PreIMO 2016

Stampato integrale delle sessioni

Autori vari

Indice

PreIMO '16 - ALGEBRA (mattino)

Titolo nota 26/05/2016

[1] $p(x), q(x) \in \mathbb{C}[x]$ di grado 2016

$$p(x) + (-1)^x q(x) = 2^x \qquad x = 1, 2, \dots, 4034$$

Coefficiente di x^{2016} in $q(x)$

$d(x) = p(x) - q(x) = 2^x \qquad x = 1, 3, 5, \dots, 4033$

$s(x) = p(x) + q(x) = 2^x \qquad x = 2, 4, \dots, 4034$

Grado + 1 = # punti $\Rightarrow$ univocamente determinati

Metodo di interpolazione "tipo" polinomi di Newton

↳ funziona bene se conosco i valori per $x = 1, 2, 3, \dots, n+1$

(interi consecutivi)

$r(x) := s(2x) = 4^x \qquad x = 1, 2, \dots, 2017$

$d(x) = \frac{1}{2} r\left(\frac{x+1}{2}\right) \qquad s(x) = r\left(\frac{x}{2}\right)$

$$\boxed{q(x) = \frac{1}{2} s(x) - \frac{1}{2} d(x) = \frac{1}{2} r\left(\frac{x}{2}\right) - \frac{1}{4} r\left(\frac{x+1}{2}\right)}$$

$r(x) = \sum_i r_i x^i \qquad q(x) = \sum_i q_i x^i$

$q_{2016} = \frac{1}{2}\left(\frac{1}{2}\right)^{2016} r_{2016} - \frac{1}{4}\left(\frac{1}{2}\right)^{2016} r_{2016} = \frac{1}{4} 2^{-2016} r_{2016}$

Dato $f(x)$ polinomio sia $\Delta f(x) = f(x) - f(x-1)$

$f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots \longrightarrow \boxed{\Delta f(x) = n f_n x^{n-1} + \dots}$ (check!)

$\Delta^n f(x) = n! f_n$

$\Delta^{2016} r(x) \equiv 2016! \, r_{2016}$

x	1	2	3	$\ldots n$	2017
$r(x)$	4	16	64	$\ldots 4^n$	4^{2017}
$\Delta r(x)$	–	12	48	$\ldots 3 4^{n-1}$	$3\cdot 4^{2016}$
$\Delta^2 r(x)$	–	–	36	$9\cdot 4^{n-2}$	$3^2 4^{2015}$
$\ldots$					
$\Delta^{2016} r(x)$	–	–	–		$3^{2016}\cdot 4^1$

$$q_{2016} = \ldots = \frac{3^{2016}}{2^{2016}\cdot 2016!}$$

☆ Polinomi di Newton

$x_i = 1, 2, \ldots, n$

$p_1(x) = (x-n) \qquad p_0(x) = 1$

$p_2(x) = (x-n)(x-n+1)$

$\ldots$

$p_k(x) = (x-n)\cdot(x-n+1)\cdot\ldots\cdot(x-n+k-1)$

$p_{n-1}(x) = (x-n)\cdot\ldots\cdot(x-2)$

$$p_{n-1}(x_i) = \begin{cases} \pm n! & x_i = 1 \\ 0 & x_i \neq 1 \end{cases}$$

$\exists\, a_k$ facili da trovare : $\sum_{k=0}^{n-1} a_k p_k(x_i) = y_i$

$\Delta p_k(x) = c \cdot p_{k-1}(x)$

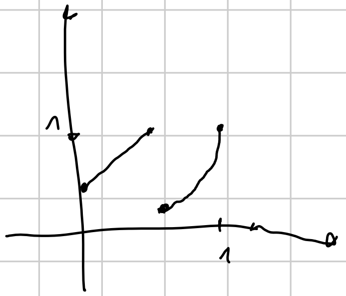
$$r(x) = 4^x = (1+3)^x = \sum_{k=0}^{x} \binom{x}{k} 1^{x-k} 3^k \qquad \binom{x}{k} = \frac{1}{k!} x(x-1)(x-2)\cdot\ldots\cdot(x-k+1)$$

$\boxed{2}$

$$f:(0,1)\longrightarrow(0,1)$$

$$f(x)=\begin{cases} x+\frac{1}{2} & \text{se } x<\frac{1}{2}\\ x^2 & \text{se } x\geq\frac{1}{2}\end{cases}$$

$a_0\in(0,1)$ $\quad a_n=f(a_{n-1})$



$a_0\neq b_0 \quad a_0>b_0$

a_n-b_n

$$a_{n+1}-b_{n+1}=(a_n-b_n)\underbrace{(a_n+b_n)}_{\geq 1}$$

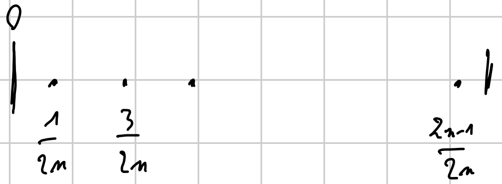
$\geq\frac{1}{2}$	$<\frac{1}{2}$		
a_n	$a_{n+1}=a_n^2$	$a_{n+2}=a_{n+1}+\frac{1}{2}$	$a_{n+3}=a_{n+2}^2$
b_n	$b_{n+1}=b_n^2$	$b_{n+2}=b_{n+1}+\frac{1}{2}$	$b_{n+3}=b_{n+2}^2$

$\boxed{3}$ $f:\mathbb{R}_+\to\mathbb{R}_+$ $\quad a,b,c$ distinti $\quad a,b,c$ lati $\Delta \iff f(a),f(b),f(c)$ lati di Δ

$a<b+c \iff f(a)<f(b)+f(c)$

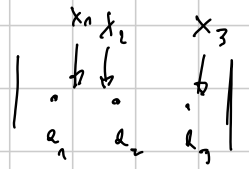
$\boxed{4}$ $\quad f:[0,1]\longrightarrow\mathbb{R}$ crescente

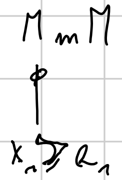
$$\max\sum_{i=1}^{n} f\left(\left|x_i-\frac{2i-1}{2n}\right|\right) \qquad 0\leq x_1\leq\cdots\leq x_n\leq 1$$

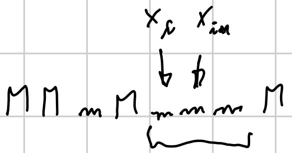


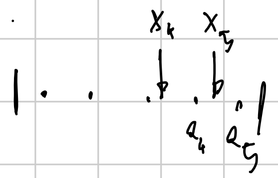
$\frac{2i-1}{2n}=a_i$

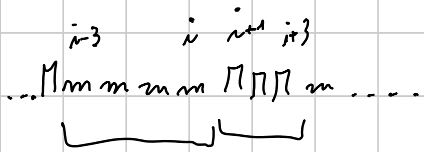
dati $x_1 \dots x_n$ m M

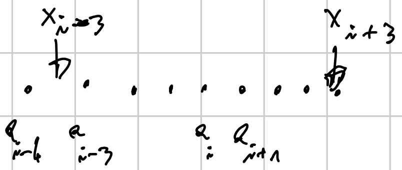


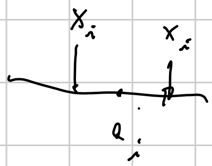


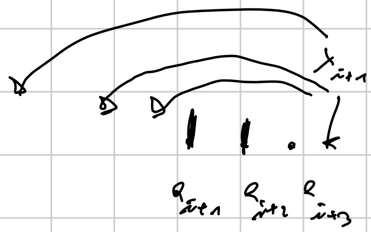












$a_{i-4} \leq x_{i-3} \leq a_{i-3}$ $x_{i+1} = x_{i+3} \leq a_{i+4}$

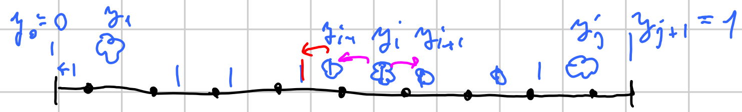
$$\Downarrow$$

$$2a_{i+1} - x_{i+1} \geq 2a_{i+1} - a_{i+4} = a_{i-2}$$

Alla fine mi ritrovo con tutti gli x_i uguali

Idea: trovo una sequenza di mosse che manda qualunque n-upla in quella ottima

- aumentando sempre la somma
- numero di passi limitato



Considero che in un passo intermedio i punti siano raggruppati in $j \leq n$ punti $y_1, y_2, \dots, y_j$ con molteplicità $k_1, k_2, \dots, k_j$

gruppo i ha spazio $y_{i+1} - y_{i-1}$ e k_i punti

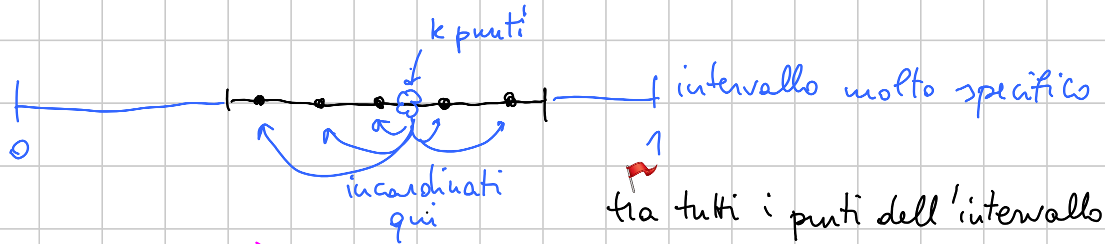
allora almeno uno ha spazio $\geq$ di $\frac{k_i}{n}$

RPA $\quad y_{i+1} - y_{i-1} < \frac{k_i}{n} \quad \forall i \Rightarrow \sum_{i=1}^{j} (y_{i+1} - y_{i-1}) < \frac{1}{n} \sum k_i = 1$

$$\sum_{2}^{j+1} y_i - \sum_{0}^{j-1} y_i = 1 + y_j - y_1 - 0 \geq 1 \text{ assurdo}$$

$y_j \geq y_1$

Considero un intervallo largo almeno $\frac{k}{n}$ con k punti raggruppati



tra tutti i punti dell'intervallo il max è se il gruppo è ad un estremo

PREIMO 2016 - ALGEBRA - POMERIGGIO

Titolo nota 26/05/2016

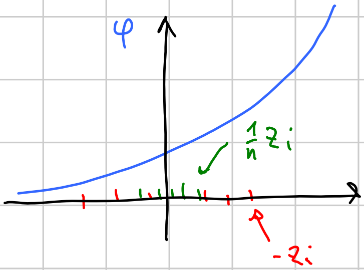
$\boxed{5}$ $x_1, x_2, \dots, x_{n+1} > 0$ $\quad \prod x_i = 1$ $\quad \sum_i z_i = 0$

$$\sum_i \sqrt[x_i]{n} \overset{?}{\geq} \sum_i n^{\sqrt[n]{x_i}}$$

$$\sum_i n^{x_i^{-1}} \overset{?}{\geq} \sum_i n^{x_i^{1/n}} \qquad \varphi(z) = n^{e^z}$$

$$\sum_i \varphi(-\log x_i) \overset{?}{\geq} \sum_i \varphi\left(\tfrac{1}{n}\log x_i\right) \qquad z_i := \log x_i$$

$$\sum_i \varphi(-z_i) \overset{?}{\geq} \sum_i \varphi\left(\tfrac{1}{n} z_i\right)$$



Disuguaglianza di Karamata

$a_i = -z_i \quad i = 1, \dots, n+1 \quad a_1 < a_2 < \dots < a_{n+1}$

$b_i = \frac{1}{n} z_{n-i+2} \quad i = 1, \dots, n+1 \quad b_1 < b_2 < \dots < b_{n+1}$

φ convessa

$\sum a_i = \sum b_i$ stesso baricentro

b maggiorizza a

basta $\longrightarrow$ $b_1 + b_2 + \dots + b_k \geq a_1 + a_2 + \dots + a_k \quad k = 1, \dots, n+1$

ts: $\sum \varphi(b_i) \leq \sum \varphi(a_i)$

$z_1 \geq z_i \ \forall i$

$k = 1 \quad b_1 \overset{?}{\geq} a_1 \quad \frac{1}{n} z_{n+1} \overset{?}{\geq} -z_1 \quad z_{n+1} + n z_1 \overset{?}{\geq} 0$

$\geq z_{n+1} + z_n + \dots + z_2 + z_1 = 0$ ✓

k generico

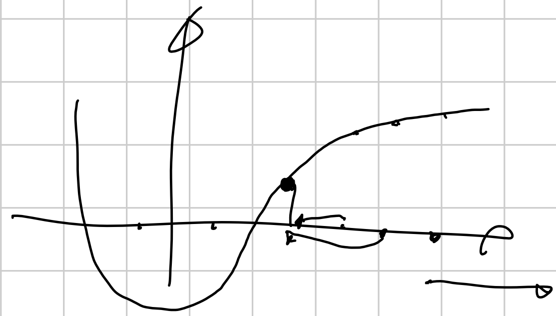
Oppure: AM-GM $\displaystyle\sum_{i \neq j} \sqrt[x_i]{n} \geq n \sqrt[n]{n^{\sum_{i\neq j} \frac{1}{x_i}}} \geq n \sqrt[n]{n^{n\sqrt[n]{x_j}}} = n \cdot n^{\sqrt[n]{x_j}}$

Sommo su j e ho finito

$t_i \in \mathbb{R} \qquad \sum t_i = 0 \qquad (t_i = \log x_i)$

$$\sum e^{\log n \, e^{-t_i}} - e^{\log n \, e^{\frac{t_i}{n}}} \overset{?}{\geq} 0$$

$$\psi(t) = e^{(\log n) e^{-t}} - e^{(\log n) e^{\frac{t}{n}}}$$



$x_1 = x_2 = \dots = x_n = x \qquad x_{n+1} = \frac{1}{x^n}$

$\boxed{6}$ n. Dire se $\exists a_0, \dots, a_n : \forall e_0, \dots, e_n \in \{-1, 1\}$

il poly $\sum a_i e_i x^i$ ha n radici reali distinte.

