Stage Senior 2010 – Livello Advanced

Stampato integrale delle lezioni

Autori vari

Indice

SENIOR 2010 – ADVANCED

Titolo nota 06/09/2010

$\boxed{\text{SERIE}}$ $\sum_{n\geq 0}^{\infty} a_n$ $S_n = a_0 + a_1 + \dots + a_n$

$S_n \xrightarrow{?}$ $L \in \mathbb{R}$, $\pm\infty$, NON ESISTE LIM

Se $a_n \geq 0$ ci sono solo 2 poss: $L \in \mathbb{R}$, $+\infty$

Esempio 1 Serie telescopica $\sum_{n\geq 1}^{\infty} \frac{1}{n(n+1)} = \sum_{n\geq 1}^{\infty} \left(\frac{1}{n} - \frac{1}{n+1}\right) = 1$

Si dim. che $S_n = 1 - \frac{1}{n+1}$

Esempio 2 $\sum_{n\geq 1}^{\infty} \log\left(1+\frac{1}{n}\right) = \sum_{n\geq 1}^{\infty} [\log(n+1) - \log n]$

$S_n = \log(n+1) - \log 1 \to +\infty$

Esempio 3 $\sum_{n\geq 0}^{\infty} a^n$ (a parametro) GEOMETRICA

$S_n = \frac{a^{n+1}-1}{a-1}$

- se $a \geq 1$ Div. a $+\infty$
- se $a \in (-1,1)$ Conv. a $\frac{1}{1-a}$
- se $a \leq -1$ Non ha limite

Esempio 4 $\sum_{n\geq 1}^{\infty} \frac{1}{n^a}$ (armonica generalizzata)

- converge se $a > 1$
- diverge a $+\infty$ se $a \leq 1$

$\boxed{\text{Dim 1}}$ Con $a = 1$ diverge

$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \dots + \frac{1}{8} + \dots \geq$

$1 + \underbrace{\frac{1}{2}}_{\frac{1}{2}} + \underbrace{\frac{1}{4} + \frac{1}{4}}_{\frac{1}{2}} + \underbrace{\frac{1}{8} + \dots + \frac{1}{8}}_{\frac{1}{2}}$ Formalmente: $S_{2^n} \geq \frac{n}{2}$

A maggior ragione: con $a < 1$ diverge

Con $a=2$ converge visto ieri $S_n \le 2 - \frac{1}{n}$

Oppure $\frac{1}{n^2} \le \frac{1}{n(n-1)} \Rightarrow \sum_{n=2}^{\infty} \frac{1}{n^3} \le \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1$

VISTA SOPRA

A maggior ragione: con $a \ge 2$ converge

Btw: $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ (Non banale) $\sum_{n=1}^{\infty} \frac{1}{n^{2k}}$ c'è formula ($k \in \mathbb{Z}$)

Restano gli $a \in (0,1)$

<u>Dim 2</u> Idea di Ieri: $S_n^a = \frac{1}{1^a} + \dots + \frac{1}{n^a}$ $\quad S_n^a \le M_a - \frac{N_a}{n^{a-1}}$

Cerco M_a ed N_a in modo da fare induzione

P.I.
$$S_{n+1}^a = S_n^a + \frac{1}{(n+1)^a} \underset{\uparrow \text{Hp}}{\le} M_a - \frac{N_a}{n^{a-1}} + \frac{1}{(n+1)^a} \le$$
$$\underset{\uparrow \text{Hope}}{\le} M_a - \frac{N_a}{(n+1)^{a-1}}$$

Serve
$$\frac{N_a}{(n+1)^{a-1}} + \frac{1}{(n+1)^a} \le \frac{N_a}{n^{a-1}}$$
$$N_a \left(\frac{1}{n^{a-1}} - \frac{1}{(n+1)^{a-1}} \right) \ge \frac{1}{(n+1)^a}$$
$$N_a \ge \underbrace{\frac{n^{a-1}(n+1)^{\cancel{a}-1}}{\cancel{(n+1)}^a \left[(n+1)^{a-1} - n^{a-1} \right]}}_{\text{serve che sia LIMITATO}} \sim \frac{n^{a-2}}{n^{a-2}}$$

$$\frac{\cancel{n^{a-1}}}{n\left(1+\frac{1}{n}\right) \cancel{n^{a-1}} \left[\left(1+\frac{1}{n}\right)^{a-1} - 1 \right]} = \frac{1}{n\left[\left(1+\frac{1}{n}\right)^a - 1 - \frac{1}{n} \right]}$$

$(1+x)^\alpha \ge 1 + \alpha x$

VERA per $x \ge 0$ e $\alpha \ge 1$ (se è così è OK solo per $a \ge 2$)

$$\ge \frac{1}{n\left(\cancel{1} + \frac{a}{n} - \cancel{1} - \frac{1}{n} \right)} = \frac{1}{a-1} \quad \text{ok!!}$$

$N_a \to +\infty$ per $a \to 1$ (ottimo!)

Dim 3 Criterio di condensazione di Cauchy

$\sum_{n=\dots}^{\infty} a_n$ Ipotesi: • $a_n \geq 0$
• a_n debolm. decresc.

Allora $\sum a_n$ converge $\Leftrightarrow$ $\sum 2^n \cdot \boxed{a_{2^n}}$ converge

indice = potenza di 2

$a_1 + a_2 + a_3 + a_4 + \dots + a_8 + \dots \geq$
$a_1 + a_2 + a_4 + a_4 + a_8 + \dots + a_8$

$= a_1 + a_2 + 2a_4 + 4a_8 + 8a_{16}$ se serve $\geq$

$a_1 + a_2 + a_3 + \dots + a_8 \leq a_1 + \overbrace{a_2 + a_2}^{2-3} + \overbrace{a_4 + \dots + a_4}^{4-7} + \overbrace{a_8 + \dots}^{8-15}$
$a_1 + 2a_2 + 4a_4 + 8a_8 + \dots$

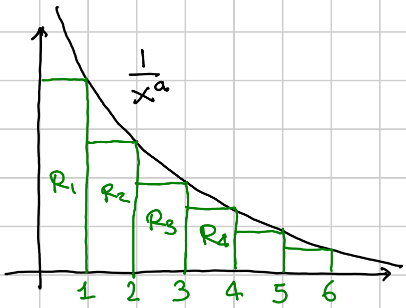
Applicazione:

$$\sum_{n=1}^{\infty} \frac{1}{n^a} \text{ converge} \Leftrightarrow \sum_{n=1}^{\infty} 2^n \cdot \frac{1}{2^{an}} = \sum_{n=1}^{\infty} \left[\frac{2}{2^a}\right]^n$$

= geometrica che converge $\Leftrightarrow \frac{2}{2^a} < 1$
$\Leftrightarrow a > 1$.

