Stage Senior 2018 – Livello Advanced

Stampato integrale delle lezioni

Autori vari

Indice

SENIOR 2018 – ALGEBRA – Advanced (Max)

Note Title 04/09/2018

Disequazioni funzionali

Idee che è utile provare (portarsi da casa)

1. Cercare di ottenere $f(x) \geq$ q.c.
   $f(x) \leq$ q.c. (possibilmente la stessa)

   (oss. le disug. classiche, con il verso invertito, producono uguaglianze)

2. Occhio ai segni quando si moltiplica / divide

3. Reiterare delle stime

4. Provare a dimostrare una tesi più forte.

5. Dare dei valori che permettano di semplificare 2 termini!

6. Vedere l'eq. funzionale come una diseq. nella "variabile" $f(x)$
   ⇝ comodo quando è di grado basso e non ci sono composizioni

7. Passare alcuni parametri al limite

8. Quando siamo su $\mathbb{N}$, ci sono i minimi!!

9. Guardare la CRESCITA

10. Pensare alla MONOTONIA

11. Situazione con
    $\geq$ su progr. geom.
    $\leq$ su progr. aritm.
    + monotonia

① $f:\mathbb{R}\to\mathbb{R}$ $\quad f(x+y)+f(y+z)+f(z+x)\geq 3f(x+2y+3z)$

② $f:\mathbb{R}\to\mathbb{R}$ $\quad f(xy)\leq x f(y)$

③ $f:[0,1]\to[0,+\infty)$ $\quad$ (i) $f(1)=1$

(ii) $f(x)+f(y)\leq f(x+y)$ quando poss.

Dimostrare che $f(x)\leq 2x$.

$\boxed{1}$ $P(0,0,0) \Rightarrow 3f(0)\geq 3f(0)$ ☺

$P(x,0,0) \Rightarrow 2f(x)+f(0)\geq 3f(x) \rightsquigarrow f(x)\leq f(0)$

$P(x,x,-x) \Rightarrow f(2x)+2f(0)\geq 3f(0) \rightsquigarrow f(2x)\geq f(0)$

$\rightsquigarrow f(x)\geq f(0)$ ☺

Quindi solo le costanti

$\boxed{2}$ $P(x,1) \Rightarrow f(x)\leq x f(1) \qquad \forall x\in\mathbb{R}$

$P(\underbrace{\tfrac{1}{x},x}_{\text{occhio}}) \Rightarrow f(1)\leq \frac{1}{x}f(x) \underset{\text{ho usato } x>0}{\rightsquigarrow} f(x)\geq x f(1) \qquad \forall x>0$

Quindi $\exists\, a\in\mathbb{R}$ t.c. $f(x)=ax \qquad \forall x>0$

$P(\tfrac{1}{x},-x) \Rightarrow f(-1)\leq \frac{1}{x}f(-x) \rightsquigarrow f(-x)\geq x f(-1) \qquad \forall x>0$

$P(x,-1) \Rightarrow f(-x)\leq x f(-1) \qquad \forall x>0$

Quindi $\exists\, b\in\mathbb{R}$ t.c. $f(x)=bx \qquad \forall x<0$

Mancano : $\to f(0)$

$\to$ verifica

$P(x,0) \Rightarrow f(0)\leq x f(0)$ $\quad$ $x=2 \rightsquigarrow f(0)\geq 0$, $\quad x=0 \rightsquigarrow f(0)\leq 0$ $\quad \rightsquigarrow f(0)$

Ora occorre verificare che tutte le funzioni

$$f(x)=\begin{cases} ax & \text{se } x\geq 0\\ bx & \text{se } x\leq 0\end{cases}$$

vanno bene.

$x \geq 0 \quad y \geq 0 \quad$ ok

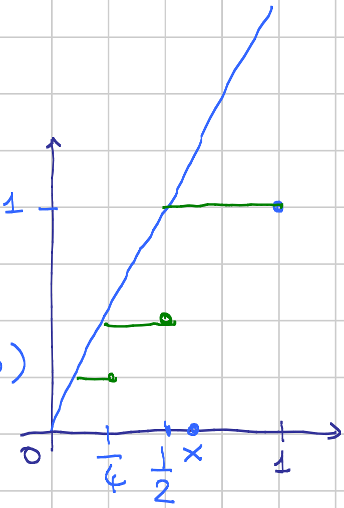
$x \leq 0 \quad y \leq 0 \quad axy \leq bxy \quad \rightsquigarrow \quad a \leq b \quad (xy \geq 0)$

$x > 0 \quad y < 0 \quad +bxy \leq +bxy \quad$ ok

$x < 0 \quad y > 0 \quad bxy \leq axy \quad \rightsquigarrow \quad b \geq a \quad (xy < 0)$

Quindi: serve $a \leq b$.

$\boxed{3}$ Procediamo per fasce



Prendo $x \in [\frac{1}{2}, 1]$ e dico che $f(x) \leq 1$

(se no uso $P(x, 1-x)$ e uso che $f(1-x) \geq 0$)

quindi ok in questa zona

Osservo che $f(\frac{1}{2}) \leq \frac{1}{2}$ (uso $P(\frac{1}{2}, \frac{1}{2})$)

Prendo $x \in [\frac{1}{4}, \frac{1}{2}]$ e dico che $f(x) \leq \frac{1}{2}$

(Come prima uso $P(x, \frac{1}{2} - x)$)

E così via per induzione usando $[\frac{1}{2^{k+1}}, \frac{1}{2^k}]$

④ $f: \mathbb{R} \to \mathbb{R} \quad y^2 f(x)(f(x)+2x) \leq 1 - x^2y^2$

⑤ $f: \mathbb{R} \to \mathbb{R} \quad f(xy) + f(x-y) \geq f(x+y)$

(1) esistono sol. non costanti

(2) $f(x) \geq 0 \quad \forall x \in \mathbb{R}$

⑥ $f: \mathbb{R} \to \mathbb{R} \quad f(x^3+x) \leq x \leq f(x)^3 + f(x)$.

$\boxed{5}$ Faccio in modo che $xy = x+y$ $\qquad y = \frac{x}{x-1}$

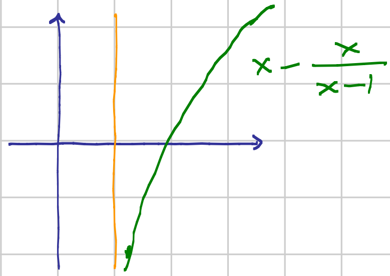
$$P\left(x, \frac{x}{x-1}\right) \Rightarrow f\left(\cancel{\frac{x^2}{x-1}}\right) + f\left(x - \frac{x}{x-1}\right) \geq f\left(\cancel{\frac{x^2}{x-1}}\right)$$

$$\leadsto f\left(\frac{x^2-2x}{x-1}\right) \geq 0 \qquad \forall x \neq 1$$

Spero che ogni $z \in \mathbb{R}$ si scriva come $\frac{x^2-2x}{x-1} = z$ con $x \neq 1$

Questo è un conto di eq. di 2° grado

Spero che ax^2 sia soluzione...



$$a x^2y^2 + \cancel{ax^2} + \cancel{ay^2} - 2axy \geq \cancel{ax^2} + \cancel{ay^2} + 2axy$$

$$a x^2y^2 - 4axy \geq 0$$

☹ Ritento $ax^2+b \leadsto ax^2y^2 - 4axy + b \geq 0$

Prendo $a=1$ e $b = 1000$ e ☺

$\boxed{4}$ Divido per y e faccio $y \to +\infty$

$$f(x)\,(f(x)+2x) \leq \underbrace{\boxed{\frac{1-x^2y^2}{y^2}}}_{\downarrow\, -x^2}$$

$$f(x)^2 + 2x f(x) + x^2 \leq 0 \qquad (f(x)+x)^2 \leq 0 \qquad ☺$$

$\boxed{6}$ Sia $\varphi(x) := x + x^3$. Questa è bigettiva come $f: \mathbb{R} \to \mathbb{R}$.

La sua inversa $\psi(x)$ è la soluzione.

Riscrivo il testo nella forma

$$f(\varphi(x)) \leq x \leq \varphi(f(x))$$

Applico ψ alla disug. di dx (posso perché è strett. cresc.)

$$\psi(x) \le \psi(\varphi(f(x))) = f(x)$$

Metto $\psi(x)$ al posto di x in quella di sx

$$f(x) = f(\varphi(\psi(x))) \le \psi(x)$$ ☺

— o — o —

⑦ $f : \mathbb{N} \to \mathbb{N}$ $\quad f(n+1) > f(f(n))$ (IMO 1977-6 ?)

L'unica sol. è $f(n) = n \quad \forall n \in \mathbb{N}$

$\boxed{\text{Dim 1}}$ Sia $n_0 \ge 0$ t.c. $f(n_0) = \min\{f(n) : n \ge 0\}$
p.to di min.

Dico che $n_0 = 0$
Se fosse $n_0 > 0$, allora

$P(n_0 - 1) \Rightarrow f(n_0) > f(\underbrace{f(n_0-1)}_{\ge 0}) \ge f(n_0)$ assurdo

Quindi $n_0 = 0$ e $f(n) \ge f(0) + 1 \quad \forall n \ge 1$

Sia $n_1 \ge 1$ t.c. $f(n_1) = \min\{f(n) : n \ge 1\}$

Dico che $n_1 = 1$.
Se fosse $n_1 > 1$, allora

$P(n_1 - 1) \Rightarrow f(n_1) > f(\underbrace{f(n_1-1)}_{\ge f(0)+1 \ge 1}) \ge f(n_1)$ assurdo

Quindi $n_1 = 1$ e $f(n) \ge f(1) + 1 \quad \forall n \ge 2$

Ora $P(0) \Rightarrow f(1) > f(f(0))$ Se $f(0) > 0$ sarebbero guai

Andando avanti con $n_2, n_3, \dots$ si ottiene la tesi

Esercizio Scrivere per bene che cosa si sta dimostrando per induzione.

$\boxed{\text{Dim 2}}$ Lemma Se $k \geq n$, allora $f(k) \geq n$

$\boxed{\text{Dim}}$ Per induzione $n=0$ è banale

$\boxed{n \Rightarrow n+1}$ Supponiamo $k \geq n+1$, cioè $k-1 \geq n$.

Allora per ipotesi $f(k-1) \geq n$ e ancora per ipotesi

$$f(k) > f(f(k-1)) \geq n$$

Quindi $f(k) \geq n+1$ ☺

Il vantaggio del lemma è che ora ho una affermazione a 2 parametri $Q(k,n)$

- $Q(n,n) \Rightarrow f(n) \geq n$

- $Q(f(n), f(n)) \Rightarrow f(f(n)) \geq f(n) \Rightarrow f(n+1) > f(n)$
  $\rightsquigarrow$ strett. crescente

- $f(n+1) > f(f(n)) +$ stretta crescenza $\rightsquigarrow n+1 > f(n)$

Fatto generale $f(a) > f(b)$ + f strett. cresc. $\rightsquigarrow a > b$

—o—o—

$\boxed{8}$ $f, g : \mathbb{N}_* \longrightarrow \mathbb{N}_*$

$$f^{(g(n)+1)}(n) + g^{(f(n))}(n) = f(n+1) - g(n+1) + 1$$

ordini di composizione

$$f(n+1) = f^{(\dots)}(n) + \underbrace{g^{(\dots)}(n)}_{\geq 1} + \underbrace{g(n+1) - 1}_{\geq 0} > f^{(\dots)}(n)$$

L'esercizio 7 si generalizza facilmente a

$f(n+1) > f^{(k)}(n)$ con $k \geq 2$ fisso

(stessa dim.)

ma anche a

$f(n+1) > f^{(k_n)}(n)$ con $k_n \geq 2$ succ. data

Una volta che uno sa che $f(n) = n$ si trova g facile.

— o — o —

$\boxed{9}$ $f: \mathbb{N} \to \mathbb{N}$ iniettiva $f(f(n)) \leq \dfrac{n+f(n)}{2}$

- Supponiamo per assurdo che $\exists\, n_0 \geq 1$ t.c. $f(n_0) < n_0$

$P(n_0) \Rightarrow f(f(n_0)) \leq \dfrac{n_0+f(n_0)}{2} < n_0$

Questa si itera producendo per induzione $f^{(k)}(n_0) < n_0$

$P(f(n_0)) \Rightarrow f^{(3)}(n_0) \leq \dfrac{f(n_0)+f^{(2)}(n_0)}{2} < n_0$ e così via...

Quindi ci sono $f^{(a)}(n_0) = f^{(b)}(n_0)$, mentre per iniettività dovrebbero essere tutti diversi.

- Supponiamo per assurdo che $\exists\, n_1 \geq 1$ t.c. $f(n_1) > n_1$. Allora

$$\underbrace{f(f(n_1))}_{n_0} \leq \frac{n_1+f(n_1)}{2} < \underbrace{f(n_1)}_{n_0}$$

e quindi siamo al caso precedente. ☺

(10) $f: \mathbb{R} \to \mathbb{R}$ $\quad f(x+y^2) \geq (y+1)\, f(x)^2$

(11) $f: (0,+\infty) \to (0,+\infty)$ $\quad f(x+y) \geq y f(x) + f(f(x))$

(12) $f: (0,+\infty) \to (0,+\infty)$ $\quad f(x+y) \geq f(x) + y f(f(x))$

(13) $f: \mathbb{R} \to \mathbb{R}$ stessa equ. di sopra $+$ $f(0) \geq 0$

(10) $P(x,0) \Rightarrow f(x) \geq f(x)^2 \Rightarrow f(x) \in [0,1]$

Supp. $f(x_0) > 0$, allora $P(x_0, y)$ con y enorme produce un assurdo.

(11) • $f(x+y) \geq y f(x)$ Fisso x e mando $y \to +\infty$
Ottengo $\lim_{y \to +\infty} f(y) = +\infty$

In realtà mi serve solo: $\exists\, x_0 > 0$ t.c. $f(x_0) \geq 8$

• $\exists\, x_1 \in \mathbb{R}$ t.c. $f(x_1) \geq 7 x_1$

Faccio $P(x_0, y)$ con y grande: $f(x_0+y) \geq y f(x_0) \geq 8y$

Mi basta $8y \geq 7(x_0+y)$ ← vera per y grande

• $P(x_1, \underbrace{f(x_1) - x_1}_{>0})$ e trovo un assurdo.

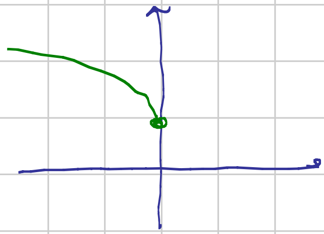
(12) Step 1 $\quad \lim_{x \to +\infty} f(x) = +\infty$ (come prima)

Step 2 $\quad \lim_{x \to +\infty} f(f(x)) = +\infty$ (facile conseguenza del prec.)

Da qui in poi è come prima: $\exists\, x_0 > 0$ t.c. $f(f(x_0)) \geq 8 \ldots$

(13) <u>Step 1</u> Se $\exists\, x_0 \in \mathbb{R}$ t.c. $f(f(x_0)) > 0$, allora è come prima.

<u>Step 2</u> Resta il caso $f(f(x)) \leq 0$ sempre, da cui segue f debolm. decr., quindi
$f(x) \geq 0$ per ogni $x \leq 0$



<u>Step 3</u> Qual è il segno per $x > 0$?
Se fosse $f(x) < 0$, allora $f(f(x)) \geq 0$
e quindi l'unica possibilità è che sia 0
Se è sempre $f(x) \geq 0$, allora $f(f(x)) \geq 0$.

<u>Step 4</u> Gestire bene il caso 0 ...

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

$$\boxed{y = f(x) - x} \rightsquigarrow \quad f(f(x)) \geq f(x) + (f(x)-x)\, f(f(x))$$

$$\underbrace{f(f(x))}_{+}\ \underbrace{(f(x)-x-1)}_{+} + \underbrace{f(x)}_{+} \leq 0$$

Sto usando che, assumendo $\exists\, x_0$ t.c. $f(f(x_0)) > 0$
deduco che
- $f(f(x)) > 0$ per x grande $(\to +\infty)$
- $f(x) > 0$ " " $(\to +\infty)$
- $f(x) > 7x$ per x grande

— o — o —

(14) $f : (0,+\infty) \to \mathbb{R}$ (i) $f(x) + f(y) \leq \dfrac{f(x+y)}{2}$

(ii) $\dfrac{f(x)}{x} + \dfrac{f(y)}{y} \geq \dfrac{f(x+y)}{x+y}$

__Step 1__ $P(x,x) \Longrightarrow \quad f(2x) = 4f(x)$

__Step 2__ Iterazione $\Longrightarrow \quad f(2^k x) = 4^k f(x)$

__Step 3__ Provo $f(x) = a x^2 \rightsquigarrow$ la (ii) è gratis, la (i) viene

$$a(x^2+y^2) \leq \frac{1}{2} a (x+y)^2 = \frac{1}{2} a x^2 + \frac{1}{2} a y^2 + a xy$$

$$a (x^2+y^2) \leq 2a\, xy$$

Ok se $a \leq 0$. Quindi $f(x) = ax^2$ con $a \leq 0$ è Ok.

__Step 4__ Cambio variabili $f(x) = -x g(x)$.
Nella variabile $g(x)$ l'eq. diventa

$$g(x) + g(y) \leq g(x+y) \qquad x g(x) + y g(y) \geq \frac{x+y}{2} g(x+y)$$

__Step 5__ Spero $g(x) \nearrow$:

$$x g(x) + y g(y) \geq \frac{x+y}{2} g(x+y) \geq \frac{x+y}{2} (g(x) + g(y))$$

$$2x g(x) + 2y g(y) \geq \cancel{x g(x)} + \cancel{y g(y)} + x g(y) + y g(x)$$

$$x (g(x) - g(y)) - y (g(x) - g(y)) \geq 0$$

$$(x-y)(g(x) - g(y)) \geq 0 \rightsquigarrow \text{monotonia crescente deb.}$$

__Step 6__ $g(2^k x) = 2^k g(x)$ come prima

__Step 7__ $g(mx) \geq m\, g(x)$ iterando la prima

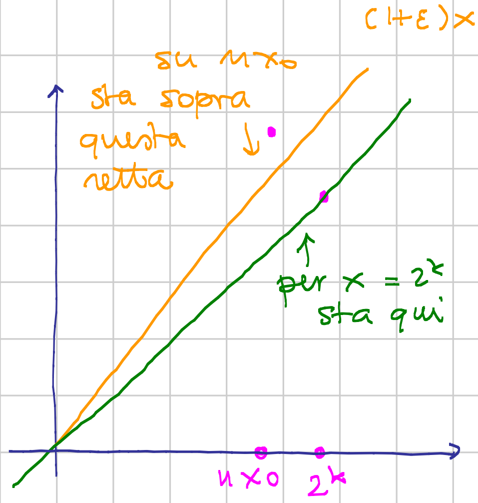
__Step 8__ Se serve, posso assumere $g(1) = 1$.

Step 9

$$\left.\begin{array}{l} g(nx) \geq n\, g(x) \\ g(2^k x) = 2^k g(x) \\ \text{monotona} \end{array}\right\} \Rightarrow \text{linearità}$$

Supponiamo $g(1) = 1$ e per assurdo $\exists\, x_0 > 0$ t.c.

$$g(x_0) = (1+\varepsilon)\, x_0$$



Vorremmo trovare n e k tali che

$$n x_0 < 2^k \quad \text{ma} \quad n(1+\varepsilon) x_0 > 2^k$$

cioè

$$\frac{2^k}{(1+\varepsilon) x_0} < n < \frac{2^k}{x_0}$$

quindi mi serve che esista un intero fra

$$\frac{2^k}{(1+\varepsilon) x_0} \quad \text{e} \quad \frac{2^k}{x_0}$$

Questo è possibile perché la lungh. dell'intervallo raddoppia passando da k a $k+1$

Step 10 Come concludere

Modo 1 Al passaggio prec. abbiamo ottenuto $g(x) \leq x$ supponendo $g(1) = 1$. In realtà abbiamo ottenuto

$$g(x) \leq g(1)\, x$$

o ancora più in generale

$$g(x) \leq g(x_0)\, \frac{x}{x_0}$$

Questa deve valere per ogni $x > 0$ e ogni $x_0 > 0$

Basta dividere

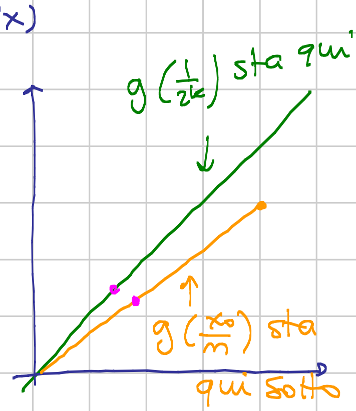
$$\frac{g(x)}{x} \leq \frac{g(x_0)}{x_0}$$

e scambiare x e x_0

<u>Modo 2</u> Reitero verso 0, cioè uso

$$g\left(\frac{1}{2^k}\right) = \frac{1}{2^k} \quad \text{e} \quad g\left(\frac{x}{m}\right) \leq \frac{1}{m}\, g(x)$$

e ora sono dalla parte giusta



— o — o —

$\boxed{\text{IMO } 2011-3}$ $f : \mathbb{R} \to \mathbb{R}$ $f(x+y) \leq y f(x) + f(f(x))$

Tesi: $f(x) = 0$ $\forall x \leq 0$

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

(i) $f(x) f(y) \geq f(xy)$

(ii) $f(x) + f(y) \leq f(x+y)$

(iii) $\exists\, a > 1$ t.c. $f(a) = a$

$\boxed{\text{CARINO}}$ $f : (0, +\infty) \to (0, +\infty)$ $f(x)^2 \geq f(x+y)\,(f(x) + y)$

$\boxed{2011}$

Step 1 Supponiamo $\exists\, x_0 \in \mathbb{R}$ t.c. $f(x_0) > 0$.

