Stage Senior 2017 – Livello Medium

Stampato integrale delle lezioni

Autori vari

Indice

Senior 2017 - A1 MEDIUM Anér

Note Title 9/4/2017

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

Def. Un anello è un insieme con due operazioni, $+$ e $\cdot$, con le proprietà che vi aspettate, in particolare

- oltre a $+$ ho anche $-$
- non assumo la divisione

Esempi $\mathbb{Z}$ è l'anello degli interi

$\boxed{\mathbb{Q}, \mathbb{R}, \mathbb{C}}$ sono anelli (di un tipo particolare)

$\mathbb{Z}/n\mathbb{Z}$ è un anello

Esempio/costruzione Se A è un anello, posso definire $A[x] \overset{\text{definizione}}{=} \{$polinomi in x con coefficienti in $A\}$

Def Un campo è un anello in cui ogni elemento $\neq 0$ ammette un inverso molt.

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono campi

oss In $\mathbb{Z}$ vale la legge di annullamento del prodotto: se m e $n \neq 0$, allora $mn \neq 0$

OSS $\mathbb{Z}/10\mathbb{Z}$, per esempio, non ha questa proprietà

$\mathbb{Z}$ è un dominio

Esempio $\mathbb{R}[x]$ è un dominio, come $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{C}[x]$

Posso costruire le frazioni con num. e den. $(\neq 0)$ in un dominio A, e questo sarà un campo. $C(A)$

Filosofia A è un dominio, e_i ed e_f elementi di A.

$$\underset{\substack{\cup\\ A}}{e_i} = \underset{\substack{\cup\\ C(A)}}{f_1} = f_2 = f_3 = \ldots = f_n = e_f$$

Domanda Esistono anelli $\mathbb{Z} \subsetneq A \subsetneq \mathbb{Q}$?

- $A = \left\{ \text{frazioni del tipo } \frac{n}{2^k} \right\}$ razionali diadici

- $A = \left\{ \text{'' \quad ''} \quad \frac{n}{2^k \cdot 3^h} \right\}$

x CASA Gli anelli "tra $\mathbb{Z}$ e $\mathbb{Q}$" sono tutti così: Dato $S \subseteq$ numeri primi, costruiamo

$A = \mathbb{Z}[S^{-1}] = \{$fraz. in cui il den. si fattorizza in $S\}$

Esempio Polinomi di Laurent

$\mathbb{C}[x, x^{-1}] = \{$ scritture del tipo

$$a_{-m}x^{-m} + a_{-m+1}x^{-m+1} + \ldots + a_0 + \ldots + a_n x^n \}$$

$= \{$ frazioni algebriche della forma $\dfrac{p(x)}{x^m}$ $\}$

$$\mathbb{C}[x] \subset \mathbb{C}[x, x^{-1}] \subset C(\mathbb{C}[x]) = \mathbb{C}(x)$$

Se A è un dominio, anche $A[x]$ è un dominio cioè se $p(x), q(x)$ sono polinomi non nulli a coeff. in A, anche $p(x) \cdot p(x) \neq 0 \Rightarrow$ guardo i coefficienti direttivi.

Divisione euclidea 1° caso (noto) i coeff. in un campo C ad esempio $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

$p(x), q(x) \in C[x]$ voglio trovare $r(x)$ e $s(x)$ t.c. $p(x) = q(x) \cdot s(x) + r(x)$ e $\deg r < \deg q$ (oppure $r(x) = 0$)

$$p(x) = a_n x^n + \ldots + a_0$$
$$q(x) = b_m x^m + \ldots + b_0$$

supponiamo $n > m$

divido $\dfrac{a_n}{b_m}$, e comincio a sottrarre

$$\left(\frac{a_n}{b_m}\right) \cdot x^{n-m} \cdot q(x) \text{ a } p(x)$$

2° caso coeff. in un dominio: allargo gli orizzonti e lavoro nel campo delle frazioni (e comunque tutti i denominatori saranno potenze di b_m)

3° caso coeff. in un anello, se il divisore è monico tutto va bene!

Cosa fare con pol. in più variabili?

$\mathbb{C}[x,y]$ $\quad p(x,y) = x^2+y^2 \quad q(x,y) = x^2+xy$

Div. risp. alla x $\quad p(x,y) = q(x,y)\cdot 1 + (y^2-xy)$

Div. risp. alla y $\quad p(x,y) = q(x,y)\cdot \dfrac{y}{x} + (x^2-xy)$

Problema $p(x,y)$ coeff. reali; $\forall n \in \mathbb{N}$ $p(n,n^2)=0$. Allora p è un multiplo di $y-x^2$.

Divido p per $y-x^2$ usando y come var. principale

$$p(x,y) = s(x,y)\cdot(y-x^2) + r(x,y)$$

$r(x,y)$ ha grado 0 in $y \rightsquigarrow r(x,y) = R(x)$

$R(n)=0$ $\forall n$ naturale, ma un polinomio a coeff. reali non ha infinite radici!

$R(x)\equiv 0$ e abbiamo finito.

Teo Un polin. $p(x) \in \mathbb{R}[x]$ di grado n ha al massimo n radici distinte.

$p(x)$ se α è radice divido per $(x-\alpha)$, il resto ha grado 0, è un numero, e deve essere 0

$p(x) = (x-\alpha) \cdot p_1(x)$. Prendo β un'altra radice (diversa da α). Poiché $\beta - \alpha \neq 0$, serve $p_1(\beta)=0$ e parte l'induzione...

OSS Lo stesso argomento vale in un campo qualsiasi e perfino in un dominio!

Ma non in un non-dominio!

Se A non è un dominio (esempio $A = \mathbb{Z}/10\mathbb{Z}$)

prendo $a, b \neq 0$ con $a \cdot b = 0$ (esempio $a=2$ $b=5$, $a \cdot b = 10 = 0$)

considero $(x-a)(x-b)$: ha radici

$a, b, 0, a+b$ (nel nostro esempio $2, 5, 0, 7$)

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

Antefatto $(x-y) \mid [p(x) - p(y)]$ dove

$p(t) \in \mathbb{R}[t]$ è un pol. in una variabile

Infatti: $p(t) = a_n t^n + \ldots + a_0$

$p(x) - p(y) = a_n(x^n - y^n) + \dots + a_1(x-y)$

<u>Problema x casa</u> $p(t), q(t) \in \mathbb{R}[t]$;

$[p(x)-p(y)] \mid [q(x)-q(y)]$. Allora $\exists\, r(t) \in \mathbb{R}[t]$

t.c. $q(t) = r(p(t))$

Un polinomio $p(x)$ in $A[x]$ è irriducibile se <u>non</u> esistono $p_1(x), p_2(x)$ di grado > 0 t.c.

$p(x) = p_1(x) \cdot p_2(x)$ (supponiamo A dominio)

<u>Teo</u> Ogni polinomio in $A[x]$ ammette un'unica fattorizzazione in irriducibili a meno di permutazioni e riscalamenti dei fattori, per i seguenti A: $\mathbb{Z}$, campi. Vero anche per $A[x,y]$, $A[x,y,z]$, ...

<u>Esempi</u> • $\mathbb{C}[x]$ qui avrò fattori di grado 1

• $\mathbb{R}[x]$ // /// / 1 o 2

• $\mathbb{Q}[x]$ // / / / / qualsiasi

• $\mathbb{Z}[x]$ / / / / qualsiasi

<u>Lemma di Gauss</u> Se $p(x) \in \mathbb{Z}[x]$ è un polin.

a coeff. interi (e quindi razionali), allora la fattoriz. in irriducibili in $\mathbb{Z}$ e in $\mathbb{Q}$ sono uguali a meno di riscalamento.

<u>Esempio</u> $(2x+1)(x+2) = 2x^2+5x+2 = \left(x+\frac{1}{2}\right)(2x+4)$

Quindi passando da $\mathbb{Z}$ a $\mathbb{Q}$ le possibilità di fattorizzazione non migliorano

---

Radici razionali di $p(x) \in \mathbb{Z}[x]$: come cercarle?

$p(x) = a_n x^n + \ldots + a_0$ e $\frac{a}{b}$ è radice di p

$(a,b)=1$, allora $a \mid a_0$ e $b \mid a_n$

Per dim. che p è irriducibile ho i seguenti mezzi:

- ridurre modulo n (modulo un primo): se $p(x)$ considerato modulo n è irriducibile, allora a maggior ragione p sarà irriducibile. Al contrario

$p(x)$ a coeff. interi. $p(x) = q(x) \cdot r(x)$ a coeff. interi

$p(x) \equiv q(x) \cdot r(x) \mod n$ (cioè come polinomi a coeff. in $\mathbb{Z}/n\mathbb{Z}$)

<u>Esempio</u> $x^3 - 4$ è irriducibile: infatti è irrid. mod 7 (se si fattorizzasse avrebbe un fattore lineare, ma allora 4 sarebbe residuo cubico mod 7, assurdo!)

- Eisenstein. Preliminare: $\mathbb{Z}/n\mathbb{Z}$ non è un dominio se n non è un primo, ma $\mathbb{Z}/p\mathbb{Z}$ è un campo!

Sia $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$

p primo $p \nmid a_n$, $p \mid a_{n-1}, \dots a_1, a_0$

$p^2 \nmid a_0$. Allora f è irriducibile.

<u>Esempio</u> $x^{10} - 10$

<u>Dim</u> Suppongo per assurdo $f(x) = g(x) \cdot h(x)$ in $\mathbb{Z}[x]$

mod p ho $a_n x^n \equiv g(x) \cdot h(x) \pmod{p}$

Per la fattorizzazione unica in $\mathbb{Z}/p\mathbb{Z}[x]$ (infatti $\mathbb{Z}/p\mathbb{Z}$ è un campo) ho che

$g(x) \equiv b x^m \quad h(x) \equiv c x^l \quad \text{mod } p$

$m, l > 0$. Allora $p \mid$ termini noti di g e h, il cui prodotto è a_0, che però non è div. per p^2.

- Terza via: ridurre a un numero finito di tentativi e provarli tutti. Dato $p(x) \in \mathbb{Z}[x]$, un suo divisore ha grado limitato da $\deg p$, ma i coefficienti?

<u>PASSO 1</u> Capire quanto grandi (in modulo) sono le radici complesse di p, usando i coeff. di p

Per semplificare, supponiamo p monico $p(x) = x^n + a_{n-1}x^{n-1} + \dots a_0$

Se $\alpha \in \mathbb{C}$ è radice di p, serve per la triangolare

$$|\alpha|^n \le |a_{n-1}||\alpha|^{n-1} + \dots + |a_1|\cdot|\alpha| + |a_0|$$

PASSO 2 Stimare i moduli dei coeff. di un div. di p avendo una stima sui moduli delle radici di p

$$q(x) = x^m + b_{m-1}x^{m-1} + \dots + b_0 \quad \text{divide } p.$$

Le radici di q sono anche radici di p, in modulo $< N$

$b_0 =$ prodotto radici $\quad |b_0| < N^m$

$b_{m-1} =$ somma radici $\quad |b_{m-1}| < m \cdot N$

Bezout per polinomi in $C[x]$ $\quad$ C un campo.

$p(x)$, $q(x)$ pol. senza fattori irriducibili in comune.

Allora esistono $a(x), b(x) \in C[x]$ per cui

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

Si usa la divisione euclidea, quindi serve dividere per i coefficienti che di volta in volta si presentano

Esempio $\quad p(x) = x^2 - 2 \qquad q(x) = x$

$$p(x) = q(x)\cdot x \underbrace{-2}_{r(x)} \qquad q(x) = (-2)\cdot \frac{-1}{2}x + 0$$

$$-\frac{1}{2}p(x) + \frac{1}{2}\cancel{x}\,q(x) = 1 \rightsquigarrow -p(x) + x\,q(x) = 2$$

Esempio Proviamo con $\mathbb{C}[x,y]$ $p(x,y)=x$
$q(x,y)=y$. Esistono $a(x,y)$, $b(x,y)$ t.c.
$a(x,y)\cdot x + b(x,y)\cdot y = 1$? NO perché
a sinistra manca il termine noto
porre $(x,y)=(0,0)$

- $p = x-1$ $q = y-1$

$$a(x,y)(x-1) + b(x,y)(y-1) = 1 \quad ?$$

No perché ponendo $(x,y)=(1,1)$

In generale se esistono x_0, y_0 complessi t.c. $p(x_0,y_0)=q(x_0,y_0) = 0$
allora non esistono $a(x,y)$, $b(x,y)$ come sopra!

Teo (Hilbert Nullstellensatz) Se $p(x,y)$ e $q(x,y)$ non si annullano simultaneamente su una coppia di complessi (x_0,y_0), allora esistono $a(x,y)$ e $b(x,y)$ come in Bezout. Vale anche per più polinomi e più variabili. Esempio p_1, p_2, p_3, p_4 polinomi in $\mathbb{C}[x,y,z]$. Allora o esiste (x_0,y_0,z_0) che annulla tutti i p_i, oppure esistono polinomi $a_1 \dots a_4 \in \mathbb{C}[x,y,z]$ t.c. $a_1 \cdot p_1 + a_2 \cdot p_2 + a_3 \cdot p_3 + a_4 p_4 = 1$

Serve coeff. in $\mathbb{C}$: coeff. reali non funziona!
$p(x,y) = x^2+y^2+1$ Esiste $a(x,y)$ t.c. $a(x,y)\cdot p(x,y)=1$
No perché p ha zeri complessi, anche se

non reali!

Caso ancora più semplice: una variabile: $p(x) = x^2+1$

Serve un campo per cui vale il teorema fond. dell'algebra! (E in effetti basta).

Derivate $\quad p(x) = a_n x^n + \dots + a_0$

$$p'(x) = \frac{d}{dx} p(x) = n \cdot a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1$$

Proprietà fondamentali

① Linearità $\frac{d}{dx}\left[p(x) + q(x)\right] = \frac{d}{dx} p(x) + \frac{d}{dx} q(x)$

Ⓑ λ è una costante nell'anello

$$\frac{d}{dx}\left(\lambda \cdot p(x)\right) = \lambda \left(\frac{d}{dx} p(x)\right)$$

② Regola di Leibniz: $\frac{d}{dx}\left(p(x) \cdot q(x)\right) = \left(\frac{d}{dx} p(x)\right) \cdot q(x) + p(x) \cdot \left[\frac{d}{dx} q(x)\right]$

③ $\frac{d}{dx} x = 1$

Proprietà ①, ②, ③ determinano $\frac{d}{dx}$ univocamente

La derivata abbassa il grado $\rightsquigarrow$ permette dim. per induzione sul grado. Ci sono anche altre operazioni che abbassano il grado ...

① Divido per $(x-\alpha)$ dove α è una radice

② Tolgo il termine noto e divido per x

③ $p(x+1)-p(x)$ ha grado minore

① $\dfrac{p(x)}{(x-\alpha)} = \dfrac{p(x)-p(\alpha)}{x-\alpha}$

② $\dfrac{p(x)-a_0}{x} = \dfrac{p(x)-p(0)}{x-0}$

③ $\dfrac{p(x+1)-p(x)}{(x+1)-x}$

$p(x) \in \mathbb{C}[x]$. α è radice doppia di $p(x)$ se e solo se α è radice di $p(x)$ e anche di $p'(x)$

Scrivo $p(x)=(x-\alpha)\cdot q(x)$. Allora

$$p'(x) = 1\cdot q(x) + (x-\alpha)\cdot q'(x)$$

A che serve? Se ad esempio vogliamo che $p(x)$ sia il $\square$ di un polinomio, è necessario che ogni radice di p compaia almeno 2 volte ...

$$p(x) = (x-\alpha_1)(x-\alpha_2)\cdot\ldots\cdot(x-\alpha_n)$$

$$\frac{d}{dx}p(x) = \sum_{i=1}^{n}(x-\alpha_1)\ldots(x-\alpha_{i-1})\cdot 1\cdot(x-\alpha_{i+1})\cdot\ldots(x-\alpha_n)$$

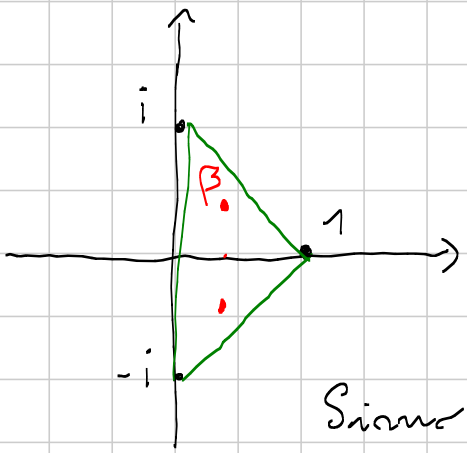
$$= \sum_{i=1}^{n}\frac{p(x)}{x-\alpha_i}$$

Esempio in $\mathbb{C}$ $\quad p(x) = (x^2+1)(x-1) = x^3 - x^2 + x - 1$

$p'(x) = 3x^2 - 2x + 1$

le radici di p' sono

$\frac{1}{3} \pm \frac{\sqrt{2}}{3} i$



Le radici di p' sono nell'inv. convesso di quelle di p (dentro $\mathbb{C}$)

Verifichiamolo!

Siano $\alpha_1, \dots, \alpha_n$ le radici di p

Sia β una radice di p'.

OSS 0 è radice di $p'(x+\beta)$. WLOG (con le dovute verifiche...) $\beta = 0$ a meno di traslare

$$p'(x) = \sum_{i=1}^{n} \frac{p(x)}{x-\alpha_i} \qquad \text{pongo } x = 0$$

$$0 = \sum \frac{p(0)}{-\alpha_i} = -p(0) \cdot \sum \frac{1}{\alpha_i}.$$

Trattiamo il caso $p(0) \neq 0$, ossia $\beta = 0$ non è già radice di p.

$$\sum \frac{1}{\alpha_i} = 0 \qquad \sum \frac{\overline{\alpha_i}}{\overline{\alpha_i} \cdot \alpha_i} = 0 \quad \text{coniugo tutto}$$

$$\sum \frac{\alpha_i}{|\alpha_i|^2} = 0 \qquad \text{Se } \sum \frac{1}{|\alpha_i|^2} = 1 \text{ ho finito,}$$

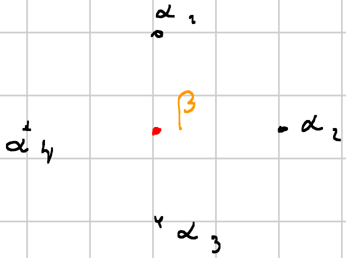
altrimenti divido!

$$\sum_{i=1}^{n} \alpha_i \cdot \boxed{\frac{\frac{1}{|\alpha_i|^2}}{\sum_{j=1}^{n} \frac{1}{|\alpha_j|^2}}} = 0 \qquad > 0$$

la somma dei coeff non è 1

Risultato: $\beta = 0 = \sum_{i=1}^{n} \lambda_i \alpha_i$ con $\lambda_i > 0$, $\sum \lambda_i = 1$

Esempio



$$\beta = \frac{1}{2}\alpha_1 + \frac{1}{2}\alpha_3$$
$$= \frac{1}{2}\alpha_2 + \frac{1}{2}\alpha_4$$

Algebra 2 — Disuguaglianze M

Note Title 9/5/2017

Scambret

- → Ripasso
- → Convessità
- → (Forte) ABC
- → Disuguaglianze tra frazioni (CS)
- → Disuguaglianze tra radici

— o — o —

Ripasso

Riarrangiamento

$a_1 \le a_2 \le \dots \le a_n$
$b_1 \le b_2 \le \dots \le b_n$

$$S = \sum a_i b_{\sigma(i)} \qquad \sigma : \{1, \dots, n\} \to \{1, \dots, n\}$$

max $\sigma(i) = i$

min $\sigma(i) = n+1-i$

Dim $\exists \hat{\sigma}$ (Esiste?) e vogliamo trovare il max

$$j > i \qquad \hat{\sigma}(j) < \hat{\sigma}(i)$$

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

Ex $x_1, \dots, x_n > 0$

$$\sum_{i=1}^{n} \frac{x_i}{x_{i+1}} \geq n \qquad e \quad x_{n+1} = x_1$$

wlog $x_1 \geq x_2 \geq \dots \geq x_n$ NO!!!

$$\frac{1}{x_1} \leq \dots \leq \frac{1}{x_n}$$

$y_1 = \max\{x_i\}$

$y_2 = 2^\circ$ più grande $\{x_i\}$

$\vdots$

$y_n = \min\{x_i\}$

$$y_1 \geq \dots \geq y_n$$

$$\frac{1}{y_1} \leq \dots \leq \frac{1}{y_n} \qquad n \leq \sum y_i \cdot \frac{1}{y_{\sigma(i)}}$$

$\blacksquare$

$$a_1 \leq \dots \leq a_n, \qquad b_1 \leq \dots \leq b_n$$

$$\left(\frac{1}{n}\sum a_i\right) \cdot \left(\frac{1}{n}\sum b_i\right) \leq \frac{1}{n}\sum a_i b_i$$

Dim

$$a_1b_1 + a_2b_2 + \dots + a_nb_n \geq a_1b_1 + \dots + a_nb_n$$

$$a_1b_1 + \dots + a_nb_n \overset{!}{\geq} a_1b_2 + a_2b_3 + \dots + a_nb_1$$

$$\sum a_ib_i \geq \sum a_ib_{i+k}$$

$$n\sum a_i b_i \geq \left(\sum a_i\right)\left(\sum b_i\right)$$

CS $\quad a, b$ con componenti in $\mathbb{R}$

$$\left(\sum a_i b_i\right)^2 \leq \left(\sum a_i^2\right)\left(\sum b_i^2\right)$$

$$\left(\sum a_i b_i c_i\right)^3 \leq \_\ \_\ \_ \qquad \text{NO!}$$

$$3\cancel{abc} \leq a^3+b^3+c^3 \qquad b=0 \leftarrow$$

$$2ab \leq a^2+b^2 \leftarrow$$

Dim

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

$$= x^2 \sum b_i^2 + 2x \sum a_i b_i + \sum a_i^2 \geq 0$$

$$\Delta = \left(\sum a_i b_i\right)^2 - \sum a_i^2 \sum b_i^2 \leq 0$$

ii) $$\left(\sum a_i^2\right)\left(\sum b_i^2\right) - \left(\sum a_i b_i\right)^2$$

$$= \boxed{\sum_{1 \leq i < j \leq n} (a_i b_j - a_j b_i)^2} \geq 0$$

iii) $$\left(\sum a_i b_i\right)^2 \leq \left(\sum a_i^2\right)\left(\sum b_i^2\right)$$

$\lambda, (a_1, \dots, a_n), \mu (b_1, \dots, b_n) \qquad \lambda^2 \mu^2 \text{ LHS} \leq \lambda^2 \mu^2 \text{ RHS}$

wlog $\quad \sum a_i^2 = \sum b_i^2 = 1 \quad \rightsquigarrow \quad \sum a_i b_i \leq 1$

$$ab \le \frac{a^2+b^2}{2}$$

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

AGGIUSTARE I DETTAGLI

$$ab \le \frac{1}{p}a^p + \frac{1}{q}b^q \qquad \text{Young} \left(\frac{1}{p}+\frac{1}{q}=1\right)$$

$p, q > 1$

Parenti $\quad a, b, c$ positivi

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

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

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

$p, q > 1$

$$\frac{a+b}{2} \ge \sqrt{ab}$$

$$a_i = \frac{c_i}{\sqrt{d_i}} \qquad b_i = \sqrt{d_i}$$

e ottenete il Lemma di Titu !!!

— o — o —

Medie $\quad a_1, \dots, a_n > 0 \quad , p \in \mathbb{R}$

$$f(p) = \sqrt[p]{\frac{a_1^p + \dots + a_n^p}{n}} = M_p$$

"Definiamo"
- $p = +\infty \quad f(p) = \max\{a_i\}$
- $p = -\infty \quad f(p) = \min\{a_i\}$
- $p = 0 \quad GM$

$p > q \Rightarrow f(p) > f(q)$

Dim + $AM \geq GM$ (e questo qui sistema il confronto p contro 0)

* $AM \leq M_p$ $p \geq 1$ (questo sistema p contro q, $p, q \neq 0$)

$AM \geq GM$ 1) Induzione $n=2$ ok!

$n=2$ $n \Rightarrow 2n$!!! $2 \to 4 \to 8 \to 16 \to 15 \to 14 \to 13$

$n \Rightarrow n-1$

Tizio fittizio

$$\left(a_1, \dots, a_{n-1}, \frac{a_1 + \dots + a_{n-1}}{n-1} \right)$$

$b_1, \dots, b_{n-1}, b_n$

$$\frac{b_1 + \dots + b_n}{n} \geq \sqrt[n]{b_1 \cdots b_n} \Rightarrow$$

$b_n = AM_{n-1}$

$AM_{n-1} \geq GM_{n-1}$

II) Jensen $f\left(\sum \lambda_i x_i\right) \leq \sum \lambda_i f(x_i)$ f convessa

$\sum \lambda_i = 1$

$\lambda_i = \frac{1}{n}$ $f(x) = \log x$

$$f\left(\sum \frac{x_i}{n}\right) \geq \frac{1}{n} \sum f(x_i)$$

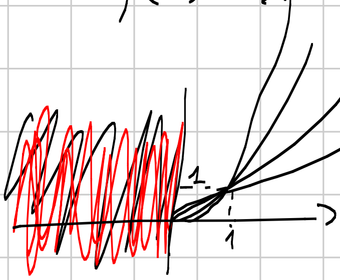
$$\log\left(\frac{x_1 + \dots + x_n}{n}\right) \geq \frac{\log x_1 + \dots + \log x_n}{n} \overset{!}{=} \frac{\log(x_1 \cdots x_n)}{n} \overset{!}{=} \log(x_1 \cdots x_n)^{\frac{1}{n}}$$

$$\overset{!}{\Longrightarrow} \frac{x_1 + \dots + x_n}{n} \geq \sqrt[n]{x_1 \cdots x_n}$$

— o — o —

$AM \leq M_p \qquad p \geq 1$

Jensen $\quad f(x) = x^p \quad$ f convessa



— o — o —

Bunching / Schur

$K \succ N \qquad k_1 \geq \dots \geq k_m$, $\quad n_1 \geq \dots \geq n_m$

$k_1 \geq n_1$

$k_2 + k_1 \geq n_2 + n_1$

$\vdots$

$k_{m-1} + k_{m-2} + \dots + k_1 \geq n_{m-1} + \dots + n_1$

$\sum k_i = \sum n_i$

$x_1, \dots, x_n \in \mathbb{R}^+$

$$\sum_{sym} x_i^{k_i} \geq \sum x_i^{n_i}$$

$$2(a^3+b^3+c^3) = \sum_{sym} a^3 b^0 c^0$$

$$\vee\!/$$

$$a^2b + a^2c + b^2a + b^2c + c^2a + c^2b = \sum_{sym} a^2 b^1 c^0$$

$$\vee\!/$$

$$6abc = \sum_{sym} a^1 b^1 c^1$$

$(0,1,2)$

$(0,0,3)$

Dim $[3,0,0] \succ [2,1,0]$

$$\frac{a^3+a^3+b^3}{3} \geq \sqrt[3]{a^6b^3} = a^2b$$

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

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

$$a^3+b^3+c^3 \geq a^2b + b^2c + c^2a$$

Schur

Forte + Debole $\geq$ Medi(o)

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

wlog $a \geq b \geq c$ No!

wlog $\max\{a,b,c\} = a$ Sì!

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

$$\sum_{sym}(a^3+abc-2a^2b) \geq 0$$

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

$a=xy \quad b=yz \quad c=zx$

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

——o——o——

BMO 12/2

$x,y,z \geq 0$

$$\sum_{cyc}(x+y)\sqrt{(z+x)(z+y)} \geq 4(xy+yz+zx)$$

Dim i) $(x+y)\sqrt{(z+x)(z+y)} \geq 2(xy)+yz+zx$!!!

ii) $x+y=a^2$
$y+z=b^2$
$z+x=c^2$

$$x=\frac{a^2+c^2-b^2}{2}$$

$$\sum_{cyc} a^2bc \geq \text{- - - -}$$ Schur

TST 09/6

$a_1,\dots,a_n>0$
$b_1,\dots,b_n>0$

$$a_1 \cdots a_n + b_1 \cdots b_n \leq (a_1^n + b_1^n)^{\frac{1}{n}} \cdots (a_n^n + b_n^n)^{\frac{1}{n}}$$

Dim

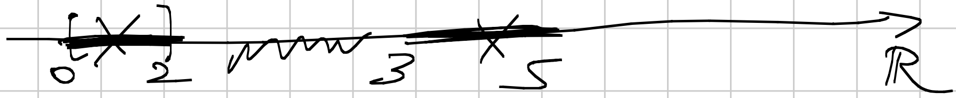
$$= \sqrt[n]{(a_1^n + b_1^n) \cdots (a_n^n + b_n^n)}$$

$\stackrel{\cdot}{=}$ Tesi di CS a n vettori di $\mathbb{R}_+^2$

Jensen / Convessità

$I \subseteq \mathbb{R}$ se $\forall a,b \in I$ tutto il segmento $AB \in I$

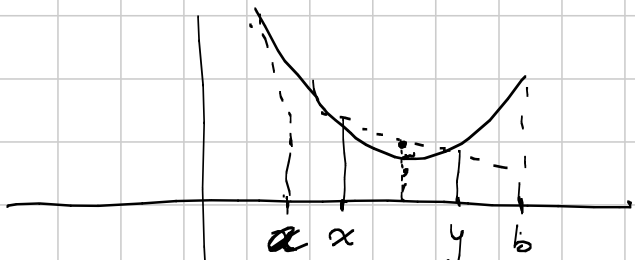
I si dice convesso



$f: I \to \mathbb{R}$ f convessa se $\forall x,y \in I$ e $\lambda \in [0,1]$

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

$\left[\lambda = \frac{1}{2}\right]$ $$f\left(\frac{x+y}{2}\right) \leq \frac{1}{2}\left[f(x)+f(y)\right]$$



$f''(x) \geq 0 \quad \forall x \in I \Rightarrow$ $\boxed{f \text{ è convessa}}$

$\cdot\, x^r$ $\nearrow r \geq 1$ f è convessa $[0,+\infty)$; $\searrow r < 1, r > 0$ f è concava $[0,+\infty)$

$r \geq 1$ $\quad f''(x) = \underbrace{r(r-1)}\underbrace{x^{r-2}}_{>0} \Rightarrow f$ è convessa

$0 < r \leq 1$ $\quad f$ è concava

$\log(x)$ è concavo $(0, +\infty)$

$-\frac{1}{x^2} < 0$

e^x è convessa in $\mathbb{R}$

$e^x > 0$

f, g convesse $\quad c > 0 \implies \left.\begin{matrix} c \cdot f \\ f(ax+b) \\ f+g \end{matrix}\right\}$ convesse

Problema

$a, b, c > 0$

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

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

$f(x) = x \ln x$? sì ... $f''(x) = \frac{1}{x} > 0$

per Jensen si finisce

$$\frac{9}{a+b+c} \leq 2\left(\frac{1}{a+b} + \frac{1}{b+c} + \frac{1}{c+a}\right) \quad a, b, c > 0$$

Dim $\quad a+b+c = 1 \quad$ wlog

$$\frac{9}{2} \le \sum_{cyc} \frac{1}{1-a}$$

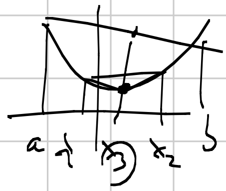
$f(x) = \frac{1}{1-x}$ convessa $(0,1)$

$\frac{1}{x}$

$f(ax+b)$ OK

$f(x) =$

END POINT CONVEX



f convessa $[a,b]$

$$\boxed{\max\{f(x) : x \in [a,b]\} = \max\{f(a), f(b)\}}$$

Step I Il massimo esiste!

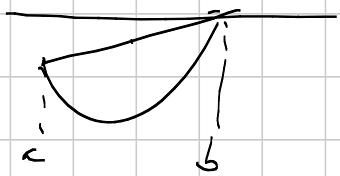
Step II

$$f(\lambda x + \mu y) \le \lambda f(x) + \mu f(y) \quad \forall x, y \in I$$

$\mu + \lambda = 1$.

$x = a,\ y = b$

AGGIUSTARE I DETTAGLI...



i) Bulgaria 1995

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

$$0 \le x_1, \dots, x_n \le 1$$

$x_1 - x_1x_2 - x_1x_n + \text{roba}$ $\qquad x_i = \{0,1\}$

$\underbrace{x_1(1-x_2)} + x_2(1-x_3) + \dots + x_n(1-x_1)$

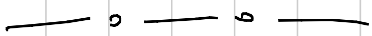
$x_1 = 0$ o $x_2 = 1$ $\qquad 1 \Leftrightarrow x_i = 1$ e $x_{i+1} = 0$

ii) USATO 80/5

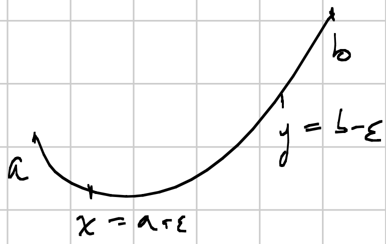
$$\frac{a}{b+c+1} + \frac{b}{c+a+1} + \frac{c}{a+b+1} + (1-a)(1-b)(1-c) \leq 1$$

$0 \leq a,b,c \leq 1.$

$$\frac{\text{roba}_2}{\text{roba}+a}$$



Smoothing



$a+b = x+y$

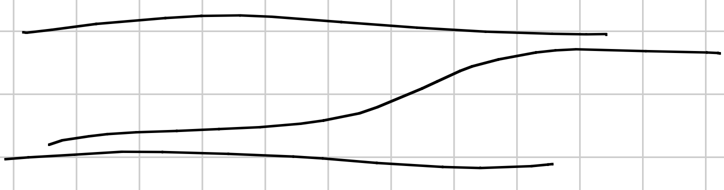
$x \leq y$

$$f(a)+f(b) \geq f(a+\varepsilon) + f(b-\varepsilon)$$

Teorema Non esiste nessun numero reale > 1.

Dim: Sia M $\qquad M^2 > M > 1$ $\blacksquare$

NO!



$$\frac{a+b+c}{3} \geq \sqrt[3]{abc}$$

$$(a,b,c) \to \left(\frac{a+b}{2}, \frac{a+b}{2}, c\right)$$ no!

Wlog $a \leq b \leq c$

$$(a,b,c) \to (a+\varepsilon, b, c-\varepsilon)$$

$$\varepsilon_1 = \frac{a+b+c}{3} - a$$

$$\left(\frac{a+b+c}{3}\right)^2 \geq \sum_{cyc} a\sqrt{bc}$$

$$c\sqrt{ab} + \sqrt{c}\sqrt{ab}(\sqrt{a}+\sqrt{b})$$

$$(a,b,c) \to \left(\frac{a+b+c}{3}, b, c-\varepsilon_1\right)$$!

Karamata $\overset{!}{\Rightarrow}$ Jensen

$X \succ Y$ f convessa

$$\sum f(x_i) \geq \sum f(y_i)$$

Disuguaglianze tra frazioni (CS)

TT 2017.1

$x, y, z > 0$

$$\frac{x}{2x+y} + \frac{y}{3y+z} + \frac{z}{4z+x} \geq k$$

$a, b, c > 0$

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

$$\left(\sum a_i b_i\right)^2 \leq \left(\sum a_i^2\right)\left(\sum b_i^2\right)$$

$$\sqrt{\frac{a}{b+c}}, \quad \sqrt{a(b+c)} \qquad a_i b_i = \sqrt{\frac{a}{b+c}}\sqrt{b+c}\sqrt{a}$$

$$(\text{TESTO})\underbrace{(ab+ac+bc+ba+ca+cb)}_{\text{Den}} \geq (a+b+c)^2$$

$$\text{TESTO} \overset{!}{\geq} \frac{(a+b+c)^2}{2(ab+bc+ca)} \overset{?}{\geq} \frac{3}{2} \qquad \text{ok}$$

Brillante

$$\frac{z}{4z+x} \geq \frac{z}{4(x+y+z)}$$

Bovino

$$\sqrt{\frac{x}{2x+y}} \qquad \sqrt{x(2x+y)}$$

$$\text{TESTO} \geq \frac{(x+y+z)^2}{(2x^2+xy+3y^2+yz+4z^2+zx)} \geq k$$

$$1 \quad 1 \quad 1 \qquad\qquad k\cdot 2 \quad k\cdot 3 \quad k\cdot 4$$

$$x^2+y^2+z^2+2(xy+yz+zx)$$

$$\geq k(2x^2)+k(3y^2)+k(4z^2)$$
$$+\,k(xy+yz+zx)$$

$$1 \geq 2k \ \checkmark$$
$$1 \geq 3k \ \checkmark \qquad k \leq \frac{1}{4}$$
$$1 \geq 4k \ \checkmark$$

$$\frac{1}{4}+a$$

IMO 95/2

$$abc=1 \qquad \sum_{cyc} \frac{1}{a^3(b+c)} \geq \frac{3}{2} \qquad a=\frac{1}{bc}$$
$$\frac{1}{a}=bc$$

$$\sqrt{\frac{1}{a^3(b+c)}}\,, \quad \sqrt{a(b+c)}$$

$$\text{TESTO} \geq \frac{\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right)^{\cancel{2}}}{2(\cancel{ab+bc+ca})} \geq \frac{3}{2}$$

$$ab+bc+ca \geq 3 \qquad abc=1 \qquad \text{ok!}$$

$$\boxed{\frac{a+b+c}{3} \geq \sqrt{\frac{ab+bc+ca}{3}} \geq \sqrt[3]{abc}}$$

IMO 05/3

$xyz \geq 1$ $\qquad \displaystyle\sum_{cyc} \frac{x^5 - x^2}{x^5+y^2+z^2} \geq 0$

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

$x^5+y^2+z^2 - x^2 - y^2 - z^2$

$$\sum_{cyc} \frac{1}{x^5+y^2+z^2} \overset{!}{\leq} \frac{3}{x^2+y^2+z^2}$$

$(\sqrt{x^5}, y, z)$ e $\left(\sqrt{\frac{1}{x}}, y, z\right)$ $\qquad xyz \geq 1$, $yz \geq \frac{1}{x}$

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

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

$$\sum_{cyc} \frac{x^2+y^2+z^2}{x^5+y^2+z^2} \leq \frac{\sum yz + y^2+z^2}{x^2+y^2+z^2} = 2 + \frac{xy+yz+zx}{x^2+y^2+z^2} \leq 3 \quad \checkmark$$

IMO 01/2

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

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

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

$$\frac{a^2}{a^2+b^2+c^2} \qquad \sum_{cyc}^{\text{Casa}} \frac{a}{b+2c+d} \geq 1$$

i) $\left(\frac{\sqrt{a}}{\sqrt[4]{a^2+8bc}}\right), \left(\sqrt[4]{a^2+8bc}\,\sqrt{a}\right)$

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

$$\left(\sum a\right)^2 \geq \underbrace{\sum a\sqrt{a^2+8bc}} \Rightarrow \boxed{\text{Tesi}}$$

1) Jensen $\sum a\sqrt{a^2+8bc} \leq \sum a\sqrt{a^2+4(\underbrace{b^2+c^2}_{1-a^2})} \leq \left(\sum a\right)^2$

$$3 \leq \left(\sum a\right)^2 \qquad \sum a^2 = 1$$

$$\geq$$

$$x\sqrt{1-3x^2}$$

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

$$a^2+8bc = z^2 \qquad a$$
$$b^2+8ca = x^2$$
$$c^2+8ab = y^2$$

3) Termine a termine $a(a+b+c)+b(b+c+a)+\ldots$

$$\cancel{a}(a+b+c) \geq \cancel{a}\sqrt{a^2+8bc}$$

$$\cancel{a^2}+b^2+c^2+\underline{2ab}+2bc+\underline{2ca} \geq \cancel{a^2}+\underline{8bc}$$

$$ab + ca \geq 2bc$$

$$a\sqrt{a^2+8bc} \overset{?}{\leq} \frac{a^2+a^2+8bc}{2} = a^2+4bc$$

Point of Incidence

1) AM−GM $\quad 3a\sqrt{a^2+8bc} \leq \frac{9a^2+a^2+8bc}{2} = 5a^2+4bc$

$$a\sqrt{a^2+8bc} \leq \frac{5}{3}a^2 + \frac{4}{3}bc$$

$$\frac{5}{3}(a^2+b^2+c^2) + \frac{4}{3}(ab+bc+ca)$$

$$\leq (a^2+b^2+c^2) + 2(ab+bc+ca)$$ NO!

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

$$2ab\sqrt{a^2+8bc}\sqrt{b^2+8ca}$$

~~3) (forse) CS~~

5) "Idea" Jensen omogeneizzato

$$abc = 1$$

$$\sum a^2 + \frac{2}{a} \overset{!}{\geq} \sum\sqrt{a^4+8a} \qquad a^2+\frac{8}{2} \quad \sqrt{a^4+8a}$$

$$\cancel{a^4} + \cancel{4a} + \frac{4}{a^2} \geq \cancel{a^4} + \cancel{8}a$$

$$a^3 \leq 1 \to a \leq 1$$

$$a^4 + a + a + \dots + a$$

$$a^4 + 2a$$

$x = a+b$
$y = b+c$
$z = c+a$

$a^2 + 8bc = \square^2$

$\left(\frac{x+z-y}{2}\right)^2 + 8\left(\frac{y+z-x}{2}\right)\left(\frac{x+y-z}{2}\right)$

$= \boxed{?}$ boh...

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

≥ 1

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

CS

$a \geq b \geq c$

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

$2 - \frac{4}{a^2} \rightsquigarrow$

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

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

$\underbrace{\left(\sum a^2\right)}\underbrace{\left(\sum a^2+8bc\right)} \leq \underbrace{\left(\sum a\right)}^4$ no!