— o — o —

Dim. 4 Confronto serie integrali (convergenza per $a > 1$)



Area $(R_i) = \frac{1}{i^a}$

$$R_2 + R_3 + \dots + R_n \leq \underbrace{\int_1^n \frac{1}{x^a}\,dx}_{\text{area sotto il grafico da 1 ad } n}$$

$$= \frac{1}{1-a}\left[\frac{1}{x^{a-1}}\right]_1^n$$

$$\int x^\alpha\,dx = \frac{1}{\alpha+1}x^{\alpha+1}$$
$\alpha = -a$

$$= \frac{1}{1-a}\left[\frac{1}{n^{a-1}} - 1\right]$$

$\frac{1}{n^{a-1}} \to 0$ se $a > 1$

IMO 1991? – 6 Determinare se esiste una successione x_n LIMITATA t.c.

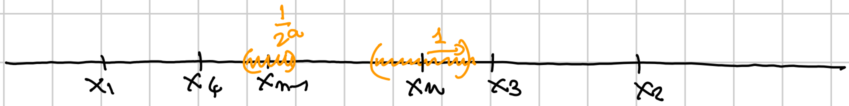
$$|x_n - x_m| \geq \frac{1}{|n-m|^a} \qquad \forall\, n \neq m$$

(a parametro > 1)

<u>Oss.1</u> Se non ci fosse limitata sarebbe banale!

<u>Oss2</u> Posso prendere x_n crescente? NO! Ognuno dista almeno 1 dal precedente!

Tento per induzione. Dati $x_1, \dots, x_n$, dove devo prendere x_{n+1}?



Devo escludere $I(x_n, 1)$ ← intervallo di centro x_n e raggio 1

$I\left(x_{n-1}, \frac{1}{2^a}\right)$

$I\left(x_{n-2}, \frac{1}{3^a}\right)$

$\vdots$

Il caso peggiore è se sono DISGIUNTI

L'area della zona esclusa è $\leq 2\left(1 + \frac{1}{2^a} + \dots + \frac{1}{n^a}\right)$

$\leq 2M_a$ ← non dipende da n!!!

Ricostruzione della dim:

- Fisso un intervallo di ampiezza $> 2M_a$
- ad ogni passo resta sempre almeno un p.to buono nell'interv.

(Nota bene: gli intervalli esclusi passo-passo possono anche scappare da quello iniziale!)

—o—o—

Criterio del confronto asintotico

$\sum_{n=0}^{\infty} a_n \qquad \sum_{n=0}^{\infty} b_n$ Ipotesi:

- $a_n \geq 0$
- $b_n > 0$
- $\lim_{n \to +\infty} \frac{a_n}{b_n} = \ell \ \begin{smallmatrix} \neq 0 \\ \neq +\infty \end{smallmatrix}$

Allora le 2 serie hanno lo stesso comportamento (le somme possono essere diverse)

Dim. basta osservare che $\frac{1}{2}\ell \leq \frac{a_n}{b_n} \leq 2\ell$ per n grande

$$\frac{1}{2}\ell b_n \leq a_n \leq 2\ell b_n$$

Esempio (serviva in RMM 2009) $\sum_{n=1}^{\infty} \underbrace{\arctan \frac{1}{n}}_{a_n} = +\infty$

Prendo $b_n = \frac{1}{n}$:

$$\lim_{n \to +\infty} \frac{a_n}{b_n} = \lim_{n \to +\infty} \frac{\arctan \frac{1}{n}}{\frac{1}{n}} \underset{x = \frac{1}{n}}{=} \lim_{x \to 0} \frac{\arctan x}{x} = 1$$

Poiché $\sum \frac{1}{n}$ diverge, anche l'altra diverge ($\arctan x \sim x$ per $x \to 0$)

—o—o—

Serie a segno alterno $\sum_{n=0}^{\infty} (-1)^n \alpha_n$

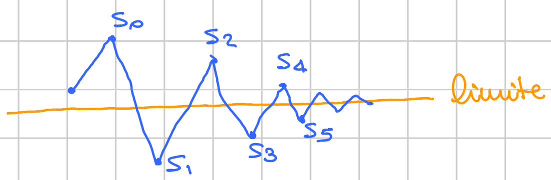
$\boxed{\text{CRITERIO DI LEIBNITZ}}$ Ipotesi:

1. $\alpha_n \geq 0$
2. $\alpha_n \to 0$
3. $\alpha_{n+1} \leq \alpha_n \quad \forall n \in \mathbb{N}$

Tesi: la serie converge

"Dim." $S_{2n} \searrow \qquad S_{2n+1} \nearrow \qquad S_{2m} \geq S_{2n+1} \quad \forall m \ \forall n$

$S_{2n} \to \ell \qquad S_{2n+1} \to m \qquad S_{2n} - S_{2n-1} = \alpha_n \to 0$



Esempio $\quad 1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\ldots = \sum (-1)^{n+1}\frac{1}{n}$ converge!

(e si sa anche la somma: $\log 2$)

$\sum (-1)^n \frac{1}{n^a}$ converge $\iff a>0$

—o—o—o—

$1-\frac{1}{2}-\frac{1}{4}+\frac{1}{3}-\frac{1}{6}-\frac{1}{8}+\frac{1}{5}$ Converge?

Achtung!!!! $\sum a_n$ converge + $\sum |a_n|$ converge

$\Downarrow$

posso riordinare i termini!!!!

Se $\sum a_n$ converge, ma $\sum |a_n| = +\infty$, allora riordinando posso ottenere qualunque somma!