Allora $P(x_0, y)$ e $y \to -\infty$ $\Rightarrow$ $\lim\limits_{y \to -\infty} f(y) = -\infty$

$\Rightarrow \lim\limits_{x \to -\infty} f(f(x)) = -\infty$

Ma allora $P(-x, x)$: $f(0) \leq x f(-x) + f(f(-x))$

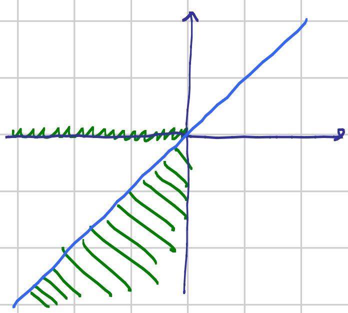
Mando $x \to +\infty$ ed è un guaio.

Conclusione $f(x) \leq 0$ per ogni $x \in \mathbb{R}$.

Step 2 $P(x, f(x) - x) \Rightarrow$ $0 \leq (f(x) - x) f(x)$

Per $x < 0$ $\nearrow f(x) = 0$

$\searrow f(x) \leq x$



Step 3

$P(x, -x) \Rightarrow f(0) \leq \overset{+}{-x f(x)} + \overset{\leq 0}{f(f(x))}$

Prendo x molto negativo

se $f(x) \neq 0$, questo è un numero negativo di val. assol. $\geq x^2$ $\leadsto$ guaio

quindi $f(x) = 0$ per ogni x abbastanza negativo

Step 4 $\quad f(0)=0$

$P(x,x) \Rightarrow \quad \underset{\overset{\shortparallel}{0}}{f(2x)} \leq x\,\underset{\overset{\shortparallel}{0}}{f(x)} + \underset{f(0)}{f(f(x))} \qquad x$ molto neg.

Step 5 $\quad$ Supponiamo $\exists\, x_0 < 0$ t.c. $f(x_0) < 0$

$P(x_0,-x_0) \Rightarrow \quad 0 = f(0) \leq -x_0 f(x_0) + f(f(x_0)) \leq \underset{+}{-x_0}\, \underset{-}{f(x_0)}$

FINE.

— o — o —

$\boxed{2013}$

Step 1 $\quad$ Iterazioni: $\quad f(x^k) \leq f(x)^k$
$\qquad f(nx) \geq n f(x)$

Step 2 $\quad f(1) \geq 1 \qquad P(1,a) \Rightarrow \quad f(1)\,\underset{\overset{\shortparallel}{a}}{f(a)} \geq \underset{\overset{\shortparallel}{a}}{f(a)}$

$f(n) \geq n$

Step 3 $\quad f\left(\frac{p}{q}\right) \geq 0$ sempre $\qquad \leadsto$ MONOTONIA

$f\left(\underset{+}{q \cdot \frac{p}{q}}\right) \leq \underset{+}{f(q)} \cdot f\left(\frac{p}{q}\right)$

perché sono interi

Step 4 $\quad$ Monotonia + $f(nx_0) \geq n f(x_0)$ + $f(a^k) \leq a^k$
$\leadsto$ solito trucco $\leadsto$ $f(x) \leq x$ per $x \geq 1$

Step 5 $\quad$ In maniera analoga all'esempio analogo
si ottiene pure $f(x) \geq x$.

Senior 2018 - C1 Advanced - Aner

Titolo nota 03/09/2018

Problemi con punti nel piano (Comb./Geom.)

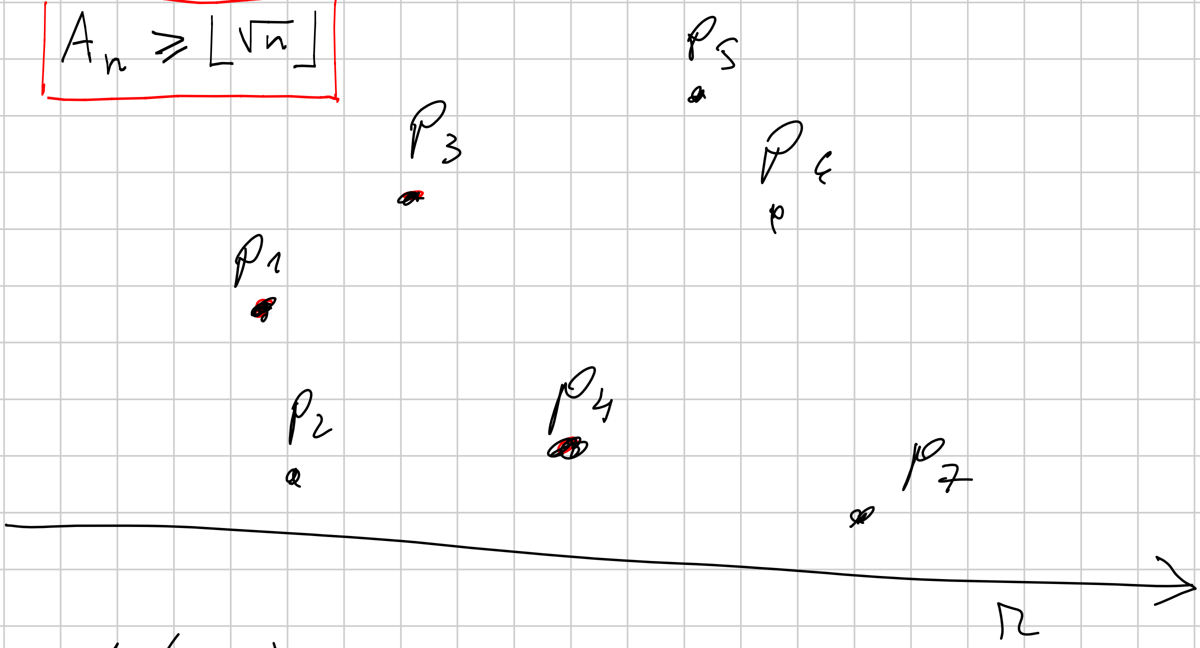
Problema Se prendo n punti nel piano $P_1 \dots P_n$, quante distanze vedo come minimo?

$$\min_{\text{conf di } n \text{ punti}} \left| \left\{ \overline{P_i P_j} \mid i \neq j \right\} \right| = A_n = ?$$

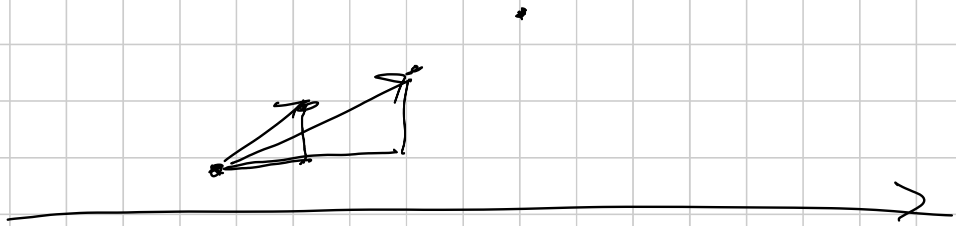
Esempio: se gli n punti sono $(1,0)\ (2,0) \dots (n,0)$

Vediamo $(n-1)$ distanze diverse

$$\boxed{A_n \geq \lfloor \sqrt{n} \rfloor}$$



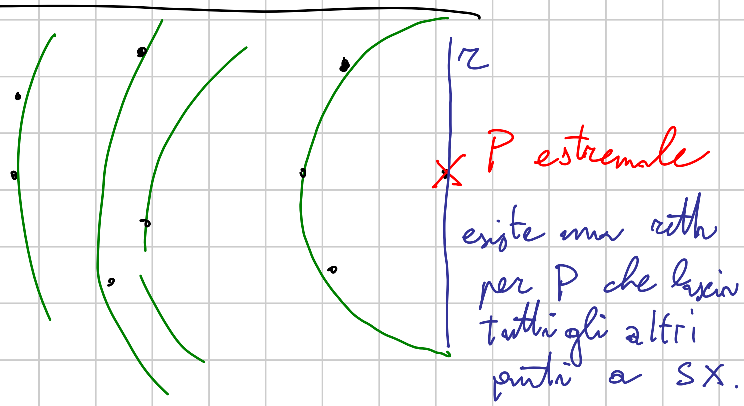
$d(p_i)$ = distanza tra p_i e r



Dilworth: data una stringa di n reali distinti riesco a trovare una sottostringa monotona di almeno $\lceil \sqrt{n} \rceil - 1$

$$\lceil \sqrt{n} \rceil - 2$$

Altra strategia



Traccio tutte le cfr centrate in P passanti per gli altri punti.

Se ci sono $\geq \lfloor \sqrt{n} \rfloor$ cfr. abbiamo vinto.

Se ci sono $\leq \lfloor \sqrt{n} \rfloor - 1$ cfr., una contiene almeno

$$\frac{n-1}{\lfloor \sqrt{n} \rfloor - 1} \geq \frac{n-1}{\sqrt{n}-1} = \sqrt{n}+1 \geq \lfloor \sqrt{n} \rfloor + 1$$

sono tutti sulla stessa semicirconferenza

Teo Se ho numeri reali $x_1, \dots, x_{ab+1}$ tutti distinti, c'è una sottosucc. lunga $(a+1)$ crescente o una lunga $(b+1)$ decrescente. $a, b \geq 0$

Dim Induzione su b. $\boxed{b=0}$ x_1 è una sottosucc. decr. lunga 1 ✓

Passo induttivo $b \rightsquigarrow b+1$

Voglio trovare in $x_1 \dots x_{ab+a+1}$ una $(a+1)$ crescente o una $(b+2)$ decrescente

$\underbrace{x_1\, \dots\, \cancel{x_{k_1}}\, x_{ab+1}}$ $\dots$ x_{ab+a+1}

qui trovo una $(b+1)$ decrescente

$\underbrace{x_1 \dots \cancel{x_k}\ \cancel{x_{k_2}}\ x_{ab+2}}$

qui trovo una $(b+1)$ decrescente

Trovo $a+1$ succ. lunghe $(b+1)$ decrescenti, tutte con ultimi termini diversi tra loro

Considero la succ. $x_{k_1}, \dots, x_{k_{a+1}}$.

Se sono sfortunato, non è crescente, ma allora $\exists$ $x_{k_h} > x_{k_{h+1}}$, ma allora la succ. lunga $b+1$ che termina in x_{k_h} può essere allungata $\square$

Problema un po' più difficile $k \geq 3$. n punti nel piano, no k allineati. Quante distanze almeno?

Sia ℓ il n° di distanze che occorrono.

Contiamo i triangoli isosceli: sono al più $\binom{n}{2} \cdot (k-1)$:

infatti ogni coppia di pti la uso al max $(k-1)$ volte come base.

$d_1 \dots d_\ell$ distanze che occorrono. x_{ij} = n° di pti a distanza d_j da P_i, $j \le \ell$, $i \le n$.

$$\forall i \quad \sum_{j=1}^{\ell} x_{ij} = n-1$$

$$(k-1)\binom{n}{2} = (k-1)\frac{\cancel{n}(n-1)}{\cancel{2}}$$

$$\geq$$

$$\sum_{i,j}\binom{x_{ij}}{2} \textcolor{red}{= \text{n° tr. isosceli}} \underset{\text{Jensen}}{\geq} \cancel{\ell}\cdot\cancel{n}\,\frac{\left[\cancel{(n-1)/\ell}\right]\left[(n-1)/\ell - 1\right]}{\cancel{2}}$$

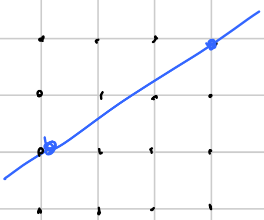
$$\boxed{\frac{x^2-x}{2} \text{ è convessa}}$$

$$(k-1) \geq \frac{n-1}{\ell} - 1$$

$$\boxed{\ell \geq \frac{n-1}{k}} \text{ lineare in } n$$

Per $n = k^2$ ho la configurazione $\{1, \dots, k\} \times \{1, \dots, k\}$

In questa conf. quante distanze vedo? Tante quanti gli interi $1 \le m \le 2n$ che si possono scrivere come somma di due quadrati. Quali interi positivi che si scrivono come somma di 2 quadrati?



$$1 \le h \le 2n$$

$$h = 2^{\alpha} \cdot p_1^{\alpha_1} \cdots p_r^{\alpha_r} \cdot q_1^{\beta_1} \cdots q_s^{\beta_s} \quad \text{con } p_i \equiv 1 \pmod 4 \text{ e } q_i \equiv 3 \pmod 4.$$

Allora $h = x^2 + y^2$ se e solo se tutti i β_i sono pari

Non abbiamo ottenuto tutti i numeri da 1 a $2n$!

Esempio non ho i $\equiv 3, 6 \pmod 9$. $\rightsquigarrow$ ho al

max $2n \cdot \left(1 - \frac{3-1}{3^2}\right)$. Analogamente per il 7, l'11...

Su larghe scale ho al massimo

$$\underbrace{2n \cdot \left(1 - \frac{3-1}{3^2}\right)\left(1 - \frac{7-1}{7^2}\right)\left(1 - \frac{11-1}{11^2}\right) \cdots \left(1 - \frac{p-1}{p^2}\right)}_{\text{diventa piccolo a piacere!}}$$

Problema aperto capire con che velocità cresce davvero

$$\lfloor \sqrt{n} \rfloor < A_n < \frac{C \cdot n}{\log n}$$ per qualche C positivo

---

Happy ending theorem (Paul Erdős - George Szekeres, 1935)

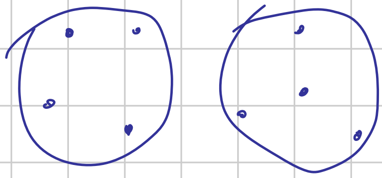
Per ogni $K \geq 2$ esiste un N abbastanza grande $\left(N = \binom{2k-4}{k-2} + 1 \text{ basta} \right)$ per cui comunque si prendano N punti nel piano, a 3 a 3 non allineati, ne esistono K che formano un poligono convesso.

Caso particolare $K=4$ (Esther Klein, 1933)

Per $K=4$ basta $N=5$.

Da questo segue in realtà il teorema per k generico: prendiamo N punti nel piano e associamo a ogni quaterna $\{P, Q, R, S\}$ un colore scelto tra 2 colori $\{\text{conv.}, \text{conc.}\}$

P,Q,R,S convessi   P,Q,R,S concavo



Ramsey ci dice che se N è molto grande rispetto ai parametri (K, h, s) (5, 4) se coloro le s-uple di un insieme U di N elementi con 2 colori, allora esiste un $A \subseteq U$ con $|A| = K$ e A monocromatico conv.
oppure $B \subseteq U$ $|B| = h$ B mocrom. conc.

Da qui segue H.E.T. (con una stima peggiore): per N grande trovo o 5 punti con tutte le quaterne concave (assurdo), o K punti con tutte le quaterne convesse $\rightsquigarrow$ K-agono convesso.

H.E.T. si chiama così perché Klein pose il problema generale, Szekeres lo risolse, i due si sposarono, Erdős diede questo nome al teorema.

Prendo N punti nel piano. Fisso le coordinate cartesiane in modo che tutte le ascisse siano diverse e tutte le ordinate siano diverse. $\underbrace{(x_1, y_1)}_{P_1}, \ldots \underbrace{(x_N, y_N)}_{P_N}$

con $x_1 < x_2 < \ldots < x_N$.

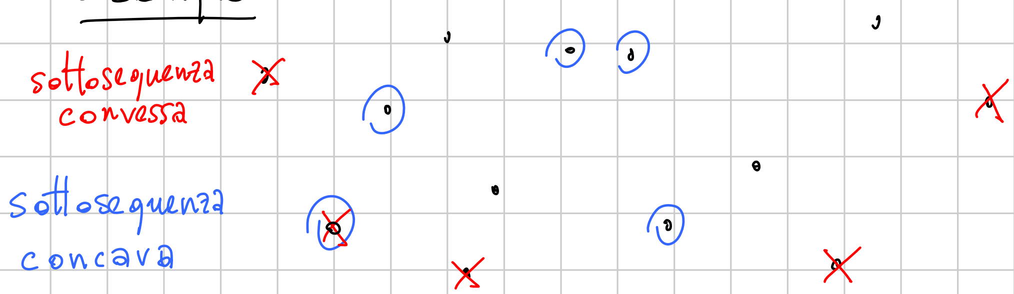
Diciamo che una sottosequenza $P_{i_1}\ P_{i_2}\ ,\dots\ P_{i_h}$

$(i_1 < \dots < i_h)$ è <u>convessa</u> se i rapporti incrementali sono crescenti.

$$\frac{y_{i_2}-y_{i_1}}{x_{i_2}-x_{i_1}} < \frac{y_{i_3}-y_{i_2}}{x_{i_3}-x_{i_2}} < \dots < \frac{y_{i_h}-y_{i_{h-1}}}{x_{i_h}-x_{i_{h-1}}}$$

è <u>concava</u> se i rapp. incr. sono decresenti.

<u>Esempio</u>



<u>Entrambe generano nel piano</u> un poligono convesso

$ES(k,h)$ è un numero N abb. grande tale che

$\forall N$ punti $P_1=(x_1,y_1)\dots\ P_N=(x_N,y_N)$ esiste una k-sottosequenza convessa, o una h-sottoseq. concava.

<u>Tesi</u> $ES(k,h)$ esiste $\left(\leq \binom{k+h-4}{k-2}+1 \right)$

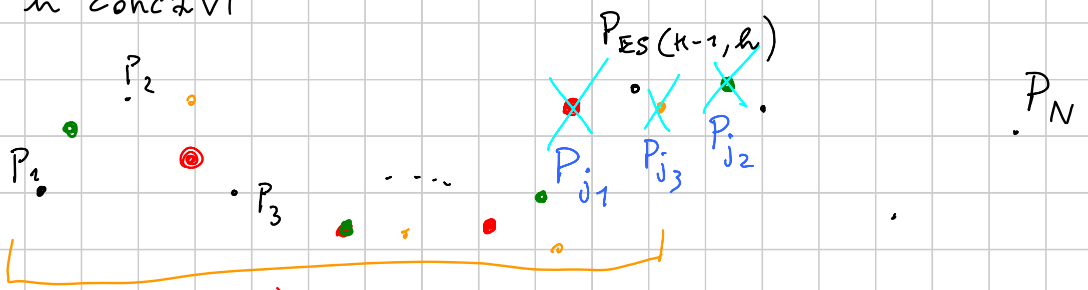
Induzione su k e h (<u>induzione su $k+h$</u>, <u>induzione su h</u>..)

<u>Passo base</u> $h=2$, k qualsiasi.

Bastano 2 punti: fanno sempre una 2-sequenza concava!

$$\binom{k+2-4}{k-2}+1=2$$

Passo induttivo Prendiamo $N = ES(k-1,h) + ES(k,h-1) - 1$ punti nel piano. Voglio trovarne k convessi o h concavi



trovo $(k-1)$ convessi

trovo $(k-1)$ convessi

trovo $(k-1)$ conv.

$\boxed{\text{Non assumo che } x_{j_1} < x_{j_2} < \dots}$

Trovo un insieme $P_{j_1} \dots P_{ES(k,h-1)}$ punti, tutti questi sono al termine di una $(k-1)$-seq. convessa.

Tra questi ci sono o una k seq. convessa (caso fortunato), oppure una $(h-1)$ seq. concava.

$k-1$ seq. convessa

$h-1$ seq. concava

La lotta tra i due rapporti incrementali determina se c'è una k-seq. convessa o una h-seq. concava

$ES(k,h)$ possiamo prenderlo pari a

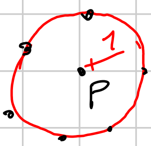
$$ES(k-1,h)+ES(k,h-1)-1 = \binom{k-1+h-4}{k-1-2}+1$$
$$+\binom{k+h-1-4}{k-2}+\cancel{1} \quad -\cancel{1} = \binom{k+h-4}{k-2}+1$$

Problemi per la pausa

1. $n \geq 3$ punti nel piano. La minima distanza tra 2 punti è 1. Allora ci sono non più di $3n-6$ coppie a distanza 1

2.
   - Dim. che esistono ∞ punti del piano a distanze $\in \mathbb{Q}$, non tutti allineati
   - Dim. che // ∞ punti, distanze $\in \mathbb{Q}$, a 3 a 3 non allineati
   - Dim. che se ∞ punti del piano hanno tutte distanze $\in \mathbb{N}$, allora sono tutti allineati.

