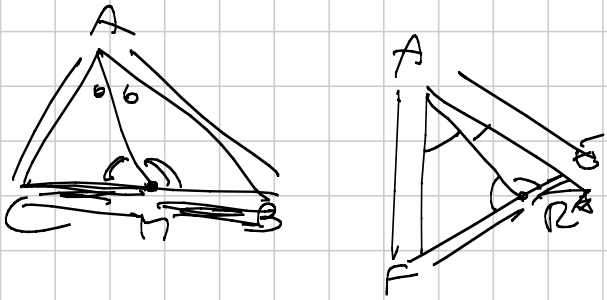
$\Leftrightarrow E, R, F$ allineati

$R^* \quad \overline{R}^*$

$\hookrightarrow GI \cap EF \rightarrow AM \cap EF$



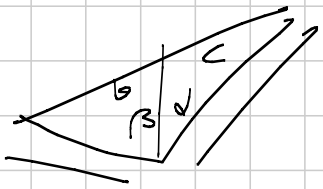
$$\frac{ER^*}{R^*F} = \frac{E\overline{R}^*}{\overline{R}^*R}$$



$$\frac{\sin \widehat{FAR^*}}{\sin \widehat{R^*AB}} = \frac{b}{c}$$

$$\frac{AF}{\sin R^*} = \frac{FR}{\sin FAR} \qquad \frac{AE}{R^*} = \frac{\overline{R}^*R}{}$$

$$\frac{FR^*}{R^*E} = \frac{b}{c}$$



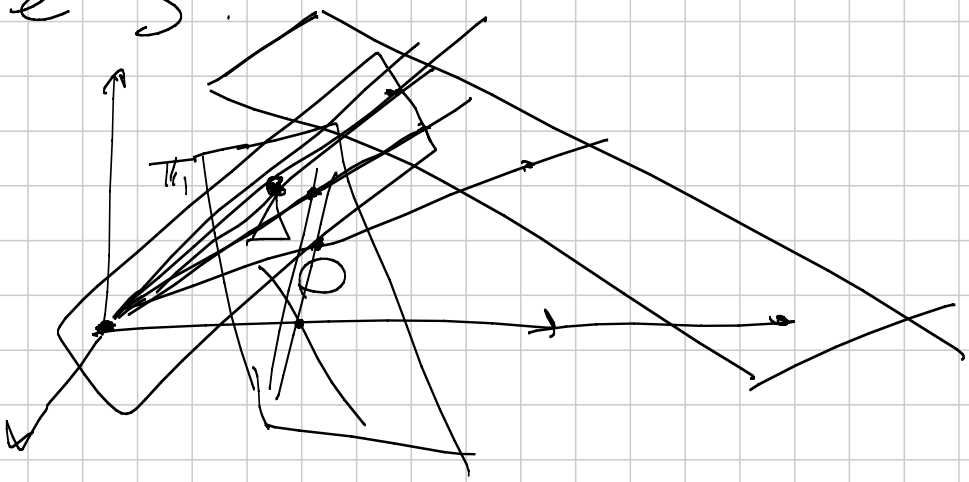
$$\frac{FR^*}{R^*E} = \frac{b}{c} = \frac{F\bar{R}^*}{\bar{R}^*E}$$

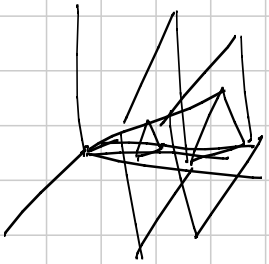
$$\bar{R}^* \equiv R^*$$

$\Rightarrow$ EF, GI, AM Concorrono.

FINE

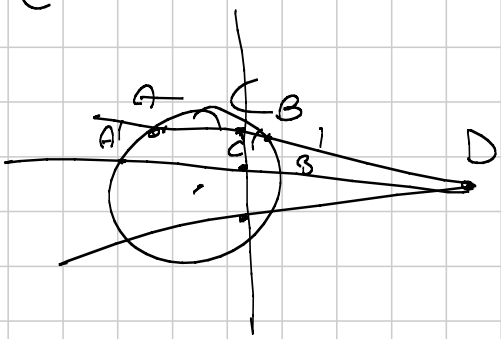
PARTE 3:





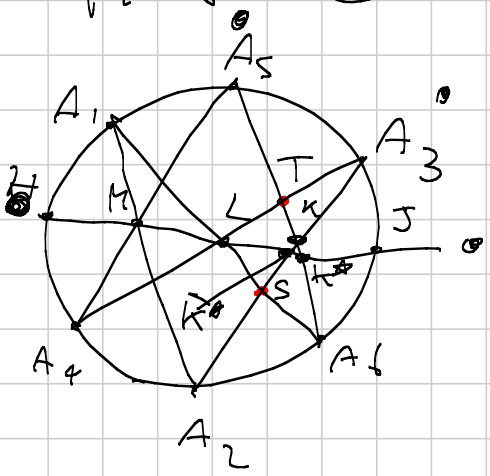
SARA

La Proiettività manda coniche in coniche



Teorema di Pascal

$A_1A_2 \cap A_4A_5$
$A_2A_3 \cap A_5A_6$
$A_3A_4 \cap A_6A_1$
Sono allineati



$(H, M; L, J) \overset{\hat{A}_4}{=} (H, A_5; A_3, J)$

$\overset{\hat{T}}{=} (H, K^*; L, J)$

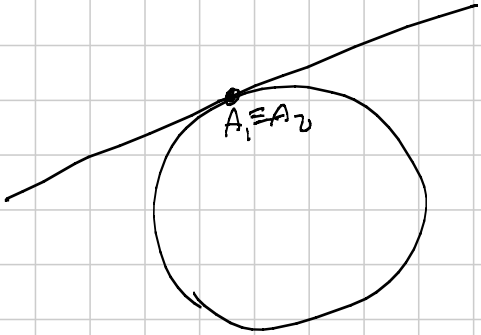
$(H, M; L, J) \overset{\hat{A}_1}{=} (H, A_2; A_6, J)$

$\hat{S} \cong (\mathbb{H}, \vec{k}, i, L, J)$

$\vec{k}^* \equiv k^*$

$\vec{h}^* \equiv K^*$

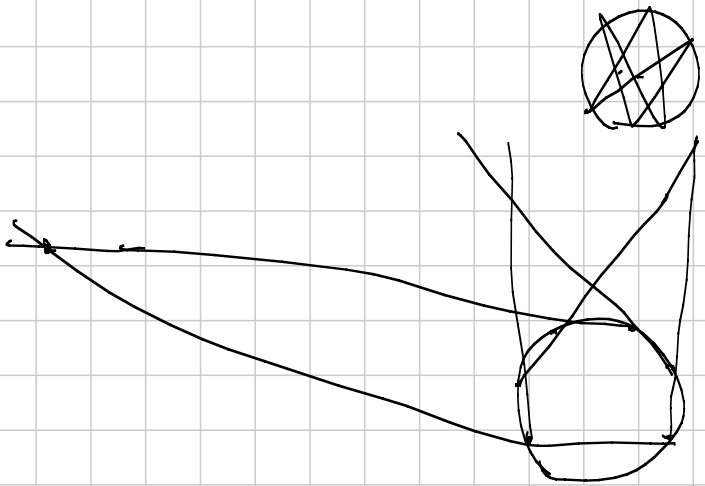
FINE



$A_1A_2 \cap A_4A_5$

120 modi di ordinare i punti

$\Rightarrow$ 120 allineati

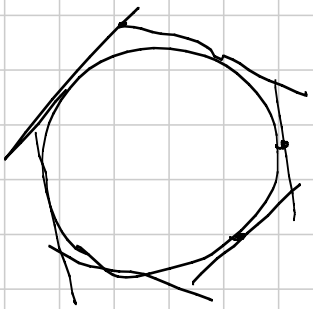


Teorema di Poppo

≡ Pascal, con coppie di rette.

⇒ una proiettività che manda una circonferenza in una coppia di rette qualunque.

Teorema di BRIANCHON



r_1 r_2 r_3 r_4 r_5 r_6

$A_1 = r_1 \cap r_2$ $A_2 = r_4 \cap r_5$ R_1

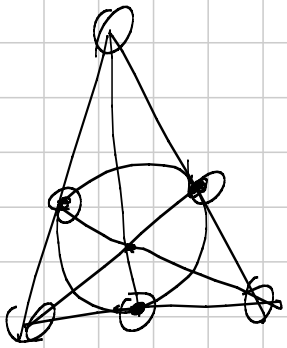
$r_2 \cap r_3$ $r_5 \cap r_6$ R_2

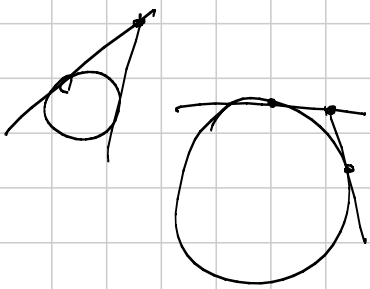
$r_3 \cap r_4$ $r_6 \cap r_1$ R_3

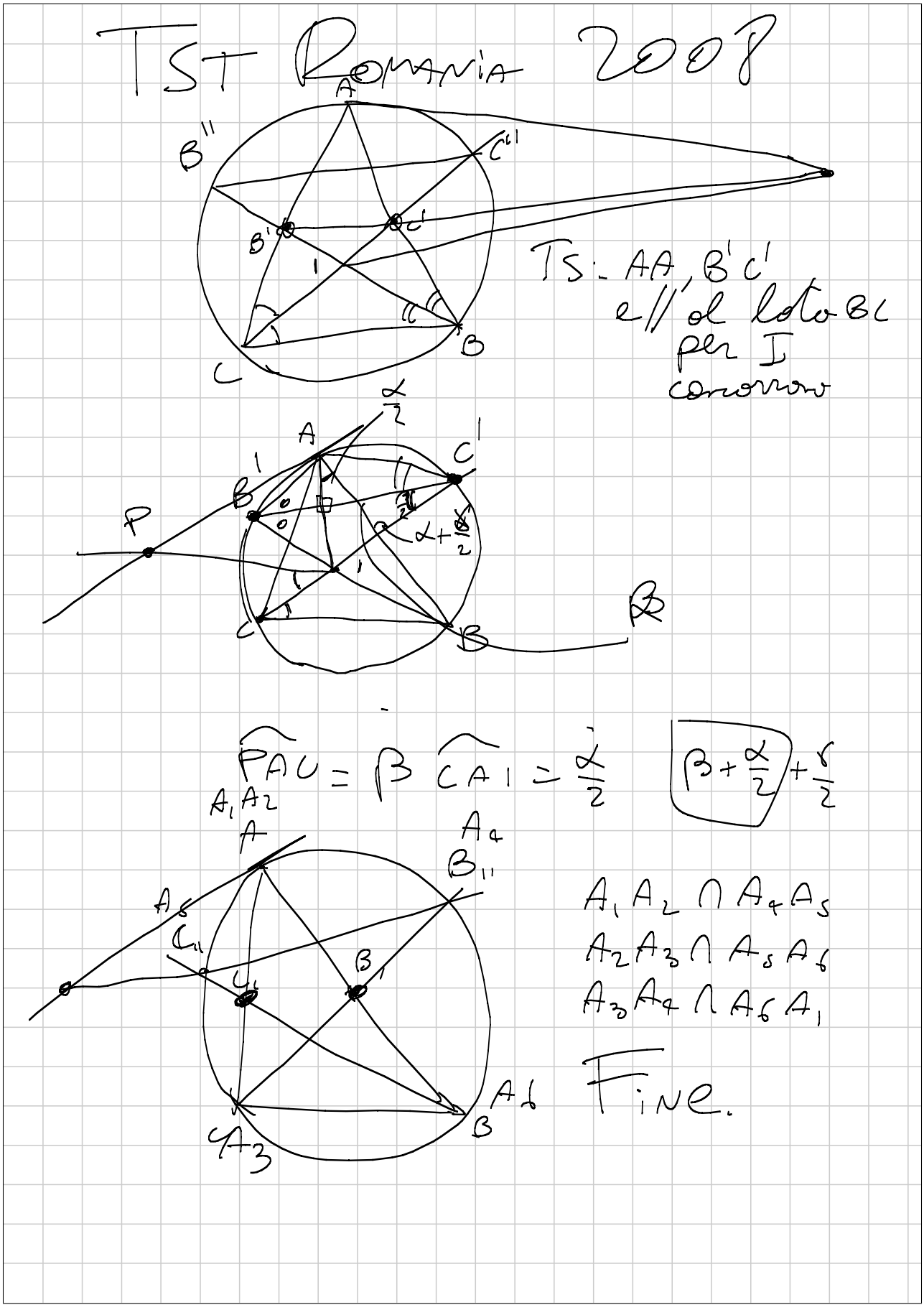
R_1 R_2 R_3

Concorrono

Dim: Pascal + polari di ogni cosa.



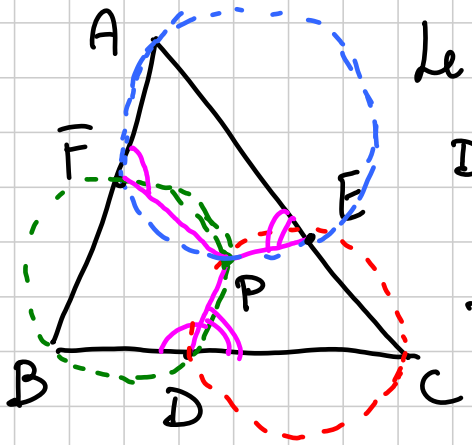



TST ROMANIA 2008
TS - AA', B'C' e // al lato BC per I conorro
P
R
$\widehat{PAU} = \beta \widehat{CA_1} = \frac{\alpha}{2}$
$\beta + \frac{\alpha}{2} + \frac{\gamma}{2}$
$A_1A_2 \cap A_4A_5$
$A_2A_3 \cap A_5A_6$
$A_3A_4 \cap A_6A_1$
FINE.