—o—o—

$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ "Dimostrazione" $\quad \sin x = x - \frac{1}{6}x^3 + \frac{1}{5!}x^5 - \frac{1}{7!}x^7 + \ldots$

$f(x) = \frac{\sin x}{x} = 1 - \frac{1}{6}x^2 + \frac{1}{5!}x^4 + \ldots$

$g(x) = \frac{\sin(\pi x)}{x} = \frac{1}{x}\left(\pi x - \frac{1}{6}\pi^3 x^3 + \ldots\right) = \pi - \frac{1}{6}\pi^3 x^2 + \ldots$

$g(x) = 0 \iff x \in \mathbb{Z}\setminus\{0\}$

In un polinomio, la somma dei reciproci delle radici al $\square$ è

$P(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots \qquad r_1, \ldots, r_n$ radici

$\frac{1}{r_1^2} + \frac{1}{r_2^2} + \ldots + \frac{1}{r_n^2} = \text{Somma}^2 - \text{doppi prodotti}$

$= \left(\frac{a_1}{a_0}\right)^2 - 2\frac{a_2}{a_0}$

Se fosse vero per le serie di potenze... $\sum_{n\in\mathbb{Z}\setminus\{0\}} \frac{1}{n^2} = -2\frac{a_2}{a_0} = \frac{\pi^2}{3}$

contano 2 volte...

$\boxed{\text{Max e min}}$ $[a,b] \subseteq \mathbb{R}$ intervallo

Teorema di WEIERSTRASS $f : [a,b] \to \mathbb{R}$ $\boxed{\text{continua}}$, allora esistono

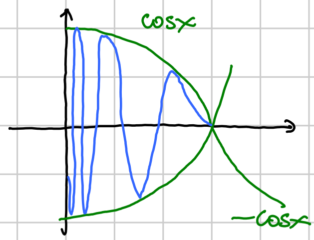
estremi compresi

$$\max\{f(x) : x \in [a,b]\}$$
$$\min\{\quad " \quad\}$$

Esercizio $\exists\, f : (0,1]$ continua che non ammette né max, né min?

Esempio 1: $f(x) = \frac{1}{x} \sin \frac{1}{x}$ e se la volessi pure limitata ...

Esempio 2: $f(x) = \cos x \cdot \sin \frac{1}{x}$



Dove trovare max/min

3 categorie di candidati:

① p.ti $x \in (a,b)$: $f'(x) = 0$ (stazionari interni)

② " " f' non esiste (singolari interni)

③ Bordo $x = a$ e $x = b$.

Esempio $[-2,2]$ $f(x) = |x|$ $\min = 0$ p.to di min $x = 0$ ②

$\max = 2$ p.ti di max $x = \pm 2$ ③

— o — o —

In 2 o più variabili $A \subseteq \mathbb{R}^n$ $f : A \to \mathbb{R}$

- A si dice **limitato** se è contenuto in una opportuna palla
$$B(\underbrace{x_0}_{\in\mathbb{R}^n}, \underbrace{r}_{>0}) = \{x \in \mathbb{R}^n : \operatorname{dist}(x, x_0) \le r\}$$

- A si dice **chiuso** se (brutalmente: contiene il bordo)
rigorosamente $\forall\, x \notin A \ \exists\, r > 0$ t.c. $B(x,r) \cap A = \emptyset$

- A si dice **compatto** se è chiuso + limitato

Teo. Weierstrass $f : A \to \mathbb{R}$ con f continua e A compatto
$\Rightarrow$ esistono max e min.

Dove trovare p.ti di max/min

① P.ti $x \in$ interno di A (p.ti $x \in A$ per cui $\exists\ B(x, r) \subseteq A$)
con derivate parziali nulle

$$\begin{cases} f_x = 0 \\ f_y = 0 \end{cases}$$ in 2 variabili $\qquad \underbrace{\nabla f}_{\text{gradiente di } f} = (f_x, f_y) = (0,0)$

② P.ti $x \in$ interno di A in cui "qualche deriv. parz. non esiste".

③ Bordo (in generale sono ∞ p.ti)

— o — o —

MOLTIPLICATORI DI LAGRANGE Caso di 1 moltiplicatore

$$V = \{x \in \mathbb{R}^n : \underbrace{\Phi(x) = 0}_{\text{equazione di } V}\}$$

Data $f(x)$, trovare max/min di f in V

Teorema Supponiamo x_0 p.to di max/min per f in V (se V fosse compatto, esisterebbero tali punti).
Allora ci sono 3 possibilità

① In x_0 non esiste ∇f o non esiste $\nabla \Phi$
② In x_0 $\nabla \Phi(x_0) = 0$ (cioè si annullano tutte le deriv. parziali)
③ In x_0 $\nabla \Phi(x_0)$ e $\nabla f(x_0)$ sono paralleli, cioè $\exists\ \lambda \in \mathbb{R}$ t.c.

$$\nabla f(x_0) = \boxed{\lambda} \nabla \Phi(x_0)$$

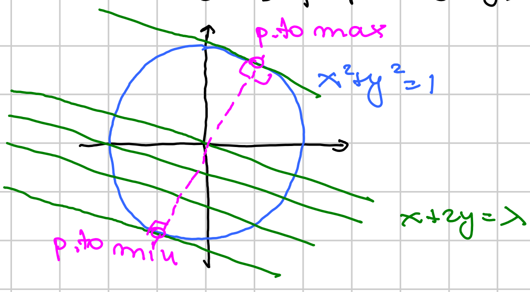
moltiplicatore

Esempio 1 $\quad$ max/min $\{x + 2y : x^2 + y^2 = 1\}$

Per via elementare: AM-QM pesata o C-S:

$$x + 2y \le \sqrt{5}\sqrt{x^2+y^2} \quad \text{con} = \iff (1,2) \text{ prop a } (x,y)$$

Via linee di livello:



Via moltiplicatori:

- Max e min esisto per W.
- Vedo 3 possibili situazioni $\Phi(x,y) = x^2+y^2-1$ $f(x,y) = x+2y$

① Nulla $\emptyset$

② $\begin{cases} 2x = 0 \\ 2y = 0 \\ x^2+y^2=1 \end{cases}$ $\nabla \Phi(x,y) = (2x, 2y)$

Nulla $\emptyset$ (di solito è così!)

③ Devo cercare i p.ti $(x,y) \in V$ t.c. $\nabla f(x,y) = \lambda \nabla \Phi(x,y)$

$(1,2) = \lambda(2x, 2y)$

$\begin{cases} 1 = 2\lambda x \\ 2 = 2\lambda y \\ x^2+y^2=1 \end{cases}$ 3 equ in 3 incognite

Dalla 1ª e 2ª ottengo $y = 2x$

sostituisco nella 3ª e fine!