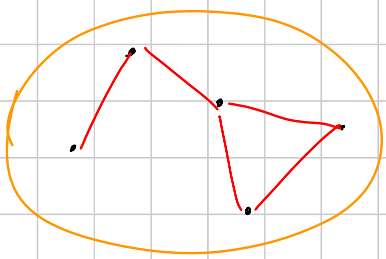
1. •



Ci sono ≤ 6 punti a distanza 1 da P (altrimenti 1 non è la min. distanza).

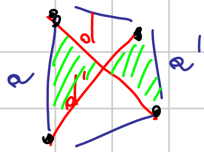
\# coppie ordinate a distanza 1 $\leq 6n$

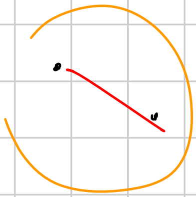
\# // non ord. // // $\leq 3n$

• 

Se colleghiamo i punti a distanza 1 con dei segmenti otteniamo un grafo planare.
Non ho

$d+d' > a+a'$



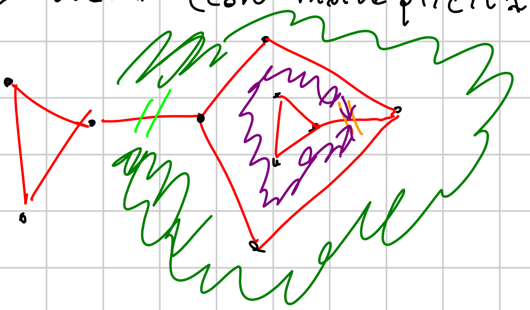


È connesso il grafo? Se non lo è avvicino q.b. le componenti connesse.

wlog
$\rightsquigarrow$ connesso

• $F+V-S=2$ Eulero

• A meno che il grafo non sia •—• ($n=2$, quindi supponiamo solo $n \geq 3$) ogni faccia tocca (con molteplicità) almeno 3 lati.



$$\boxed{3F \leq 2S}$$

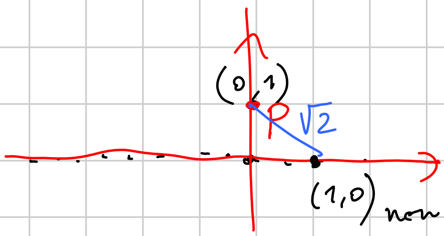
$F \leq \frac{2}{3} S$ $\qquad \frac{2}{3} S + V - S \geq 2$

$-\frac{1}{3} S + n - 2 \geq 0$ $\qquad S \leq 3n - 6$

□

2 • .. tutti i pti della forma $(u,0)$ con $u \in \mathbb{Q}$

Provo ad aggiungere $P=(0,1)$.



non va più bene.

Ci sono punti $(u,0)$ che continuano ad andare bene? Vogliamo $\boxed{1+u^2=v^2}$ per $v \in \mathbb{Q}$.
Questo capita ∞ volte. ha ∞ soluzioni in $\mathbb{Q}$.

- Invertiamo in P con raggio 1.

Q e R due pti qualsiasi della forma $(u,0)$, $(u',0)$ con u, u' buoni. $\overline{QR} \in \mathbb{Q}$ $\overline{PR} \in \mathbb{Q}$ $\overline{PQ} \in \mathbb{Q}$.

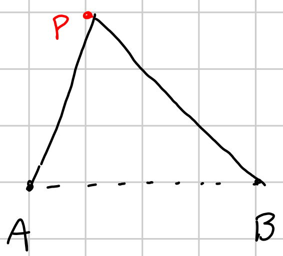
$Q \rightsquigarrow Q'$ $R \rightsquigarrow R'$

$$\overline{Q'R'} = \frac{\overline{QR} \cdot 1^2}{\overline{PQ} \cdot \overline{PR}} \in \mathbb{Q}$$

. I pti $Q'R'$, e gli altri .... si trovano su una circonferenza (a 3 a 3 non allineati)

- Non esistono ∞ punti a distanza intera (non tutti allineati)

Prendiamo 3 pti non allineati A, B, C a distanza intera. Quanti punti (e dove) posso aggiungere?



$\overline{PA}, \overline{PB} \in \mathbb{N}$

$\overline{PA} - \overline{PB}$ è intero

$$\underbrace{-\overline{AB} \le \overline{PA} - \overline{PB} \le \overline{AB}}_{\text{Fissati A e B, ho finiti valori possibili.}}$$

Se fisso $\lambda \in [-\overline{AB}, \overline{AB}]$, il luogo dei pti P con $\overline{PA} - \overline{PB} = \lambda$ è un ramo di iperbole

($\lambda = 0$ viene l'asse di AB, $\lambda = \pm \overline{AB}$ viene una semiretta)

Tutti i punti P della collezione giacciono su una tra $(2\overline{AB}+1)$ curve (rami di iperbole o rette).

Idem per B e C, ogni P giace su una tra $2\overline{BC}+1$ curve determinate da B e C.

Un'iperbole (retta) con asse focale $= AB$ non può coincidere con un'iperbole/retta con asse focale $= BC$.

(Per una retta, nel caso dell'asse prendo la perp., nel caso sia una semiretta, prendo la retta a cui appartiene).

Supponiamo che $AB \not\perp BC$ (altrimenti uso AC)

Se ho n punti nel piano, ci sono $\lesssim n^{3/2}$ coppie a distanza 1 ($\lesssim$ vuol dire $\leq$ a meno di piccole perturbazioni del RHS che vi lascio per esercizio).

$x_i = n°$ di pti a distanza 1 da P_i

$\{P_1 \ldots P_n\}$. wlog $x_1 \geq x_2 \geq \ldots \geq x_n$.

Siamo interessati a disuguaglianze del tipo

$$\sum_{i=1}^{n} x_i \leq \, ?$$

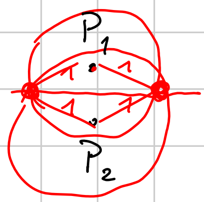
Scegliamo j tra 1 e n

$$\sum_{i=1}^{j} x_i \le n + 2\binom{j}{2}$$

$$\sum_{i=1}^{j} \underbrace{\left[x_i - (2i-2)\right]}_{\ge} \le n$$

n° di pti P_h per cui i è il minimo indice ℓ per cui $\overline{P_h P_\ell} = 1$

$$x_1 + \underbrace{(x_2 - 2)}_{\ge} + \underbrace{(x_3 - 4)}_{\ge}$$



pti a distanza 1 da P_1

pti a dist. 1 da P_2 ma non da P_1

pti a dist. 1 da P_3 ma non da P_1 né da P_2

Fisso $j \simeq \sqrt{n}$

$$\sum_{i=1}^{j} x_i \le n + 2\binom{j}{2} \simeq n + 2\,\frac{\sqrt{n}\,(\sqrt{n}-1)}{2}$$

$$= 2n - \sqrt{n} \simeq 2n$$

$$x_j \le \frac{2n}{j} \simeq 2\sqrt{n}\,.$$

$$\sum_{i=j+1}^{n} x_i \le 2\sqrt{n}\cdot\left(n - \sqrt{n}\right) = \boxed{2n^{3/2} - 2n}$$

$$\square + \bigcirc = 2n^{3/2}$$

Quindi $\sum_{i=1}^{n} x_i \lesssim 2n^{3/2}$

$\parallel$

$2(\#\text{coppie a distanza } 1)$

C2 Advanced LucaMac

Titolo nota 07/09/2018

Metodo Probabilistico

Cosa è una variabile aleatoria?

"È una cosa che prende un po' di valori con un po' di probabilità"

Esempio: Se prendiamo un dado non truccato e chiamo D_6 la variabile aleatoria relativa
$\forall k \in \{1, \dots, 6\}$ vale $\mathbb{P}(D_6 = k) = 1/6$

Supponiamo che i nostri valori siano in $\mathbb{N}$. Sia X v.a.
Dunque $\sum_{n=0}^{\infty} \mathbb{P}(X=n) = \sum_{n\in\mathbb{N}}' \mathbb{P}(X=n) = 1$

oss: possono anche essere tutti >0. (Ad esempio $\mathbb{P}(X=n) = \frac{1}{2^{n+1}}$ oppure $\mathbb{P}(Y=n) = \frac{1}{(n+1)^2} \cdot \frac{6}{\pi^2}$).

oss2: Una condizione necessaria è $\lim_{n\to+\infty} \mathbb{P}(X=n) = 0$

oss3 (che doveva essere la prima) $\mathbb{P}(X=n) \in [0,1]$ $\forall n \in \mathbb{N}$

oss4: Dato $A \subseteq \mathbb{N}$ vale $\mathbb{P}(X \in A) = \sum_{n\in A}' \mathbb{P}(X=n)$

Esempio: consideriamo la X di oss1. E voglio $\mathbb{P}(X \in \{\text{numeri pari}\}) =$
$= \sum_{n\in\mathbb{N}}' \mathbb{P}(X=2n) = \sum_{n\in\mathbb{N}} \frac{1}{2\cdot 4^n} = \frac{1}{2} \cdot \frac{1}{1-\frac{1}{4}} = \frac{2}{3}$ (<1 ☺)

Def: Data X variabile aleatoria definisco il suo valore atteso come
$$\mathbb{E}[X] = \sum_{n\in\mathbb{N}}' n\,\mathbb{P}(X=n) \in [0, +\infty]$$ c'è $+\infty$

OSS: se $X \leq \text{cost} \Rightarrow \mathbb{E}[X] \leq \text{cost}\ (< +\infty)$

Esempio stupido: $\mathbb{E}[D_6] = \frac{1}{6}\sum_{n=1}^{6} n = \frac{7}{2} = 3.5$

OSS: se $X \geq Y$ v.a. $\Rightarrow \mathbb{E}[X] \geq \mathbb{E}[Y]$

Esempio concreto: Lancio due dadi Y = primo valore X = somma dei valori

$X \geq Y \Rightarrow \mathbb{E}[X] \geq \mathbb{E}[Y]$

(Per fare OSS serve la "vera" definizione di $X : \Omega \to \mathbb{N}$)

—o—o—

Indipendenza di 2 v.a.

Intuitivamente è $\forall n, k \in \mathbb{N}$ $\mathbb{P}(X = n \mid Y = k) = \mathbb{P}(X = n)$

Ovvero il valore di Y non cambia la distribuzione di X.

Formalmente è $\forall A, B \subseteq \mathbb{N}$ $\mathbb{P}(X \in A, Y \in B) = \mathbb{P}(X \in A)\mathbb{P}(Y \in B)$

OSS: $\mathbb{P}(X \in A \mid Y \in B) = \dfrac{\mathbb{P}(X \in A, Y \in B)}{\mathbb{P}(Y \in B)}$

Quindi X, Y indipendenti $\iff \forall A, B \subseteq \mathbb{N}$ $\mathbb{P}(X \in A \mid Y \in B) = \mathbb{P}(X \in A)$.

Lemma:

Se X ed Y sono indipendenti $\Rightarrow \mathbb{E}[X+Y] = \mathbb{E}[X] + \mathbb{E}[Y]$

Dim: Facile.

Lemma più figo: $\mathbb{E}[X+Y] = \mathbb{E}[X] + \mathbb{E}[Y]$

Cosa vuol dire $X+Y$?

Diamo la definizione "vera". (con un errore)

X è una v.a. se è una funzione $X : \Omega \to \mathbb{N}$

$X(\omega) \in A \iff \omega \in X^{-1}(A)$

(Se $f : A \to B$ e $C \subseteq B$ $f^{-1}(C) = \{a \in A : f(a) \in C\}$)

Allora $(X+Y)(\omega) := X(\omega) + Y(\omega)$.

"Dim Lemma + fig 2"

$$\mathbb{E}[X+Y]=\sum_{n=0}^{\infty}{}' n\,\mathbb{P}(X+Y=n)=\sum_{n=0}^{\infty}{}'\sum_{k=0}^{n}{}' n\,\mathbb{P}(X=k,Y=n-k)=$$

$$=\sum_{n=0}^{\infty}{}'\sum_{k=0}^{n}{}' n\,\mathbb{P}(X=k)\cdot\mathbb{P}(Y=n-k\mid X=k)\underset{\text{tutto}\geq 0}{=}\sum_{k=0}^{\infty}{}'\sum_{n=k}^{\infty}{}' n\,\mathbb{P}(X=k)\cdot\mathbb{P}(Y=n-k\mid X=k)=$$

$m=n-k$

$$=\sum_{k=0}^{\infty}{}'\sum_{m=0}^{\infty}{}'(m+k)\,\mathbb{P}(X=k)\,\mathbb{P}(Y=m\mid X=k)=\sum_{m=0}^{\infty}{}'\sum_{k=0}^{\infty}{}'(m+k)\,\mathbb{P}(X=k)\cdot\mathbb{P}(Y=m\mid X=k)=$$

$$=\sum_{m=0}^{\infty}{}'\Big(m\underbrace{\sum_{k=0}^{\infty}{}'\mathbb{P}(X=k)\cdot\mathbb{P}(Y=m\mid X=k)}_{\mathbb{P}(Y=m)}\Big)+\sum_{k=0}^{\infty}{}'\Big(k\,\mathbb{P}(X=k)\underbrace{\sum_{m=0}^{\infty}{}'\mathbb{P}(Y=m\mid X=k)}_{1}\Big)=$$

$$=\sum_{m=0}^{\infty}{}' m\,\mathbb{P}(Y=m)+\sum_{k=0}^{\infty}{}' k\,\mathbb{P}(X=k)=\mathbb{E}[X]+\mathbb{E}[Y]$$

Tutto quello che abbiamo fatto funziona in modo analogo se al posto di $\mathbb{N}$ ci metto un qualunque $A\subseteq\mathbb{R}_{\geq 0}$ numerabile.

Disuguaglianza di Markov

Se $X\geq 0$ v.a. e $c>0$. Allora

$$\mathbb{P}(X\geq c)\leq\frac{\mathbb{E}[X]}{c}$$

Dim: $I_{\{X\geq c\}}=\begin{cases}1 & \text{se } X\geq c\\ 0 & \text{se } X<c\end{cases}$

Vale $c\,I_{\{X\geq c\}}\leq X$ perché $\begin{cases} X\geq c \to X\geq c\\ X<c \to X\geq 0\end{cases}$

Allora $\mathbb{E}[X]\geq\mathbb{E}[c\,I_{\{X\geq c\}}]=c\cdot\mathbb{P}(X\geq c)+0\cdot\mathbb{P}(X<c)=c\,\mathbb{P}(X\geq c)$

$$\Rightarrow \mathbb{P}(X\geq c)\leq\frac{\mathbb{E}[X]}{c}$$

Def: Si dice Varianza di X $\quad \mathrm{Var}(X):=\mathbb{E}[\,|X-\mathbb{E}[X]|^2]=\mathbb{E}[X^2]-\mathbb{E}[X]^2$

$LHS=\mathbb{E}[X^2]-\cancel{2}\,\mathbb{E}[X]^2+\cancel{\mathbb{E}[X]^2}$

Disuguaglianza di Chebishev

X v.a. (ma consideriamo ancora $X \geq 0$) e $c > 0$

$$\mathbb{P}(|X - \mathbb{E}[X]| \geq c) \leq \frac{Var(X)}{c^2}$$

oss: $|X - \mathbb{E}[X]| \geq 0$

MARKOV su $|X-\mathbb{E}[X]|^2 \geq 0$ e $c^2 > 0$

$$\mathbb{P}(|X - \mathbb{E}[X]| \geq c) = \mathbb{P}(|X - \mathbb{E}[X]|^2 \geq c^2) \leq \frac{\mathbb{E}[|X-\mathbb{E}[X]|^2]}{c^2} = \frac{Var(X)}{c^2}$$

—o—o—

Calcolare il valore atteso del # di pt fissi in una permutazione di $\{1, \dots, n\}$

$$X_i(\sigma) = \begin{cases} 1 & \text{se } i \text{ punto fisso di } \sigma \\ 0 & \text{altrimenti} \end{cases}$$

$X_i : S_n \to \{0,1\}$

$$\mathbb{E}[X_1 + \dots + X_n] = \sum_{i=1}^{n} \mathbb{E}[X_i] = \sum_{i=1}^{n} \frac{(n-1)!}{n!} = \sum_{i=1}^{n} \frac{1}{n} = n \cdot \frac{1}{n} = 1$$

Esempi: $n\left\{\begin{array}{cc} \bullet & \bullet \\ \vdots & \vdots \\ \bullet & \bullet \end{array}\right\}n$ Grafo bipartito e ci sono almeno n^2-n+1 lati. Tesi: $\exists$ perfect matching.

Scelgo n coppie disgiunte in modo random

$$X_i = \begin{cases} 1 & \text{se collegati} \\ 0 & \text{altrimenti} \end{cases}$$

Se avessi $\sum_{i=1}^{n} X_i = n$ una volta avrei vinto.

$$\mathbb{E}\left[\sum_{i=1}^{n} X_i\right] = \sum_{i=1}^{n} \mathbb{E}[X_i] \geq \sum_{i=1}^{n} \frac{n^2-n+1}{n^2} = \frac{n^2-n+1}{n} = n-1+\frac{1}{n}$$

$\sum_{i=1}^{n} X_i$ è intero $\Rightarrow$ almeno una volta è n

Es 2 n numeri reali $\sum_{i=1}^{n} a_i = 0$ e non sono tutti 0.

Tesi: $\exists$ permutazione di questi $b_1, \dots, b_n$ t.c. $b_1 b_2 + \dots + b_n b_1 < 0$

$$\mathbb{E}\left[\sum_{i=1}^{n}{}' b_i b_{i+1}\right] = \sum_{i=1}^{n}{}' \mathbb{E}[b_i b_{i+1}] = n\,\mathbb{E}[b_1 b_2] = n \cdot \frac{\sum_{i\neq j}' a_i \cdot a_j}{\frac{n(n-1)}{2}} =$$

$$= \frac{2}{n-1} \sum_{i<j}{}' a_i a_j = \frac{1}{n-1}\left(\left(\sum_i{}' a_i\right)^2 - \sum_i{}' a_i^2\right) = -\frac{\sum a_i^2}{n-1} < 0$$

Da qui è easy.

Nuova tecnica: IMC 2017

In una città ci sono n persone. Ogni persona conosce esattamente 1000 persone.
Dimostrare che $\exists$ S insieme di persone t.c. almeno $\frac{n}{2017}$ persone in S conoscono esattamente 2 persone in S.

Ogni persona scelgo (indipendentemente) con probabilità p di metterla in S

$$X_i = \begin{cases} 1 & \text{se } i \in S \text{ ed esattamente 2 amici sono in } S \\ 0 & \text{altrimenti} \end{cases}$$

Voglio che almeno una volta $\sum' X_i \geq \frac{n}{2017}$, quindi mi basta $\mathbb{E}\left[\sum' X_i\right] \overset{?}{\geq} \frac{n}{2017}$

$$\mathbb{E}\left[\sum X_i\right] = \sum{}' \mathbb{E}[X_i] = \sum{}' p \cdot \binom{1000}{2} p^2 (1-p)^{998} = n\binom{1000}{2} \cdot p^3 \cdot (1-p)^{998}$$

$$\binom{1000}{2} p^3 (1-p)^{998} \overset{?}{\geq} \frac{1}{2017} \qquad p = \frac{3}{1001}$$

$$\binom{1000}{2} \cdot \left(\frac{3}{1001}\right)^3 \cdot \left(1 - \frac{3}{1001}\right)^{998} \geq \binom{1000}{2} \cdot \left(\frac{3}{1001}\right)^3 \cdot \underbrace{\left(1 - \frac{3}{1001}\right)^{1001}}_{\geq e^{-3}}$$

$$\frac{1000 \cdot 999}{2} \cdot \frac{1}{(1001)^3} \overset{?}{\geq} \frac{1}{2017}$$

$n \geq 1000$ $\quad (2n+17)n(n-1) \overset{?}{\geq} 2(n+1)^3$ fate il conto

$9n^2 \overset{?}{\geq} 23n + 2$ che è vero!

$\Rightarrow \mathbb{E}[\sum X_i] \geq \frac{e^{-3} \cdot 27}{2017} \geq \frac{1}{2017}$ Tesi

(4) G grafo con n vertici e grado medio $d \geq 1$.

$\Rightarrow \exists$ anticricca con almeno $\frac{n}{2d}$ vertici.