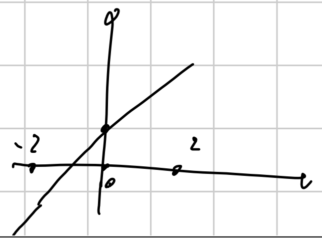
Fisso $\varepsilon = \frac{1}{100}$

$a_0 = 1 \qquad r_0 = 0 \qquad$ Il segno di $p(r_0)$ è determinato da e_0.

$a_1 = 1 \qquad r_1 = 2 \qquad$ Il segno di $p(\pm r_1)$ è determinato da e_1.

Voglio a_2 t.c. $a_2 r_1^2 \ll a_1 r_1$

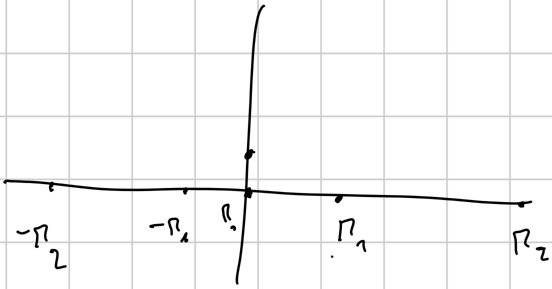
chiedo $a_2 < \frac{\varepsilon}{n} a_1 \frac{1}{r_1}$



r_2 t.c. $a_2 r_2^2 \gg a_1 r_2$
a_0

$> \frac{n}{\varepsilon} a_1 r_2 \qquad > \frac{n}{\varepsilon} a_0$

Il segno di $p(\pm r_2)$ è determinato da e_2



$p(-r_1) \quad p(r_0) \quad p(r_1)$

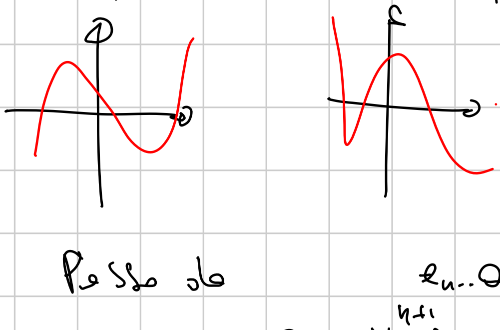
$-a_1 e_1 r_1 \quad a_0 e_0 \quad a_1 e_1 r_1$

$p(-r_2) \quad p(-r_1) \quad p(r_1) \quad p(r_2)$

$a_2 e_2 r_2^2 \quad -a_1 e_1 r_1 \quad a_1 e_1 r_1 \quad a_2 e_2 r_2^2$

PIANO: INDUZIONE

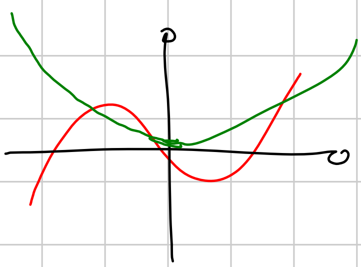
Suppongo ok per grado n,



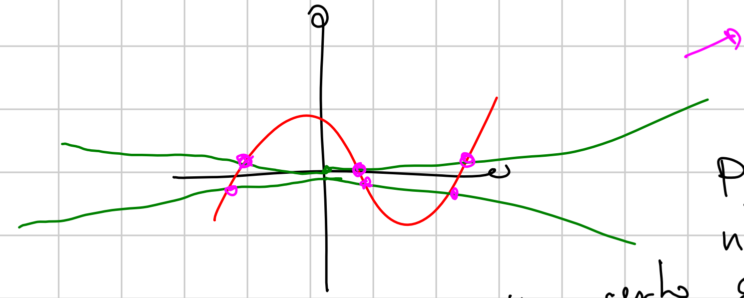
2^n polinomi

Passo da $e_n a_n X^n + e_{n-1} a_{n-1} X^{n-1} + \dots + e_0 a_0$

a $e_{n+1} a_{n+1} X^{n+1} +$ " " " "

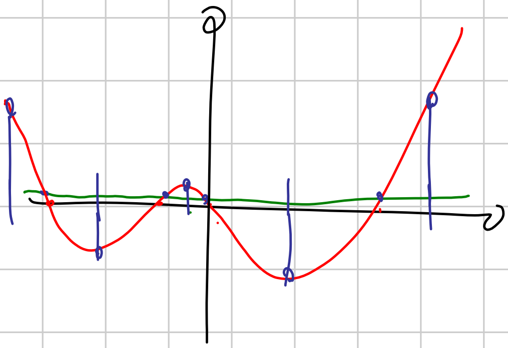


$- e_{n+1} a_{n+1} X^{n+1}$



Per ogni poli. di grado n che va bene, esiste un certo ε

Alternativamente: dato $p(x)$ di grado n che funziona, $\varepsilon x^{n+1}+p(x)$ e anche Faccio: $x\,p(x)+\varepsilon$



$\boxed{7}$ $f:\mathbb{R}_+\to\mathbb{R}$

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

$f\equiv 0 \quad f\equiv -2$

$$f(\underbrace{x}+\underbrace{y+z}_{y'})^2 = f(x)^2+2f(xy+xz)+f(y+z)^2$$

$$= f(x)^2+f(y)^2+f(z)^2+2f(xy+xz)+2f(yz)$$

rimmetrizzo $\longrightarrow$ $= \;''\quad ''\quad '' + 2f(yz+yx)+2f(xz)$

$\forall x,y,z>0$ $f(\overset{c}{xy}+\overset{b}{xz})+f(\overset{a}{yz}) = f(\overset{a}{yz}+\overset{c}{xy})+f(\overset{b}{xz})$ senza quadrati!

$$\boxed{f(a+b)+f(c)=f(a)+f(b+c)\qquad \forall a,b,c>0}$$

dati $a,b,c>0$ $\left(a=yz \quad b=xz \quad c=xy\right)$ hope

$\sqrt{\dfrac{ab}{c}} =: z$ e cicliche definisco x,y,z

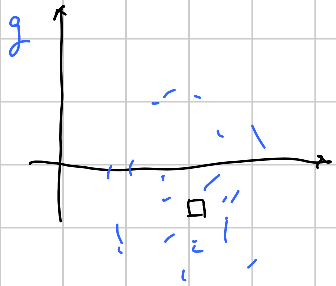
potrebbe essere una retta non per l'origine

$\forall x>0 \quad g(x) = f(a+x) - f(a)$ $\qquad a>0$ fissato per sempre

$g(x+y) = f(a+x+y) - f(a) \overset{?}{=} f(a+x) - f(a) + f(a+y) - f(a)$

$$\underbrace{f(a+y+x)}_{A} + \underbrace{f(a)}_{C} = \underbrace{f(a+x)}_{B} + \underbrace{f(a+y)}_{A}$$ ✓

Cerco una disuguaglianza



$\forall x,y>0 \qquad 2f(xy) \leq f(\underbrace{x+y}_{=s})^2$

$=s$ fissato maggiore di $10\sqrt{a}$

$(x',y') : x'+y' = s \quad x',y' > \sqrt{a}$

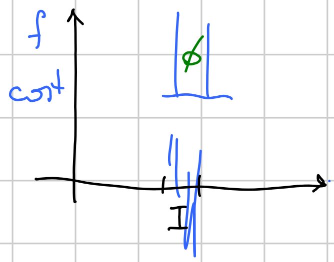
c'è un intervallo di valori di x' che soddisfano

→ " " " " " " $x'y' > a$ che soddisfano

$\exists I : \forall u \in I, \; u > a \quad f(u) \leq \text{cost}$

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

$g(u-a) \leq \text{cost}_1 \quad u \in I$



Allora $g(x) = \alpha x \implies f(x) = \alpha x + \beta$

Sostituisco: quattro soluzioni $f(x) = 0, -2, x, x-2$

$\boxed{8}$ $\qquad x_i \in \mathbb{R} \qquad \sum_1^n x_i = 0 \qquad \sum_1^n x_i^2 = 1$

$\forall A \subseteq T = \{1, 2, \dots, n\} \qquad S_A := \sum_{i \in A} x_i \qquad S_\emptyset = 0$

$\forall \lambda > 0 \quad \#\{A \subseteq T : S_A \geq \lambda\} \leq 2^{n-3} \lambda^{-2}$

$S_{\bar{A}} = -S_A$ $\qquad \#\{S_A \geq \lambda\} = \frac{1}{2}\#\{|S_A| \geq \lambda\} = \frac{1}{2}\#\underbrace{\{S_A^2 \geq \lambda^2\}}_{T_\lambda}$

$$\underset{\text{non negative}}{\sum_{A\subseteq T} S_A^2} \geq \sum_{A\subseteq T_\lambda} S_A^2 \geq \lambda^2 \# T_\lambda \qquad \# T_\lambda \leq \frac{1}{\lambda^2}\sum_{A\subseteq T} S_A^2$$

$$\sum_{A\subseteq T} S_A^2 = \sum_{A\subseteq T}\Big(\sum_{i\in A} x_i\Big)^2 = \sum_{A\subseteq T}\Big(\sum_{i\in A} x_i^2 + 2\sum_{\substack{i<j\\ i,j\in A}} x_i x_j\Big)$$

$$= \sum_{i=1}^{n} x_i^2 \underbrace{\sum_{A\ni i} 1}_{2^{n-1}} + 2\sum_{i<j} x_i x_j \underbrace{\sum_{A\ni i,j} 1}_{2^{n-2}} = 2^{n-1}\sum_i x_i^2 - 2^{n-2}\sum_i x_i^2 = 2^{n-2}$$

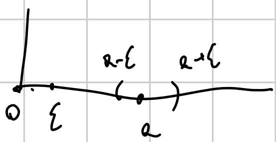
$$0 = \Big(\sum x_i\Big)^2 = \sum_i x_i^2 + 2\sum_{i<j} x_i x_j$$

Metto assieme tutto e chiudo

$\boxed{3}$ $f : (0,+\infty) \longrightarrow (0,+\infty)$

$\forall a, b, c$ distinti $\quad a, b, c$ lati di $\Delta \iff f(a)\, f(b)\, f(c)$ lati di Δ

STEP 1 Prendo a scelgo $\varepsilon < \frac{a}{2}$



$\forall b \in (a-\varepsilon, a+\varepsilon)$ ho $f(b) < f(a) + f(\varepsilon)$

STEP 2 Prendo a, ε come sopra

$\forall b \in (0, \varepsilon)$ $\quad a, b, a+\frac{b}{2}$ sono lati di Δ

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

STEP 3 $f \to 0$ per $x \to 0$

se per assurdo $f \not\to 0$, trovo $x_i \longrightarrow 0$
con $f(x_i) \longrightarrow \lambda \neq 0$

$f(x_i), f(x_j) \in \left(\lambda \left(1 - \frac{1}{10}\right), \lambda \left(1 + \frac{1}{10}\right) \right)$

$x_k < |x_i - x_j| \quad f(x_k) \in \left(\lambda \left(1 - \frac{1}{10}\right), \dots \right)$

ASSURDO perché x_i, x_j, x_k non Δ
$f(x_i)$ $f(x_j)$ $f(x_k)$ sì

STEP 4 Fisso a prendo degli $\varepsilon \ll a$
per $b \in (a - \varepsilon, a + \varepsilon)$

ε, a, b sono Δ $\Rightarrow$ $|\underbrace{f(a)}_{f(a)} - f(\varepsilon)| < f(b) < \underbrace{f(a)}_{f(a)} + f(\varepsilon)$

$\Rightarrow f$ continua

STEP 5 Supp. $a \neq b$ $f(a) = f(b)$
prendo ε tale che $\varepsilon < |a - b|$
e $f(\varepsilon) < f(a)$

ε, a, b non Δ ma $f(\varepsilon), f(a), f(b)$

$\Rightarrow f$ iniettiva

STEP 6 f crescente (segue da 4 e 5)

STEP 7

$a, b+\varepsilon, a+b$ Δ $\Rightarrow$ $f(a+b) < f(a) + f(b+\varepsilon)$

$f(b)$

$\searrow$ ttengo $f(a+b) \leq f(a) + f(b)$

$a, b-\varepsilon, a+b$ non Δ $\Rightarrow$ $f(a+b) \geq f(a) + f(b-\varepsilon)$

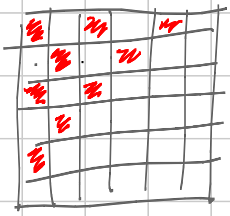
$\Rightarrow f(a+b) \geq f(a) + f(b)$

PreIMO 2016 - COMBINATORIA (mattino)

Titolo nota 24/05/2016

C1

un drago si nasconde in una tabella 2015×2015



1 passo: coloriamo a scacchiera

2 passo: colpiamo le bianche poi le rosse poi ancora le bianche

ora abbiamo finito di sparare perché il drago si sposta su una casella del colore diverso

al più servono $\left\lfloor \frac{2015^2}{2} 3 \right\rfloor$

3 passo: se considero

devo sparare almeno 3 volte

intanto devo colpirle entrambe

se sparo solo 2 volte non sono sicuro: se il drago stava sulla seconda potrebbe spostarsi sulla prima

4 passo: tassello la scacchiera con 2×1 lasciando un angolino

$\Rightarrow$ mi servono almeno

$3 \times$ ogni tessera 2×1 +

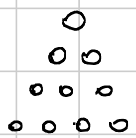
1 sull'angolino

C2 36 persone, nessuno stringe la mano a qualcuno con lo stesso numero di strette di mano. Quante strette di mano al max?