— o — o —

Esempio 2 AM-GM $\sqrt[n]{x_1 \cdot \ldots \cdot x_n} \leq \frac{x_1 + \ldots + x_n}{n}$

Osservo che è omogenea, quindi posso assumere LHS = 1 oppure RHS = 1

Scelgo LHS = 1 Vuol dire che

$V = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_1 \cdot \ldots \cdot x_n = 1, x_1 \geq 0, \ldots, x_n \geq 0\}$

È compatto? NO! $\left(\frac{1}{n}, n, 1, \ldots, 1\right) \in V$ $\forall n$ NO LIMITATO

Scelgo RHS = 1 $V = \{(\ ) \in \mathbb{R}^n : x_1 + \ldots + x_n = 1, x_1 \geq 0, \ldots, x_n \geq 0\}$

Ora $V \subseteq [0,1]^n \Rightarrow$ limitato

Ora so che esiste Max del LHS (per W.)

cerco i p.ti di max in ①, ②, ③

$\Phi(x_1, \ldots, x_n) = x_1 + \ldots + x_n$ $f(x_1, \ldots, x_n) = x_1 \cdot \ldots \cdot x_n$

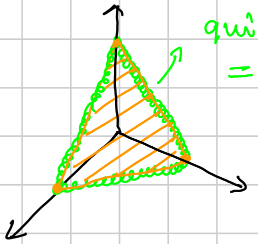
① $\emptyset$ ② $\emptyset$ $\nabla \Phi = (1, \ldots, 1)$ ③ $\nabla f = \lambda \nabla \Phi$

$\begin{cases} x_2 \cdot \ldots \cdot x_n = \lambda \\ x_1 \cdot x_3 \cdot \ldots \cdot x_n = \lambda \\ \vdots \\ x_1 + \ldots + x_n = 1 \end{cases}$ Tutte le variabili sono uguali (se posso dividere)

$\rightarrow x_1 = \ldots = x_n = \frac{1}{n}$ e si conclude

Achtung! Se V è descritto da 1 equazione + un po' di disequazioni compaiono i "bordi dei bordi"

$\boxed{n=3}$



Il metodo va bene per trovare i candidati nell' "interno" di V, cioè dove le disug. sono strette.

Cosa dire
- Max e min esistono per W.
- Se p.to di max sta nel "bordo del bordo" allora LHS=0
- Se non sta lì, posso dividere e finisco

—o—

Esempio 3 $\min \{x^2+y^4+z^6 : \underbrace{xyz=n}_{\text{non compatto}}\}$ $x, y, z \geq 0$

Mettendo $x=n$, $y=1$, $z=1$ ottengo $\min \leq n^2+2$

Quindi min originario $= \min \{x^2+y^4+z^6 : \underbrace{xyz=n, x\leq n, y\leq n, z\leq n}_{\text{compatto !!!}}\}$

Quindi il minimo esiste, e non è in un bordo del bordo (perché altrimenti cambio n con $2n$ ...)

i p.ti di minimo stanno nel gruppo 3 $\nabla f = \lambda \nabla \phi$

$(2x, 4y^3, 6z^5) = \lambda(yz, xz, xy)$

$$\begin{cases} 2x = \lambda yz & \cdot x \\ 4y^3 = \lambda xz & \cdot y \\ 6z^5 = \lambda xy & \cdot z \\ xyz = n \end{cases}$$

$2x^2 = 4y^4 = 6z^6$ e da qui si chiude basta sostituire nella 4ª:

$$x^2+y^4+z^6 \geq c\,[xyz]^{\frac{12}{11}}$$

—o—o—

Achtung! Alla fine i punti vanno sostituiti per trovare max/min

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

SENIOR 2010 – ADVANCED – A

Titolo nota 08/09/2010

Più moltiplicatori di Lagrange

$$V = \{x \in \mathbb{R}^n : \ \phi_1(x) = \dots = \phi_k(x) = 0\}$$ k equazioni $(k < n)$

$f : \mathbb{R}^n \to \mathbb{R}$ $\qquad \max/\min \{f(x) : x \in V\}$

Teorema Se $x_0 \in V$ è p.to di max/min, allora succede una di queste 3 cose

- ∇f o qualche $\nabla \phi_i$ non esiste in x_0
- Costruiamo la matrice che ha come righe i k gradienti

$$\begin{matrix} \nabla \phi_1 \\ \nabla \phi_2 \\ \vdots \\ \nabla \phi_k \end{matrix} \qquad \text{Matrice } k \times n$$

[Rango di una matrice = dimensione della massima sottomatrice quadrata $r \times r$ con $\det \neq 0$
= max numero di righe lin. indip.
= " " " colonne " "
= dimensione dell'immagine]

In x_0 il rango è $< k$ (cioè tutte le sottomatrici $k \times k$ hanno determinante $= 0$ $\left(\binom{n}{k}\right.$ condizioni$\left.\right)$)

- In x_0 si ha che ∇f è combinazione lineare dei $\nabla \phi_i$, cioè $\exists \lambda_1, \dots, \lambda_k$ t.c.

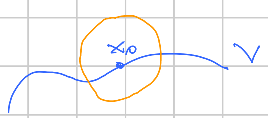
$$\nabla f(x_0) = \boxed{\lambda_1} \nabla \phi_1(x_0) + \dots + \boxed{\lambda_k} \nabla \phi_k(x_0)$$

moltiplicatori

— o — o —

Idea per una dim. con 1 moltiplicatore:

$V = \{x \in \mathbb{R}^n : \ \phi(x) = 0\}$ $\qquad x_0 \in V$ p.to di min per $f(x)$ ristretta a V



Prendo $B(x_0, 1)$ chiusa

Per ogni n calcolo $\min\{f(x) + n\,\phi^2(x) : x \in B(x_0, 1)\}$

Esiste ed è raggiunto in un p.to x_n. Si può dimostrare che $x_n \to x_0$.