Prendo ogni vertice con probabilità p. $\mathbb{E}[\#\text{vertici}] = np$

Considero un lato. Qual è la prob che entrambi i vertici sono presi? p^2

$\mathbb{E}[\#\text{lati t.c. ci sono entrambi i vertici}] = p^2 \cdot \#\text{lati} = \frac{1}{2} n d p^2$

Tolgo un vertice per ogni lato con due vertici presi

$\mathbb{E}[\#\text{vertici tolti}] \leq \frac{1}{2} n d p^2$

$\mathbb{E}[\#\text{vertici restanti}] \geq np - \frac{1}{2} n d p^2 \overset{p = \frac{1}{d} \leq 1}{=} \frac{n}{d} - \frac{1}{2}\frac{n}{d} = \frac{n}{2d}$

Ora {vertici restanti} formano un'anticricca

$\Rightarrow \exists$ anticricca con almeno $\frac{n}{2d}$ vertici.

(5) Stessa cosa, senza l'ipotesi $d \geq 1$, e $\sum \frac{1}{d_i + 1}$

Consideriamo una permutazione random σ (tutte prob $= 1/n!$)

Sia A_i l'evento $\sigma(i) < \sigma(j)$ $\forall j$ vicino ad i $\Rightarrow \mathbb{P}(A_i) = \frac{1}{d_i + 1}$

$\{\sigma : \text{vale } \sigma(i) < \sigma(j)\ \forall j \text{ vicino ad } i\}$

$X(\sigma) = \sum_{i=1}^{n} I_{\{\sigma \in A_i\}}$

Se $\exists\, \sigma$ t.c. $X(\sigma) \geq m \Rightarrow \exists$ anticricca grande m

Basta $\mathbb{E}[X] \overset{!}{=} \sum' \frac{1}{d_i+1}$

$$\mathbb{E}[X] = \sum' \mathbb{E}[I_{\sigma \in \{A_i\}}] = \sum' \mathbb{P}(\sigma \in A_i) = \sum' \mathbb{P}(A_i) = \sum' \frac{1}{d_i+1}$$

<u>OSS</u>: Per AM-HM $\sum' \frac{1}{d_i+1} \geq \frac{n^2}{(\sum d_i)+n} = \frac{n}{d+1} \underset{d \geq 1}{\geq} \frac{n}{2d}$

6) USAMO 2012.6

$n \geq 2$ $\quad x_1, \dots, x_n \in \mathbb{R}$ con $x_1 + \dots + x_n = 0$ $\quad x_1^2 + \dots + x_n^2 = 1$

$\forall A \subseteq \{1, \dots, n\}$ definiamo $S_A = \sum_{i \in A}' x_i$

$\forall \lambda > 0$ $\exists$ al più $\frac{2^{n-3}}{\lambda^2}$ sottoinsiemi A con $S_A \geq \lambda$.

7) RUSSIA QUALCOSA

Ad ogni ragazzo piace almeno una ragazza.

Dimostrare che $\exists\, S$ con almeno la metà delle persone nel mondo t.c. ad ogni ragazzo in S piacciono un numero dispari di ragazze in S

8) IMO 1998. qualcosa

In una competizione ci sono a partecipanti e b giudici con $b \equiv_2 1$. Ogni giudice dice V o X $\forall$ partecipante. Sappiamo che $\forall$ coppia di giudici $\#$partecipanti con lo stesso "voto" è $\leq k$. Dimostrare che $k \geq \frac{a(b-1)}{2b}$.

9) (quasi) IMO 2014.6

n rette in pos. generale. Dimostra che per n abb. grande si possono colorare almeno $\sqrt{n}$ rette di viola in modo tale che nessuna regione finita abbia tutti i bordi colorati

(<u>Nota</u>: punti parziali per $c\sqrt{n}$ con $c < 1$)

Fatelo $\forall c < \frac{2}{3}$

6) $X : \mathcal{P}(\{1,\dots,n\}) \longrightarrow \{\text{un po' di valori}\}$
$X(A) = S_A$ (scrivere S_A)

$\mathbb{E}[S_A] = 0$ perché
$S_A + S_{A^c} = 0$

$\# S_A$ t.c. $\geq \lambda$ è $\overset{?}{\leq} \dfrac{2^{n-3}}{\lambda^2}$

ovvero $\mathbb{P}(S_A \geq \lambda) \overset{?}{\leq} \dfrac{1}{8\lambda^2}$

$\mathbb{P}(S_A \geq \lambda) = \frac{1}{2}\mathbb{P}(|S_A| \geq \lambda)$ perché $\lambda > 0$ e $S_{A^c} = -S_A$.

Dunque basta $\mathbb{P}(|S_A| \geq \lambda) \leq \dfrac{1}{4\lambda^2}$

Ora vorrei usare Chebishev:
per Chebishev
$$\mathbb{P}(|S_A| \geq \lambda) \leq \frac{Var(S_A)}{\lambda^2}$$

$$Var(S_A) = \mathbb{E}[S_A^2] \left(-\mathbb{E}[S_A]^2\right)$$

Ora $\mathbb{E}[S_A^2] = \dfrac{1}{2^n}\sum_{A \subseteq \{1,\dots,n\}} \left(\left(\sum_{i \in A} x_i\right)^2\right) = \dfrac{1}{2^n}\sum_{A \subseteq \{1,\dots,n\}} \left(\sum_{i \in A} x_i^2 + 2\sum_{\substack{i,j \in A \\ i<j}} x_i x_j\right) =$

$= \dfrac{1}{2^n}\left[\sum_{i=1}^{n} 2^{n-1} x_i^2 + \sum_{i<j} 2^{n-2} x_i x_j\right] = \dfrac{1}{2}\left(\sum x_i^2 + \frac{1}{2}\left(\left(\sum x_i\right)^2 - \sum x_i^2\right)\right) =$

$= \dfrac{1}{4}$

$\mathbb{P}(|S_A| \geq \lambda) \leq \dfrac{1}{4\lambda^2}$ che è quello che volevamo.

7) Scegliamo con probabilità $1/2$ (ed in modo indipendente) ogni rosetta, e prendiamo tutti i rosetti a cui ne piacciano un # dispari.

Sia $G = \#$ girls $\quad B = \#$boys

$$\mathbb{E}[\#\text{ ragazze prese}] = \frac{G}{2}$$

$$\mathbb{E}[\#\text{ ragazzi presi}] = \sum_{\text{ragazzi}} \mathbb{P}(\text{preso}) = \sum_{\text{ragazzi}} \frac{1}{2} = \frac{B}{2}$$

$$\mathbb{E}[\#\text{ persone prese}] = \frac{B+G}{2}$$

Dunque $\exists$ configurazione in cui ne prendo almeno $\frac{B+G}{2}$.

8) C contestant random (in maniera equiprobabile)

Ora v ed x $\#v$ e $\#x$.

Sappiamo $v+x=b$

Ora quanti i sono i giudici che concordano su C?

$$\binom{v}{2}+\binom{x}{2} \overset{?}{\geq} \frac{(b-1)^2}{4}$$

$$\iff v^2+x^2-(v+x) \overset{?}{\geq} \frac{(b-1)^2}{2} = \frac{b^2+1}{2} - b$$

$$\iff v^2+x^2 \overset{?}{\geq} \frac{b^2+1}{2}$$

Ma $v^2+x^2 \geq \frac{(b-1)^2}{4} + \frac{(b+1)^2}{4} = \frac{b^2+1}{2}$ (oppure Q.M.-A.M. + $\nexists$ =)

$$\frac{1}{a}\cdot|I| = \mathbb{E}\left[\binom{v}{2}+\binom{x}{2}\right] \geq \frac{(b-1)^2}{4}$$

dove $I = \{(\alpha,\beta,\gamma)$ con α,β giudici γ partecipante e α,β hanno dato lo stesso voto a $\gamma\}$

$$|I| \leq K\binom{b}{2}$$

$$\Rightarrow K \geq \frac{a(b-1)^2}{4}\cdot\frac{2}{b(b-1)} = a\,\frac{(b-1)}{2b} \qquad \text{Tesi!}$$

9) IMO 2014.6

Coloro ogni retta con prob p

$\mathbb{E}[\#\text{rette colorate}] = np$

Quante sono le aree finite (al più)? $\leq \frac{n^2}{2}$

Allora $\mathbb{E}[\#\text{aree cattive}] \leq \frac{n^2}{2} p^3$

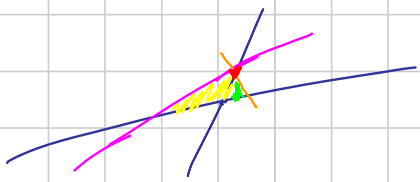
Al solito tolgo 1 retta $\forall$ area cattiva

E viene $\mathbb{E}[\#\text{rette colorate restanti}] \geq np - \frac{n^2 p^3}{2}$

$n = \frac{3}{2} n^2 p^2 \quad p = \sqrt{\frac{2}{3n}}$

$\mathbb{E}[\quad - \quad - \quad - \quad] \geq \sqrt{n}\left[\sqrt{\frac{2}{3}} - \frac{1}{2} \cdot \frac{2}{3} \cdot \sqrt{\frac{2}{3}}\right] = \sqrt{n} \cdot \left(\frac{2}{3}\right)^{3/2}$

Facciamo una cosa un po' più raffinata



Voglio contare $\max\{\#\Delta\}$.

Ogni vertice è al più in 2 triangoli (dim audio e figura)

$\Rightarrow \#\Delta \leq \#\text{vertici} \cdot \frac{2}{3} \leq \frac{n^2}{3}$

Quindi faccio come prima, solamente se non Δ cambio p^4

Come prima, stimando gli "almeno quadrilateri" come al più $\frac{n^2}{2}$, otteniamo

$$np - \frac{n^2}{3}p^3 - \frac{n^2}{2}p^4 \qquad p = \frac{k}{\sqrt{n}}$$

$$\sqrt{n}\underbrace{\left(k - \frac{k^3}{3}\right)}_{k=1} - \frac{k^4}{2}$$

$$\frac{2}{3}\sqrt{n} - \frac{1}{2}.$$

Allora, visto che $\forall c < \frac{2}{3}$ per n abbastanza grande si ha
$$\frac{2}{3}\sqrt{n} - \frac{1}{2} \geq c\sqrt{n}$$
$\Rightarrow$ Ho la tesi $\forall c < \frac{2}{3}$.

C'è un metodo simile, ma più complicato, attraverso il quale si arriva alla stima $c\sqrt{n \log n}$ per un qualche $c > 0$.

G1 ADVANCED LucaMac

Titolo nota 03/09/2018

- Parallele

$x+y+z=0$

BMO 2015.2

ABC scaleno, I incentro e ω circoscritta. $AI\cap\omega=\{A,D\}$, $BI\cap\omega=\{B,E\}$; $CI\cap\omega=\{C,F\}$. La parallela a BC per I interseca EF in K. Analogamente si definiscono L, M.

Tesi: K, L, M allineati.

Soluzione

$AI: yc=zb \qquad \omega: \sum_{cyc} a^2yz=0$

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

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

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

$EF: -xbc\cancel{a}\cancel{(\sum_{cyc}a)}+y\cancel{a}c(a+c)\cancel{(\sum_{cyc}a)}+z\cancel{a}b(a+b)\cancel{(\sum_{cyc}a)}=0$

$EF: -xbc+yc(a+c)+zb(a+b)=0$

$\infty_{BC}=(0,1,-1)$

$I=(a,b,c)$

$I\infty_{BC}: x(b+c)-ya-za=0$

$K=(a(b-c), b^2, -c^2)$

$L=(a^2, -b^2, c(a-b))$

$M=(-a^2, b(c-a), c^2)$

Tesi diventa $\det\begin{pmatrix} \cancel{a}(b-c) & b^{\cancel{2}} & -c^{\cancel{2}} \\ a^{\cancel{2}} & -b^{\cancel{2}} & \cancel{c}(a-b) \\ -a^{\cancel{2}} & \cancel{b}(c-a) & c^{\cancel{2}} \end{pmatrix} \overset{?}{=} 0$

o si fa il determinante,

$-bc(b-c) - ab(a-b) - ac(c-a) \overset{?}{=} (b-c)(a-b)(c-a)$

$-\sum_{cyc} a^2b + \sum_{cyc} ab^2 \overset{?}{=} -\sum_{cyc} a^2b + \sum_{cyc} ab^2$ vero!

CONIUGATI (in ABC)

ISOGONALI $(\alpha,\beta,\gamma) \longleftrightarrow \left(\frac{a^2}{\alpha}, \frac{b^2}{\beta}, \frac{c^2}{\gamma}\right)$

ISOTOMICI $(\alpha,\beta,\gamma) \longleftrightarrow \left(\frac{1}{\alpha}, \frac{1}{\beta}, \frac{1}{\gamma}\right)$

DISTANZE

P_1, P_2 normalizzati $\sum_{cyc} x = 1$

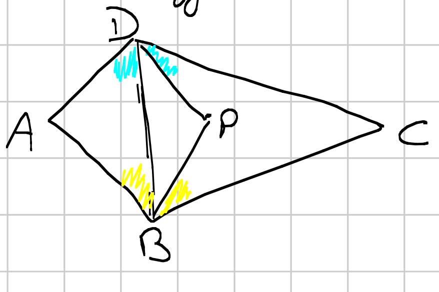
$\overrightarrow{P_1P_2} = (x_1, y_1, z_1)$ $\quad \sum_{cyc} x_1 = 0$

$P_1P_2^2 = -\sum_{cyc} a^2 y_1 z_1$

IMO 2004.5

$ABCD$ quadrilatero convesso tale che BD NON è bisettrice né di $A\hat{B}C$ né di $A\hat{D}C$. P interno ad $ABCD$ con $P\hat{B}C = D\hat{B}A$ e $P\hat{D}C = B\hat{D}A$.

Tesi: $ABCD$ ciclico iff $AP = CP$



Soluzione

1° oss A e C coniugati isogonali in PBD.

E PBD non degenere perché BD non è bisettrice.

Facciamo baricentriche su PBD.

$BD = a$ $\quad PB = c$ $\quad PD = b$.

$A=(\alpha,\beta,\gamma)$ $\qquad C=\left(\frac{a^2}{\alpha},\frac{b^2}{\beta},\frac{c^2}{\gamma}\right)=(a^2\beta\gamma, b^2\alpha\gamma, c^2\alpha\beta)$

oss: $\alpha\beta\gamma\neq 0$

$\boxed{1}$ ABCD ciclico

$\Gamma:\ \sum_{cyc} a^2yz=\left(\sum_{cyc}x\right)ux$

$A\to\ \sum_{cyc}a^2\beta\gamma=\left(\sum_{cyc}\alpha\right)\alpha u$

$C\to\ \cancel{a^2}b^2c^2\alpha\cancel{\beta\gamma}\sum_{cyc}\alpha=\left(\sum_{cyc}a^2\beta\gamma\right)\cancel{a^2\beta\gamma}\,u$

ABCD ciclico iff $\boxed{\alpha^2b^2c^2\left(\sum_{cyc}\alpha\right)^2=\left(\sum_{cyc}a^2\beta\gamma\right)^2}$

$\boxed{2}$ $AP=CP$ $(\iff AP^2=CP^2)$

$P=(1,0,0)$

$A=\frac{1}{\sum\alpha}(\alpha,\beta,\gamma)$ $\qquad \overrightarrow{AP}=\left(\frac{\beta+\gamma}{\sum\alpha},\frac{-\beta}{\sum\alpha},\frac{-\gamma}{\sum\alpha}\right)$

$$AP^2=\frac{1}{\left(\sum\alpha\right)^2}\left(-a^2\beta\gamma+(\beta+\gamma)(\beta c^2+\gamma b^2)\right)$$

$$CP^2=\frac{1}{\left(\sum a^2\beta\gamma\right)^2}\left(-a^2b^2c^2\alpha^2\beta\gamma+(b^2\alpha\gamma+c^2\alpha\beta)(b^2c^2)(\alpha\gamma+\alpha\beta)\right)$$

$$\shortparallel$$

$$\frac{b^2c^2\alpha^2}{\left(\sum a^2\beta\gamma\right)^2}\Big(\underbrace{-a^2\beta\gamma+(b^2\gamma+c^2\beta)(\gamma+\beta)}_{\text{schifo}}\Big)$$

Quindi diventa la cosa di prima dopo aver dimostrato che schifo $\neq 0$

schifo $\neq 0$ perché $A\not\equiv P$. ☺

POTENZE

Sempre prendremo le coordinate normalizzate, diciamo $P=(x,y,z)$

$\Gamma:\ \sum_{cyc}a^2yz=\left(\sum x\right)\left(\sum ux\right)$ per opportuni $u,v,w\in\mathbb{R}$

$$Pow_\Gamma(P)=-\sum_{cyc}a^2yz+\left(\sum_{cyc}x\right)\left(\sum_{cyc}ux\right)$$

IMO SL 2011 G2

A_1, A_2, A_3, A_4 non conciclici. O_i ed r_i centro e raggio di $\odot\{A_j\}_{j\neq i}$

Tesi: $\sum_{cyc}' \frac{1}{O_iA_i^2 - r_i^2} = 0$

Soluzione

$O_iA_i^2 - r_i^2 = Pow_{\Gamma_i}(A_i)$

Tesi equivale a $\sum_{cyc}' \frac{1}{Pow_{\Gamma_i}(A_i)} \overset{?}{=} 0$

Riferimento $A_1A_2A_3$ $A_1A_2 = c$ $A_1A_3 = b$ $A_2A_3 = a$

$A_4 = (\alpha, \beta, \gamma)$ $\sum_{cyc}\alpha \neq 0$

$\Gamma_4 : -\sum_{cyc} a^2 yz = 0$ $\Gamma_3 : -\sum_{cyc} a^2yz + \left(\sum_{cyc} x\right) z \cdot \frac{\sum'_{cyc} a^2\beta\gamma}{\gamma \sum_{cyc}\alpha} = 0$

$Pow_{\Gamma_4}(A_4) = -\left(\sum_{cyc}' a^2\beta\gamma\right) \cdot \frac{1}{\left(\sum'_{cyc}\alpha\right)^2}$

$Pow_{\Gamma_3}(A_3) = \frac{\sum_{cyc} a^2\beta\gamma}{\gamma \sum'_{cyc} \alpha}$

Tesi equivale a $\frac{-\left(\sum'_{cyc}\alpha\right)^2}{\sum'_{cyc} a^2\beta\gamma} + \sum_{cyc}\left(\frac{\gamma\sum_{cyc}\alpha}{\sum'_{cyc} a^2\beta\gamma}\right) \overset{?}{=} 0$ vero!

Perpendicolari

$\vec{v_1} = (x_1, y_1, z_1)$ $\vec{v_2} = (x_2, y_2, z_2)$ $\sum_{cyc}' x_1 = 0$

$\vec{v_1} \perp \vec{v_2}$ iff $-\sum_{cyc}' a^2(y_1z_2 + y_2z_1) = 0$

Dim: $\vec{v_1} = x_1\vec{A} + y_1\vec{B} + z_1\vec{C}$

$\vec{v_1}\cdot\vec{v_2} = \underbrace{\cancel{(x_1+y_1+z_1)}}_{0}(x_2+y_2+z_2)R^2 - \frac{1}{2}\sum_{cyc} a^2(y_1z_2+y_2z_1)$

OSS: Funziona assumendo $\sum \vec{v_i} \neq 0$ solo se ho messo il centro vettoriale nel circocentro di ABC.

IMO SL 2012 G4

ABC con $AB \neq AC$ ed O circocentro. Bisettrice di $B\hat{A}C$ interseca BC in D. Riflettendo D rispetto al pt medio di BC si ottiene E. Le $\perp$ a BC per D ed E intersecano risp AO ed AD in X e Y.