$\left(\sqrt{x}, \sqrt{a^3+8abc}\right) = \left(\frac{a}{\sqrt{x}}, \sqrt{x}\sqrt{a^2+8bc}\right)$

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

$$\sum (a^3 + 8abc) \le \left(\sum a\right)^3$$

$$\sum a^3 + 24abc \le \sum a^3 +$$

Disuguaglianze tra radici LHS $\le$ RHS

i) LHS $\le c \le$ RHS $c \in \mathbb{R}$

ii) Fondere le radici " $a\sqrt{a^2+8bc}$ "

iii) Maggiorare termine a termine

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

$$\frac{a}{\sqrt{(a+b)(a+c)}} \le \frac{1}{2} \quad !!!$$

$$\cancel{4}^{3} a^2 \le \cancel{a^2} + ab + ac + bc$$

$$\cancel{a}(b+c+a) \ge 3a^{\cancel{2}}$$

$$b+c \ge 2a$$

$$\frac{\cancel{a}}{\sqrt{(a+b)(a+c)}} \le \frac{3}{2}\frac{\cancel{a}}{a+b+c}$$

$$2(a+b+c) \le 3\sqrt{(a+b)(a+c)}$$

$$8ca + 8bc + 8ab + 4a^2 + 4b^2 + 4c^2 \le 9a^2 + 9ab + 9ac + 9bc$$

$$\frac{3}{4}\,\frac{b+c}{a+b+c}$$

$$a+b = x^2$$
$$b+c = y^2$$
$$c+a = z^2$$

$$\sum_{cyc} \frac{x^2+z^2-y^2}{xz} \le 3$$

$$\sum_{cyc} y(x^2+z^2-y^2) \le 3xyz$$

$\boxed{\text{Schur}}$

$$\underbrace{\sum a\sqrt{b+c}} \le \frac{3}{2}\sqrt{a+b}\sqrt{b+c}\sqrt{c+a}$$

CS $\left(a, \sqrt{b+c}\right) \leftarrow$ CONTI $\geq$ $\left(\frac{a}{\sqrt{a}}, \sqrt{a}\sqrt{b+c}\right)$

$\left(\sqrt{a}, \sqrt{ab+ac}\right) \leftarrow$

$$\sum a\sqrt{b+c} \le \sqrt{\left(\sum a\right)\sqrt{\sum ab+ac}} \overset{?}{\le} \frac{3}{2}\sqrt{a+b}\sqrt{b+c}\sqrt{c+a}$$

$$4\sum a \cdot 2\sum ab \le 3(a+b)(b+c)(c+a) \checkmark$$

Vera!

ii) $a+b+c=1$ $\quad a,b,c \geq 0$

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

Come si fa? $\quad f(x) = \sqrt{1-x}$

RENDERSENE CONTO!

$$\sum\sqrt{b+c} = LHS$$

$$\boxed{\sqrt{A}+\sqrt{B}+\sqrt{C} \le \sqrt{3}\sqrt{A+B+C}} = \sqrt{3}\sqrt{3-a-b-c} = \sqrt{6}$$

$$\left(\frac{1}{\sqrt{A}}, \frac{1}{\sqrt{B}}, \frac{1}{\sqrt{C}}\right)$$

$$LHS \le \sqrt{6}$$

$$\cancel{\sqrt{6}}^{\sqrt{3}} \le \cancel{\sqrt{2}}\left(\sqrt{\sum ab} + 2\sqrt{\sum a^2}\right) \qquad \boxed{a+b+c=1}$$

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

$$a^2+b^2+c^2 = 1-2(ab+bc+ca)$$

$$a+b+c=1 \qquad \sqrt{\frac{a^2+b^2+c^2}{3}} \geq \frac{a+b+c}{3} \qquad ab+bc+ca \leq \frac{1}{3}$$

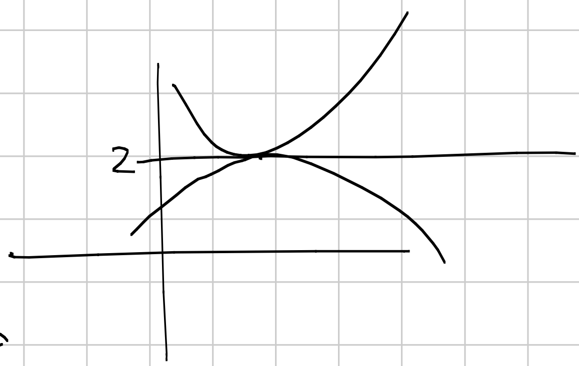
$$4 - 8\sum ab + \sum ab + 4\sqrt{\sum ab}\sqrt{\sum a^2} \geq 3$$

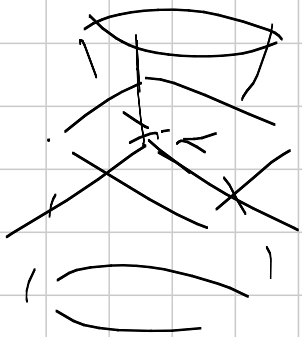
$$1 + 4\sqrt{\sum ab}\sqrt{\sum a^2} \geq 7\sum ab$$

$$a^2+b^2+c^2+2(ab+bc+ca)$$

$$\sum a^2 + \boxed{4\sqrt{\sum ab}\sqrt{\sum a^2}} \geq 5\sum ab$$

$$\sum a^2 \geq \sum ab$$





IMO SL 09/A4

$ab+bc+ca \le 3abc$ $\qquad \frac{1}{a}+\frac{1}{b}+\frac{1}{c} \le 3$

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

$$\boxed{\sqrt{2}\sqrt{a+b} \overset{?}{\ge} \sqrt{\frac{a^2+b^2}{a+b}} + 1}$$

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

$$2a^2+4ab+2b^2$$

$$\sqrt{\frac{1}{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}}} \ge \sqrt{\frac{1}{3}}$$

$$a^2 > a$$

$$\sqrt{2}\sqrt{a+b} \ge \sqrt{\frac{a^2+b^2}{a+b}} \cdot + \frac{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}}{3} \le \dots$$ no!

$$\sqrt{2}\sqrt{a+b} \qquad \sqrt{\frac{a^2+b^2}{a+b}}$$

$$\sqrt{\frac{a^2+b^2}{2}} \cdot \frac{1}{\sqrt{a+b}}$$

CS $\qquad \sqrt{2}\sqrt{a+b} \qquad \sqrt{\frac{a^2+b^2}{a+b}}$

$$= \sqrt{2}\sqrt{\frac{a^2+b^2+2ab}{a+b}} \underset{\boxed{CS}}{\ge} \sqrt{\frac{a^2+b^2}{a+b}} + \sqrt{\frac{2ab}{a^2+b^2}}$$

$$\sum \sqrt{\frac{2ab}{a+b}} \ge 3 \qquad \frac{1}{a}+\frac{1}{b}+\frac{1}{c} \le 3$$

Brillante

$$M_{\frac{1}{2}} \ge M_{-\frac{1}{2}}$$

Bovina $\sum \sqrt{\frac{2}{x+y}} \geq 3$

PER CASA

$\frac{1}{a} = x$

$x+y+z \leq 3$

A3 – medium (succ e funz)

Note Title 9/7/2017

Scamb...

→ Successioni → ripasso → nuovo → "analisi"

→ Funzionali → ripasso → tecniche

Successioni

- Ripasso

$$a_{n+2} = \lambda a_{n+1} + \mu a_n \quad n \geq 0 \quad \boxed{\begin{matrix} a_0 \\ a_1 \end{matrix}} \quad (1)$$

OMOG

$$x^2 = \lambda x + \mu \longrightarrow R_1 \text{ e } R_2$$

Perchè ?

$$a_n = R_1^n \cdot c_1 + R_2^n \cdot c_2 \quad (2)$$

$\bar{a}_n, a_n^*$

$$\boxed{c_1 \bar{a}_n + c_2 a_n^*} \text{ risolve } (1)$$

$\bar{a}_n + a_n^* \Rightarrow (1)$

$c\bar{a}_n \to (1)$

$$a_n = R^n$$

$$R^2 = \lambda R + \mu$$

- Novità

$$a_{n+2} = \lambda a_{n+1} + \mu a_n + f(n) \quad (3)$$

NON OMOG

$\bar{a}_n$ e a_n^* risolvono (3)

$\Rightarrow \underbrace{\bar{a}_n - a_n^*}_{b_n}$ risolve l'equazione omogenea (1)

$$\bar{a}_{n+2} - a_{n+2}^* = \lambda(\bar{a}_{n+1} - a_{n+1}^*) + \mu(\bar{a}_n - a_n^*)$$

$\bar{a}_n$ risolve (3) e a_n^* risolve (3) $\Rightarrow \bar{a}_n - a_n^*$ (1)

$$\bar{a}_n = (\bar{a}_n - a_n^*) + a_n^*$$

$$\Uparrow$$

$$\left\{\begin{array}{c}\text{Soluzione}\\ \text{generale}\\ \text{della}\\ \text{non omogenea}\end{array}\right\} = \left\{\begin{array}{c}\text{Soluzione}\\ \text{generale}\\ \text{della}\\ \text{omogenea}\end{array}\right\} + \left\{\begin{array}{c}\text{Soluzione}\\ \text{particolare}\\ \text{della non}\\ \text{omogenea}\end{array}\right\}$$

- Esempi

$$a_{n+1} = ca_n + d \quad \Big\} \quad a_0 = \alpha$$

1) Induzione

$$a_0 = \alpha$$
$$a_1 = \alpha c + d$$
$$a_2 = \alpha c^2 + cd + d$$
$$a_3 = \alpha c^3 + c^2 d + cd + d$$

$$\Rightarrow a_n = \alpha c^n + d(c^{n-1} + \ldots + 1)$$

$$a_n = \alpha c^n + d\frac{c^n - 1}{c - 1} \quad (\text{se } c \neq 1)$$

$$a_n = \alpha + dn \quad (\text{se } c = 1)$$

2) Shift $\quad b_n = a_n - \underline{\ell} \qquad b_{n+1} = cb_n$

$$\begin{cases} a_{n+1} - \ell = c(a_n - \ell) \\ a_{n+1} = ca_n + d \end{cases}$$

$$d = \ell - c\ell \qquad c \neq 1$$

$$\ell = \frac{d}{1-c} \qquad \checkmark$$

3) Usare i potenti mezzi

$$a_{n+1} = ca_n + \underline{d}$$

$\underline{a_n}$ che risolve la omogenea generale

a_{n_*} che risolve la non omogenea (basta una particolare)

$\underline{a_n} = R^n \qquad R^{n+1} = cR^n$

$$\boxed{c = R}$$

$$\underline{a_n} = \lambda \cdot c^n$$

$a_{n_*} = k$

$$k = ck + d$$

$$\Rightarrow k = \frac{d}{1-c} = a_{n_*}$$

$$a_n = \lambda \cdot c^n + \frac{d}{1-c}$$

$$a_0 = \alpha$$

Es. 2 $\quad a_{n+2} = 3a_{n+1} - 2a_n + n$

$$\underline{a_n} = \lambda_1 \cdot 1^n + \lambda_2 \cdot 2^n$$

$$a_{n_*} = bn + c$$

$$b(n+2)+c = 3b(n+1)+3c-2bn-2c+n$$

$$\lambda_1+\lambda_2\cdot 2^n+bn+c$$

Es. 3

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

$$x^2=3x-2$$

$$a_n = \mu\cdot 3^n$$

$$\mu\cdot 3^{n+2}=3\mu\cdot 3^{n+1}-2\cdot\mu\cdot 3^n+3^n$$

$$\cancel{9\mu}=\cancel{9\mu}-2\mu+1 \Rightarrow \mu=\frac{1}{2}$$

$$a_n=\lambda_1+\lambda_2\cdot 2^n+\frac{1}{2}\cdot 3^n$$

Es. 4

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

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

$$a_n=\mu\cdot 2^n$$

$$4\mu=6\mu-2\mu+1 \Rightarrow 0=1$$

$$2^n\cdot p(n)$$ dove deg(p(n)) = molteplicità di 2 nell'eq. omogenea (m)

$$(An+B)\cdot 2^n$$

$$An\cdot 2^n \qquad \mu\, 2^n\cdot n^m$$

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

$$An^2 2^n \rightsquigarrow$$

Se k risolve l'eq. omogenea con molteplicità m,
poniamo $a_n = \underline{c \cdot n^m \cdot k^n}$

Esiste sempre un c? PROVATELO...

$$a_{n+w} = \ldots\ldots + k^n$$

$x^w = \ldots\ldots$ ha m volte la radice k

$\boxed{w \geq m}$

Esercizi

BMO 05/1

$$\begin{cases} a_{2004} = ? \\ a_{m+n} + a_{m-n} - m + n - 1 = \frac{1}{2}(a_{2m} + a_{2n}) \end{cases}$$

$m \geq n \geq 0$
$a_1 = 3$

$\vdots$

$$a_{m+2} - 2a_{m+1} + a_m = \underline{2 \cdot 1^m}$$

$a_0 = 1$
$a_1 = 3$

$$\underline{a_n} = \lambda_1 \cdot 1^n + \lambda_2 \cdot n \cdot 1^n$$

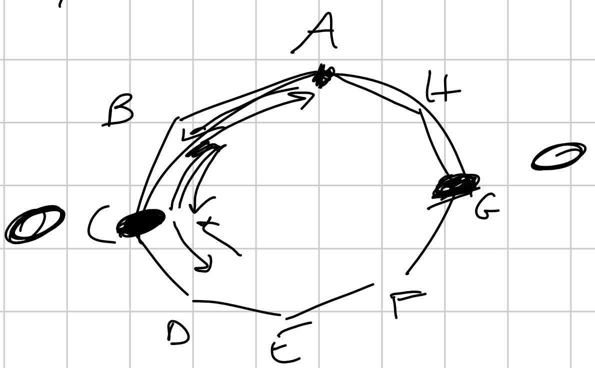
$$a_n = c \quad \}$$
$$cn + d \quad \}$$

$$a_{n*} = 1^n \cdot n^2 \cdot c$$

$$a_n = cn^2 + \lambda_2 n + \lambda_1$$

$$\boxed{a_n = n^2 + n + 1}$$

IMO 79/6



P_n

$P_{2n} \equiv 0$

A_n

O_n

$A_{2n+1} \equiv 0$

$O_{2n+1} \equiv 0$

$$\begin{cases} A_{2n+2} = 2A_{2n} + O_{2n} \\ O_{2n+2} = 2O_{2n} + 2A_{2n} \end{cases}$$

A_{2n} O_{2n} $\longrightarrow$ risposta . . .

$$\boxed{x_{n+1} = \sqrt{5x_n - 6}}$$

$x_0 = 2017$

$x_{n+1} = 2x_n^2 - 1$

$\ell = 3$

$f(x) = \sqrt{5x - 6}$

i) $3 \le x_n \le 2017$

ii) $x_{n+1} \le x_n$

iii) $x_n \to \ell$

iv) $\ell = 3$

$x \to \sqrt{5x-6}$

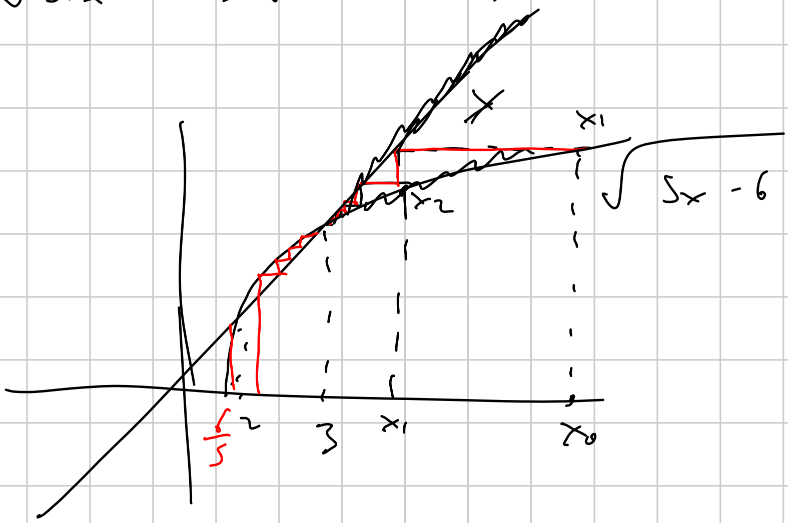
$x_0 = 2017$

ver

$x_{n+1} = \sqrt{5x_n - 6} \le \sqrt{5 \cdot 2017 - 6} \le 2017$

$x_0 = 2017 \ge 3$

$x_{n+1} = \sqrt{5x_n - 6} \ge \sqrt{5 \cdot 3 - 6} \ge 3$



$x_n \to \ell$

$\ell = \sqrt{5\ell - 6}$

$\ell = 2$

$\ell = 3$

$x_{n+1} = x_n^3$

a) $x_0 = \boxed{2}$

i) $x_n \geq 2$

ii) $x_{n+1} \geq x_n$

iii) ℓ esiste ✓

iv) $\ell \to +\infty$ ✓

b) $x_0 = \frac{1}{2}$

i) $0 \leq x_n \leq \frac{1}{2}$

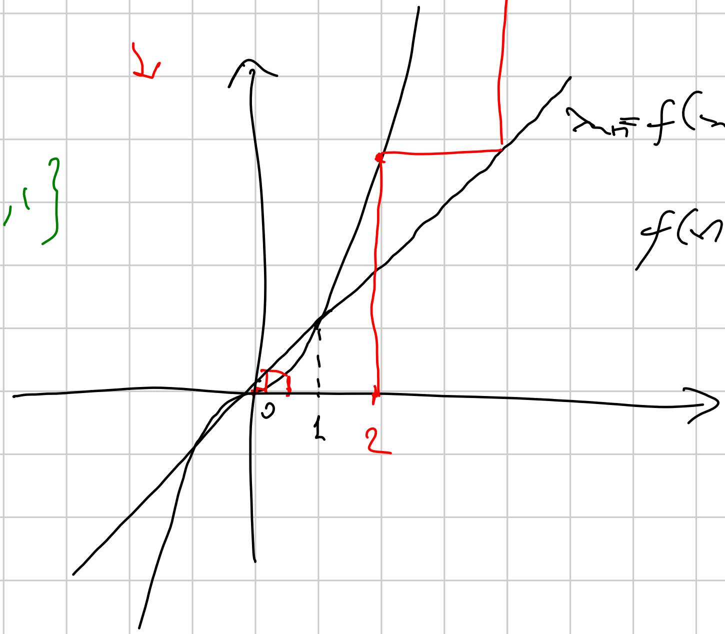
ii) $x_{n+1} \leq x_n$

iii) $\exists\, \ell$ ✓

iv) $\ell \to 0$

$\ell = \ell^3$

$\ell = \{-1, 0, 1\}$



$x_{n+1} = f(x_n)$

$f(x) = x^3$

T1 2017/2

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

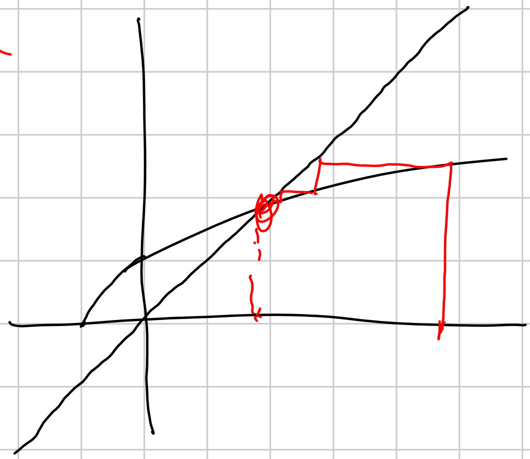
$x_{n+1} = \sqrt{1+x_n}$ $x_0 = \alpha$

$x_{n+s} = x_n$

$\sqrt{1+x} \gtrless x$

$\sqrt{1+\sqrt{1+x}} \gtrless x$

$x = \sqrt{1+x}$



Funzionali

$f: S \to S$ $\quad$ $f(x+y) = f(x) + f(y)$

$S \subseteq \mathbb{R}$

- $S = \mathbb{Q}$ $\quad$ Risposta: $f(x) = f(1) \cdot x$

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

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

$P(-x,x)$: f è dispari

$P(n,1)$: $f(n) = nf(1)$ $\quad$ $f(\sum x) = \sum f(x)$

$P(n,x)$: $f(nx) = nf(x)$

$P(n, \frac{m}{n})$: $mf(1) = nf(\frac{m}{n})$

Se $S = \mathbb{R}$

- f continua $\boxed{\text{IMO}}$
- f monotona
- f limitata
- $\exists$ un rettangolo in $\mathbb{R}^2$ t.c. non ci sono punti $(x, f(x))$

Se f è monotona $\Rightarrow$ $f(x) = kx$

wlog crescente

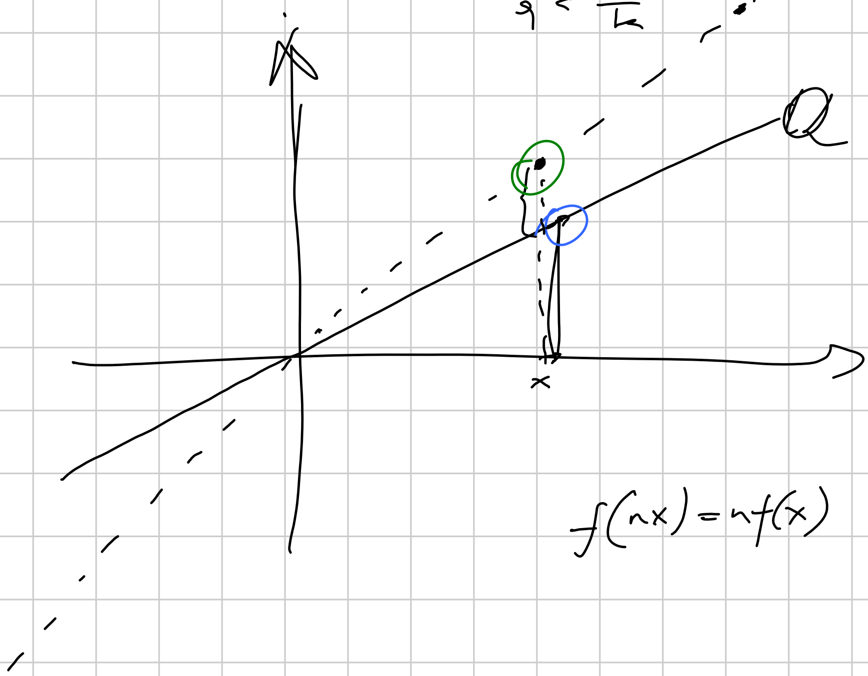
$f(q) = kq$ $\quad$ $q \in \mathbb{Q}$

x : $f(x) = bx$ $\quad$ $b \neq k$

$b < k$ $\boxed{\frac{bx}{k}} < q < \boxed{x}$ ——

$$f(q) < f(x)$$
$$\| \qquad \|$$
$$qk \qquad bx$$

$$qk < bx$$
$$q < \frac{bx}{k}$$



$$f(nx) = nf(x)$$

$P(a,b)$: $f(a+b^2) = f(a) + f(b^2)$ $a,b \in \mathbb{Q}$

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

$P(-b^2,b)$: f è dispari su $[\mathbb{Q}]^2$ $f(x^2) = -f(-x^2)$ $x \in \mathbb{Q}$

$P(nb^2,b)$: $f(nb^2) = nf(b^2)$ $Q(n,b)$

$f(n) = nf(1) = nk \Leftarrow Q(n,1)$

$\underline{Q\left(q^2, \frac{p}{q}\right)}$ $f(p^2) = q^2 f\left(\left(\frac{p}{q}\right)^2\right) \Rightarrow f(x^2) = kx^2$

$$f(nb^2) = n f(b^2) = k \cdot nb^2$$

$n = pq,\ b = \frac{1}{q})$

$Q(pq, \frac{1}{q})$:

$$f\left(pq \cdot \frac{1}{q^2}\right) = k \cdot pq \cdot \frac{1}{q^2}$$

$$f\left(\frac{p}{q}\right) = k \cdot \frac{p}{q}$$

Iniettività e surgettività

IMO SL 02 / 1 $\qquad f: \mathbb{R} \to \mathbb{R}$

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

$$f(\ldots) = \mathbb{R}$$

$$f(f(n)) = n + 2 \qquad f: \mathbb{N}_{\geq 0} \to \mathbb{N}_{\geq 0}$$

$\boxed{y = -f(x)}$

$z \quad z, -f(z)$

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

f surgettiva

$$\exists x_0 : f(x_0) = 0$$

$$f(f(y)) = 2f(y)$$

$$f(z) = 2z$$

$x = x_0 \qquad f(y) = 2x_0 + f(f(y) - x_0)$

$$f(y) = z$$

TT 2017.3 (BST 2012 / 4)

$f: \mathbb{Q} \to \mathbb{Q}$ $\qquad f(x+f(y+f(z))) = \underline{y+f(x+z)}$

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

$f(f(y)) = y$

$\cancel{f}(x+f(y+f(z))) = y+f(x+z) = y+f(z+x)$

$= \cancel{f}(z+f(y+f(x)))$

$f(y_1)=f(y_2) \Rightarrow y_1 = y_2$

$f(f(x)) = x$

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

$x \to f(x)$

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

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

$-f(0) \quad -f(0) \qquad -2f(0)$

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

$f(x) = Ax+B$

$f(x)=x \qquad f(x) = -x+c$

Sostituzioni (furbe?)

Argentina TST 10/13 (modificato)

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

$$f(x+xy+f(y)) = \left(f(x)+\tfrac{1}{2}\right)\left(f(y)+\tfrac{1}{2}\right)$$

$y=-1$ $\qquad \underbrace{f(f(-1))}_{0} = \left(f(x)+\tfrac{1}{2}\right)\underbrace{\left(f(-1)+\tfrac{1}{2}\right)}_{0}$

$$f(x)=c$$

$$f(-1)=-\frac{1}{2} \Rightarrow \boxed{f\left(-\tfrac{1}{2}\right)=0}$$

$\boxed{\text{OK}}$ magari non si può davvero fare!!!

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

$$\boxed{f(\alpha)=-\tfrac{1}{2} \iff \alpha=-1}$$

$y=\alpha$ $\qquad f\left(\underbrace{(\alpha+1)x}_{\in\mathbb{R}}-\tfrac{1}{2}\right)=0 \qquad \alpha+1=0$

$$x+xy+f(y)=-\frac{1}{2} \qquad \boxed{x=\frac{-\frac{1}{2}-f(y)}{y+1}}, \; y\neq -1$$

$$0=f\left(-\tfrac{1}{2}\right)=\left(f(x)+\tfrac{1}{2}\right)\left(f(y)+\tfrac{1}{2}\right)$$

$x = -1$

$\frac{1}{2} + f(y) = y + 1$ ✓

IMO SL 16/4 $\qquad f: \mathbb{R}^+ \to \mathbb{R}^+$

$$x f(x^2) f(f(y)) + f(y f(x)) = f(xy)\left(f(f(x^2)) + f(f(y^2))\right)$$

$$x f(x^2) f(f(y)) + f(y f(x)) = y f(y^2) f(f(x)) + f(x f(y))$$

$x = y = 1$ $\qquad \boxed{f(1) = 1}$

$y = 1$ $\qquad x f(x^2) = f(x)$ $\qquad x = f(y)$

$x = 1$ $\qquad f(f(y)) = f(y) f(f(y^2))$

$f(f(y)) = f(y)\, f(f(y)^2)$

$\cancel{f}(f(y^2)) = \cancel{f}(f(y)^2)$

$\frac{f(x)}{x} = f(x)^2$ ✓

Se $f(x_1) = f(x_2)$ e vogliamo $x_1 = x_2$

$\Rightarrow f(x_1^2) = f(x_2^2)$

$f(x_1) = f(x_2) \Rightarrow f(x_1 y) = f(x_2 y)$

$y = \frac{x_2}{x_1}$ $\quad f(x_1)=f(x_2) = f\left(\frac{x_2^2}{x_1}\right)$

$= f\left(\frac{x_2^3}{x_1^2}\right)$

$y=x_1$ $\quad f(x_1^2) = f(x_1 x_2) = f(x_2^2)$

Lavorare coi positivi

MO SL 07/4 $\quad f: \mathbb{R}^+ \to \mathbb{R}^+$

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

$f(\ldots) \neq 0$ $\quad f(X) = f(Y) + f(Z)$

$X = Y$

$x + f(y) = x + y \Rightarrow f(y) = 0$ no! $f(y) \neq y$

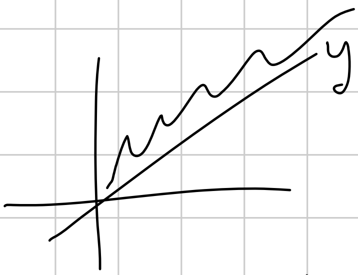
$x + f(y) = y \Rightarrow f(x+y) = 0 \Rightarrow x = y - f(y) > 0$

no!

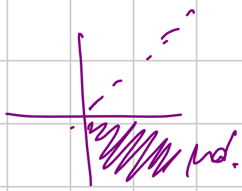
$f(y) \geq y$

$f(y) > y > 0$

$f(y) > y$



$g(y) = \boxed{f(y) - y}$ $\quad g: \mathbb{R}^+ \to \mathbb{R}^+$ $\quad \mathbb{R}^+ \to$



$$g(x+y+g(y)) = g(x+y) + y \qquad x,y \in \mathbb{R}^+ \quad g: \mathbb{R}^+ \to \mathbb{R}^+$$

$$g(a+g(b)) = g(a)+b \qquad a > b > 0$$

$$g(b_1)=g(b_2) \Rightarrow b_1 = b_2 \qquad \text{mmmm...} \qquad a = \max\{b_1, b_2\} + 2017$$

$$\boxed{g \text{ iniettiva}}$$

$$g(a+g(b)) = \underline{g(a)+b}$$

$$g(a+g(b+c)) = \underline{g(a)+b}+c$$

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

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

$$g(a+g(b)+g(c))$$

Immagini

MO SL OS/2 $\qquad f: \mathbb{R}^+ \to \mathbb{R}^+$

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

$$x+yf(x) = y+xf(y) \qquad f(x) = \cancel{Ax}+1$$

$x = x+yf(x)$ no

$$xy = x+yf(x) \qquad y = \frac{x}{1-f(x)} > 0 \Rightarrow f(x) = 2$$

$$1-f(x) > 0$$

$$f(x) < 1$$

$\boxed{f(x) \ge 1}$

$f(x)f(y) = 2f(\dots)$

$a,b \in Im\, f \Rightarrow \frac{ab}{2} \in Im\, f$

$\times \qquad (1,+\infty]$

Brutal mode

$m < 2$

$\frac{m^2}{2} < m \Rightarrow m \ge 2$

$\frac{f(x)}{2} \cdot \frac{f(y)}{2} = f\frac{(x+yf(x))}{2}$

$\frac{f(x)}{2} \ge \frac{1}{2}$

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

$a^n \in Im\frac{(f)}{2}$

$a<1$ e $a \in Im\frac{(f)}{2} \Rightarrow a^n \in Im\frac{(f)}{2}$

$f(x) \ge 2$

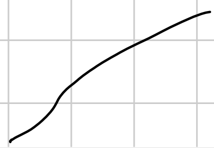
$f(x)f(y) \ge 2f(x)$

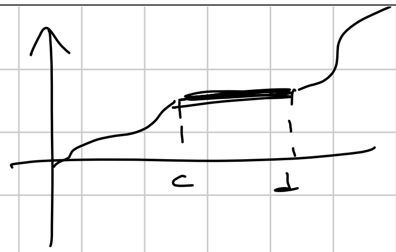
$\shortparallel$

$2f(x+yf(x))$

$f(x+\dots) \ge f(x) \Rightarrow$ f crescente

$x \in (c,d):\ f(c) = f(x) = f(d)$





$x = c$

$\cancel{f(c)}\, f(y) = 2\, \cancel{f(\underbrace{c+yf(c)})}$

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

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

$f(y) = 2$

$0 < y < \underbrace{\frac{d-c}{f(c)}}_{\alpha}$

$x = y: \ f(x) = 2 \Rightarrow f(3x) = 2$

$0 < x < 3^k \alpha \to f(x) = 2$

TST 06/3

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

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

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

$\underbrace{f(n) - 2n}_{c} = \underbrace{f(m) - 2m}_{c}$

$f(m) = 2m + c$

$a, b \in \mathrm{Im} f \Rightarrow a + b \in \mathrm{Im} f$

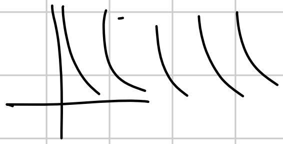
$a \in \mathrm{Im} f \Rightarrow na \in \mathrm{Im} f$

$a \neq 0 \Rightarrow |\mathrm{Im} f| = +\infty$

$a = 0 \Rightarrow f \equiv 0$

$f:\mathbb{Z}\to\mathbb{Z}$ e f periodica $\Rightarrow$ f limitata

$f(x)=\frac{1}{x}$ $\quad [0,1)$



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

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

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

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

$$f(m) = f(m+a-\cancel{f(a)}-b+\cancel{f(b)})$$

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

Algebra 3 (Medium) – Alberto Alfarano

BMO 07/2 $\qquad f:\mathbb{R}\to\mathbb{R}$

$$f(f(x)+y) = \underline{f(f(x)-y)} + \underline{4f(x)y}$$

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

$$f(z) = z^2 + f(0)$$

NO!!!!!!

per $z\in\mathbb{R}$

SI :)

per $z\in 2\,\mathrm{Im} f$

$f(x)-y = 2f(\omega)$

$y = f(x) - 2f(\omega)$

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

$$\boxed{f(z) = z^2 + f(0)}$$

SI :)

$z\in 2\,\mathrm{Im} f - 2\,\mathrm{Im} f$

o $f(x)=0 \qquad$ ok $\leftarrow$

$\exists x_0 : f(x_0)\neq 0 \qquad \leftarrow$

$$f(\quad) - f(\quad) = \underbrace{4f(x)y}_{=\mathbb{R}}$$

$f(x_0)$

$\mathrm{Im} f - \mathrm{Im} f = \mathbb{R}$

IMO 09/5

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

(a) $f(b)$, $f(b+f(a)-1)$

$a=1$ $\quad$ $1, f(b), f(b+f(1)-1)$

$$f(b)=f(b+f(1)-1)$$

$\boxed{f(1)=1}$

$$2+a=f(f(a))$$

$$a=f(f(a))$$

NO! per discorsi di iniettività e surgettività

$f(a), f(b), f(a+b-1)$ ←

$a, b, f(f(a)+f(b)-1)$ ←

$$f(a)+f(b) \geq f(a+b-1)+1$$

$$f(a)+f(2) \geq f(a+1)+1$$

$$a, b, f(f(a)+f(b)-1)$$

$a=b=2$ $\quad$ $f(2f(2)-1) \leq 4$

$f(f(2f(2)-1))=f(k)$ $\quad$ $k \leq 3$

$$2f(2)-1=f(k)$$

$$f(3) = 2f(2) - 1$$

$a=3,\ b=2$ $$f(3f(2)-2) = k \qquad k \leq 4$$

$$3f(2) - 2 = f(k)$$

$$3f(2) - 2 = 2f(2) - 1 \implies f(2) = 1$$

$$f(4) = 3f(2) - 2$$

$$f(n) = (n-1)f(2) - (n-2) \qquad n \geq 2$$

$a=n,\ b=2$

$$f(n) + f(2) - 1 = f(k) \qquad k \leq n+1$$

$$nf(2) - (n-1) = f(k)$$

Se $k \neq n+1$, $k \leq n$

$$nf(2) - (n-1) = (k-1)f(2) - (k-2) \qquad \text{no!}$$

$$\underline{n}(f(2)-1) = \underbrace{(k-1)(f(2)-1) - f(2) + 1}_{k(f(2)-1)-1} \qquad \text{Conti...}$$

$$f(2) \geq 2$$

$$f(n) = (n-1)f(2) - (n-2)$$

$$= n(f(2)-1) + \underbrace{2 - f(2)}_{c} = n$$

$$f(2) = h \geq 3 \qquad f(n) = \underbrace{n(h-1) + 2 - h}$$

$An + B$

$A \neq 1$ per assurdo.

$A = 2$

$2n + B$

$2n + 2 + B$

$2n + 1 + B$

$f(2) = 2$

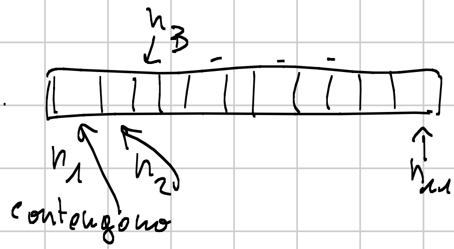
P-medium (C $\frac{1}{2}$ medium)

Note Title 9/2/2017

Non-esistenza

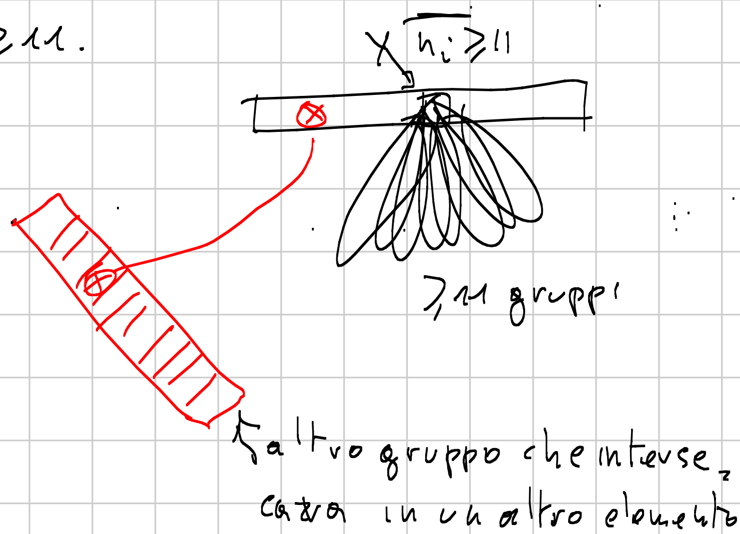
112 gruppi di 11 persone, che si intersecano a due a due in esattamente 1 persona.
Dimostrare che c'è una persona che appartiene a tutti i gruppi.

Fisso un gruppo



$n_1+\dots+n_{11} = 111 = 11\cdot 10+1$ Per il Princ. dei cassetti,

$\exists$ almeno un $n_i \geq 11$.



Gli 11 gruppi non contengono x e devono intersecare il gruppo rosso in elementi distinti, perché già si intersecano in x. Ma non ci sono abbastanza elementi.

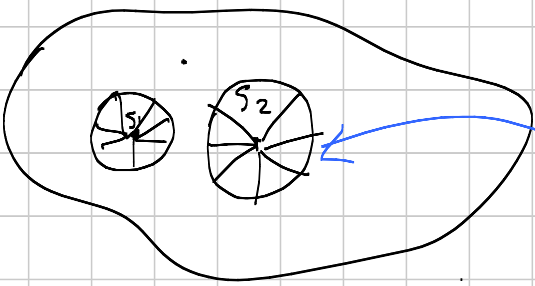
EGMO 2013/6 | 7 nani vanno a lavorare in miniera o a raccogliere fragole nel bosco (e non tutt'e due nello stesso giorno), per 16 giorni di fila. Risulta che il primo giorno siano andati tutti in miniera, mentre in ogni coppia di giorni almeno tre nani hanno scelto attività diverse. Dimostrare che c'è stato un giorno in cui sono andati tutti nel bosco a cogliere fragole.

1 2 3 4 5 6 7
M F M M F M F

$M \to 0$
$F \to 1$

$d(s_1, s_2) = \#$ simboli diversi
è una distanza

128 stringhe binarie



vicinato di raggio 1

Se per assurdo non esistesse la gita per fragole, esistono 16 stringhe $\neq 1111111$ i cui vicinati di raggio 1 sono disgiunti a 2 a 2

Oss. 16 vicinati da 8 stringhe, disgiunti, coprono tutte le 128 stringhe.

Distinguo le stringhe a seconda del numero di "1".

0	1	2	3	4	5	6	7
$\boxed{1}$	7	21	35	35	21	7	1

28 28

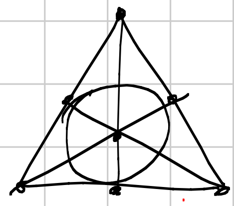
0000000

quindi per coprire tutto devo per forza usare

1111111.

Piano di Fano

7 insiemi di 3 elementi che si intersecano in esattamente 1 elemento a 2 a 2.



piano $\frac{k^3-1}{k-1}$

retta $\frac{k^2-1}{k-1}$.

Quante rette?

k rette

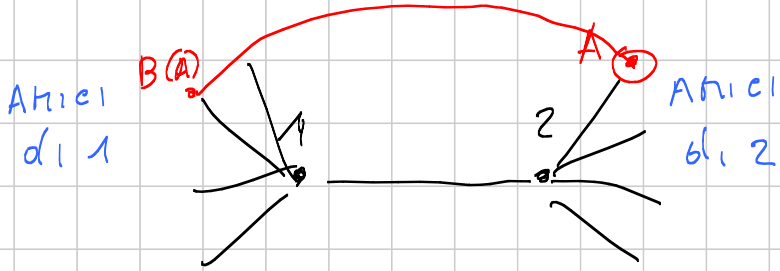
$\frac{k\cdot(k-1)}{2}$ intersez.

$4\cdot k - \frac{k\cdot(k-1)}{2} +$

$k\cdot(k-1)\#2$ gruppi da k el. con intersez. di 1 solo el. $\Rightarrow$ 1 el $\in$ tutti

BMO 1994/4 Minimo num. $n^{\cancel{7}5}$ di persone t.c. sia possibile che i) se 2 sono amici, non hanno amici in comune 2) se 2 non sono amici, hanno esatt. 2 amici comuni.

1° passo: tutti hanno lo stesso numero di amici!