In x_n si ha che $\nabla(f(x) + n\,\phi^2(x)) = 0$, cioè $\nabla f(x) + 2n\,\phi(x)\,\nabla\phi(x) = 0$

cioè in x_n $\nabla f(x_n)$ è multiplo di $\nabla \phi(x_n)$. Passo al ~~limite~~

Lemma sui vettori $v_n \to v_\infty$ $\forall n$ si ha che v_n è multiplo
$w_n \to w_\infty$ di w_n

Allora $\to$ o $w_\infty = 0$
o v_∞ è multiplo di w_∞

— o — o —

Con k equazioni la dim. è la stessa

$$\min \{ f(x) + n\,\phi_1^2(x) + \dots + n\,\phi_k^2(x) \}$$

Nel p.to di min x_n si ha che

$$\nabla f(x_n) + 2n\,\phi_1(x_n)\,\nabla\phi_1(x_n) + \dots + 2n\,\phi_k(x_n)\,\nabla\phi_k(x_n) = 0$$

cioè $\nabla f(x_n)$ è comb. lineare dei $\nabla\phi_i(x_n)$

Lemma Date $k+1$ succ. di vettori $v_n \to v_\infty$
$w_n^1 \to w_\infty^1$
$\vdots$
$w_n^k \to w_\infty^k$

Hp: per ogni n si ha che v_n è comb. lin. dei w_n^i

Tesi: $\to$ o il limite è ancora comb. lin.
$\to$ o i w_∞^i non sono lin. indip., cioè la matrice da essi formata non ha rango max.

Dim. Ipotesi dice che la matrice $\begin{pmatrix} v_n \\ w_n^1 \\ \vdots \\ w_n^k \end{pmatrix}$ $(k+1) \times n$

ha rango $\leq k$, cioè tutte le s. matrici $(k+1)\times(k+1)$ hanno det $= 0$
Quindi anche la matrice limite ha rango $\leq k$, cioè
$\to$ o i k sotto sono dip. tra di loro
$\to$ o il primo dipende dagli altri.

— o — o —

A meno di cambiare $f(x)$ con $f(x) + \text{dist}^{10}(x, x_0)$ possiamo supporre x_0 p.to di minimo stretto (basta il $\square$).

— o — o —

Problemi ad applicare i moltiplicatori
$\to$ sapere che max / min esistono (guadagnare compattezza)
$\to$ bordi dei bordi
$\to$ risolvere il sistema !

— o — o —

CONVESSITÀ

Def. Sia $A \subseteq \mathbb{R}^n$ un insieme convesso (per ogni coppia di p.ti contiene tutto il segmento)

$f : A \to \mathbb{R}$ si dice convessa se

$$f(\lambda x + (1-\lambda) y) \leq \lambda f(x) + (1-\lambda) f(y) \qquad \forall x \in A \ \forall y \in A \quad \forall \lambda \in [0,1]$$

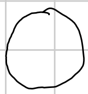
Oss. In una variabile si può verificare con $f''(x) \geq 0$
In più variabili ci sarebbe la matrice Hessiana, oppure sfruttando che è somma di funzioni convesse semplici (distanza da un p.to, distanza^2 da un p.to, distanza da una retta, ...)

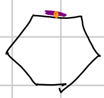
Oss. f è convessa $\Leftrightarrow$ il sopragrafico $\{(x,y) \in A \times \mathbb{R} : y \geq f(x)\}$ è un insieme convesso di $\mathbb{R}^{n+1}$

— o — o —

Teorema Se $A \subseteq \mathbb{R}^n$ è un convesso compatto, allora $\max \{f(x) : x \in A\}$, se f è convessa e continua, esiste e tra i p.ti di max c'è almeno un p.to estremale di A (solo estremali se f è stretta. convessa)

Def. $x_0 \in A$ è p.to estremale $\Leftrightarrow$ quando $x_0 \in$ segmento $\subseteq A$ si ha che x_0 è un estremo del segmento

Esempi  p.ti estremali = bordo

 p.ti estremali = vertici

— o — o —

Esempio Trovare in un triangolo il p.to per cui è massima la somma delle distanze dai vertici

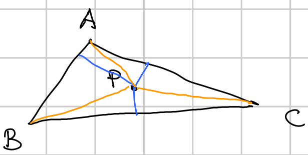
Soluzione La somma delle distanze è convessa (anzi strettamente convessa perché i 3 vertici non sono allineati ...), quindi il max si realizza in un p.to estremale, cioè in un vertice (quello opposto al lato minore)

Come si dim. per bene che è strett. convessa

$$f(x) = \operatorname{dist}(x,A) + \operatorname{dist}(x,B) + \operatorname{dist}(x,C).$$

La disug. "$\leq$" nella definizione è facile. Se ci fosse "$=$" i p.ti x e y dovrebbero essere allineati con A, B, C (il che è impossibile).
Infatti dovrebbe esserci "$=$" sui 3 addendi.

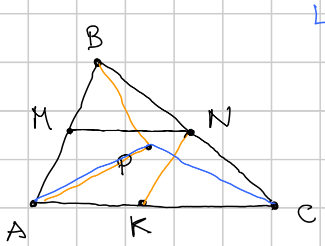
Esempio 2 La somma delle distanze dai lati di un $\triangle$ è convessa, anzi è affine nel triangolo (il grafico è un piano, perché somma di 3 piani).
Quindi il max è almeno in un vertice, quindi è l'altezza + lunga



Esempio 3 IMOSL 99 Dim. che in un triangolo ABC se prendo un p.to P si ha che

$$\underbrace{AP + BP + CP + \min\{AP, BP, CP\}}_{LHS} \leq AB + BC + CA$$

Dim.



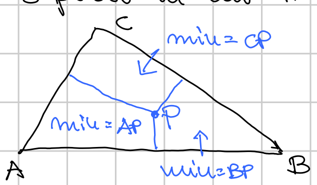
Facile: $AP + CP \leq AM + MN + NC$
$AP + BP \leq BN + NK + AK$

Sommo:

$$LHS \leq 2AP + BP + CP \leq \tfrac{1}{2}AB + \tfrac{1}{2}AC + \tfrac{1}{2}BC + \tfrac{1}{2}BC + \tfrac{1}{2}AB + \tfrac{1}{2}AC = \text{Perim.}$$

Osservazione: è sempre vero che P è dentro almeno 2 "trapezi"

$\boxed{\text{Dim. "bovina"}}$ Pongo $f(P) = AP + BP + CP + \min\{AP, BP, CP\}$
È convessa? FORGET IT!! Su tutto il triangolo NO, ma lo è nei 3 pezzi in cui il minimo so chi è.



Nelle 3 zone $f(P)$ è convessa (strett.) perché somma di convesse

$2AP + BP + CP$

Basta quindi controllare i p.ti estremali delle 3 zone, cioè
→ vertici
→ p.ti medi dei lati
→ circocentro
Da qui si finisce.