Tesi: $BXCY$ ciclico

Soluzione

$$O = (a^2 S_A, b^2 S_B, c^2 S_C)$$

$$D = (0, b, c) \qquad E = (0, c, b)$$

$$\infty_{AH} = (-a^2, S_C, S_B)$$

$$DX: \ x(bS_B - cS_C) - y a^2 c + z a^2 b = 0$$

$$AO: \ y c^2 S_C = z b^2 S_B$$

$$x(bS_B - cS_C) b S_B + y(\underbrace{-a^2 c b S_B + a^2 c^2 S_C}_{a^2 c(cS_C - bS_B)}) = 0$$

$$X = (a^2 bc, b^2 S_B, c^2 S_C)$$

$$EY: \ x(cS_B - bS_C) - y a^2 b + z a^2 c = 0$$

$$AD: \ yc = zb$$

$$xb(cS_B - bS_C) + y(-a^2 b^2 + a^2 c^2) = 0$$

$$cS_B - bS_C = \frac{c(a^2+c^2-b^2)}{2} - \ldots = \frac{1}{2}[a^2(c-b) + (c-b)(c^2+cb+b^2) + bc(c-b)] = \frac{1}{2}(c-b)(a^2+(b+c)^2)$$

$$xb(a^2+(b+c)^2) + 2ya^2(b+c) = 0$$

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

$$\Gamma: \ \sum_{cyc} a^2 yz = \left(\sum_{cyc} x\right) ux$$

$$X: \ \cancel{a^2} b^2 c^2 (S_B S_C + a^2 bc) = (a^2 bc + b^2 S_B + c^2 S_C) u \cdot \cancel{a^2} bc$$

$$u = \frac{bc(S_B S_C + a^2 bc)}{a^2 bc + b^2 S_B + c^2 S_C}$$

(Y) $$\cancel{a}^2 bc\left(a^2+(b+c)^2\right)\left[\cancel{a^2+(b+c)^2} - 2(b+c)^2\right] =$$
$$= (b+c)\left(\cancel{(b+c)^2 - a^2}\right) v \left(\cancel{+}2\cancel{a}^2(b+c)\right)$$

$$v = \frac{bc\left(a^2+(b+c)^2\right)}{2(b+c)^2}$$

Tesi iff $2(S_BS_C + a^2bc)(b+c)^2 = \left(a^2+(b+c)^2\right)\left(a^2bc + b^2S_B + c^2S_C\right)$

$$(b+c)^2\left(2S_BS_C + a^2bc - b^2S_B - c^2S_C\right) \overset{?}{=} a^2\left(a^2bc + b^2S_B + c^2S_C\right)$$
$$(b+c)^{\cancel{2}}\left(\cancel{a^2}bc - S_A\cancel{a^2}\right) \overset{?}{=} \cancel{a^2}(bS_B + cS_C)\cancel{(b+c)}$$
$$(b+c)(bc - S_A) \overset{?}{=} (bS_B + cS_C)$$
$$bc(b+c) \overset{?}{=} c^2b + b^2c \quad \underline{\text{vero!}}$$

IMO SL 2005 G5

ABC acutangolo, $AB \neq AC$. H ortocentro, $\vec{M} = \dfrac{\vec{B}+\vec{C}}{2}$. $D \in AB$, $E \in AC$.
$AE = AD$; D, H, E allineati.
<u>Tesi</u> $HM \perp$ asse radicale tra $\odot(ABC)$ e $\odot(ADE)$.

Soluzione

$D = (c-\ell, \ell, 0)$ $\quad E = (b-\ell, 0, \ell)$ $\quad H = (S_BS_C, -\,-\,-)$

$$\det\begin{pmatrix} c-\ell & \ell & 0 \\ b-\ell & 0 & \ell \\ S_BS_C & S_AS_C & S_AS_B \end{pmatrix} = 0$$

$$-\cancel{\ell}(c-\ell)S_AS_C + \ell^{\cancel{2}}S_BS_C - \cancel{\ell}(b-\ell)S_AS_B = 0$$
$$\boxed{\ell(S_AS_C + S_BS_C + S_AS_B) = S_A(cS_C + bS_B)}$$

$\odot ADE$: $\sum_{cyc} a^2yz = \left(\sum_{cyc} x\right)(vy + wz)$

(D) $c^2\ell(c-\ell) = c(\ell v) \rightsquigarrow v = c(c-\ell)$

(E) $w = b(b-\ell)$

l'asse radicale è $c(c-\ell)y + b(b-\ell)z = 0$

Due punti a caso ① A

② $\cap BC = P\,(0,\ b(b-\ell),\ -c(c-\ell))$

A meno di scalare $\vec{AP} = (c(c-\ell)-b(b-\ell),\ b(b-\ell),\ -c(c-\ell))$

$$\vec{HM} = \vec{M} - \vec{H} = \frac{\vec{B}+\vec{C}}{2} - (\vec{A}+\vec{B}+\vec{C}) = \left(-1, -\frac{1}{2}, -\frac{1}{2}\right) \sim (2,1,1)$$

Tesi diventa:

$$a^2(b(b-\ell)-c(c-\ell)) + b^2(-b(b-\ell)-c(c-\ell)) + c^2(c(c-\ell)+b(b-\ell)) \overset{?}{=} 0$$

$$a^2(b(b-\ell)-c(c-\ell)) + (c^2-b^2)(c(c-\ell)+b(b-\ell)) \overset{?}{=} 0$$

$$a^2(b+c-\ell) \overset{?}{=} (b+c)(c(c-\ell)+b(b-\ell))$$

$$\ell \overset{?}{=} \frac{(b+c)(b^2+c^2-a^2)}{(b+c)^2-a^2}$$

Ora sappiamo $\sum_{cyc} S_A S_B = \frac{1}{4}(a+b+c)\prod_{cyc}(a+b-c)$

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

$$cS_C + bS_B = \frac{1}{2}\left[a^2(b+c) + bc(b+c) - (b+c)(b^2-bc+c^2)\right] =$$

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

e ora è ovvio!

POLI e POLARI

Come si fanno? Sdoppiamento?

$x^2 \mapsto xx_0$

$xy \mapsto \dfrac{xy_0+yx_0}{2}$

La polare di (α,β,γ) risp a $\sum_{cyc} a^2yz = 0$

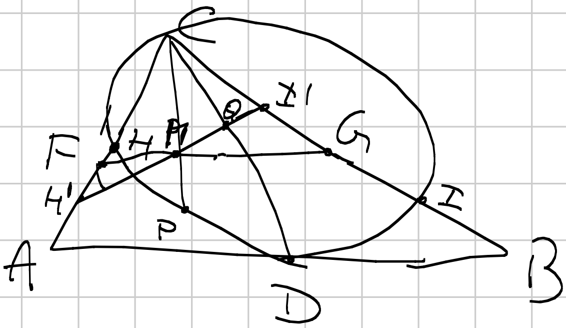
$$\sum_{cyc} a^2(y\gamma+z\beta) = 0$$

La polare di $(1,0,0)$ risp a $\sum_{cyc} a^2yz = (\sum x)(\sum ux)$

$$b^2z + c^2y = 2ux + vy + wz$$

TST 2016.6 (IMO SL 2015 G5)

ABC triangolo con $AC \neq BC$. D, F, G punti medi di AB, AC, BC risp. Γ passa per C e tange AB in D. $\Gamma \cap \overline{AF}$ è H e $\Gamma \cap \overline{BG}$ è I. H' e I' i simmetrici di H ed I rispetto a F e G, rispettivamente. $H'I'$ interseca CD in Q e FG in M. $CM \cap \Gamma = \{C, P\}$. Tesi: $CQ = QP$.



Soluzione

$$D = (1,1,0)$$

$$\Gamma: \sum_{cyc} a^2yz = \left(\sum_{cyc} x\right)(ux+vy)$$

$$c^2 = 2(u+v)$$

$c^2xy = (x+y)(ux+vy)$ ha $\Delta = 0$

ovvero $4uv = (u+v-c^2)^2 = \frac{c^4}{4}$

$uv = \frac{c^4}{16}$ $\quad u+v = \frac{c^2}{2}$ $\quad u = v = \frac{c^2}{4}$

$$\Gamma: \sum_{cyc} a^2yz = \frac{c^2}{4}\left(\sum_{cyc} x\right)(x+y)$$

$\Gamma \cap \{x=0\} \Rightarrow a^2\cancel{y}z = \frac{c^2}{4}\cancel{y}(y+z)$ $\qquad yc^2 = z(4a^2-c^2)$

$I = (0,\ 4a^2-c^2,\ c^2)$ $\qquad H = (4b^2-c^2,\ 0,\ c^2)$

$I' = (0,\ c^2,\ 4a^2-c^2)$ $\qquad H' = (c^2,\ 0,\ 4b^2-c^2)$

$CD: \ x = y$

$$H'I': \ \det\begin{pmatrix} x & y & z \\ 0 & c^2 & 4a^2-c^2 \\ c^2 & 0 & 4b^2-c^2 \end{pmatrix} = 0$$

$$H'I': \ x\cancel{c^2}(4b^2-c^2) + y\cancel{c^2}(4a^2-c^2) - zc^2\cdot\cancel{c^2} = 0$$

$$(4b^2+4a^2-2c^2)x = zc^2$$

$$Q = (c^2,\ c^2,\ 2(2a^2+2b^2-c^2))$$

$FG: \ z = x+y$

$$AM: \ x(2b^2-c^2) + y(2a^2-c^2) = 0$$

$$c^2 \quad c^2 \quad 2(2a^2+2b^2-c^2)$$

$$\infty_A = (-a^2,\ S_C,\ S_B)$$

$$Q\infty_A: \ x\left(c^2S_B - 2S_C(2a^2+2b^2-c^2)\right) +$$
$$+\, y\left(-2a^2(2a^2+2b^2-c^2) - c^2S_B\right) + zc^2(a^2+S_C) = 0$$

$$Q\infty_A \cap \{x=0\} \rightsquigarrow Q_A = \left(0,\ c^2(a^2+S_C),\ c^2S_B + 2a^2(2a^2+2b^2-c^2)\right)$$

ω di centro Q che passa per C $\left(\Rightarrow \text{per } 2Q_A - C \text{ e } 2Q_B - C\right)$

$$\sum Q_A = 4a^2(a^2+b^2) \rightsquigarrow C = (0,\ 0,\ 4a^2(a^2+b^2))$$

$$2Q_A - C = \left(0,\ c^2(a^2+S_C),\ c^2S_B + 2a^2(2a^2+2b^2-c^2) - 2a^2(a^2+b^2)\right)$$

$$2Q_A - C = \left(0,\ c^2(a^2+S_C),\ c^2S_B + 2a^2(a^2+b^2-c^2)\right)$$

$$\omega: \ \sum_{cyc} a^2yz = \left(\sum_{cyc} x\right)(ux+vy)$$

$2Q_A - C$ $\quad a^2\cancel{c^2}\cancel{(a^2+S_C)}\left(c^2S_B + 2a^2(a^2+b^2-c^2)\right) = 2\cancel{a^2}(a^2+b^2)\,v\,\cancel{c^2}\cancel{(a^2+S_C)}$

$$v = \frac{c^2 S_B + 2a^2(a^2+b^2-c^2)}{2(a^2+b^2)} = \frac{c^2 S_B + 4a^2 S_C}{2(a^2+b^2)}$$

$$U = \frac{c^2 S_A + 4b^2 S_C}{2(a^2+b^2)}$$

Tesi equivale ad CM: coincide con $\left(CM: x(2b^2-c^2)+y(2a^2-c^2)=0\right)$

$$\left(\frac{c^2 S_B + 4a^2 S_C}{2(a^2+b^2)} - \frac{c^2}{4}\right) y + (\text{sym}) x = 0$$

$$\frac{2c^2 S_B + 8a^2 S_C - a^2c^2 - b^2c^2}{\cancel{4(a^2+b^2)}} y + (\text{sym}) x = 0$$

Tesi $\iff \dfrac{2c^2 S_B + 8a^2 S_C - a^2c^2 - b^2c^2}{2a^2-c^2}$ è sym in a e b

$$c^2(\cancel{a^2}+c^2-b^2) + 4a^2(a^2+b^2-c^2) - \cancel{a^2c^2} - b^2c^2$$

$$\underbrace{4a^4}_{0} + \underbrace{4a^2b^2}_{0} - \underbrace{\underbrace{4a^2c^2}_{-2a^2c^2}}_{0} - \underbrace{2b^2c^2}_{0} + \underbrace{c^4}_{0} \;\Big|\; \frac{2a^2-c^2}{2a^2+2b^2-c^2}$$

Tesi $\iff 2a^2+2b^2-c^2$ sym in a e b 😊

Senior 2018 - N1 Advanced - Anér

Titolo nota 04/09/2018

$$\sum_{p \text{ primo}} \frac{1}{p} = +\infty.$$

Def Sia $a_1, a_2, \ldots$ una successione di reali ≥ 0.

Allora la successione $S_n = \sum_{i=1}^{n} a_n$ è debolmente crescente. Se $\ell = \lim_{n \to \infty} S_n < +\infty$, allora diciamo che $\sum_{n=1}^{+\infty} a_n = \ell$ "La serie converge a ℓ". Altrimenti $\sum_{n=1}^{+\infty} a_n = +\infty$ "La serie diverge a $+\infty$".

Per i primi $p_1, p_2, p_3, \ldots$

$$\begin{matrix} p_1, & p_2, & p_3, & \ldots \\ \parallel & \parallel & \parallel & \parallel \\ 2 & 3 & 5 & 7 \; \ldots \end{matrix}$$

$$\sum_{p \text{ primo}} \frac{1}{p} = \sum_{i=1}^{\infty} \frac{1}{p_i}.$$

S è un $\overbrace{\text{insieme}}^{\text{anche infinito}}$, $a : S \to [0, \infty)$ $\quad a(s) = a_s \quad s \in S$

$$\sum_{s \in S} a_s = \sup_{\substack{T \subseteq S \\ T \text{ finito}}} \left(\sum_{s \in T} a_s \right)$$

Esempio $a_n = \lambda^n$ (partendo da $a_0 = 1$) $\lambda \geq 0$

$$\sum_{i=0}^{\infty} \lambda^i = \begin{cases} +\infty & \text{se } \lambda \geq 1 \text{ : ogni volta aggiung } \lambda^n \geq 1 \\ \frac{1}{1-\lambda} & \text{: infatti } \sum_{i=0}^{n} \lambda^i = \frac{1-\lambda^{n+1}}{1-\lambda} \xrightarrow{n \to \infty} \frac{1}{1-\lambda} \end{cases}$$

Esempio $a_n = \dfrac{1}{n(n+1)}$ (partendo da a_1).

$$\sum_{i=1}^{\infty} \frac{1}{i(i+1)} = \sum_{i=1}^{\infty} \left[\frac{1}{i} - \frac{1}{i+1}\right] \stackrel{?}{=} 1$$

Infatti $\displaystyle\sum_{i=1}^{n} \left[\frac{1}{i} - \frac{1}{i+1}\right] = 1 - \frac{1}{n+1}$

Variante $a_n = \dfrac{1}{n^2}$. $\displaystyle\sum_{i=1}^{\infty} \frac{1}{i^2}$ converge o no?

Sì: a parte il primo termine $\dfrac{1}{1^2}$, ogni altro

$a_i = \dfrac{1}{i^2} < \dfrac{1}{i(i-1)}$ e la serie di questi ultimi converge.

Esempio $s > 0$ $a_n = \dfrac{1}{n^s}$ con $n \geq 1$

$\displaystyle\sum_{i=1}^{\infty} \frac{1}{i^s}$ converge? Sí se $s > 1$; No se $s \leq 1$

CRITERIO DI CONDENSAZIONE DI CAUCHY

$a_n \geq 0$, a_n è decrescante (deb.), allora

$\displaystyle\sum_{n=1}^{\infty} a_n$ converge se e solo se $\displaystyle\sum_{k=1}^{\infty} 2^k a_{2^k}$ converge

diverge // / / diverge

$\displaystyle\sum_{i=1}^{\infty} \frac{1}{i^s}$ converge se e solo se $\displaystyle\sum_{k=1}^{\infty} 2^k \frac{1}{2^{ks}}$ converge

$\shortparallel$

mi riconduco alla serie geometrica $\sum_{k=1}^{\infty} \underbrace{\left(\frac{1}{2^{s-1}}\right)}_{\lambda}^{k}$

$$\sum_{n=1}^{\infty} \frac{1}{n} = +\infty$$

Excursus sui logaritmi

Diamo una definizione di e.

Lemma La successione $x_n = \left(1+\frac{1}{n}\right)^n$ è crescente $n \geq 1$

La successione $\left(1+\frac{1}{n}\right)^{n+1}$ è decrescente $n \geq 1$

DIM

$$\left(1+\frac{1}{n}\right)^n \overset{?}{<} \left(1+\frac{1}{n+1}\right)^{n+1}$$

$$\left(\frac{n+1}{n}\right)^n \overset{?}{<} \left(\frac{n+2}{n+1}\right)^n \cdot \left(\frac{n+2}{n+1}\right)$$

$$1-\frac{1}{n+2} = \frac{n+1}{n+2} \overset{?}{<} \left(\frac{n(n+2)}{(n+1)^2}\right)^n = \left(1-\frac{1}{(n+1)^2}\right)^n$$

$$\left(1-\frac{1}{(n+1)^2}\right)^n \underset{\text{Bernoulli}}{>} \cancel{1} - \frac{n}{(n+1)^2} \overset{?}{>} \cancel{1} - \frac{1}{n+2}$$

$$\frac{1}{n+2} \overset{?}{>} \frac{n}{(n+1)^2} \qquad 1 \overset{?}{>} \frac{n(n+2)}{(n+1)^2} \quad \checkmark$$

L'altra per esercizio.

e è il lim della succ. crescente $\left(1+\frac{1}{n}\right)^n$

e è il lim // // decr. $\left(1+\frac{1}{n}\right)^{n+1}$

$$\forall n \quad \left(1+\frac{1}{n}\right)^n < e < \left(1+\frac{1}{n}\right)^{n+1}$$

$$\frac{1}{n+1} < \log\left(1+\frac{1}{n}\right) < \frac{1}{n}$$

$\sum_{p \text{ primo}} \frac{1}{p} = +\infty$. Basta dim. che $\sum_{p \text{ primo}} \frac{1}{p-1} = +\infty$:

levo il primo termine qui, ogni altro termine è $<$ di quello qui rel. al primo precedente.

Siano $p_1 \dots p_k$ i primi fino a N.

$$\sum_{i=1}^{k} \frac{1}{p_i - 1} > \sum_{i=1}^{k} \log\left(1+\frac{1}{p_i-1}\right) = \log\left(\prod_{i=1}^{k} \frac{1}{1-\frac{1}{p_i}}\right) >$$

$$> \log\left(\prod_{i=1}^{k} \frac{1-\left(\frac{1}{p_i}\right)^{\lceil \log_{p_i}(N)\rceil + 1}}{1-\frac{1}{p_i}}\right) =$$

$$= \log\left(\prod_{i=1}^{k}\left(1+\frac{1}{p_i}+\dots+\frac{1}{p_i^{\lceil \log_{p_i}(N)\rceil}}\right)\right) =$$

$$= \log\left(1+\frac{1}{2}+\frac{1}{3}+\dots+\frac{1}{N}+\sum_{\text{finiti}} \text{altri } \frac{1}{M}\right) > \underbrace{\log\left(1+\dots+\frac{1}{N}\right)}_{\text{diventa arbitr. grande}}$$

Variazione sul tema: $\displaystyle\sum_{\substack{p \text{ primo} \\ p\equiv 1 \pmod 4}} \frac{1}{p} = +\infty$

$n \geq 1$ $\qquad n = 2^{\alpha} \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ $\qquad p_i$ dispari (tutto in $\mathbb{N}$)

n si scrive come somma di quadrati u^2+v^2 con $u,v \in \mathbb{Z}$

in quanti modi?

Interi di Gauss $\qquad n = u^2+v^2 = (u+iv)(u-iv) = m \cdot \overline{m}$

Abbiamo già visto che i primi $\equiv 3 \pmod 4$ devono comparire con esp. pari.

Se $p_i^{\alpha_i} \| n$ $\quad \alpha_i$ pari $\quad p_i \equiv 3 \ (4)$, allora

$p_i^{\alpha_i/2}$ deve dividere sia u che v.

Il caso interessante è quello con 2 e primi $\equiv 1 \ (4)$.

$p_i = q_i \cdot \overline{q_i}$

$$n = i^t (1+i)^{2\alpha} \, q_1^{\alpha_1} \cdot \overline{q_1}^{\alpha_1} \cdot \ldots \cdot q_k^{\alpha_k} \cdot \overline{q_k}^{\alpha_k} = m \cdot \overline{m}$$

m deve avere la forma $\; i^{r} (1+i)^{\alpha} \cdot q_1^{\beta_1} \cdot \overline{q_1}^{\alpha_1-\beta_1} \cdot \ldots \cdot q_k^{\beta_k} \, \overline{q_k}^{\alpha_k-\beta_k}$

Posso scegliere r in 4 modi e β_i in (α_i+1) modi

$\rightarrow$ n si scrive come u^2+v^2 in $4(\alpha_1+1)\cdot \ldots \cdot (\alpha_k+1)$ modi con $u,v \in \mathbb{Z}$.

Per casa: sistemare i particolari sulla convergenza/divergenza

GRANDE CONGETTURA

$$\sum_{\substack{(u,v)\in\mathbb{Z}^2\\(u,v)\neq(0,0)}} \frac{1}{u^2+v^2} = \sum_{n=1}^{\infty} \frac{\#\{(u,v) : u^2+v^2=n\}}{n}$$

$$\overset{*}{=} 4\cdot\left(\frac{1}{1-\frac{1}{2}}\right)\cdot\prod_{p\equiv 3\ (\mathrm{mod}\ 4)}\left(\frac{1}{1-\frac{1}{p^2}}\right)\cdot\prod_{p\equiv 1\ (\mathrm{mod}\ 4)}\left(\frac{1}{1-\frac{1}{p}}\right)^2$$

Lemma Se $\lambda\in(0,1)$ $a_n=(n+1)\cdot\lambda^n$ $(n\geq 0)$.

Allora $\displaystyle\sum_{i=0}^{\infty}(i+1)\lambda^i=\left(\sum_{i=0}^{\infty}\lambda^i\right)^2$.