Quante persone possono stringere la mano a tutti? Solo 1

In generale, quanti posso stringere la mano a $36-k$ persone? Al massimo k. Infatti, se m è il numero di persone che fanno $36-k$ strette, allora questi possono stringere la mano solo a $36-m$ persone

Si ottiene che $m \leq k$

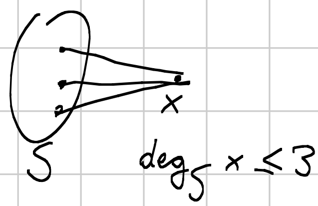


Se io dispongo le 36 persone a triangolo, e faccio in modo che ogni persona stringa la mano a quelli che non stanno sulla sua riga, allora ho vinto.

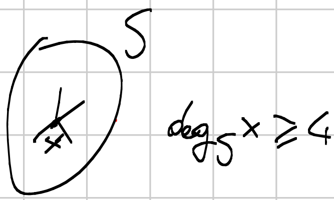
C3.

In un grafo G esiste sempre $S \subseteq V(G)$ t.c. non succedono né

A



B



Cosa faccio?

→ costruisco S aggiungendo un vertice alla volta... ... FALLISCO

→ cerco un algoritmo "sensato" che mi dica l'ordine in cui aggiungere i vertici... ... FALLISCO

Nuova idea! Voglio caratterizzare S come massimizzante una certa funzione f della configurazione.

CIOÈ voglio f che so far aumentare se sono in A o in B.

$S \subseteq V(G)$ sono finiti $\to \exists S$ che massimizza f; questo deve per forza soddisfare la tesi.

ingredienti candidati per f: $|S|$, $E(S)$ ← archi dentro S

mossa A $x \in A \setminus S$ $\deg_S x \leq 3$

x $A \setminus S \to S$

$\Delta |S| = +1$

$\Delta E(S) \leq 3$

mossa B $x \in S$ $\deg_S x \geq 4$

x $S \to A \setminus S$

$\Delta |S| = -1$

$\Delta E(S) \leq -4$

posso prendere $f(S) = \pi |S| - E(S)$

mossa A $\Delta f(S) \geq \pi - 3 > 0$

B $\Delta f(S) \geq 4 - \pi > 0$

C4 $A, B \subseteq \mathbb{N}$, A finito. Ogni $n \in \mathbb{N}$ si scrive come $a+b$ in un unico modo. Mostrare che B è periodico.

A	B
0	0
1	
2	
3	
4	
	5
	10
	15
20	
21	

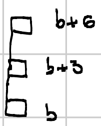
Metodo costruttivo: brutto

Cercare condizioni su A: non funziona

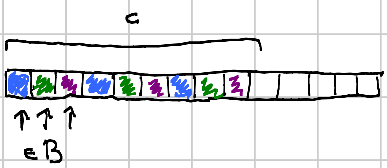
Idea: per ogni $b \in B$, considero $b + A = \{b+a : a \in A\} = X_b$

Questi X_b sono invarianti per traslazione, sono dei tasselli

Devo tassellare $\mathbb{N}$ con gli X_b



Nell'esempio $A = \{0, 3, 6\}$



Guardo come è fatto $\mathbb{N}$ a un certo momento

Inizio: tutto vuoto

1: • • × · · × · · ·

2: • × × · × × · · · · ·

3: • · · · • • • • •

Da un certo punto in poi è tutto vuoto, quindi un numero finito di possibilità

Se io ho i buchi fatti un un certo modo, in modo unico so come saranno fatti i buchi dopo aver messo un tassello.

Ma io so come è fatto il tassello che ho appena messo.

Quindi la sequenza è periodica

Soluzione trollosa.

$a = \sum_{i \in A} 10^{-i}$ $\qquad b = \sum_{i \in B} 10^{-i}$

$a \in \mathbb{Q}$, $b \in \mathbb{R}$

$ab = 1,\overline{1}$

$b = \frac{10}{9a} \in \mathbb{Q}$, non ha antiperiodo e quindi è periodico. FINE

Euristica sulla soluzione trollosa

l'ipotesi $\qquad a(x) := \sum_{i \in A} x^i \left(= \sum_{i=0}^{\infty} \varepsilon_i x^i \right)$

$$\varepsilon_i = \begin{cases} 0 & i \notin A \\ 1 & i \in A \end{cases}$$

$b(x)$,,

→ è equivalente a $\boxed{a(x)b(x) = \frac{1}{1-x}}$

poi $a(x)$ è un polinomio

se voglio B periodico (di periodo c)

→ voglio $\boxed{b(x)(1-x^c)}$ sia un polinomio di grado $< c$ (in particolare i coeff. sono definitivamente nulli)

la tesi si riconduce a dimostrare che

$$\frac{1-x^c}{(1-x)\,a(x)}$$ è un polinomio

cioè voglio che le radici del denominatore sia radici dell'unità distinte

È vero perché $b(x) = \frac{1}{(1-x)\,a(x)}$ ha coefficienti interi e limitati

Infatti quando avete $\frac{P(x)}{Q(x)} \in \mathbb{R}[[x]]$

potete scrivere $= \sum_{i,j} \frac{c_{ij}}{(x-r_i)^j}$

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

⇒ i coeff. della serie formale sono

$$[x^n]\,\frac{P(x)}{Q(x)} = \sum_{i,j} c_{ij}\, r_i^n \binom{n}{j-1}$$

⇒ se sono interi e limitati

→ r_i sono radici dell'unità e le molteplicità sono 1

PreIMO '16 COMBINATORIA (pomeriggio)

Titolo nota 24/05/2016

C5 idea: induzione; dimostro che posso fare qualunque permutazione della n-upla $1 \dots n$

passo base: $n = 1, 3$

hp. induttiva: so fare tutte le permutazioni di $1 \dots n$

passo induttivo: mi basta saper scambiare $n+1$ con un altro numero x

perché → so scambiare $n+1$ con qualunque y. $((n+1\ y) = (y\ x)(n+1\ x)(y\ x))$

hp. induttiva

→ so fare tutte le trasposizioni su $1 \dots n+1$ → tesi.

— se $n+1$ è pari so fare $\left(\frac{n+1}{2}, n+1\right)$

— se $n+1$ è dispari, sostengo di saper fare $\left(n+1\ \ \frac{n}{2}+1\right)$

Faccio:

$1\ 2 \dots \frac{n}{2}+1 \dots n+1$

$1\ 1 \dots \frac{n}{2}+1 \dots n+2$ ← pari

$1\ 1 \dots n+2 \dots \frac{n}{2}+1$

ora voglio trasformare in

$1\ 2 \dots n+1 \dots \frac{n}{2}+1$

pongo

$$f(a,b) = \begin{cases} \left(\frac{a}{2}, b+\frac{a}{2}\right) & \text{se } a \text{ è pari} \\ \left(a+\frac{b}{2}, \frac{b}{2}\right) & \text{se } b \text{ è pari} \end{cases}$$

$a+b$ è dispari

voglio dire che $\exists k \quad f^{(k)}(1, m+2) = (2, m+1)$

$(c,d) = f(a,b)$ so chi sono a e b

2 possibilità: $\nearrow (a,b) = (2c, d-c)$

$\searrow (a,b) = (c-d, 2d)$

MA solo una delle due coppie è "positiva"

$\rightarrow$ solo una va bene

Quindi so che $\exists k \quad f^{(k+1)}(1, m+2) = (1, m+2)$

$(1, m+2)$

questo non può succedere perché ed prima che vedo due volte è immagine di 2 coppie diverse a meno che non sia $(1, m+2)$.

Ma allora $f^{(k)}(1, m+2) = (2, m+1)$

$\rightarrow$ HO VINTO! $\square$

C6

una parola composta da H e V
è buona se inizia con 2 volte
la stessa stringa

eg. HVVHVVVV è buona

c'è un automa che controlla se una
parola è buona o cattiva

Oss: esiste una parola cattiva per ogni lunghezza
HVVVVV_ _ _ V

Oss 2: voglio costruire una famiglia di parole P_n
tali che il # di confronti in funzione
della lunghezza di P_n cresca in modo più che
lineare

Oss 2bis: non mi piacciono le parole buone

Eg: $HV\underbrace{HH}\underbrace{HVHV}\underbrace{HVHHHVHH}$ _ _ _ _

questo esempio funziona!

Dico che $P_0 = H$
$P_{n+1} = P_n \tilde{P}_n$ dove se p è una parola
$\tilde{p}$ ha le stesse
lettere tranne
l'ultima

Faccio un'altra costruzione:

$$\sigma : \begin{array}{l} H \mapsto HV \\ V \mapsto HH \end{array}$$

noto che $p_{n+1} = \sigma(p_n)$

devo solo mostrare che

$$p_n$$
$$\downarrow$$
$$p_n \widetilde{p_n}$$
$$\searrow$$
$$\sigma(p_n)\,\sigma(\widetilde{p_n})$$
$$\overset{?}{=}$$
$$\sigma(p_n)\,\widetilde{\sigma(p_n)}$$

è chiaro che $\sigma(\widetilde{p_n})$ e $\widetilde{\sigma(p_n)}$ coincidono con $\sigma(p_n)$ per tutte le lettere tranne le ultime 2

poi, la penultima è H (è uguale)
l'ultima è diversa da quella di $\sigma(p_n)$

Devo ancora verificare che

- le p_n sono cattive
- # confronti su p_n è minorato da una funzione che cresce più delle rette (qualcosa come $C \cdot n\, 2^n$)

Sono cattive: se confronto la lunghezza ℓ

per ℓ dispari: sbaglio al + al 2° confronto

$$\underbrace{H \qquad H}_{\ell}\ \underbrace{H\ H}_{\ell}$$

posto dispari

voglio = la prima lettera

ma la 2ª lettera è sempre V

se ℓ pari allora: torno alla parola P_{n-1} riunendo le lettere a blocchetti di 2 usando la costruzione di σ

(sto facendo induzione su $v_2(\ell)$)

Conto il # di confronti effettuati

Per ogni ℓ, sia $f(\ell)$ il numero di confronti per la lunghezza ℓ.

- $f(\ell) \geq 1 \quad \forall \ell = 1, \dots, 2^{n-1}$
- $f(2\ell) = 2f(\ell) \quad \forall \ell = 1, \dots, 2^{n-2}$

il primo punto è facile

per il secondo

l'ipotesi è che confrontando lungh ℓ

P_n $\quad \underbrace{f(\ell)}_{\ell}\ \underbrace{f(\ell)}_{\ell}$

σ

$p_n = p_{n+1}$ $\underbrace{\qquad\qquad}_{2\ell}\underbrace{\qquad\qquad}$

però le prime 4ℓ lettere le trovo uguali in p_n (perché $p_{n+1} = p_n \tilde{p}_n$) quindi sto lavorando in p_n

allora devo fare sicuramente $2\cdot(f(\ell)-1)$ confronti per la lungh 2ℓ
poi vedo $2H$ e continuo per il confronto n° $2f(\ell)$ che sbaglia

Ho finito: $\displaystyle\sum_{\ell=1}^{2^{n-1}} f(\ell)$ voglio una stima

se chiamo $g(\ell)$ t.c. $\begin{cases} g(\ell)=1 & \text{se } \ell \text{ dispari} \\ g(2\ell)=2g(\ell) \end{cases}$

ho mostrato che $f(\ell) \geq g(\ell)$

$$\sum_{\ell=1}^{2^{n-1}} f(\ell) \geq \sum_{\ell=1}^{2^{n-1}} g(\ell) \underset{\text{per casa}}{=} \frac{1}{4} n 2^n$$

$\square$

C7 100 giudici; non ne esistono 3 x, y, z tali che ci sono 3 concorrenti A, B, C per cui

x: $A > B > C$

y: $B > C > A$

z: $C > A > B$

TESI: esiste una classifica globale

"condivisibile"

Definisco un graf "diretto" sull'insieme dei concorrenti. ($G(A,B)$ = insieme dei giudici che preferiscono A a B.)

$$A \longrightarrow B \quad \text{se} \quad \#G(A,B) > 50$$

$$A \longleftrightarrow B \quad \text{se} \quad \#G(A,B) = 50 = \#G(B,A)$$

LEMMA:

$$\begin{tikzcd} A \arrow[r] & B \arrow[dl] \\ C \arrow[u] & \end{tikzcd}$$

non succede!

$$\#G(A,B) > 50$$
$$\#G(B,C) > 50$$
$$\#G(C,A) > 50$$

$\rightarrow \exists\, x \in G(A,B) \cap G(B,C) \rightarrow$ per cui $A > B > C$

e cicliche $\rightarrow$ contraddice l'ipotesi.