— o — o —

Equivalente in + variabili di $f''(x)$. Derivate parziali seconde! (sono n^2)

$$\begin{pmatrix} f_{xx} & f_{xy} & f_{xz} \\ f_{yx} & f_{yy} & f_{yz} \\ f_{zx} & f_{zy} & f_{zz} \end{pmatrix}$$

La matrice è simmetrica

<u>Def.</u> Una Matrice simmetrica $n \times n$ si dice <u>semidefinita positiva</u> se

$$x \cdot Ax \geq 0 \qquad \forall x \in \mathbb{R}^n$$

<u>Def.</u> Forma quadratica in $\mathbb{R}^n$ = somma di monomi di 2° grado in n variabili

Esempio $(n=2)$ $\quad q(x,y) = ax^2 + by^3 + 2c\,xy$
$(n=3)$ $\quad q(x,y,z) = ax^2 + by^2 + cz^2 + 2dxy + 2eyz + 2fzx$

Una forma è semidefinita pos. se viene ≥ 0 per ogni $x \in \mathbb{R}^n$

Forme ⟺ matrici simmetriche

$$ax^2 + by^2 + 2cxy \qquad (x \;\; y)\begin{pmatrix} a & c \\ c & b \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

<u>Teorema</u> f è convessa in A " ⟺ " la matrice delle derivate seconde è semidefinita positiva

se ci sono le derivate

Come stabilire se una forma è positiva, negativa o "indefinita"
→ autovalori della matrice
→ ogni forma è somma / differenza di quadrati

$$x^2 + 3xy - y^2 = x^2 + 2x\frac{3y}{2} + \frac{9}{4}y^2 - \frac{9}{4}y^2 - y^2 = \left(x + \frac{3y}{2}\right)^2 - \frac{13}{4}y^3$$

→ condizione sufficiente (ma non necessaria) per essere positiva

tutte det > 0

—— o —— o ——

<u>DISOG. DI JENSEN</u> $I \subseteq \mathbb{R}$ convesso $f: I \to \mathbb{R}$ convessa

$$f(\lambda_1 x_1 + \dots + \lambda_n x_n) \le \lambda_1 f(x_1) + \dots + \lambda_n f(x_n)$$

$x_1, \dots, x_n \in I$

$\lambda_1 + \dots + \lambda_n = 1$

$\lambda_i \ge 0$

<u>Dim.</u> Induzione UP and DOWN

$\boxed{1}$ Vera per $n \Rightarrow$ vera per $2n$ ($n=2$: def. di funzione convessa)

$\boxed{2}$ Vera per $n \Rightarrow$ vera per $(n-1)$: basta usare un λ nullo

<u>Dim.</u> $\boxed{1}$

$$f(\overbrace{\lambda_1 x_1 + \dots + \lambda_n x_n}^{\lambda x} + \overbrace{\lambda_{n+1} x_{n+1} + \dots + \lambda_{2n} x_{2n}}^{(1-\lambda) y}) =$$

$$f\left((\lambda_1 + \dots + \lambda_n) \frac{\lambda_1 x_1 + \dots + \lambda_n x_n}{\lambda_1 + \dots + \lambda_n} + (\lambda_{n+1} + \dots + \lambda_{2n}) \frac{\lambda_{n+1} x_{n+1} + \dots}{\lambda_{n+1} + \dots + \lambda_{2n}}\right)$$

$$\le (\lambda_1 + \dots + \lambda_n) f(\quad) + (\lambda_{n+1} + \dots + \lambda_{2n}) f(\quad)$$

Ora uso Jensen su n vero per ipotesi induttiva (i coefficienti sono $\dfrac{\lambda_1}{\lambda_1 + \dots + \lambda_n}, \dots, \dfrac{\lambda_n}{\lambda_1 + \dots + \lambda_n}$ che fanno somma 1

Occhio a trattare il caso della divisibilità per zero ...

$\boxed{\text{Oss.}}$ Caso particolare $f\left(\dfrac{x_1 + \dots + x_n}{n}\right) \le \dfrac{f(x_1) + \dots + f(x_n)}{n}$

Volendola dim. direttamente faccio $\boxed{1}$ come prima, ma per $\boxed{2}$ è più complicato:
sono dati $x_1, \dots, x_{n-1}$ e devo scegliere $x_n = \dfrac{x_1 + \dots + x_{n-1}}{n-1}$.
Mi ritrovo

$$\underbrace{f\left(\frac{x_1 + \dots + x_{n-1}}{n-1}\right)}_{\text{LHS}} = f\left(\frac{x_1}{n} + \dots + \frac{x_{n-1}}{n} + \frac{x_n}{n}\right)$$

$$x_1\left(\frac{1}{n} + \frac{1}{n(n-1)}\right) = x_1 \frac{\cancel{n}}{\cancel{n}(n-1)}$$

$$\le \frac{1}{n} f(x_1) + \dots + \frac{1}{n} f(x_{n-1}) + \underbrace{\frac{1}{n} f(x_n)}_{\frac{1}{n}\text{LHS}}$$

Porto a sx e viene

LHS $\frac{n-1}{n} \leq$ RHS

— o —

Applicazione 1 AM – QM (Jensen su $f(x) = x^2$)
(N.B. vale senza Hp di segno)

Applicazione 2 GM – AM (Jensen sulla concava $f(x) = \log x$: qui servono $x_i > 0$)

$$\log\left(\frac{x_1 + \dots + x_n}{n}\right) \overset{\text{concava}}{\geq} \frac{1}{n}(\log x_1 + \dots + \log x_n)$$

$$= \log [x_1 \cdot \ldots \cdot x_n]^{\frac{1}{n}}$$

Usando i λ si ottengono versioni pesate.

Applicazione 3 $M_p(x_1, \dots, x_n) \leq M_q(x_1, \dots, x_n)$ $p \leq q$
ci si riduce facilmente a $0 < p < q$ e $p = 1$ $q = \alpha > 1$
Ora è Jensen su x^α che è convessa per $\alpha \geq 1$ $(x \geq 0)$

Applicazione 4 $ab \leq \frac{1}{p} a^p + \frac{1}{q} b^q$ se $a > 0, b > 0, p > 0, q > 0$
$\frac{1}{p} + \frac{1}{q} = 1$

Jensen su $\log x = f(x)$ $x = a^p$ $y = b^q$ $\lambda = \frac{1}{p}$ $(1-\lambda) = \frac{1}{q}$

$$\log(\lambda x + (1-\lambda) y) \geq \lambda f(x) + (1-\lambda) f(y)$$

$$\log\left(\frac{1}{p} a^p + \frac{1}{q} b^q\right) \geq \frac{1}{\cancel{p}} \log(a^{\cancel{p}}) + \frac{1}{\cancel{q}} \log(b^{\cancel{q}})$$

$$= \log a + \log b = \log(ab)$$

Analogo $abc \leq \frac{1}{p} a^p + \frac{1}{q} b^q + \frac{1}{r} c^r$ $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1$

Serve per dimostrare C–S a 3 specie (Hölder)

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

Per omogeneità posso assumere
$\sum a_i^p = \sum b_i^q = \sum c_i^r = 1$ e poi sommo sui i le YOUNG.