G3 medium – Same

Titolo nota 05/09/2014

Teorema (Miquel)



Le circonf. circo ai Triangoli $\triangle DCE$, $\triangle EAF$, $\triangle FBD$ hanno un punto in comune.

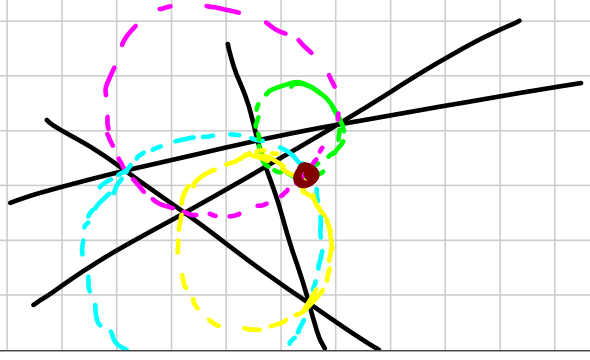
Dim: P = intersez. delle cfr. verde e rossa diversa da D

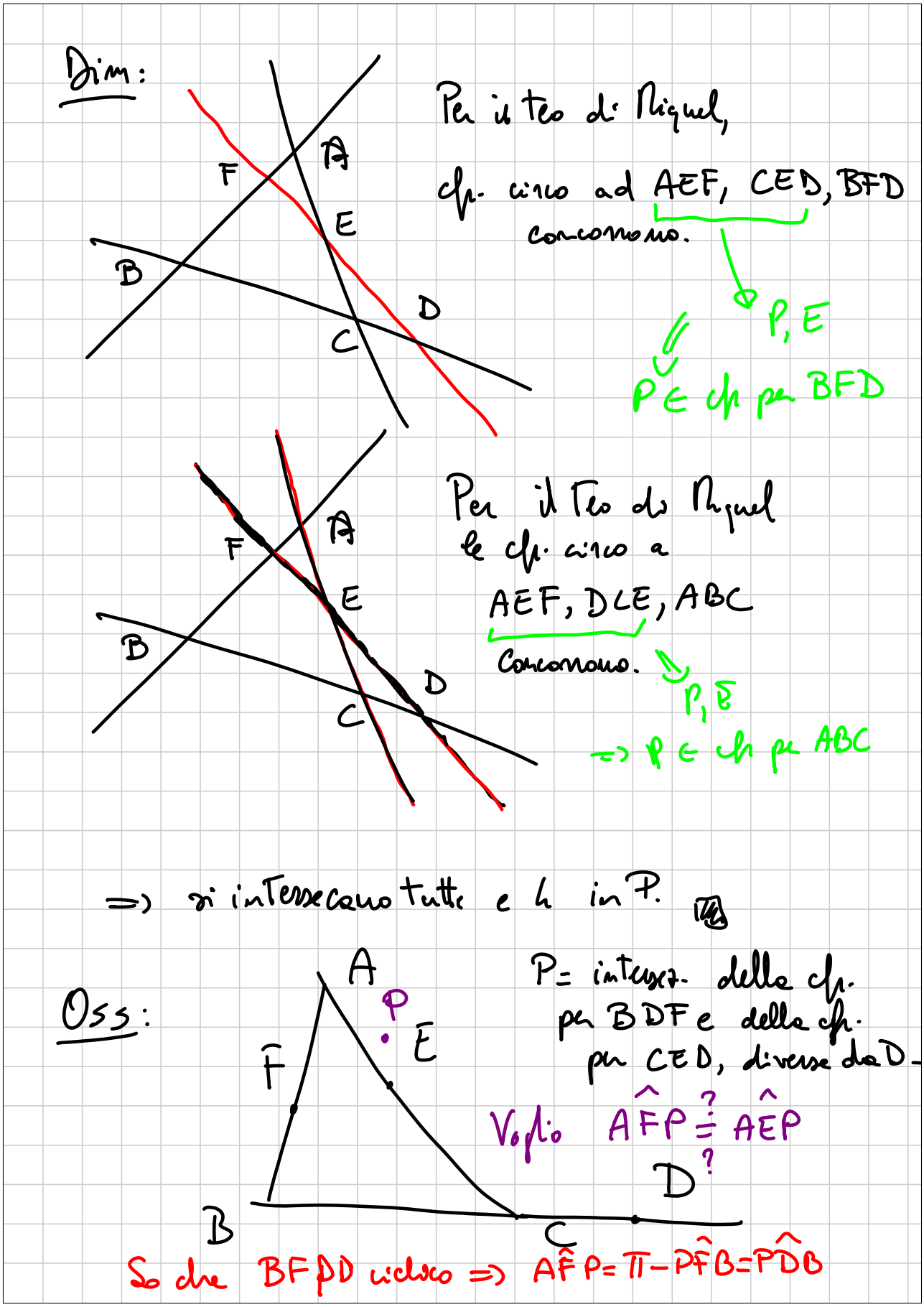
Voglio dim che $AFPE$ è ciclico

$\widehat{AFP} = \widehat{PDB}$ $\widehat{PEA} = \widehat{PDC}$ $\Rightarrow$ finito. ∎

Teo (Mquel) 4 rette a 3 a 3 non concorrenti r_1, r_2, r_3, r_4. Sia Γ_i la circonf. circo. al Tw formato dalle rette $r_j r_k r_h$ con $\{i,j,k,h\} = \{1,2,3,4\}$

Allora $\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4$ hanno un punto in comune




Dim:
A
F
E
B
D
C
Per il teo di Miquel,
ch. circo ad AEF, CED, BFD
concorrono.
P, E
P ∈ ch per BFD
Per il Teo di Miquel
le ch. circo a
AEF, DCE, ABC
Concorrono.
P, E
⇒ P ∈ ch per ABC
⇒ si intersecano tutte e 4 in P.
Oss:
P = interseg. delle ch.
per BDF e della ch.
per CED, diverse da D.
Voglio AFP ≟ AEP
So che BFPD ciclico ⇒ AFP = π − PFB = PDB

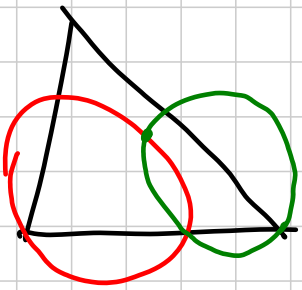
Se $DPEC$ ciclico $\Rightarrow A\hat{E}P = \pi - P\hat{E}C = P\hat{D}C$.

fine.

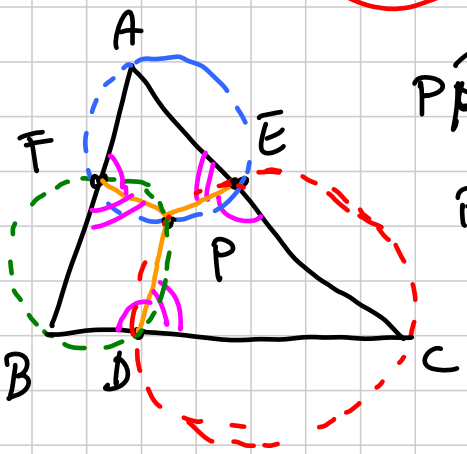
1. (STudiosa) STudiarsi gli angoli orientati.
2. (Scansafatiche) Dire "so che non è uguale, ma più o meno forma lo stesso, a patto di scambiare alcuni supplementari con congruenti".

INO 2013-4

INO 2011-6



Oss:



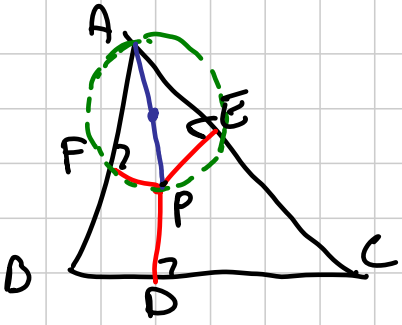
$P\hat{F}A = P\hat{D}B = P\hat{E}C$ (*)

$\Updownarrow$

$P\hat{F}B = P\hat{D}C = P\hat{E}A$ (**)

Viceversa: dato P, se trovo D, E, F t.c. valga (*) oppure (**) allora P è il punto di Miquel per D, E, F

Se: $P\hat{F}A = P\hat{D}B = P\hat{E}C = \frac{\pi}{2}$ triangolo pedale di P.

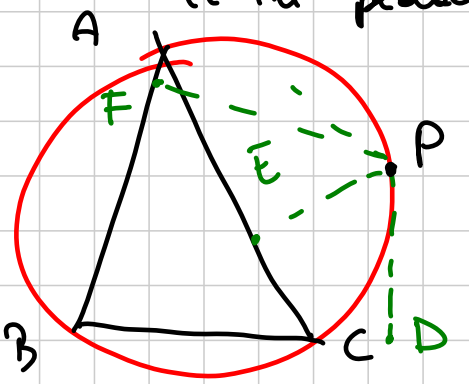


$EF = AP \cdot \sin\alpha = \frac{AP \cdot BC}{2R}$

$ED = \frac{CP \cdot AB}{2R}$ $\quad DF = \frac{BP \cdot AC}{2R}$

Teo di Tolomeo: $ABCD$ è ciclico (non intrecciato) se e solo se $AB \cdot CD + BC \cdot AD = AC \cdot BD$

Che succede se $P \in$ ch. circ. a ABC e ne faccio il tri pedale?



$P \in$ ch. per ABC

$\Leftrightarrow AP \cdot BC + PC \cdot AB = BP \cdot AC$

$\Downarrow$ (Tolomeo)

$2R(EF + ED) = 2R \cdot FD$

$\Downarrow$

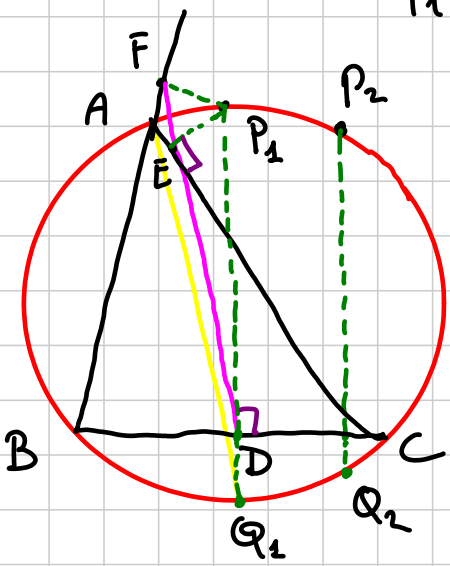
$EF + ED = FD$

$\Rightarrow F, E, D$ allineati

Teo (Simson): $P \in$ ch. circ. $\Rightarrow$ il tri pedale degenera in una retta (retta di Simson)

Proprietà 1: P_1, P_2 punti sulla ch., s_1, s_2 rette di Simson $\Rightarrow$ l'angolo tra s_1, s_2 è $\frac{1}{2} P_1 \hat{O} P_2$

Dim:

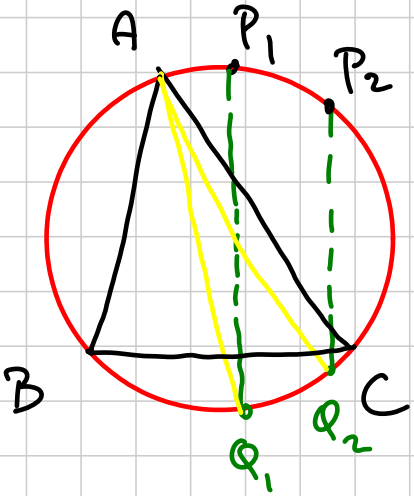


Il quadrilatero P_1EDC è ciclico

$$A\hat{Q}_1P_1 = A\hat{C}P_1 = E\hat{C}P_1 = E\hat{D}P_1$$

$\Rightarrow$ la retta di Simson di P_1 è parallela ad AQ_1.

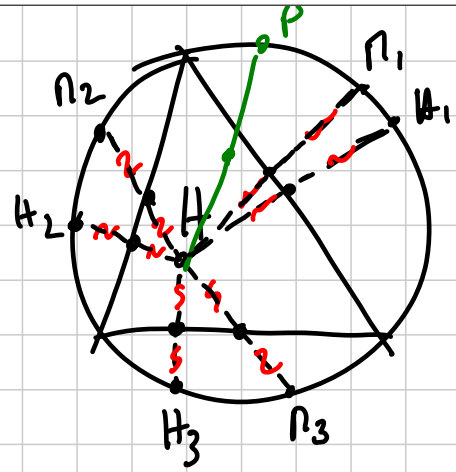
$\Rightarrow$ Se ora prendo P_2 e prolungo le $\perp$ da P_2 su BC fino alla ch. trovo Q_2 e ho che la retta di Simson di P_2 è parallela a AQ_2



$\Rightarrow$ l'angolo tra s_1 e s_2 è $Q_1\hat{A}Q_2 = \frac{1}{2}Q_1\hat{O}Q_2 = \frac{1}{2}P_1\hat{O}P_2$. $\square$

Proprietà 2: La retta di Simson di P passa per il punto medio di PH, H ortocentro.

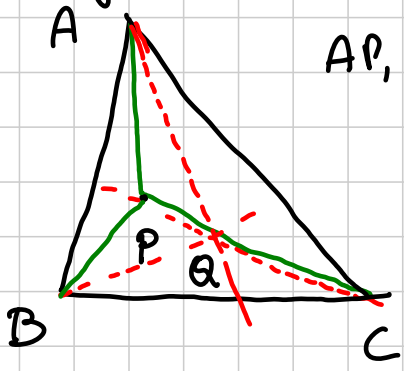
Proprietà 3: Il punto medio di PH sta sulla ch. di Feuerbach



$\Rightarrow$ omot. di centro H e fattore $\frac{1}{2}$ manda gli N_i nei pt. medi dei lati e gli H_i nei piedi delle altezze

Oss: I simm. di $P \in \odot$ circ. rispetto ai lati stanno su una retta $\parallel$ alla retta di Simson di P passante per H.