LEMMA+:

$$\begin{tikzcd} A \arrow[r] & B \arrow[d] \\ & C \arrow[ul, leftrightarrow] \end{tikzcd}$$

neanche questo può succedere!

LEMMA+ $\Rightarrow$ non esistono cicli diretti

$$\begin{tikzcd} A_1 \arrow[r] & A_2 \arrow[r] & \cdots \arrow[r] & A_n \arrow[lll, bend left] \end{tikzcd}$$

prendo il ciclo più piccolo (per assurdo); LEMMA $\rightarrow n > 3$. LEMMA+ mi dice che non ho $A_2 \longleftrightarrow A_n$; LEMMA mi

dice che non ho $A_2 \to A_n$.
Quindi ho $A_n \to A_2$; ma allora
$A_2 \to A_3 \to \ldots \to A_n$ è un ciclo più corto: assurdo!

FATTO: se non ci sono cicli diretti allora posso fare una classifica "condivisibile".
Per induzione sul numero di concorrenti. $\square$

C 8 Ci sono h camere e hm parlamentari;

alcuni sono nemici (il grafo ha N archi)

Qual è il minimo N per cui esiste un grafo delle inimicizie che non riesco a far stare in parlamento.

Ci sono alcuni bound facili

- se c'è una cricca grossa $h+1$ non ci sta
- se c'è un parlamentare antipatico con grado $\geq hm - m + 1$

La risposta è $N = \min\left\{ \frac{h(h+1)}{2}, hm - m + 1 \right\}$

Per mostrare la minimalità voglio riuscire a disporre ogni grafo con $N-1$ archi; in parlamento

per la disposizione uso un algoritmo greedy

- ordino i parlamentari per la loro antipati
- cerco di far sedere il primo che mi rimane fuori
  - la prima camera non è piena e non contiene nemici (lo metto lì)

    altrimenti cerco di farlo stare nella seconda

    e così via

- se in questo modo non riesco a metterlo

(1) allora c'è almeno una camera piena e senza nemici

sposto uno di questi in un'altra camera (2) (non piena e senza nemici) e ci faccio stare lui

Mi rimangono da mostrare

(1) : sia P_k il parlamentare che voglio aggiungere

$\Rightarrow \deg(P_k) \geq h$

e $k > h$

$$\Rightarrow \sum_{i=1}^{k} \deg(P_i) \geq h(h+1) > 2N \quad \text{assurdo}$$

sto sommando i gradi

sto guardando il # di archi

(2) 

$\underbrace{\qquad\qquad}$ P camere piene

$\underbrace{\qquad}$ Q camere senza nemici di P_k

$Q \leq P$; $P \leq h-1$; $(1) \Rightarrow Q \geq 1$

$$\sum_{P_i \text{ t.c. stanno sulle camere piene } \neq P_k} \deg(P_i) \geq P \cdot m \cdot \deg(P_k) + \deg(P_k)$$

$$\sum_{P_i \text{ che già stanno sulle camere non piene}} \deg(P_i) \geq \underbrace{(h-P)}_{\text{le camere}} \cdot \underbrace{1}_{\text{almeno 1 per camera}} \cdot \deg(P_k)$$

$$\deg(P_k) \geq h-Q$$

$$\sum_{P_i \text{ camere non piene}} \deg(P_i) \geq \underbrace{(h-P)}_{\text{le camere}} (Qm+1)$$

in ogni camera c'è almeno un nemico per ognuno di quelli già seduti nelle Q e nemico di P_k

Come si imposta il conto:

ho mostrato che $2N \geq (Pm+1)(h-Q) + (h-P)(h-Q)$

e $2N \geq (Pm+1)(h-Q) + (h-P)(Qm+1)$

ma queste contraddicono $N \leq \min\left\{\frac{h(h+1)}{2}, hm - m + 1\right\}$

a meno di $h \leq 2$ ~~o~~ $m = 2$

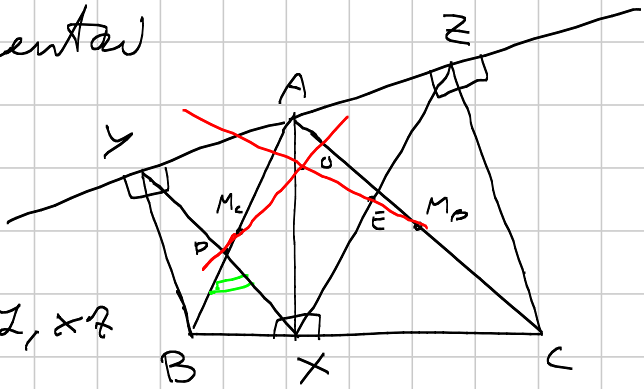
Il punto chiave è che fissati h, m, P sono lineari in Q e fissati h, m, Q sono lineari in P
(è utile fare il caso $P = Q$)

$\square$

Geometria mattino - PreIMO 2016

Titolo nota 25/05/2016

AXBY ciclici di centri M_B M_C
AXCZ



$\widehat{M_C O M_B} = \pi - \alpha$

D, E p.ti medi XY, XZ

Ciclicità ⇒ asse XY passa per M_C

$\widehat{M_C O M_B} = \widehat{BAC} + \widehat{AM_CO} + \widehat{OM_BA}$

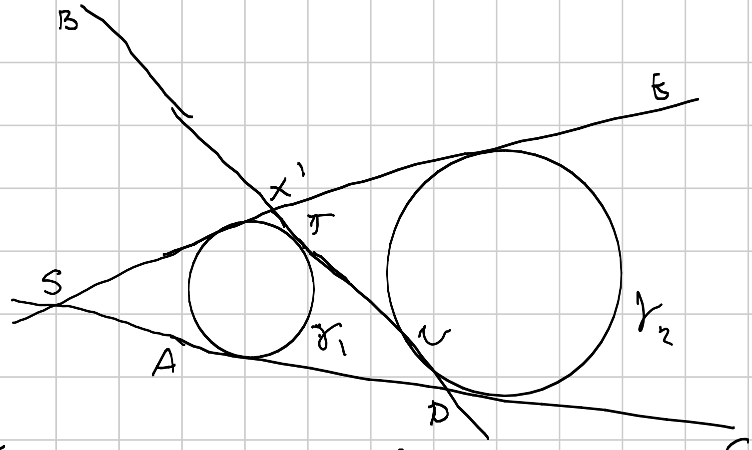
$\widehat{DM_CB} = \frac{\pi}{2} - (\pi - \beta - \widehat{BAY}) = \beta + BAY - \frac{\pi}{2}$

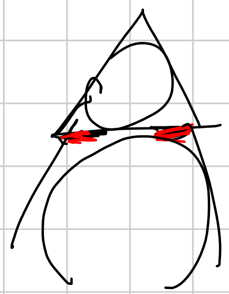
$\widehat{AM_BE} = \gamma + \widehat{CAZ} - \frac{\pi}{2}$

$\widehat{M_C O M_B} = \alpha + \beta + \widehat{BAY} - \frac{\pi}{2} + \gamma + \widehat{CAZ} - \frac{\pi}{2} =$

$= \alpha + \beta + \gamma - \pi + \pi - \alpha = \beta + \gamma$

$= \pi - \alpha$





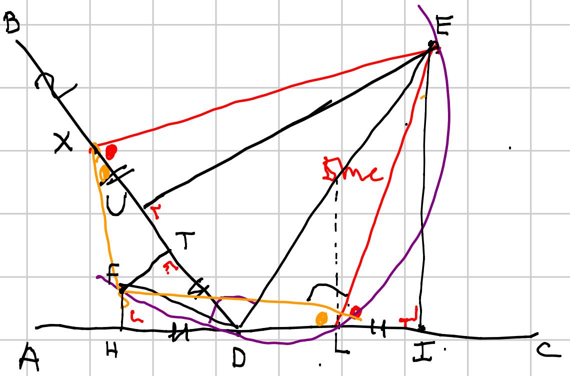
I. Idea

$X' = E \cap BD \implies BX' = BP = \frac{AB+BC-AC}{2}$

Oss. $AT = DU \implies$

$\implies DX' = DT + DU = \frac{BD+AD-AB}{2} + \frac{BD+DC-BC}{2}$

Allora $BX' = BD - DX' = BD - \frac{BD+AD-AB}{2} - \frac{BD+DC-BC}{2} = BP$



$HL = AL - AH = \frac{AB+AC-BC}{2} - \frac{AB+AD-BD}{2} = \frac{BD+DC-BC}{2} = DI$

$HL = DI \implies HD = LI$

$HD = DT = XU$

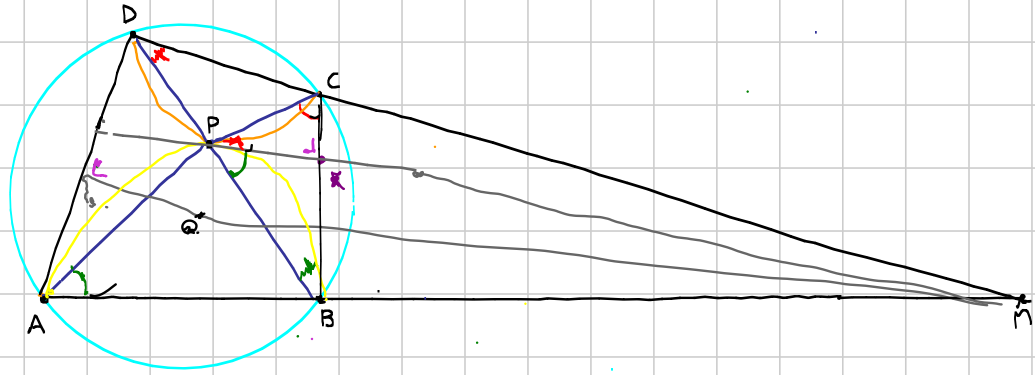
$XU = BD - BX - DU = BD - \frac{AB+BC-AC}{2} - \frac{BD+DC-BC}{2} = \frac{BD+AD-AB}{2} = DT$

Th $\iff \widehat{FXE} = 90^\circ \iff \widehat{FLE} = 90^\circ$

$FLE = 90^\circ \iff F\hat{H}L \sim L\hat{I}E \iff \frac{FH}{HL} = \frac{LI}{IE} \iff \frac{FT}{DU} = \frac{HD}{IU} \iff \widehat{FDE} = 90^\circ$

$F\hat{D}T \sim D\hat{E}U$

$$\boxed{\widehat{FDE} = \widehat{FLE} = 90^\circ}$$



Γ_{PCD} è tangente a Γ_{PAB}

ℓ tange Γ_{PCD} in P $\ell \hat{P}C = P\hat{D}C$. Vogliamo mostrare $\ell \hat{B}P = P\hat{A}B$

Vogliamo $C\hat{P}B = P\hat{D}C + P\hat{A}B$

$C\hat{P}B = 180 - C\hat{B}P - B\hat{C}P = (90 - C\hat{B}P) + (90 - B\hat{C}P) = B\hat{A}P + C\hat{D}P$

Analogo per Q.

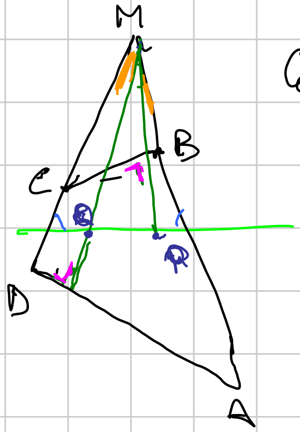
$M \in$ tang(P) (concorrenza di tre assi radicali in M)

$M \in$ tang Q

$MA \cdot MB = MP^2 = MQ^2$ $\quad MP = MQ$

$x\hat{P}C + x\hat{C}P = C\hat{D}P + B\hat{C}P = 90^\circ \Rightarrow$ tang(P) $\perp CB$

Allo stesso modo tang(Q) $\perp AD$



Con simmetria risp bisettrice di $A\hat{M}D$

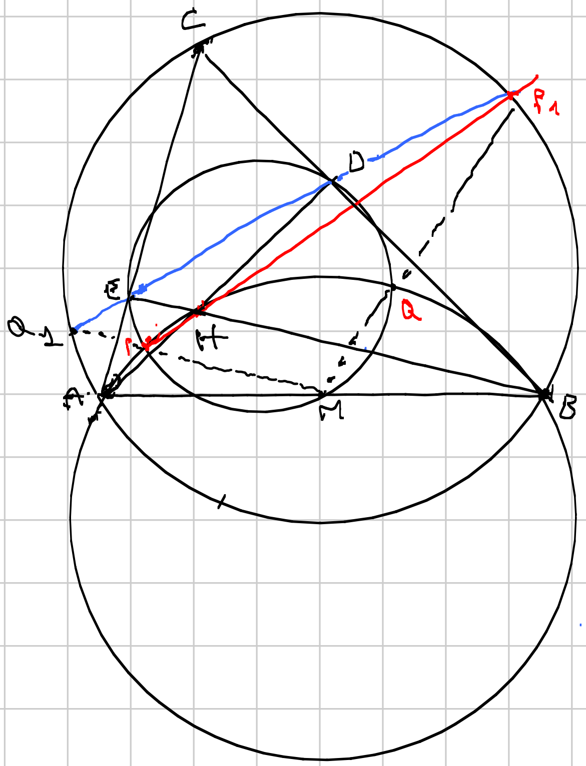
BC $\longrightarrow$ retta // AD (ABCD ciclico)