A e 1 non sono amici, quindi oltre a 2

hanno un altro amico comune,
B (A)

Questo dà una corrisp. biunivoca tra {amici di A} e {amici di B}.
Se 1 e 3 non sono amici, passo attraverso un amico comune. □

Conto le persone. 1. amici di 1 amici degli amici di 1

k amici di 1.

1 contato k volte

amici degli amici $= k^2 - (k-1) - (n-k-1) = n-k$

amici degli amici contati 2 volte

$k^2 + k = 2n - 2$ però $n-2 \geq 2k$ anche, se no non è possibile la condiz. ①

$1 \to 2 < 5$
$2 \to 4 < 5$
$3 \to 7 < 3\cdot 2 + 2$
$4 \to 11$ NO
$5 \to 16$ SI

Imo SL 2016 C3) 3 n-agoni convessi hanno bordi C_1, C_2, C_3 nel piano. $C_1 \cap C_2$, $C_1 \cap C_3$ e $C_2 \cap C_3$ sono insiemi finiti di punti. Calcolare il valore massimo di $|C_1 \cap C_2\, C_3|$

BMO 07/4

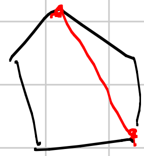
$(n,6)=1$ Coloriamo i vertici di un n-agono regolare di 3 colori, in modo che il numero di vertici di ogni colore sia dispari. Dimostrare che esiste un triangolo isoscele con i 3 vertici di 3 colori diversi.

a, b, c $\qquad n = a+b+c$.

X = # triang. isosc. monocolore

Y = # triang. isosc. 2-1

Ogni diagonale (coppia di vertici) partecipa a 3 triang. isosceli.



Double counting: $\boxed{\text{se non ci sono tri. isosc. multicol.}}$

$$\left|\left\{\left(\underset{\text{isosc.}}{\Delta},\ \underset{\substack{\text{che}\\ \text{congiunge}\\ \text{2 ver. dello stesso col.}}}{\text{lato}}\right)\right\}\right| = 3X + Y = 3\left[\binom{a}{2}+\binom{b}{2}+\binom{c}{2}\right]$$

contando per lati

Ma $X+Y = \binom{n}{2}$

mod 2, $\qquad X+Y \equiv \binom{n}{2}$

$$3X+Y \equiv 3\left[\binom{a}{2}+\binom{b}{2}+\binom{c}{2}\right] \equiv \binom{a}{2}+\binom{b}{2}+\binom{c}{2}$$

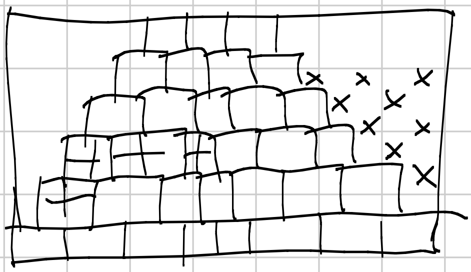
mod 4	a	b	c	n
	1	1	1	3
	1	1	3	1
	1	3	3	3
	3	3	3	1

3 pari $\to$ disp.
2 pari, 1 disp. $\to$ pari
1 pari, 2 disp. $\to$ disp.
3 disp. $\to$ pari.

ass.

RMM 2016/2 $\qquad n \geq m$. Tab. m righe $2n$ colonne.

voglio metterci il max numero di tasselli 2x1
in modo che i) non facciano mai
2) la riga in basso
sia piena di n tasselli orizz.
Quant'è il max?



Combinatoria 2 Medium

Note Title 9/3/2017

Esistenza non costruttiva

Estremale

In un insieme finito $\subseteq \mathbb{R}$ $\exists$ min/max
In un " $A \subseteq \mathbb{N}$, $A \neq \emptyset$ $\exists$ min

Modalità d'uso - normale

sia A un insieme, sia f una "valutazione" su A
$f: A \to \mathbb{R}$
$\Rightarrow$ posso prendere (uno dei) $a \in A$ tali che
$f(a)$ sia minimo

Di solito voglio mostrare che in A $\exists\, a$ t.c.
$P(a)$
allora mi invento f, prendo a t.c. $f(a)$ min
e dimostro che a soddisfa $P(a)$.

Es: sia G un grafo: dimostrare che esiste
una partizione $G = A \cup B$ t.c. $A \cap B = \emptyset$
t.c. $\forall\, a \in A$ l'insieme dei vicini $(a) \cap B$
$\forall\, b \in B$ sia più grande $\geq$
" $\cap A$

l'idea informale è "voglio massimizzare gli archi tra A e B"

più formalmente la $f : \left\{ \begin{matrix} \text{partizioni di } G \text{ in} \\ 2 \text{ sottoinsiemi} \end{matrix} \right\} \to \mathbb{N}$

e f conta quanti sono gli archi tra A e B

Sia A_{max}, B_{max}, voglio dimostrare la proprietà del testo

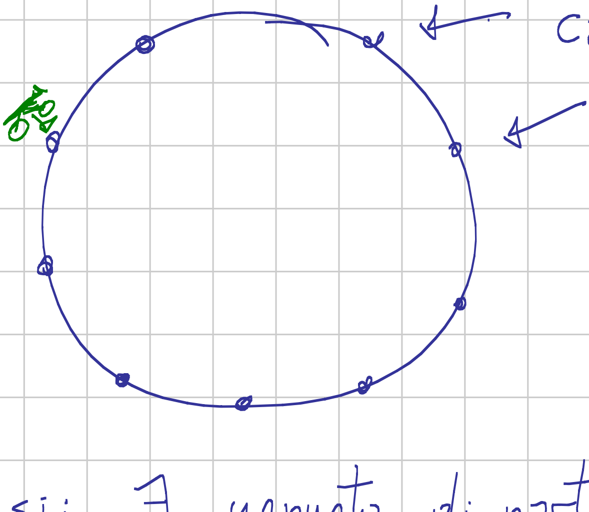
sia $a \in A_{max}$, allora supponiamo x ass. che

i vicini di a stiano strett. più in A_{max} che in B_{max};

sia $A_{max} \setminus \{a\}$, $B_{max} \cup \{a\}$

allora questa partizione viola la massimalità.

Es:



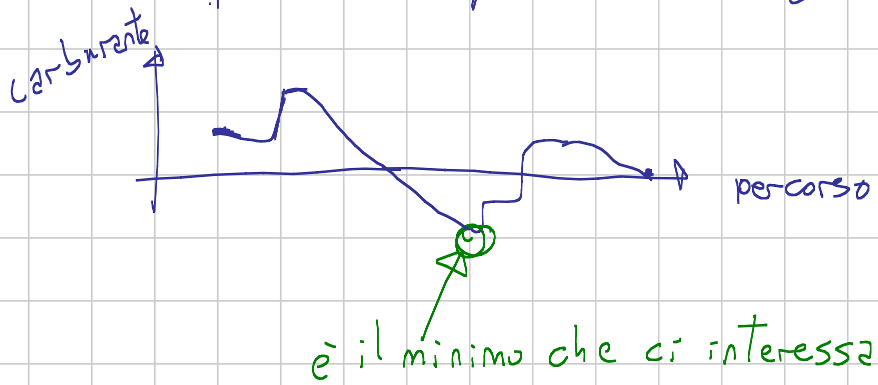
carburante

Σ carburanti è appena sufficiente per fare un giro

Tesi: $\exists$ un punto di partenza che permette l'intero giro

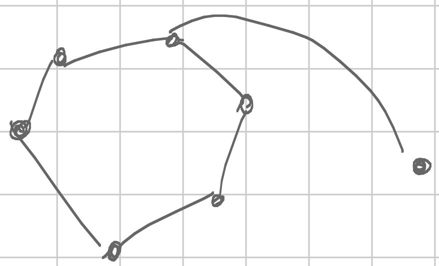
Idea: serve un minimo "globale"

Idea 2: proviamo a percorrere il giro comunque



Es: BMO13.4

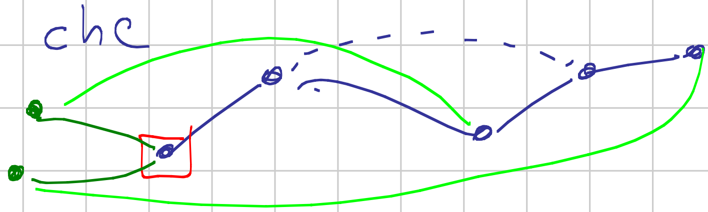
C'è un grafo con questa proprietà



poligono senza diagonali $\Rightarrow \exists \leq 1$ lato verso il poligono

Tesi: $\exists$ vertice v : $\deg(v) \leq 2$

Idea: cammino massimale in modo che



ora considero un estremo di questo cammino

quindi il $\boxed{\bullet}$ non poteva avere 2 ulteriori figli

Un approccio un po' diverso:

dato uno spazio S e una proprietà P che identifica alcuni sottoinsiemi di S

dimostrare che esiste uno di questi sottoins. T t.c. $|T| \geq$ qualcosa

L'idea generale è di prendere un sottoinsieme con massima cardinalità.

Es (vecchissimo TST):

A insieme, ci sono $T_1, \ldots, T_n$ terne di elementi t.c. $|T_i \cap T_j| \leq 1$

Tesi: $\exists$ un $S \subseteq A$ t.c. $|S| \geq \sqrt{|A|}$

S non contiene i T_i

Sol:

Prendo S massimale con la propr. che

"non contiene T_i"

la massimalità si traduce in una mappa

$$f: A \setminus S \longrightarrow \{\text{coppie non ordinate di } S\}$$

Oss: f è iniettiva come segue dall'ipotesi sull'intersezione delle T_i

$s = |S|$

$$|A| - s \leq \binom{s}{2}$$

$n = |A|$

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

$$2n \leq s^2 + s$$

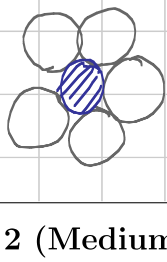
$$s \geq \sqrt{n}$$

Applicazioni geometriche

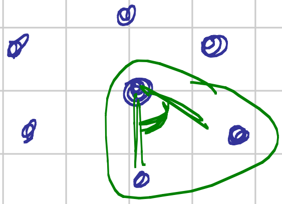
Es: ci sono alcuni cerchi finiti sul piano che non si intersecano, ma alcune coppie sono tangenti, i diametri sono tutti diversi

Tesi: $\exists$ cerchio con ≤ 5 tangenti

Sol: prendo il cerchio più piccolo!



suppongo x ass. che $\exists$ 6 cerchi tangenti



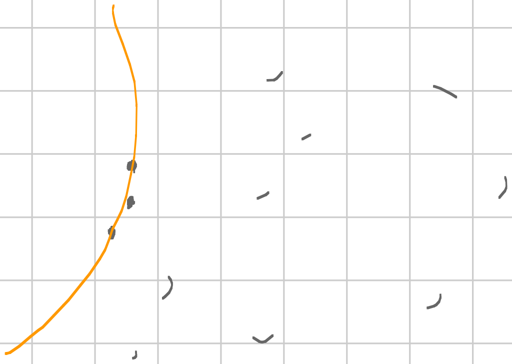
allora $\measuredangle > \frac{\pi}{3}$, assurdo.

Per casa: trovare il minimo n° di cerchi tangenti

Es (dal forum): ci sono n punti distinti non allineati allora

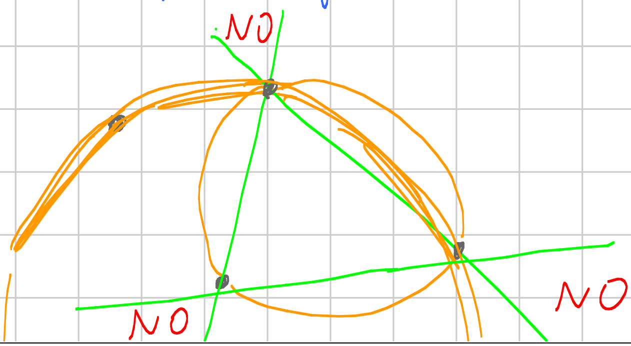
Tesi: $\exists$ 3 tali che la circonf. per loro 3 contiene tutti gli n punti

Sol: la circ. + grande NO (non subito)



L'idea è l'inviluppo convesso (è un oggetto massimale)

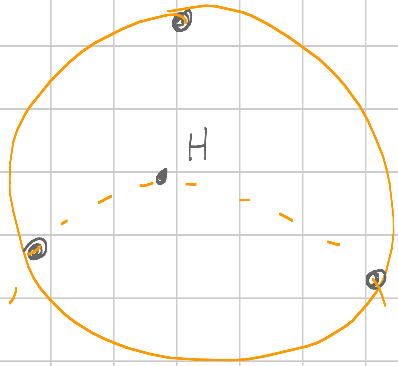
ora si posso prendere la circ. + grande



ha raggio strett. maggiore

Es: voglio una circonferenza che non contenga nessun punto (interno)
(con l'ipotesi che i punti non sia a 4 a 4 conciclici)

Sol:

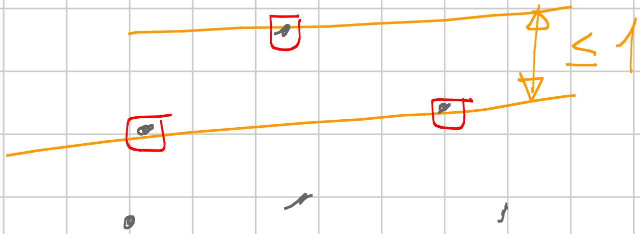


minimizzare la circonferenza e massimizz. un angolo intero

oppure

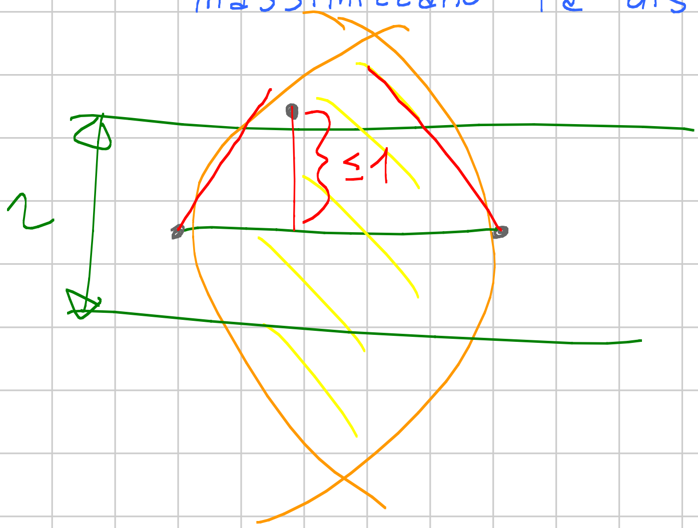
Prendere 2 vertici i più vicini possibile

Es: BMO 10.3

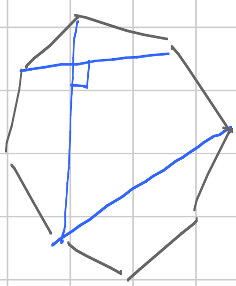


Tesi: tutti i punti sono contenuti in una fascia larga ≤ 2

Sol: Idea: prendo una delle coppie che massimizzano la distanza



Es: IMOSL 16 C5



Tesi: trovare il massimo n° di diagonali t.c.

non si intersecano oppure si intersecano $\perp$

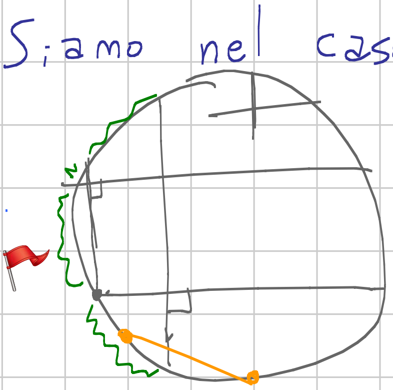
Sol:

Oss 1: se non ho intersezioni

al massimo ho $n-3$ diagonali

Oss 2 (x casa): nel caso dispari $n-3$ è già ottimale

Siamo nel caso pari

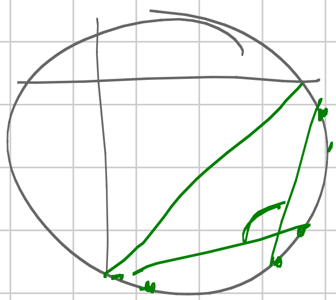


se guardo meglio le diagonali più lunghe ottengo il $+2$

ho preso k diagonali, quindi almeno k vertici $= \ell \geq k+2$

Per ogni archetto posso avere delle altre diagonali, ma nessuna diagonale può collegare archetti diversi

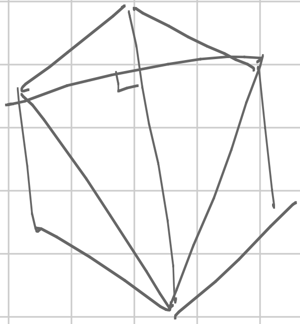
$A_1, \ldots, A_\ell$



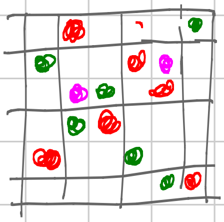
n° di diagonali prese $\leq$ ℓ

$$k + \sum_{i=1} (|A_i| - 2) = k - 2\ell + (n + \ell)$$

$$\overset{!}{=} n + k - \ell \leq n - 2$$

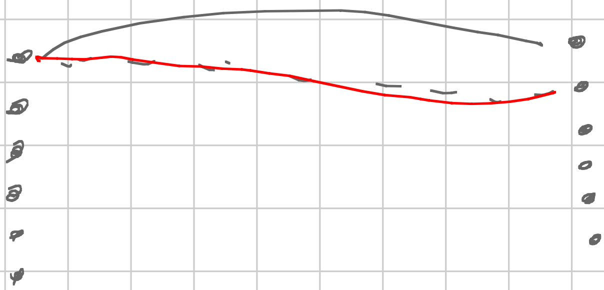


Es:



Costruisco un grafo bipartito

A = righe B = le colonne



Matching: è un insieme di archi tali che gli estremi sono tutti distinti.

Oss: ogni nodo (a sinistra) deve essere collegato a q.l.c.

ogni coppia deve avere collegati ≥ 2 vertici

Lemma di Hall (dei matrimoni):

in un grafo bipartito considero questa funzione

$$\Gamma : \mathcal{P}(A) \longrightarrow \mathcal{P}(B)$$
$$X \longmapsto \{ b \in B : b \text{ è collegato con uno dentro } X \}$$

se $\forall X \in A$, $|X| \leq |\Gamma(X)|$ allora riesco a estrarre un matching che comprenda tutti gli elementi di A

Sol: Se tutte le $\leq$ dell'ipotesi sono $<$, allora posso collegare un tizio $a \in A$ a caso

Devo verificare l'ipotesi induttiva

$A \setminus \{a\}$ $\qquad$ $B \setminus \{\text{vicino estratto a caso}\}$

$\cup\!|$

$Y \longrightarrow \Gamma_{B\setminus caso}(Y)$

$$|Y| > |\Gamma_{B\setminus caso}(Y)|$$

se guardo Y nel problema originale

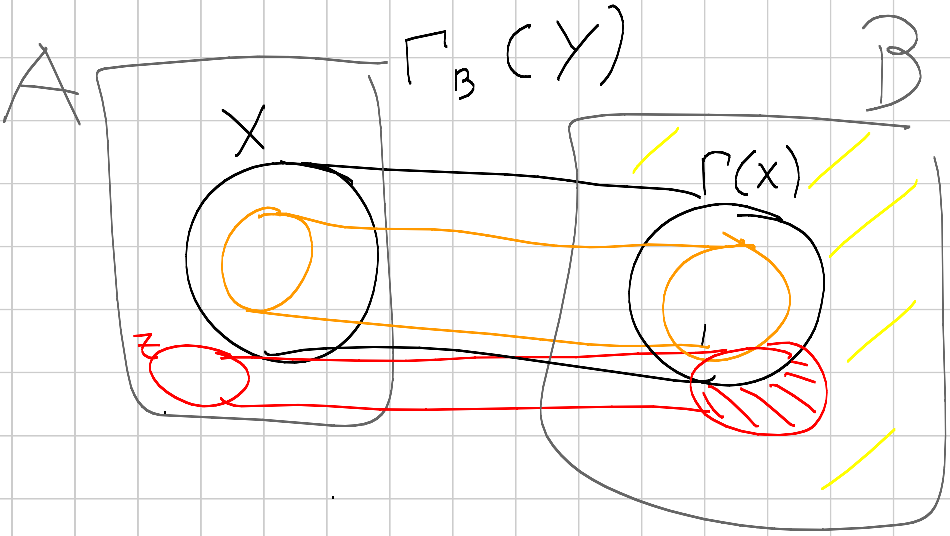
$$|Y| < |\Gamma_B(Y)|$$

ma $|\Gamma_B(Y)| - |\Gamma_{B\setminus caso}(Y)| \leq 1$

Se invece ho un' $=$

$$|X| = |\Gamma_B(X)|$$

$$Y \subseteq X, \quad |\Gamma_{\Gamma_B(X)}(Y)| \geq |Y|$$
$$\Gamma_{\Gamma_B(X)}(Y) = \Gamma_B(Y)$$



$$Z \subseteq A \setminus X \qquad \Gamma_B(Z) \setminus \Gamma(X) =: \Gamma_{B\setminus\Gamma(X)}(Z)$$

qui, non è detto che
$$\Gamma_{B\setminus\Gamma(X)}(Z) = \Gamma_B(Z)$$

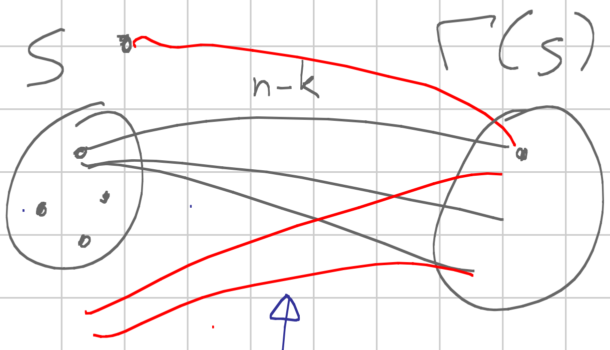
$$\cancel{|X|} + |Z| = |X \cup Z| \leq |\Gamma_B(X \cup Z)|$$
$$= \underbrace{|\Gamma_B(X)|}_{= \cancel{|X|}} + \underbrace{|\Gamma_B(Z) \setminus \Gamma_B(X)|}_{= |\Gamma_{B\setminus\Gamma(X)}(Z)|}$$

Torniamo alla Tabella:

dobbiamo verificare che $\forall\, S \subseteq \text{righe}$
$|\Gamma(S)| \geq |S|$

in una tabella $n \times n$ ho già usato k colori

per il $k+1$ colore ogni riga è collegata a $n-k$ colonne e viceversa



$$|S|(n-k) = \underbrace{|E|}_{\text{gli archi in mezzo}} = |\Gamma(S)|(n-k) - |\{\cancel{\ }\}| \leq |\Gamma(S)|(n-k)$$

Lemma: vale il Lemma di Hall se
$\deg(a) \geq \deg(b) \quad \forall a \in A, b \in B$

Es: Vietnam 2010 TST 5

$n > m > 1$

nazioni

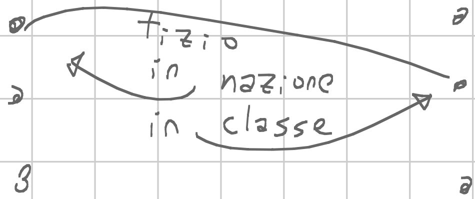
n classi

m persone $\forall$ nazione
ogni classe contiene m persone di nazioni diverse

Tesi: $\exists$ un rappresentante $\forall$ nazione che rappresentino anche le classi

Sol: costruisco un grafo bipartito

Nazioni Classi



Vale l'ipotesi del Lemma del Lemma di Hall $\square$

Ordini parziali

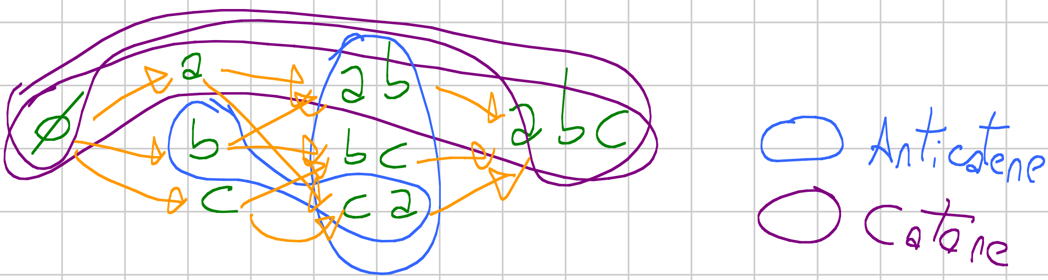
relazione antisimmetrica (antiriflessiva) e transitiva in un insieme

- il $\subseteq$ (tra insiemi)
- la $|$ (in $\mathbb{Z}$)

Una **Catena** è un sottoinsieme di elementi tra loro confrontabili

Una **Anticatena** è un sottoinsieme di el. tra loro mai confrontabili

Es X insieme $= \{a, b, c\}$



Th (Dilworth): C una catena, P_A una partizione in anticatene

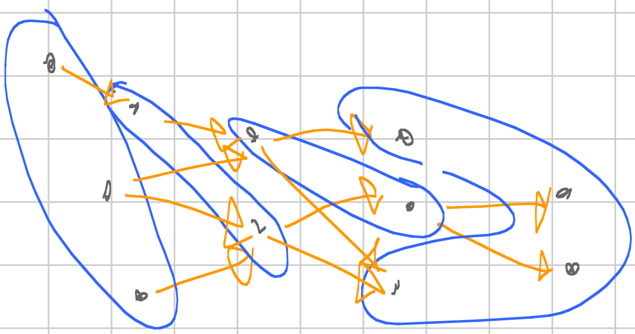
$$|C| \leq |P_A|$$

1) $\exists\ C, P_A$ t.c. $|C| = |P_A|$

$$|A| \leq |P_C|$$

2) $\exists\ A, P_C$ t.c. $|A| = |P_C|$

Dim:



prendo i + grandi = dove non arrivano frecce

togliendo loro procedo per induzione sulla lunghezza della catena più lunga $\square$

Es (lemma ab+1)

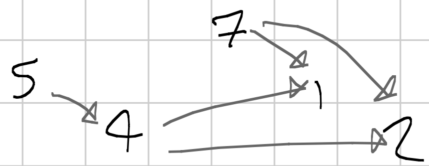
5 4 7 1 2 ho ab+1 reali scritti in fila

Anticatena

Tesi: $\exists$ a+1 reali crescenti $\vee$

$\exists$ b+1 reali decrescenti Catena

Sol:



se $\nexists$ b+1 decr., allora la max catena è lunga $\leq b$

$\Rightarrow$ $\exists$ partizione in $\leq b$ anticatene

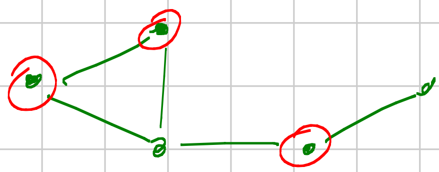
Dilworth

$\Rightarrow$ $\exists$ una anticatena $\geq a+1$

Pigeonhole

La seconda parte di Dilworth discende (abbastanza) facilmente dal seguente:

Def: Covering di un grafo è un insieme di nodi t.c. ogni arco ha un estremo in uno di questi



Th (Koenig): Dato un grafo bipartito $G = A \cup B$, allora

$\mathcal{M}$ matching, $\mathcal{C}$ covering

$$|\mathcal{M}| \leq |\mathcal{C}|$$

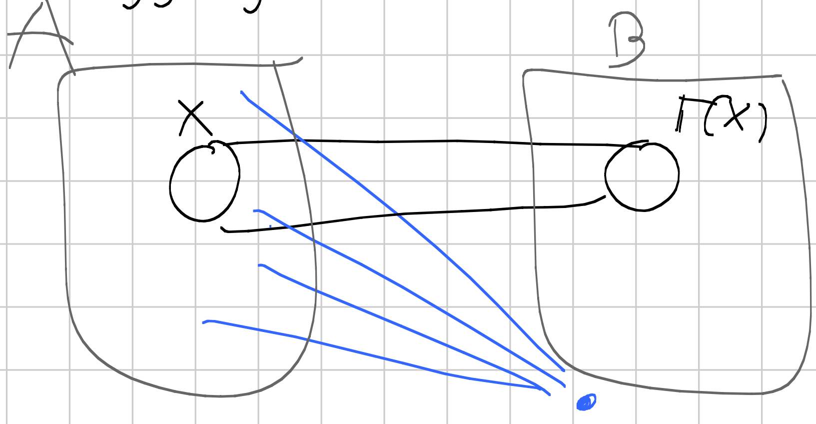
$$\exists\ \mathcal{M}, \mathcal{C} : |\mathcal{M}| = |\mathcal{C}|$$

Dim: prendiamo

$$|X| \leq |\Gamma(X)| \quad \forall X \subseteq A$$

supponiamo $|X| \leq |\Gamma(X)| + 1$

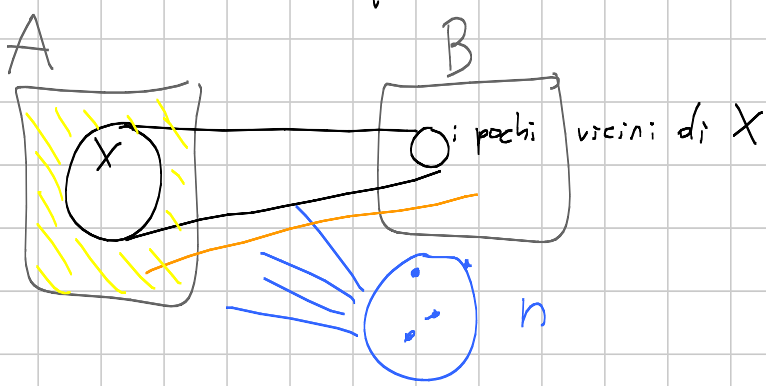
aggiungendo un tizio a B amico di tutto A



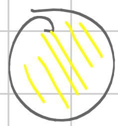
Per il Lemma di Hall $\exists$ matching tra A e $B \cup \{\bullet\}$, trascurando ora $\bullet$ ottengo un matching di tutti tranne al + 1 tizio $a \in A$

Prendo X t.c. massimizza $|X| - |\Gamma(X)|$

sia n questo massimo



Hall
$\Rightarrow$ $\exists$ matching di cardinalità $|A| - n$

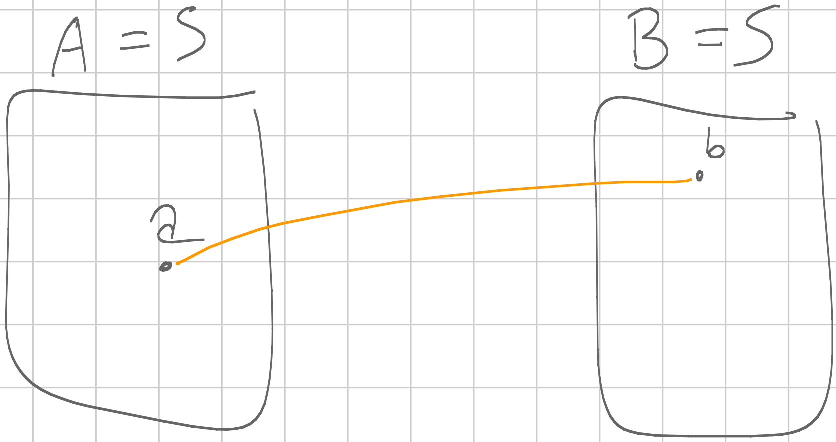
Per il covering: prendo $\Gamma(X)$ e  $A \setminus X$

$\Rightarrow$ il covering ha cardinalità $|A| - |X| + |\Gamma(X)|$ $\square$

Per dimostrare Dilworth 2

S con ordine parziale

$A = B = S$



$a \cdot \quad \cdot\, b$ quando $a < b$.

Per Casa: – Completare questa dimostrazione

– Calcolare la massima cardinalità di una $\mathcal{F} \subseteq \mathcal{P}(X)$ t.c.
$\forall\ I, J \in \mathcal{F} \quad I \not\subseteq J \ \wedge\ I \not\supseteq J$

Combinatoria 3 ½ Medium

Tess

Note Title 9/7/2017

Esistenza Costruttiva

- [x] Conservare i casi di = in una stima del bound

Es: Belarus 2004 A6

30 partecipanti ad una gara di 8 problemi
ciascuno risolve oppure no ciascun problema
alla fine un problema vale tanti punti quanti NON l'hanno risolto
risulta che un solo tizio arriva ultimo
Quanto ha fatto al max?

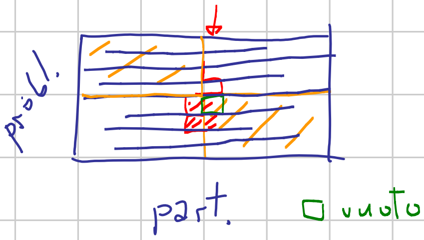
Sol: conto, o meglio, stimo la somma dei punteggi

$$2n^2 \geq \sum_{i=1}^{8} k_i(n-k_i) = \underset{\text{per problema}}{\Sigma \text{ punteggi}} \geq \underset{\text{per partec.}}{u + (n-1)(u+1)}$$

$$= \underbrace{(n-1)}_{n+1} + un$$

$u \leq 2n - 1$

quindi $u \leq 59$



59 | 74 + 14 | 58 | 59

Il problema si finisce rifinendo la disuguaglianza

Algoritmi

Es: G un grafo $\deg(v_i) < d \Rightarrow$ posso colorare G con d colori

(Def: una colorazione di G è una mappa

$\mathcal{C}: V \to \{\text{colori}\}$ t.c. se v_1, v_2 sono vicini
$\mathcal{C}(v_1) \neq \mathcal{C}(v_2)$)

Sol: tecnica alla "greedy" coloro un tizio alla volta del primo colore disponibile

(fisso un ordinamento di V e dei colori)

Oss: l'algoritmo produce una colorazione (valida)

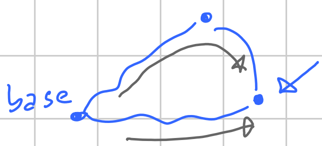
Oss: uso al max d colori.

[Colorazioni di grafi bipartiti in particolare:

posso bi-colorare un grafo $\Leftrightarrow$ non ammette cicli dispari

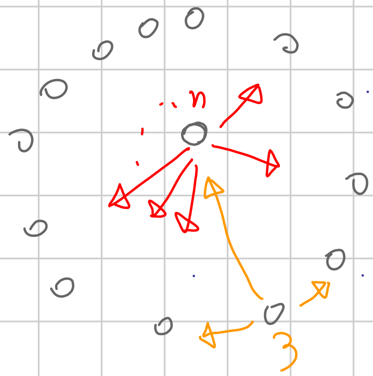
un tizio lo coloro a caso e parto da lui per colorare gli altri

va male solo se



ho trovato un ciclo dispari]

Es (China recente, ma facile)



n posizioni attorno al centro
ogni posizione contiene gettoni
in totale $\geq n^2+3n+1$
2 mosse:

Tesi: mostrare che riesco a porre almeno $n+1$ gettoni ovunque

Sol: per livellare le esterne, applico tantissime finché nessuno ha >2 gettoni

ora applico la $n+1$ volte, sono sicuro che sulla circonferenza ho almeno $n+1$ gettoni per posizione

al centro però ho $\geq n^2+3n+1-(n+1)n$ − quelli che non ho mai portato al centro

anche 2 per posizione

≥ 3

allora, invece che applicare subito tutte le ne faccio una così, tutti i tizi che mi davano note avendo 2 gettoni ne ottengono 3
e voglio ottenere al massimo tanti tizi con 3 quanti con 1
mi basta alternare tizi da 3 con tizi da 1

No a cose come $3^{32}\ 2\ 3$

x casa trovate delle super-mosse che tolgono queste situazioni

Es: (Turàn) In un grafo non ho k-cricche, quanti sono al massimo gli archi?

Sol: facciamo le seguenti mosse:

assegno un reale ad ogni vertice

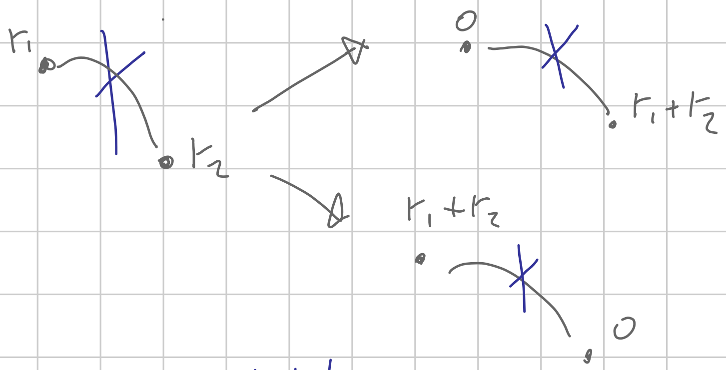
all'inizio 1

$$X = \sum_E r_1 \cdot r_2$$

dove 1 e 2 sono gli estremi dell'arco

all'inizio $X = |E|$

ora, ad ogni mossa, prendo un arco t.c. i 2 estremi hanno $r_i \neq 0$ e trasferisco uno dei 2 all'altro



scelgo la possibilità che non fa calare la X

X varia in questo modo:

~~perdo $r_1 r_2$~~

perdo $\not\! \;\; r_1 \cdot \left(\sum_{\text{vicini di } 1} r_i \right)$

$\not\! \;\; r_2 \cdot \left(\sum_{\text{vicini di } 2} r_i \right)$

guadagno $\to \;\; r_1 \cdot \left(\sum_{\text{vicini di } 2} r_i \right)$

$\searrow \;\; r_2 \left(\sum_{\text{vicini di } 1} r_i \right)$

l'algoritmo finisce e lascia una cricca di vertici non nulli

allora $$|E| \le X \le \sum_{\substack{i<j \\ \in \text{cricca}}} r_i r_j \le \left(\frac{\sum r_i}{R-1} \right)^2 \cdot \binom{R-1}{2} = \left(\frac{n}{R-1} \right)^2 \binom{R-1}{2}$$

Es: (BMO 12.3)

$$A = \{ 2^n, 2^{n-1} \cdot 3, 2^{n-2} \cdot 3^2, \dots, 3^n \}$$

$$y \in [0, 3^{n+1} - 2^{n+1})$$

Dimostrare che $\exists \; S \subseteq A$ t.c. $\sum_{s \in S} s = \Sigma(S)$

$$0 \le \Sigma(S) - y < 2^n$$

Sol: algoritmo greedy: metto dentro S il + grande che non fa sforare $<$

Devo verificare che allora
$\Sigma(S) \geq y$

Suppongo per assurdo che $\Sigma(S) < y$, allora

per esempio $S \ni 2^n$, si procede in questo modo

X casa: scrivere le disuguaglianze che chiudono

Es: (IMO 14.5) Esistono solo monete
del valore di $\frac{1}{n}$ per $n>0$ intero

Dispongo di una somma $\leq 99 + \frac{1}{2}$

Tesi: mettere tutto in 100 scatole, t.c. ciascuna
non abbia più di 1.

Sol: dispongo la moneta + grossa nella scatola
più piena che la contiene

Da qui si scrivono delle disuguaglianze, ma non torna

Idea ulteriore: cercare di accorpare le monete
es: se ho $\frac{1}{3}, \frac{1}{3}, \frac{1}{3}$ fingo di avere solo
una da 1
accorpo anche cose come $\frac{1}{10} \; \frac{1}{10} \to \frac{1}{5}$

(mi riservo la possibilità di fare
$\frac{1}{15} \; \frac{1}{15} \; \frac{1}{15} \to \frac{1}{5}$)

ora dispongo di una disuguaglianza forte:

$$\sum_{m_i<1} m_i \leq \frac{1}{2}+\frac{2}{3}+\frac{3}{4}+\frac{4}{5}+\ldots$$

$$\hookrightarrow \leq \frac{1}{2}+\frac{2}{3}+\frac{1}{4}+\frac{4}{5}+\frac{1}{6}+\ldots$$

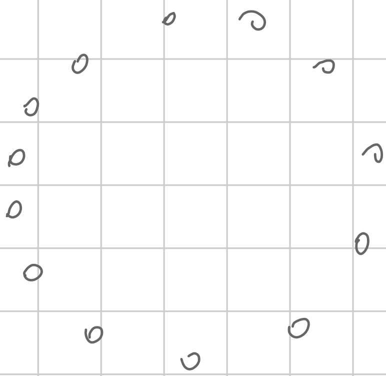
La disug. da impostare è

stimare spazio vuoto
e la moneta + grossa che rimane fuori

per casa risolvete il problema

Es per casa IMOSL 13.1

Es: BMO 2017.4



una moneta $\forall$ vertice (in tot $= n$)

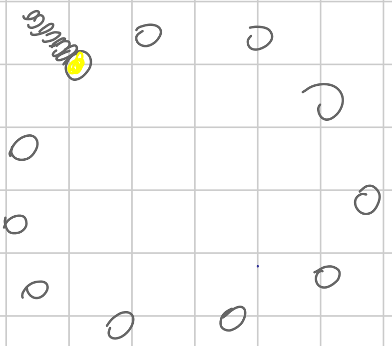
- sposto una moneta al vicino
- mando k moneta ad un vicino le altre all'altro

Una mossa completa è scegliere $\forall$ vertice quale eff.