Coniugati isogonali



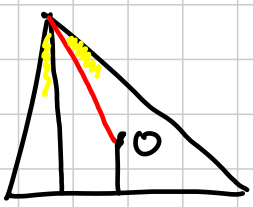
AP, BP, CP concorrono

$$\frac{\sin P\hat{A}B}{\sin P\hat{A}C} \cdot \frac{\sin P\hat{C}A}{\sin P\hat{C}B} \cdot \frac{\sin P\hat{B}C}{\sin P\hat{B}A} = 1$$

le simmediane concorrono (in Q)

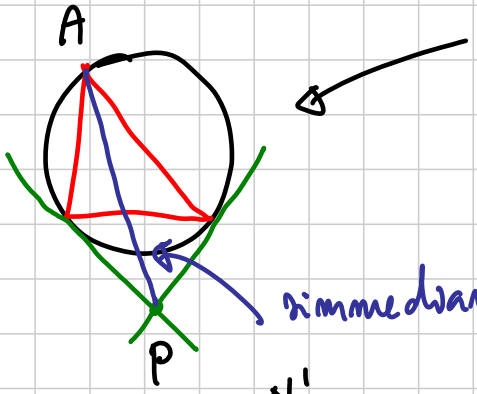
Q = coniugato isogonale di P.

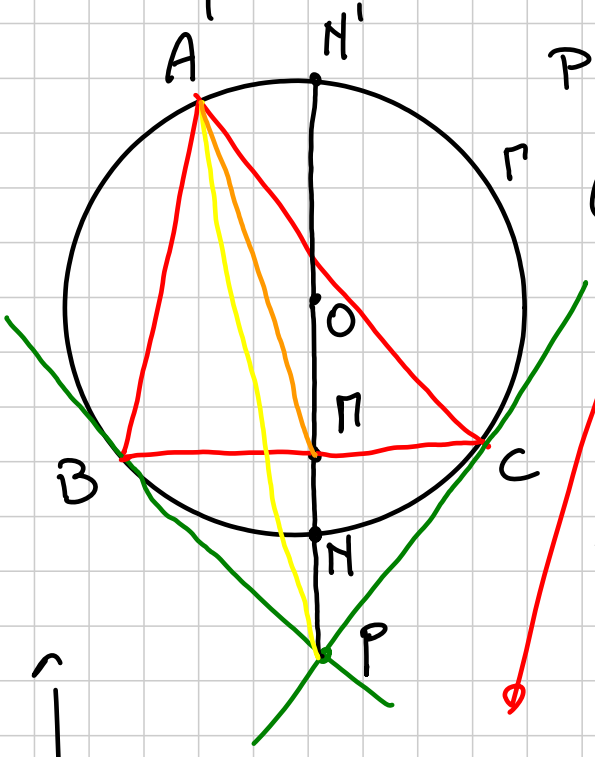
Es: Coniugato isogonale dell'incentro è l'incentro
" " dell'ortocentro è il circocentro



Coniugato isogonale del baricentro δ punto di Lemoine

= intersez. delle simmediane





$P = pol_\Gamma(BC)$

$(N', N, M, P) = -1$

$(AN', AN, A\Gamma, AP) = -1$

$(X, Y, Z, W) = \frac{XZ}{ZY} \Big/ \frac{XW}{WY} = \frac{XZ}{ZY} \cdot \frac{WY}{XW}$

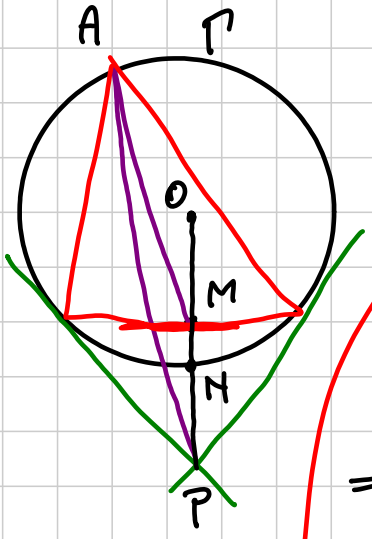
$\frac{\sin(N'AM)}{\sin(MAN)} \cdot \frac{\sin(PAN)}{\sin(N'AP)} = -1$

$\tg(N'\hat{A}M)\,(-\tg P\hat{A}N) = -1$

$\tg P\hat{A}N = \frac{1}{\tg N'AM} = \tg M\hat{A}N$

$\Rightarrow P\hat{A}N = M\hat{A}N$. □

2ª dim:

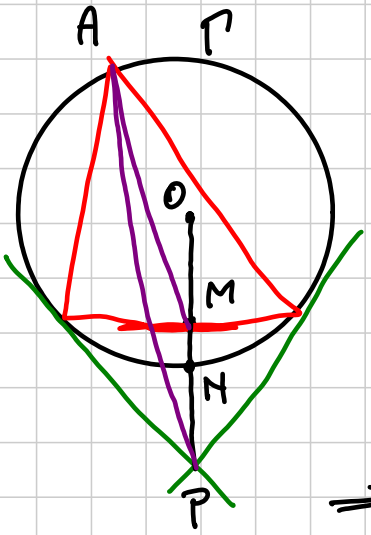


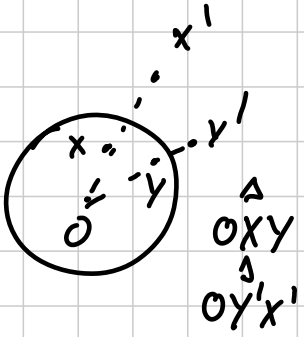
Π e P sono inversi rispetto a Γ

$OΠ \cdot OP = ON^2$

$$\frac{MN}{NP} = \frac{ON - OΠ}{OP - ON} = \frac{1 - \frac{OΠ}{ON}}{\frac{OP}{ON} - 1} = \frac{1 - x}{\frac{1}{x} - 1} = x$$

$$x = \frac{OΠ}{ON} = \frac{ON}{OP}$$





$\frac{AΠ}{AP}$

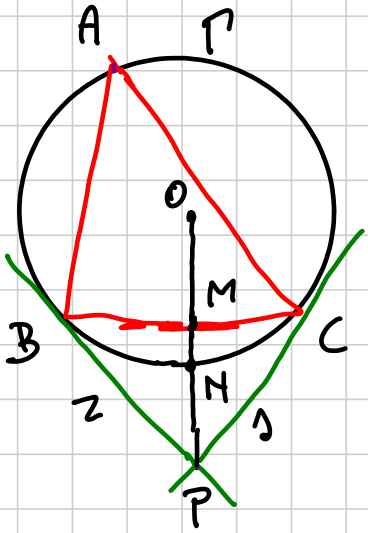
$\triangle OΠA$ e $\triangle OAP$ sono simili

$$\Rightarrow \frac{AΠ}{AP} = \frac{OA}{OP} = \frac{ON}{OP} = \frac{OΠ}{ON} = x.$$

$\Rightarrow$ per il teo della bisett. $\left(\frac{MN}{NP} = \frac{AΠ}{AP}\right)$

ho che AN bisecа $\widehat{PAΠ}$. □

3ª dim: Applico una inversione di centro A e raggio $r = \sqrt{BA \cdot CA}$ seguita da una simmetria rispetto alla bisettrice di $\widehat{BAC}$.



$B \longrightarrow C$

$C \longrightarrow B$

$\Gamma \longrightarrow BC$

$BC \longrightarrow \Gamma$

$= \omega_1$

$\alpha \longrightarrow$ circonf. per A tg. a BC in C

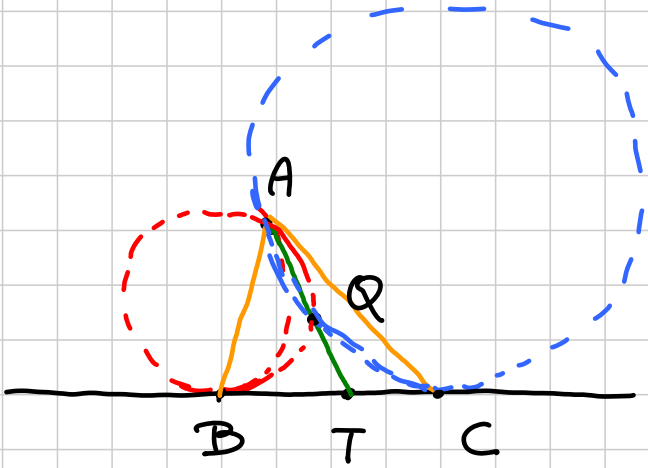
$\Delta \longrightarrow$ " " tg BC in B

$= \omega_2$

$P \longrightarrow$ ulteriore intersez. di ω_1 e ω_2

$= Q$

$AP \longrightarrow AQ$ = simm. di AP risp. alla bisett. di $B\hat{A}C$



AQ = asse radicale di ω_1 e ω_2

$\Downarrow$

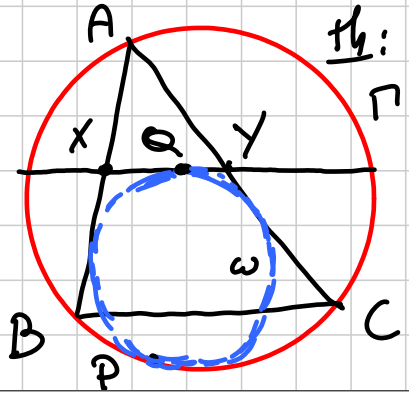
$BT^2 = TC^2$

$\Downarrow$

$BT = TC$

$\Rightarrow AT$ è mediana di $\triangle ABC$. ∎

EGMO 2013 - 5



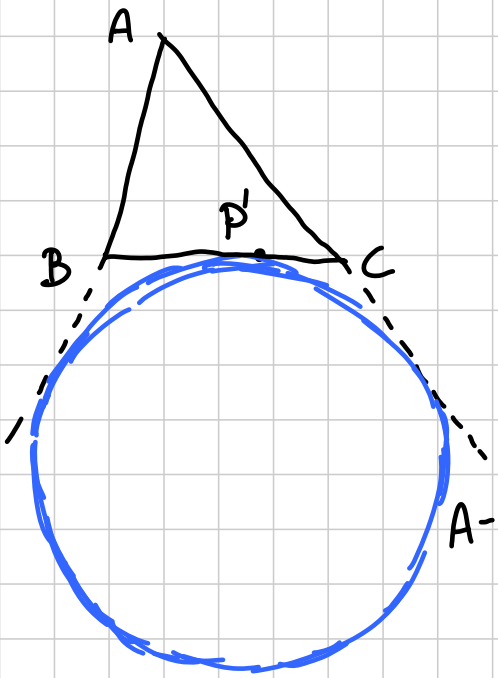
th: $B\hat{A}P = C\hat{A}Q$

inv. in A con $r = \sqrt{AB \cdot AC}$ + simm. nella bisett.

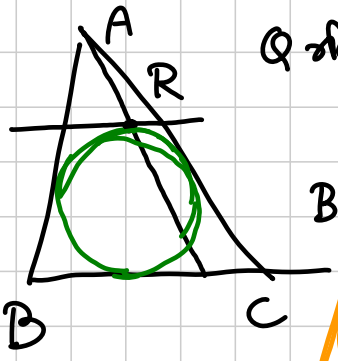
$B \longrightarrow C$, $C \longrightarrow B$

$\Gamma \longrightarrow BC$, $BC \longrightarrow \Gamma$

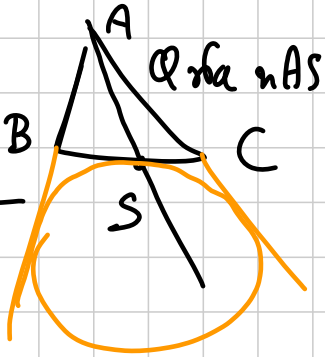
$\omega \longrightarrow$ A-excerchio di ABC



A-excerchio



Q sta su AR



omotetia!!

$Q \in AP' \Rightarrow Q \in$ simm. di AP risp. alla bisett.