DIM Sto sommando i seguenti numeri

$$\begin{matrix} 1 & \lambda & \lambda^2 & \lambda^3 & \cdots \\ \lambda & \lambda^2 & \lambda^3 & \ddots & \\ \lambda^2 & \lambda^3 & \ddots & & \\ \lambda^3 & \ddots & & & \\ \vdots & & & & \end{matrix}$$

Se espando

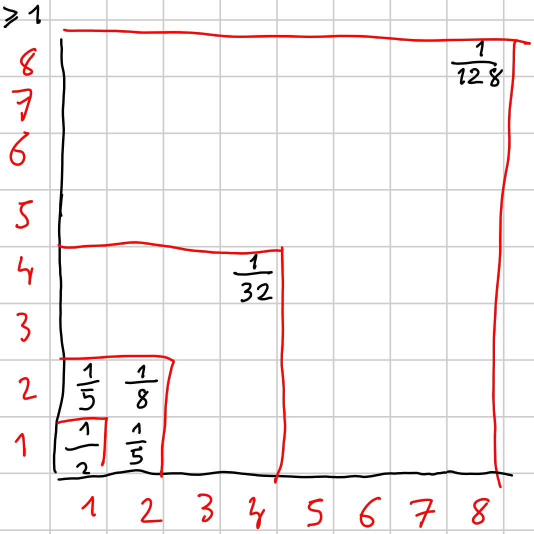
$$4\cdot\left(\frac{1}{1-\frac{1}{2}}\right)\cdot\prod_{p\equiv 3\ (\mathrm{mod}\ 4)}\left(\frac{1}{1-\frac{1}{p^2}}\right)\cdot\prod_{p\equiv 1\ (\mathrm{mod}\ 4)}\left(\frac{1}{1-\frac{1}{p}}\right)^2=$$

$$=4\cdot\left(1+\frac{1}{2}+\frac{1}{4}+\ldots\right)\cdot\prod_{p\equiv 3\ (4)}\left(1+\frac{1}{p^2}+\frac{1}{p^4}+\frac{1}{p^6}+\ldots\right)\cdot\prod_{p\equiv 1\ (\mathrm{mod}\ 4)}\left(1+\frac{2}{p}+\frac{3}{p^2}+\frac{4}{p^3}+\ldots\right)$$

quante volte ottengo $\frac{1}{n}$? GRANDE CONGETTURA DIMOSTRATA!

Adesso dim. che $\displaystyle\sum_{\substack{(u,v)\\ \neq\\ (0,0)}} \frac{1}{u^2+v^2}$ diverge. Basta

dim che $\displaystyle\sum_{u,v\geq 1} \frac{1}{u^2+v^2}$ diverge



$$\sum_{u,v\geq 1} \frac{1}{u^2+v^2} > \frac{1}{2} + \sum_{k=0}^{\infty} \frac{3\cdot \cancel{4^k}}{8\cdot \cancel{4^k}} = +\infty$$

Nel prodotto con termini ≥ 1

$$4\cdot\left(\frac{1}{1-\frac{1}{2}}\right)\cdot \prod_{p\equiv 3\ (\mathrm{mod}\ 4)} \left(\frac{1}{1-\frac{1}{p^2}}\right)\cdot \prod_{p\equiv 1\ (\mathrm{mod}\ 4)} \left(\frac{1}{1-\frac{1}{p}}\right)^2$$

Un fattore deve divergere a $+\infty$. Ma

$$\prod_{p\equiv 3} \left(\frac{1}{1-\frac{1}{p^2}}\right) = \sum_{n\geq 1} \frac{1}{n^2} < \sum_{n\geq 1} \frac{1}{n^2} = \frac{\pi^2}{6}$$

n sifatti, solo con primi $\equiv 3\ (4)$ — qualsiasi

Quindi $\displaystyle\prod_{p\equiv 1\ (n)} \left(\frac{1}{1-\frac{1}{p}}\right)^2 = +\infty$, ma allora

$$2\sum_{p\equiv 1} \log\left(1+\frac{1}{p-1}\right) = +\infty$$

$$\wedge$$

$$2\sum_{p\equiv 1}\frac{1}{p-1} \rightsquigarrow \sum_{p\equiv 1}\frac{1}{p-1} = +\infty$$

ma allora anche $\displaystyle\sum_{p\equiv 1}\frac{1}{p} = +\infty$

Teo (Dirichlet) Se a, b sono coprimi, allora

$$\sum_{\substack{p \text{ primo} \\ p\equiv a\ (\mathrm{mod}\ b)}} \frac{1}{p} = +\infty$$

D'ora in poi niente più analisi.

Sia $f:\mathbb{N}_0 \to \mathbb{C}$ una funzione (spesso a valori naturali)

f è moltiplicativa se $f(mn) = f(m)\cdot f(n)$ $\forall\, m,n$ coprimi.

f è completamente moltiplicativa se $f(mn)=f(m)f(n)$ sempre.

Esempio $f(n) \equiv 1$

Esempio $f(n) = \begin{cases} 1 & \text{se } n \text{ è coprimo con } K \\ 0 & \text{altrimenti} \end{cases}$

Esempio $\varphi(n)$ è moltiplicativa, ma non compl.

$\left[\tau(n) = \#\text{ divisori } \geq 1 \text{ di } n\right]$ è molt., ma non c.m.

$\left[\sigma(n) = \sum_{d|n} d\right]$ è molt., ma non c.m.

Esempio di prima $F(n) = \frac{1}{4}\#\{(u,v) : n = u^2+v^2\}$

è moltiplicativa !

In generale posso considerare, data una funzione $F : \mathbb{N}_0 \to \mathbb{C}$, la serie formale di Dirichlet associata

$$\sum_{n=1}^{\infty} \frac{F(n)}{n^s}.$$

Ho un'operazione di convoluzione, corrispondente al prodotto

è una nuova funzione di n

$$\left(\sum_{n=1}^{\infty} \frac{F(n)}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{g(n)}{n^s}\right) = \sum_{n=1}^{\infty} \frac{\left[\sum_{d|n} F(d)\cdot g\left(\frac{n}{d}\right)\right]}{n^s}$$

Esempio importante $\mu : \mathbb{N}_0 \to \{0, 1, -1\}$

Funz. di Möbius

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

$$\mu(n) = \begin{cases} 0 & \text{se c'è un } \alpha_i \geq 2 \quad (n \text{ non è libero da quadrati}) \\ \text{altrimenti} & \begin{cases} 1 & \text{se } k \text{ pari} \\ -1 & \text{se } k \text{ dispari} \end{cases} \end{cases}$$

μ è moltiplicativa.

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_{p \text{ primo}} \left(1 - \frac{1}{p^s}\right)$$

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ primo}} \left(\frac{1}{1 - \frac{1}{p^s}}\right)$$

Se calcolo $\sum_{d|n} \mu(d) \cdot 1 = \begin{cases} \text{se } n=1 & \text{viene } 1 \\ \text{se } n \geq 2 & \text{viene } 0 \end{cases}$

$$\sum \frac{\tau(n)}{n^s} = \prod_p \left(\frac{1}{1 - \frac{1}{p^s}}\right)^2 = \left(\sum \frac{1}{n^s}\right)^2$$

In generale se f è moltiplicativa

$$\sum \frac{f(n)}{n^s} = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots\right)$$

se f è compl. molt.

$$= \prod_p \left(\frac{1}{1 - \frac{f(p)}{p^s}}\right)$$

Esercizi ① Calcolare / interpretare

$$\sum \frac{\varphi(n)}{n^s}$$

② Definiamo ricorsivamente $a_n \in \mathbb{Z}$ con la formula $\sum_{d|n} a_d = 2^n$. Allora $n \mid a_n$

<u>Per casa</u>

(3) Sia a_n una successione crescente di naturali con $b_n = a_{n+1} - a_n$ debolmente crescente.

Sappiamo che $\forall i \neq j$, a_i e a_j sono coprimi.

Dimostrare che $\sum \frac{1}{a_n}$ converge.

$\boxed{M19}$ Problems in Elementary Number theory (PEN)

(4) a_n è definita da $a_1 = 1$ $a_2 = K \geq 2$, poi a_n è il più piccolo intero positivo diverso da $a_1 \dots a_{n-1}$ e non coprimo con a_{n-1}.

<u>Tesi</u> Tutti gli interi positivi prima o poi compaiono.

---

(1)
$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \prod_{p \text{ primo}} \left(1 + \frac{p-1}{p^s} + \frac{(p-1)p}{p^{2s}} + \dots\right) =$$

$$= \prod_{p \text{ primo}} \left(1 + \frac{p-1}{p^s}\left(1 + \frac{p}{p^s} + \frac{p^2}{p^{2s}} + \dots\right)\right)$$

$$= \prod_{p \text{ primo}} \left(1 + \frac{p-1}{p^s}\left(\frac{1}{1 - p^{1-s}}\right)\right)$$

$$\sum_{d \mid n} \varphi(d) = n \qquad \underbrace{\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right)}\left(\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s}\right) = \sum_{n=1}^{\infty} \frac{n}{n^s}$$

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \right) \underbrace{\left(\sum_{n=1}^{\infty} \frac{1}{n^{s-1}} \right)}_{\zeta(s-1)}$$

$$\varphi(n) = \sum_{d \mid n} d \cdot \mu\left(\frac{n}{d}\right)$$

---

(2) $2^n = \sum_{d \mid n} a_d \cdot 1 \qquad \left(\sum_{n=1}^{\infty} \frac{a_n}{n^s} \right) \cdot \left(\sum_{n=1}^{\infty} \frac{1}{n^s} \right) = \left(\sum_{n=1}^{\infty} \frac{2^n}{n^s} \right)$

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \left(\sum_{n=1}^{\infty} \frac{2^n}{n^s} \right) \cdot \left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \right)$$

$a_n = \sum_{d \mid n} 2^d \cdot \mu\left(\frac{n}{d}\right)$ è un multiplo di n

$n = 2^\alpha \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Ragioniamo un primo alla volta

$\boxed{\text{Se } \alpha \geq 1}$

$2^\alpha \mid a_n$. Infatti gli addendi interessanti sono quelli con $\frac{n}{d}$ libero da quadrati

$\rightsquigarrow 2^{\alpha-1} \mid d \rightsquigarrow d \geq 2^{\alpha-1} \qquad 2^d > 2^{\alpha-1}$

e quindi ogni addendo è multiplo di 2^α.

$\boxed{p_i^{\alpha_i}}$ $\qquad a_n = \sum_{\substack{e \mid n \\ e \text{ lib. da quadrati}}} \mu(e) \cdot 2^{n/e} =$

$$e \mid 2 \cdot p_1 \cdots p_k$$

$$= \sum_{e \mid 2 \cdot p_1 \cdots \widehat{p_i} \cdots p_k} \mu(e)\left[2^{n/e} - 2^{n/e \cdot p_i}\right]$$

$$2^{n/e} - 2^{n/e \cdot p_i} = \underbrace{2^{n/e \cdot p_i}\left(2^{\frac{n}{e \cdot p_i}(p_i - 1)} - 1\right)}_{\text{è un multiplo di } p_i^{\alpha_i}}$$

$\varphi(p_i^{\alpha_i}) = (p-1) \cdot p_i^{\alpha_i - 1}$ divide l'esponente.

Posso risolvere il problema anche con qualsiasi $b \geq 1$ al posto di 2 (x CASA).

$$b^n = \sum_{d \mid n} a_d$$

Uno potrebbe verificare a mano che definita

$$\mu(n) = \begin{cases} 0 & \text{--} \\ 1 & \text{--} \\ -1 & \text{--} \end{cases}$$

come sopra

Se $b_n := \sum_{d \mid n} a_d$ allora $a_n = \sum_{d \mid n} b_d \cdot \mu\left(\frac{n}{d}\right)$

Infatti $\sum_{d \mid n} b_d \, \mu\left(\frac{n}{d}\right) = \sum_{d \mid n} \sum_{e \mid d} a_e \cdot \mu\left(\frac{n}{d}\right) =$

$$= \sum_{e \mid n} a_e \cdot \left[\sum_{d' \mid \frac{n}{e}} \mu\left(\frac{n}{d'}\right)\right] = a_n$$

TDN 2 ADVANCED

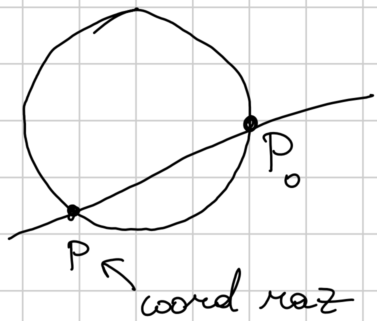
darkcrystal

Titolo nota 06/09/2018

Parametrizzazioni (delle cubiche singolari)

(x, y) razionali su $x^2+y^2=1$

$P_0 = (1, 0)$



$$\begin{cases} x^2+y^2=1 \\ y = m(x-1) \end{cases}$$

$y = m(x-1)$
con $m \in \mathbb{Q}$

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

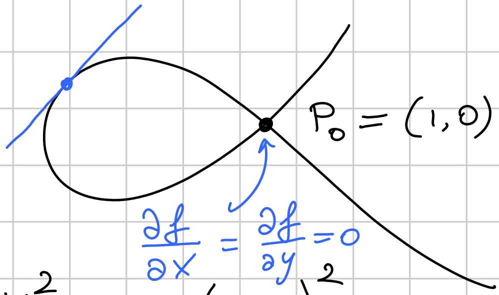
$$x_1 = 1 \qquad x_2 = \frac{m^2-1}{m^2+1} \rightsquigarrow y = \frac{-2m}{m^2+1}$$

$$(x, y) = \left(\frac{1-m^2}{1+m^2}, \frac{2m}{m^2+1}\right)$$

Terne pitagoriche: $a^2+b^2=c^2$

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$$

Cubica singolare:



$$f(x,y) = y^2 - x(x-1)^2$$

$$y^2 = x(x-1)^2$$

$(1,0) + t(a,b)$ ← posso supporre (a,b) interi coprimi

$$y = tb \qquad x = 1 + ta$$

$$t^2 b^2 = (1+ta)\, t^2 a^2$$

$$\Downarrow$$

$t = 0$ oppure $\left(\frac{b^2}{a^2} - 1\right) \cdot \frac{1}{a} = t$

Parametrizz.: $(1,0) + \left(\frac{b^2 - a^2}{a^3}\right)(a,b)$

IMO SL 2014 N2

$$\sqrt[3]{7x^2 - 13xy + 7y^2} = |x-y| + 1$$

Wlog $x > y$.

$$0 = \overbrace{7x^2 - 13xy + 7y^2 - \left(1 + 3(x-y) + 3(x-y)^2 + (x-y)^3\right)}^{f(x,y)}$$

Deriviamo!
$$\begin{cases} 0 = 14x - 13y - \left(3 + 6(x-y) + 3(x-y)^2\right) \\ 0 = -13x + 14y - \left(-3 + 6(x-y)(-1) - 3(x-y)^2\right) \\ f(x,y) = 0 \end{cases}$$

$$\begin{cases} 0 = x+y \\ 0 = 14x + 13x - \left(3 + 12x + 12x^2\right) \\ 0 = 7x^2 + 13x^2 + 7x^2 - \left(1 + 6x + 12x^2 + 8x^3\right) \end{cases}$$

$$\begin{cases} y = -x \\ 0 = -12x^2 + 15x - 3 \\ 0 = -8x^3 + 15x^2 - 6x - 1 \end{cases} \qquad \left\{ \begin{array}{cc} x=1, & \pm 1/4 \\ \text{OK} & \text{NO} \end{array} \right.$$

Punto bello: $(1, -1)$

$$\begin{cases} x = 1 + at \\ y = -1 + bt \end{cases} \qquad \text{con } a, b \text{ interi coprimi}$$

$$7(1+at)^2 - 13(1+at)(-1+bt) + 7(-1+bt)^2 =$$
$$= 1 + \left(2 + t(a-b)\right)^3 + 3\left(2 + t(a-b)\right)^2 + 3\left(2 + t(a-b)\right)$$

$$7a^2t^2 - 13abt^2 + 7b^2t^2 = t^3(a-b)^3 + 3 \cdot 2 \cdot t^2(a-b)^2$$
$$+ 3t^2(a-b)^2$$

$$t = \frac{-2a^2 + 5ab - 2b^2}{(a-b)^3}$$

Tutte le soluz. raz:
$$\begin{cases} 1 + a\,\dfrac{-2a^2 + 5ab - 2b^2}{(a-b)^3} \\ -1 + b\,\dfrac{-2a^2 + 5ab - 2b^2}{(a-b)^3} \end{cases}$$

Se $p \mid a-b$, $p \nmid a$

$$\begin{aligned}-2a^2+5ab-2b^2 &\equiv -2a^2+5a^2-2a^2 \\ &\equiv a^2 \mod p \\ &\not\equiv 0\end{aligned}$$

Soluzioni intere: $a = b \pm 1$

Seconda applicazione Numero delle coppie (x,y) t.c.

$$x^2+y^2 \equiv 1 \pmod p$$

$(x_0, y_0) = (1,0)$ funziona

Sia (x,y) una qualunque soluz. con $x \neq 1$

Allora definisco $m = \frac{y}{x-1} \in \mathbb{Z}/p\mathbb{Z}$

e (x,y) è soluzione di $\begin{cases} x^2+y^2 \equiv 1 & (p) \\ y \equiv m(x-1) & (p) \end{cases}$

$$\begin{cases} x^2 + m^2(x-1)^2 \equiv 1 & (p) \\ y \equiv m(x-1) \end{cases}$$

$$\Rightarrow \begin{cases} x+1 + m^2(x-1) \equiv 0 & (p) \\ y \equiv m(x-1) & (\bmod p) \end{cases}$$

$$\begin{cases} x \equiv \dfrac{m^2-1}{m^2+1} \mod p \\ y \equiv m(x-1) \mod p \end{cases}$$

Caso 1: $p \equiv 3 \mod 4$. La param. funziona per ogni m, quindi trovo p soluzioni $+ 1$ trovata all'inizio

Caso 2: $p \equiv 1$ (4). Ci sono 2 valori "proibiti" per m $\rightsquigarrow$ $p-1$ soluzioni

Sollevamento di Hensel

Macchinario per passare da congruenze mod p a congruenze mod p^n

Lemma Sia $f(x) \in \mathbb{Z}[x]$ e $a \in \mathbb{Z}$.