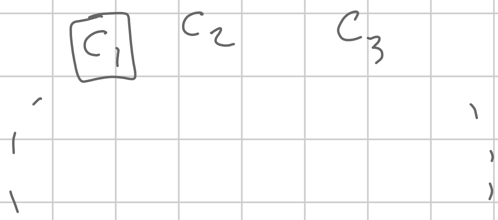
Tesi: contare (capire) quali conf. ottengo

Sol: Raccolgo tutte le monete su un vertice

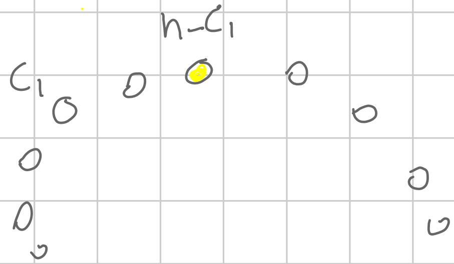
(se n dispari, faccio il giro dall'altra parte e raccolgo tutto non in 2 ma in 1 vertice)



Cerco di usare solo le



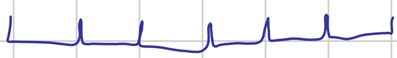
Ne stacco c_1, le altre le mando avanti



Su tutti vertici tranne ○ faccio la mandando tutto all'indietro, su ○ stacco la quantità giusta e la mando indietro; il resto avanti (anche il gettone ○ va avanti)

per casa esercizio di scrittura

Es per casa: IMO 2010 . 5



tutte hanno un gettone

butto 1 da B_i e ne aggiungo 2 alla B_{i+1}

butto 1 da B_i e scambio B_{i+1} e B_{i+2}

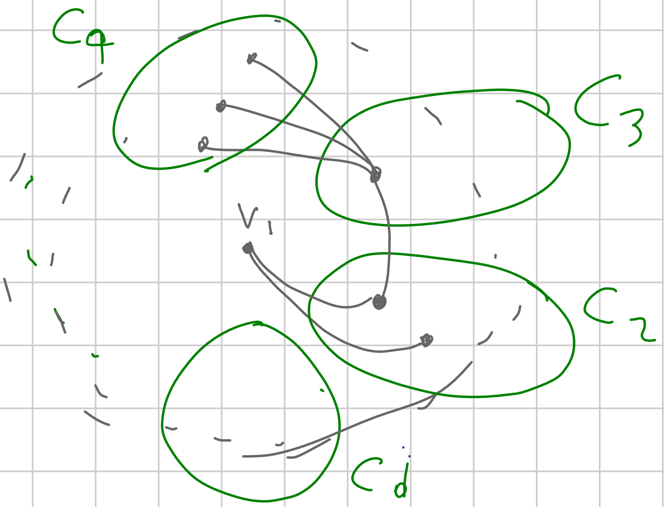
Tesi: ne voglio esattamente $2010^{2010^{2010}}$ sulla B_6

Es: Lemma chiave di IMOSL2015 C8

Se un G è d-colorabile, ma non $d-1$ colorabile allora esiste un ciclo che prende tutti i colori. $(d > 2)$

Oss: è facile vedere che esiste un cammino che attraversa tutti i colori   per casa
(potete provare Dilworth ...)

Sol: seleziono $v_1 \in C_1$



Oss 1: per assicurarmi di un ponte tra v_1 e C_2 cerco di colorare il minimo numero di vertici col colore C_1 (e così via per tutti i C_i)

Oss 2: tutti i tizi • sono collegati con v_1

Mega trucco: sposto i grigi in avanti di 1 colore (tranne v_1)

Oss 3: ottengo ancora una colorazione lecita

Ora c'è un tizio • t.c. ora sta in C_2
prima era in C_d collegato con v_1

altrimenti v_1 lo potevo spostare (in C_2 o C_d ...)

▨ Costruzioni induttive

Es: IMO 2017.5

$N(N+1)$ tizi in fila
ne voglio eliminare $N(N-1)$, quindi rimarranno $2N$ tizi
$b_1, b_2, b_3, \dots, b_{2N}$

Tesi: voglio che nell'ordine con cui rimangono nessuno
stia tra b_1 e b_2 ; "
" b_2 b_3 ⋮
... b_{2N-1} b_{2N}

Sol: se b_1 e b_2 sono vicini, la prima condizione è soddisfatta

Oss: voglio una costruzione induttiva

Nel passo induttivo voglio eliminare $2N$ e ricordarmi i tizi che diventeranno b_1 b_2.

$N+1$ blocchi da N

vorrei prendere $b_1\, b_2$ da uno stesso blocco, eliminare i tizi di quel blocco e altri N da gli altri blocchi

da ogni blocco c'è una coppia candidata a (b_1, b_2) prendo quello con b_2 più basso

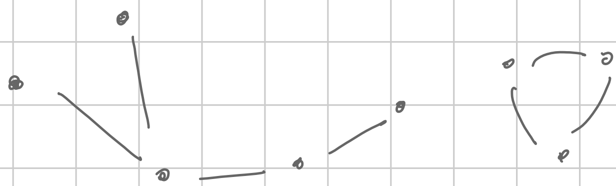
gli altri N sono tolti 1 per blocco (il + basso b_1)

Es: voglio contare quante sono le colorazioni con $|d|$ colori di un Grafo G

$G =$

Sol: voglio un'induzione su G togliendo archi o vertici

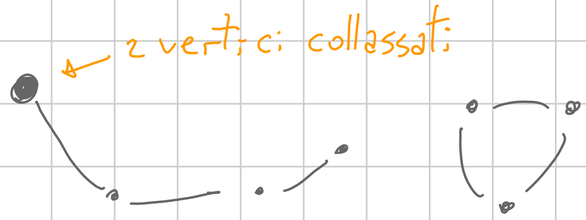
$G' =$



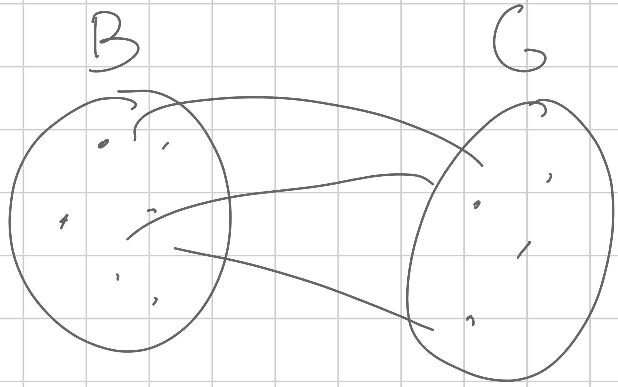
Sia $\mathcal{C}(G)$ il # di colorazioni allora relazione tra $\tau(G)$ $\tau(G')$?

$$\tau(G') - \tau(G) = \tau(G'')$$

$G'' =$



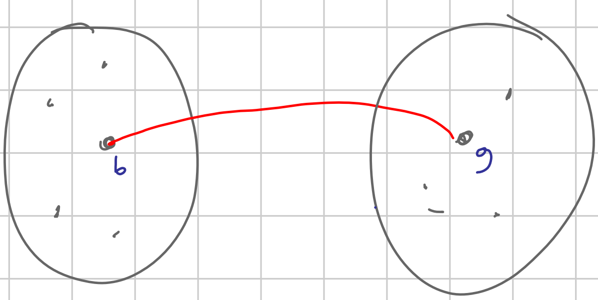
Es: (RMM 2012.1)



$f(B,G)$ = numero di sottoinsiemi di B "popolari"
$g(B,G)$ = " G "

Tesi $f(B,G) \equiv g(B,G) \mod 2$

Sol: dimostro la tesi induttivamente



$f(B', G')$, $g(B', G')$ dove B', G' sono gli stessi di B, G ma senza

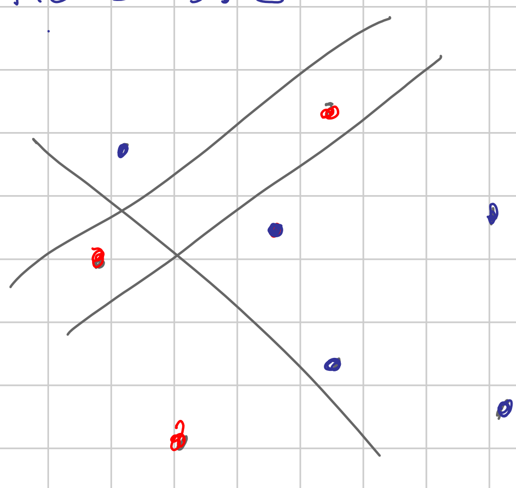
$f(B, G) - f(B', G') = ?$

$f(B' \setminus B_g \; , \; G' \setminus G_b)$

per casa — conoscenti di g — conoscenti di b

Ora l'ipotesi induttiva (induzione estesa) finisce

Es IMO 2013.2



rossi blu
2014 + 2013 punti disegnati
non allineati a 3 a 3

ho a disposizione 2013 rette voglio dividere i punti • dai punti •

Sol: Spero in un'induzione sul numero di punti blu che è = al numero di rette

potrei usare 2 rette per separarne 2

Infatti, dati 2 punti blu, traccio 2 parallele alla loro congiungente molto vicine

Devo però sistemare l'ultimo punto (conviene sistemarlo in anticipo)

per casa: completare

(una possibile idea è trovare  senza • all'interno ... vedere se funziona.)

Es: TUR 2013 TST 9

G un grafo t.c. il grado minore è $\geq k$
su n vertici connesso

allora posso colorare G con $n-k$ colori,
t.c. $\forall$ coppia di archi esiste un cammino multicolor che li congiunge

Sol: traccia:

induzione (estesa) sul grafo G

i) studiare quando si riesce a togliere un arco

ii) " togliere un vertice di grado k
(si riesce a ricondursi al caso più piccolo se i vicini hanno almeno $k+1$ vicini)

iii) diminuire le cricche di tizi che hanno grado k

per casa provare questo problema (PreIMO 14 C7)

Es stupido: se un grafo G è t.c. $\forall$ sottografo $\exists$ un vertice di grado $\leq k$ allora si può $k+1$ - colorare G

Giochi

Th: A e B giocano al seguente gioco: ciascuno a turno eff. una mossa dopo finite mosse uno tra A e B viene dichiarato vincitore

$\Rightarrow$ uno tra A e B ha una strategia vincente

Dim: induzione sull'albero delle partite

↳ assumendo finite config. e finite mosse possibili per terminare il gioco

P.B. dalle foglie ...

P.I. sono in un vertice V, tocca wlog A

se A può effettuare una mossa per lasciare B in un V perdente la fa (e V diventa vincente per A)
altrimenti A gioca a caso e perde (V diventa vincente per B)

Oss: alla fine i vertici sono tutti colorati di V o P

se un giocatore sta su un V, allora $\exists$ mossa che lo manda in P

e se " " P, $\forall$ mossa il vertice in arrivo è V

Es stupido: c'è una pila di gettoni e ciascuno (A e B) possono togliere 1, 2, 3, 4 gettoni; chi non può togliere perde!

Sol: P = { config. dove ci sono $\equiv 0$ (5) gettoni }

V = le altre

Es (Nim): ci sono tante pile di gettoni; ciascuno (A e B) deve scegliere una pila e togliere almeno un gettone; vince chi toglie l'ultimo

Sol: in ogni momento $(g_1, g_2, \dots, g_n)$

scrivo in binario g_i e faccio XOR

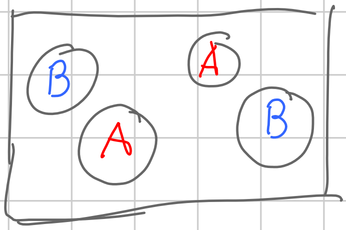
$(5, 6, 7)$

$$\begin{array}{r} \to 101 \\ 110 \\ 111 \\ \hline 100 \end{array}$$

se il risultato è 0 sono in P, altrimenti in V per casa: dimostrate che questa è una distinzione corretta

☑ L'opposizione nei giochi:

Es: Gioco della preparazione della tavola:



chi non può mettere piatti perde

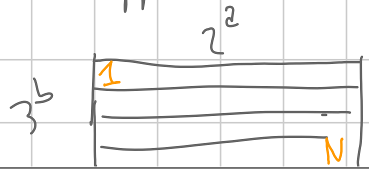
Sol: A vince giocando al centro
poi A gioca ponendo il piatto all'opposto di come gioca B

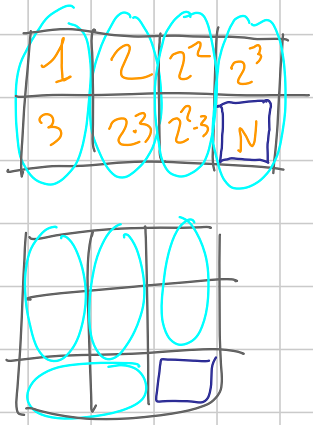
Es: Si gioca con i divisori di N

A, B possono cancellare uno dei divisori (>0) di N che all'inizio sono scritti alla lavagna

A inizia cancellando N
però se uno gioca d, dopo l'altro deve giocare d' t.c. $d \mid d' \vee d' \mid d$

Sol: supponiamo $N = 2^a \cdot 3^b$





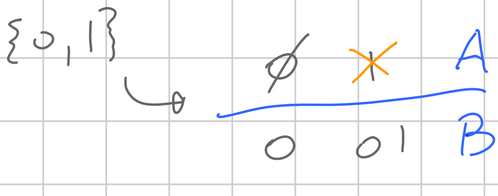
se A gioca dentro un 0
B risponde " lo stesso 0

per casa esercizio di scrittura: dire come eff. la suddivisione in coppie

Es: IMOSL 2014 C8

A e B prelevano ad ogni mossa uno dei sottoinsiemi di $\{0, \dots, 9\}$

Alla fine ciascuno controlla se ha pescato un sottoinsieme t.c. tolto quello ogni cifra compare un numero pari di volte, se ci riesce, vince



Tesi: dire chi vince dopo ciascuna mossa di A

Sugg. chiave: $\displaystyle\sum_{k \text{ dispari}} \binom{n}{k} = \sum_{k \text{ pari}} \binom{n}{k}$

Sol (con D-C): scelgo $x \in A$ dove $|A| = n$

ci sono sottoinsiemi che hanno x

e altri che non ce l'hanno

Per casa, pensateci!

G1 medium - Contazzi

Note Title 9/3/2017

TI 2017 : 10) $z_1 = 18+83i$ $z_2 = 18+39i$

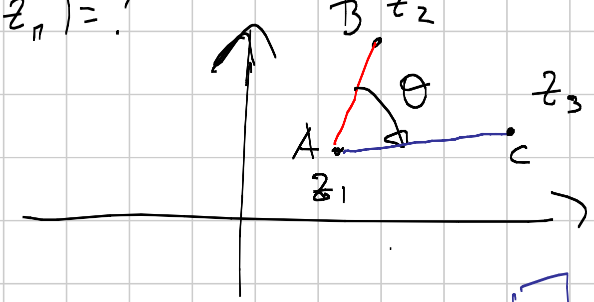
$z_3 = 78+99i$

$$S = \left\{ z \in \mathbb{C} : \frac{z_3 - z_1}{z_2 - z_1} \cdot \frac{z - z_2}{z - z_3} \in \mathbb{R} \right\}$$

$z_\Pi \in S$ è "quello con la parte immaginaria maggiore".

$Re(z_\Pi) = ?$

Sol:

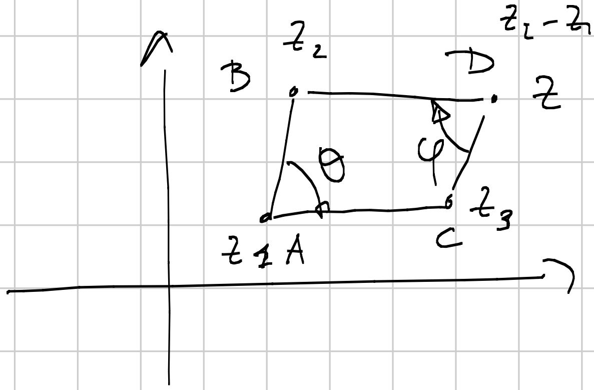


$\mathbb{C}$

$x \longrightarrow \dfrac{x - z_1}{z_2 - z_1}$

$$\frac{z_3 - z_1}{z_2 - z_1} = \underbrace{\boxed{\frac{AC}{AB}}}_{\in \mathbb{R}} e^{i\theta}$$

$\mathbb{R}$



$$\frac{z - z_2}{z - z_3} = \boxed{\frac{DB}{DC}} e^{i\varphi}$$

$z \in S$

$\Updownarrow$

$e^{i\theta} \cdot e^{i\varphi} \in \mathbb{R}$

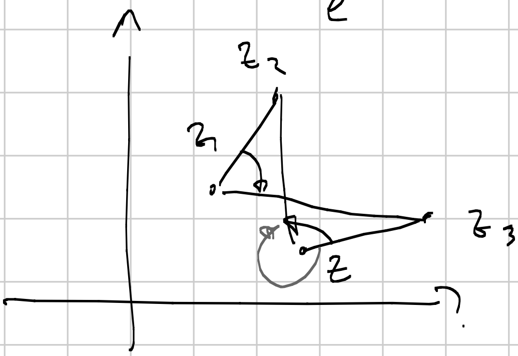
$\parallel$

$\theta + \varphi = k\pi \quad k \in \mathbb{Z} \iff e^{i(\theta+\varphi)} \in \mathbb{R}$

$\theta + \varphi = \pi \iff z_1, z$ stanno da parti opp. di BC e ABCD ciclico

$\theta+\varphi = \underset{0}{2\pi} \iff z_1, z$ stanno dalla stessa parte di BC

e $\widehat{BAC}=\widehat{BDC} \iff$ ABCD ciclico.



$\Rightarrow \quad S = $ cfr per z_1, z_2, z_3

Oss: Se z_1, z_2, z_3 sono allineati, S diventa.... una retta!

$\Downarrow$

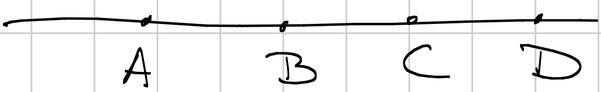
$\frac{z_3-z_1}{z_2-z_1}\in\mathbb{R}$

$z\in S \iff \frac{z-z_2}{z-z_3}\in\mathbb{R}$

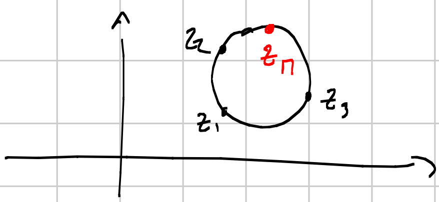
$\Updownarrow$

$\varphi = 0, \pi$

$\frac{z_3-z_1}{z_2-z_1}\cdot\frac{z-z_2}{z-z_3}$

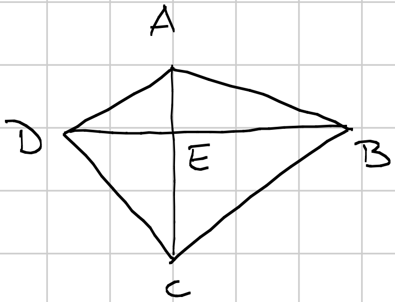


$\frac{AC}{AB}\cdot\frac{BD}{CD}$ birapporto $(A, D; B, C)$



Re(centro) = 56

TI '17 - II)



i simmetrici di E risp. ai lati sono conciclici.

$\boxed{\text{V/F?}}$

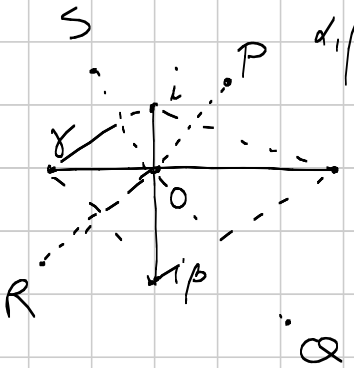
rimetto tutto a posto.

$$x \longrightarrow x-a \longrightarrow \frac{x-a}{b-a} \longrightarrow \frac{\bar{x}-\bar{a}}{\bar{b}-\bar{a}} \longrightarrow \frac{\bar{x}-\bar{a}}{\bar{b}-\bar{a}}(b-a)$$

traslo A in O — porto B in 1 — coniugo

$$\frac{\bar{x}-\bar{a}}{\bar{b}-\bar{a}}(b-a)+a$$

$\alpha,\beta,\gamma\in\mathbb{R}$



$$P=\frac{i}{\alpha+i}(\alpha-i)+i$$

$$Q=\frac{i\beta}{\alpha+i\beta}(\alpha-i\beta)+i\beta$$

$$R=\frac{i\beta}{\gamma+i\beta}(\gamma-i\beta)+i\beta$$

$$S=\frac{i}{\gamma+i}(\gamma-i)+i$$

$$P=\frac{i}{\alpha+i}(\alpha-i)+i=i\left(\frac{\alpha-i+\alpha+i}{\alpha+i}\right)=\frac{2\alpha i}{\alpha+i}$$

$$Q=\frac{2\alpha\beta i}{\alpha+i\beta}\qquad R=\frac{2\gamma\beta i}{\gamma+i\beta}\qquad S=\frac{2\gamma i}{\gamma+i}$$

$$\frac{p-q}{p-r}\cdot\frac{s-r}{s-q}\in\mathbb{R} \longleftarrow \text{per casa}$$

Oss: se $a, b \in$ cf. unitaria

$$\frac{\bar x-\bar a}{\bar b-\bar a}(b-a)+a = \frac{\bar x - \frac{1}{a}}{\frac{1}{b}-\frac{1}{a}}(b-a)+a =$$

$$= \frac{\frac{\bar x a-1}{\cancel{a}}}{\frac{\cancel{a-b}}{\cancel{a}b}}\,\overset{-1}{\cancel{(b-a)}} + a =$$

$$= b - \bar x a b + a = a+b-ab\bar x$$

Vettori: 1) Combinazioni convesse

2) Prodotto scalare

3) Prodotto vettore

1)

$$\boxed{\frac{AP}{PB}} = \lambda \qquad \vec P = ?$$

$$\vec P = \frac{\lambda\vec B + \vec A}{\lambda+1}$$

$$\vec P - \vec A = \lambda(\vec B - \vec P)$$

retta AB

$$\boxed{\vec P = \frac{\alpha\vec A + \beta\vec B}{\alpha+\beta} = h\vec A + k\vec B \qquad \boxed{h+k=1}}$$

$$\boxed{\vec P = \alpha\vec A + \beta\vec B, \quad \alpha,\beta\in\mathbb{R}}$$ tutti i punti del piano

$$\vec P - \vec A = \frac{\alpha A + \beta B - \alpha A - \beta A}{\alpha+\beta} = \frac{\beta}{\alpha+\beta}(B-A)$$

$$B - P = \frac{B\alpha + B\beta - \alpha A - \beta B}{\alpha+\beta} = \frac{\alpha}{\alpha+\beta}(B-A)$$

$$\boxed{\frac{AP}{PB} = \frac{\beta}{\alpha}}$$

$$\vec{P} = \frac{\alpha\vec{A} + \beta\vec{B} + \gamma\vec{C}}{\alpha+\beta+\gamma}$$

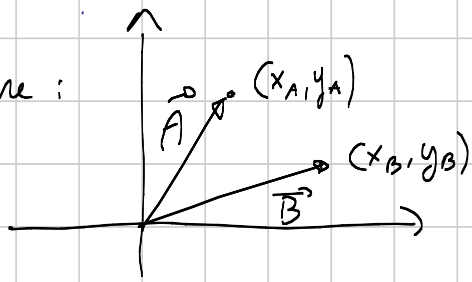
$$\vec{I} = \frac{a\vec{A} + b\vec{B} + c\vec{C}}{a+b+c}$$

$$\vec{I}_A = \frac{-a\vec{A} + b\vec{B} + c\vec{C}}{-a+b+c}$$

$\vdots$

$$\alpha=\beta=\gamma \longrightarrow \vec{G} = \frac{\vec{A}+\vec{B}+\vec{C}}{3}$$

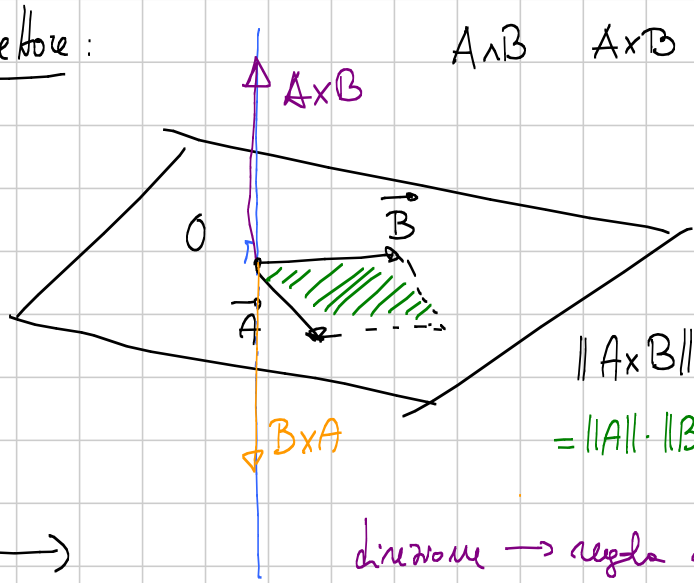
2) Prodotto scalare:

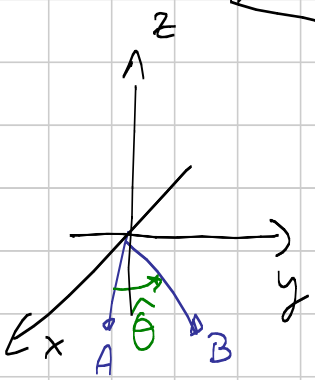


$$\vec{A}\cdot\vec{B} = x_A x_B + y_A y_B \qquad |AB|^2 = (\vec{A}-\vec{B})\cdot(\vec{A}-\vec{B}) =$$
$$= \vec{A}\cdot\vec{A} + \vec{B}\cdot\vec{B} - 2\vec{A}\cdot\vec{B}$$

3) Prodotto vettore:

$A \wedge B \qquad A \times B$





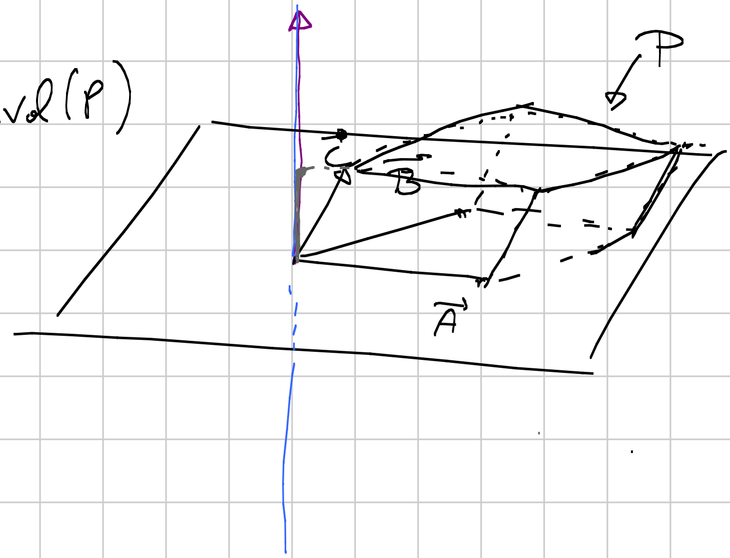
$$\|A\times B\| = \text{area verde} = \|A\|\cdot\|B\|\cdot|\sin \widehat{AB}|$$

direzione $\longrightarrow$ regola della mano dx

θ = angolo orientato da $\vec{A}$ verso $\vec{B}$

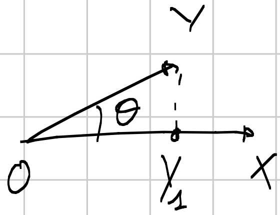
$$A\times B = (0,\, 0,\, \|A\|\cdot\|B\|\cdot\sin\theta)$$

Oss: $(A \times B) \cdot C = \pm \mathrm{vol}(P)$



$X \cdot Y = \|X\| \cdot \|Y\| \cdot \cos \widehat{XY} =$

$= \|X\| \cdot \|$ proiez. di Y su $X \|$



$$X \cdot Y = OY_1 \cdot OX$$

$$(A \times B) \cdot C = \det(A, B, C)$$

1) dimostro che $(A_1 + A_2) \times B =$

$$= A_1 \times B + A_2 \times B$$

1b) dimostro che $(kA) \times B = k(A \times B) \quad k \in \mathbb{R}$

2) $\hat{\imath} = (1,0,0) \qquad \hat{\jmath} = (0,1,0) \qquad \hat{k} = (0,0,1)$

$$\hat{\imath} \times \hat{\jmath} = \hat{k} \qquad \hat{\jmath} \times \hat{k} = \hat{\imath} \qquad \hat{k} \times \hat{\imath} = \hat{\jmath}$$

3) $(x_1 \hat{\imath} + y_1 \hat{\jmath} + z_1 \hat{k}) \times (x_2 \hat{\imath} + y_2 \hat{\jmath} + z_2 \hat{k})$

$$\begin{array}{c} \begin{array}{ccc} + & - & + \end{array} \\ \begin{pmatrix} i & j & k \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{pmatrix} \end{array} \rightsquigarrow (y_1 z_2 - y_2 z_1)\hat{\imath} - (x_1 z_2 - x_2 z_1)\hat{\jmath} +$$

$$+ (x_1 y_2 - x_2 y_1)\hat{k}$$

$$\begin{array}{c} \begin{matrix} + & - & + \end{matrix} \\ \begin{pmatrix} i & j & k \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{pmatrix} \end{array} \qquad \begin{array}{c} \begin{matrix} + & - & + \end{matrix} \\ \begin{pmatrix} i & j & k \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{pmatrix} \end{array}$$

<u>Es</u> $(1,2,3)\times(1,2,1) = (-4,2,0)$

$$\begin{pmatrix} i & j & k \\ 1 & 2 & 3 \\ 1 & 2 & 1 \end{pmatrix} = i(-4) - j(-2) + k(0) =$$
$$= -4i + 2j + 0k$$

$$\Rightarrow \det(A,B,C) = (A\times B)\cdot C =$$

$$= x_C(y_A z_B - y_B z_A) - y_C(x_A z_B - x_B z_A) + z_C(x_A y_B - x_B y_A)$$

$$\det\begin{pmatrix} x_A & x_B & x_C \\ y_A & y_B & y_C \\ z_A & z_B & z_C \end{pmatrix} = x_A y_B z_C + x_B y_C z_A + y_A z_B x_C -$$
$$- x_C y_B z_A - y_C z_B x_A - x_B y_A z_C$$

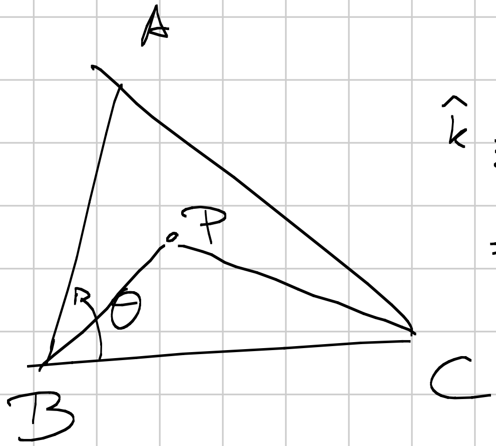
$$A = (a_{ij})_{\substack{i=1\dots n \\ j=1\dots n}} \qquad \det A = \sum_{\sigma\in S_n} (-1)^{|\sigma|} \prod_{i=1}^{n} a_{i\sigma(i)}$$

<u>Es</u>:
$$\det\begin{pmatrix} a & -a & a \\ -b & b & b \\ c & c & -c \end{pmatrix} = -4abc$$

$$\det\begin{pmatrix} a & -b & c \\ a & b & -c \\ 1 & 0 & 0 \end{pmatrix} = 0$$

Ponte: $\vec{P} = \dfrac{\alpha A + \beta B + \gamma C}{\alpha + \beta + \gamma}$

$\frac{1}{2}\|A \times B\| =$ Area $(\overset{\triangle}{AOB})$
compatibile con
aree orientate



$\hat{k}\ \frac{1}{2} BC \cdot BA \sin\theta =$

$= \frac{1}{2}(C-B) \times (A-B)$

$$[PBC] = \frac{1}{2}(C-B) \times (P-B) =$$

$$= \frac{1}{2}(C-B) \times \left(\frac{\alpha A + \beta B + \gamma C}{\alpha+\beta+\gamma} - B \right) =$$

$$= \frac{1}{2}(C-B) \times \left(\frac{\alpha(A-B) + \gamma(C-B)}{\alpha+\beta+\gamma} \right) =$$

$$= [ABC] \cdot \frac{\alpha}{\alpha+\beta+\gamma}$$

$$[PAB] = \frac{\gamma}{\alpha+\beta+\gamma}[ABC] \qquad [APC] = \frac{\beta}{\alpha+\beta+\gamma}[ABC]$$

Coordinate baricentriche di P rispetto ad $\overset{\triangle}{ABC}$

$([PBC], [APC], [ABP])$ o un suo multiplo

notazione alternativa: $[\alpha : \beta : \gamma] \leftarrow$ terna omogenea

Coord. esatte: $\left(\dfrac{[PBC]}{[ABC]}, \dfrac{[APC]}{[ABC]}, \dfrac{[ABP]}{[ABC]} \right)$

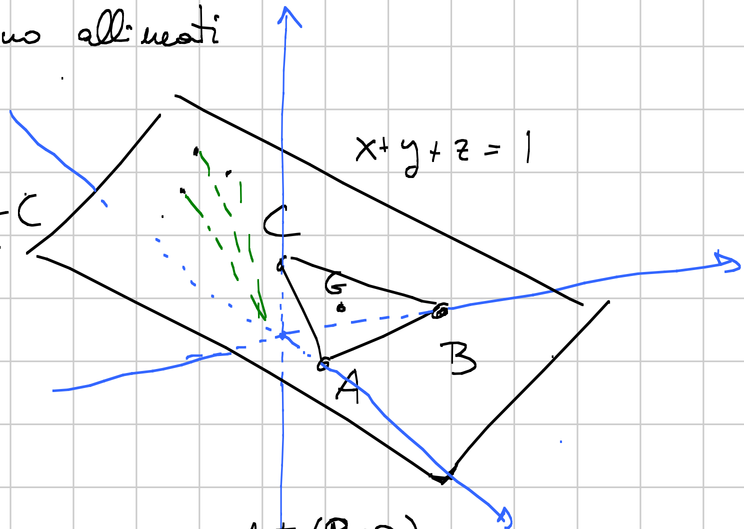
Es: G baricentro di $ABC \Rightarrow G = (1, 1, 1)$

Es: I incentro di $ABC \Rightarrow I = (a, b, c)$

I_A A-excentro $\longrightarrow I_A = (-a, b, c)$

Es: I_C, A, I_B sono allineati

$$P = \frac{\alpha}{\alpha+\beta+\gamma} A + \frac{\beta}{\alpha+\beta+\gamma} B + \frac{\gamma}{\alpha+\beta+\gamma} C$$



P, Q, R allineati

$\Updownarrow$

$\mathrm{Vol}(OPQR) = 0 \iff \det(PQR) = 0$

$$\Rightarrow I_C, A, I_B \text{ allineati} \iff \det\begin{pmatrix} a & b & -c \\ a & -b & c \\ 1 & 0 & 0 \end{pmatrix} = 0$$ che è vero!

Eq. di una retta

Es: mediana $A = (1, 0, 0)$, $G = (1, 1, 1)$

$$\left\{ (x, y, z) \text{ omogenee t.c. } \det\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ x & y & z \end{pmatrix} = 0 \right\}$$

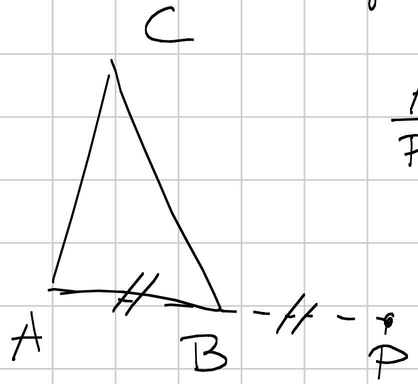
$$z - y = 0 \iff z = y$$

$\Rightarrow$ pt. medio di BC $\begin{cases} z = y \\ x = 0 \end{cases} \longrightarrow (0, \lambda, \lambda)$, $\lambda \in \mathbb{R}$

$\to (0,1,1)$

$$\frac{AP}{PB} = \frac{\lambda}{\mu} \Rightarrow$$
$$\Rightarrow P = \frac{\mu A + \lambda B}{\lambda + \mu}$$

<u>Es</u>: Simmetrico di A rispetto a B

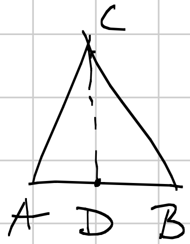


$$\frac{AP}{PB} = -2$$

$$\vec{P} = \frac{-2\vec{B} + \vec{A}}{-1} = 2\vec{B} - \vec{A}$$

$A = (1,0,0)$
$B = (0,1,0)$
somma $= 1$ $\Rightarrow P = 2(0,1,0) - (1,0,0) =$
$= (-1,2,0)$

<u>Es</u>: <u>Piede della bisettrice</u>



$$\frac{AD}{DB} = \frac{b}{a} \qquad \vec{D} = \frac{a\vec{A} + b\vec{B}}{a+b}$$

$$\vec{D} = \left(\frac{a}{a+b}, \frac{b}{a+b}, 0 \right)$$
$$= (a, b, 0)$$

perché posso molt. per $(a+b)$ per omogeneità.