Es: Coniugati isog. dei punti di Nagel e Gergonne sono i centri di omotetia tra cfr. inscritta e circ. circoscritta

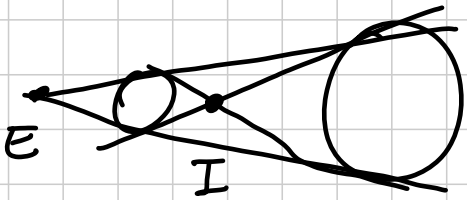
Se X è centro di simil. esterna tra Γ_1 e Γ_2

Y è centro di simil. esterna tra Γ_2 e Γ_3

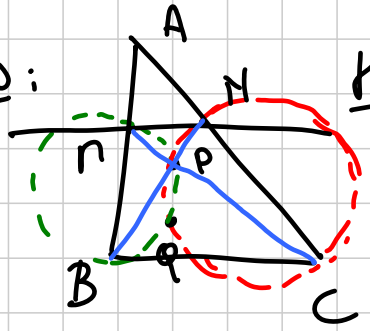
Z " " " " esterna " Γ_3 e Γ_1

allora X, Y, Z sono allineati (Monge)

Esempi:



Es: **Hp:** $B\hat{A}Q = C\hat{A}P$ **BMO 2003-2**



Oss: $AP \cap BC = G$

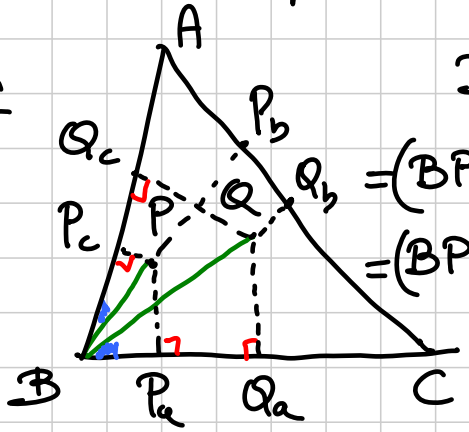
dalla ceva su AP, CP, BP segue che $BG = CG$

AP mediana

$$\frac{AN}{NC}\cdot\frac{CG}{GB}\cdot\frac{BM}{MA} = 1$$

Teo: P, Q coniug. isog. $\Rightarrow$ le circonf. circoscritte dei loro tri pedali coincidono

Dim



$$BP_a \cdot BQ_a = (BP\cdot\cos P\hat{B}C)(BQ\cdot\cos Q\hat{B}C) = (BP\cdot\cos Q\hat{B}A)(BQ\cdot\cos P\hat{B}A) = (BP\cdot\cos P\hat{B}A)(BQ\cdot\cos Q\hat{B}A) = BP_c\cdot BQ_c$$

$\Rightarrow P_a, Q_a, P_c, Q_c$ sono su una circ.

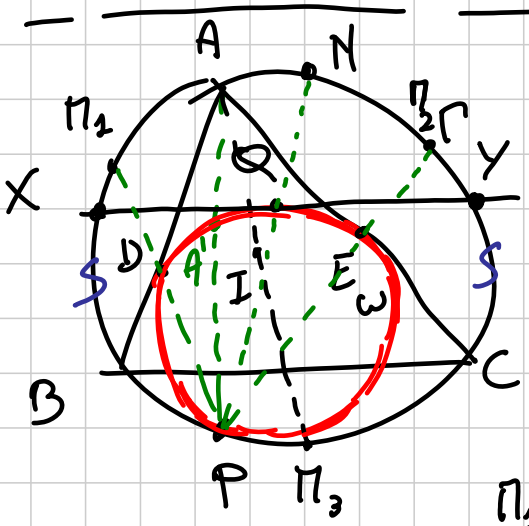
Allo stesso modo $P_aQ_aP_bQ_b$ sono su una circ.

Ancora $P_cQ_cP_bQ_b$ sono su una circ

Se fossero circ. diverse, i 3 assi radicali sarebbero AB, AC, BC, che non concorrono $\Rightarrow$ unica circ.

E il centro è il pt. medio di PQ.

EGMO 2013 – 5 di nuovo



Omotet. di centro P che manda ω in Γ, manda Q nel pt. medio dell'arco $\widehat{XY}$ = pt. medio dell'arco $\widehat{BC}$

P, Q, N allineati.

Π_2 pt. med di $\widehat{AB}$ $\Rightarrow$ P, D, Π_1 allineati

Π_2 pt. med di $\widehat{AC}$ $\Rightarrow$ P, E Π_2

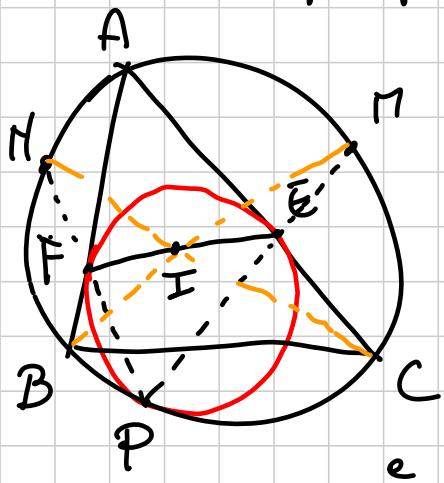
$AN \parallel A'Q$ $AN \perp A\Pi_3$ ($\Pi_3 N$ diametro)

$\Rightarrow A\Pi_3 \perp A'Q$ e il centro di ω sta su $A\Pi_3$

$\Rightarrow A\Pi_3$ è diametro.

$\Rightarrow$ fine per simmetria.

Oss:



NPMBAC è un esagono CICLICO

Per PASCAL

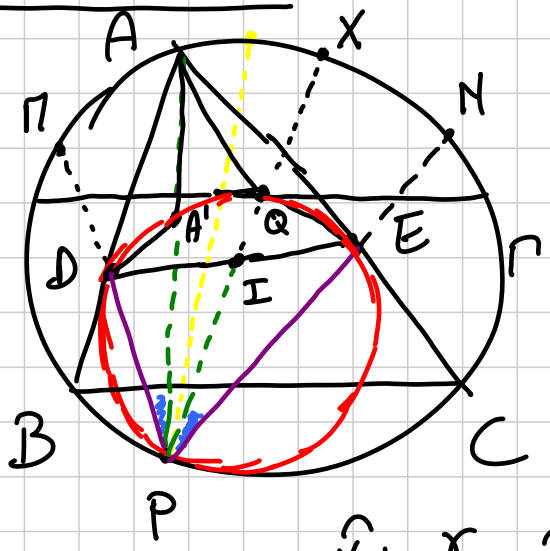
$NP \cap BA = F$

$PM \cap AC = E$ sono allineati

$MB \cap CN = I$

e I è punto medio.

EGMO 2013-5 Reloaded



PI è mediana in $\triangle DPE$

PA è simmediana in $\triangle DPE$

PI interseca Γ in X t.c. $A\Pi = XN$

$\hat{XN} = \frac{\gamma}{2}$ $\hat{NC} = \beta/2 \Rightarrow \hat{CX} = \frac{\gamma}{2} + \frac{\beta}{2}$

$\Rightarrow$ X pt. medio di $\hat{BC} \Rightarrow P, I, Q, X$ allineati

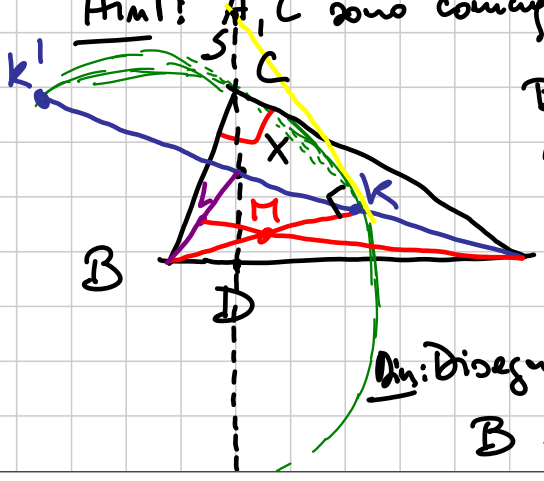
$D\hat{P}A = I\hat{P}E = Q\hat{P}E \Rightarrow A\hat{D}A' = A\hat{E}Q$

e $AE = AD$, $DA' = QE$ $\Rightarrow D\hat{A}P = D\hat{A}A' = Q\hat{A}E = Q\hat{A}C$.

A proposito di coniugati isogonali: IMO 2004 - 5

Hint: A, C sono coniug. isog. in $\triangle DBP$.

IMO 2012-5



$BK = BC$

$AL = AC$

Th: $\Pi K = \Pi L$

Dim: Disegno Γ_1 ch. di centro B e raggio $BC = BK$

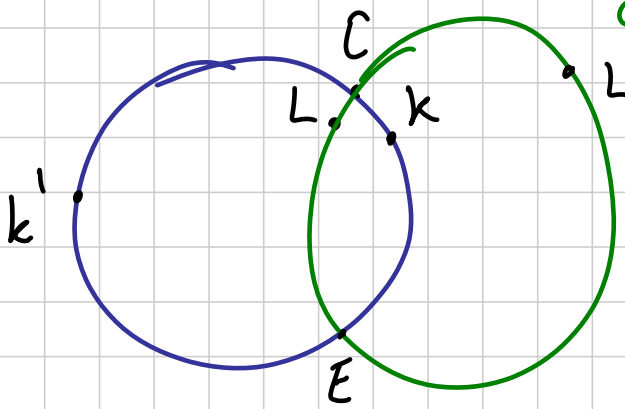
E E = altra intersez. di CD con Γ_1

CA, AE tg. a Γ_1 per hanno. $A = pol_{\Gamma_1}(CE)$

k' ulteriore intersez. di AK con Γ_2

$\Rightarrow$ (lemma della polare) $(A, X, K, K') = -1$.

$\Rightarrow (C, E, K, K') = -1$ Faccio lo stesso con centro in A e ottengo $(C, E, L, L') = -1$



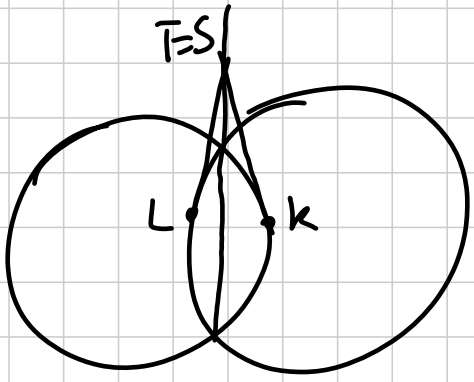
Proietto da K su CE $(KC, KE, KK, KK') = -1$

$\hookrightarrow (C, E, S, X) = -1$

Proietto da L su CE $(LS, LE, LL, LL') = -1$

$T = tg\ in\ L \cap CE$ $(C, E, T, X) = -1$

$\Rightarrow T = S$



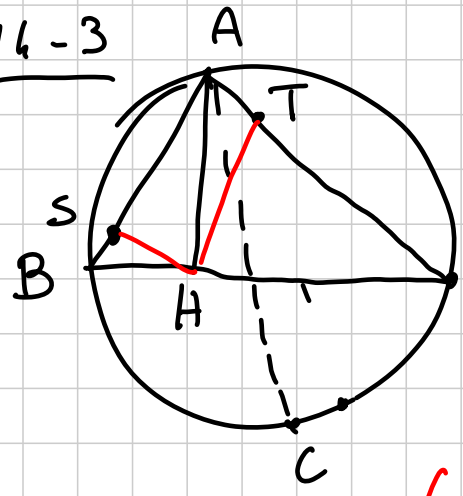
$TL = TK$

e $\hat{BKT} = \hat{ALT} = 90°$

$\Rightarrow \hat{TLN}$ e $\hat{TKN}$ sono congruenti

$\Rightarrow NK = NL$.

Imo 2014 - 3



$\hat{CHS} - \hat{CSB} = \frac{\pi}{2}$

$\hat{THC} - \hat{DTC} = \frac{\pi}{2}$

H è interno a $\overset{\Delta}{CST}$

$\Rightarrow$ BD tg alla circonf. per T, S, H.

(ch. di Apollonio).

Teoria dei Numeri 1 - Medium

Titolo nota 03/09/2014

Polinomi in $\mathbb{Z}/p\mathbb{Z}[x] = \mathbb{F}_p[x] = \mathbb{Z}/(p)[x]$

Espressione formale

$$a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

con gli $a_i \in \mathbb{F}_p$

Si può calcolare $p([n])$ dove $[n]$ è una classe di resto mod p

Cosa funziona? TUTTO

- Un pol. di grado n ha $\leq n$ radici
- Principio di identità dei polinomi: ⚠ Vale con le giuste ipotesi sul grado

Esempio: $X^p - X$ coincide (come funzione, non come polinomio) con 0

- Divisione con resto, Ruffini, fattorizzaz. unica

Esercizio Sia $f : \mathbb{F}_p \longrightarrow \mathbb{F}_p$. Allora esiste $q(x) \in \mathbb{F}_p[x]$ tale che per ogni $[n] \in \mathbb{F}_p$ si abbia $q(n) = f(n)$.

Soluzione Quante sono le funzioni? p^p

Quando succede che due polinomi $q_1(x)$, $q_2(x)$ rappresentano la stessa funzione?

$q_1(n) = q_2(n)$ per $n = 0, 1, 2, \dots, p-1$

$$\Rightarrow q_1(x) - q_2(x) = \underbrace{x(x-1)(x-2)\cdots(x-(p-1))}_{x^p - x} r(x)$$

$x^p - x$ e $\prod_{i=0}^{p-1}(x-i)$ hanno lo stesso grado, stesse radici, stesso coeff. di grado massimo

Ci interessano solo le classi di resto modulo $x^p - x$.