Supponiamo: $\begin{cases} f(a) \equiv 0 \mod p \\ f'(a) \not\equiv 0 \mod p \end{cases}$

Allora $\forall n$ esiste una soluzione della congr.

$$f(x) \equiv 0 \mod p^n$$

Dim $\boxed{p \to p^2}$ $\quad f(x) = f(a) + (x-a)\, q(x)$

Scelgo $x = a + pK$

$$f(a+pK) = f(a) + pK\, q(a+pK)$$

Scrivo $f(a) = pm$: voglio risolvere

$$0 \equiv pm + pK\, q(a+pK) \mod p^2$$

$$0 \equiv m + K\, q(a) \mod p$$

Si risolve $\Leftarrow$ $q(a) \not\equiv 0 \mod p \iff f'(a) \not\equiv 0\ (p)$

D'altro canto, se derivo $f(x) = f(a) + (x-a)\, q(x)$

trovo $f'(x) = q(x) + (x-a)\, q'(x)$

$\Rightarrow f'(a) = q(a)$

D

Conseguenza $a \not\equiv 0\ (p)$ è residuo quadr. mod p^n

$(n \geq 1,\ p$ dispari$)$ $\iff$ lo è mod p

$f(x) = x^2 - a \qquad f'(x) = 2x$

Ipotesi: $x^2 - a \equiv 0\ (p)$ abbia una soluzione

Se $b^2 \equiv a \pmod p \Rightarrow f'(b) = 2b \not\equiv 0\ (p)$

Esercizio $y^2 = p^3 + 10p^2 - 6p + 1$

Mod $p \longrightarrow y^2 \equiv \pm 1$ mod $p \xrightarrow{\text{"wlog"}} y \equiv 1\ (p)$

Mod p^2: $y = 1 + kp$

$1 + 2kp \equiv -6p + 1$ mod p^2

$2k \equiv -6$ mod p — $p = 2$, NO; $k \equiv -3\ (p)$

$\Rightarrow y \equiv 1 - 3p$ mod p^2

$y = 1 - 3p + kp^2 \Rightarrow 1 + 9p^2 - 6p + 2kp^2 \equiv 1 - 6p + 10p^2$ mod p^3

$$2Kp^2 \equiv p^2 \mod p^3$$

$$2K \equiv 1 \mod p$$

$$\Rightarrow \quad y = 1 - 3p + \frac{p+1}{2} p^2 + \underbrace{\text{multiplo di } p^3}_{jp^3}$$

Supponiamo $j < 0 \Rightarrow y \leq 1 - 3p + \frac{p+1}{2} p^2 - p^3$

$$\leq -p^3/2 + p^2/2 - 3p + 1$$

$$\leq -p^3/2 + p^2/2$$

$$\begin{array}{c} y^2 \geq \frac{1}{4}(p^3 - p^2)^2 \geq \frac{1}{4} p^4 (p-1)^2 \geq p^4 \\ \wedge\!\!| \\ p^3 + 10p^2 - 6p + 1 \leq p^3 + 10p^2 \end{array}$$

$$p^2 \leq p + 10$$

$$\Rightarrow p \leq 3$$

e similmente per $j \geq 0$

Uniche sol: $p = 3$, $y = \pm 10$

Soluzioni di $a^2+b^2=2c^2 \iff \left(\frac{a}{c}\right)^2+\left(\frac{b}{c}\right)^2=2$

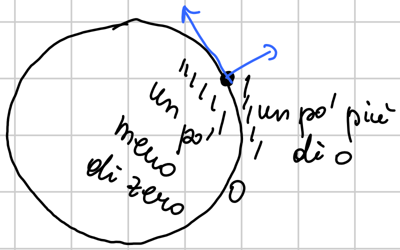
Come prima! $a=b=c=1$ $\qquad x^2+y^2=2$

$$\begin{aligned} x &= 1+at \\ y &= 1+bt \end{aligned}$$

sviluppo, faccio il conto, viene

Fatto (difficile) Per le equaz. di 2° grado in 2 variabili razionali: c'è una soluz razionale se e solo se ci sono soluz mod p^n $\forall p\ \forall n$

$\boxed{\text{Tangenti}}$ $\qquad f(x,y)=0 \qquad (x_0,y_0)$ t.c. $f(x_0,y_0)=0$



x^2+y^2-1

La direzione di max crescita è

$$\begin{pmatrix} \frac{\partial f}{\partial x}(x_0,y_0) \\ \frac{\partial f}{\partial y}(x_0,y_0) \end{pmatrix}$$

$$f(x,y) = f(x_0,y_0) + \frac{\partial f}{\partial x}\cdot(x-x_0) + \frac{\partial f}{\partial y}(y-y_0) + \dots$$

$$= \begin{pmatrix} \partial f/\partial x \\ \partial f/\partial y \end{pmatrix} \cdot \begin{pmatrix} x-x_0 \\ y-y_0 \end{pmatrix} + \text{cose piccole}$$

Morale: la tg e' perpendicolare a $\begin{pmatrix} \partial f/\partial x \\ \partial f/\partial y \end{pmatrix}$

Esempio $f(x,y) = x^2+y^2-1$

$$\partial f/\partial x = 2x \qquad \partial f/\partial y = 2y$$

Prendiamo $(x,y) = \left(1/\sqrt{2}, 1/\sqrt{2}\right)$

Direzione max crescita : $/\!/ \begin{pmatrix} \sqrt{2} \\ \sqrt{2} \end{pmatrix} /\!/ \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

$$\text{tg} \;/\!/\; \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Hensel in 2 variabili

$$f(x,y) \in \mathbb{Z}[x,y] \quad ; \quad f(a,b) \equiv 0 \mod p$$

Se $\frac{\partial f}{\partial x}(a,b) \not\equiv 0$ OPPURE $\frac{\partial f}{\partial y}(a,b) \not\equiv 0 \;(p)$

allora trovo soluzioni modulo p^n

Contare soluzioni mod p

$$x^2+y^2 \equiv 1 \pmod{p}$$

$$\sum_{a+b=1} N(x^2 \equiv a) \cdot N(y^2 \equiv b) =$$

$$= \sum_{a+b=1} \left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{b}{p}\right)\right) =$$

$$= \underbrace{\sum_{a+b=1} 1}_{p} + \underbrace{\sum_{a+b=1} \left(\frac{a}{p}\right)}_{0} + \underbrace{\sum_{a+b=1} \left(\frac{b}{p}\right)}_{0} + \sum_{a+b=1} \left(\frac{ab}{p}\right)$$

$$= p + \sum_{\substack{a+b=1 \\ b\neq 0}} \left(\frac{a/b}{p}\right) = p + \sum_{a\neq 1} \left(\frac{a/(1-a)}{p}\right)$$

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

$$\iff a = \frac{c}{c+1}$$

$$\sum_{a\neq 1} \left(\frac{a/(1-a)}{p}\right) = \sum_{c\neq -1} \left(\frac{c}{p}\right) = -\left(\frac{-1}{p}\right)$$

$$\#\{(x,y) \mid x^2+y^2 \equiv 1 \ (p)\} = p - \left(\frac{-1}{p}\right)$$

$\boxed{\text{CARATTERI}}$ Un carattere è una funzione

$$\chi : \mathbb{F}_p^* \longrightarrow \{1, \zeta_{p-1}, \dots, \zeta_{p-1}^{p-2}\}$$

tale che $\chi(ab) = \chi(a)\chi(b)$

[in soldoni: $\chi(g) = \zeta_{p-1}^{a}$

$\chi(g^i) = \zeta_{p-1}^{ai}$]

NON NECESSARIAMENTE $(a, p-1) = 1$

Esempio $\chi(n) = \left(\frac{n}{p}\right)$

Per comodità: $\chi(0) = 0$

Domanda Quanti caratteri ci sono? $p-1$

Uno di questi è il carattere che fa sempre 1

Per questo carattere χ_0 si pone $\chi_0(0) = 1$

Fissiamo χ carattere. Quanto fa $\sum_{a \in \mathbb{F}_p} \chi(a) = 0$?

(se $\chi \neq \chi_0$)

$$\sum_{a \in \mathbb{F}_p} \chi(a) = \sum_{a \neq 0} \chi(a) = \sum \chi(g^i)$$

$$= \sum_{i=0}^{p-2} \zeta_{p-1}^{bi} = 0$$

Viceversa: $\displaystyle\sum_{\chi} \chi(a) = \sum_{b=0}^{p-2} \zeta_{p-1}^{bi} = 0$

$a = g^i$

Def. χ è di ordine $n \mid p-1$ se la sua immagine ha ordine n

Ex $\left(\frac{\cdot}{p}\right)$ ha ordine 2

Lemma Sia χ un carattere di ordine $n \mid p-1$

Allora $\displaystyle N\left(x^n \equiv a \mod p\right) = \sum_{i=0}^{n-1} \chi(a)^i$

Dim. Se c'è una soluz. ce ne sono n.

$N(x^n \equiv 1 \ (p)) = n \qquad g^{\frac{p-1}{n}}, g^{2\frac{p-1}{n}}, \dots$

Soluzioni $\Leftrightarrow a \equiv g^{nk}$

$$\sum_{i=0}^{n-1} \chi(a)^i = \sum_{i=0}^{n-1} 1^i = n$$

No soluz $\Leftrightarrow a \equiv g^r$ con $n \nmid r$

$\Leftrightarrow \chi(a) = \zeta_n^r$

$$\sum_{i=0}^{n-1} \zeta_n^{r} = 0 \text{ se } n \nmid r \qquad \square$$

Supponiamo ora di voler contare

$$N(x^5+y^2-1 \equiv 0\ (p)) = \begin{cases} p, & \text{se } p \not\equiv 1\ (5) \\ ?? & \text{se } p \equiv 1\ (5) \end{cases}$$

Fissiamo χ carattere di ordine 5

$$\sum_{a+b=1} N(x^5 \equiv a\ (p))\, N(y^2 \equiv b\ (p))$$

$$= \sum_{a+b=1} \left(1+\chi(a)+\dots+\chi(a)^4\right)\left(1+\left(\frac{b}{p}\right)\right)$$

$$= p + \underset{\sum \chi}{0} + \underset{\sum \chi^2}{0} + \underset{\sum \chi^3}{0} + \underset{\sum \chi^4}{0} + \underset{\sum \left(\frac{b}{p}\right)}{0}$$

$$+ \underbrace{\sum_{a+b=1} \chi(a)\left(\frac{b}{p}\right)}_{\sim \sqrt{p}} + \dots$$

Somme di Gauss

$$g_a(\chi) = \sum_{t \in \mathbb{Z}/p\mathbb{Z}} \chi(t)\, \zeta_p^{at}$$

① $$g_a(\chi) = \sum_t \chi(t)\, \zeta_p^{at} = \frac{1}{\chi(a)} \sum_t \chi(at)\, \zeta_p^{at}$$

$$= 1/\chi(a) \sum_t \chi(t)\, \zeta_p^{t} = \chi(a^{-1})\, g_1(\chi)$$

(2) $\sum_a g_a(\chi)\overline{g_a(\chi)} =$

$\sum_a \|g(\chi)\|^2 \chi(a^{-1})\overline{\chi(a^{-1})} = \|g(\chi)\|^2 \cdot (p-1)$

Ma è anche $= \sum_a \sum_{t_1} \chi(t_1)\zeta_p^{at_1} \overline{\left(\sum_{t_2} \chi(t_2)\zeta_p^{at_2}\right)}$

$= \sum_{a,t_1,t_2} \zeta_p^{a(t_1-t_2)} \chi(t_1)\chi(t_2)^{-1}$

$= \sum_{t_1=t_2} (p-1)\chi(t_1)\chi(t_2^{-1})$

$= \sum_{t_1} (p-1)\chi(t_1 \cdot t_1^{-1}) = p(p-1)$

Conseguenza: $\|g(\chi)\| = \sqrt{p}$

Corollario: $\sum_t \chi(t)\zeta_p^t = \sum_{t=\square} \zeta_p^t - \sum_{t\neq\square} \zeta_p^t$

Legendre

ha valore assoluto $\sqrt{p}$; in realtà è

proprio $\pm\sqrt{\pm p}$

$\zeta_5 + \zeta_5^4 - \zeta_5^2 - \zeta_5^3 = \sqrt{5}$

Teorema Se χ_1, χ_2 sono caratteri con $\chi_1 \neq 1$, $\chi_2 \neq 1$, $\chi_1 \chi_2 \neq 1$ allora

$$\sum_{a+b=1} \chi_1(a)\chi_2(b) = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}$$

In particolare $\left| \sum_{a+b=1} \chi_1(a)\chi_2(b) \right| = \sqrt{p}$

Tornando al conto di prima:

$$N(y^2+x^5 \equiv 1 \ (p)) = \sum_{a+b=1} \left(1+\chi(a)+\dots+\chi(a)^4\right)\left(1+\left(\frac{b}{p}\right)\right)$$

$= p + 4$ termini di ordine $\sqrt{p}$

$$N(ay^2+bx^3 \equiv c \ (p)) =$$

$$= \sum_{u+v=c} N(ay^2=u)\,N(bx^3=v)$$

$$= \sum_{u+v=c} N(y^2=a^{-1}u)\,N(x^3=b^{-1}v)$$

$$= \sum_{u+v=c} \left(1+\left(\frac{a^{-1}u}{p}\right)\right)\left(1+\chi(b^{-1}v)+\chi(b^{-1}v)^2\right)$$

$$= p + \sum_{u+v=c} \left(\frac{a^{-1}u}{p}\right)\chi(b^{-1}v) + \dots$$

$$= p + \left(\frac{a^{-1}}{p}\right)\chi(b^{-1}) \sum_{\substack{u+v=c \\ cu'+cv'=c}} \left(\frac{u}{p}\right)\chi(v) + \dots$$

$$= p + \left(\frac{a^{-1}}{p}\right)\chi(b^{-1})\left(\frac{c}{p}\right)\chi(c) \underbrace{\sum_{u'+v'=1}\left(\frac{u'}{p}\right)\chi(v')}_{\text{la sappiamo!}}$$

$\boxed{\text{Morale}}$ Numero di soluz è p + errore

che è $\leq K\sqrt{p}$, $K = \prod(\text{esponenti} - 1)$

Ha senso controllare mod p solo per p "piccolo" (cioè $p - K\sqrt{p} < 0$)

E di solito (Hensel) andare mod p^n non serve a niente

Cosa fare quando tutto fallisce?

$$2y^2 = x^4 - 17$$

1 ✓ Dim che ci sono soluz mod p^n $\forall p\ \forall n$

2 • Dim che non ci sono soluzioni intere

Moduli: ≤ 7, oppure 17

2 • Idea: combinare informazioni modulo primi diversi con la reciprocità quadratica

Unici primi che ha senso guardare: quelli modulo i quali ci sono solo 2 termini.

Guardiamo modulo un divisore p di y

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

$$= \begin{cases} \left(\frac{q}{p}\right) & \text{se } p \equiv 1\ (4) \text{ o } q \equiv 1\ (4) \\ -\left(\frac{q}{p}\right) & \text{se } p \equiv q \equiv 3\ (4) \end{cases}$$

Sia $p \mid y$. Allora $0 \equiv x^4 - 17 \mod p$

$$\Rightarrow \left(\frac{17}{p}\right) = +1 \overset{RQ}{\Rightarrow} \left(\frac{p}{17}\right) = +1$$

e' se $p=2$?

Quindi $y \equiv z^2 \mod 17$

$$2z^4 \equiv x^4 \quad (\mathrm{mod}\ 17)$$

Siccome $z \not\equiv 0\ (17) \Rightarrow 2 \equiv (x/z)^4 \mod 17$

$$\Rightarrow 2^4 \equiv (x/z)^{16} \equiv 1 \quad (17)$$

NON E' VERO! :)

Due equazioni della stessa razza:

$$y^2 = x^3 - x^2 + 8$$

$$y^2 = x^3 + 7$$

Vediamo che la seconda ha soluzione mod p $\forall p$

$$\sum_{x \in \mathbb{F}_p} 1 + \left(\frac{x^3+7}{p}\right) \equiv \sum_{x \in \mathbb{F}_p} (x^3+7)^{\frac{p-1}{2}}$$

$$\equiv \sum_{x} \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} x^{3j}\, 7^{\frac{p-1}{2}-j} \quad (p)$$

$$\equiv \sum_{j=0}^{(p-1)/2} \binom{\frac{p-1}{2}}{j} 7^{\frac{p-1}{2}-j} \sum_{x \in \mathbb{F}_p} x^{3j} \quad (p)$$

$$\overset{p\equiv 1(3)}{\equiv} -\binom{\frac{p-1}{2}}{\frac{p-1}{3}} 7^{\frac{p-1}{6}} \pmod{p}$$

Congruenza + bound di prima $\Rightarrow$ numero esatto!

TDN ADVANCED 3 (PELL ...)

Titolo nota 07/09/2018

Equazione di Pell

$$x^2 - dy^2 = 1 \qquad d \in \mathbb{Z} \qquad d \neq \square$$

$$(x - \sqrt{d}\, y)(x + \sqrt{d}\, y)$$

Def. $N(x + y\sqrt{d}) = x^2 - dy^2$

$$N\left((x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d})\right) = N(x_1 + y_1\sqrt{d})\,N(x_2 + y_2\sqrt{d})$$

Oss Supponiamo di conoscere una soluz di

$x_1^2 - dy_1^2 = m$ e una di $x_2^2 - dy_2^2 = n$

Allora conosciamo una sol di $x_3^2 - dy_3^2 = mn$

$N(x_1 + \sqrt{d}\, y_1) = m$, $N(x_2 + \sqrt{d}\, y_2) = n$

Posso prendere $x_3 = x_1 x_2 + d y_1 y_2$

$$y_3 = x_1 y_2 + x_2 y_1$$

TEOREMA Esistono ∞ soluzioni intere di

$$x^2 - dy^2 = 1$$

Dim Per Dirichlet esistono infinite coppie (p,q) di interi positivi t.c.

$$\left| \sqrt{d} - p/q \right| < \frac{1}{q^2}$$

Uno vorrebbe prendere $x=p$ e $y=q$

$$|x^2 - dy^2| = |(x - y\sqrt{d})(x+y\sqrt{d})|$$

$$= \Big| y \underbrace{\left(\frac{x}{y} - \sqrt{d}\right)}_{< 1/y^2} (x+y\sqrt{d}) \Big| \le \frac{x+y\sqrt{d}}{y}$$

$$\lesssim 2\sqrt{d} + 1$$

Per pigeonhole, c'è un qualche intero k, con $|k| \le 2\sqrt{d}+1$, che si scrive come

$$p^2 - dq^2 = k$$

per infinite coppie (p,q)

Prendiamone 2, (p_1,q_1) e (p_2,q_2)

$$N\left(\frac{p_1+q_1\sqrt{d}}{p_2+q_2\sqrt{d}}\right) = \frac{N(p_1+q_1\sqrt{d})}{N(p_2+q_2\sqrt{d})} = \frac{k}{k} = 1$$

$$\frac{p_1+q_1\sqrt{d}}{p_2+q_2\sqrt{d}} = A + B\sqrt{d} \quad \text{con } A, B \text{ razionali}$$

$$\frac{(p_1+q_1\sqrt{d})(p_2-q_2\sqrt{d})}{(p_2+q_2\sqrt{d})(p_2-q_2\sqrt{d})} = \frac{(p_1p_2-dq_1q_2)+(p_2q_1-q_2p_1)\sqrt{d}}{K}$$

Affinché i coeff. siano interi occorre e basta che

$$\begin{cases} p_1p_2 - d\,q_1q_2 \equiv 0\ (K) \\ p_2q_1 - q_2p_1 \equiv 0\ (K) \end{cases} \qquad q_1/q_2 \equiv p_1/p_2\ (K)$$

Se per caso $p_1 \equiv p_2\ (K)$ e $q_1 \equiv q_2\ (K)$

avremmo vinto (2^a congr. OK; prima congr:

$$p_1^2 - d\,q_1^2 = K \equiv 0\ (K)\ )$$

E queste esistono perché originariamente

avevamo infinite coppie.

Sia (x_0, y_0) una soluzione, $u = x_0 + \sqrt{d}\,y_0$.

Allora $N(u) = 1 \implies N(u^K) = 1 \quad \forall K \geq 0$

Non solo: anche $N(u^{-K}) = 1$

$$u^{-1} = \frac{1}{x_0+\sqrt{d}\,y_0} \cdot \frac{x_0-\sqrt{d}\,y_0}{x_0-\sqrt{d}\,y_0} = \frac{x_0-\sqrt{d}\,y_0}{x_0^2-dy_0^2}$$

$$= x_0 - \sqrt{d}\,y_0 \qquad \square$$

Struttura di tutte le soluzioni

Esiste $u = x_0 + \sqrt{d}\, y_0$ con $N(u) = 1$

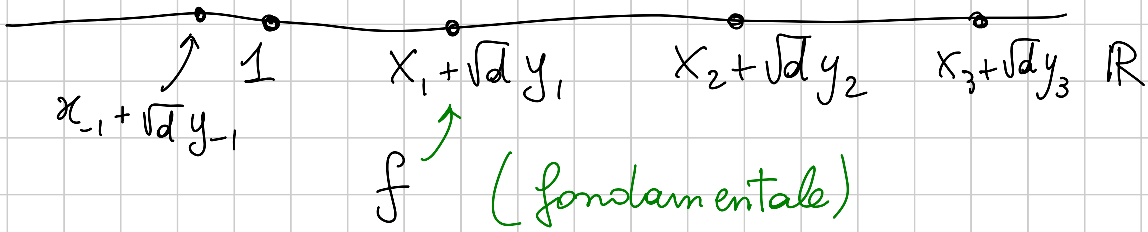
tale che TUTTE le soluzioni "siano" del

tipo $\pm u^k$ con $k \in \mathbb{Z}$

Più precisamente: $$x = \frac{(x_0 + \sqrt{d}\, y_0)^k + (x_0 - \sqrt{d}\, y_0)^k}{2}$$

$$= \frac{u^k + u^{-k}}{2}$$

e $$y = \frac{u^k - u^{-k}}{2\sqrt{d}}$$



Sia f il minimo numero reale > 1 che si

scrive come $x + \sqrt{d}\, y$, $x^2 - dy^2 = 1$

Sia poi $s = a + b\sqrt{d}$ una soluzione.

Anche $s \cdot f^k$, $k \in \mathbb{Z}$, sono soluzioni.