<u>Notazione di Conway</u>

$$S = 2[ABC], \quad S_\theta = S \cdot \cot\theta \quad S_{\theta\varphi} = S_\theta \cdot S_\varphi$$

$$S_A = S \cdot \cot A = 2[ABC]\frac{\cos A}{\sin A} = bc \cdot \cos A =$$

$$= \cancel{bc}\,\frac{b^2+c^2-a^2}{2\cancel{bc}} = \frac{b^2+c^2-a^2}{2} \qquad S_B = \frac{a^2+c^2-b^2}{2}$$

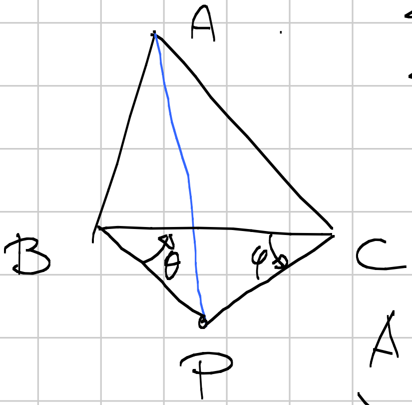
$$S_C = \frac{a^2+b^2-c^2}{2}$$

Oss: $S_B + S_C = a^2$

$A+B+C=\pi$

$$S_{AB}+S_{BC}+S_{CA} = S^2 \qquad (\cot A\cot B+\cot B\cot C+\cot C\cot A = 1)$$

Formula di Conway

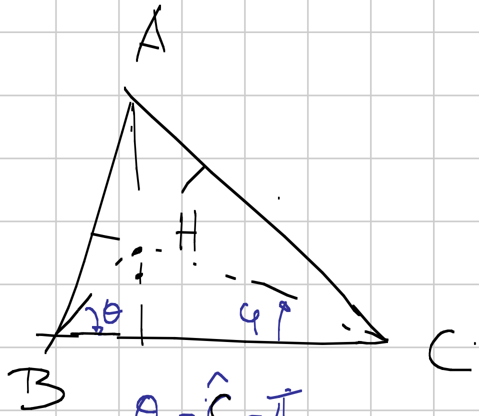


$\sphericalangle PBC = \theta$

$\sphericalangle BCP = \varphi$

$$\Rightarrow P : (-a^2, S_C + S_\varphi, S_B + S_\theta)$$

Es: Ortocentro



$\theta = \hat{C} - \frac{\pi}{2}$ $\qquad \cot\theta = -\operatorname{tg}\hat{C}$

$\varphi = \hat{B} - \frac{\pi}{2}$ $\qquad \cot\varphi = -\operatorname{tg}\hat{B}$

$$H : (-a^2; S_C + S_\varphi; S_B + S_\theta) = \qquad S_\theta = S\cdot\cot\theta =$$

$$= -S\operatorname{tg}\hat{C} =$$

$$= \left(-a^2; S_C - \frac{S^2}{S_B}; S_B - \frac{S^2}{S_C}\right) = \qquad = -\frac{S^2}{S_C}$$

$$= \left(-a^2 S_B S_C : S_C\,(S_C S_B - S^2) : S_B\,(S_B S_C - S^2)\right) =$$

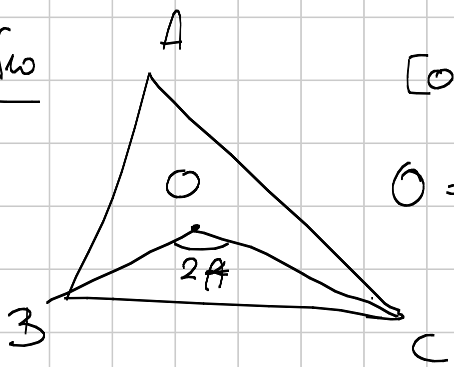
$$= \left(-(S_B + S_C) S_B S_C : S_C\,(-S_{AC} - S_{AB}) : S_B\,(-S_{AC} - S_{AB})\right) =$$

$$= \left((S_B + S_C) S_{BC} : S_{AC}\,(S_C + S_B) : S_{AB}\,(S_C + S_B)\right) =$$

$$= \left(S_{BC} : S_{AC} : S_{AB}\right) = \left(\cot B \cot C : \cot A \cot C : \cot A \cot B\right) =$$

$$= \left(\frac{1}{\cot A} : \frac{1}{\cot B} : \frac{1}{\cot C}\right) = \left(\operatorname{tg} A : \operatorname{tg} B : \operatorname{tg} C\right)$$

Es: O circocentro



$$[OBC] = \frac{1}{2} R^2 \sin 2A$$

$$O = (\sin 2A : \sin 2B : \sin 2C)$$

Es: Centro della circonf. di Feuerbach?

$$O = (a^2 S_A : \text{cyc} : \text{cyc})$$

$$H = (S_B S_C : S_A S_C : S_B S_A)$$

$$O = (S_A S_B + S_A S_C : \text{cyc} : \text{cyc})$$

$$H \to \Sigma = S^2$$

$$O \to \Sigma = 2S^2$$

$$\cot A = \frac{\cos A}{\sin A}$$

$$\cot A \cdot \sin^2 A = \frac{1}{2} \sin 2A$$

$$S_A \cdot \sin^2 A = \frac{S}{2} \sin 2A$$

$$S_A \frac{a^2}{4R^2} = \frac{S}{2} \sin 2A$$

$$S_A a^2 = \boxed{2R^2 S} \sin 2A$$

$$\frac{1}{2}\left(\left(S_{BC}:S_{AC}:S_{AB}\right)+\left(\frac{S_{AB}+S_{AC}}{2}:\frac{S_{BA}+S_{BC}}{2}:\frac{S_{CA}+S_{CB}}{2}\right)\right)=$$

$$=\left(\frac{S_{AB}+S_{AC}+2S_{BC}}{\cancel{2}\,4}:cyc:cyc\right)=$$

$$=\left(S^2+S_{BC}:cyc:cyc\right)$$

$$S^2(1+\cot B\cot C)=$$

$$=S^2\frac{(\sin B\sin C+\cos B\cos C)}{\sin B\sin C}=$$

$$=\frac{S^2}{\sin B\sin C}(\cos(B-C))$$

$$=ac\,ab\,(\cos(B-C))=$$

$$=\boxed{abc}\cdot a\cos(B-C)$$

simmm (basta cyc)

$$=(a\cos(B-C):cyc:cyc)$$

Es: Punto medio di AH.

$$H=(S_{BC}:S_{AC}:S_{AB})$$

$$\Sigma=S^2$$

$$A:(S^2:0:0)$$

pt. medio di $AH=$

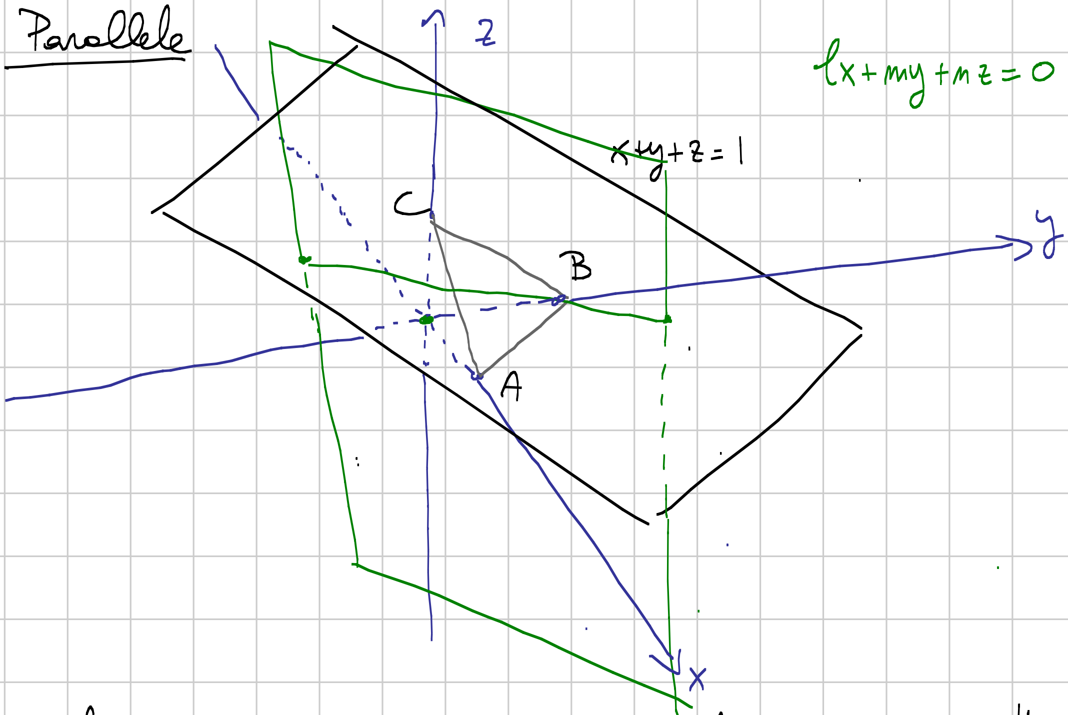
$$=\cancel{\tfrac{1}{2}}\left(S^2+S_{BC}:S_{AC}:S_{AB}\right)=$$

$$=\left(\cancel{abc}\,a\cos(B-C):\underbrace{\boxed{\frac{S^2}{\sin A\sin C}}}_{\cancel{abc}\cdot b}\cos A\cos C:\underbrace{\boxed{\frac{S^2}{\sin A\sin B}}}_{\cancel{abc}\cdot c}\cos A\cos B\right)=$$

$$= \left(a\cos(B-C) : b\cos A\cos C : c\cos A\cos B \right)$$

Rette parallele e perpendicolari

1) Parallele



Oss: il piano $x+y+z=0$ non corrisponde a nessuna retta sul nuovo piano.

$$\underbrace{(A\cap B)}_{\text{retta sul nuovo piano}} \cap \underbrace{(C\cap B)}_{\text{retta sul nuovo piano}} = \underbrace{(A\cap C)}_{\text{retta per l'origine}} \cap \underbrace{B}_{\text{nuovo piano.}}$$

$\emptyset$ $\emptyset$

$= \emptyset \iff A\cap C \subseteq x+y+z=0$

Due rette sono parallele $\iff$ la soluzione del sistema rispetta $\boxed{x+y+z=0}$

$$\begin{cases} lx + my + nz = 0 \\ l'x + m'y + n'z = 0 \end{cases}$$

Es: AH $\qquad A: (1:0:0) \qquad H = (\operatorname{tg} A : \operatorname{tg} B : \operatorname{tg} C)$

$$0 = \det \begin{pmatrix} 1 & 0 & 0 \\ \operatorname{tg} A & \operatorname{tg} B & \operatorname{tg} C \\ x & y & z \end{pmatrix} \iff \operatorname{tg} B \cdot z = \operatorname{tg} C \cdot y$$

$O\Pi_A \qquad \Pi_A: (0:1:1) \qquad O: (\sin 2A : \sin 2B : \sin 2C)$

$$0 = \det \begin{pmatrix} 0 & 1 & 1 \\ \sin 2A & \sin 2B & \sin 2C \\ x & y & z \end{pmatrix} = \sin 2C \cdot x + \sin 2A \cdot y - \sin 2B \cdot x - \sin 2A \cdot z =$$

$$= x(\sin 2C - \sin 2B) + y \sin 2A - z \sin 2A$$

$$\begin{cases} \operatorname{tg} B \cdot z = \operatorname{tg} C \cdot y \\ x(\sin 2C - \sin 2B) = \sin 2A (z - y) \end{cases} \qquad z = \frac{\operatorname{tg} C}{\operatorname{tg} B} y$$

$$x = \frac{\sin 2A}{\sin 2C - \sin 2B} \left(\frac{\operatorname{tg} C - \operatorname{tg} B}{\operatorname{tg} B} \right) y$$

$$\left(\frac{\sin 2A}{\sin 2C - \sin 2B} \cdot (\operatorname{tg} C - \operatorname{tg} B) : \operatorname{tg} B : \operatorname{tg} C \right)$$

$$\boxed{\text{Due rette sono parallele} \iff \text{intersezione} \in x + y + z = 0}$$

Digressione: come si intersecano due piani in $\mathbb{R}^3$ per l'origine.

$\alpha x+\beta y+\gamma z=0$ $\qquad$ $\ell x+my+nz=0$

$\downarrow$ $\qquad$ $\downarrow$ piano $\perp$ (ℓ,m,n)

$(x,y,z)\cdot(\alpha,\beta,\gamma)=0$

$\downarrow$ $\qquad$ $\rightarrow$ la loro intersezione è la retta generata da $(\alpha,\beta,\gamma)\times(\ell,m,n)$

piano $\perp$ a (α,β,γ)

$\Rightarrow$ il punto di intersez. delle rette corrisp. in coord. baricentriche è $(\alpha,\beta,\gamma)\times(\ell,m,n)$

voglio sapere se questo punto appartiene alla retta $px+qy+rz=0$

$\downarrow$ retta t.c. $(p,q,r)\cdot(x,y,z)=0$

$\Rightarrow$ voglio sapere se $\big((\alpha,\beta,\gamma)\times(\ell,m,n)\big)\cdot(p,q,r)=0$

$$\Updownarrow$$

$$\det\begin{pmatrix}\alpha & \ell & p\\ \beta & m & q\\ \gamma & n & r\end{pmatrix}=0 \iff \begin{cases}\alpha x+\beta y+\gamma z=0\\ \ell x+my+nz=0\\ px+qy+rz=0\end{cases} \text{concorrono}$$

Corollario: due rette sono //

$$\Updownarrow$$

$$\det\begin{pmatrix}\ell & \ell' & 1\\ m & m' & 1\\ n & n' & 1\end{pmatrix}=0$$

Rette per lo parallele

Es: parallela a BC per I

1) scrivo BC $x=0$

2) trovo il "punto all'infinito" $\begin{cases} x=0 \\ x+y+z=0 \end{cases} \to P_\infty = (0:1:-1)$

3) trovo la retta per I e P_∞

$$0=\det\begin{pmatrix} a & b & c \\ 0 & 1 & -1 \\ x & y & z \end{pmatrix} = az - bx - cx + ay =$$

$$= -(b+c)x + a(y+z)$$

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

2) Perpendicolari: 2a) casi speciali

perpendicolari ai lati = parallele alle altezze

2b) formula generale [lasciatela perdere]

Extra: Circonferenze | Coniugati isogonali

$\updownarrow$ distanze e angoli

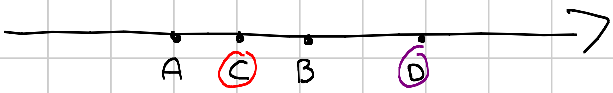
$$(x:y:z) \to \left(\frac{a^2}{x} : \frac{b^2}{y} : \frac{c^2}{z}\right)$$

Note Title 9/5/2017

G2 Medium - Geometria Proiettiva

- Lunghezze con segno

Fissiamo una retta orientata



da sx a dx i segmenti sono di lungh. positiva altrimenti negativa

AB +

BA −

Ad esempio $\frac{AC}{CB}$ + $\frac{AD}{DB}$ −

D • Birapporto. Dati 4 punti allineati A, B, C, D

$$(A, B; C, D) := \frac{AC}{CB} \cdot \frac{BD}{DA}$$

Ex. 24 permutazioni di $(A, B; C, D)$. Quanti birapporti diversi? 6!

D • (A, B, C, D) sono q. armonica sse $(A, B; C, D) = -1$

Oss. $\boxed{(A, B; C, D) = (A, B; C, D') \Rightarrow D \equiv D'}$

Perché? $\frac{\cancel{AC}}{\cancel{CB}} \cdot \frac{BD}{DA} = \frac{\cancel{AC}}{\cancel{CB}} \cdot \frac{BD'}{D'A}$

$$\frac{BD}{DA} = \frac{BD'}{D'A} \Rightarrow D \equiv D'$$

I

P P
? ?

B

I

D D'

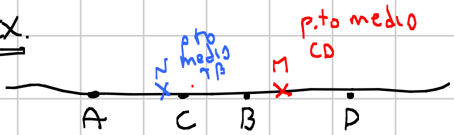
A

I $\frac{BD}{DA} = \frac{BD'}{D'A} \rightarrow \frac{BD}{\cancel{BA}} = \frac{BD'}{\cancel{BA}}$

D' D

II $\frac{BD}{DA} = \frac{BD'}{D'A} \Rightarrow \frac{BD}{DB+BA} = \frac{BD'}{D'B+BA}$

Ex.



TFAE:

① $(A, B; C, D) = -1$

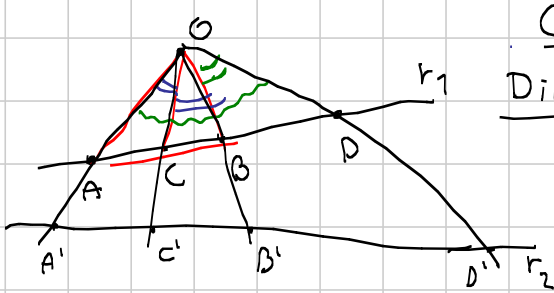
② $\frac{2}{AB} = \frac{1}{AC} + \frac{1}{AD}$

③ $MA \cdot MB = MC^2$

④ $CA \cdot CB = CD \cdot CN$

⑤ $AB^2 + CD^2 = 4MN^2$

• Il birapporto si conserva per proiezione da un p.to esterno



Claim: $(A,B;C,D) = (A',B';C',D')$

Dim. $\dfrac{AC}{CB} \cdot \dfrac{BD}{DA}$ $(*)$

th seni $O\hat{A}C$: $\dfrac{AC}{\sin A\hat{O}C} = \dfrac{AO}{\sin O\hat{C}A}$

" $O\hat{B}C$: $\dfrac{CB}{\sin C\hat{O}B} = \dfrac{OB}{\sin O\hat{C}B}$

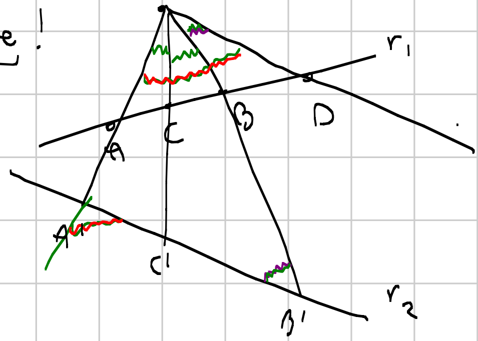
Dunque $\dfrac{AC}{CB} = \dfrac{AO}{OB} \cdot \dfrac{\sin A\hat{O}C}{\sin C\hat{O}B}$

Analogamente $\dfrac{BD}{DA} = \dfrac{OB}{AO} \cdot \dfrac{\sin B\hat{O}D}{\sin D\hat{O}A}$

Dunque $(*) = \dfrac{\sin A\hat{O}C}{\sin C\hat{O}B} \cdot \dfrac{\sin B\hat{O}D}{\sin D\hat{O}A}$ $(**)$

Ripetendo su r_2 ottengo il claim perché $(**)$ dipende solo dagli angoli formati da OAA', OBB', OCC', ODD'.

Caso limite!



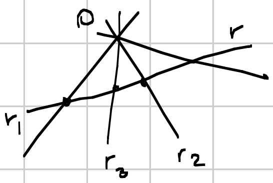
• Su ogni retta mettiamo un p.to all'∞ [tutte le rette parallele "passano" per questo punto]

• $\boxed{D}$ $D \equiv \infty$ $[A,B;C,D] = \dfrac{AC}{CB} \cdot \cancel{\dfrac{BD}{DA}}$ Importante

$C = \infty$ $[A,B;C,D] = \cancel{\dfrac{AC}{CB}} \cdot \dfrac{BD}{DA}$

Ex. Tutto torna con l'invarianza

Def. Birapporto fra rette

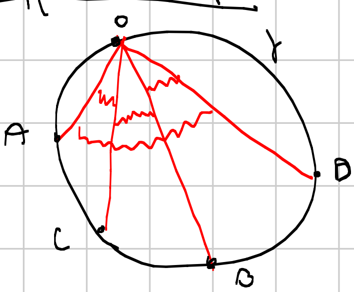


$(r_1, r_2; r_3, r_4)_r \overset{def}{:=} (r_1 \cap r, r_2 \cap r, r_3 \cap r, r_4 \cap r)$

Oss. è una buona def.

Oss. $(r_1, r_2; r_3, r_4)_r = \dfrac{\sin r_1\hat{O}r_3}{\sin r_3\hat{O}r_2} \cdot \dfrac{\sin r_2\hat{O}r_4}{\sin r_4\hat{O}r_1}$

Def. Birapporto su cfr



Prendo A,B,C,D su γ cfr.

Prendo $O \in \gamma$

$(A,B;C,D)_\gamma := (OA, OB; OC, OD)_r$

Oss. È una buona def! Perché il bir. fra rette dipende solo dagli angoli che queste formano e viceversa e in questo tali angoli rimangono uguali

<u>Oss.</u> $O \in \{A, B, C, D\}$. E.g. $O = A$, AA è la retta tangente

<u>Oss.</u> $$(A, B; C, D)_\gamma = \frac{\sin A\hat{O}C}{\sin C\hat{O}B} \cdot \frac{\sin B\hat{O}D}{\sin D\hat{O}A} = \frac{\frac{AC}{\cancel{2R}}}{\frac{CB}{\cancel{2R}}} \cdot \frac{\frac{BD}{\cancel{2R}}}{\frac{DA}{\cancel{2R}}} = \frac{AC}{CB} \cdot \frac{BD}{DA}$$

<u>Ex.</u> I birapporti si conservano per inversione

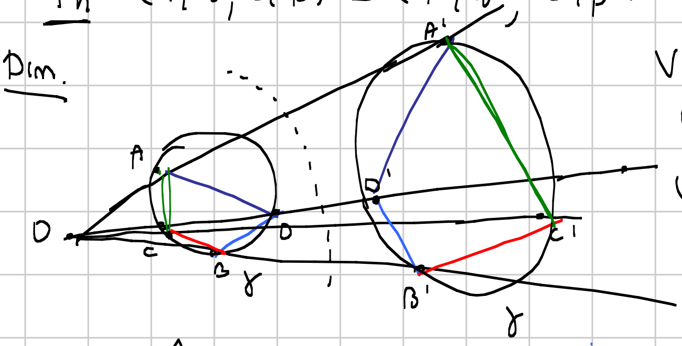
A, B, C, D allineati (o conciclici)

A', B', C', D' immagini tramite un'inversione di centro O $\notin \{A, B, C, D\}$

(e quindi anche loro sono allineati o conciclici)

<u>Th</u> $(A, B; C, D) = (A', B'; C', D')$, $\boxed{\text{Per cosa gli altri casi}}$

<u>Dim.</u>



Vogliamo

$(A, B; C, D)_\gamma = (A', B'; C', D')_{\gamma'}$

Uso la relazione di prima

$LHS = \frac{AC}{CB} \cdot \frac{BD}{DA}$

$RHS = \frac{A'C'}{C'B'} \cdot \frac{B'D'}{D'A'}$

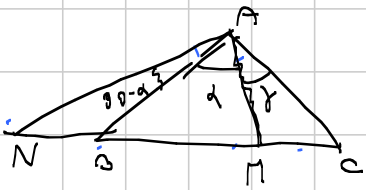
$O\hat{A}C \sim O\hat{C'}A'$

$$\frac{AC}{A'C'} = \frac{OC}{OA'} \qquad \frac{CB}{C'B'} = \frac{OB}{OC'}$$

$$\frac{BD}{B'D'} = \frac{OB}{OD'} \qquad \frac{DA}{D'A'} = \frac{OA}{OD'}$$

$$\Rightarrow \frac{LHS}{RHS} = \frac{OC}{OA'} \cdot \frac{\cancel{OB}}{\cancel{OD'}} \cdot \frac{OC'}{\cancel{OB}} \cdot \frac{\cancel{OD'}}{OA} = \frac{R^2}{R^2} = 1$$

<u>Ex.</u> \ <u>Lemma</u> Delle seguenti, due qualsiasi implicano la terza:



1) AM bisettrice

2) $(B, C; M, N) = -1$

3) $M\hat{A}N = 90°$

<u>1) & 2)</u>

$1) \Rightarrow \frac{BM}{MC} = \frac{AB}{AC}$ (Th. della bis.)

$2) \Rightarrow \frac{BM}{MC} \cdot \frac{CN}{NB} = -1 \overset{(1)}{\Rightarrow} \left|\frac{CN}{NB}\right| = \frac{AC}{AB}$ Th. bisettrice esterna inverso

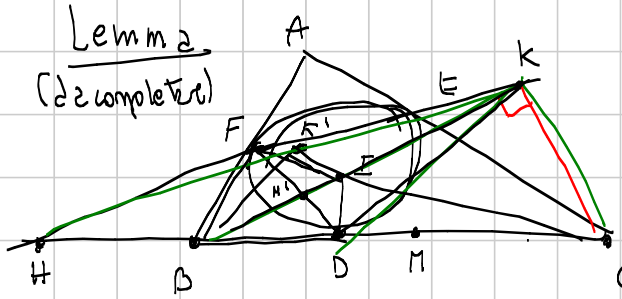
AN bisettrice esterna $\overset{(1)}{\Rightarrow}$ $M\hat{A}N = 90$.

<u>1) & 3)</u> ok.

<u>2) & 3)</u> $(B, C; M, N) = -1$ $\Rightarrow$ usando l'uguaglianza dei triangoli in nullo gli angoli e prendendo i moduli $\frac{\sin\alpha}{\sin\gamma} \cdot \frac{\sin(90+\gamma)}{\sin(90-\alpha)} = 1$

$\Rightarrow \operatorname{tg}\alpha = \operatorname{tg}\gamma \Rightarrow \alpha = \gamma.$

Lemma
(da completare)



$BI \cap EF =: K$

Th $CK \perp KB$

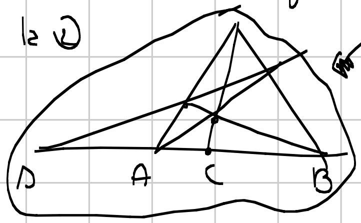
Dim. Dobbiamo verificare che

① KB biseca $H\hat{K}D$

② $(H, D; B, C) = -1$

Per la ① cosa devo fare? BI è l'asse di FD. Allora $FK = KD$, però $BI \cap FD = M'$ punto medio di DF.
Dunque KB biseca $H\hat{K}D$ perché è altezza/mediana/bisettrice in un triangolo isoscele.

Per la ②

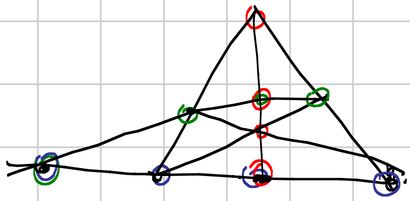


In questo caso $(A, B; C, D) = -1$

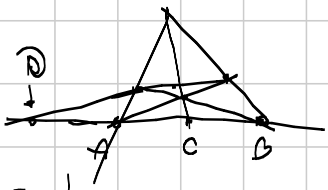
In virtù di questo

$(B, C; D, H) = -1 \longrightarrow \frac{BD}{DC} \cdot \frac{CH}{HB} = -1$

$\xrightarrow{\text{l'inv.}} \frac{HB}{BD} \cdot \frac{DC}{CH} = -1 \Rightarrow (H, D; B, C) = -1$



Come costruire il IV armonico?



Desargues / Pappo - Pascal

De. $A_1 A_2 A_3$, $B_1 B_2 B_3$ triangoli

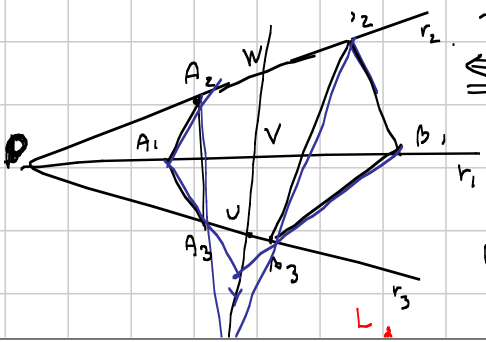
$A_1 A_2 \cap B_1 B_2 =: Z$

$A_1 A_3 \cap B_1 B_3 =: Y$

$A_2 A_3 \cap B_2 B_3 =: X$

X, Y, Z allineati $\Leftrightarrow$ $A_1 B_1$, $A_2 B_2$, $A_3 B_3$ concorrono

Dim. $\Leftarrow$), $\Rightarrow$) per assurdo.

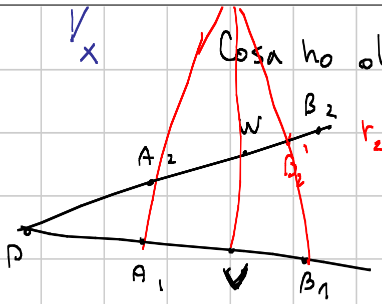


$\Leftarrow$) $X := A_2 A_3 \cap B_2 B_3$

$Y := A_1 A_3 \cap B_1 B_3$

Voglio che XY, $A_1 A_2$, $B_1 B_2$ concorrono

$(P, V; A_1, B_1) \underset{\text{da } Y \text{ su } r_3}{=} (P, U; A_3, B_3) \underset{\text{da } X \text{ su } r_2}{=} (P, W; A_2, B_2)$



Cosa ho ottenuto

$(P,V;A_1,B_1)=(P,W;A_2,B_2)$

$\Downarrow$

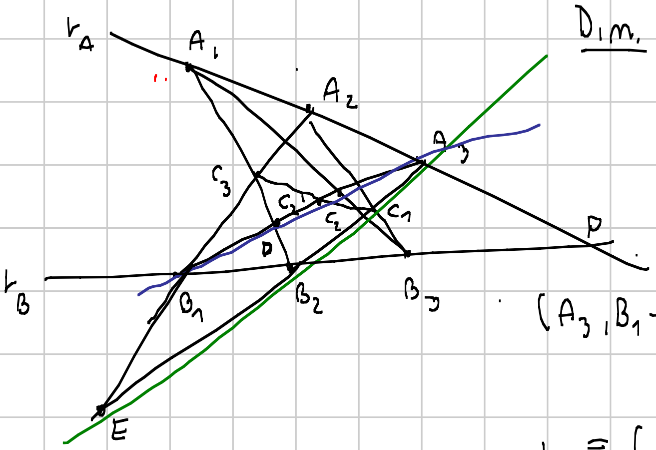
A_1A_2, VW, B_1B_2 concorrono

Per assurdo non fosse vero

Sia $L := A_1A_2 \cap VW$. $B_2' := LB_1 \cap r_2$.

Allora $PWA_2B_2' \underset{\text{per proiezione da } L}{=} PVA_1B_1 \underset{h_p}{=} PWA_2B_2 \Longrightarrow B_2 \equiv B_2'$ ↯

Thm (Pappo)



Th C_1, C_2, C_3 allineati

Dim. P.a. non lo sono $C_2' := C_1C_3 \cap B_1A_3$

Voglio che $C_2 \equiv C_2'$

$D := A_1B_2 \cap B_1A_3$

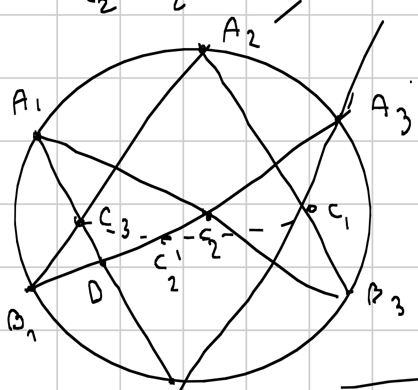
$E := A_2B_1 \cap B_2A_3$

$(A_3,B_1;D,C_2) \underset{\text{da } A_1 \text{ su } r_B}{=} (P,B_1;B_2,B_3) \underset{\text{da } A_2 \text{ su } -}{=} (A_3,E;B_2,C_1)$

$\underset{\text{da } C_3 \text{ su } -}{=} (A_3,B_1;D,C_2')$ $\cdot E$

$\Rightarrow C_2 \equiv C_2'$

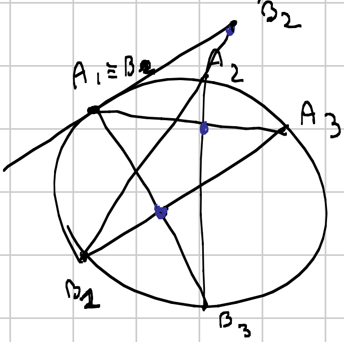
Thm (Pascal)



C_1, C_2, C_3 allineati

Dim. Copiamo esattamente quella di sopra

Oss. Pascal funziona anche se due punti dovessero coincidere



POLI/POLARI

Polare rispetto ad una circonferenza γ. [o due rette r_1, r_2]

Def. Traccio le rette che passano per P e intersecano γ in A, B.
La polare (di P risp. a γ) è il luogo dei punti X t.c. $(A, B; P, X) = -1$.

Fig. 1

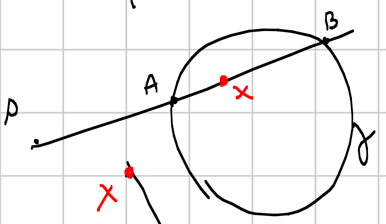
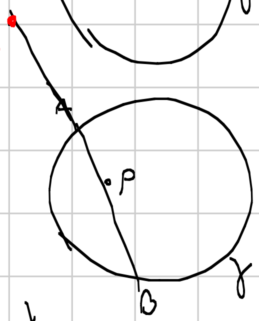


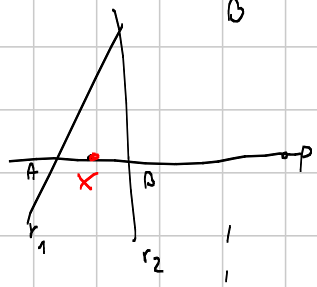
Fig. 2



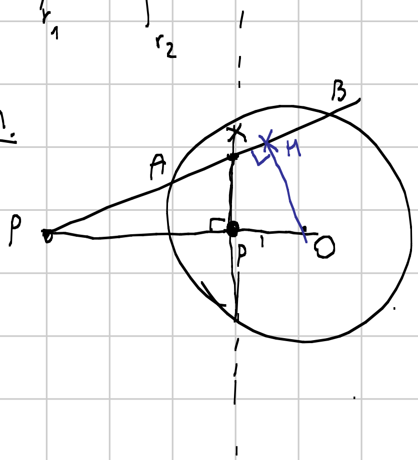
Domanda: Che luogo è? (nel caso della circonferenza)

Risposta: La retta perpendicolare a OP passante per P', dove P' è l'immagine di P mediante un'inversione circolare in γ.

Fig. 3



Dim.



Voglio mostrare che $(A, B; P, X) = -1$

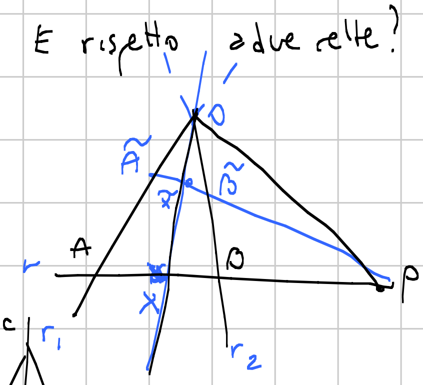
Questo è vero sse $MX \cdot MP = MA^2$ [Ex. in note

$$MX \cdot MP \underset{\text{Pitag.}}{=} MP^2 - PX \cdot MP \underset{\substack{MXP'O\\ \text{ciclico}}}{=} MP^2 - PP' \cdot PO =$$

$$= MP^2 - (OP^2 - \underbrace{OP' \cdot OP}_{P,P' \text{ inversi } = OA^2}) = MP^2 - OP^2 + OA^2$$

$$= -OM^2 + OA^2 = AM^2.$$

E rispetto a due rette?



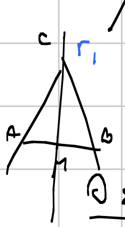
Prendo una retta r a caso e sia X t.c. $(A, B; P, X) = -1$

Claim. la polare è OX

sia $\tilde{r}$ un'altra retta e $\tilde{X} := \tilde{r} \cap OX$

Per proiezione $(\tilde{A}\,\tilde{B}\,P\,\tilde{X}) = (A\,B\,P\,X) = -1$

e quindi $\tilde{X} \in$ luogo

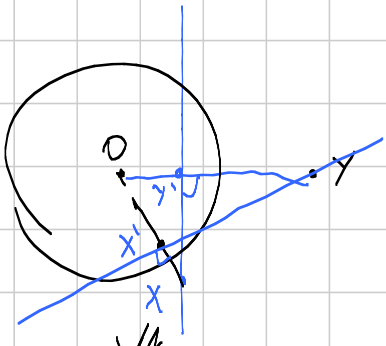


Oss. $(OA, OB; OP, OX)_r = -1$ ←

Dualità: $X \in \text{pol}\, Y \Rightarrow Y \in \text{pol}\, X$

Conseguenza: X, Y, Z allineati sse $\text{pol}\, X, \text{pol}\, Y, \text{pol}\, Z$ concorrono.

Dim.

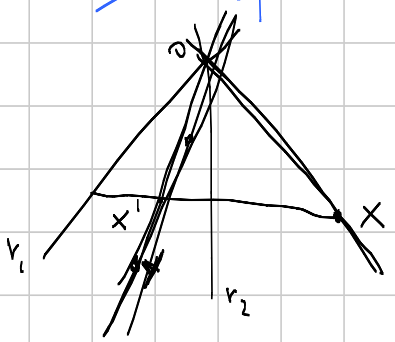


Mi basta mostrare che $X'Y \perp OX$

$OX' \cdot OX = r^2 = OY' \cdot OY$

inv.

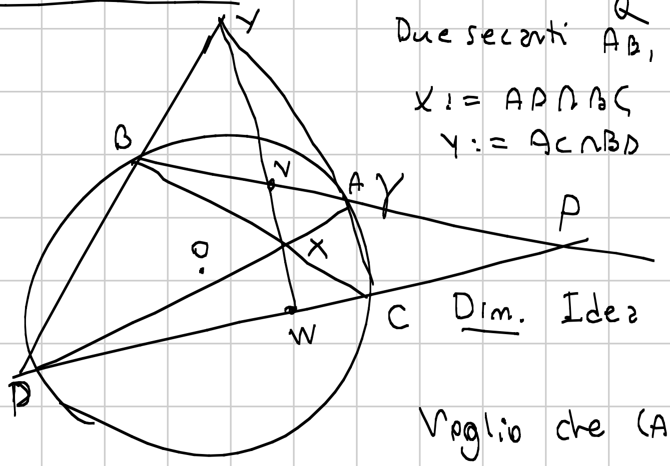
Dunque $X'XYY'$ ciclico $\Rightarrow X\hat{X'}Y = X\hat{Y'}Y = 90°$



$(r_1, r_2; OX, \text{pol}\, X)_r = -1$

$(r_1, r_2; \text{pol}\, X, OX) = -1$

LEMMA DELLA POLARE



P esterno a γ

Due secanti AB, CD

$X := AD \cap BC$

$Y := AC \cap BD$

Th. $XY = \text{pol}\, P$

Dim. Idea $XY \cap AB =: V$

$XY \cap CD =: W$

Voglio che $(A, B; P, V) = (C, D; P, W) = -1$

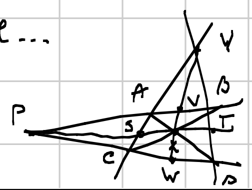
$(A, B; P, V) \underset{\text{da } X \text{ su } CD}{=} (D, C; P, W) \underset{\text{da } Y \text{ su } AB}{=} (B, A; P, V)$

Abbiamo ottenuto $(A, B; P, V) = (B, A; P, V) \Rightarrow$

$$\Rightarrow \underbrace{\frac{AP}{PB} \cdot \frac{BV}{VA}}_{x} = \underbrace{\frac{BP}{PA} \cdot \frac{AV}{VB}}_{\frac{1}{x}} \Rightarrow \left(\frac{AP}{PB} \cdot \frac{BV}{VA}\right)^2 = 1$$

$$\Rightarrow \frac{AP}{PB} \cdot \frac{BV}{VA} = -1$$

Giusto per riscrivere...

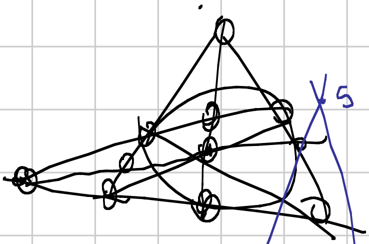


$XY = \text{pol}\, P$

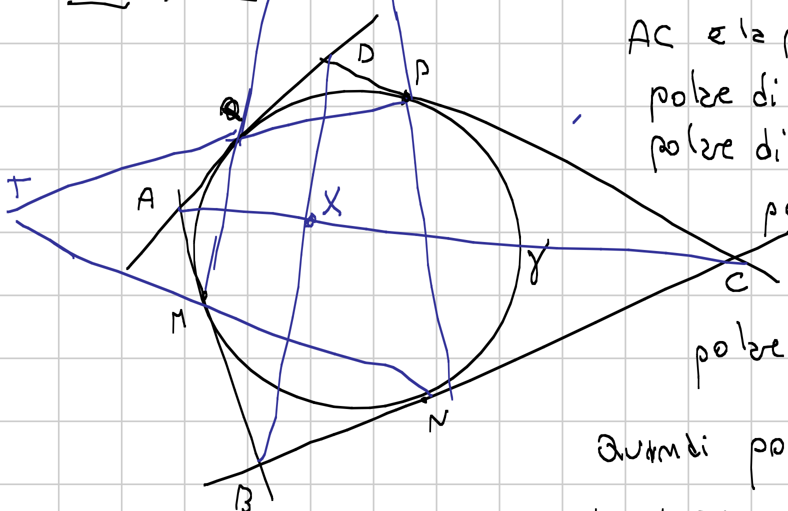
Quindi $(A, B; P, V) = (C, D; P, W) = -1$

$(A, C; Y, S) = (B, D; Y, T) = -1$

$(S,T,P,X) = (V,W,Y,X) = -1$



Ex.\Lemma (Newton)



MP, NQ, AC, BD concorrono

AC è la polare di

polare di A → MQ

polare di C → NP

polo di AC → $MQ \cap NP = S$

polo di BD → $QP \cap MN = T$

polare $(\underbrace{AC \cap BD}_{= X})$ → ST

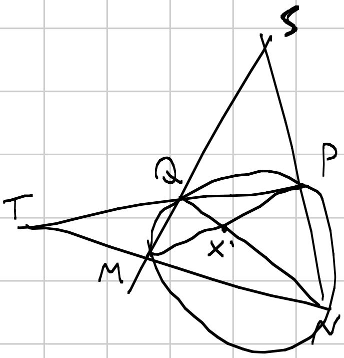
Quindi polo ST = X

polare di T → SX'

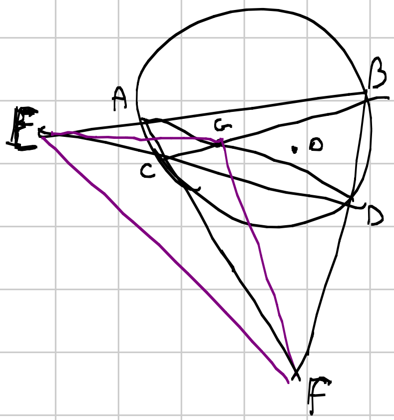
polare di S → TX' (lemma della polare)

→ polo ST = X'

Dunque $\underbrace{X}_{= AC\cap BD} = \underbrace{X'}_{= MP\cap NQ}$ → MP, NQ, AC, BD concorrono! ∎



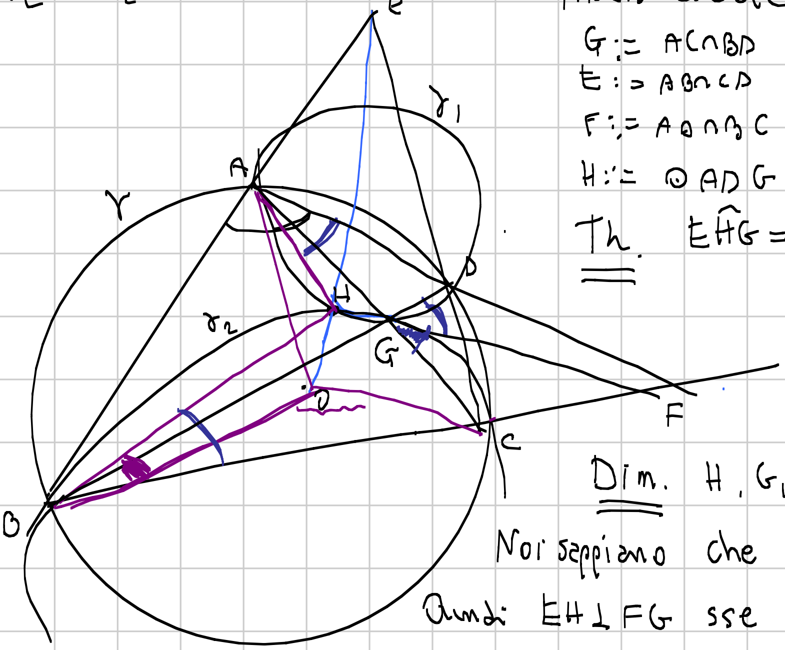
Lemma O è l'ortocentro di EFG



Dim. FG ⊥ OE
perché per il lemma della polare FG è la polare di E
Analogamente
EG ⊥ OF
⇓
O è l'ortocentro

EFG = self polar triangle

Ex. \ Lemma



ABCD ciclico

$G := AC \cap BD$

$E := AB \cap CD$

$F := AD \cap BC$

$H := \odot ADG \cap \odot BGC$

Th. $E\hat{H}G = 90°$

Dim. H, G, F allineati (assi radicali)

Noi sappiamo che $EO \perp FG$ [Lemma polare]

Quindi $EH \perp FG$ sse E, H, O allineati

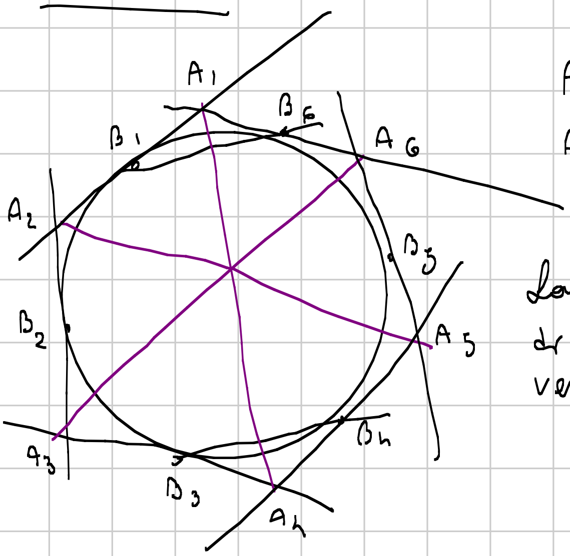
Claim. ABHO, HOCD ciclici. Poi la tesi segue per assi radicali (*)

$H\hat{B}O = H\hat{B}C - O\hat{B}C = F\hat{G}C - (90 - \widehat{BC})$

$H\hat{A}O = H\hat{A}D - O\hat{A}D = \widehat{BC} + \widehat{CD} - D\hat{H}F - (90 - \widehat{AB})$

$H\hat{B}O = H\hat{A}O$ sse $F\hat{G}C + D\hat{H}F = \widehat{CD} + \widehat{AB}$ Th. angolo esterno in BGC

Th (Brianchon)



Th A_1A_4, A_3A_6, A_2A_5 concorrono

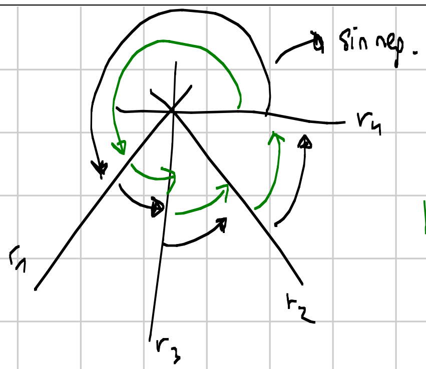
$A_1A_4 = \text{pol}(B_1B_6 \cap B_3B_4)$

$A_3A_6 = \text{pol}(B_5B_6 \cap B_2B_3)$

$A_2A_5 = \text{pol}(B_1B_2 \cap B_4B_5)$

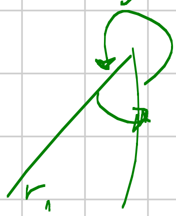
La tesi (per dualità) equivale a dire che i 3 poli sono allineati vero per Pascal

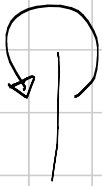
123456



$$\frac{r_1\hat{O}r_3}{r_3\hat{O}r_2} \cdot \frac{r_2\hat{O}r_4}{r_4\hat{O}r_1}$$

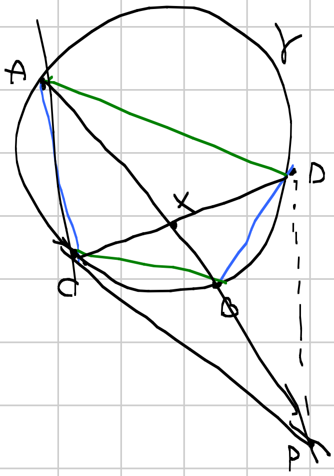
$$r_1\hat{O}r_3 + r_3\hat{O}r_1 = 360°$$





Quad. armonici

Def. $ABCD$ armonico sse $(A, B; C, D)_\gamma = -1$



Oss. Def. sse $AC \cdot BD = CB \cdot AD$

Oss. Tan C, Tan D, AB concorrono
[Analogamente Tan A, Tan B, CD concorrono]

Dim. Sia $P := CC \cap AB$

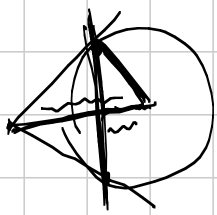
Sia $X := CD \cap AB$

$$\underset{\overset{\|\,\text{def.}}{-1}}{(A, B; C, D)_\gamma} \overset{\text{def}}{=} (CA, CB; CC, CD)_r \overset{\text{proiettando su AB}}{=} (A, B; P, X)$$

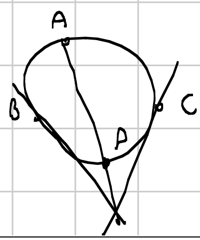
Dunque $(A, B; P, X) = -1 \to X \in$ pol P

Però $C \in$ pol P perché PC tange γ

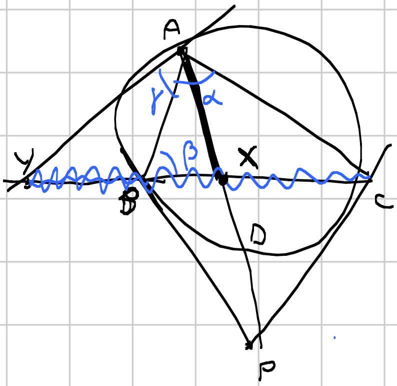
Allora CX è la polare di P, poiché $CX \cap \gamma = D$, allora PD tange γ. [Lemma simm.] **Oss.** AX è simmediana di $A\hat{C}D$ relativa a CD.