Quindi due polinomi diversi di grado $\leq p-1$ rappresentano funzioni diverse

$$\{\text{polinomi di grado} \leq p-1\} \xrightarrow[\varphi]{\text{iniettiva}} \{\text{funzioni}\}$$

$$|\{\text{polinomi}\}| = p^p \qquad |\{\text{funzioni}\}| = p^p$$

Quindi φ è bigettiva (in particolare è surgettiva)

Esercizio stupido $\binom{p-1}{j} \equiv (-1)^j \pmod p$

Considero $(1+x)^{p-1} = \sum_{j=0}^{p-1} \binom{p-1}{j} x^j$

$$\frac{(1+x)^p}{(1+x)} \equiv \frac{1+x^p}{1+x} \equiv x^{p-1} - x^{p-2} + \dots + 1$$

Uguaglianza tra polinomi $\Rightarrow$ ug. dei coeff. $\pmod p$

GENERATORI MOD p

Sostengo che per ogni k che divide $p-1$ ci siano esattamente $\varphi(k)$ elementi di ordine k

Induzione: $k=1$ OK

$$\left\{\begin{array}{l}\text{elementi di ordine}\\ \text{che divide } k\end{array}\right\} = \left\{\text{radici di } x^k-1\right\}$$

Quante radici ha x^k-1?

$$\underbrace{x^{p-1}-1}_{p-1 \text{ radici}} = \underbrace{(x^k-1)}_{\leq k \text{ rad.}} \cdot \underbrace{r(x)}_{\leq p-1-k \text{ radici}}$$

Quindi x^k-1 ha esattamente k radici

$$x^k-1 = \prod_{\text{ord}_p(r)\mid k}(x-r) = \prod_{\text{ord}(r)=k}(x-r) \times \prod_{\substack{\text{ord}(r)\mid k\\ \text{ord}(r)\neq k}}(x-r)$$

Gradi: LHS ha grado k

RHS " " n° el. di ordine k + $\sum_{\substack{j\mid k\\ j\neq k}}$ n° di elem. di ord j

$$\Rightarrow \quad \cancel{K} = (\text{n° di elem. ord } k) + \sum_{\substack{j \mid k \\ j \neq k}} \varphi(j)$$

$$= \quad " \quad + \underbrace{\sum_{j \mid k} \varphi(j)}_{\cancel{K}} - \varphi(k)$$

In particolare, ci sono $\varphi(p-1)$ generatori $\square$

GENERATORI MOD m

$$X^{\varphi(m)} \equiv 1 \ (m) \quad \text{per ogni} \quad (x, m) = 1$$

Un generatore è un elemento (coprimo con m) di ordine esattamente $\varphi(m)$. Esiste se e solo se m è

* 2 o 4
* p^n o $2p^n$ con p primo dispari

RESIDUI QUADRATICI (e superiori)

Si dice che a è un **residuo quadratico** mod p se esiste n tale che $n^2 \equiv a \pmod p$

Sono $1 + \frac{p-1}{2}$

lo zero ↑ ↖ quelli seri

$\{0, 1, 2, \dots, (p-1)\} \xrightarrow{\square}$ Residui Quadratici

Cosa fa fallire l'iniettività?

$$x_1^2 \equiv x_2^2 \pmod p$$

$$\iff (x_1 - x_2)(x_1 + x_2) \equiv 0 \pmod p$$

$$\iff p \mid x_1 - x_2 \text{ o } p \mid x_1 + x_2$$

Se mi restringo a $\{0, 1, \dots, \frac{p-1}{2}\}$ la funz. $\square$ è iniettiva e surgettiva (perché se $n^2 \equiv a$ e $n \in \{\frac{p+1}{2}, \frac{p+3}{2}, \dots, p-1\}$, allora $a \equiv (-n)^2$ e $-n \in \{1, 2, \dots, \frac{p-1}{2}\}$

$$\Rightarrow |RQ| = 1 + \frac{p-1}{2}$$

Simbolo di Legendre

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ è RQ mod } p \\ -1, & \text{se } a \text{ NON è RQ " "} \\ 0, & \text{se } p \mid a \end{cases} \qquad \boxed{p \neq 2}$$

Proprietà: $* \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

$*$ (Criterio di Eulero) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

Oss: Eulero $\Rightarrow$ Moltiplicatività

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \bmod p$$

Siccome LHS, RHS $\in \{0, 1, -1\}$, la congruenza è una uguaglianza.

Esempio: almeno uno tra 2, 3 e 6 è RQ mod p per ogni primo.

Se 2 non è RQ e 3 nemmeno, allora

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)(-1) = 1$$

Dimostrazione di Eulero

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv a^{p-1} \equiv 1 \mod p$$

$$\Rightarrow a^{\frac{p-1}{2}} \in \{+1, -1\}$$

Consideriamo $\underbrace{x^{\frac{p-1}{2}} - 1}_{q(x)}$ (come polinomio mod p)

Ha al max $\frac{p-1}{2}$ radici, e tutti i quadrati sono radici: $\square^{\frac{p-1}{2}} - 1 \equiv (n^2)^{\frac{p-1}{2}} - 1$

$\equiv n^{p-1} - 1 \equiv 0 \ (p)$

Quindi $q(x) \equiv 0 \pmod p \iff x$ è RQ

$\Updownarrow$

$x^{\frac{p-1}{2}} \equiv 1 \pmod p$

In termini di generatori: $x \equiv g^k \bmod p$

e x è RQ $\iff k$ è pari

$\Updownarrow$ $x^{\frac{p-1}{2}} \equiv 1 \ (p) \iff g^{k \cdot \frac{p-1}{2}} \equiv 1 \pmod p$ $\Updownarrow$

Quando è che -1 è un RQ?

Risposta: se e solo se $p \equiv 1 \ (4)$, perché

$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$

$+1$ se e solo se $\frac{p-1}{2}$ è pari

$\iff p \equiv 1 \bmod 4$

Esercizio $x^2 = y^3 + 7$

$$x^2 + 1 = y^3 + 8 = (y+2)(y^2 - 2y + 4)$$

Mod 8 $\quad x^2 \equiv y^3 + 7 \mod 8$

Se y fosse pari, MALE

(x è multiplo di 4)

Se $y \equiv 1 \mod 4$, allora $y+2 \equiv 3 (4)$ e c'è (nel fattore di dx) almeno un primo $p \equiv 3 (4)$. Mod p abbiamo

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

$$-1 \equiv x^2 \ (p),$$

che contraddice $\left(\frac{-1}{p}\right) = -1$

Se $y \equiv 3 \mod 4$, $y^2 - 2y + 4 \equiv 3 \ (4)$ e si conclude allo stesso modo.

Quindi non ci sono soluzioni

Che dire di $\left(\frac{2}{p}\right)$?

$-1 \equiv (p-1)! \equiv (p-1)!!\,(p-2)!!$

↑ Wilson

$\equiv (2\cdot 4\cdot 6\cdot \ldots \cdot p-1)\,(p-2)!!$

$\equiv 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!\,(p-2)!!$

$1\cdot 3\cdot 5\cdot 7\cdot 9 = 1\cdot 3\cdot 5\cdot (-4)(-2) \quad (p=11)$

$= \left(\frac{11-1}{2}\right)!$

$1\cdot 3\cdot 5\cdot 7\cdot 9\cdot 11\cdot 13\cdot 15\cdot 17 \qquad p=19$

$\underbrace{}_{(-8)}\ \underbrace{}_{(-6)}\ \underbrace{}_{(-4)}\ \underbrace{}_{(-2)}$

$1\cdot 3\cdot 5\cdot 7\cdot 9\cdot 11 \qquad p=13$

$$(p-2)!! = \begin{cases} (-1)^{\frac{p-1}{4}} \left(\frac{p-1}{2}\right)! & \frac{p-1}{2} \text{ pari} \\ (-1)^{\frac{p-3}{4}} \left(\frac{p-1}{2}\right)! & \frac{p-1}{2} \text{ dispari} \end{cases}$$

$$-1 \equiv 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!\,(p-2)!!$$

$$\equiv 2^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \cdot \begin{cases} (-1)^{\frac{p-1}{4}} & p\equiv 1\ (4) \\ (-1)^{\frac{p-3}{4}} & p\equiv 3\ (4) \end{cases}$$

$$\equiv 2^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \cdot (p-1)! \cdot \begin{cases} (-1)^{(p-1)/4} \\ (-1)^{(p-3)/4} \end{cases}$$

$$\Rightarrow 2^{\frac{p-1}{2}} \equiv (-1)(-1)(-1)^{\frac{p-1}{2}} \begin{cases} (-1)^{(p-1)/4} \\ (-1)^{(p-3)/4} \end{cases}$$

Dipende solo da $p \bmod 8$

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv \begin{cases} +1, & \text{se } p \equiv \pm 1 \ (8) \\ -1, & \text{se } p \equiv \pm 3 \ (8) \end{cases}$$

Residui "superiori"

a è residuo k-esimo se $\exists n$ tale che

$$n^k \equiv a \mod p$$

Sono $1 + \dfrac{p-1}{(p-1,k)}$

Residui cubici mod 17: TUTTI!

Ogni classe di resto si scrive g^k per un certo k. Posso scegliere $k \equiv 0\ (3)$?

Se $n \equiv g^k$, n è anche $\equiv g^{k+(p-1)}$

$\equiv g^{k+2(p-1)}$

e siccome $p-1 \not\equiv 0\ (3)$ (almeno) uno tra

$k,\ k+16,\ k+32$ è $0 \mod 3$

"Criterio di Eulero"

n è un residuo k-esimo $\iff$ $n^{\frac{p-1}{(k,p-1)}} \equiv 1 \mod p$

Esercizi

BMO 2014/2

$$2014 = \frac{a^3+2b^3}{c^3+2d^3}$$

$$= 2 \cdot 19 \cdot 53$$

$2014\,(c^3+2d^3) = a^3+2b^3$

Mod 19: $0 \equiv a^3+2b^3 \mod 19$

Moralmente, $-2 \equiv \left(\frac{a}{b}\right)^3 \mod 19$

↳ in gara: "se $b \not\equiv 0 \mod 19$"

-2 è residuo cubico mod 19 $\iff (-2)^6 \equiv 1\ (19)$ (64)

$\iff$ (NO) (siccome $(-2)^{\frac{19-1}{(3,18)}} \not\equiv 1 \mod 19$,

-2 NON è residuo cubico mod 19)

$\Rightarrow b \equiv 0\ (19) \Rightarrow a \equiv 0\ (19)$

E ora discesa infinita. (FATELA!)

RMM 2013/1

Sia a un intero positivo.

$x_1 = a, \quad x_{n+1} = 2x_n + 1, \quad y_n = 2^{x_n} - 1$

Qual è il più grande K per cui esiste a tale che $y_1, y_2, \ldots, y_K$ siano tutti primi

$a = 2 \longrightarrow y_1 = 3, \quad y_2 = 31$

Osservazione: Se gli y_n sono primi, anche gli x_n sono primi

Per assurdo: y_1, y_2, y_3 primi

$$y_2 = 2^{x_2} - 1 \equiv 2^{\frac{x_3-1}{2}} - 1 \mod x_3 \quad (*)$$

x_3 divide y_2 se 2 è RQ mod x_3

perché $2^{\frac{x_3-1}{2}} \equiv \left(\frac{2}{x_3}\right) \mod x_3$ $(*)$

Vogliamo $\left(\frac{2}{x_3}\right) = 1$, cioè $x_3 \equiv \pm 1 \pmod 8$

Parto da $x_1 \rightsquigarrow \underbrace{2x_1+1}_{\equiv 3 \bmod 4} \rightsquigarrow 2(2x_1+1)+1 \equiv 7 \bmod 8$

Quindi: x_1 è primo, quindi o $x_1 = 2$ o x_1 dispari. $x_1 = 2$ si prova a mano.

x_1 dispari $\Rightarrow x_3 \equiv 7 \ (8) \overset{(*)}{\Rightarrow} x_3 \mid y_2$

$$\Rightarrow x_3 = y_2 = 2^{x_2} - 1$$

$$x_3 = 2x_2 + 1$$

Questo è possibile solo per $x_2 = 3$, ma non funziona

IMO 2006/4 $\quad y^2 = 1 + 2^x + 2^{(2x+1)}$

Mod 2^x : $y^2 \equiv 1 \pmod{2^x}$

$(y+1)(y-1) \equiv 0 \pmod{2^x}$

quasi coprimi: uno dei due è $\equiv 0 \ (2^{x-1})$

$y = \pm 1 + K \cdot 2^{x-1}$

$1 \pm K \cdot 2^x + K^2 \cdot 2^{2(x-1)} = 1 + 2^x + 2^{2x+1}$

A mano : $x \leq 2$

$$\pm K + K^2 \cdot 2^{x-2} = 1 + 2^{x+1}$$

$\geq$ ← wlog $K > 0$ (1)

$$K\left(\frac{K}{4} 2^x - 1\right) \geq 4(2^x - 1)$$

crescente in K. Per $K = 4$

Quindi: o $x \leq 2$ o $K \leq 3$ (A MANO)

LEMMA LTE ("lifting the exponent")

Notazione: $v_p(n)$ = l'esponente di p nella fattorizzazione di n

* $v_p(ab) = v_p(a) + v_p(b)$
* $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$

con $=$ se $v_p(a) \neq v_p(b)$

$a = p^{v_p(a)} \cdot r, \quad b = p^{v_p(b)} \cdot s$

$v_p(a) > v_p(b)$

$a+b = p^{v_p(b)} \left(\underbrace{p^{v_p(a)-v_p(b)} r + s}_{\not\equiv 0 \ (p)} \right)$

Enunciato • p primo dispari

• a, b NON multipli di p

• $p \mid a-b$

Allora $v_p\left(a^n - b^n\right) = v_p(a-b) + v_p(n)$

Corollario Se n è dispari, lo applico a "a" e "$-b$" e quindi vale anche con il $+$

$$\begin{cases} p \nmid a,\ p \nmid b,\ p \mid a+b \\ v_p\left(a^n+b^n\right) = v_p(a+b) + v_p(n) \\ n \text{ dispari} \end{cases}$$

Dimostrazione

$v = v_p(a-b)$

Caso $n = p$ $\quad a - b = kp^v$ con $(k,p)=1$

$$a^p - b^p = (b + kp^v)^p - b^p =$$

$$= b^p + p \cdot b^{p-1} \cdot (kp^v) + \sum_{j=2}^{p} \binom{p}{j} b^{p-j} (k \cdot p^v)^j - b^p$$

$$v_p(a^p - b^p) = v_p\left(kb^{p-1} \cdot p^{v+1} + p^{2v+1}(\dots)\right)$$

$$= v+1 = v_p(a-b) + 1$$

Caso $(n,p) = 1$ $\quad a^n - b^n =$

$$= \cancel{b^n} + n \cdot b^{n-1} \cdot (kp^v) + \sum_{j=2}^{n} \binom{n}{j} b^{n-j} (k \cdot p^v)^j - \cancel{b^n}$$

$$v_p(a^n - b^n) = v = v_p(a-b)$$

Caso generale "Induzione"

$n = p^{v_p(n)} \cdot r$ con $(r,p) = 1$

$$v_p(a^n - b^n) = v_p\left((a^{v_p(n)})^r - (b^{v_p(n)})^r\right)$$

caso $(n,p) > 1$

$$= v_p\left(a^{p^{v_p(n)}} - b^{p^{v_p(n)}}\right)$$

caso $n=p$ applicato $v_p(n)$ volte

$$= v_p(a-b) + v_p(n)$$

$$v_p\left(a^{p^2} - b^{p^2}\right) = v_p\left((a^p)^p - (b^p)^p\right)$$

$$= v_p\left(a^p - b^p\right) + 1$$

$$= v_p(a-b) + 2$$

GUADAGNO DI UN PRIMO

p "primo dispari"

"a^p+b^p ha un fattore primo che $a+b$ non ha, a meno che $a=2$, $b=1$, $p=3$ oppure $a=b=1$"

$$a^p+b^p = \left(\frac{a^p+b^p}{a+b}\right)(a+b)$$

Dimostrazione Sia q un fattore primo di $a+b$

Per LTE, $v_q\left(\frac{a^p+b^p}{a+b}\right) = v_q\left(a^p+b^p\right) - v_q(a+b)$

$$= v_q(a+b) + v_q(p) - v_q(a+b)$$

$$= v_q(p)$$

Conclusione: $a+b$, $\frac{a^p+b^p}{a+b}$ sono coprimi tranne al più un singolo fattore p.