Caso speciale : $i \in \{1,2\}$ $\quad p_1 = p_2 = \dots = p_n = n$

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

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

(a_1, b_1)
(a_2, b_2)
$\vdots$
(a_n, b_n)

Dimostrazione diretta : UP and DOWN

Applicazione 5 $\quad \min \{ f(x_1) + \dots + f(x_n) \; : \; x_1 + \dots + x_n = A \}$

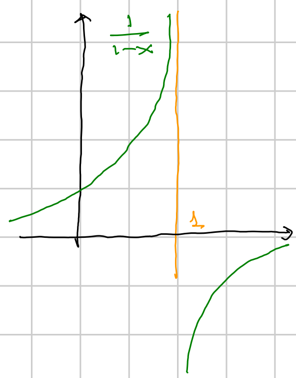
Se f è convessa, allora il minimo è quando sono tutti uguali

$$f(x_1) + \dots + f(x_n) \geq n f\left(\frac{x_1 + \dots + x_n}{n}\right) = n f\left(\frac{A}{n}\right)$$

Nesbit $\quad \dfrac{a}{b+c} + \dfrac{b}{c+a} + \dfrac{c}{a+b} \geq \dfrac{3}{2} \qquad a, b, c > 0$

Per omogeneità assumo $a+b+c = 1$ $\qquad \dfrac{a}{1-a} + \dfrac{b}{1-b} + \dfrac{c}{1-c} \geq \dfrac{\frac{1}{3}}{1-\frac{1}{3}} 3$

Se $f(x) = \dfrac{1}{1-x}$ è convessa ho finito



Rigoroso: $f''(x) = \dots$ oppure

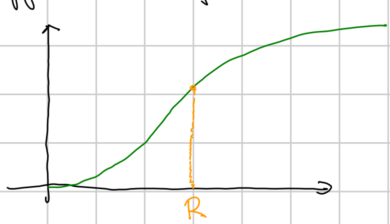
cambio variabile e diventa $\frac{1}{x}$ per la quale uso la definizione.

Achtung! Precisare sempre DOVE si lavora.
In questo caso : $[0, 1)$

— o — o —

$\boxed{\text{LEMMA CONVEX-CONCAVE}}$ $\quad \min \{ f(x_1) + \dots + f(x_n) : x_1 + \dots + x_n = A, \; x_i \geq 0 \}$

Supponiamo f convex-concave. Per il minimo se la giocano 2 configurazioni



→ $x_1 = \dots = x_n$ nella zona convessa

→ $x_1 = \dots = x_{n-1}$ nella zona convessa e x_n nella zona concava per aggiustare la somma

Ponendo $x = x_n$ mi riduco a studiare

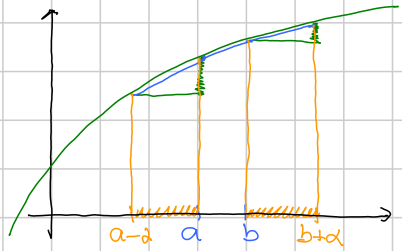
$$f(x) + (n-1)\, f\left(\frac{A-x}{n-1}\right)$$

oppure, ponendo $x_1 = x$: $(n-1)\, f(x) + f(A-(n-1)x)$
e si può fare studiando la funzione.
Idee alla base del convex–concave:

$\boxed{1}$ min esiste se f è continua in $[0,A]$: Weierstrass.
$\boxed{2}$ tutti gli x_i che stanno nella zona convessa si possono rendere uguali conservando la somma ed abbassando $\sum f(x_i)$
$\boxed{3}$ A max ce n'è uno nella zona concava: se ce ne sono 2 li "allargo" conservando la somma fino a quando il sx cade nella zona convessa (il dx non può arrivare ad A senza che tutti gli altri siano zero)

<u>Lemma di allargamento</u> (versione concava)

$$f(a-\alpha) + f(b+\alpha) \le f(a) + f(b)$$

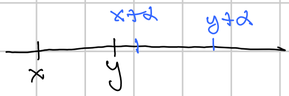


il che equivale a

$$\underbrace{f(b+\alpha) - f(b)}_{\alpha f'(c_1)} \le \underbrace{f(a) - f(a-\alpha)}_{\alpha f'(c_2)}$$

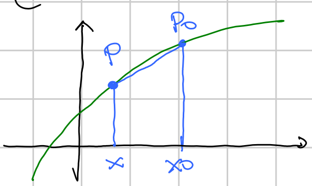
Più in generale: se $y > x$ e $\alpha \ge 0$, allora

$$f(y+\alpha) - f(y) \le f(x+\alpha) - f(x)$$



Non ho garanzia di ordinamento fra c_1 e c_2.

Idea: fissato un punto x, il rapporto incrementale è monotono (crescente o decrescente a seconda di convessità concavità)



il coeff. angolare della retta PP_0 diminuisce quando P sale (fissato P_0)
(si dimostra a partire dalla def. di convessità)

$\boxed{\text{DISUGUAGLIANZA DI KARAMATA}}$ $f: I \to \mathbb{R}$ convessa

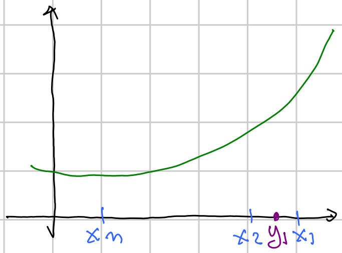
$(x_1, \dots, x_n) \succ (y_1, \dots, y_n)$ in stile bunching, cioè

- $x_1 \geq y_1$
- $x_1 + \dots + x_k \geq y_1 + \dots + y_k \qquad k = 1, \dots, n-1$
- $x_1 + \dots + x_n = y_1 + \dots + y_n$ (controllare !!!!)
- $x_1 \geq x_2 \geq \dots \geq x_n, \qquad y_1 \geq y_2 \geq \dots \geq y_n$

Allora: $\qquad f(x_1) + \dots + f(x_n) \geq f(y_1) + \dots + f(y_n)$

KARAMATA $\Rightarrow$ JENSEN $\qquad$ Ordino gli x_i e poi uso $y_1 = \dots = y_n = \dfrac{x_1 + \dots + x_n}{n}$

Idea della dim: induzione + Lemma di allargamento



Prendo x_1 e lo sposto verso y_1 e contemporaneamente alzo x_n finché non ho "contatti" tra x e y.
Dopo il contatto semplifico e scendo di uno. Così però magari la somma $x_1 + x_2 + x_3$ è scesa ...
Forse è meglio lavorare con x_1 e x_2 ...
Alternativa: spostare x_1 e y_1 a sx fino a quando ...