Oss. Come completare il quadrilatero armonico?



Lemma Simmediana



Th. AD simmediana

Dim. So che ABDC è armonico

$(A, D; B, C)_\gamma = -1$

$\Downarrow$

$(AA, AD; AB, AC)_r = -1$

$\Downarrow$ proiettando su BC

$(Y, X; B, C) = -1$

$\Downarrow$

$\frac{YB}{BX} \cdot \frac{XC}{CY} = -1$

In modulo $\frac{BY}{YC} = \frac{BX}{XC}$

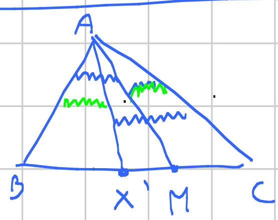
$\frac{BY}{\sin\gamma} = \frac{AY}{\sin\beta}$

$\frac{YC}{\sin(\gamma+\alpha)} = \frac{AY}{\sin\gamma}$

$\sin(\gamma+\alpha) = \sin\beta$

$\Longrightarrow \frac{BY}{YC} = \left(\frac{\sin\gamma}{\sin\beta}\right)^2$

Dunque $\frac{BX}{XC} = \left(\frac{\sin\gamma}{\sin\beta}\right)^2$



$\frac{BX'}{\sin m} = \frac{AB}{\sin A\hat{X'}B}$

$\frac{X'C}{\sin m} = \frac{AC}{\sin A\hat{X'}C}$

$\Rightarrow \frac{BX'}{X'C} = \frac{\sin\gamma}{\sin\beta} \cdot \frac{\sin m}{\sin m}$

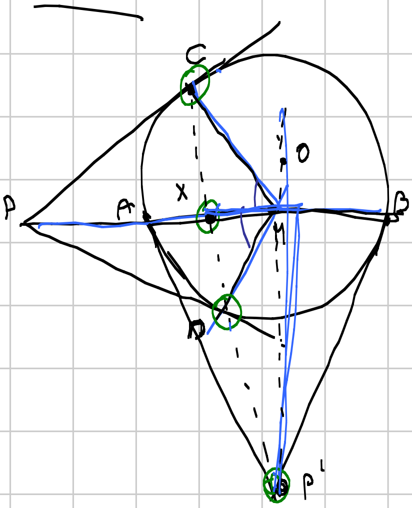
Però $\frac{BM}{\sin m} = \frac{AB}{\sin A\hat{M}B}$

$\frac{MC}{\sin m} = \frac{AC}{\sin A\hat{M}C}$

$\rightarrow \frac{\sin m}{\sin m} = \frac{AB}{AC} = \frac{\sin\gamma}{\sin\beta}$

Dunque $\frac{BX'}{X'C} = \left(\frac{\sin\gamma}{\sin\beta}\right)^2$.

Lemma



- M punto medio di AB
- ABCD armonico

Th. MP biseca $C\hat{M}D$

Dim. O, M, P' (:= tg A ∩ tg B) allineati

E anche C, D, P' (quad. armonico)

Quanto vale $(C, D; P', X)$? $= -1$!

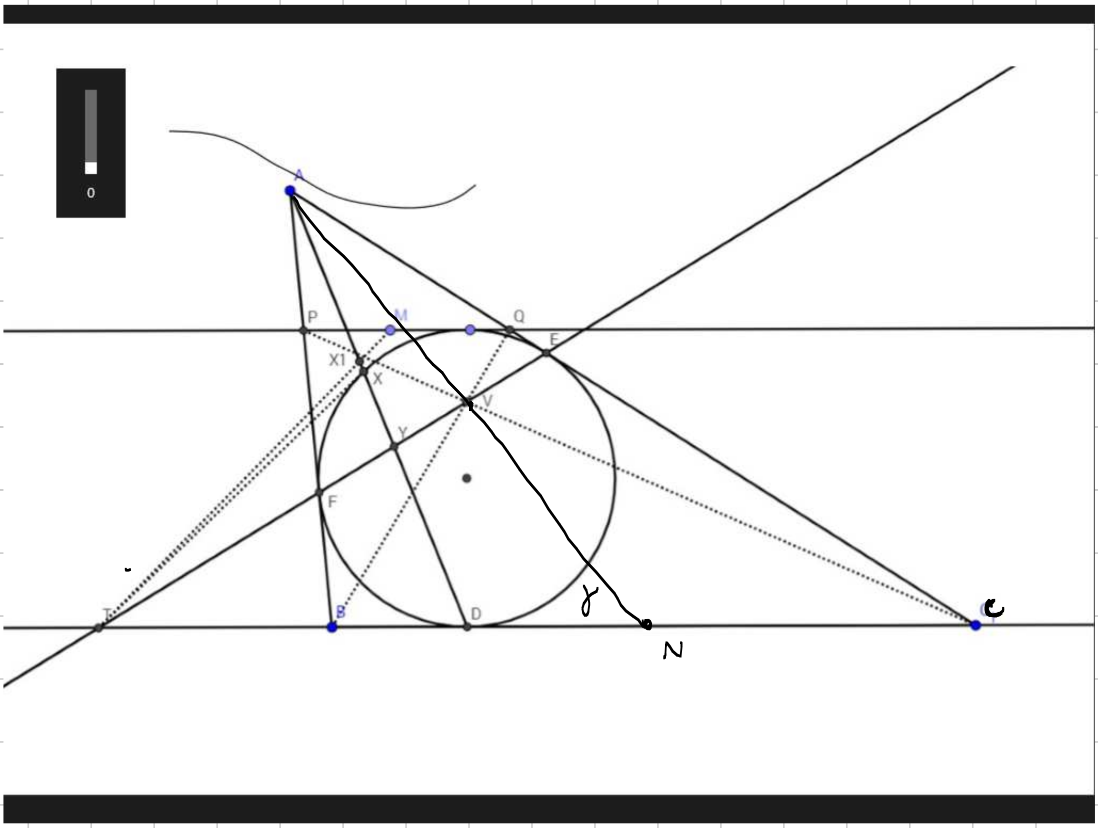
Quindi per il lemma interno MX biseca $C\hat{M}D$.

[redacted]

IRAN TST

- ABC triangolo, DEF triangolo di contatto (int. dell'incerchio con i lati)
- PQ tangente a γ, incerchio, parallelo a BC
- M punto medio di PQ e $T := EF \cap BC$

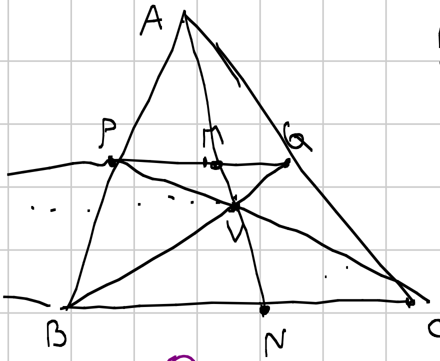
Th. TM tange γ.



Oss. 1 $AD \cap \gamma =: X$
Cosa posso dire di TX?
La polare di A wrt a γ è EF $\overset{\text{dualità}}{\Rightarrow}$ $A \in \text{pol}\, T$
Però anche $D \in \text{pol}\, T$ $\Rightarrow$ $AD = \text{pol}\, T$ e quindi si avere $X = AD \cap \gamma$, TX tange γ. E di più $(X, D; A, Y) = -1$

Oss. 2 il trucco è questo: definisco $X_1 := TM \cap AD$ e voglio mostrare $(X_1, D; A, Y) = -1$

Oss. 3 $V := PC \cap QB \Rightarrow V \in EF$ (Newton)



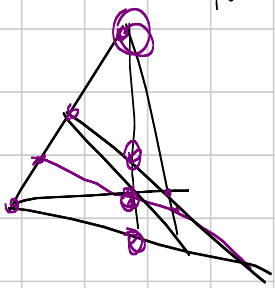
Oss. 4 AV è la polare di ∞_{BC} wrt. (AB, AC)

Dunque $AV \cap PQ$, $AV \cap BC$ sono i punti medi di PQ e BC rispettivamente

$(M, N; A, V) = -1$

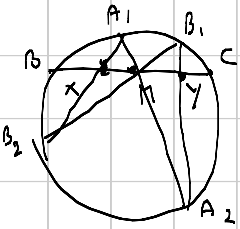
Fine: Proiettando da T su AD ottengo $(X_1; D; A, Y) = -1$

Dunque $X_1 \equiv X$ e ho concluso.



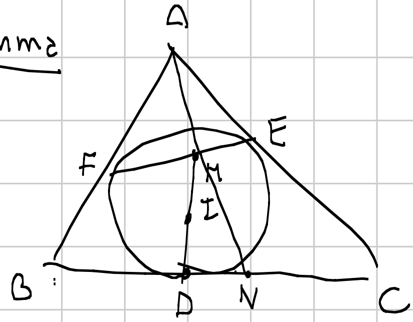
Gare: IMO 2014-4 / IMO SL 2007-G8

Es. Th della farfalla



Th. $MX = MY$

Lemma



ABC triangolo, DEF contatto

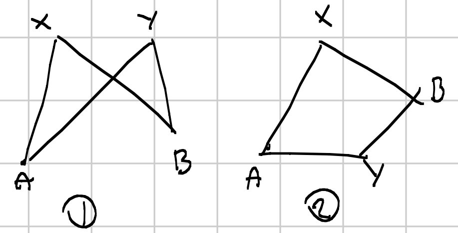
$M := ID \cap EF$, N p.to medio di BC

Th A, M, N allineati

G3 Medium – Sintetica (Miquel, Mistilinee, Inv.)

Note Title 9/6/2017

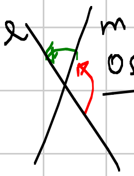
Angoli orientati [Evan Chen]



ABXY è ciclico sse
① $A\hat{X}B = A\hat{Y}B$
② $A\hat{X}B + A\hat{Y}B = \pi$

Def. m, ℓ rette

$\measuredangle(m, \ell)$ = angolo (antiorario) di cui ruotare m per sovrapporsi con ℓ



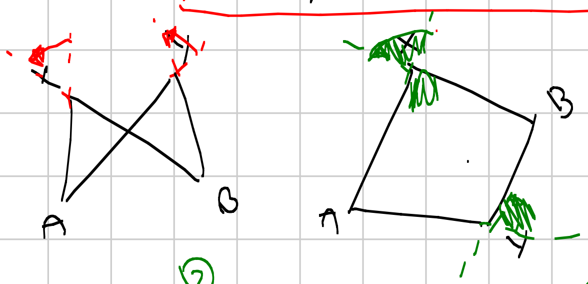
Oss. $\measuredangle(\ell, m)$, $\measuredangle(m,\ell) + \measuredangle(\ell, m) = \pi$

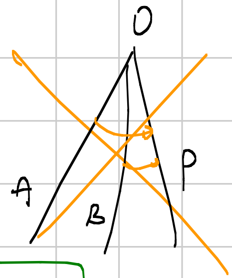
Consideriamo tutto mod π, $\measuredangle(m,\ell) = -\measuredangle(\ell, m)$

Def. $\measuredangle AOB \overset{def}{=} \measuredangle(AO, OB)$

Ex. (Verifica) Vale il seguente

THM $\boxed{A, B, X, Y \text{ ciclico sse } \measuredangle AXB = \measuredangle AYB}$ ①



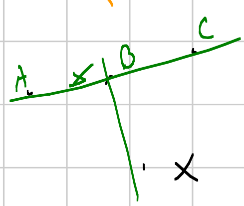


②

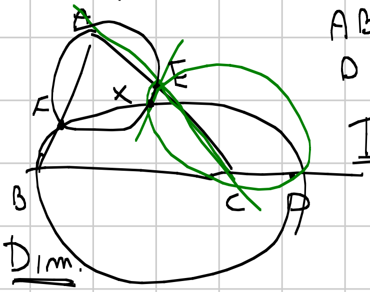
Proprietà • $\boxed{\measuredangle AOP + \measuredangle POB = \measuredangle AOB}$

• $\measuredangle ABC + \measuredangle BCA + \measuredangle CAB = \text{⊗}$

③ → • $\boxed{A, B, C \text{ allineati sse } \measuredangle XBC = \measuredangle XBA}$ [dato X un punto]



Th di Miquel su un triangolo



ABC triangolo

D, E, F su (le rette di) BC, CA, AB

Th $\odot AEF$, $\odot BDF$, $\odot CDE$ concorrono

Dim.

$X := \odot AEF \cap \odot BFD$. Th $\iff$ X, E, C, D ciclico

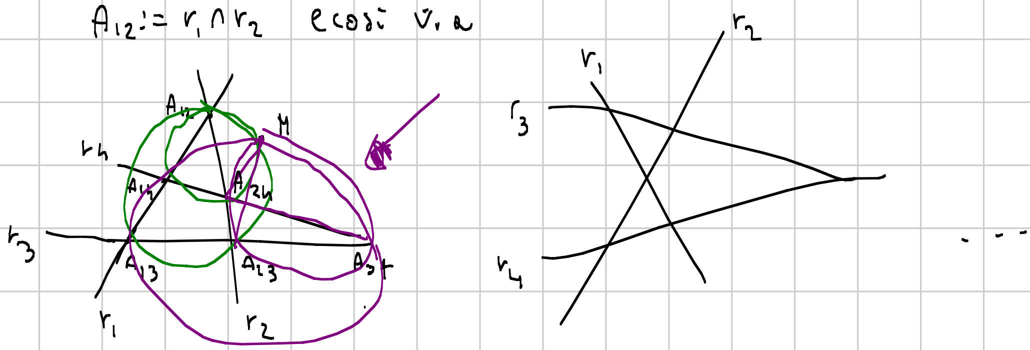
X, E, C, D ciclico sse $\measuredangle XEC = \measuredangle XDC$.

Però $\measuredangle XEC \underset{③}{=} \measuredangle XEA \underset{①}{=} \measuredangle XFA \underset{③}{=} \measuredangle XFB \underset{①}{=} \measuredangle XDB \underset{③}{=} \measuredangle XDC$

Th di Miquel (quadrangolo)

Siano r_1, r_2, r_3, r_4 4 rette "in posizione generica"

$A_{12} := r_1 \cap r_2$ e così via



Th. $\odot A_{12}A_{23}A_{31}$, $\odot A_{12}A_{24}A_{41}$, $\odot A_{23}A_{34}A_{24}$, $\odot A_{13}A_{34}A_{41}$ concorrono in M p.to di Miquel del quadrangolo

Dim. Sia $M := \odot A_{12}A_{24}A_{41} \cap \odot A_{12}A_{23}A_{13}$

① $M \in \odot A_{23}A_{34}A_{24}$

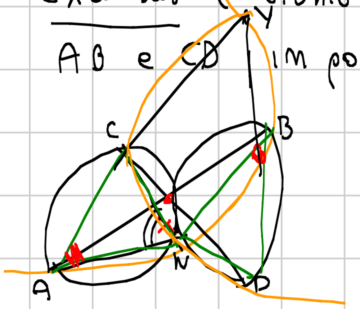
$\measuredangle MA_{24}A_{34} \underset{③}{=} \measuredangle MA_{24}A_{14} \underset{①}{=} \measuredangle MA_{12}A_{14} \underset{③}{=} \measuredangle MA_{12}A_{13} \underset{①}{=} \measuredangle MA_{23}A_{13} \underset{③}{=} \measuredangle MA_{23}A_{34}$

e quindi si conclude per lo ①.

② Analogamente $M \in \odot A_{13}A_{34}A_{41}$

Excursus (Rotomotetie)

AB e CD in posizione generica



Q1 Quante rotomotetie esistono che mandano ordinatamente $A \to C$, $B \to D$?

R1 1! Perché? Se esistesse siano z_0, ~~...~~ ragione centro e ragione della rotomotetia dell'omotetia e θ l'angolo

$$p \longrightarrow z_0 + \underbrace{\rho e^{i\theta}}_{\alpha}(p - z_0) =: p'$$

$$c = z_0 + \alpha(a - z_0) \longrightarrow z_0 = \dots$$
$$d = z_0 + \alpha(b - z_0) \qquad \alpha = \dots$$

Costruiamola. Sia $X := AB \cap CD$ [se sono paralleli... aggiusti]

Sia $W := \odot ACX \cap \odot BDX$

Con angoli orientati... $\measuredangle WAB = \measuredangle WAX = \measuredangle WCX = \measuredangle WCD$ (1)

$\measuredangle WBA = \measuredangle WBX = \measuredangle WDX = \measuredangle WDC$ (2)

(1) + (2) $\Rightarrow$ $W\hat{A}B \approx W\hat{C}D$

[$\measuredangle WAB = \measuredangle WCD$, $\measuredangle WBA = \measuredangle WDC$ $\Rightarrow$ $W\hat{A}B \approx W\hat{B}C$ $\not\Leftarrow$?]

Oss. W è ANCHE il centro della rotomotetia che manda AC in BD

$\measuredangle AWC = \measuredangle AXC = \measuredangle BXD = \measuredangle BWD$

$\measuredangle WAC = \measuredangle WXC = \measuredangle WXD = \measuredangle WBD$

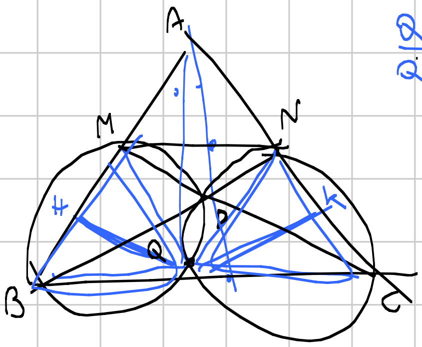
(4)

$W\hat{A}C \simeq W\hat{B}D$

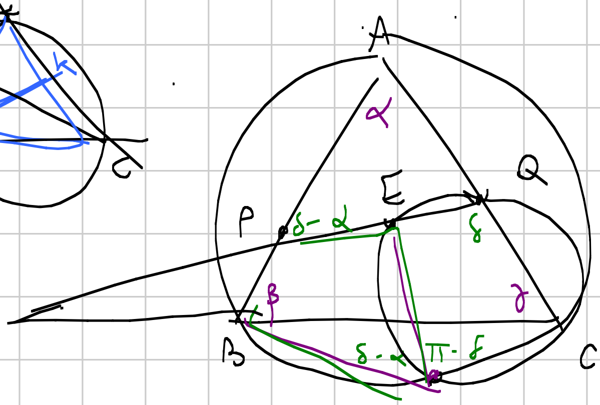
Ma allora dove altro sta ~~W~~??

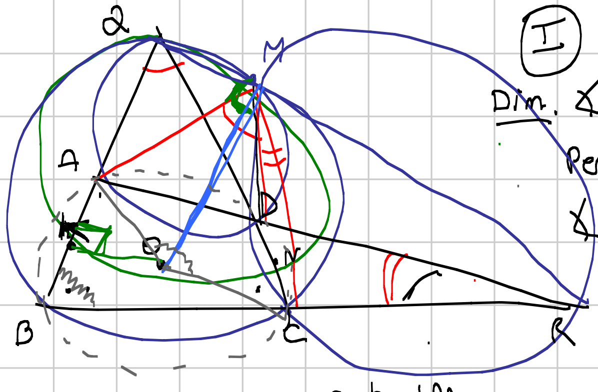
Quindi se $Y := AC \cap BD$ AYWB e CYWD ciclici

Appl. (G3)



$$\frac{QH}{QK} = \frac{MB}{NC} = \frac{AB}{AC}$$





(I) $M \in QR$ sse $ABCD$ ciclico

Dim. $\measuredangle DMQ = \measuredangle DAQ = \measuredangle DAB$ (*)

Però

$\measuredangle DMR = \measuredangle DCR = \measuredangle DCB$ (**)

$\measuredangle DMQ = \measuredangle DMR \overset{(*),(**)}{\Longleftrightarrow} \measuredangle DAB = \measuredangle DCB$

$(3)\Updownarrow$ $\qquad\qquad\qquad \Updownarrow \mathcal{D}$

Q, M, R allineati $\qquad ABCD$ ciclico

(II) $ABCD$ ciclico $\Rightarrow OM \perp QR$

Dim. M è il centro della rotomotetia che porta AB in DC ma pure porta anche AK in DN, K medio di AB e N medio di DC. Dunque per quanto detto su sulle rotomotetie $M \in \odot QKN$, inoltre $O \in \odot QKN$ $(\angle QKO + \angle QNO = \pi/2 + \pi/2 = \pi)$. Dunque $QKONM$ ciclico e quindi $\angle QMO = \angle QKO = \pi/2$

(III) $MAOC$ e $BODM$ ciclici ($ABCD$ è ciclico)

Dim. $\angle AMC = \angle AMD + \angle DMC = \angle AQD + \angle DRC = 180 - \hat{B} - \hat{Q} + 180 - \hat{A} - \hat{B}$

$= 180 - 2\hat{B} = 180 - \angle AOC \Rightarrow \angle AMC + \angle AOC = 180$ ∎

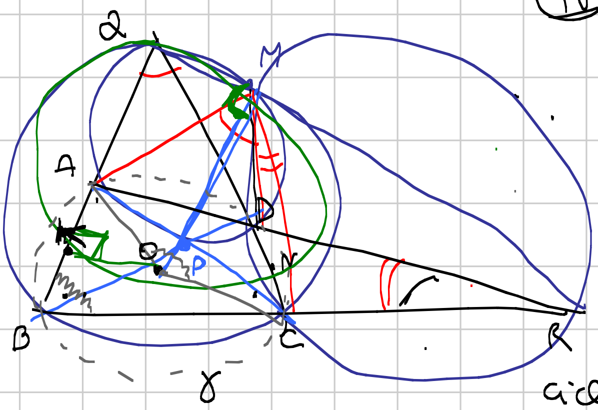
(IV) MO biseca $A\hat{M}C$

MO biseca $B\hat{M}D$

Dim. (III) $A\hat{M}O = A\hat{C}O$

$O\hat{M}C = O\hat{A}C$

Però $O\hat{A}C$ è isoscele e quindi $A\hat{M}O = O\hat{M}C$.



Analogamente usando $BODM$ ciclico ho ≈

(V) Consideriamo la terna di quad. ciclici: $ABCD$, $AOCM$, $BODM$. I tre assi radicali sono AC, BD, OM. Quindi $P := AC \cap BD$, O, P, M allineati.

(VI) Se inverto nella cfr circoscritta ad ABCD,

BD → ⊙ BOD

AC → ⊙ AOC

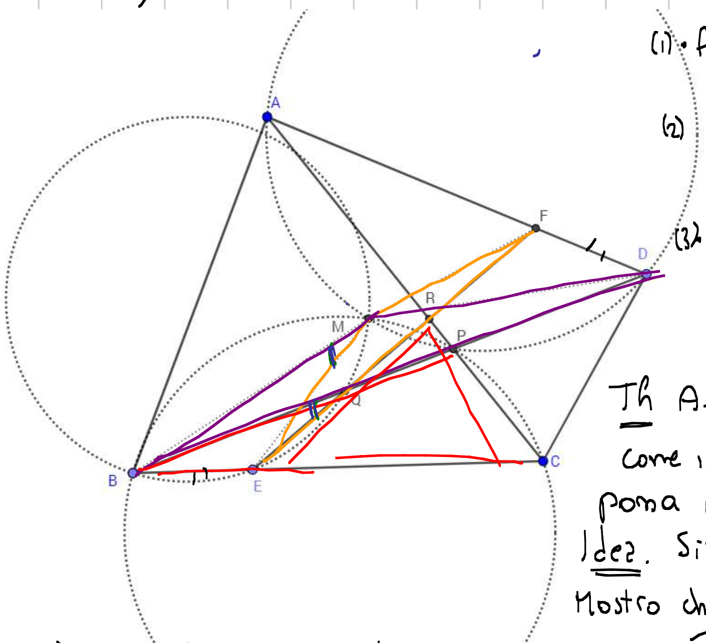
P = BD ∩ AC → ⊙ BOD ∩ ⊙ AOC = M per il punto III.

Dunque P ed M sono uno l'inverso dell'altro rispetto all'inversione nella cfr circoscritta ad ABCD.

(VII) Aggiungete l'esercizio "EHF = 90°" di ieri.

H sarà l'inverso di Q wrt a Γ

IMO 5 (2005)



(1) · ABCD convesso con BC = AD

(2) · E ∈ BC, F ∈ AD t.c. BE = DF

(3) Q = BD ∩ EF

P = AC ∩ BD

R = EF ∩ AC

Th Al variare di E, F come in (2), ⊙ PQR passa per uno stesso punto

Idea. Sia M := ⊙ BPC ∩ ⊙ APD. Mostro che M ∈ ⊙ PQR.

Oss.1 M è il centro della roto-omotetia che porta AC in DB, ma è anche quella che porta AD in CB ⟶ ∠MAD = ∠MCB (*)
∠MDA = ∠MBC (**)

Oss.2 ⊙ APD, ⊙ BPC sono congruenti (*) ⟹ MD = MB (***)
(**) ⟶ MA = MC

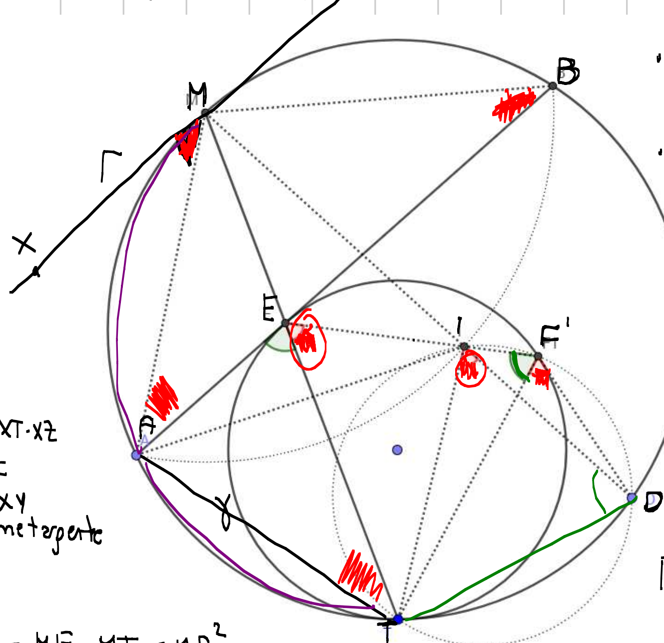
Oss.3 (***) + (**) ⟹ $M\hat{B}E \cong M\hat{D}F$, e fra l'altro $ME = MF$, $\angle BME = \angle FMD$
+ hp (BE = DF)

Quindi MBD e MEF sono triangoli isosceli rotomotetici (✓).

Ma allora BEQM ciclico.

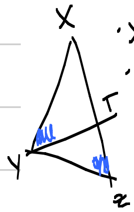
Fine M = ⊙ BEQ ∩ ⊙ BCP ⟹ M è il punto di Miquel del quadrilatero BECQPR e quindi M ∈ ⊙ PQR

Un'avventura misti...linea



- Γ e γ tangenti internamente in T
- AB, corda di Γ, tange γ in E

(I) $M := TE \cap \Gamma$.
M è il p.to medio dell'arco $\overset{\frown}{AB}$.
Dim. Omotetia di centro T che porta γ in Γ.
$E \to M$
$AB \to$ tangente in M a Γ ed è $/\!/ AB$.
Dunque $X\hat{M}A = M\hat{A}B$ ($/\!/$)
$X\hat{M}A = M\hat{B}A$ (su Γ ins. su MA)



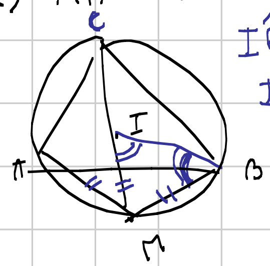
- $XY^2 = XT \cdot XZ$
- $OYTZ$ ha XY come tangente

(II) $MA^2 = ME \cdot MT = MB^2$

- Sia $D \in \overset{\frown}{ATB}$. Sia I l'incentro di $A\hat{D}B$. Sia $F' := EI \cap \gamma$.

Voglio mostrare che $\boxed{ITDF' \text{ ciclico}}$.

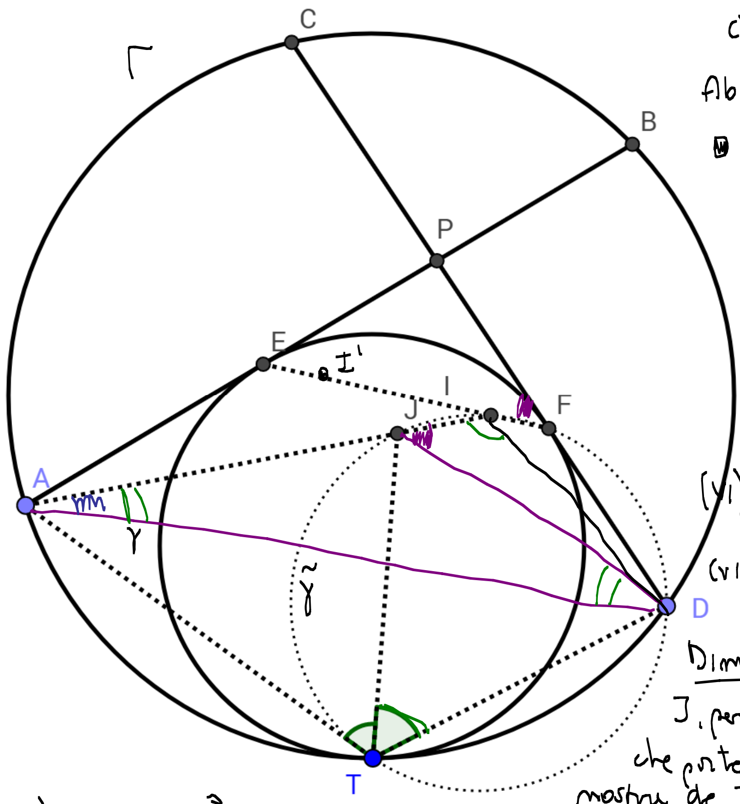
(III) $MA = MI = MB$. (I)+(III) $\Rightarrow MI^2 = ME \cdot MT$ ← (III bis)



$I\hat{B}M = I\hat{B}A + A\hat{B}M = \frac{\beta}{2} + \frac{\delta}{2}$
$I\hat{M}B = \alpha$
Quindi $I\hat{M}B = \pi - \alpha - \frac{\beta}{2} - \frac{\delta}{2} = \frac{\beta}{2} + \frac{\delta}{2}$

(IV) $T\hat{F'}E = T\hat{E}A = M\hat{A}E + E\hat{M}A = M\hat{B}E + E\hat{M}A = M\hat{D}T$
E questo conclude la ciclicità.

(V) Mostro DF' tange γ. Mi basterebbe mostrare $D\hat{F'}T = F'\hat{E}T$. Però per (II) $ITDF'$ ciclico $\Rightarrow D\hat{F'}T = D\hat{I}T$. Dunque mi rimarrebbe da mostrare $D\hat{I}T = E\hat{I}T$. Questo è vero per (III bis)



- Γ e γ tg. internamente in T
- AB, CD corde di Γ che toccano γ in E, F

Abbiamo mostrato

- I incentro di ABD sta su EF (I' incentro di ACD sta su EF)
- $IFTD$ ciclico [$\tilde{\gamma}$] ($I'ETA$ ciclico)

Vogliamo mostrare

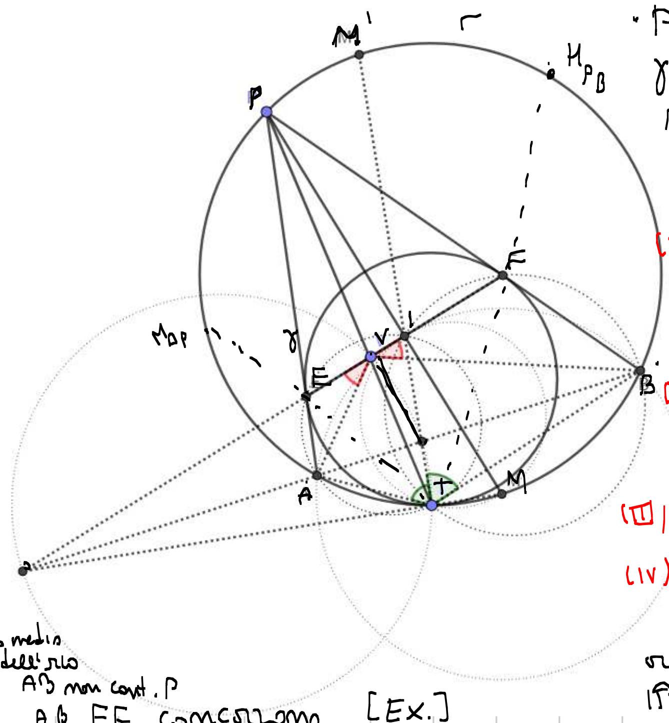
- (vi) J incentro di PAD sta su $\tilde{\gamma}$
- (vii) TJ biseca $A\hat{T}D$

Dim. (vi) Prendo $J := AI \cap \tilde{\gamma}$. J, per def, sta sulla bisettrice che parte da $\hat{A}$ in $P\hat{A}D$. Voglio mostrare che J sta anche sulla bisettrice che parte da D in $P\hat{A}D$. Però $\angle IJD = \angle IFP = 90 - \frac{A\hat{P}D}{2}$

Dunque $\angle JDA = \angle IJD - \angle JAD = 90 - \frac{A\hat{P}D}{2} - \frac{P\hat{A}D}{2} = \frac{P\hat{D}A}{2} \Rightarrow DJ$ è bisettrice di $P\hat{D}A \Rightarrow J$ è incentro di $A\hat{P}D$.

(vii) $J\hat{T}D = \pi - J\hat{I}D = I\hat{A}D + I\hat{D}A = \frac{B\hat{A}D}{2} + \frac{B\hat{D}A}{2} = \frac{\pi}{2} - \frac{A\hat{B}D}{2} = \frac{\pi - A\hat{B}D}{2} =$

$= \frac{A\hat{T}D}{2}$ ∎



- PAB triangolo, Γ cfr circoscritta, γ cfr. che tange PA in E, PB in F, Γ in T

Cosa abbiamo mostrato fino ad ora

(I) I incentro di APB, sta su EF

<u>Dim. 2</u> Pascal su $PM_{AP}ATMM_{PB}$

(II) $EI = IF$

PI è bisettrice/altezza/mediana nel triangolo isoscele $\widehat{PEF}$.

(III) $IFBT$, $IEAT$ ciclici

(IV) TI biseca $A\hat{T}B$. Dunque $T, I, M' \to$ p.to medio dell'arco $\overset{\frown}{APB}$, allineati, cioè $I\hat{T}M = \pi/2$

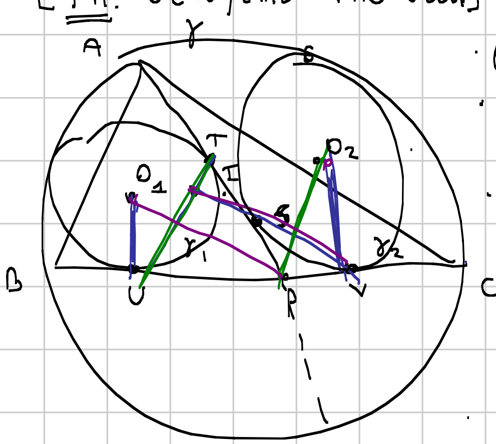
(V) TM, AB, EF concorrono [Ex.]

<u>Hint.</u> $\odot TMI$, $\odot AIB$, Γ [Le prime due tangono EF]

(VI) $V := PT \cap EF$. Allora $E\hat{V}A = F\hat{V}B$ [Ex.]

<u>Hint:</u> Lavorateci...

[<u>Th.</u> Sawayama-Thébault] [Ex.]

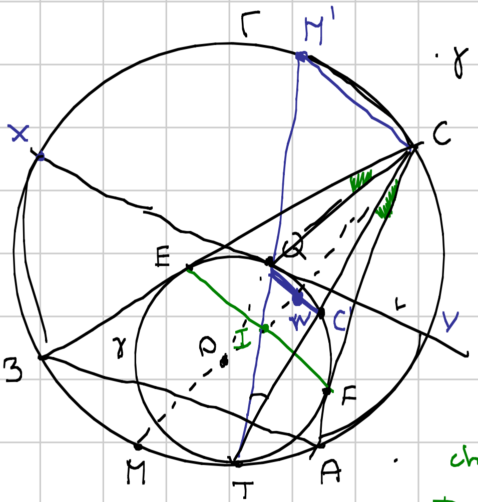


- ABC triangolo, γ circoscritta
- AP ceviana, γ_1 mixt. (AP, PB, γ) di centro O_1, γ_2 mixt. (AP, PC, γ) di centro O_2
- I incentro di ABC

<u>Th</u>: O_1, I, O_2 allineati

<u>Hint.</u> $I \in SV$ deriva dalla II figura
$I \in UT$
+ Th. di Pappo $\Rightarrow$ <u>Thesi</u>.

EGMO 2013 - 5



- ABC triangolo, Γ circoscritta
- γ circ. mixtilinea (BC, AC, Γ) con p.ti di tangenza E, F, T
- r ∥ AB tangente a γ in Q

Th $B\hat{C}Q = T\hat{C}A$.