Se (per assurdo) $\frac{a^p+b^p}{a+b}$ non ha fattori primi "nuovi" (risp. ad $a+b$), allora $\frac{a^p+b^p}{a+b} = \begin{cases} p \\ 1 \end{cases}$

Se $a \geq 2$, $b \geq 2$ abbiamo $a^p > ap$

$b^p > bp$

e sommando le ASSURDO. Quindi $\min\{a,b\}=1$

$a=1,\ b\geq 2$ $\qquad 1+b^p = p(1+b)$

$$1+\underbrace{[1+(b-1)]^p}_{\text{''}} \geq 1+1+p(b-1) + \frac{p(p-1)}{2}(b-1)^2$$

$$2p \geq 2 + p\frac{(p-1)}{2}(b-1)^2 \geq p\left(\frac{p-1}{2}\right)(b-1)^2$$

$$2 \geq \left(\frac{p-1}{2}\right)(b-1)^2 \Rightarrow \begin{matrix}(b-1)\leq 1 \\ \frac{p-1}{2}\leq 2\end{matrix}$$

... si trattano a mano i casi piccoli.

GENERATORI MOD p^n ($p \neq 2$)

(1) Fatto: esiste un gen. mod p^n

(2) Fatto migliore: se g è un generatore mod p allora o g o $g+p$ è un generatore modulo p^2

(3) Fatto ancora migliore: se h genera mod p^2, genera anche mod p^n per ogni n

Dim di (2) $g^{p-1} \equiv 1 \mod p$. Per essere gen mod p^2: $g^{p-1} \not\equiv 1 \mod p^2$ (*)

Claim: (*) è condizione sufficiente per generare mod p^2, ammesso che g generi modulo p

Qual è l'ordine di g mod p^2?

$\operatorname{ord}_{p^2}(g)$ è multiplo di $\operatorname{ord}_p(g) = p-1$

$(p-1) \mid \operatorname{ord}_{p^2}(g) \mid \varphi(p^2) = p(p-1)$

non è un uguale

Quindi $\operatorname{ord}_{p^2}(g) = p(p-1)$ e g genera.

Ci siamo ridotti a: "se g genera mod p, o $g^{p-1} \not\equiv 1 \mod p^2$ o $(g+p)^{p-1} \not\equiv 1 \ (p^2)$".

Supponiamo quindi $g^{p-1} \equiv 1 \ (p^2)$. Allora

$$\begin{aligned}(g+p)^{p-1} &\equiv g^{p-1} + (p-1)g^{p-2}p \\ &\quad + \text{termini in } p^2 \\ &\equiv 1 + \underbrace{p(p-1)g^{p-2}}_{\text{non è zero mod } p^2 \text{ perché ha esattamente un fattore } p} \pmod{p^2} \\ &\not\equiv 1\end{aligned}$$

Se g genera mod p^2, genera mod p^n.

$$g^{p-1} \not\equiv 1 \ (p^2) \qquad g^{p-1} \equiv 1 \ (p)$$

$$v_p\left(g^{p-1} - 1\right) = 1$$

Quanto vale $\operatorname{ord}_{p^n}(g)$?

$$= (p-1)\cdot p^r$$

Tesi $\hookrightarrow$ $\operatorname{ord}_{p^n}(g) = \varphi(p^n) = (p-1)\,p^{n-1}$

$\Leftrightarrow$ $r = n-1$. Stimiamo r:

$$g^{(p-1)p^r} \equiv 1 \mod p^n$$

$$n \le v_p\left(g^{(p-1)p^r} - 1\right) = v_p\left(\left(g^{(p-1)}\right)^{p^r} - 1^{p^r}\right)$$

$$\overset{\text{LTE}}{=} v_p(p^r) + v_p\left(g^{p-1} - 1\right)$$

$$= r + 1$$

$\Rightarrow \quad r \geq n - 1$

SNS 2014/1 $a^7 + b^7 = 7^c \qquad a, b, c \geq 1$

$$a^7 + b^7 = \left(\frac{a^7+b^7}{a+b}\right)(a+b)$$

- $a+b$ = potenza di 7 $(\neq 1)$
- Guadagno di un primo $\Rightarrow$ $\frac{a^7+b^7}{a+b}$ ha un fattore primo $\neq 7$, quindi non è una potenza di 7

NO SOLUZIONI

Esercizio $a^7 + b^7 = 7^c 3^d$

Es $x^5 + 4^y = 2013^z \quad (2013 = 3 \cdot 11 \cdot 61)$

Mod 11: $x^5 + 4^y \equiv 0 \pmod{11}$

$\ord_{11}(4) = 5$: perché?

$\ord_{11}(4) \mid 10$

$4^5 \equiv 4^{\frac{11-1}{2}} \equiv 1 \pmod{11}$ (Eulero)

$4^y \not\equiv -1 \pmod{11}$ perché $4^y = \square$ e -1 non lo è (perché $11 \equiv 3 \pmod 4$)

Unica configurazione ammessa: $x^5 \equiv -1 \pmod{11}$

$4^y \equiv 1 \pmod{11}$

$\Rightarrow \quad 5 \mid y \qquad y = 5a$

$$(x+4^a)\left(\frac{x^5+4^{5a}}{x+4^a}\right) = 2013^z = 3^z\, 11^z\, 61^z$$

coprimi! In generale potrebbero avere in comune un fattore 5, ma $5 \nmid RHS$

Se $x+4^a \equiv 0 \pmod{11^z}$

$$\Rightarrow \quad x^5+4^{5a} \geq 2\left(\frac{x+4^a}{2}\right)^5 \geq \frac{1}{16}\,11^{5z} >> 2013^z$$

Sennò, $x+4^a = 3^z$, ma allora

$$x^5+4^{5a} \leq (x+4^a)^5 \leq \underbrace{243^z}_{3^5} << 2013^z$$

IMO 2000

Domanda: esiste un n con esattamente 2000 fattori primi diversi e t.c. $n \mid 2^n+1$?

Risposta: **Sì**

$p \mid 2^p+1 \Rightarrow p \mid 3 \Rightarrow p=3$

$n=3$ rispetta $3 \mid 2^3+1$

Osservazione: se abbiamo n : $n \mid 2^n+1$ e p è un fattore primo di 2^n+1 che n non ha, allora np rispetta $np \mid 2^{np}+1$

Basta dim che $p \mid 2^{np}+1$, $n \mid 2^{np}+1$

$1+2^{np} \overset{\text{FLT}}{\equiv} 1+2^n \equiv 0 \pmod p$ ($\uparrow p \mid 2^n+1$ per ipotesi)

$n \mid 2^n+1 \mid (2^n)^p+1^p$

Per inizializzare la ricorrenza prendo $n=9$

$9 \mid 2^9+1$

Ora $2^9+1 = (2^3+1)\left(\frac{2^9+1}{2^3+1}\right)$ ha un fattore primo $\neq 3$ (dicono 19)

$n_1 = 9 \qquad n_2 = 9 \cdot 19$

$$2^{n_2}+1 = \left(\frac{(2^{n_1})^{19}+1}{2^{n_1}+1}\right)\left(2^{n_1}+1\right)$$

↑ ha un fattore primo che $2^{n_1}+1$ non ha

Ma $n_1 \mid 2^{n_1}+1$, quindi questo fattore primo p non sta neppure in n_1.

D'altro canto, n_2 è n_1 × un fattore primo di $2^{n_1}+1$. Quindi $p \nmid n_1$, $p \nmid 2^{n_1}+1$

$\Rightarrow p \nmid n_2$, e quindi posso prendere

$$n_3 = p n_2$$

+ Induzione

Es Esistono infiniti n tali che

$$n \nmid 2^n+1, \qquad n \mid 2^{2^n+1}+1$$

Soluzione

$a_n = 2^{3^n}+1$ e p_n un primo che divide a_n ma non a_{n-1} (quad di un primo)

Prendo $b_n = p_n \cdot 3^{n-1}$

(1) $b_n \nmid 2^{b_n}+1$

(2) $b_n \mid 2^{2^{b_n}+1}+1$

(1) $2^{b_n}+1 = \left(2^{3^{n-1}}\right)^{p_n}+1 \equiv 2^{3^{n-1}}+1$

$\equiv a_{n-1} \not\equiv 0 \pmod{p_n}$

(2) $3^{n-1} \overset{?}{\mid} 2^{2^{b_n}+1}+1 \iff v_3\left(2^{2^{b_n}+1}+1\right) \geq n-1$

$v_3(2+1) + v_3\left(2^{b_n}+1\right) \overset{LTE}{=}$

$1 + v_3(2+1) + v_3(b_n)$

$2 + (n-1) = n+1$

$p_n \overset{?}{\mid} 2^{2^{b_n}+1}+1 \qquad p_n \mid 2^{3^n}+1$

$$v_3\left(2^{b_n}+1\right) = v_3(2+1) + v_3(b_n) = n$$

$$2^{b_n} + 1 = 3^n \cdot c$$

$$p_n \overset{?}{\mid} 2^{c\cdot 3^n} + 1 \text{ : sì, perché}$$

$$p_n \mid 2^{3^n} + 1 \mid 2^{3^n \cdot c} + 1$$

IMO 2003 / 6

Sia p un numero primo. Esiste un primo q tale che per ogni n $n^p - p \not\equiv 0 \pmod q$

Soluzione Tesi: p non è un residuo p-esimo modulo q. In particolare $p \mid q-1$

(altrimenti, il numero dei residui p-esimi mod q sarebbe $1 + \frac{q-1}{(q-1,p)} = q$ e tutto, in particolare p, sarebbe un residuo p-esimo)

Criterio di Eulero generalizzato:

$$p^{\frac{q-1}{p}} \not\equiv 1 \pmod q$$

$$\iff \operatorname{ord}_q(p) \nmid \frac{q-1}{p}$$

Prova: prendo $\operatorname{ord}_q(p)$ un primo

Mica tanto facile! L'ordine di p mod q divide $q-1$, ma non deve dividere $\frac{q-1}{p}$

Hope: riesco a trovare q t.c. $\operatorname{ord}_q(p) = p$ e $q \not\equiv 1 \mod p^2$ $\left(\iff p \nmid \frac{q-1}{p}\right)$

$p^p \equiv 1 \mod q \Rightarrow$ se un tale q esiste, è un fattore di $p^p - 1$.

Cerchiamo un q che divida $\frac{p^p-1}{p-1}$ e non sia $\equiv 1 \ (p^2)$. Esiste?

Se non esistesse, $\frac{p^p-1}{p-1}$ sarebbe $\equiv 1 \ (p^2)$

Ma non è vero: $1 \equiv \frac{p^p-1}{p-1} \pmod{p^2}$

$$\Rightarrow p - 1 \equiv p^p - 1 \pmod{p^2}$$

$p - 1 \equiv p$, $p^p - 1 \equiv 0$,

ASSURDO

Quindi $\exists q$: $\mathrm{ord}_q(p) = p$, $p^2 \nmid q-1$, e un tale q funziona (per Eulero)

Teoria dei Numeri 2 - Medium

Titolo nota 04/09/2014

Lemma Sia p un primo, $q(x) \in \mathbb{Z}/p\mathbb{Z}[x]$. Supponiamo che $\deg q \leq p-2$. Allora

$$\sum_{n=0}^{p-1} q(n) \equiv 0 \pmod{p}$$

Dimostrazione

(1) Basta farlo per i monomi (ax^k)

(2) $a = 1$

$$\sum_{n=0}^{p-1} 2n^3 \equiv 0 \pmod{p}$$

(3) $$\sum_{n=0}^{p-1} n^k \equiv \sum_{n=1}^{p-1} n^k \equiv$$

$k > 0$

dove g è un generatore $\equiv \sum_{j=0}^{p-2} (g^j)^k$

$$\equiv \sum_{j=0}^{p-2} (g^k)^j \equiv \frac{(g^k)^{p-1} - 1}{g^k - 1} \equiv 0$$

La formula per la somma della progr geometrica funziona purché $g^k \not\equiv 1 \pmod p$
$\iff (p-1) \nmid k$

(4) Se $k=0$: un polinomio di grado 0 è una costante a. $\sum_{j=0}^{p-1} a = p \cdot a \equiv 0$

Osservazione Per x^{p-1} la somma vale -1

$$\sum_{j=0}^{p-1} j^{p-1} \equiv 0 + \underbrace{1 + \dots + 1}_{(p-1)\ \text{FLT}} \equiv -1 \pmod p$$

Lemma ++ Se $q(x)$ non ha monomi di grado divisibile per $p-1$ (e non costanti) allora $\sum_{n=0}^{p-1} q(n) \equiv 0 \mod p$

Chevalley - Warning

Sia
$$\begin{cases} f_1(x_1, \dots, x_n) \equiv 0 \pmod p \\ \vdots \\ f_k(x_1, \dots, x_n) \equiv 0 \pmod p \end{cases}$$
un sistema polinomiale di congruenze.