MP $\longrightarrow$ retta che passa per M
e $\perp$ AD
è la retta MQ

QP $\perp$ bisettrice di $A\hat{M}D$

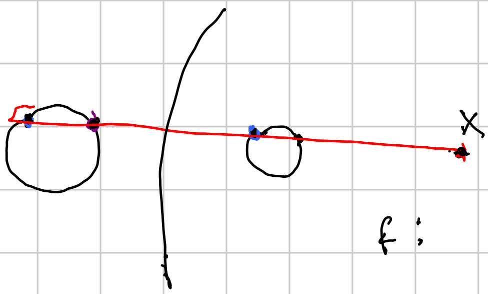
$\Rightarrow$ fa angoli uguali con i lati MD e MA

ES. 4



DIGRESSIONE 1:

•) Fatto noto: i centri di similitudine di (ABC) e (DEM) sono H e G.



f: f(•) = •

è un'inversione centrata in X

•) INVERSIONI:

a) DURA E PURA

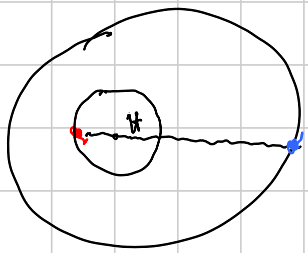
raggio a caso P → P'

b) FINE (solo se necessario)

raggio non a caso

ORA :

$AH \cdot HD = BH \cdot HE = r^2$



φ = inversione centro H e raggio r + sym in H

$D \leftrightarrow A$, $E \leftrightarrow B$

$(ABC) \leftrightarrow (DEM)$

Chiamiamo P_1 l'immagine di P

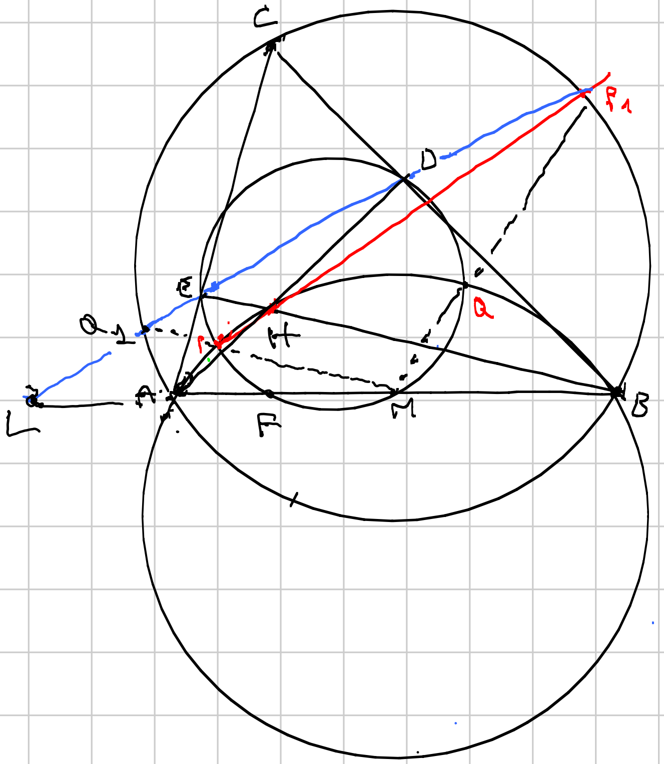
$P \in (DEM) \Rightarrow P_1 \in (ABC)$

$\varphi(P) = \varphi((DEM) \cap (ABH)) \subseteq \varphi((DEM)) \cap \varphi((ABH))$

$= (ABC) \cap DE$

$\Rightarrow P_1 \in DE$

$\Rightarrow$ (ABC), DE, PH concorrono in P_1



$CF \perp AB$

oss:

$PH \cdot HP_1 = QH \cdot HQ_1$

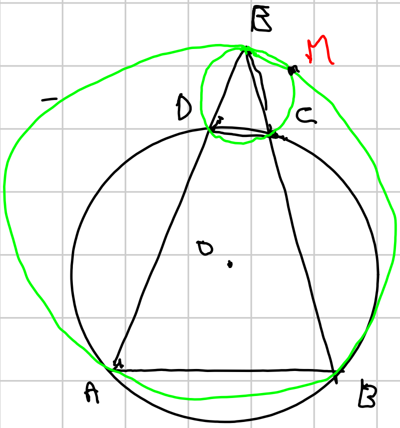
$\Rightarrow PP_1QQ_1$ ciclico

se $L = DE \cap AB$

$LQ_1 \cdot LP_1 =$
$LA \cdot LB =$
$LE \cdot LD =$
$LF \cdot LM$

$\Rightarrow P_1Q_1MF$ ciclico (*)

DIGRESSIONE 2



M pt. di Miquel di ABCD

Fatto noto:

$M = (AOC) \cap (BOD)$

(Dim: angoli)

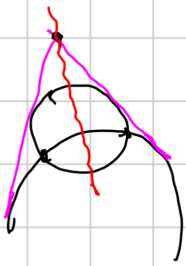
ORA: applico il fatto noto ad (P_1Q_1PQ)

Qual è il suo centro?

è C, che sta sull'asse di P_1Q_1

perché $CO \perp DE$

ma C sta sull'asse di PQ
perché C è il centro dell'omotetia di fattore 2
che manda (DEM) in (ABH)



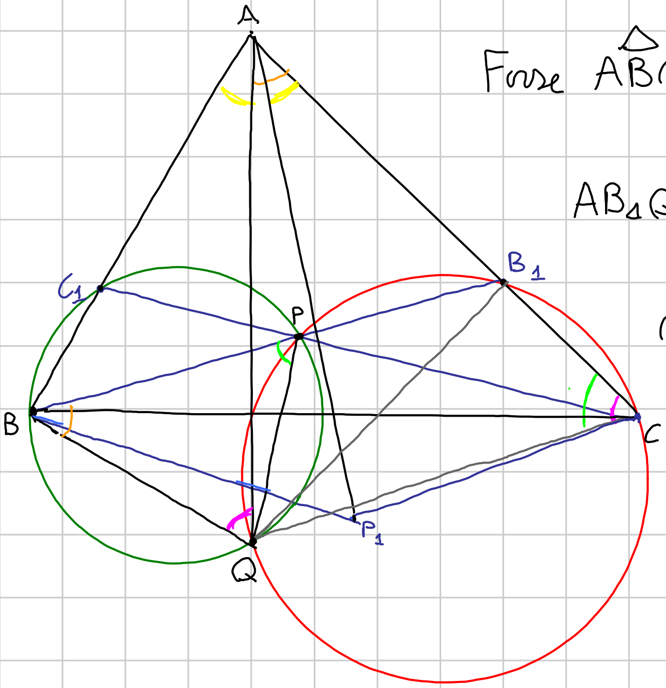
Il pt. di Miquel di $P_1 Q_1 P Q$ è
(per il fatto noto)
$(P_1 PC) \cap (Q_1 QC) = F$

ma CFP_1P è ciclico perché
$CH \cdot HF = PH \cdot HP_1 = r^2$

ma allora $Q_1 P \cap P_1 Q = (PQF) \cap (P_1 Q_1 F) = M$
$PQFM$ è Feuerbach
$P_1 Q_1 FM$ è ciclico per (*)

PreIMO '16 - GEOMETRIA (pomeriggio)

Es. 5



Forse $\overset{\triangle}{ABQ} \sim \overset{\triangle}{AP_1C}$

AB_1QB ciclico

$Q\hat{B_1}C = Q\hat{P}C$

$= 180° - Q\hat{P}C_1$

$= C_1\hat{B}Q = A\hat{B}Q$

$$B\hat{Q}A \underset{\substack{ABQB_1\\ \text{ciclico}}}{=} B\hat{B_1}A \underset{CP_1 /\!/ BB_1}{=} A\hat{C}P_1$$

Vogliamo provare a dimostrare $\dfrac{AQ}{BQ} = \dfrac{AC}{CP_1}$

Questa è vera $\Longleftrightarrow \dfrac{AQ}{BQ} = \dfrac{AC}{PB} \Longleftrightarrow \dfrac{AQ}{AC} = \dfrac{BQ}{BP}$

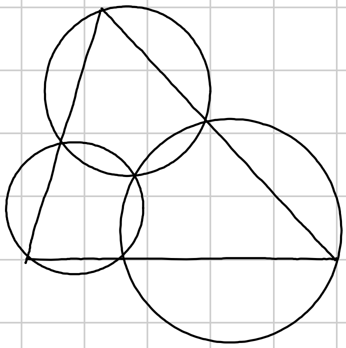
Vediamo $\overset{\triangle}{AQC} \sim \overset{\triangle}{BQP}$

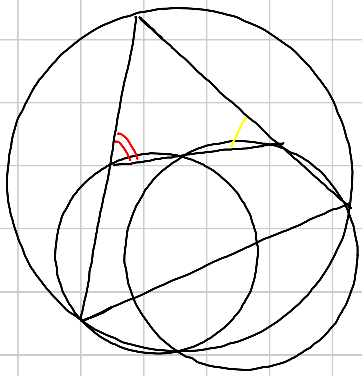
$Q\hat{B}P = Q\hat{A}C$ (per ciclicità $ABQB_1$)

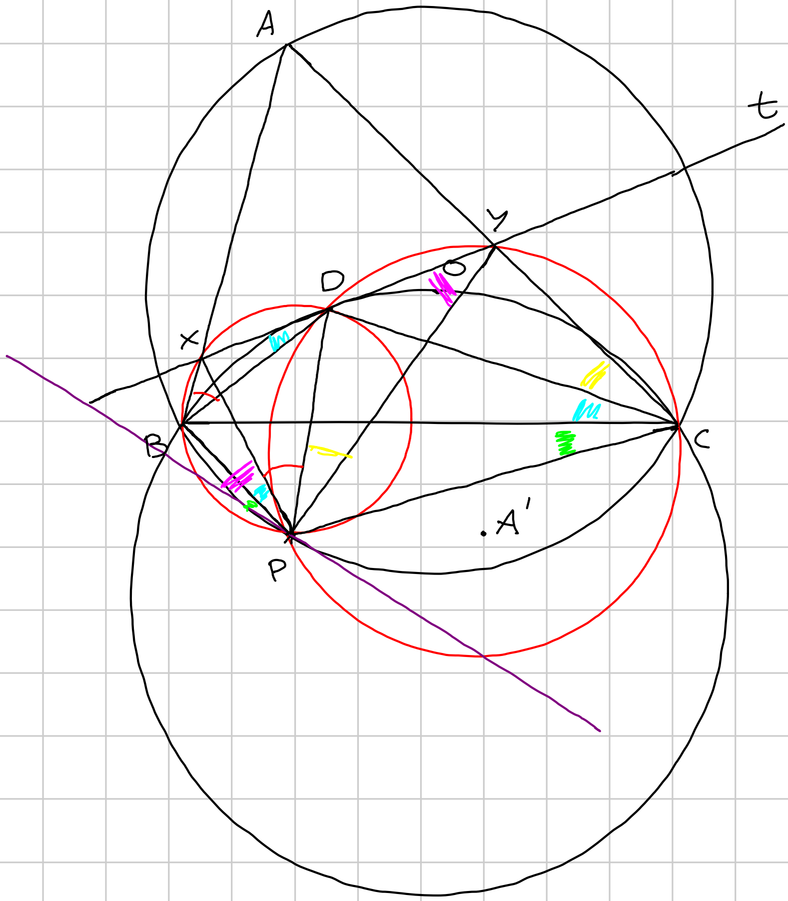
$$B\hat{P}Q = 180° - Q\hat{P}B_1 \underset{\substack{\text{ciclicità}\\ \text{rossa.}}}{=} Q\hat{C}B_1$$

$\Rightarrow \overset{\triangle}{BQP} \sim \overset{\triangle}{AQC} \Rightarrow \overset{\triangle}{ABQ} \sim \overset{\triangle}{AP_1C} \Rightarrow B\hat{A}Q = P_1\hat{A}C$