Dim. $TQ \cap \Gamma =: M'$ p.to medio di XY, ma anche di AB perché AB ∥ XY

Prima dobbiamo mostrare che T, I, M' allineati. Quindi T, I, Q, M' allineati.

Traccio CI ... $CI \cap \Gamma =: M$. Allora MM' diametro

Su CI c'è anche O centro di γ

Noi vorremmo CI bisettrice di $Q\hat{C}T$ ... e avremmo la tesi

Sia $C' := TC \cap \gamma$. $QC' \parallel M'C \perp MC \Rightarrow QC' \perp CI$

omot. M'M diam.

Siccome CI passa per O et è $\perp C'Q$, $C'Q \cap CI$ (=W) è p.to medio di QC'

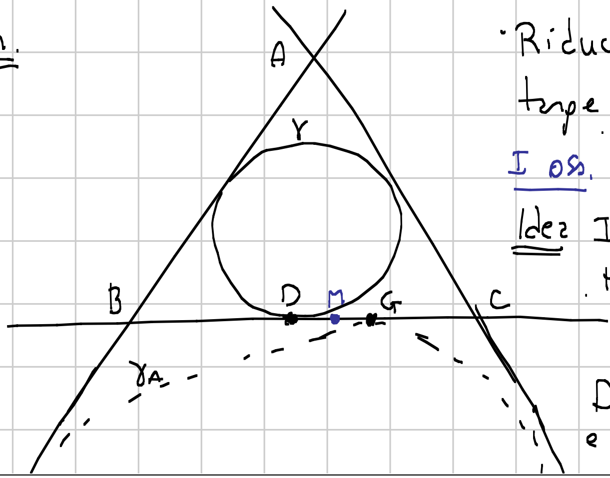
Quindi in CQC', CW è mediana e altezza → il triangolo è isoscele, CW è anche bisettrice ⇒

⇒ $Q\hat{C}I = I\hat{C}T$ ⇒ $B\hat{C}Q = T\hat{C}A$.

Inversione

Thm (Feuerbach) [p>γ] La cfr di Feuerbach di ABC tange l'inscritta e le exinscritte

Dim.



- Riduciamo la tesi a Feuerbach tange γ e γ_A.

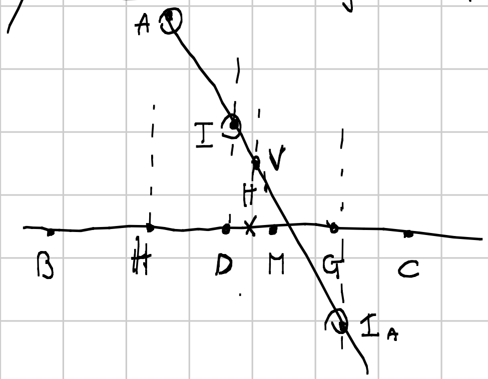
I oss. MD = MG

Idea Invertire nel punto medio con raggio MD=MG. Allora D e G restano fissi

Ma anche γ e γ_A restano fisse!

Dove va a finire Feuerbach e mostrare che va a finire in una retta che tange γ e γ_A.

Q1 Dove va a finire H?



H va a finire in un punto H' t.c. $MH \cdot MH' = MD^2$

$\Rightarrow$

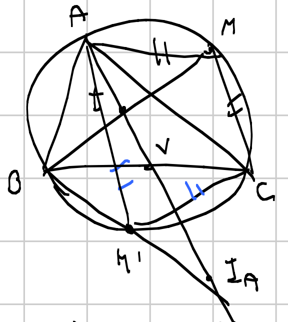
$(H, H', D, G) = -1 \Rightarrow$

$(A, V, I, I_A) = -1$

Oss.

$(A, V, I, I_A) = -1$ sse $(A, C, M, M')_\gamma = -1$

sse $\left|\frac{AM}{MC} \cdot \frac{CM'}{M'A}\right| = 1$

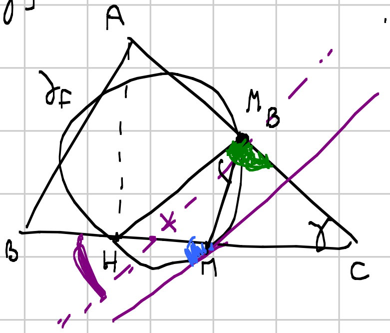


Dunque $V \equiv$ piede della bisettrice

$H \to X$ piede della bisettrice.

Q2 Che angolo forma Feuerbach con BC?

$[\beta > \gamma]$



Invertendo in M, γ_F va a finire in una retta // alla retta r.

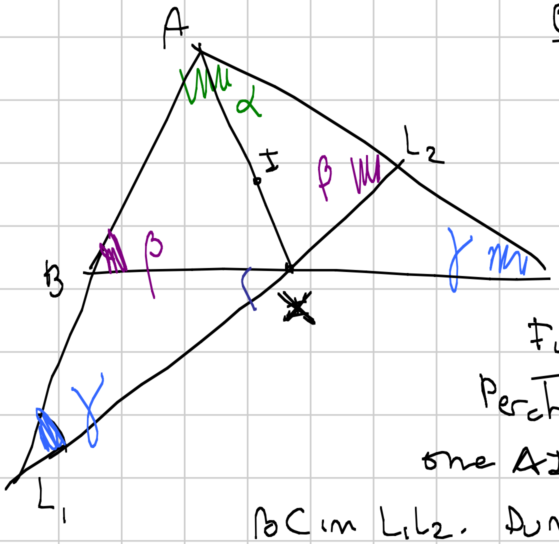
Q3 Come determiniamo ?

$H\hat{M}_B C = 180 - 2\gamma$

$M\hat{M}_B C = \alpha$

$H\hat{M}_B M = \underline{180 - \gamma - \alpha} - \gamma = \beta - \gamma$

Dunque $\gamma_F \to$ nella retta per X t.c. l'angolo è $\beta - \gamma$



Q4 $A\widehat{L_1}L_2 \overset{?}{=} A\hat{B}C - B\hat{X}L_1 = \beta - (\beta - \gamma) = \gamma$

Dunque chi è L_1L_2?
È la simmetrica di BC rispetto ad AX.

Fine.

Perché una simmetria assiale di asse AI fissa γ e γ_A e manda BC in L_1L_2. Dunque la tangente rimane corretta per simmetria assiale e quindi L_1L_2 tange γ e γ_A.

Ex. [IMO 2015-3]

TEORIA DEI NUMERI - MEDIUM 1

Note Title 9/4/2017

Ballo

- POLINOMI IN $\mathbb{Z}_p$ E AFFINI
- ESTENSIONI "PICCOLE" DI $\mathbb{Z}_p$
- RESIDUI QUADRATICI IN $\mathbb{Z}_p$
- GENERATORI E POLINOMI CICLOTOMICI (PROBABILMENTE NELLA PROSSIMA)

TEOREMA DI FERMAT (PICCOLO)

$(a,n)=1$

MCD

$a^{\varphi(n)} \equiv 1 \ (n)$

ALLORA IL TEOREMA DI EULERO

SE n È PRIMO SI CHIAMA FERMAT

L'IDEA È QUELLA DI PRENDERE TUTTI I RESIDUI MOD n COPRIMI CON n.

CON $n=10$

$1, 3, 7, 9$

E CONSIDERARE LA MAPPA

$$x \mapsto ax \quad (n)$$

CON $(a, n) = 1$ FISSATO

SE PRENDO TUTTI I RESIDUI COPRIMI CON n E LI MOLTIPLICO PER a LI STO PERMUTANDO

$$\begin{array}{ccc} & a=3 & \\ 1 & \longrightarrow & 3 \\ 3 & \longrightarrow & 9 \\ 7 & \longrightarrow & 1 \\ 9 & \longrightarrow & 7 \end{array}$$

$$\cancel{1 \cdot 3 \cdot 7 \cdot 9} \equiv 3 \cdot 9 \cdot 1 \cdot 7 \quad (10)$$

$$\downarrow$$

$$a \cdot 1 \cdot a \cdot 3 \cdot a \cdot 7 \cdot a \cdot 9 \quad (10)$$

$$\cancel{1 \cdot 3 \cdot 7 \cdot 9} \cdot a^4 \quad (10)$$

$$a^4 \equiv 1 \quad (10)$$

WILSON p PRIMO

$$(p-1)! \equiv -1 \ (p)$$

- CON GLI INVERSI

SE FACCIO IL PRODOTTO DI TUTTI I RESIDUI $\not\equiv 0 \ (p)$

ACCOPPIO (a,b) CON $a \cdot b \equiv 1 \ (p)$

TUTTI SI POSSONO ACCOPPIARE PERCHÉ $a \neq b$, TRANNE QUELLI CON

$$a^2 \equiv 1 \ (p)$$

LORO SI ACCOPPIANO DA SOLI

$a^2 \equiv 1 \ (p)$ HA SOLO ± 1 COME SOLUZIONE

$$(a-1)(a+1) \equiv 0 \ (p) \rightarrow \begin{array}{l} a \equiv -1 \ (p) \\ a \equiv 1 \ (p) \end{array}$$

COSÌ HO: 1 DA SOLO
−1 DA SOLO

$p > 2$

TUTTI GLI ALTRI ACCOPPIATI } IL LORO PRODOTTO FA 1

(È IL PRODOTTO DI TANTE COPPIE CHE FANNO 1)

$$\longrightarrow -1 \quad (p)$$

- GENERATORI (QUASI UGUALE)
- POLINOMI

CONSIDERIAMO IN $\mathbb{Z}_p$ IL POLINOMIO

$$x^{p-1}-1$$

CHE RADICI HA? (FERMAT)

$\{1, 2, \dots, p-1\}$ SONO RADICI

$$x^{p-1}-1 \equiv (x-1)(x-2)(x-3)\dots(x-(p-1)) \quad (p)$$

STESSO TERMINE NOTO

$$-1 \equiv (-1)\cdot(-2)\cdot\ldots\cdot(-(p-1)) \equiv (-1)^{p-1}\cdot(p-1)! \quad (p)$$

SE $p>2$ $\quad -1 \equiv (p-1)! \quad (p)$

IL PROBLEMA DI QUESTA DIMOSTRAZIONE
È ☆

NON È DETTO CHE POSSIAMO SCRIVERE QUELL' UGUAGLIANZA SOLO SAPENDO LE RADICI

$x^2 - 4 \quad (15)$

CHE RADICI HA?

$2 \quad 7$

$-2 \quad -7$

$x^2 - 4 \not\equiv (x-2)(x+2)(x+7)(x-7) \quad (15)$

SE CI METTO DENTRO $x=0$

$-4 \not\equiv 1 \quad (15)$

IN REALTÀ ☆ HA SEMPRE SENSO MODULO p (A DOPO IL MOTIVO)

ORDINI MOLTIPLICATIVI

$ord_n(a)$ IL MINIMO $K>0$ T.C.

$$a^K \equiv 1 \ (n)$$

$ord_n(a) \mid \varphi(n)$

$ord_p(a) \mid p-1$

SIA $n>1$ INTERO POSITIVO p PRIMO T.C.

$$p \mid 2^{2^n}+1$$

$$\longrightarrow 2^{n+1} \mid p-1$$

$$2^{2^n} \equiv -1 \ (p) \xrightarrow{\square} 2^{2^{n+1}} \equiv 1 \ (p)$$

$ord_p(2) \mid 2^{n+1}$ SE $ord_p(2) = 2^K$

CON $K < n+1$

$$\boxed{ord_p(2) \mid p-1}$$

$$2^{2^K} \equiv 1 \ (p)$$

ELEVO AL $\square$

$m-K$ VOLTE

$$2^{2^m} \equiv 1 \ (p)$$

ASSURDO! $2^{2^n} \equiv 1 \ (p)$ $2^{2^n} \equiv -1 \ (p)$

$\longrightarrow p = 2$ ($2^{2^n} + 1$ È DISPARI).

PERCIÒ $\mathrm{ord}_p(2) = 2^{n+1}$

$$2^{n+1} \mid p-1$$

FINE DEL RIPASSO

QUANDO POSSO SCRIVERE I POLINOMI SAPENDO LE LORO RADICI?

QUALE CONDIZIONE È NECESSARIA PER SCRIVERE UN POLINOMIO $f(x)$ DI GRADO n NELLA FORMA

$$(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$$

IN MODO UNICO

LEGGE DELL'ANNULLAMENTO DEL PRODOTTO

AVERE PIÙ DI n RADICI

(SENNÒ $(x-\alpha_1)\dots(x-\alpha_k)$ AVREBBE GRADO $>n$)

LEGGE DELL'ANNULLAMENTO DEL PRODOTTO:

$$a \cdot b = 0 \rightarrow a=0,\ b=0$$

✓ $\mathbb{Z}_p$ ✗ $\mathbb{Z}_{15}$ $3 \cdot 5 = 0$

$\mathbb{Q}, \mathbb{C}, \mathbb{Z}$

AD ESEMPIO: I NOSTRI POLINOMI POSSONO AVERE n RADICI, DI PIÙ, DI MENO

ABBASTANZA BENE

$x^2 - 19$

$\mathbb{Q}$: 0; $\pm\sqrt{19}$ IRRAZIONALE

$\mathbb{C}$: 2 $\pm\sqrt{19}$

$\mathbb{Z}_{15}$: 4 2, −2, 7, −7

$\mathbb{Z}_{17}$: 2 ± 6

$$x^2 - 19 \equiv x^2 - 36 \quad (17)$$

$$(x-6)(x+6) \equiv 0 \quad (17)$$

PRIMO

$\mathbb{Z}_{13}$: 0 / 2

$x^2 - 19$

SUPPONIAMO a SIA UNA SUA RADICE

$$a^2 \equiv 19 \ (13) \rightarrow a^2 \equiv 6 \ (13)$$

$$a^{12} \equiv 6^6 \ (13)$$

$$1 \equiv 216^2 \ (13)$$

$$1 \equiv 8^2 \ (13)$$

$$1 \equiv -1 \ (13)$$

L'ASSURDO STA NELL'AVER SUPPOSTO CHE ESISTA UN a INTERO.

PRENDIAMO $x^2 - 2$ (3)

0 RADICI.

ALLORA LE CREO: NE CREO UNA (α)

$\mathbb{Z}_3$	$\mathbb{Z}_3(\alpha)$		
	0	α	2α
0			
1	1	$1+\alpha$	$1+2\alpha$
2	2	$2+\alpha$	$2+2\alpha$

ORA METTO LE REGOLE:

$$\alpha^2 \equiv 2 \quad (\mathbb{Z}_3(\alpha))$$

$$(a + b\alpha) + (c + d\alpha) \equiv (a+c)_{\mathbb{Z}_3} + (b+d)_{\mathbb{Z}_3}\, \alpha$$

$$(a+b\alpha)\cdot(c+d\alpha) \overset{\text{NORMALE}}{=}$$

$$ac+bc\alpha+ad\alpha+bd\cancel{\alpha^2}$$

2

$$(ac+2bd)_{\mathbb{Z}_3}+\alpha(bc+ad)_{\mathbb{Z}_3}$$

$+$ E $\cdot$ COMMUTATIVI

VORREMMO CHE $\mathbb{Z}_3(\alpha)$ AVESSE, COME $\mathbb{Z}_3$, LA LEGGE DI ANNULLAMENTO DEL PRODOTTO, SENNÒ COSA CI SCOMPONGO I POLINOMI?

$a\neq 0,\ b\neq 0 \rightarrow ab\neq 0$

in $\mathbb{Z}_3(\alpha)$ in $\mathbb{Z}_3(\alpha)$

NON SONO INTERI a E b STANNO IN $\mathbb{Z}_3(\alpha)$

ASSURDO: $a\neq 0$

$b\neq 0$

$ab=0$

$$a = (3x + y) + \alpha(3z + w)$$
$$b = (3\bar{x} + \bar{y}) + \alpha(3\bar{z} + \bar{w})$$

x, y, z, w
$\bar{x}, \bar{y}, \bar{z}, \bar{w}$

INTERI

$(y, w) \neq (0, 0)$
$(\bar{y}, \bar{w}) \neq (0, 0)$

$x, \bar{x}, z, \bar{z}$ CI SERVONO? NO

$3x$ SONO TUTTI INTERI MA NON α

- SOMMA OK
- PRODOTTO PER α È OK

$3k + \alpha$ ✓

$3k \cdot \alpha$

$$(3x + 3y\alpha) \cdot \alpha \to \overbrace{3x\alpha}^{0} + \overbrace{6y}^{0}$$

α^2 È INTERO

$x, \bar{x}, t, \bar{t}$ VIA

$$(y + w\alpha)(\bar{y} + \bar{w}\alpha) =$$

$$y\bar{y} + y\bar{w}\alpha + w\bar{y}\alpha + 2w\bar{w} \equiv 0$$

$$\begin{cases} y\bar{y} + 2w\bar{w} \equiv 0 \ (3) \\ y\bar{w} + w\bar{y} \equiv 0 \ (3) \end{cases}$$

$$y\bar{y} - w\bar{w} \equiv 0 \ (3)$$

$$\bar{w} \equiv \frac{y\bar{y}}{w} \ (3)$$

— CASO 1

$w \equiv 0 \ (3)$

$$y\bar{y} \equiv 0 \ (3)$$

$$y\bar{w} \equiv 0 \ (3)$$

$y \equiv 0 \ (3)$

$(y + \alpha w) = 0$

$\bar{y} \equiv 0 \ (3)$ $\bar{w} \equiv 0 (3)$

$(\bar{y} + \bar{w}\alpha) = 0$

CASO 2: $w \not\equiv 0\ (3)$

$$\bar{x} + \alpha \bar{w} \equiv 0\ (3)$$

$$\bar{w} \equiv \frac{y\bar{y}}{w}\ (3)$$

$$\bar{w} \equiv 0\ (3)$$

$$\frac{y^2\bar{y}}{w} + w\bar{y} \equiv 0\ (3)$$

$$\bar{y} \equiv 0\ (3)$$

$$\bar{y}\,(y^2 + w^2) \equiv 0\ (3)$$

$y^2 + w^2 \equiv 0\ (3)$ (FERMAT)

$$y^2 + w^2 \equiv y^2 - 2w^2$$

$$(y + \alpha w)(y - \alpha w) = y^2 - 2w^2$$

BISOGNA USARE CHE $x^2 - 2$ NON ABBIA RADICI PER L'ANNULLAMENTO DEL PRODOTTO

SE NON VI FIDATE PROVATE A FARE GLI STESSI CONTI CON

$p = 37 \qquad \alpha^2 = 29$

AFFINCHÉ $\quad y^2 - 2w^2 \equiv 0\ (3) \rightarrow (y, w) = (0, 0)$

Se $w \equiv 0 \ (3) \rightarrow y \equiv 0 \ (3)$

Altrimenti $\boxed{\left(\frac{x}{w}\right)^2 - 2 \equiv 0 \ (3)}$

Prendiamo $p = 7$ $\quad A^2 = 2$

e consideriamo $\mathbb{Z}_7(\sqrt{2})$.

Vale l'annullamento del prodotto?

$\sqrt{2} \equiv \pm 3 \ (7)$

$$x^2 - 2 \rightarrow (x+3)(x-3)$$

$$\underbrace{(\sqrt{2}+3)}_{\neq 0}\underbrace{(\sqrt{2}-3)}_{\neq 0} = 2 - 9 = 0 \quad \text{in } \mathbb{Z}_7(\sqrt{2})$$

$\mathbb{Z}_p(\sqrt{A})$ ha senso (nel senso che è bello) se e solo se $x^2 - A \ (p)$ non ha soluzioni.

- Se ha soluzione k allora $(k + \sqrt{A})(k - \sqrt{A}) = k^2 - A = 0$
- Se non ce l'ha, fate i conti e viene

COSA ABBIAMO FATTO PRIMA?

ABBIAMO VISTO LE PROPRIETÀ DEI CAMPI.

CAMPO: UN INSIEME CON DUE OPERAZIONI:

$+$ COMMUTATIVO, ASSOCIATIVO E HA:
- ELEMENTO NEUTRO (0)
- INVERSO $(a \to -a)$

$\cdot$ COMMUTATIVO, ASSOCIATIVO E HA:
- ELEMENTO NEUTRO (1)
- INVERSO (TUTTI TRANNE 0) $(a \to a^{-1})$

LEGGE DI ANNULLAMENTO DEL PRODOTTO

SE $a \neq 0$, $b \neq 0 \to ab \cdot a^{-1} \cdot b^{-1} =$
$= a \cdot a^{-1} \cdot b \cdot b^{-1} = 1 \cdot 1 = 1$ $\Rightarrow$ ab HA INVERSO

(PER COMPLETEZZA DIMOSTRIAMO CHE

$a \cdot 0 = 0$)

$$a \cdot (b-b) \underset{\text{DIST.}}{=} ab - ab = 0$$

(0 A PRIORI È SOLO L'EL. NEUTRO DEL +)

$$\mathbb{Z}_3(\sqrt{2})$$

$a + b\sqrt{2}$ TROVIAMO L'INVERSO

FACCIO IL CONTO

$$(a+b\sqrt{2})(c+d\sqrt{2}) =$$

$$\underbrace{(ac+2bd)}_{=1} + \sqrt{2}\,\underbrace{(bc+ad)}_{=0}$$

$$bc + ad \equiv 0 \ (3) \qquad d \equiv -\frac{bc}{a} \ (3)$$

CASO 1: $a \equiv 0 \ (3)$

$$(\cancel{b}\sqrt{2}) \cdot \boxed{(\cancel{b}^{-1} \cdot \sqrt{2}) \cdot (-1)} \equiv 1 \ (\mathbb{Z}_3[\sqrt{2}])$$

$$b \neq 0$$

$$\hookrightarrow d \equiv 2b^{-1}$$

$$c \equiv 0$$

$$(b\sqrt{2})(c + d\sqrt{2}) \equiv 1 \ (\mathbb{Z}_3[\sqrt{2}])$$

CASO 2: $a \not\equiv 0 \ (3)$

$$ac - 2b\frac{bc}{a} \equiv 1 \ (3)$$

$$c(a^2 - 2b^2) \equiv a \ (3)$$

$$\hookrightarrow \not\equiv 0 \quad (\Leftarrow (a,b) \neq (0,0))$$

$$c \equiv \frac{a}{a^2 - 2b^2} \ (3) \quad \left(\text{ANCHE NEL CASO } 1\right)$$

$$d \equiv -\frac{bc}{a} \equiv -\frac{ba}{a(a^2-2b^2)} \ (3)$$

$$\equiv -\frac{b}{a^2 - 2b^2} \ (3) \quad \left(\text{ANCHE NEL CASO } 1\text{? SÌ: } a = 0 \text{ E DIVENTA } \tfrac{1}{2}b^{-1}\right)$$

L'INVERSO DI $(a+b\sqrt{2})$ È

$$\left(\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}\right)$$

$$\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}$$ (IN REAL LIFE)

(BASTAVA RAZIONALIZZARE)

CHE CAMPI CONOSCIAMO?

$\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$, $\mathbb{Q}$, $\mathbb{Z}_p(\sqrt{a})$

p PRIMO

x^2-a NO SOL. (p)

CHE PROPRIETÀ HANNO I POLINOMI A COEFFICIENTI IN UN CAMPO?

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$$

$a_n \neq 0$

POSSO MOLTIPLICARE PER a_n^{-1} TUTTO:

A MENO DI COSTANTI MOLTIPLICATIVE, TUTTI I POLINOMI SONO MONICI.

(I.E.: $\mathbb{Z}$ $\quad$ $x+1$ DIVISO $2x$ È ANTIPATICO:

$$x+1 = 2x\, p(x) + q(x)$$

$q(x)$ HA SEMPRE GRADO ≥ 1.

(UNO SPERA IN UN RESTO PIÙ PICCOLO)

NEI CASI, SE HO $p(x)$ E $q(x)$ POSSO FARE LA DIVISIONE EUCLIDEA.

IN $\mathbb{Z}_{439}$.

$$7x^8 + 23x^6 + x - 1 \quad \text{DIVISO} \quad 13x^4 + 7x - 1$$

$$(13x^4 + 7x - 1) \cdot \Bigg(\underbrace{\frac{7x^8}{13x^4}}_{(c\,x^4)} \Bigg)$$

FACCIO LA DIVISIONE EUCLIDEA TRA

$$\big(\underline{p(x) - q(x) \cdot c x^4}\big) \,/\, q(x)$$

QUINDI SI OTTIENE UN RESTO:

$$p(x) = q(x) \cdot \bar{q}(x) + \underline{r(x)}$$

(FUNZIONA ANCHE IN $\mathbb{Z}$ SE $q(x)$ È MONICO)

$$\deg r < \deg p$$

IN UN CAMPO, $f(x)$ DI GRADO n, QUANTE RADICI PUÒ AVERE?

AL MASSIMO n

VEDIAMO SE VALE RUFFINI.

SE $f(\alpha)=0 \to f(x)=(x-\alpha)\,g(x)$

FACCIAMO LA DIVISIONE EUCLIDEA TRA

$f(x)\,/\,(x-\alpha)$

deg 1 HA GRADO 0

$$f(x)=g(x)(x-\alpha)+\underbrace{r(x)}_{r}$$

α

$$0=f(\alpha)=g(\alpha)\cdot 0+r$$

$r=0. \to$ RUFFINI

$$f(x)=(x-\alpha)\,g(x)$$

INDUZIONE!

Hp. Ind. OGNI POLINOMIO DI GRADO n HA AL PIÙ n RADICI

$$\underbrace{f(x)}_{\deg n} = (x-\alpha)\cdot \underbrace{g(x)}_{\deg n-1}$$

AL PIÙ 1 RADICE

AL PIÙ $n-1$ RADICI

LEGGE DELL'ANNULLAMENTO DEL PRODOTTO!!!

SE α È RADICE DI $p(x)\,q(x)$, ALLORA α È RADICE DI $p(x)$ O DI $q(x)$.

(FATE IL PASSO BASE)

[NON INTERROGHIAMOCI SUL GRADO DI 0, DICIAMO CHE NON HA GRADO]

VOGLIAMO LA FATTORIZZAZIONE UNICA.

(A MENO DI COSTANTI $\neq 0$)

INVERTIBILI

ASSUMIAMOCI QUINDI MONICI.

CI SONO DUE TIPI DI POLINOMI:

- FATTORIZZABILI IN 2 O + POLINOMI; $f(x) = p(x)\,q(x)$
- IRRIDUCIBILI.

OGNI POLINOMIO SI SCRIVE COME PRODOTTO DI FATTORI IRRIDUCIBILI

SI VA PER INDUZIONE:

f — IRRIDUCIBILE ✓

$f = p(x) \cdot q(x)$

... IRRIDUCIBILE ... IRRIDUCIBILE ...

PER COME HO DEFINITO IRRIDUCIBILE (A UNA CERTA ARRIVO A GRADO 0)

IN $\mathbb{Z}_{15}$ $\quad x^2-4 \equiv (x-2)(x+2)$

$$\eqcirc$$

$$(x-7)(x+7)$$

IN UN CAMPO È DAVVERO UNICA?

PER ASSURDO:

$$\prod_{i=1}^{n} \underbrace{p_i}_{\text{IRRIDUCIBILI}}(x) = \prod_{i=1}^{m} \underbrace{q_i}_{\text{IRRIDUCIBILI}}(x)$$

- VORREI ANNULLARCI CON UN A_i MA, AD ESEMPIO, IN $\mathbb{Q}$ x^2+1 NON HA RADICI

SUPPONIAMO CHE $p_1(x)$ NON SIA NESSUN $q_i(x)$.

$p_1(x)$ DIVIDE $\prod p_i(x)$

$p_1(x)$ DIVIDE $\prod q_i(x)$

PER LA DIVISIONE EUCLIDEA:

$$\prod q_i(x) = g(x) \cdot p_1(x)$$

SE $p_1(x)$ DIVIDE $a(x) \cdot b(x)$

VOGLIAMO MOSTRARE CHE $p_1(x) \mid a(x)$

OPPURE $p_1(x) \mid b(x)$

$$a(x) = p_1(x) \cdot \alpha(x) + r_a(x)$$
$$b(x) = p_1(x) \cdot \beta(x) + r_b(x)$$

$$p_1(x) \mid (p_1(x) \cdot \alpha(x) + r_a(x))(p_1(x) \cdot \beta(x) + r_b(x)) = p_1(x)\big(p_1(x)\,\alpha(x)\,\beta(x) + r_a(x) + r_b(x)\big) + r_a(x)\, r_b(x)$$

$$\longrightarrow \underbrace{p_1(x)}_{\deg = k} \mid \underbrace{r_a(x)}_{\deg < k} \underbrace{r_b(x)}_{\deg < k}$$

USIAMO BÉZOUT

(FIGLIO DELL'ALGORITMO DI EUCLIDE)

$$p_1(x) = r_2(x)\cdot v_1(x) + \mu_1(x)$$

$$r_2(x) = \mu_1(x)\cdot v_2(x) + \mu_2(x)$$

$$\mu_1(x) = \mu_2(x)\cdot v_3(x) + \mu_3(x)$$

$$\dots$$

$$\mu_j(x) = \boxed{\mu_{j+1}(x)}\cdot v_{j+2}(x) + 0$$

PER QUESTIONI DI GRADO

(PASSAGGIO PRIMA ...)

$$\mu_{j-1}(x) = \mu_j(x)\cdot v_{j+1}(x) + \mu_{j+1}(x)$$

$$\boxed{\mu_{j+1}(x)} = \mu_{j-1}(x) - \mu_j(x)\cdot v_{j+1}(x)$$

$$\mu_j(x) = \mu_{j-2}(x) - \mu_{j-1}(x)\cdot v_j(x)$$

$$\dots$$

$$\mu_2(x) = r_2(x) - v_2(x)\cdot \mu_1(x)$$

$$\mu_1(x) = p_1(x) - v_1(x)\cdot r_2(x)$$

QUINDI:

$$m_{j+1}(x) = a(x) \cdot p_1(x) + b(x) r_0(x)$$

È VERO CHE m_{j+1} DIVIDE ENTRAMBI!?

☆ m_{j+1} DIVIDE m_j

QUINDI

m_{j-1}

...

DIVIDE $r_0(x)$ E $p_1(x)$

QUINDI $m_{j+1}(x) = 1$ (O COSTANTE)

$= p_1(x) \cdot$ COSTANTE

QUESTIONI DI GRADO

$= p_1(x)$: $r_0(x)$ NON È MULTIPLO DI m_{j+1}

A MENO CHE $r_0(x) = 0$

(MA ALLORA $p_1(x) \mid a(x)$)

$= 1$

$$\boxed{p_1(x)\cdot a(x) + r_a(x)\cdot b(x) = 1}$$

Hp. $p_1(x) \mid r_a(x)\, r_b(x)$

MOLTIPLICHIAMO PER $r_b(x)$

$$\underbrace{p_1(x)\cdot a(x)\cdot r_b(x)}_{\text{MULT. DI } p_1} + \underbrace{r_a(x)\cdot r_b(x)\cdot b(x)}_{\text{MULT. DI } p_1} = r_b(x)$$

MULT. DI p_1

QUINDI È 0.

QUINDI SE $p_1(x) \mid a(x)\cdot b(x) \rightarrow$
$p_1(x) \mid a(x)$, $p_1(x) \mid b(x)$

IRRIDUCIBILE

$$p_1(x) \mid \prod_{i=1}^{m} q_i(x) = q_1(x)\cdot \prod_{i=2}^{m} q_i(x)$$

$p_1(x)$
- DIVIDE $q_1(x)$ IRRIDUCIBILE $\rightarrow p_1(x) = q_1(x)$
- DIVIDE $\prod_{i=2}^{m} q_i(x)$
  - $q_2(x)$
  - $\prod$

QUINDI UN $q_i(x) = p_1(x)$

$$p_1(x) \cdot \prod_{i=2}^{n} p_i(x) = p_1(x) \cdot \prod_{\substack{i=1 \\ i \neq k}}^{m} q_i(x)$$

VORREMMO CHE $p_1(x)$ ANDASSE VIA

IL PROBLEMA SONO COSE TIPO

$$p_1^2 \cdot p_2 = p_1 \cdot p_2^2$$

RACCOGLIAMO $p_1(x)$

$$p_1(x)\left(\prod p_i(x) - \prod q_i(x)\right) = 0$$

$= 0$

ANNULLAMENTO DEL PRODOTTO,
MA L'ABBIAMO SOLO SUI COEFFICIENTI,
MA SUI POLINOMI È GRATIS:

BASTA IL TERMINE DI GRADO MASSIMO

O COME POLINOMIO!

POSSO QUINDI DIRE

$$\prod_{i=2}^{n} p_i(x) = \prod_{\substack{i=1 \\ i \neq j}}^{m} q_i(x)$$

TEOREMA (LO DIMOSTRIAMO ALLA II LEZIONE)

OGNI CAMPO FINITO AMMETTE UN GENERATORE.

OVVERO UN ELEMENTO g CHE HA ORDINE MOLTIPLICATIVO $= \#$ ELEMENTI INVERTIBILI

(L'ORDINE MOLTIPLICATIVO IN CAMPO $\mathbb{K}$ DI x È IL MINIMO INTERO POSITIVO n t.c. $x^n = 1$ (IN $\mathbb{K}$).)

$1, g^1, g^2, \ldots, g^{s-1}$ DOVE s È IL NUMERO DI ELEMENTI INVERTIBILI $(|\mathbb{K}| - 1)$ SONO TUTTI

GLI ELEMENTI DEL CAMPO TRANNE ZERO.

(INFINITI NOI TIPO $\mathbb{Q}$).

ESERCIZI TIPO TEORICI.

DIMOSTRARE CHE IN $\mathbb{Z}_p(\sqrt{\alpha})$ CON $x^2-\alpha$ SENZA RADICI IN $\mathbb{Z}_p$ VALE

$$x^{p^2-1} \equiv 1 \ (\mathbb{Z}_p(\sqrt{\alpha})) \quad \forall x \neq 0.$$

CONSIDERIAMO:

$$\prod_{\substack{x \in \mathbb{Z}_p(\sqrt{\alpha}) \\ x \neq 0}} x \qquad \underline{\hspace{4cm}}$$

$x \mapsto \alpha x$ (PERMUTAZIONE)

$x \mapsto \alpha x$ $\quad x \neq y \to \alpha x \neq \alpha y$

$y \mapsto \alpha y$ $\quad$ PERCHÉ POSSO MOLTIPLICARE PER α^{-1}

$0 \mapsto 0$

LE FUNZIONI INIETTIVE SU INSIEMI FINITI SONO PERMUTAZIONI (SULLO STESSO)

$$\prod_{\substack{x \neq 0 \\ x \in \mathbb{Z}_p(\sqrt{a})}} (a x) = a^{|\mathbb{Z}_p(\sqrt{a})|-1} \cdot \prod_{\substack{x \neq 0 \\ x \in \mathbb{Z}_p(\sqrt{a})}} x$$

$$a^{p^2-1} \equiv 1 \quad (\mathbb{Z}_p(\sqrt{a}))$$

WILSON

$$\prod_{\substack{x \neq 0 \\ x \in \mathbb{Z}_p(\sqrt{a})}} x$$

CONSIDERIAMO IL POLINOMIO:

$$x^{p^2-1} - 1 \quad \text{IN } \mathbb{Z}_p(\sqrt{a})$$

HA p^2-1, TUTTI E SOLI GLI EL. INVERTIBILI

È VERO CHE:

$$x^{p^2-1}-1=\prod_{\alpha \text{ invertibile}}(x-\alpha) \quad ?$$

QUANDO LE RADICI IN UN CAMPO DI UN POLINOMIO SONO TANTE QUANTE IL SUO GRADO SÌ.

OGNI $x-\alpha$ DIVIDE $x^{p^2-1}-1$

QUINDI

$$\prod_{\alpha \text{ invertibile}}(x-\alpha) \quad \text{DIVIDE} \quad x^{p^2-1}-1 \quad \text{PERCHÉ}$$

GLI $x-\alpha$ SONO IRRIDUCIBILI

HA GRADO p^2-1

VISTO CHE SONO MONICI:

$$\prod_{\alpha \text{ invertibile}}(x-\alpha)=x^{p^2-1}-1$$

$$x=0 \rightarrow (-1)^{p^2-1}\cdot\prod_{\alpha \text{ invertibile}}\alpha=-1$$

$\square$

SIA $p>5$ PRIMO E SIA $F_0=0$, $F_1=1$,
$F_{n+2}=F_{n+1}+F_n$ (FIBONACCI),
SI MOSTRI CHE $p \mid F_{p^2-1}$

CONSIDERIAMO $\overline{\mathbb{Z}_p(\sqrt{5})}$

CASO I: x^2-5 (p) HA SOLUZIONE

$$F_n=\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

$a+b\sqrt{5}$ CON a,b RAZIONALI NON CON DENOMINATORI MULTIPLI DI p, HA SENSO VEDERLI COME NUMERI MODULO p, PONENDO
$\sqrt{5}=k$ T.C. $p \mid k^2-5$

PROBLEMA 1: k O $-k$?

$p = 7$

$$4+\sqrt{2} \begin{cases} 4+3 \\ 4+4 \end{cases}$$

$$(a+b\sqrt{\alpha})(c+d\sqrt{\alpha}) =$$

$$= \underline{ac+\alpha bd} + \sqrt{\alpha}(bc+ad) \equiv K^2 \ (p)$$

MOTIVO CRUCIALE: QUANDO FACCIO $(a+b\sqrt{\alpha})(c+d\sqrt{\alpha}) = x+y\sqrt{\alpha}$

SE NEL FARE I CONTI $y \equiv 0 \ (p)$,

POSSO SCEGLIERE INDIFFERENTEMENTE $\sqrt{\alpha} \begin{cases} k \\ -k \end{cases}$

$$\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{p^2-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{p^2-1}\right) \equiv$$

$$\boxed{K^2 \equiv 5 \ (p)}$$

$$\equiv \frac{1}{K}\left(\left(\frac{1+K}{2}\right)^{p^2-1} - \left(\frac{1-K}{2}\right)^{p^2-1}\right) \equiv$$

$$\hookrightarrow (\wedge(p-1))^{\wedge(p+1)}$$

FERMAT

$$\equiv \frac{1}{\cancel{\sqrt{5}}}(1-1) \equiv 0 \ (p)$$

• II CASO: $\mathbb{Z}_p(\sqrt{5})$ ESISTE ED È UN CAMPO

a^{p^2-2} È L'INVERSO DI a

$$\frac{1}{\sqrt{5}}\left(\underbrace{\left(\frac{1+\sqrt{5}}{2}\right)^{p^2-1}}_{1} - \underbrace{\left(\frac{1-\sqrt{5}}{2}\right)^{p^2-1}}_{1}\right) \equiv 0 \ (\mathbb{Z}_p(\sqrt{5}))$$

(ES. PER CASA: PROVATE A VEDERE SE IN $\mathbb{Z}_p(\sqrt{5})$ BECCO

$$\left(\frac{1+\sqrt{5}}{2}\right)^{p+1} = \pm 1$$

(MA ANCHE SOLO CON IL + FORSE)

ESERCIZI PER CASA / CAMERA

[1] $a_0 = 2$, $a_{n+1} = 2a_n^2 - 1$

SE $p \mid a_n \rightarrow 2^{n(+3)} \mid p^2 - 1$

[2] SIA IN $\mathbb{Z}_p$ CHE IN $\mathbb{Z}_p(i)$, OGNI VALORE È ASSUNTO DA: (n FISSATO)

$$x_1^n + \ldots + x_n^n$$

Teoria dei Numeri 2 - Medium

Note Title 9/6/2017

(Ballo)

OGGI:
- LTE;
- GENERATORI E POLINOMI CICLOTOMICI;
- RESIDUI QUADRATICI;
- PELL / INTERI DI GAUSS / NIENTE.

LTE

PRELIMINARMENTE:

$v_p(n) = k$

↳ VALUTAZIONE p-ADICA

t.c. $p^k \mid n$ e $p^{k+1} \nmid n$

$v_p(n)$ È L'ESPONENTE DI p NELLA FATTORIZZAZIONE DI n. (I.E. $v_3(87)=1$)

LTE: p PRIMO DISPARI

$(a \neq b)$ a, b INTERI NON MULTIPLI DI p

$a-b$ MULTIPLO DI p.

n INTERO POSITIVO.

Th $\rightarrow$ $v_p(a^n - b^n) = v_p(a-b) + v_p(n)$

IDEA FONDAMENTALE: FACCIO IL CASO n PRIMO.

PERCHÉ? I.E.: $n = 60$ p

$$v_p(a^{60} - b^{60}) = v_p(a^{30} - b^{30}) + v_p(2) =$$

$$= v_p(a^{15} - b^{15}) + v_p(2) + v_p(2) =$$

$$= v_p(\boxed{a^5} - \boxed{b^5}) + v_p(2) + v_p(2) + v_p(3) =$$

$$= v_p(a-b) + v_p(2) + v_p(2) + v_p(3) + v_p(5) =$$

$$= v_p(a-b) + v_p(60)$$

SE LO SO FARE CON n PRIMO LO SO FARE

CON OGNI n.

CONTROLLIAMO CHE IN OGNI SINGOLA UGUAGLIANZA SIANO RISPETTATE LE IPOTESI DI LTE

$\underline{\text{Hp.}}$ $p \mid a-b,\ p \nmid a,\ p \nmid b$

OCCHIO: SOPRA NON ABBIAMO SEMPRE APPLICATO LTE AD a E b, MOLTO SPESSO L'ABBIAMO USATO SU a^k E b^k

$\underline{\text{Hp.}}$ NUOVE: $p \mid a^k-b^k,\ p \nmid a^k,\ p \nmid b^k$

OVVIA

OVVIA PERCHÉ p PRIMO

$p \mid a-b \mid a^k-b^k \rightarrow p \mid a^k-b^k$

QUINDI BASTA DAVVERO n PRIMO.