Supponiamo che $\sum \deg f_k < n$.

Allora se c'è una soluzione ce n'è almeno un altra

Esempio $x^2 - 3y^2 = 47z^2$

Inutile controllare mod p per $p \neq 3, 47$.

Infatti CW (per $p \neq 3, 47$) dice:

- ci sono 3 variabili
- il grado è 2
- c'è una soluzione banale: $(0,0,0)$

$\Rightarrow$ ce n'è anche una non banale

Versione "aritmetica"

Il numero di soluzioni (al sistema...)

è $\equiv 0 \pmod p$

Dimostrazione

$$f_i^{p-1}(x_1, \dots, x_n) \equiv \begin{cases} 0, & \text{se } f_i(x_1, \dots, x_n) = 0 \\ 1 & \text{altrimenti} \end{cases}$$

$$\prod_{i=1}^{k} \left(1 - f_i^{p-1}\right) \equiv \begin{cases} 1, & \text{se } (x_1, \dots, x_n) \text{ è una soluzione} \\ 0 & \text{se anche solo un } f_i(x_1, \dots, x_n) \neq 0 \end{cases}$$

$$\#\text{soluzioni} \equiv \sum_{x_1} \sum_{x_2} \dots \sum_{x_n} \prod_{i=1}^{k} \left(1 - f_i^{p-1}\right)$$

Esempio 2 variabili, grado 1

$$x_1 + 2x_2 - 5$$

(x_1, x_2) è soluzione $\iff (x_1 + 2x_2 - 5)^{p-1} \equiv 0$

$$\iff 1 - (x_1 + 2x_2 - 5)^{p-1} \equiv 1 \pmod p$$

Se sommiamo $\sum_{x_1=0}^{p-1} \sum_{x_2=0}^{p-1} \left(1 - (x_1 + 2x_2 - 5)^{p-1}\right)$

ottenia mo $\sum_{x_1} \sum_{x_2} \begin{cases} 1, & \text{se } (x_1, x_2) \text{ è sol} \\ 0 & \text{altrimenti} \end{cases}$

e cioè il # soluzioni

Fissiamo $p = 7$. $\quad - x_1^6$

$$- \binom{6}{2} x_1^2 (2x_2)^4$$

$$\vdots$$

Trucco $\quad \sum_{x_1=0}^{p-1} \sum_{x_2=0}^{p-1} x_1^a x_2^b \equiv 0 \mod p$

- Se $a \leq p-2$,

$$\sum_{x_2=0}^{p-1} \sum_{x_1=0}^{p-1} x_1^a x_2^b \equiv$$

$$\equiv \sum_{x_2=0}^{p-1} x_2^b \left(\sum_{x_1=0}^{p-1} x_1^a \right)$$

$$\equiv \sum_{x_2=0}^{p-1} x_2^b \cdot 0 \equiv 0 \mod p$$

- Uguale se $b \leq p-2$
- Può essere $a \geq p-1$, $b \geq p-1$? Certamente no, perché altrimenti $\deg (x_1 + 2x_2 - 5)^{p-1}$

$\geq 2(p-1)$ ASSURDO

In generale Sviluppando

$$\sum_{x_1} \cdots \sum_{x_n} \prod \left(1 - f_i(x_1, \ldots, x_n)^{p-1}\right)$$

possiamo trovare un termine $x_1^{a_1} \cdots x_n^{a_n}$ con tutti gli $a_i > 0$ e $\equiv 0 \ (p-1)$?

No, perché altrimenti $\sum (\deg f_i)(p-1) \geq (p-1) \cdot n$, assurdo per ipotesi. □

Corollario Se gli $f_i(x_1, \ldots, x_n)$ sono omogenei (o senza termine noto), allora ci sono almeno $(p-1)$ soluz. non banali ($+1$ banale, che è $(0, 0, \ldots, 0)$)

Esercizio Per ogni primo p esiste $k < p$ e x, y, z tali che $x^2 + y^2 + z^2 = kp$

Soluzione con CW Il polinomio $x^2 + y^2 + z^2$ è omogeneo, in 3 variabili, di grado 2

Quindi la congruenza $x^2+y^2+z^2 \equiv 0 \pmod p$ ha una soluz. non banale

Scegliamo $0 \le x, y, z \le \frac{p-1}{2}$; allora

$$x^2+y^2+z^2 < 3\left(\frac{p}{2}\right)^2 = \left(\tfrac{3}{4}p\right)\cdot p$$

IMO ~ 2008 (SL)

p primo. A è un insieme di interi positivi, $q_1, \dots, q_{p-1}$ sono primi

* Ogni intero in A si scrive come prodotto dei q_i (detto meglio: tutti i fattori primi sono tra i q_i)

* Ogni prodotto di elementi di A non è una potenza p-esima perfetta

Qual è al massimo $|A|$?

Elementi di A = vettori di lunghezza $(p-1)$

$(e_1, \dots, e_{p-1})$

Condizione: la somma di alcuni di questi vettori non ha tutte le coordinate $\equiv 0 \pmod p$

$p=2$ $\rightsquigarrow$ * tutti gli elementi di A sono

della forma q_i^j

* c'è al più un elem: dev'essere q^{dispari}, ma se ce ne sono 2 il prodotto è un quadrato

$p=3 \rightsquigarrow 2,\ 3,\ 6=2\cdot 3,\ 2\cdot 3^3$ ④

q_1	q_1^{1+p}	q_1^{1+2p}	...	$(p-1)$
⋮				⋮
q_{p-1}	q_{p-1}			$(p-1)$
			Totale	$(p-1)^2$

Tentativo: se sono $> (p-1)^2$?

$(e_{1,1}, \dots, e_{1,p-1})$
$(e_{2,1}; \dots; e_{2,p-1})$
⋮

} Sono k almeno $(p-1)^2+1$

Cerco $a_1, \dots, a_k \in \{0,1\}$ in modo che $\sum a_i (e_{i,1}; \dots; e_{i,p-1})$ abbia tutte le coord. $\equiv 0 \ (p)$

$$\begin{cases} a_1^{p-1} e_{1,1} + a_2^{p-1} e_{2,1} + \dots + a_k^{p-1} e_{k,1} \equiv 0 \pmod p \\ a_1^{p-1} e_{1,2} + a_2^{p-1} e_{2,2} + \dots + a_k^{p-1} e_{k,2} \equiv 0 \pmod p \\ \vdots \end{cases}$$

Numero di incognite : k

" " equazioni $= p-1$

Grado totale: $(p-1)^2$

Se $k > (p-1)^2$, siccome c'è la soluzione banale $(0, 0, \dots, 0)$, ce n'è anche una non banale. Quindi trovo un sottoins di A il prodotto dei cui elementi è una potenza p-esima, MALE.

Ritorno su $y^2 = x^3 + 7$

Affermazione: questa ha soluzioni mod p per ogni primo p.

(x,y) è soluzione mod p $\iff$

$$1 - (y^2 - x^3 - 7)^{p-1} \equiv 1 \mod p$$

$$\#\text{soluzioni mod } p \equiv \sum_x \sum_y \left[1 - (y^2 - x^3 - 7)^{p-1}\right]$$

$$\equiv -\sum_x \sum_y \sum_{j=0}^{p-1} \binom{p-1}{j} y^{2j} (-x^3 - 7)^{p-1-j}$$

$$\equiv -\sum_x \sum_j \binom{p-1}{j} (-x^3-7)^{p-1-j} \sum_y y^{2j}$$

Chi sopravvive? $j = \frac{p-1}{2}, p-1$

In realtà anche $j = p-1$ somma a zero perché c'è $\sum_x$

$$\equiv -\sum_x \binom{p-1}{\frac{p-1}{2}} \cdot (-1) \cdot (-x^3 - 7)^{\frac{p-1}{2}}$$

$$\equiv +\sum_x \binom{p-1}{\frac{p-1}{2}} \sum_{k=0}^{\frac{p-1}{2}} (-x^3)^k (-7)^{\frac{p-1}{2}-k} \binom{\frac{p-1}{2}}{k}$$

$$\equiv \binom{p-1}{\frac{p-1}{2}} \sum_{k=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k} (-7)^{\frac{p-1}{2}-k} \sum_x (-x)^{3k}$$

I k muoiono tutti, tranne quelli per cui $(p-1) \mid 3k$, $k>0$, cioè solo $\frac{p-1}{3}$

$p \equiv 1 \pmod 3$

$$\equiv \binom{p-1}{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{\frac{p-1}{3}} (-7)^{\frac{p-1}{6}} \cdot (-1)$$

$\not\equiv 0$ se $p \neq 7$

E gli altri? $y^2 = x^3 + 7$ modulo $p \equiv 2 \pmod 3$

ogni numero è un residuo cubico

$$\left(\#\text{residui cubici} = 1 + \frac{p-1}{(p-1,3)} = p \right)$$

e la radice cubica è unica

$$x = \sqrt[3]{y^2 - 7} \pmod p,$$

quindi le soluzioni sono esattamente p

[$p = 2, 3, 7$ a mano]

Soluzioni modulo p^n (Hensel dei poveri)

$p \neq 2, 3, 7$. Sia x, y una soluzione modulo p.

$$(y + bp)^2 - (x + ap)^3 - 7 \equiv 0 \pmod{p}$$

Vorrei trovare a, b in modo che

$$y^2 + 2byp - (x^3 + 3x^2 \cdot a \cdot p) - 7 \overset{?}{\equiv} 0 \pmod{p^2}$$

$$kp + p(2by - 3ax^2) \overset{?}{\equiv} 0 \pmod{p^2}$$

$$k + 2by - 3ax^2 \overset{?}{\equiv} 0 \pmod{p}$$

(Questa ha una soluz. (a, b) a meno che

$$2y \equiv 0 \pmod{p} \text{ e } -3x^2 \equiv 0 \pmod{p}$$

$\overset{p \neq 2,3}{\Longrightarrow}$ $x \equiv 0 \equiv y \pmod{p}$; sostituendo otteniamo

$$0 \equiv 0 + 7 \mod p$$

assurdo per $p \neq 7$

E da p^n a p^{n+1} ?

Se (x,y) è soluz mod p^n, ne so costruire una mod p^{n+1} della forma

$$x + a \cdot p^n, \quad y + b \cdot p^n$$

PELL, PELL, PELL (LE 6 L)

Fissiamo $d > 0$ e cerchiamo di risolvere

$$x^2 - dy^2 = 1$$

Oss. 1 Se $d = \square$ si fattorizza e non è interessante

Oss 2 Si può supporre d libero da quadrati

Claim Se $d \neq \square$ ci sono infinite soluz.

$$x^2 - dy^2 = (x + \sqrt{d}\, y)(x - \sqrt{d}\, y)$$

Norma $N(x + \sqrt{d}\, y) = x^2 - dy^2$

$$N\big((x + \sqrt{d}\, y)(w + \sqrt{d}\, z)\big) = N(x + \sqrt{d}\, y)\, N(w + \sqrt{d}\, z)$$

"Pell" = "$N(x + \sqrt{d}\, y) = 1$"

Idea Per trovare una soluzione della Pell (= una cosa di norma 1) cerchiamo due cose con la stessa norma e facciamo il rapporto

$$\frac{x + \sqrt{d}\, y}{z + \sqrt{d}\, w} = \frac{(x + \sqrt{d}\, y)(z - \sqrt{d}\, w)}{z^2 - dw^2}$$

$$= \frac{(xz - dwy) + \sqrt{d}\,(yz - xw)}{N(z + \sqrt{d}\, w)}$$

Supponiamo di avere $x + \sqrt{d}\, y$, $z + \sqrt{d}\, w$ con la stessa norma N.

Ci serve $N \mid (xz - dwy)$

$N \mid yz - xw$

" $y/x \equiv w/z$ $\Leftarrow$ (*) $\begin{cases} y \equiv w \\ x \equiv z \end{cases}$ mod N

$x^2 - dy^2 \equiv 0 \ (N)$ "

Meglio: se ne troviamo infiniti con la stessa norma, allora due rispettano (*) e il rapporto è intero.

⌜Dirichlet: se α è irrazionale, $\exists$ infiniti

⌞ p/q : $|\alpha - p/q| < 1/q^2$

Applichiamolo ad $\alpha = \sqrt{d}$

$(x - \sqrt{d}y)(x + \sqrt{d}y) = N$

tende a 0 tende a ∞

$x - \sqrt{d}y \approx 0 \iff x/y \approx \sqrt{d}$

Dirichlet $\Rightarrow$ esistono infiniti p/q t.c.

$|\sqrt{d} - p/q| < 1/q^2$

$$|N(p+\sqrt{d}\,q)| = |(p+\sqrt{d}\,q)(p/q-\sqrt{d})\cdot q|$$

$$< 1/q^2 \cdot q \cdot |p+\sqrt{d}\,q|$$

$$= |p/q+\sqrt{d}| \le 2\sqrt{d} + 1/q^2$$

$$\le 2\sqrt{d}+1$$

Per Pigeonhole, trovo infinite coppie (p,q) t.c. $N(p+\sqrt{d}\,q) = N$, per almeno un N tra $-2\sqrt{d}-1$ e $2\sqrt{d}+1$.