Problema 2







Miquel inverso $\Rightarrow$ le circ. rosse si incontrano su $\odot(ABC)$

STEP 1: $XYA'P$ ciclico

$$\Longleftrightarrow \widehat{XPY} = \alpha$$

$$\widehat{XPY} = \widehat{XPD} + \widehat{DPY} = \widehat{XBD} + \widehat{DCY} =$$

$$= \pi - \alpha - \widehat{DBC} - \widehat{BCD} =$$

$$\pi - \alpha - (\pi - 2\alpha) = \alpha$$

STEP 2: r tangente $\odot(ABC)$ in P

$$\text{TS} \Longleftrightarrow \widehat{rPX} = \widehat{PYX}$$

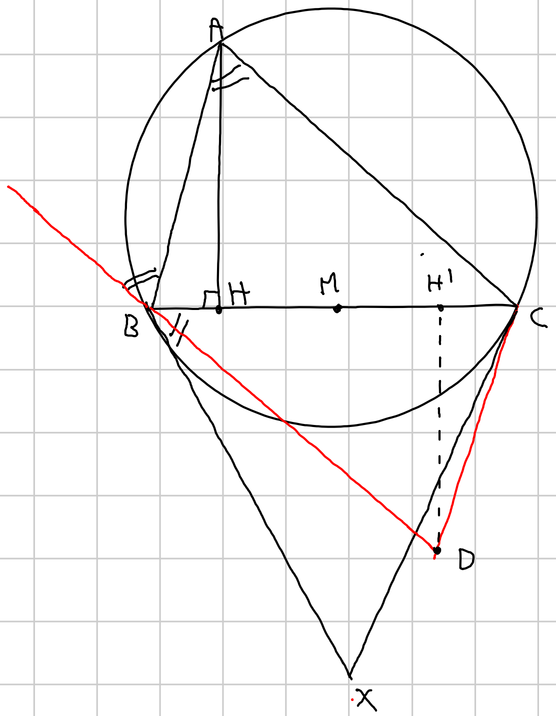
$$\widehat{rPX} = \widehat{rPB} + \widehat{BPX}$$

$$\widehat{rPB} = \widehat{PCB}$$

$$\widehat{BPX} = \widehat{BDX} = \widehat{BCD}$$

$$\widehat{rPX} = \widehat{PCB} + \widehat{BCD} = \widehat{PCD}$$

ESERCIZIO 7



$\angle(BD, AB) = \angle(AC, AB)$

$\Rightarrow BD \parallel AC$

$\Rightarrow$ ABDC é un parallelogramma

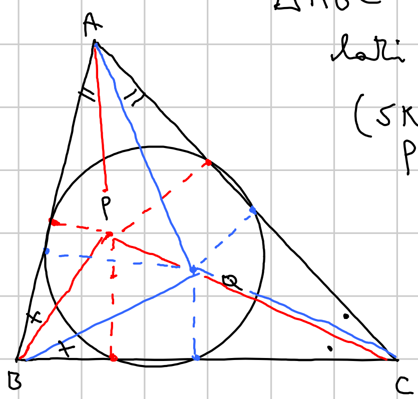
D simm. di A risp. a M

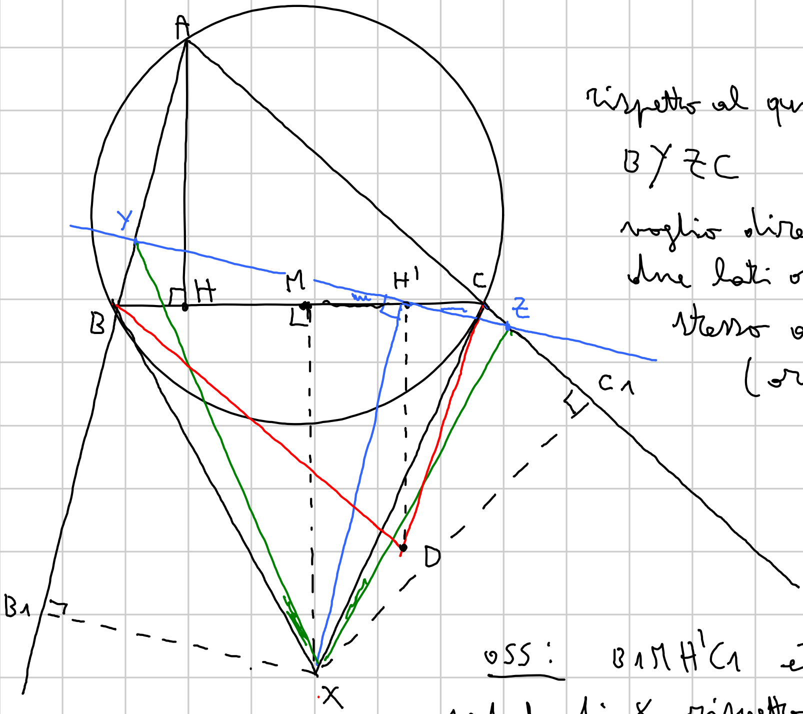
H' simm. di H risp. a M

allora $AH \perp BC \Rightarrow DH' \perp BC$

LEMMA: se P e Q sono coniugati isogonali in $\triangle ABC$ allora le loro proiezioni sui lati stanno su una circonferenza

(SKETCH: se faccio i simmetrici di P risp. a BC, CA, AB ho un triangolo di centro Q)





rispetto al quadrilatero
$BYZC$
voglio dire che X vede
due lati opposti sotto lo
stesso angolo
(orientato)

<u>oss</u>: $B_1MH'C_1$ è il quadrilatero
pedale di X rispetto a $BYZC$

ma D è il coniugato isogonale di X in $\triangle ABC$
e $DH' \perp BC$

<u>LEMMA</u> $\Rightarrow$ $B_1MH'C_1$ è ciclico

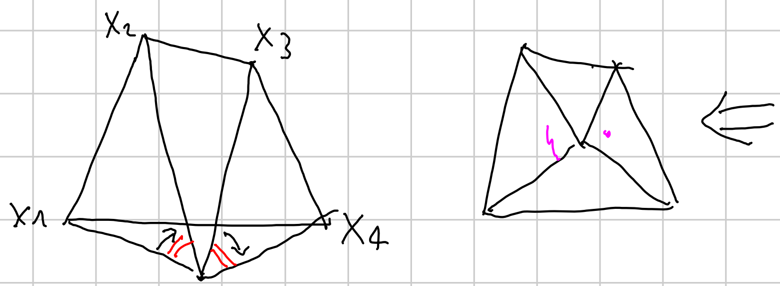
Ora
$$
\begin{aligned}
\widehat{BXY} &= \widehat{B_1XY} - \widehat{B_1XB} \\
&= \widehat{B_1H'Y} - \widehat{B_1MB} \\
&= \widehat{B_1H'B} + \widehat{BH'Y} - \widehat{B_1MB} = \widehat{BH'Y} - \widehat{H'B_1M}
\end{aligned}
$$

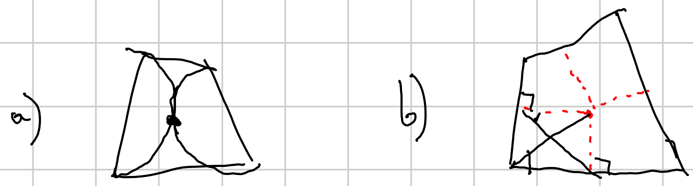
analogamente $\widehat{CXZ} = \widehat{CH'Z} - \widehat{H'C_1M}$

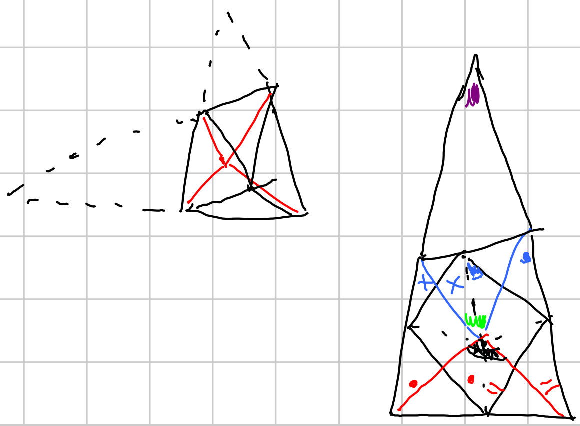
sapendo che $H'B_1C_1M$ è ciclico ottengo
$$\widehat{H'B_1M} = \widehat{H'C_1M}$$

e quindi $\widehat{BXY} = \widehat{CXZ}$

IN GENERALE:





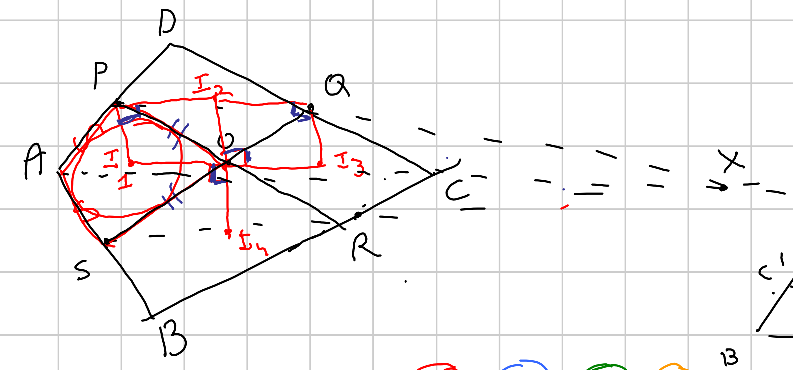


$\angle + \angle + \angle = \angle$

e ho $\angle + \angle = 180^\circ$

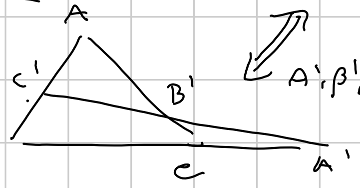
Esercizio 8

PQ, AC, RS concorrono (o sono parallele)



$$\frac{AC'}{C'B}\cdot\frac{BA'}{A'C}\cdot\frac{CB'}{B'A}=1$$

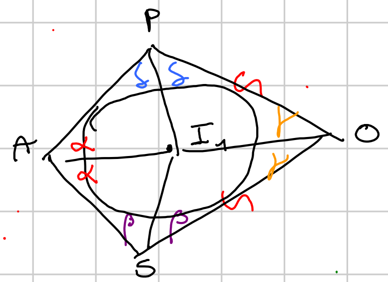
$\Updownarrow$ A', B', C' allin.



Concorrenza rette $\Longleftrightarrow$ $\frac{AP}{PD}\cdot\frac{DQ}{QC}\cdot\frac{CR}{RB}\cdot\frac{BS}{SA}=1$

$$\frac{AP}{SA}=\frac{\sin(\alpha+\delta)\,PI_1}{\underbrace{\sin(\alpha+\beta)}\,SI_1}$$

$$\frac{OP}{SO}=\frac{\sin(\gamma+\delta)\,PI_1}{\underbrace{\sin(\beta+\gamma)}\,SI_1}$$



$$\sin x\sin y=\frac{\cos(x-y)-\cos(x+y)}{2}$$

$$\sin(\alpha+\delta)\sin(\gamma+\delta)=\frac{\cos(\alpha-\gamma)-\cos(\alpha+\gamma+2\delta)}{2}$$

$$\sin(\alpha+\beta)\sin(\beta+\gamma)=\frac{\cos(\alpha-\gamma)-\cos(\alpha+(2\beta+\gamma))}{2}$$

Identità

$$\boxed{\frac{AP}{SA}\cdot\frac{OP}{SO}=\frac{PI_1^2}{SI_1^2}}$$

$$\frac{AP}{SA}=\frac{PI_1^2}{SI_1^2}\cdot\frac{SO}{OP}$$

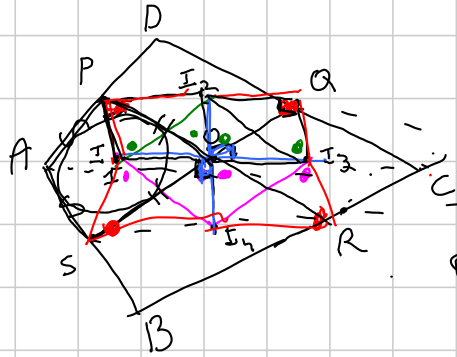
$$\frac{DQ}{PD}=\frac{QI_2^2}{PI_2^2}\cdot\frac{OP}{OQ}$$

$$\frac{CR}{QC}=\frac{RI_3^2}{QI_3^2}\cdot\frac{OQ}{OR}$$

$$\frac{BS}{RB}=\frac{SI_4^2}{RI_4^2}\cdot\frac{OR}{OS}$$

Th $\Longleftrightarrow$ $\cdot\cdot\cdot\cdot=1$

$$\Longleftrightarrow \frac{PI_1^2}{SI_1^2}\cdot\frac{QI_2^2}{PI_2^2}\cdot\frac{RI_3^2}{QI_3^2}\cdot\frac{SI_4^2}{RI_4^2}=1$$



Th $\Longleftrightarrow \cdots\cdots = 1$

$$\Longleftrightarrow \frac{PI_1^2}{SI_1^2}\cdot\frac{QI_2^2}{PI_2^2}\cdot\frac{RI_3^2}{QI_3^2}\cdot\frac{SI_4^2}{RI_4^2}=1$$

Oss. QI_3OI_2 ciclico $\Rightarrow$

$\Rightarrow Q\hat{I_3}I_2 = Q\hat{O}I_2 = I_2\hat{O}P = I_2\hat{I_1}P$

PI_2OI_1 ciclico

Quindi $P\hat{I_1}I_2 \sim Q\hat{I_3}I_2$

Quindi $\frac{PI_1}{PI_2} = \frac{QI_3}{QI_2} \Rightarrow \boxed{\frac{PI_1}{PI_2}\cdot\frac{QI_2}{QI_3}=1}$

Analogamente $RI_3I_4 \sim SI_1I_4$

$\frac{RI_3}{RI_4} = \frac{SI_1}{SI_4} \Rightarrow \boxed{\frac{RI_3}{RI_4}\cdot\frac{SI_4}{SI_1}=1}$

E dunque ■ + ■ $\Rightarrow$ th.

Un "IDEA" di soluzione

Se vi interessa ... In realtà anche ABCD è circoscrivibile.

Il punto di concorrenza è il centro di omotetia fra "altre" due circonferenze...

Preimo 2016 – Teoria dei Numeri (Mattino)

Titolo nota 23/05/2016

N2 SIANO l, m, n INTERI POSITIVI E p UN NUMERO PRIMO

TALI CHE:

$$p^{2l-1} m (mn+1)^2 + m^2$$

SIA UN QUADRATO PERFETTO.

DIMOSTRARE CHE m È UN QUADRATO PERFETTO.

MODO PER AVERE m QUADRATO PERFETTO:

$v_p(m)$ È PARI PER OGNI p PRIMO.