QUINDI DIMOSTRIAMOLO CON

$n = 1$

VOGLIAMO DIMOSTRARE CHE:

$$v_p(a^q - b^q) = v_p(a-b) + v_p(q)$$

SCRIVIAMO $a = b + kp$ PERCHÉ $p \mid b-a$

E ANDIAMO A SVILUPPARE

$$(b+kp)^q - b^q =$$

$$\cancel{b^q} + \binom{q}{1} \cdot b^{q-1} \cdot (kp) + \binom{q}{2} \cdot b^{q-2} \cdot (kp)^2 + \dots + \binom{q}{q-1} \cdot b \cdot (kp)^{q-1}$$

$$+ (kp)^q - \cancel{b^q} =$$

$$\binom{q}{1} \cdot b^{q-1} \cdot (kp) + \binom{q}{2} \cdot b^{q-2} \cdot (kp)^2 + \dots + \binom{q}{q-1} \cdot b \cdot (kp)^{q-1} + (kp)^q$$

NOI VOGLIAMO TROVARNE LA v_p

HA POCHI p DENTRO (MENO DEGLI ALTRI TERMINI)

$$\sum_{i=1}^{q} \binom{q}{i} \cdot b^{q-i} \cdot (kp)^i$$

$$v_p\left(\underline{\binom{q}{i}}\cdot \underline{b^{q-i}}\cdot \underline{(Kp)^i}\right) =$$

$$= v_p\left(\binom{q}{i}\right) + v_p\left(b^{q-i}\right) + v_p\left((Kp)^i\right) =$$

$$= v_p\left(\binom{q}{i}\right) + \underbrace{\cancel{(q-i)\,v_p(b)}}_{=0} + i\, v_p(Kp) =$$

$$= v_p\left(\binom{q}{i}\right) + i\, v_p(Kp)$$

QUESTO CI DICE CHE:

SE $i > 1$:

$$v_p\left(\binom{q}{i}\cdot b^{q-i}\cdot (Kp)^i\right) > v_p\left(\binom{q}{1}\cdot b^{q-1}\cdot (Kp)\right)$$

PERCHÉ

$$v_p\left(\binom{q}{i}\right) + i\, v_p(Kp) \overset{\star}{>} v_p\left(\binom{q}{1}\right) + v_p(Kp)$$

C'È UN PROBLEMA: SE $p = q$

$$v_p\left(\binom{q}{1}\right) > v_p\left(\binom{q}{i}\right) \quad \text{A VOLTE}$$

CASO 1: $p \neq q$

$$\longrightarrow \quad v_p\left(\binom{q}{1}\right) = 0.$$

$$v_p\left(\binom{q}{i}\right) + i\, v_p(pk) > v_p(pk)$$

VERA PER OGNI $i > 1$ PERCHÉ $v_p(pk) > 0$

IN QUESTO CASO:

$$v_p\left(\sum_{i=1}^{q} \binom{q}{i} \cdot b^{q-i} \cdot (pk)^i\right) =$$

TUTTI GLI ALTRI TERMINI NELLA Σ HANNO v_p MAGGIORE

$$= v_p\left(\binom{q}{1} \cdot b^{q-1} \cdot (pk)^1\right) =$$

$$= v_p(pk) = v_p(a-b) \quad \checkmark$$

CASO n PRIMO, $n \neq p$, A POSTO:

$$v_p(a^n - b^n) = v_p(a-b) \; (+\underbrace{v_p(n)}_{=0})$$

CASO $n=p$.

$$\sum_{i=1}^{p} \binom{p}{i} \cdot (px)^i \cdot b^{p-i}$$

PRIMA $v_p\left(\binom{p}{1}\right) = 0$

IN GENERALE $v_p\left(\binom{p}{i}\right) =?$ $\begin{cases} 0 \\ 1 \end{cases}$

PERCHÉ AL NUMERATORE C'È $p!$,
CON AL MASSIMO UN p CHE COMPARE.

$$\frac{p!}{i!\,(p-i)!}$$

$p! \rightarrow v_p = 1$

$i!\,(p-i)! \rightarrow$ STESSO $v_p = 0$

$\rightarrow$ 2 SOLI CASI IN CUI È MULTIPLO DI p: $i=0$ E $i=p$

(SENNÒ NON ARRIVO A p)

$$v_p\left(\binom{p}{i}\right) \begin{cases} 0 & \text{SE } i=0,p \\ 1 & \text{ALTRIMENTI} \end{cases}$$

EURISTICAMENTE I TERMINI PROBLEMATICI SONO CON $i=1, p$

$$v_p\left(\binom{p}{i}\cdot \cancel{b^{p-i}}\cdot (kp)^i\right) \overset{?}{>} v_p\left(\binom{p}{1}\cdot \cancel{b^{p-1}}\cdot (kp)\right)$$

LA VORREMO PER OGNI $i>1$

$$v_p\left(\binom{p}{i}\right) + i\,v_p(kp) \overset{?}{>} v_p\left(\binom{p}{1}\right) + v_p(kp)$$

$v_p(kp)>0$; QUINDI $i\,v_p(kp) > v_p(kp)$

$$v_p\left(\binom{p}{i}\right) \geq v_p\left(\binom{p}{1}\right) \quad \forall\, 1\leq i\leq p-1$$

PERCIÒ SE $i\neq p$ LA ☆ È VERA

RESTA $i=p$.

$$p\,v_p(kp) > v_p\left(\binom{p}{1}\right) + v_p(kp)$$

$$(p-1)\,v_p(kp) > 1$$

VERA PER $p>2$

MOTIVO PER CUI LTE NON VALE PER $p=2$

PERCIÒ $v_p\left(\binom{p}{i}\cdot b^{p-i}\cdot(pk)^i\right) > v_p\left(\binom{p}{1}\cdot b^{p-1}\cdot(pk)\right)$
$\forall\, i > 1$

QUINDI:

$$v_p\left(\sum_{i=1}^{p}\binom{p}{i}\cdot b^{p-i}\cdot(pk)^i\right) = v_p\left(\binom{p}{1}\cdot b^{p-1}\cdot(pk)\right) =$$
$$= 1 + v_p(pk) = v_p(pk) + v_p(n)$$

$\square$

È p CHE DEVE ESSERE DISPARI, n PUÒ ESSERE CHIUNQUE.

VALE UNA SPECIE DI LTE CON IL 2, OVVERO:

$2 \nmid a,\ 2 \nmid b,\ 8 \mid a-b$

$$\longrightarrow\ v_2(a^n - b^n) = v_2(a-b) + v_2(n)$$

DIMOSTRATELO

(HINT: È UGUALE)

Es. DIMOSTRARE CHE 2 È GENERATORE MODULO 3^n PER OGNI n INTERO POSITIVO

$$2^k \equiv 1 \ (3^n)$$

CONDIZIONE: VORREMMO TANTO k MULTIPLO DI $\varphi(3^n) = 2 \cdot 3^{n-1}$

$$v_3(2^k - 1) = v_3(2-1) + v_3(k)$$

⚠ !

$$3 \nmid 2 - 1 \ !$$

NOTIAMO CHE:

$$2^k \equiv 1 \ (3^n) \to 2^k \equiv 1 \ (3) \to k = 2J$$

$$2^{2J} \equiv 1 \ (3^n) \to 4^J \equiv 1 \ (3^n)$$

$$v_3(4^J - 1) = v_3(4-1) + v_3(J)$$

$$v_3(4^J - 1) \geq n \leftarrow 3^n \mid 4^J - 1 \quad 2^{k} - 1$$

$$v_3(4-1) = 1$$

$v_3(J) \geq n-1 \rightarrow 3^{n-1} \mid J$

$2 \cdot 3^{n-1} \mid K$

$2^K \equiv 1 \ (3^n) \rightarrow 2 \cdot 3^{n-1} \mid K$

$ord_{3^n}(2) \mid \varphi(3^n)$ MA $\varphi(3^n) \mid ord_{3^n}(2)$

QUINDI $ord_{3^n}(2) = \varphi(3^n)$

ESISTENZA DI UN GENERATORE

DEFINIAMO I POLINOMI CICLOTOMICI.

I POLINOMI CICLOTOMICI SONO I COMPONENTI IRRIDUCIBILI (NON VEDREMO QUESTO) DEGLI $X^n - 1$

n	x^n-1	Scomposizione
1	$x-1$	$(x-1)$
2	x^2-1	$(x-1)(x+1)$
3	x^3-1	$(x-1)(x^2+x+1)$
4	x^4-1	$(x-1)(x+1)(x^2+1)$
5	x^5-1	$(x-1)(x^4+x^3+x^2+x+1)$
6	x^6-1	$(x-1)(x+1)(x^2+x+1)(x^2-x+1)$
7	x^7-1	$(x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$
8	x^8-1	$(x-1)(x+1)(x^2+1)(x^4+1)$
9	x^9-1	$(x-1)(x^2+x+1)(x^6+x^3+1)$
10	$x^{10}-1$	$(x-1)(x+1)(x^4+x^3+x^2+x+1)(x^4-x^3+x^2-x+1)$

Quindi questo ci consente di definire:

$$\Phi_n(x) = \frac{x^n-1}{\prod_{\substack{d\mid n \\ d<n}} \Phi_d(x)}$$ ☆

↳ n-esimo ciclotomico

L'idea è avere

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

Ci sono dei grossi problemi:

① È una buona definizione? Il quoziente è un polinomio?

② È a coefficienti interi?

Cosa sappiamo bene di $x^n - 1$? Le radici.

Un criterio per capire quando

$$\frac{p(x)}{q(x)}$$

è intero (come polinomio)?

Le radici di q stanno nelle radici di p (con molteplicità).

1 $x-1$

2 $x+1$

3 x^2+x+1

4 x^2+1

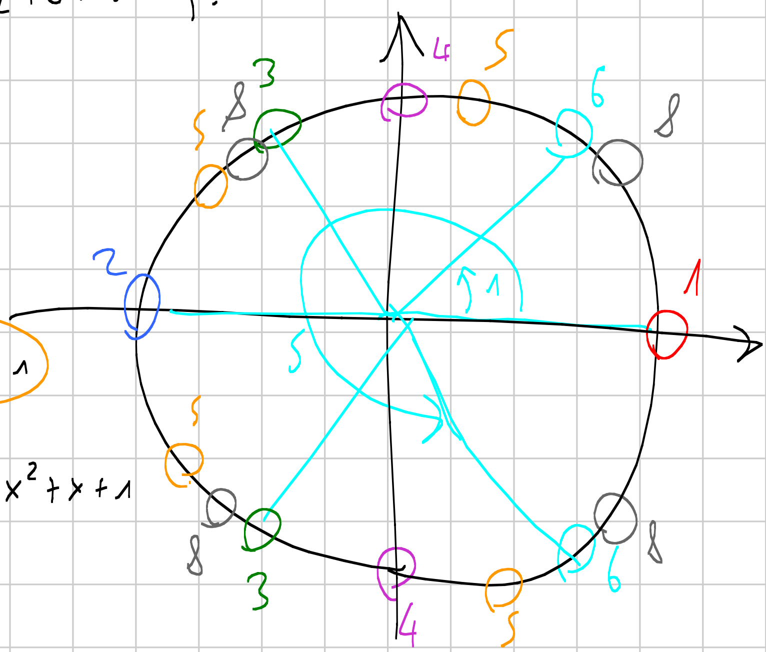
5 $x^4+x^3+x^2+x+1$

6 x^2-x+1

7 $x^6+x^5+x^4+x^3+x^2+x+1$

8 x^4+1

9 x^6+x^3+1



Noi sappiamo (speriamo) che le radici di $\prod_{d|n} \Phi_d(x)$ sono le radici n-esime dell'unità.

SE LE RADICI DI $\Phi_n(x)$ FOSSERO

ESATTAMENTE QUELLE DELLA FORMA $\omega^d - 1$

CON ω RADICE PRIMITIVA (PIÙ ADESSO)

DI $x^n - 1$ E $(d, n) = 1$ SAREMMO FELICI

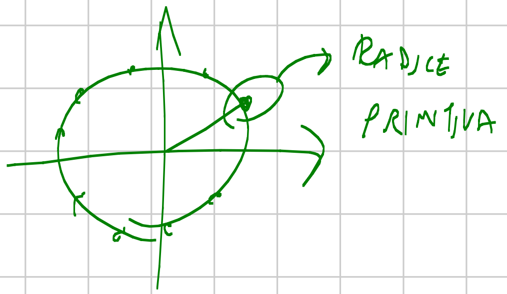
DIMOSTRIAMOLO PER INDUZIONE: (DEFINITI ATTRAVERSO ☆)

SUPPONIAMO PER IPOTESI INDUTTIVA CHE:

$\Phi_d(x)$ SIA UN POLINOMIO MONICO A COEFFICIENTI

INTERI CON RADICI ω^J DOVE $(J, d) = 1$

E ω È LA RADICE PRIMITIVA DI $x^\phi - 1$



PASSO BASE:

$n = 1 \rightarrow x - 1$ HA SOLO 1 COME RADICE

$n = 2 \rightarrow x + 1$ HA SOLO -1 COME RADICE,

PERCHÉ -1 È LA RADICE

PRIMITIVA DI $x^2 - 1$

E LE RADICI SONO $(-1)^{k}$ CON $(k,2)=1$.

PASSO INDUTTIVO

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d \mid n \\ d<n}} \Phi_d(x)}$$

COSA VOGLIAMO FORTEMENTE? VORREMMO CHE OGNI RADICE DI $\prod_{\substack{d \mid n \\ d<n}} \Phi_d(x)$ FOSSE RADICE DI $x^n - 1$

QUESTO È VERO PERCHÉ:

$$x^d - 1 = \prod_{\tilde{d} \mid d} \Phi_{\tilde{d}}(x) \rightarrow \Phi_d(x) \mid x^d - 1$$

E $x^d - 1 \mid x^n - 1$, QUINDI

$\Phi_d(x) \mid x^n - 1$, PERCIÒ LE RADICI DI $\Phi_d(x)$ STANNO IN $x^n - 1$

MANCA QUALCOSA? ALCUNE RADICI POTREBBERO COMPARIRE PIÙ VOLTE.

$$\frac{x^n-1}{\prod\limits_{\substack{d\mid n\\ d<n}} \Phi_d(x)}$$

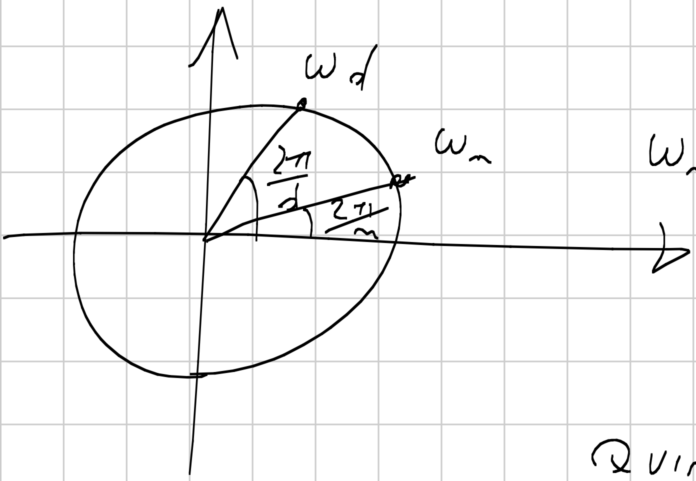
LE RADICI DI $\Phi_d(x)$ SONO DELLA FORMA

$\omega_d^{\,t}$ CON $(t,d)=1$

E ω_d RADICE PRIMITIVA DI x^d-1

INTERO

REL. FONDAMENTALE $\omega_d = \omega_n^{\left(\frac{n}{d}\right)}$



$\omega_n^{(n/d)}$ FORMA UN ANGOLO DI

$$\frac{2\pi}{n}\cdot\frac{n}{d}=\frac{2\pi}{d},$$

QUINDI È ω_d

SE LE RADICI DI $\Phi_d(x)$ SONO $\omega_d^{\,t}$ CON $(t,d)=1$, COME POSSIAMO ESPRIMERLE IN FUNZIONE DI ω_n?

$\omega_n^{\,t\cdot\frac{n}{d}}$ CON $(t,d)=1$

CON d FISSATO, CHI SONO LE

$$\omega_n^{t\cdot\frac{n}{d}} \quad \text{CON} \quad (t,d)=1$$

$$\omega_n^{K} \to \text{CARATTERIZZANDO} \quad = t\cdot\frac{n}{d}$$

BUONA DEF.

$$t \to t+d$$

$$\omega_n^{K} \to \omega_n^{K+n}$$

$$\left(t\cdot\frac{n}{d},\ n\right)=\frac{n}{d}$$

$$\to \frac{n}{d} \mid t\cdot\frac{n}{d} \qquad \frac{n}{d} \mid n$$

$$\Leftarrow (t,d)=1 \quad \exists\, a,b \text{ t.c.}$$

$$at-bd=1$$

$$a\cdot t\cdot\frac{n}{d}-bd\cdot\frac{n}{d}=\frac{n}{d}$$

$$a\cdot\left(t\cdot\frac{n}{d}\right)-b\cdot n=\frac{n}{d}$$

SONO TUTTI?

$$\text{SE } (K,n)=\frac{n}{d} \to K=J\cdot\frac{n}{d}$$

$(j, d) \overset{?}{=} 1$

$$\left(\frac{k}{(n/d)}, \frac{n}{(n/d)}\right) =$$

PROP.

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1 = (j, d) = 1$$

ALTRO MODO: COMBINAZIONI LINEARI

SE $(k, n) = \frac{n}{d} \rightarrow k$ È DELLA FORMA $j \cdot \frac{n}{d}$ CON $(j, d) = 1$

QUINDI LE $\omega_n^k = \omega_n^{j \cdot \frac{n}{d}}$ CON $(j, d) = 1$

SONO ESATTAMENTE QUELLE CON $(k, n) = \frac{n}{d}$

$x^n - 1$ → NON HA RADICI DOPPIE PERCHÉ NE CONOSCIAMO GIÀ n DISTINTE

$\rightarrow$ TUTTE QUELLE DEL TIPO ω_n^s

$\Phi_d(x)$, $d \mid n$, $d < n$ → NON HA RADICE PER IPOTESI INDUTTIVE

$\rightarrow$ TUTTE QUELLE DEL TIPO ω_n^s CON $(s, n) = \frac{n}{d}$

CI SONO 2 MODI DI AVERE RADICI DOPPIE:

① $\Phi_d(x)$ HA RADICI DOPPIE (MA NON È VERO PER Hp. INDUTTIVA: ABBIAMO ESATTAMENTE ω_d^k CON $(k,d)=1$) [OPPURE FAI IL CONTO]

② $\Phi_d(x)$ E $\Phi_{\tilde{d}}(x)$ HANNO UNA RADICE IN COMUNE CON $d \neq \tilde{d}$

ω_n^k CON $(k,n)=\frac{n}{d}$

ω_n^J CON $(J,n)=\frac{n}{\tilde{d}}$

SI VEDE GEOMETRICAMENTE, MA SE $\omega_n^J=\omega_n^k$ ALLORA $(k,n)=(J,n)$.

$$\Phi_n(x)=\frac{x^n-1}{\prod_{\substack{d\mid n\\ d<n}}\Phi_d(x)}$$

È MONICO E A COEFFICIENTI INTERI

NON HA RADICI DOPPIE E LE SUE RADICI SONO RADICI DI x^n-1

POLINOMIO MONICO A COEFFICIENTI INTERI

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d \mid n \\ d < n}} \Phi_d(x)} =$$

$$\Phi_n(x) = \frac{\prod_{i=0}^{n-1} (x - \omega_n^i)}{\prod_{\substack{d \mid n \\ d < n}} \left(\prod_{(k,n) = \frac{n}{d}} (x - \omega_n^k) \right)}$$

$\to \Phi_d(x)$

VISTO CHE $\frac{n}{d}$ VARIA TRA I DIVISORI DI n DIVERSI DA 1 E (k,n) PUÒ ASSUMERE SOLO VALORI CHE DIVIDONO n

$$\prod_{(k,n) \neq 1} (x - \omega_n^k) \longrightarrow \frac{\prod_{(k,n) \text{ QUALSIASI}} (x - \omega_n^k)}{\prod_{(k,n) \neq 1} (x - \omega_n^k)}$$

$$\Phi_n(x) = \prod_{(k,n) = 1} (x - \omega_n^k)$$

$\square$

Teorema OGNI CAMPO FINITO AMMETTE UN GENERATORE.

RICORDIAMO CHE:

POSTO $n = |\mathbb{K}| - 1$

$$x^n - 1 = \prod_{z \neq 0} (x - z)$$

$$\parallel$$

$$\prod_{d|n} \Phi_d(x)$$

$\Phi_d(x)$ È A COEFFICIENTI INTERI

E $\mathbb{Z}$ È MAPPABILE IN OGNI CAMPO:

PERCHÉ $1 \in \mathbb{K}$ E

OGNI n SI PUÒ MAPPARE IN

$$\underbrace{1 + 1 + \ldots + 1}_{n \text{ VOLTE}}$$

È CHIARO COME UN POLINOMIO A COEFFICIENTI INTERI VADA VISTO IN $\mathbb{Z}_p$.

CONTIAMO QUANTI SONO GLI ELEMENTI DI ORDINE d.

d DIVIDE n

QUINDI:

ELEMENTI DI ORDINE $1 \to 1 \quad 1 \quad (x-1)$

ELEMENTI DI ORDINE $2 \to 1 \quad -1 \quad (x+1)$

ELEMENTI DI ORDINE $3 \to 2 \quad \omega, \omega^2 \quad (x^2+x+1)$

RADICI DI x^3-1 CHE NON SONO RADICI DI $x-1$

(GLI ELEMENTI DI ORDINE 3 DI $\mathbb{Z}_5$ QUANTI SONO?) ZERO! $3 \nmid 4$

L'ORDINE È SEMPRE DIVISORE DI $n = |K| - 1$.

GLI ELEMENTI DI ORDINE 1 SONO LE RADICI DI $x-1$.

SE m DIVIDE n, GLI ELEMENTI DI ORDINE d T.C. $d \mid m$ SONO LE RADICI DI: (TUTTI GLI ELEMENTI IL CUI ORDINE DIVIDE m)

$x^m - 1$ (LE CUI RADICI SONO ESATTAMENTE QUELLE CON ORDINE DIVISORE DI m)

$\rightarrow$ $x^m - 1 \mid \underline{x^n - 1}$ $\hookrightarrow$ n RADICI DISTINTE

ANCHE $x^m - 1$ HA m RADICI DISTINTE
(PERCHÉ $x-z$ È IRRIDUCIBILE)

$\leftarrow$ SE $\operatorname{ord}_{\mathbb{K}}(z) \mid m \rightarrow z^m = 1$

E SONO PROPRIO m!

COSA ABBIAMO:

$$\prod_{ord_{\mathbb{K}}(z) \mid m} (x - z) = x^m - 1 \qquad \forall\, m \mid n$$

CRUCIALE, SENNÒ $X^m - 1$ NON SI SCOMPORREBBE COME $\prod (x - z)$

PONIAMO $$p_d(x) = \prod_{ord_{\mathbb{K}}(z) = d} (x - z)$$

$$\prod_{d \mid m} p_d(x) = x^m - 1 \qquad \forall\, m \mid n$$

QUINDI $p_d(x) = \Phi_d(x)$ VISTO SU $\mathbb{K}$

$\Phi_d(x)$ HA LE RADICI CHE SONO ESATTAMENTE QUELLE CHE HANNO ORDINE d E SONO $\deg(\Phi_d)$ $(= \varphi(d))$

$(\Phi_d(x) \mid x^n - 1)$ n RADICI DISTINTE

Φ_d HA GRADO $\varphi(d)$ PERCHÉ LE SUE RADICI (IN $\mathbb{C}$) SONO:

$$\omega_d^{\,k} \quad \text{CON} \quad (k,d)=1$$

$\longrightarrow$ SONO $\varphi(d)$

IN $\mathbb{C}$ ABBIAMO VISTO IL GRADO DI Φ_d

IN $\mathbb{K}$ Φ_d PASSA PERCHÉ A COEFFICIENTI INTERI E LE RELAZIONI SULLE RADICI (TOTALE DECOMPONIBILITÀ) DERIVANO DALLA RELAZIONE

$$\Phi_d(x) \mid x^n-1 = \prod_{z\neq 0} (x-z)$$

VALE COMUNQUE $\prod_{d\mid n} \Phi_d(x) = x^n-1$ PERCHÉ VALE SU $\mathbb{Z}[x]$

I.E.: MOD 37

$$(x^2-36)(x^2+1)$$

$$x^4-35x^2-36$$

$$(x^2+1)^2 \quad (37)$$

$$(37)$$

IN OGNI CAMPO $\underbrace{(1+1+\dots+1)}_{n \text{ VOLTE}}\underbrace{(1+1+\dots+1)}_{m \text{ VOLTE}} = \underbrace{1+1+\dots+1}_{m\cdot n}$ VOLTE.

TORNANDO A PRIMA, $\Phi_n(x)$ SU $\mathbb{K}$ HA $\varphi(n)$ RADICI.

MA $\Phi_n(x) = \prod_{ord_{\mathbb{K}}(z)=n} (x-z)$.

QUINDI CI SONO $\varphi(n)$ ELEMENTI DI $\mathbb{K}$ DI ORDINE n E OGNUNO DI LORO È UN GENERATORE.

LEMMA SIA $\mathbb{K}$ UN CAMPO FINITO E SIA $n = |\mathbb{K}| - 1$, $s > 0$

ALLORA $\displaystyle\sum_{z \neq 0} z^s = 0 \iff n \nmid s$

PRENDIAMO UN GENERATORE g.

$$\sum_{z \neq 0} z^s = \sum_{i=0}^{n-1} (g^i)^s = \sum_{i=0}^{n-1} (g^s)^i \overset{g^s \neq 1}{=}$$

$$= \frac{g^{sn} - 1}{g^s - 1}$$

CASO 1: $g^s = 1 \iff n \mid s$

g HA $\mathrm{ORD}_{\mathbb{K}} = n$

IN QUESTO CASO $\displaystyle\sum_{i=0}^{n-1} (g^s)^i = n.$

IL PROBLEMA È CHE n INTERO PUÒ ESSERE

$0 = \underbrace{1 + 1 + \ldots + 1}_{n \text{ VOLTE}}$ NEL CAMPO

(INTERROGATEVI SULLA QUESTIONE)

COMUNQUE FA SEMPRE -1

CASO 2: $g^5 \neq 1$

$$\frac{g^{5n}-1}{g^5-1} = \frac{1-1}{g^5-1} = 0$$

PER I VOLENTEROSI, PER DIMOSTRARE STA COSA SI PUÒ DIMOSTRARE:

- $\exists\, p$ PRIMO T.C. $\overbrace{1+1+\ldots+1}^{p \text{ VOLTE}} = 0 \ (\mathbb{K})$;
- $p \mid |\mathbb{K}|$ PERCHÉ ESISTONO DELLE CLASSI DI PARTIZIONE DI $\mathbb{K}$ IN p ELEMENTI

(TROVATELE)

RESIDUI QUADRATICI

SU $\mathbb{Z}_p$.

INDICHIAMO CON
$$\left(\frac{a}{p}\right) \begin{cases} 0 & \text{SE } a=0 \\ 1 & \text{SE } \exists\, t \not\equiv 0\ (p) \text{ T.C. } t^2 \equiv a\ (p) \\ -1 & \text{ALTRIMENTI} \end{cases}$$

a È R.Q. $\Leftrightarrow \left(\frac{a}{p}\right) = 1$ o 0

CRITERIO DI EULERO:

p DISPARI

$$a^{\frac{p-1}{2}} \begin{cases} 1 & \text{SE } \left(\frac{a}{p}\right)=1 \\ 0 & \text{SE } \left(\frac{a}{p}\right)=0 \\ -1 & \text{SE } \left(\frac{a}{p}\right)=-1 \end{cases}$$

CASO $a=0$:

$$\left(\frac{a}{p}\right)=0 \Leftrightarrow a^{\frac{p-1}{2}} \equiv 0\ (p)$$

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

① GENERATORI (CONTO LESTISSIMO)

② POLINOMI:

$X^{p-1} - 1$ HA $p-1$ RADICI DISTINTE MODULO p

$$\underbrace{\left(X^{\frac{p-1}{2}} - 1\right)}_{\frac{p-1}{2} \text{ RADICI DIST. MOD } p} \underbrace{\left(X^{\frac{p-1}{2}} + 1\right)}_{\frac{p-1}{2} \text{ RADICI DIST. MOD } p}$$

OGNI RESIDUO O È RADICE O DEL L'ALTRO

SE a È RESIDUO QUADRATICO:

$$a^{\frac{p-1}{2}} \equiv t^{2 \cdot \frac{p-1}{2}} \equiv t^{p-1} \equiv 1 \ (p)$$

$\longrightarrow$ TUTTI I R.Q. STANNO TRA LE RADICI DI $X^{\frac{p-1}{2}} - 1$

SE I R.Q. FOSSERO $\frac{p-1}{2}$ E TUTTI CONTENUTI IN $X^{\frac{p-1}{2}} - 1$, ALLORA LE RADICI DI $X^{\frac{p-1}{2}} - 1$ SAREBBERO ESATTAMENTE I R.Q.

I R.Q. $\neq 0$ sono $\frac{p-1}{2}$.

Mappa: $\{1, \dots, p-1\} \to \{1, \dots, p-1\}$

$$x \ (p) \to x^2 \ (p)$$

Quando $x^2 \equiv y^2 \ (p)$

$$(x+y)(x-y) \equiv 0 \ (p) \begin{cases} \nearrow x \equiv y \ (p) \\ \searrow x \equiv -y \ (p) \end{cases}$$

Cioè: (I.E. 13)

1	2	3	4	5	6
↓	↓	↓	↓	↓	↓
1	4	−4	3	−1	−3
↑	↑	↑	↑	↑	↑
12	11	10	9	8	7

Quindi sono $\frac{p-1}{2}$: $x^2 \equiv y^2 (p) \Leftrightarrow x \equiv \pm y (p)$

(Anche perché quindi

$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ sono diversi)

LEMMA DI GAUSS

SE $a^{(p)}$ È UN INTERO MODULO p, CONSIDERIAMO

I NUMERI:

VISTI MODULO p

$a, 2a, \dots, \left(\frac{p-1}{2}\right)a$ (TUTTI TRA 1 E $p-1$)

E SIA $S = \left\{ i \;\middle|\; [ia]_p > \frac{p}{2} \right\}$

I.E.: $p=13$ $a=3$ $\left(\frac{3}{13}\right)=1$

3 6 9 12 $\underset{2}{\overset{15}{\downarrow}}$ 5

$S = \{3, 4\}$

Th. $\left(\frac{a}{p}\right) = (-1)^{|S|}$

a R.Q. $\Leftrightarrow$ $|S|$ PARI

CONSIDERIAMO:

$$a,\ 2a,\ 3a,\ \dots,\ \left(\frac{p-1}{2}\right)a$$

$$\forall x \in \mathbb{Z}_p \qquad \exists!\ i \leq \frac{p-1}{2} \text{ t.c.}$$

$$ia \equiv \pm x\ (p)$$

$a, 2a, \dots, (p-1)a$ È UNA PERMUTAZIONE DI $\mathbb{Z}_p \setminus \{0\}$

SE MI FERMO A $\left(\frac{p-1}{2}\right)$:

TRA a E $(p-1)a$ NE PRENDO UNO;

TRA $2a$ E $(p-2)a$ NE PRENDO UNO;

...

HO UNA PERMUTAZIONE DA CUI TOLGO UN ELEMENTO PER OGNI COPPIA DI OPPOSTI.

$$\prod_{i=1}^{\frac{p-1}{2}} (ai) \equiv \prod_{\substack{i=1 \\ (ai)_p < \frac{p}{2}}}^{\frac{p-1}{2}} (ai) \cdot \prod_{\substack{i=1 \\ (ai)_p > \frac{p}{2}}}^{\frac{p-1}{2}} (ai) \equiv$$

$$\equiv \prod_{\substack{i=1 \\ (ai)_p < \frac{p}{2}}}^{\frac{p-1}{2}} (ai) \cdot \prod_{\substack{i=1 \\ (ai)_p > \frac{p}{2}}}^{\frac{p-1}{2}} (p-ai)\cdot(-1) \equiv$$

$|S|$ VOLTE

S È L'INSIEME DEGLI i CON QUESTA PROPRIETÀ

$$\equiv (-1)^{|S|} \cdot \prod_{\substack{i=1 \\ (ai)_p < \frac{p}{2}}}^{\frac{p-1}{2}} (ai) \cdot \prod_{\substack{i=1 \\ (ai)_p > \frac{p}{2}}}^{\frac{p-1}{2}} (p-ai)$$

$< \frac{p}{2}$ $\quad$ $< \frac{p}{2}$

IN TOTALE I TERMINI SONO $\frac{p-1}{2}$: GLI DA 1 A $\frac{p-1}{2}$ O STANNO A SX O DX

GLI ELEMENTI SONO TUTTI DIVERSI:

$ai \equiv \pm x_i \,(p)$ MA GLI x_i SONO TUTTI DIVERSI

ABBIAMO VISTO PRIMA CHE

$\pm a, \pm 2a, \dots, \pm\left(\frac{p-1}{2}\right) a$

ERANO TUTTI DIVERSI, PERCIÒ

ANCHE GLI a_i E I $(p-a_i)$ SONO

TUTTI DIVERSI

ABBIAMO $\frac{p-1}{2}$ TERMINI $< \frac{p}{2}$ DIVERSI TRA

LORO: IL PRODOTTO FA $\left(\frac{p-1}{2}\right)!$

$$\prod_{i=1}^{\frac{p-1}{2}} (a_i) \equiv (-1)^{|S|} \cdot \cancel{\left(\frac{p-1}{2}\right)!} \quad (p)$$

$$|||$$

$$a^{\frac{p-1}{2}} \cdot \prod_{i=1}^{\frac{p-1}{2}} (i) \equiv a^{\frac{p-1}{2}} \cdot \cancel{\left(\frac{p-1}{2}\right)!}$$

$$a^{\frac{p-1}{2}} \equiv (-1)^{|S|} \quad (p) \to \left(\frac{a}{p}\right) = (-1)^{|S|}$$

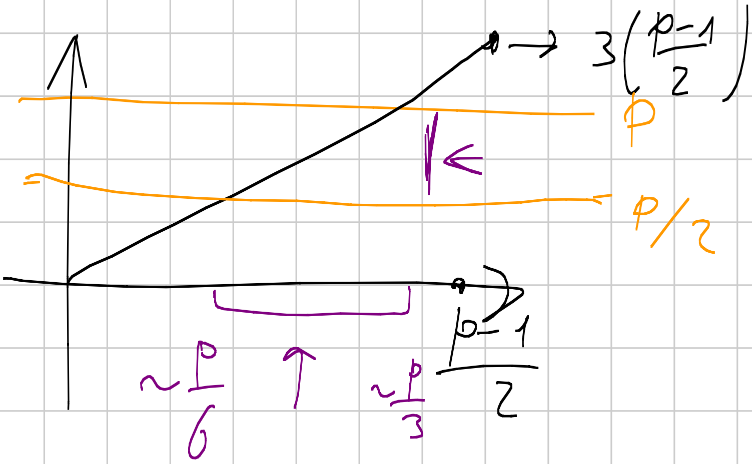
QUANDO $\left(\frac{3}{p}\right) = 1$?

((COMUNQUE A CASA PROVATE CON $\left(\frac{-3}{p}\right)$, VIENE UGUALE)
(COME METODO))

GUARDIAMO:

$$3,\ 6,\ \dots,\ 3\left(\frac{p-1}{2}\right)$$

QUALI SARANNO (mod p) IN $\left(\frac{p}{2}, p\right)$?



QUANDO $\frac{p}{2} < 3i < p$ E IN REALTÀ BASTA,
PERCHÉ $\left(\frac{p-1}{2}\right) \cdot 3 < p + \frac{p}{2}$

PERCIÒ ABBIAMO: $\frac{p}{6} < i < \frac{p}{3}$ QUINDI

$$|S| = \left\lfloor \frac{p}{3} \right\rfloor - \left\lfloor \frac{p}{6} \right\rfloor \quad \forall p > 3$$

QUAL È IL MINIMO R T.C.:

$$\left\lfloor \frac{p+R}{3} \right\rfloor - \left\lfloor \frac{p+R}{6} \right\rfloor \equiv \left\lfloor \frac{p}{3} \right\rfloor - \left\lfloor \frac{p}{6} \right\rfloor (2)$$

12! (FORSE)

$$\left\lfloor \frac{p+12}{3} \right\rfloor \equiv \left\lfloor \frac{p}{3} \right\rfloor (2)$$

$$\left\lfloor \frac{p}{3} \right\rfloor + 4 \qquad \left\lfloor \frac{p+12}{6} \right\rfloor \equiv \left\lfloor \frac{p}{6} \right\rfloor (2)$$

$$\lfloor x+1 \rfloor = \lfloor x \rfloor + 1 \qquad \left\lfloor \frac{p}{6} \right\rfloor + 2$$

$\varphi(12)$

$\underline{\hspace{1em}}$

4

PROVIAMO $p = 12K + J$ $\quad J \to 1, 5, 7, 11$

$$|S| = \left\lfloor \frac{12K+J}{3} \right\rfloor - \left\lfloor \frac{12K+J}{6} \right\rfloor =$$

$$= \left\lfloor \frac{J}{3} \right\rfloor - \left\lfloor \frac{J}{6} \right\rfloor \quad (2)$$

$p \equiv 1 \ (12) \qquad 0 - 0 \quad \to \quad \left(\frac{3}{p}\right) = 1$

$p \equiv 5 \ (12) \qquad 1 - 0 \quad \to \quad \left(\frac{3}{p}\right) = -1$

$p \equiv 7 \ (12) \qquad 2 - 1 \quad \to \quad \left(\frac{3}{p}\right) = -1$

$p \equiv 11 \ (12) \qquad 3 - 1 \quad \to \quad \left(\frac{3}{p}\right) = 1$

Es. 1 $\forall p > 1000 \quad \forall r \in \mathbb{Z}$

$\exists \, x, y$ t.c. $x^2 \equiv y^3 + r \ (p)$

Es. 2 $\forall a > 1$

$\exists \infty \ q$ t.c. $v_q(a^{q-1} - 1)$ È DISPARI

---

(1)

$(y^3 + r)^{\frac{p-1}{2}}$ VORREMMO FOSSE 1 o 0

PER ASSURDO: $(y^3 + r)^{\frac{p-1}{2}} \equiv -1 \ (p) \quad \forall y \in \mathbb{Z}_p$

$$\sum_{y=0}^{p-1} \left(y^3+k\right)^{\frac{p-1}{2}} \equiv 0 \ (p)$$

IDEA STANDARD SE UNO L'HA VISTA

BELLA PERCHÉ SAPPIAMO QUANTO FA $\sum y^i$

IN GENERALE SOMMARE SU TUTTE LE CLASSI DI RESTO MOD p È UNA BUONA IDEA

$$\sum_{y=0}^{p-1} \left(y^3+k\right)^{\frac{p-1}{2}} = \sum_{y=0}^{p-1}\left(\sum_{i=0}^{\frac{p-1}{2}} y^{3i}\cdot k^{\left(\frac{p-1}{2}-i\right)}\cdot\binom{\frac{p-1}{2}}{i}\right) =$$

$$= \sum_{i=0}^{\frac{p-1}{2}}\left(\sum_{y=0}^{p-1} y^{3i}\cdot k^{\left(\frac{p-1}{2}-i\right)}\cdot\binom{\frac{p-1}{2}}{i}\right) =$$

$$= \sum_{i=0}^{\frac{p-1}{2}} k^{\left(\frac{p-1}{2}-i\right)}\cdot\binom{\frac{p-1}{2}}{i}\left(\sum_{y=0}^{p-1} y^{\boxed{3i}}\right)$$

PROBLEMA: $y=0$, $i=0$

$y^i = ?$

SE $y=0$ NELLO SVILUPPO $0^0=1$

(p)

$i=0 \to 0$

SE $p-1 \nmid 3i \to 0$

i VARIA TRA 0 E $\frac{p-1}{2}$

SE NON È MULTIPLO DI $p-1$, VIENE 0

$p-1 \mid 3i, \quad 0 \le i \le \frac{p-1}{2}$

$i = 0$

$i = \frac{p-1}{3}$

QUINDI RESTA SOLO $i = \frac{p-1}{3}$

$\Rightarrow$ i DIVENTA SOLO $\frac{p-1}{3}$

SE $p \equiv 2\ (3) \longrightarrow 0$ (i NON C'È)

SE $p \equiv 1\ (3)$

$$V^{\left(\frac{p-1}{6}\right)} \cdot \cancel{\begin{pmatrix} \frac{p-1}{2} \\ \frac{p-1}{3} \end{pmatrix}}^{\equiv 0\ (p)} \cdot \cancel{(-1)}^{\equiv 0\ (p)} \quad (p)$$

$\equiv$

$0 \quad (p)$

$V \equiv 0\ (p)$ ✓

$y^2 \equiv x^3 + 0\ (p)$

$(1, 1)$

SE $p \equiv 2 \ (3)$?

$$y^2 \equiv x^3 + y \quad (p)$$

$$y^2 - y \equiv x^3 \quad (p)$$

ASSUME TUTTI I VALORI

SE $p \equiv 2(3)$, QUALI SONO I RESIDUI CUBICI?

SONO TUTTI, PERCHÉ IL NUMERO DI RESIDUI d-ESIMI È $\dfrac{p-1}{(p-1,d)}$

[DIMOSTRATELA]

$$x \equiv x^{2p-1} \ (p) \equiv \left(x^{\frac{2p-1}{3}}\right)^3 \quad (p)$$

SE $(d, p-1) = 1$

$$x \equiv x^{(p-1)k+1} \equiv \left(x^{\frac{(p-1)k+1}{d}}\right)^d \quad (p)$$

E SCELGO $(-)k$ INVERSO DI $(p-1)$ MODULO d