Tra questi, $\exists\ (p_1,q_1)$ e (p_2,q_2) con $p_1 \equiv p_2$ e $q_1 \equiv q_2 \pmod N$: il loro rapporto è intero ed ha norma 1.

$(p_1,q_1) \neq (p_2,q_2)$ $\quad p_1, q_1, p_2, q_2 > 0$

Se z è una soluzione $\neq 1$, allora
$\| \quad x + \sqrt{d}\, y$

$$N(z^n) = N(z)^n = 1$$

e quindi z^n è una soluzione.

Lo stesso vale per $(-z^n)$: infatti

$$N(-z^n) = N(-1)\, N(z^n) = N(-1 + 0\sqrt{d}) = 1$$

Soluzione fondamentale f

È il minimo $z > 1$ tale che $N(z) = 1$

Oss: $\frac{1}{z} = \frac{1}{x+\sqrt{d}y} \cdot \frac{x-\sqrt{d}y}{x-\sqrt{d}y} = \frac{x-\sqrt{d}y}{1}$

Hope Tutte le soluzioni sono della forma $\pm f^n$, dove n è un intero (non necessariamente positivo)

Dim. Sia z una soluz. Sostituendo z con $-z$ possiamo supporre $z > 0$.

Esiste un unico n t.c. $f^n \le z < f^{n+1}$

$N(\underbrace{z \cdot f^{-n}}_{a+b\sqrt{d},\ a \in \mathbb{Z},\ b \in \mathbb{Z}}) = 1$

$|a+b\sqrt{d}| = |z| \cdot |f|^{-n} < f$

≤ 1

Per definiz. di f, $z \cdot f^{-n} = 1 \Rightarrow z = f^n$ ∎

Esempio $x^2 - 3y^2 = 1$

Cerchiamo (x,y) più piccoli possibile.

$y = 0 \Rightarrow x = 1$ NO

$y = 1 \Rightarrow x = \pm 2$ $\quad f = 2 + \sqrt{3}$

f^2 è soluzione: $\quad f^2 = 4 + 3 + 4\sqrt{3}$

$(x, y) = (7, 4)$

Tutte le soluzioni sono della forma

$$\pm (2+\sqrt{3})^n$$

ovvero

$$x = \frac{(2+\sqrt{3})^n + (2-\sqrt{3})^n}{2}$$

$$y = \frac{(2+\sqrt{3})^n - (2-\sqrt{3})^n}{2\sqrt{3}}$$

Trovare la fondamentale

$$x^2 - 7y^2 = 1$$

$$\frac{2}{1} < \sqrt{7} < \frac{3}{1}$$

$$\frac{2}{1} \oplus \frac{3}{1} = \frac{5}{2} \qquad \frac{5}{2} < \sqrt{7} < \frac{3}{1}$$

$$\frac{5}{2} \oplus \frac{3}{1} = \frac{8}{3} \qquad 8^2 - 7 \cdot 3^2 = 1$$

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d} \qquad \text{(FAREY)}$$

Algoritmo Si parte da $\frac{n}{1} < \sqrt{d} < \frac{n+1}{1}$, con n intero.

Ad ogni passo abbiamo una disuguaglianza $a/b < \sqrt{d} < e/f$. Proviamo se

$$a^2 - db^2 = 1 \quad \text{o} \quad e^2 - df^2 = 1$$

Se sì, fine. Se no, consideriamo $\frac{a+e}{b+f}$ e otteniamo una nuova disug.

$$\frac{a+e}{b+f} < \sqrt{d} < \frac{e}{f} \quad \text{oppure} \quad \frac{a}{b} < \sqrt{d} < \frac{a+e}{b+f}$$

Esercizio Se $(m+1)^3 - m^3 = n^2$, allora

$2n-1$ è un quadrato

$3m^2+3m+1 = n^2$

$3\left(m+\frac{1}{2}\right)^2 + \frac{1}{4} = n^2$

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

$(2n, 2m+1)$ è una sol.ne di $x^2 - 3y^2 = 1$

$2n + (2m+1)\sqrt{3} = (2+\sqrt{3})^k$

k è dispari, altrimenti $\frac{(2+\sqrt{3})^k + (2-\sqrt{3})^k}{2}$

è dispari

$$2n-1 = \frac{(2+\sqrt{3})^k + (2-\sqrt{3})^k - 2}{2}$$

$$= \frac{2(2+\sqrt{3})(2+\sqrt{3})^{k-1} + 2(2-\sqrt{3})(2-\sqrt{3})^{k-1} - 2\cdot 2}{2\cdot 2}$$

Oss $(1+\sqrt{3})^2 = 4 + 2\sqrt{3} = 2(2+\sqrt{3})$

$$2n-1 = \left(\frac{(1+\sqrt{3})(2+\sqrt{3})^{(k-1)/2} + (1-\sqrt{3})(2-\sqrt{3})^{\frac{k-1}{2}}}{2}\right)^2$$

Pell generalizzate

(*) $x^2 - dy^2 = m \iff N(x + \sqrt{d}\, y) = m$

E' comunque importante studiare $x^2 - dy^2 = 1$.

Sia f la fondamentale.

(1) Se z e' una soluzione di (*), allora $\pm z \cdot f^n$ sono tutte soluzioni:

$$N(z \cdot f^n) = \underbrace{N(z)}_{m} \cdot \underbrace{N(f)^n}_{1} = m$$

(2) $z = x + \sqrt{d}\, y \rightsquigarrow$ **$x/y \bmod m$**

Esistono al piu' $\varphi(|m|)$ soluzioni

$z_1, \dots, z_k \quad (k \le \varphi(|m|))$

tali che ogni soluzione sia della forma

$$\pm z_i \cdot f^n$$

(3) $x/y \bmod m$ ha senso solo se $1 = (y, m)$

Altrimenti c'e' p che divide x, y, m

Se $m = -1$ o ± 2 c'e' al piu' una famiglia di soluzioni.

Problema: come decido se $x^2 - 82y^2 = 2$ ha o meno soluzioni?

Prendiamo uno z t.c. $N(z) = m$

Moltiplicando per f^n con n opportuno trovo un'altra soluzione nell'intervallo

$$\left[\sqrt{\frac{|m|}{f}}, \sqrt{|m|} \cdot \sqrt{f} \right]$$

$$x = \frac{z + \bar{z}}{2} = \frac{z + m/z}{2}$$

$z = x + y\sqrt{d}$

$\bar{z} = x - y\sqrt{d}$

$z\bar{z} = N(z) = x^2 - dy^2 = m$

Diciamo $m > 0$. La funzione

$$z \longmapsto \frac{z + m/z}{2}$$

è convessa, quindi il suo massimo sta in un estremo. Negli estremi questa funzione vale $\frac{1}{2}\left(\sqrt{|m| \cdot f} + \sqrt{\frac{|m|}{f}} \right)$

$$= \frac{f+1}{2\sqrt{f}} \cdot \sqrt{|m|}$$

Caso concreto $x^2 - 82y^2 = 2$

$x^2 - 82y^2 = 1$

$N(9 + \sqrt{82}) = (9+\sqrt{82})(9-\sqrt{82})$

$= 81 - 82 = -1$

$\Rightarrow N((9+\sqrt{82})^2) = +1$

$N(81 + 82 + 18\sqrt{82}) = N(163 + 18\sqrt{82})$

$f < 343$

Fatto di pagina prima $\Rightarrow$ se c'è una soluz., ce n'è una in cui $x \leq \frac{f+1}{2\sqrt{f}}\sqrt{2}$

$\leq \frac{1}{2}\frac{344}{18}\frac{3}{2} < 15$ (172, 6)

Mod 41 $\Longrightarrow$ $x^2 - 82y^2 \equiv 2 \ (41)$

$x^2 \equiv 2 \ (41)$

$\Downarrow$

$x \equiv \pm 17 \ (41)$

Un tale x non esiste!

Aside Se $p \equiv 3 \pmod 4$ e $\left(\frac{a}{p}\right) = +1$, allora le radici quadrate di a mod p sono date da $\pm a^{\frac{p+1}{4}}$

$$\left(a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a^{\frac{p-1}{2}+1} \equiv \underbrace{a^{\frac{p-1}{2}}}_{\left(\frac{a}{p}\right)=+1} \cdot a$$

Sia $a \in \mathbb{N}$ e $d = a^2 - 1$. Se x, y sono tali che $m = x^2 - dy^2$ e' (in valore assoluto) $< 2a+2$, allora $|m|$ e' un quadrato perfetto.

Prendiamo dei tali x, y con x il piu' piccolo possibile.

Fondamentale = soluz. di $x^2 - (a^2-1)y^2 = 1$ più piccola $= a + \sqrt{d}$

$$x \leq \frac{f+1}{2\sqrt{f}} \cdot \sqrt{|m|} = \sqrt{\frac{a+1}{2}} \sqrt{|m|}$$

$$\Leftrightarrow \frac{(f+1)^2}{4f} = \frac{a+1}{2}$$

$$\Leftrightarrow \left(a^2 + a^2 - 1 + 2a\sqrt{d} + 1 + 2a + 2\sqrt{d}\right) \stackrel{?}{=} 2f(a+1)$$

$$\Leftrightarrow 2a^2 + 2a\sqrt{d} + 2a + 2\sqrt{d} \stackrel{?}{=} 2f(a+1) \qquad \square$$

$$x \leq \sqrt{\frac{a+1}{2}}\sqrt{|m|} < \sqrt{\frac{a+1}{2}}\sqrt{2(a+1)}$$

$$= a+1$$

$$x^2 - dy^2 = 1$$

$$dy^2 = x^2 - 1 \leq a^2 - 1$$

$$y^2 \leq \frac{a^2-1}{d} = 1$$

Quindi esistono $x \leq a$ e $y \in \{0, 1\}$ t.c.

$$m = x^2 - dy^2$$

Per $y = 0 \Rightarrow m = x^2$

Per $y = 1 \Rightarrow \begin{cases} m = x^2 - (a^2-1) \\ x = a \end{cases} \Rightarrow m = 1$

□

$3^n - 2$ è un quadrato $\iff$ $n = 1, 3$

Mod 4 $\Rightarrow$ n è dispari

$$3^n - 2 = y^2 \qquad 3x^2 - 2 = y^2$$

$$(*)\ y^2 - 3x^2 = -2$$

$\varphi(|-2|) = 1$: una famiglia di soluzioni

$$N(1+\sqrt{3}) = -2$$

Fondamentale: $y^2 - 3x^2 = 1$ $\qquad f = 2+\sqrt{3}$

Tutte le soluzioni (positive) della (*) sono

$$y + x\sqrt{3} = (1+\sqrt{3})(2+\sqrt{3})^\ell$$

x dev'essere una potenza di 3. Guardiamo mod 9.

$$x_\ell = \frac{(1+\sqrt{3})(2+\sqrt{3})^\ell - (1-\sqrt{3})(2-\sqrt{3})^\ell}{2\sqrt{3}}$$

$$= \frac{(1+\sqrt{3})^{2\ell+1} - (1-\sqrt{3})^{2\ell+1}}{2\sqrt{3}\cdot 2^\ell}$$

$$b_\ell = 2^\ell x_\ell$$

$$X \equiv (2\ell+1) + \frac{(2\ell+1)(2\ell)(2\ell-1)}{6} \cdot 3 \bmod g$$

$$\equiv (2\ell+1)\underbrace{\left(1 + \ell(2\ell-1)\right)}_{\not\equiv 0 \ (3)} \bmod g$$

$$\Rightarrow \ell \equiv 4 \bmod g$$

b_ℓ è una potenza di 3 $\Rightarrow \ell \equiv 4 (g)$

$$\Rightarrow b_g \mid b_\ell$$

Se b_g non è una potenza di 3, lo stesso vale per X_ℓ.

(e non per colpa dei fattori 2!)

Sia $a = (1+\sqrt{3})^g$ e $b = (1-\sqrt{3})^g$

Mi chiedo se $\frac{a-b}{2\sqrt{3}}$ divida $\frac{a^n - b^n}{2\sqrt{3}}$

Funziona perché il rapporto è

$$\underbrace{a^{n-1}}_{\text{intero}} + a^{n-2}b + \dots + \underbrace{b^{n-1}}_{\text{intero}}$$

$$a^{n-2}b + b^{n-2}a = \text{intero}$$

$$(1+\sqrt{3})^3 = (1+3\cdot 3) + \sqrt{3}\,(3+3)$$

$$= (10+6\sqrt{3})$$

$$(10+6\sqrt{3})^3 = 8\,(5+3\sqrt{3})^3 = \dots$$

Alla fine, $X_9 = 9\cdot 17$, quindi X_ℓ non è una potenza di 3

$$\sum_{k \mid n} \varphi(k) = n$$

Verifichiamola se $n = p^m$

$$\sum_{k \mid p^m} \varphi(k) = \sum_{j=0}^{m} \varphi(p^j) =$$

$$= 1 + \sum_{j=1}^{m} (p-1)\, p^{j-1}$$

$$= 1 + (p-1) \sum_{j=0}^{m-1} p^j =$$

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

$$\sum_{k \mid ab} \varphi(k) = \sum_{\substack{k_1 \mid a \\ k_2 \mid b}} \varphi(k_1 k_2)$$

$(a,b) = 1$

$$= \sum_{\substack{k_1 \mid a \\ k_2 \mid b}} \varphi(k_1)\,\varphi(k_2)$$

$$= \underbrace{\left(\sum_{k_1 \mid a} \varphi(k_1) \right)}_{a} \underbrace{\left(\sum_{k_2 \mid b} \varphi(k_2) \right)}_{b}$$