($v_p(m)$ = "ESPONENTE DI p NELLA FATTORIZZAZIONE DI m")

$$p^{2l-1} m (mn+1)^2 + m^2 = \square$$

$v_q(m)$ CON q PRIMO

$$m \left(p^{2l-1} (mn+1)^2 + m \right) = \square$$

$$v_q\left(m\left(p^{2\ell-1}(mn+1)^2+m\right)\right)=\text{PARI}$$

$$v_q(m)+v_q\Big(\underbrace{p^{2\ell-1}(mn+1)^2+m}_{\alpha}\Big)$$

- $v_q(m)=0$

  $\Downarrow$

  $v_q(m)$ È PARI

- $v_q(m)>0$. $q\mid m$

SPERANZA: q NON DIVIDE α

$\Longrightarrow v_q(\alpha)=0$ (PARI) $\Rightarrow v_q(m)$ PARI

SE $q\mid m$ È

$$q\mid p^{2\ell-1}(mn+1)^2+m$$

$$\Downarrow$$

$$q\mid p^{2\ell-1}(mn+1)^2$$

ORA: $(q, mn+1)=1$

PERCHÉ $q \mid mn+1$ $q \nmid mn+1$

ALLORA POSSIAMO TOGLIERE $(mn+1)^2$

DALLA DIVISIBILITÀ E AVREMO:

$q \mid p^{2l}-1$

PERCIÒ SE $q \neq p \Rightarrow$

$v_q(m)$ È PARI.

m SARÀ DELLA FORMA:

- K^2 (ALLORA SIAMO A POSTO) $\Leftarrow$ P CON ESPONENTE PARI
- pK^2 $\Leftarrow$ P CON ESPONENTE DISPARI.

$m = pK^2$

$$p^{2l}\cdot k^2\left(pk^2n+1\right)^2+p^2k^4=\square$$

POSSIAMO RACCOGLIERE p^2k^2:

$$p^{2l-2}\left(pk^2n+1\right)^2+k^2=\square \qquad (*)$$

COSA UTILE: SCHIACCIARLO TRA DUE QUADRATI CONSECUTIVI

$$J^2<\underbrace{p^{2l-2}\left(pk^2n+1\right)^2}_{\text{GRANDE}}+\underbrace{k^2}_{\text{PICCOLO}}<(J+1)^2$$

k^4

$$J\to p^{l-1}\left(pk^2n+1\right)$$

$$p^{2l-2}(pk^2n+1)^2 \overset{?}{<} p^{2l-2}(pk^2n+1)^2 + \underline{\underline{k^2}}$$

$$\overset{?}{<} \left(p^{l-1}(pk^2n+1)+1\right)^2$$

$<$ OVVIA

$$\cancel{p^{2l-2}(pk^2n+1)^2} + k^2 \overset{?}{<} \cancel{p^{2l-2}(pk^2n+1)^2} +$$
$$+ 2p^{l-1}(pk^2n+1)+1$$

$$k^2 \overset{?}{<} 2p^{l-1}(pk^2n+1)+1$$

$$l \geq 1 \Rightarrow RHS > 2pk^2n > k^2$$

— · —

SOL. ALTERNATIVA: IN (*) USARE LA FORMA STANDARD DELLE TERNE PITAGORICHE.

N3

$$\left(b^2 + 11(a-b)\right)^2 = a^3 b$$

oss: $a = b$ é sol $\forall a \in \mathbb{Z}$.

$$b^4 + 2\cdot 11(a-b)b^2 + 11^2(a-b)^2 = a^3 b$$

$$b(b-a)(a^2+ab+b^2) + 2\cdot 11(a-b)b^2 + 11^2(a-b)^2 = 0$$

$$b(a^2+ab+b^2) - 2\cdot 11 b^2 - 11^2(a-b) = 0$$

é una quadratica in a

$\Downarrow$

$\Delta = \square$

$$11 \mid b(a^2+ab+b^2) \longrightarrow \boxed{11 \mid b}$$

$$11 \mid a^2+ab+b^2 \Longleftrightarrow 11 \mid a,\ 11 \mid b$$

$\downarrow$

$a^3 \equiv b^3 \ (11)$ se $b \not\equiv 0$ $\quad \left(\frac{a}{b}\right)^3 \equiv 1 \ (11)$

$\mathrm{ord}\left(\frac{a}{b}\right) = 1, 3 \qquad \mid \varphi(11) = 10$

$a \equiv b \ (11)$

$3a^2 \equiv 0 \ (11) \longrightarrow a \equiv b \equiv 0 \ (11)$

$b = 11K$

$\cancel{11}K(a^2+11aK+11^2K^2) - 2\cdot 11^{\cancel{3}\,2}K^2 - 11^2(a-11K) = 0$

$a^2K + 11a(K^2-1) + 11^2K(K^2-2K+1) = 0$

$\Delta = 11^2(K^2-1)^2 - 4\cdot K\cdot 11^2 K(K-1)^2$

$\overset{\shortparallel}{(K-1)^2(K+1)^2}$ $\longrightarrow K=1$ é sol $\rightarrow (0,11)$

$(K+1)^2 - 4K^2 = \square$

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

é >0 solo in $-\frac{1}{3} \leq K \leq 1$

$\Longrightarrow$ TUTTE E SOLE LE SOL SONO

(a,a) $a \in \mathbb{Z}$ e $(0,11)$

SOL. ALTERNATIVE:

$p \neq 11 \rightarrow v_p(a) = v_p(b)$

oppure considerare $\gcd(a,b)$

$\boxed{N1}$ $x^3 - 2015x = q \qquad x, q \in \mathbb{Q}$

$\exists q$ tale che ci siano ZERO SOLUZIONI.

Esempio: $q = 1$

supponiamo $x = \frac{a}{b} \qquad (a,b) = 1$

Sostituiamo e moltiplichiamo per b^3

$$\underbrace{a^3 - 2015ab^2}_{\text{MULTIPLO di } a} - b^3 = 0$$

$a \mid b^3 \qquad b \mid a^3 \qquad /$

$a = \pm b = \pm 1 \qquad$ NON FUNZIONA

Non ci possono essere due sol distinte.

$x = \frac{a}{c} \qquad y = \frac{b}{c} \qquad (a,b,c) = 1$

$c \neq 0$.

Sostituiamo x e y nell'equazione e facciamo la differenza

$$x^3 - y^3 - 2015(x-y) = 0$$

divido per $x - y$:

$$x^2 + xy + y^2 - 2015 = 0$$

$$a^2 + ab + b^2 - 2015c^2 = 0$$

MOD 5 funziona

TRACCIA DI SOL. MOD. 3

MOLTIPLICO PER 4

$$\underbrace{4a^2 + 4ab + b^2}_{(2a+b)^2} + 3b^2 - 8060c^2 = 0$$

$$c^2 - 8062c^2$$

$$3 \mid \alpha^2 + \beta^2 \Rightarrow 3 \mid \alpha \quad 3 \mid \beta.$$

Sostituendo $\underline{\text{ottengo}}$ a, b, c div. per 3.

$$f(x) = d_n x^n + d_{n-1} x^{n-1} + \dots + d_0$$

$$= \frac{c_n x^n + c_{n-1} x^{n-1} + \dots + c_0}{c} \qquad c, c_i \in \mathbb{Z}$$

$$x = \frac{a}{b} \longrightarrow \frac{c_n a^n + c_{n-1} a^{n-1} b + \dots + b^n}{c b^n}$$

Non ottengo mai $\frac{1}{q}$ per q primo "ben scelto".

Assurdo: $\frac{1}{q} = f(x)$

$q \cdot$ Numeratore $= c b^n$

$q > c \Rightarrow q \mid b$

Denominatore è divisibile per q^2 $(n \geq 2)$
RHS 1 ⊗

$LHS = q \cdot Num$
Se $q \nmid c_n$ Num non è div. per q.

IMPOSSIBILE

NA1 Proprietà: (i) $a_n < a_{n+1}$ $\forall n$
$a_n > 0$ (ii) $a_{2n} = 2a_n$ $\forall n$.

Tesi: p primo $> a_1$ $\Rightarrow$ $\exists n$ t.c. $p \mid a_n$.

$s_n = a_{n+1} - a_n > 0$ $\exists s$ minimo

$s = a_{m+1} - a_m$.

Considero k tale che $2^k > p$

$$\boxed{a_{2^k(m+1)} - a_{2^k m}} = 2\left[a_{2^{k-1}(m+1)} - a_{2^{k-1}m}\right]$$

$$= 4\left[a_{2^{k-2}(m+1)} - a_{2^{k-2}m}\right] = \dots =$$

$$= 2^k (a_{m+1} - a_m) = 2^k s.$$

si può scrivere come una somma telescopica
$a_k - a_h = (a_k - a_{k-1}) + (a_{k-1} - a_{k-2}) + \dots + (a_{h+1} - a_h)$

Il n° di addendi $= 2^k > p$.

$\to$ gli addendi sono tutti uguali a s.

(ho una prog. aritmetica).

Quindi per $2^k m \leq n < 2^k (m+1)$

$$\boxed{a_{n+1} - a_n = s}$$

Considero i primi p termini

$$n = 2^k m + i \qquad 0 \leq i < p \qquad (2^k > p)$$

Claim: sono tutti distinti modulo p.

($\to$ tesi)

Se $a_{2^k m + i} \equiv a_{2^k m + j} \pmod p$

$$0 \leq i < j < p$$

Per differenza $s(i-j) \equiv 0 \pmod p$

$\Rightarrow s \equiv 0 \pmod p$

$p > a_1 = a_2 - a_1 \geq s$ ASSURDO.

Tra i vari $a_{2^k m + i}$ c'è un

multiplo di p.

$\forall n$, n è stretto fra due potenze di 2

$$2^{k_n} \leq n < 2^{k_n + 1}$$

- $k_n \leq k_{n+1}$
- $k_{2n} = k_n + 1$

$$\boxed{a_n = np + 2^{k_n}}$$

$a_n < a_{n+1}$

$a_{2n} = 2np + 2^{k_n+1} = 2np + 2 \cdot 2^{k_n}$

$= 2(a_n)$.

PREIMO 2016 — TdN — Pomeriggio

Titolo nota 23/05/2016

N5

$(f(n), f(2^n)) = 1 \quad \forall n$

$a-b \mid f(a)-f(b)$

supp. $\exists n$ t.c. $p \mid f(2^n)$ p primo

$p \mid f(2^n+kp)$

$x_k = 2^n + kp$

$2^{x_k} - x_k \mid f(2^{x_k}) - f(x_k)$

$p \mid 2^{x_k} - x_k \qquad 2^{2^n+kp} - 2^n - kp \equiv 0 \ (p)$

$p=2 \longrightarrow$ ok

$p \neq 2 \qquad 2^{2^n - n + kp} \equiv 1 \ (p)$

$p-1 \mid 2^n - n + kp \qquad p-1 \mid 2^n - n + k$

possiamo trovare un tale k, lo chiamiamo k_0

$p \mid 2^{x_{k_0}} - x_{k_0} \mid f(2^{x_{k_0}}) - f(x_{k_0})$

$p \mid f(x_{k_0}) \Longrightarrow p \mid f(2^{x_{k_0}})$ assurdo

$(f(x_{k_0}), f(2^{x_{k_0}})) = 1$

$\forall n \quad f(2^n) = \begin{cases} 1 \\ -1 \end{cases}$

$\Rightarrow$ WLOG vale infinite volte $f(2^n)=1$

$f(x)-1$ avrebbe infinite radici

$f(x)\equiv 1$

analogamente per -1

gli unici polinomi che soddisfano

~~sono~~ $f(x)\equiv 1, -1$

N7 SIA q UN NUMERO PRIMO. DIMOSTRARE CHE ESISTE UN INTERO POSITIVO N_q TALE CHE:

- SE $K>N_q$;
- SE $qK+1$ È UN PRIMO p;

ALLORA $p \nmid 1^{q-1}+2^{q-1}+\dots+K^{q-1}$

CONSIDERARE IL POLINOMIO f TALE CHE:

$$f(n)=\sum_{i=1}^{n}(i)^{q-1}$$

CONDIZIONE: p DIVIDE $f(K)$

$qk \equiv -1 \ (p) \rightarrow k \equiv -\frac{1}{q} \ (p)$

p DIVIDE $f\left(-\frac{1}{q}\right)$

È UN NUMERO A PRIORI REALE

$\Downarrow$

IN REALTÀ RAZIONALE

IL NUMERATORE DI $f\left(-\frac{1}{q}\right)$ È MULTIPLO DI OGNI p DELLA FORMA $qk+1$ ABBASTANZA GRANDE.

$f\left(-\frac{1}{q}\right) = 0$

DIPENDE SOLO DA q

LEMMA Sia $n \in \mathbb{N}$.

Th Esistono $a_0, a_1, \dots, a_n$ INTERI TALI CHE:

$$x^n = a_n \binom{x}{n} + a_{n-1} \binom{x}{n-1} + \dots + a_0 \binom{x}{0}$$

$$\binom{x}{k} = \frac{x(x-1)\dots(x-k+1)}{k!}$$

DIM.