Scelgo k in modo che

$$1 \leq \underbrace{s \cdot f^k}_{} < f$$

soluzione! Per minimalità di f, è $= 1$

$$\Rightarrow s = f^{-k}$$

$\square$

FRAZIONI DI FAREY

$$x^2 - 5y^2 = 1$$

$$\frac{2}{1} < \sqrt{5} < \frac{3}{1} \leadsto \frac{2+3}{1+1} = 5/2$$

$$\frac{2}{1} < \sqrt{5} < \frac{5}{2} \leadsto \frac{2+5}{1+2} = 7/3$$

$$\frac{2}{1} < \sqrt{5} < \frac{7}{3} \leadsto \frac{2+7}{1+3} = 9/4 \quad \text{ECCOLA!}$$

Soluzione fondamentale: $9 + 4\sqrt{5}$

Pell generalizzate

$$x^2 - dy^2 = a \qquad\qquad \overset{f}{x^2 - dy^2 = 1}$$

Supponiamo che almeno una soluzione (x_0, y_0) esista. Allora $(x_0 + y_0\sqrt{d}) \cdot f^k$ sono ancora soluzioni

① Bound su una soluzione

Sia $s = x_0 + y_0\sqrt{d}$ una soluzione. Allora posso scegliere k t.c. $S = s f^k \in \left[\frac{\sqrt{a}}{\sqrt{f}}, \sqrt{a}\cdot\sqrt{f}\right]$

$$x = \frac{S + \text{coniugato}(S)}{2} = \frac{S + a/S}{2}$$

$$\leq \frac{1}{2}\max\left\{\sqrt{\frac{a}{f}} + \sqrt{a}\cdot\sqrt{f},\ \sqrt{a}\cdot\sqrt{f} + \frac{\sqrt{a}}{\sqrt{f}}\right\}$$

$$= \frac{1}{2}\sqrt{a}\left(\sqrt{f} + \frac{1}{\sqrt{f}}\right) \qquad (a > 0 \ldots)$$

② Famiglie di soluzioni

Vorremmo prendere due soluz. $N(s_1) = N(s_2) = a$ e dividere una per l'altra

$$\frac{x_1 + \sqrt{d}\,y_1}{x_2 + \sqrt{d}\,y_2} \cdot \frac{x_2 - \sqrt{d}\,y_2}{x_2 - \sqrt{d}\,y_2} = \frac{(x_1x_2 - dy_1y_2) + \sqrt{d}(x_2y_1 - x_1y_2)}{a}$$

Facciamo il caso $(x_1, a) = (x_2, a) = 1$

$(y_1, a) = (y_2, a) = 1$

$$\begin{cases} x_1x_2 - dy_1y_2 \equiv 0 \mod a \\ y_1/x_1 \equiv y_2/x_2 \mod a \end{cases}$$

$$0 \equiv x_1 - dy_1(y_2/x_2) \equiv x_1 - dy_1(y_1/x_1)$$

$$\equiv \frac{1}{x_1}(x_1^2 - dy_1^2) \equiv 0 \ (a)$$

Due soluz. stanno nella stessa famiglia se e solo se hanno lo stesso $(y/x \mod a)$

$\Rightarrow$ # famiglie $\leq \varphi(|a|)$

ESERCIZI

- $x^4 - 2y^2 = 17$ con le Pell
- $p \equiv 1\ (4) \Rightarrow x^2 - py^2 = -1$ ha ∞ soluz

  $p = a^2 + b^2$ con a dispari $\Rightarrow x^2 - py^2 = a$ si risolve
- $x^2 - 5183y^2 = 2$: si risolve?

SOLUZIONI

$$x^2 - 5183y^2 = 2 \qquad 5183 = 71 \cdot 73 = (72+1)(72-1)$$

$$\frac{71}{1} < \sqrt{5183} < \frac{72}{1} \qquad \text{Fondamentale: } 72 + \sqrt{5183} \approx 144$$

$$|x| \leq \frac{1}{2}\sqrt{a}\left(\sqrt{f} + \frac{1}{\sqrt{f}}\right) = \frac{1}{2}\sqrt{2}\,(12+1) < 13$$

quindi no soluz perché $x^2 - 5183y^2 \leq$
$\leq x^2 - 5183 < 0$

Più in generale: $x^2 - (n^2-1)\,y^2 = m$

allora o $m = \square$ oppure $|m|$ è "grandicello" rispetto a n.

- $x^2 - py^2 = -1 \qquad N(s) = -1$

  $p \equiv 1 \ (4) \qquad N(s^2) = 1$

  $f = a + b\sqrt{p}$ la fondamentale

  se $\sqrt{f} = x + y\sqrt{p} \implies N(\sqrt{f}) = -1$

  $1 \leq \sqrt{f} \leq f$

$$\begin{cases} x^2 + py^2 = a \\ 2xy = b \end{cases}$$

$$a^2 - pb^2 = 1$$
$$\Downarrow$$
$$(a+1)(a-1) = pb^2$$

$a^2 - b^2 \equiv 1 \mod 4 \Rightarrow a$ disp, b pari

$b = 2c$
$$\underbrace{\left(\frac{a+1}{2}\right)}_{\substack{p\square \\ \square}}\underbrace{\left(\frac{a-1}{2}\right)}_{\substack{\square \\ p\square}} = pc^2$$

$$\frac{a\pm1}{2} = \underset{x^2}{\square}, \quad \frac{a\mp1}{2} = p\underset{y^2}{\square} \Rightarrow a = \square + p\square = x^2 + py^2$$

e $\quad 2xy = 2\sqrt{\left(\frac{a\pm1}{2}\right)\left(\frac{a\mp1}{2p}\right)} = \sqrt{\frac{a^2-1}{p}} = b$

$x^2 - py^2 = a \qquad p = a^2 + b^2$

$$\begin{cases} b^2 - p\cdot1 = -a^2 \\ x^2 - py^2 = -1 \text{ ha soluz} \end{cases} \Rightarrow x^2 - py^2 = +a^2$$

- $x^4 - 2y^2 = 17 \rightsquigarrow z^2 - 2y^2 = 17$

Famiglie di soluzioni: determinate da $z/y \mod 17$

$$\left(z/y\right)^2 \equiv 2 \mod 17 \Rightarrow z/y \equiv \pm 6 \mod 17$$

$$z^2 - 2y^2 = 1 \qquad f = 3 + 2\sqrt{2}$$

Soluzione di $z^2 - 2y^2 = 17$: $z = 5,\ y = 2$

$z = -5,\ y = 2$

Tutte le soluz sono del tipo

$$z = \pm \frac{1}{2}\left[\left(\pm 5 + 2\sqrt{2}\right) \cdot \left(3 + 2\sqrt{2}\right)^k + \left(\pm 5 - 2\sqrt{2}\right)\left(3 - 2\sqrt{2}\right)^k\right]$$

$z = \square \Rightarrow z > 0 \Rightarrow$ o $+, +$

o $-, -$

$$z = \frac{1}{2}\left[\left(5 \pm 2\sqrt{2}\right)\left(3 + 2\sqrt{2}\right)^k + \text{coniugato}\right]$$

$$\begin{cases} z_{k+1} = 6 z_k - z_{k-1} \\ z_0 = 5 \ / \ 5 \\ z_1 = 23 \ / \ 7 \end{cases}$$

Modulo 8! z_k mod 8 e' $5, 7, 5, 7, \ldots$

$2+2\sqrt{28n^2+1}$ intero $\Rightarrow$ quadrato

$y^2 = 28n^2+1 \qquad y^2 - 7\cdot 2^2 n^2 = 1$

$y^2 - 7x^2 = 1$

$y=8,\ x=3 \qquad 8+3\sqrt{7} = f$

Conto $\Rightarrow$ in $\dfrac{f^k + f^{-k}}{2}$ il coeff di $\sqrt{7}$ è

pari se e solo se k è pari

$2+2\sqrt{28n^2+1} = 2+2y = 2+f^{2m}+f^{-2m}$

$= \left(f^m + f^{-m}\right)^2$

f_{28} : $127+24\sqrt{28} = \left(8+3\sqrt{7}\right)^2$

$X^2+1 = 5^n$ $\quad$ n pari OK

$n = 2K+1$

$X^2+1 = 5\cdot y^2$ $\quad$ $y = 5^K$

$X^2 - 5y^2 = -1$ $\quad$ Soluzione : $2+\sqrt{5}$

Fondam : $9+4\sqrt{5}$
$= (2+\sqrt{5})^2$

Tutte le soluz: $(2+\sqrt{5})^{2r+1}$

$$y = \frac{1}{2\sqrt{5}}\left((2+\sqrt{5})^{2r+1} - (2-\sqrt{5})^{2r+1} \right)$$

$v_5(y) = v_5(2r+1)$ per una opportuna versione di LTE

$$\frac{(2+\sqrt{5})^{2r+1}}{2\sqrt{5}} \lesssim y = 5^{v_5(y)} = 5^{v_5(2r+1)}$$

LTE "generale"

$$\frac{(2+\sqrt{5})^K - (2-\sqrt{5})^K}{2\sqrt{5}} \quad \text{con } (K,5)=1 :$$

$$= \frac{1}{2\sqrt{5}}\Big(\cancel{2^K} + K\cdot 2^{K-1}\sqrt{5} + \cancel{\binom{K}{2}2^{K-2}\cdot 5} + \binom{K}{3}2^{K-3}\cdot 5\cdot\sqrt{5} + \dots$$
$$- \cancel{2^K} + K\cdot 2^{K-1}\sqrt{5} - \cancel{\binom{K}{2}2^{K-2}\cdot 5} + \binom{K}{3}2^{K-3}\,5\sqrt{5} \Big)$$

Stesso conto quando $K=5$.

Risolubilità di $x^2-2y^2=p$

Necessario: $\left(\frac{2}{p}\right)=+1 \iff p\equiv \pm 1\ (8)$

$(x-\sqrt{2}\,y)(x+\sqrt{2}\,y)=p \rightsquigarrow \mathbb{Z}[\sqrt{2}]$ FATTORIZZAZIONE UNICA

Siccome $\left(\frac{2}{p}\right)=+1$, esiste n t.c. $p \mid n^2-2$

$\Longrightarrow p \mid (n-\sqrt{2})(n+\sqrt{2})$

$n+\sqrt{2} = p\cdot(a+b\sqrt{2})$ NO!

$\Longrightarrow$ p non è primo $\Rightarrow$ p non è irriducibile

$p=(a+b\sqrt{2})(c+d\sqrt{2})$

$$\underbrace{N(p+0\sqrt{2})}_{=p^2} = N(a+b\sqrt{2})\,N(c+d\sqrt{2}) = \underbrace{(a^2-2b^2)}_{\neq \pm 1}\underbrace{(c^2-2d^2)}_{\neq \pm 1}$$

Quindi sono $\pm p$!

$$p = ac + 2bd + \sqrt{2}\,(bc + ad)$$

$$bc = -ad \qquad a^2 - 2b^2 = c^2 - 2d^2 = \pm p$$

$(a,b) = (c,d) = 1$ e quindi $\begin{array}{l} a = \pm c \\ b = \mp d \end{array}$

Stesso ragionamento con $x^2 + 2y^2 = p$: si risolve se e solo se $\left(\frac{-2}{p}\right) = +1$

Come si dimostra la fattorizz. unica?

Lemma chiave Se "funziona" la divisione con resto c'è fattorizzazione unica

"Funziona": c'è una funzione "grandezza" (a valori interi) t.c. $\forall\, x, y \neq 0$ esistono $q, r \in$ (dove serve)

t.c. $x = q \cdot y + r$ E grandezza(resto) $<$ grandezza(y)

Nei casi facili, GRANDEZZA = NORMA

Esempio $\mathbb{Z}[i]$

Voglio dividere con resto $a+bi$ per $c+di$.

Calcolo $\dfrac{a+bi}{c+di} = \dfrac{(a+bi)(c-di)}{c^2+d^2} = (A + r_1) + (B + r_2)\,i$

dove A, B sono interi e r_1, r_2 sono razionali di $|\cdot| \leq 1/2$

$$a+bi = (A+Bi)(c+di) + \underbrace{(r_1+r_2 i)(c+di)}_{\text{resto } \in \mathbb{Z}[i]}$$

per differenza

$$N(\text{resto}) = N(c+di)\, N(r_1+r_2 i)$$
$$\leq N(c+di)\cdot \frac{1}{2} < N(c+di)$$

Applicazione $\qquad A \quad B = x^2$

$$y^2+2 = x^3 \rightsquigarrow (y+\sqrt{-2})(y-\sqrt{-2}) = x^3$$

y dispari $\Rightarrow (y+\sqrt{-2},\, y-\sqrt{-2}) =$

$$= (y+\sqrt{-2},\, 2\sqrt{-2}) = 1$$

$$\Rightarrow y+\sqrt{-2} = A^3 = (a+b\sqrt{-2})^3$$
$$= a^3+3a^2b\sqrt{-2}+3ab^2(-2)$$
$$+b^3(-2)\sqrt{-2}$$

Coeff. di $\sqrt{-2}$: $\quad 1 = 3a^2b-2b^3 = b(3a^2-2b^2)$

$\Rightarrow b=\pm 1,\ a=\pm 1$ (e in realtà $b=+1$)

$$y + \sqrt{-2} = \left(\pm 1 + \sqrt{-2} \right)^3$$

$$\Rightarrow \quad y = a^3 - 6a = \pm 5$$

Senior 2018 - P Advanced - Anér

Titolo nota 02/09/2018

Teorema (Van der Waerden, 1927)
Siano $r \geq 1$ un numero di colori e $k \geq 2$ una lunghezza. Esiste un numero naturale $N = W(r,k)$ con questa proprietà: supponiamo di colorare con r colori i numeri $\{1, \dots, N\}$; allora esiste certamente una progressione aritmetica di lunghezza k monocromatica.

OSS Se colorare N naturali basta, anche colorarne $N+m$ basta.

Domanda interessante Capire qual è il minimo N con la proprietà sopra. DIFFICILE
LASCIAMO PERDERE

Strategia Vogliamo dim. che $\forall k, \forall r$ esiste $W(r,k)$. Introdurremo un numero $\overline{W}(r,k,h)$ che sarà un naturale (abb. grande) per cui vale una proprietà che dipende da $r \geq 1, k \geq 2, h \geq 1$. Dimostreremo che $\forall k, r, h$ esiste $\overline{W}(r,k,h)$. Poi sarà evidente che se esiste $\overline{W}(r,k,1)$ allora esiste $W(r,k)$

Per dim. che $\overline{W}(r,k,h)$ esiste usiamo un'induzione strana. Dim. per ind. su k e h congiuntamente la seguente prop.: "$\forall r \geq 1$ esiste $\overline{W}(r,k,h)$" $= P(k,h)$

P.B sarà $k=2$ $h=1$. Poi aumenteremo progressivamente h, e per induzione guadagneremo tutti i $\overline{W}(r,2,h)$. A questo punto se $\overline{W}(r,2,r+1)$ esiste, anche $\overline{W}(r,3,1)$ esiste. Parte una nuova ind. su h, guadagniamo i $\overline{W}(r,3,h)$.

$$\overline{W}(r,3,r+1) \rightsquigarrow \overline{W}(r,4,1).$$

Introduciamo la nozione di pettine di lunghezza k e taglia h: è una collezione di h progressioni aritmetiche, tutte di lunghezza $k+1$, con soltanto il primo elemento in comune, ognuna, tolto il primo elemento, è monocromatica, e le h successioni (amputate del primo el. comune) esibiscono tutti colori diversi.

Il primo elem. del pettine può avere colore qualsiasi

1 2 3 4 5 6 ....

pettine di lunghezza 3 e taglia 2

$\overline{W}(r,k,h)$ è un nat. abbastanza grande per cui esiste almeno uno tra ① un pettine di taglia h e lunghezza k o ② una progr. lunga $(k+1)$, per ogni r-colorazione.

Lemma Se esiste $\overline{W}(r,k,r+1)$, allora visto che con r colori non esistono pettini di taglia $r+1$, ① non può valere, quindi vale ②, quindi esiste $W(r,k+1)$. Per $\overline{W}(r,k+1,1)$ prendo $2\cdot W(r,k+1)$ e cerco una progr. aritm. monocr. lunga $k+1$ nella seconda metà, poi aggiungete la radice

Fissiamo ora k, dimostriamo $P(k,h)$ per induzione su $h \geq 1$, assumendo il passo base (l'esistenza $\forall r$ di $\overline{W}(r,k,1)$ e anche di $W(r,k)$, che come visto deriva da casi precedenti in k).

Il passo base base $k=2$: per una progr. aritm. lunga 2, basta colorare $r+1$ naturali. Per un pettine di taglia $h=1$ e lunghezza $k=2$ bastano $2r+1$ naturali

Passo induttivo $h \rightsquigarrow h+1$. Supponiamo che $\forall r$ esiste $\overline{W}(r,k,h)$. Vogliamo dim. che esiste $\overline{W}(\overline{r},k,h+1)$ per un qualsiasi certo $\overline{r}$.

Prendiamo N un multiplo opportuno di $\overline{W}(\bar{r}, K, h)$

$N = M \cdot \overline{W}(\bar{r}, K, h)$; dividiamo i numeri $\{1, \dots, N\}$ in M blocchi da $\overline{W}(\bar{r}, K, h)$. Se coloriamo con $\bar{r}$ colori $\{1, \dots, N\}$, ogni blocco esibisce una stringa di $\overline{W}(\bar{r}, K, h)$ colori. Ci sono $\underbrace{\bar{r}^{\,\overline{W}(\bar{r}, K, h)}}_{= r'}$ possibili stringhe.

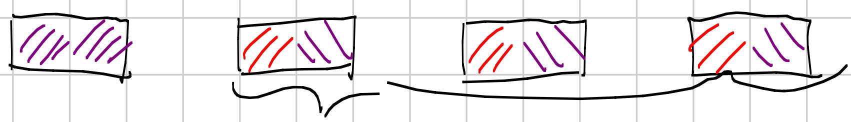
<u>Esempio</u> (per capire) $\overline{W}(\bar{r}, K, h) = 2$ $\quad \bar{r} = 2$

$M = 5 \quad N = M \cdot \overline{W}(\bar{r}, K, h) = 10$

Il nostro scopo è trovare una progr. aritmetica di pettini tutti uguali

$M = \overline{W}(r', K, 1)$ (esiste perché il caso $h = 1$ è già stato conquistato)

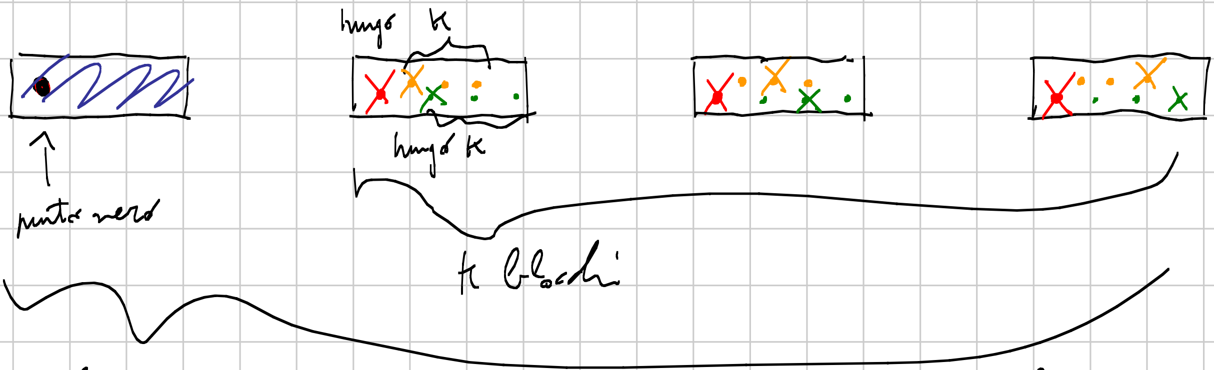
Allora comunque coloro $N = M \cdot \overline{W}(\bar{r}, K, h)$ con $\bar{r}$ colori, ci sarà un pettine di taglia 1 e lunghezza K, fatto di $K+1$ blocchi, con gli ultimi K blocchi colorati allo stesso modo.



Ogni blocco di questi K contiene un pettine

(lo stesso pettine!) di taglia h e lungh. k
(supponendo di non essere così fortunati da aver già trovato una progr. lunga $k+1$).

In part. supponiamo che la radice del pettine abbia un colore diverso dai denti



ho trovato un pettine di lunghezza k e taglia $h+1$
(se sono fortunato, il pto nero è in realtà di uno degli $h+1$ colori, quindi ho una progressione lunga $k+1$).

$\square$

Determinare il min $W(r,k)$ è difficile

Gowers ha dim. che

il minimo $W(r,k) \leq 2^{2^{r^{2^{2^{k+9}}}}}$

Se colorate $\{1, \dots, N\}$ con r colori, ci sono $\frac{1}{r}N$ numeri dello stesso colore, dove $\frac{1}{r}$ è un reale $\in (0,1]$

Teo (Szemerédi, 1975)

Fissato $\varepsilon \in (0,1]$, fissato K, esiste

$N = S(\varepsilon, K)$ abb. grande per cui comunque

scegliete almeno $\varepsilon \cdot N$ elementi di $\{1, \dots N\}$,
questi contengono una progressione aritmetica
lunga K.

Ovviamente Szemerédi $\Rightarrow$ Van der Waerden.

Congettura (Erdős) Prendete un sottoinsieme infinito

dei numeri interi positivi $A \subseteq \mathbb{N}_0$, e supponete

che $\sum_{a \in A} \frac{1}{a} = +\infty$ (es. se $A = \mathbb{N}_0$,
se $A =$ numeri primi)

Allora è vero che A contiene progr. aritm.
lunghe K per ogni $K \geq 2$?

DIM che Erdős $\rightarrow$ Szemerédi

Teo (Green-Tao, 2004) All'interno dei
numeri primi esistono progr. aritm. lunghe
K per ogni $K \geq 2$.

Anche Erdős $\rightarrow$ Green-Tao ...