INDUZIONE

P.B. $n=0$ $\quad x^0 = 1 \cdot \binom{x}{0}$

PASSO INDUTTIVO:

$$x^n - n! \binom{x}{n}$$

$$\binom{x}{n} = \frac{1}{n!} x^n + c_{n-1} \cdot \frac{1}{n!} x^{n-1} + \dots + c_0 \cdot \frac{1}{n!} \cdot x^0$$

C_i INTERI: COEFFICIENTI DI
$x(x-1)(x-2)\dots(x-n+1)$

C_i INTERI $\longrightarrow$ $n!\binom{x}{n}$ A COEFFICIENTI INTERI:

$$x^n - n!\binom{x}{n} = -c_{n-1}x^{n-1} - c_{n-2}x^{n-2} - \dots - c_0 \cdot x^0$$

$\Downarrow$ IPOTESI INDUTTIVA ESTESA

OGNI x^i È DELLA FORMA $d_i\binom{x}{i} + d_{i-1}\binom{x}{i-1} + \dots$

SOSTITUISCO OGNI x^i CON LA SUA FORMA

COME SOMMA DI BINOMIALI E DUNQUE OTTENGO UN'ALTRA SOMMA DI BINOMIALI.

<u>COROLLARIO</u>: $\binom{0}{k} + \binom{1}{k} + \dots + \binom{x}{k} = \binom{x+1}{k+1}$

PER $x \in \mathbb{N}$

ALLORA: $1^n + 2^n + 3^n + \dots + x^n =$

$$= a_n \binom{x+1}{n+1} + a_{n-1} \binom{x+1}{n} + \dots + a_0 \binom{x+1}{1}$$

DOVE GLI a_i RISPETTANO

$$x^n = a_n \binom{x}{n} + a_{n-1} \binom{x}{n-1} + \dots + a_0 \binom{x}{0}$$

x^n COME $\sum$ DI BINOMIALI $\to$ $1^n + 2^n + \dots + x^n$ COME SOMMA DI BINOMIALI

$$x^{q-1} = a_{q-1} \binom{x}{q-1} + a_{q-2} \binom{x}{q-2} + \dots + a_0 \binom{x}{0}$$

$$\underbrace{x^{q-1} - a_{q-1} \binom{x}{q-1}}_{\text{I TERMINI CON } x^{q-1} \text{ SI DEVONO SEMPLIFICARE}} = \underbrace{a_{q-2} \binom{x}{q-2} + \dots + a_0 \binom{x}{0}}_{\text{GRADO } \leq q-2}$$

$$x^{q-1} - a_{q-1}\binom{x}{q-1}$$

$$\binom{x}{q-1} = \frac{1}{(q-1)!}\cdot x^{q-1} + \dots$$ ← GRADO MINORE

DEVE VALERE $x^{q-1} - a_{q-1}\cdot\frac{1}{(q-1)!}x^{q-1} = 0$

$a_{q-1} = (q-1)!$

$$x^{q-1} = (q-1)!\binom{x}{q-1} + a_{q-2}\binom{x}{q-2} + \dots + a_0\binom{x}{0}$$

$$1^{q-1} + 2^{q-1} + \dots + x^{q-1} = (q-1)!\binom{x+1}{q} + a_{q-2}\binom{x+1}{q-1} + \dots + a_0\binom{x+1}{1} = f(x)$$

$f(x)$ È A COEFFICIENTI RAZIONALI

SUPPONIAMO CHE PER INFINITI VALORI DI x $qx+1=p$ PRIMO E $p \mid f(x)$

F(X) È A COEFFICIENTI RAZIONALI.

SE p NON DIVIDE IL DENOMINATORE DI NESSUN COEFFICIENTE DI $f(x)$, ALLORA POSSIAMO TRATTARE $f(x)$ COME POLINOMIO A COEFFICIENTI MODULO p.

POSSIAMO AD ESEMPIO CONSIDERARE $f\left(\frac{1}{2}\right) \equiv$

$$\equiv f\left(\frac{p+1}{2}\right) \quad (p)$$

VORREMMO FARE DELLE CONGRUENZE CON DEI NUMERI RAZIONALI.

$qk \equiv -1 \ (p)$. SE $p > q, k$

$$k \equiv -\frac{1}{q} \ (p)$$

PERCIÒ, SE p È SUFFICIENTEMENTE GRANDE DA:

- ESSERE $> q, k$;
- NON COMPARIRE IN $f(x)$.

ALLORA p DIVIDE IL NUMERATORE DI

$f\left(-\frac{1}{q}\right)$ PERCHÉ:

$-\frac{1}{q} \in \mathbb{Z}(p) \rightarrow f\left(-\frac{1}{q}\right) \equiv f(\mathbb{Z}) \ (p)$

ORA: $f\left(-\frac{1}{q}\right)$ DIPENDE SOLO DA q.

PERÒ È DIVISO DA INFINITI PRIMI.

$f\left(-\frac{1}{q}\right) = \frac{a}{b}$ E p DIVIDE a PER INFINITI PRIMI $p \Rightarrow a = 0$

$f\left(-\frac{1}{q}\right) \overset{?}{=} 0$. SE $f\left(-\frac{1}{q}\right) \neq 0$ ABBIAMO FINITO.

$f(x) = 1^{q-1} + \dots + x^{q-1} = (q-1)!\binom{x+1}{q} + a_{q-2}\binom{x+1}{q-1} + \dots + a_0\binom{x+1}{1}$

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

$0 \overset{?}{=} (q-1)!\binom{-\frac{1}{q}+1}{q} + a_{q-2}\binom{-\frac{1}{q}+1}{q-1} + \dots + a_0\binom{-\frac{1}{q}+1}{1}$

$$0 \overset{?}{\equiv} \frac{\cancel{(q-1)!}}{q\,\cancel{q!}}\left(-\frac{1}{q}+1\right)\left(-\frac{1}{q}\right)\left(-\frac{1}{q}-1\right)\dots\left(-\frac{1}{q}+2-q\right)+$$

$$\frac{a_{q-2}}{(q-1)!}\left(-\frac{1}{q}+1\right)\dots\left(-\frac{1}{q}+3-q\right)+\dots+\frac{a_0}{1!}\left(-\frac{1}{q}+1\right)$$

$\Downarrow$ MOLTIPLICHIAMO PER q^{q+1}

$$0 \overset{?}{\equiv} (q-1)(-1)(-1-q)\dots(-1+2q-q^2)+ \quad \not\equiv 0\ (q)$$

$$\left.\frac{a_{q-2}}{(q-1)!}\cdot q^2\,(q-1)(-1)\dots(-1+3q-q^2)+\right] \equiv 0\ (q)$$

$$\left.\frac{a_{q-3}}{(q-2)!}\,q^3\,(\dots)\qquad(\dots)+\right] \equiv 0\ (q)$$

NON HA q AL DENOMINATORE

NON HA q AL DENOMINATORE

$\dots$

$$\left.+\frac{a_0}{(1)!}\,q^q\cdot\qquad(q-1)\right] \equiv 0\ (q)$$

GUARDO MODULO q

ASSURDO!

$$\underbrace{0 \overset{?}{\equiv} \sum \text{NUMERI MULTIPLI DI } q}\ +\ \text{NON MULTIPLO DI } q$$

0 ~~V~~ NON MULTIPLO DI q.

$\boxed{TN6}$ Sol intere di $x^2+y^2 = \boxed{p+1,\ 2p+1,\ \dots,\ p(p-3)+1}$

p primo > 5.

Vedere le soluzioni di $x^2+y^2 \equiv 1 \pmod p$

$$-\frac{p-1}{2} \le x, y \le \frac{p-1}{2} \qquad -\frac{p-1}{2}, \dots, -1, 0, 1, \dots, \frac{p-1}{2}$$

Se cerco x, y qui dentro ho

$$x^2+y^2 \le 2\left(\frac{p-1}{2}\right)^2$$

Manca 1

Si verifica che $2\left(\frac{p-1}{2}\right)^2 \le p(p-3)+1$ $(p \ge 5)$

$1 = x^2+y^2 \qquad x, y \in \{0, \pm 1\}$

4 sol $(0,+1)\ (0,-1)\ (1,0),\ (-1,0)$

Mi ci vorrebbero più di 4 soluzioni della congruenza.

Contiamo quante sono ESATTAMENTE le soluzioni

$$x^2+y^2 \equiv 1 \iff y^2 \equiv 1-x^2 \quad (*)$$

Fissato x $(*)$ ha
$$\begin{cases} 2 \text{ sol} & \text{se } 1-x^2 \equiv \square \ne 0 \pmod p \\ 1 \text{ sol.} & \text{se } 1-x^2 \equiv 0 \quad " \\ 0 \text{ sol} & \text{se } 1-x^2 \not\equiv \square \pmod p \end{cases}$$

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \\ 0 \\ -1 \end{cases} \quad \text{nei tre casi precedenti}$$

Fissato x, n° sol. $= 1 + \left(\frac{1-x^2}{p}\right)$

Il n° TOTALE DI SOLUZIONI è

$$N \doteq \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left[1 + \left(\frac{1-x^2}{p}\right)\right].$$

Distinguo 2 casi: $p \equiv 1, 3 \pmod 4$

1° caso $p \equiv 3 \pmod 4$

Notazione N_0 è solo il termine per $x=0$

N^* tutti gli altri

$N_0 = 1 + \left(\frac{1-0}{p}\right) = 1 + \left(\frac{1}{p}\right) = 1+1 = 2$

Biezione $x \to x^{-1} = \frac{1}{x}$

$$S = \sum_{x\neq 0} \left(\frac{1-x^2}{p}\right) = \sum_{x\neq 0} \left(\frac{1-\frac{1}{x^2}}{p}\right) = \sum_{x\neq 0} \left(\frac{\frac{x^2-1}{x^2}}{p}\right) =$$

$$= \sum_{x\neq 0} \left(\frac{x^2-1}{p}\right) = \sum_{x\neq 0} \underbrace{\left(\frac{-1}{p}\right)}_{=-1} \left(\frac{1-x^2}{p}\right) = -S$$

$S=0$

$$N^* = \sum_{x\neq 0} \left(1 + \left(\frac{1-x^2}{p}\right)\right) = p-1+0 = p-1$$

$$\boxed{N = N_0 + N^* = 2 + (p-1) = p+1}$$

2° caso $p \equiv 1 \pmod 4$

In questo caso $\left(\frac{-1}{p}\right) = 1$.

Posso riscrivere N come $N = \sum_{x\in\mathbb{Z}/p\mathbb{Z}} \left(1 + \left(\frac{x^2-1}{p}\right)\right)$

Cambio di variabile $x \mapsto \frac{x}{a}$ $a \neq 0$

biezione (anche delle classi diverse da zero)

$$\forall a \neq 0 \quad N = \sum_{x\in\mathbb{Z}/p\mathbb{Z}} \left(1 + \left(\frac{\left(\frac{x}{a}\right)^2 - 1}{p}\right)\right) = \sum \left(1 + \left(\frac{\frac{x^2-a^2}{a^2}}{p}\right)\right)$$

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

Dimentichiamo per un attimo l'addendo 1, consideriamo solo il resto.

$$\boxed{\forall a \neq 0 \quad \sum_x \left(\frac{x}{p}\right)\left(\frac{x+2a}{p}\right) = T} \quad (\ast\ast)$$

le tesi verrà $N = p + T$

Somma $(\ast\ast)$ $\forall a \neq 0$

$$(p-1)T = \sum_x \sum_{y \neq x} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$$

$x+2a$, $x+4a$, $\vdots$ $x + 2(p-1)a$ sono tutte le classi $\neq x$

$$= \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) - \sum_x \left(\frac{x}{p}\right)\left(\frac{x}{p}\right)$$

$$= \left(\sum_x \left(\frac{x}{p}\right)\right)^2 - \sum_x \left(\frac{x}{p}\right)^2$$

$$= 0^2 - (p-1)$$

$$(p-1)T = -(p-1)$$

$$T = -1$$

$$\boxed{N = p + T = p-1}$$

$p - 1 > 4$ ok.

$\boxed{N8}$ $\quad d_1, d_2 \mid \frac{n^2+1}{2} \qquad d_1 + d_2 = n+k$

Cons. eq. del tipo

$$A\, d_1 d_2 = (d_1 + d_2 - k)^2 + 1$$

$$A\, xy = (x+y-k)^2 + 1$$

$$(x,y) \to (x, y') \to (x', y') \to (x', y'') \ldots$$

Cerco A in modo che ci sia una soluzione $(x,y) \stackrel{!}{=} (1,1)$

$$A \cdot 1 \cdot 1 = (1+1-k)^2 + 1 = (k-2)^2 + 1$$

$$\left((k-2)^2+1\right) \underline{xy} = \underbrace{(x+y-k)^2+1}_{n^2+1}$$

Considero l'equazione data come eq. di 2° grado nella x.

Diventa

$$x^2 - \left[(k-1)(k-3)y + 2k\right]x + (y-k)^2 + 1 = 0$$

(x,y) sol $\Rightarrow (x', y)$ sol $\qquad$ WLOG $x \leq y$

$$x' = (k-1)(k-3)y + 2k - x$$

$$x' \geq 4 \cdot 2 \cdot y + 2k - x > y$$

DISPARI.

$$(x,y) \to (x_1, y) \to (x_1, y_1) \to (x_2, y_1)$$

Le soluzioni crescono

I numeri $x_i + y_i$ a un certo punto sono $> k$.

Pongo $n = x_i + y_i - k \qquad x_i y_i \mid n^2+1$

DISPARI $\qquad x_i y_i \mid \frac{n^2+1}{2}$

Le sol cercate sono

$d_1 = x_i$ $d_2 = y_i$ $d_1 d_2 \mid \frac{n^2+1}{2}$

$d_1 + d_2 = n + k$