— o — o —

NB. Le funzioni convesse stanno sopra le proprie rette tangenti !!

Idea: derivata = rapporto incrementale con $P = P_0$

Applicazioni (Bernoulli con esponente $\alpha \geq 1$)

$$(1+x)^\alpha \geq 1 + \alpha x \qquad \forall x \geq -1 \quad \forall \alpha \geq 1$$

$f(x) = (1+x)^\alpha$ è convessa per $\alpha \geq 1$ $\qquad f(x) \geq \underbrace{1 + \alpha x}_{\text{retta tg. in } x = 0}$

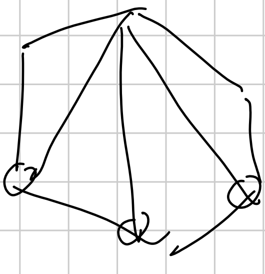
$f(0) = 1 \qquad f'(x) = \alpha (1+x)^{\alpha - 1} \qquad f'(0) = \alpha$

COMBINATORICS.

Titolo nota 06/09/2010

1. Induction.

1.1. Given a convex polygon^n, triangulated by diagonals, such that the number of segments meeting at each vertex is even.



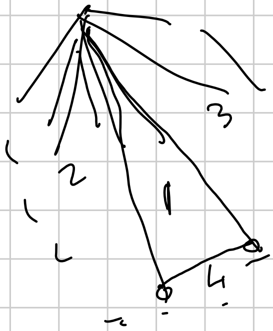
Question? When?

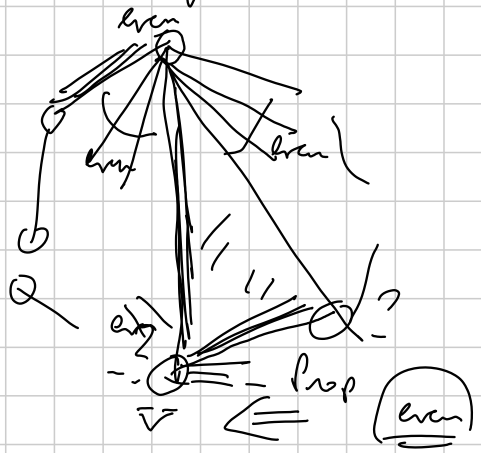
$n = 3$ ✓

$n = 4$ —

$n = 5$ —

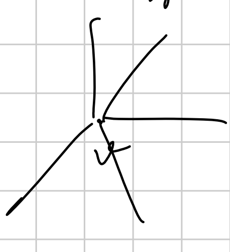
$n = 6$ ✓





Claim v also has even # segments

Polygon + sides diagonals = Graph $G = (V, E)$



$\deg v$ = # edges incident at v.

$$\sum_{v \in V} \deg v = 2|E| \quad \text{even}$$

$$\#\left(\text{vertices of odd degree}\right) \text{ — } \sum_{\deg v = \text{odd}} \deg v = \underline{\underline{\text{even}}}$$

$\Rightarrow$ ↘ even : Proposition. The number of vertices of odd degree in a finite graph is even.

Start again. "Define" the induction predicate.

Induction on # of sides have to be ≥ 3.

Sufficient condition — show how (exhibit / example) Necessary condition

1) to just describe example

2) to inductively build it.

Find some "special value" — "threshold" value

Example. $\{1, 2, \ldots, 2n\}$

What is minimum cardinality of a subset so that there must exist 2 coprime numbers in that subset.

(D) prove that $|S| \geq t$ holds

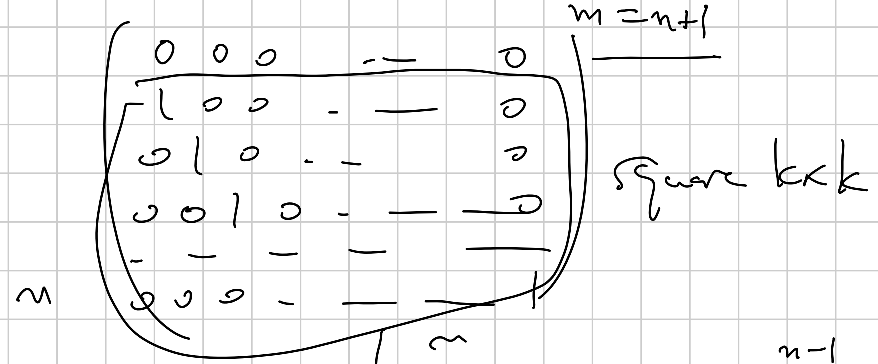
$\Downarrow$ "~~prove~~" that $|S| = t-1$ not true.

(E) example.

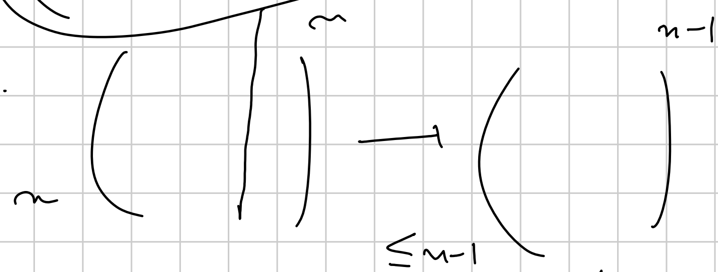
Problem. Given is $n \times n$ matrix, entries are symbols a_{ij}. Each row i seen

$$(a_{i1}, a_{i2}, \ldots, a_{in}) \in (\text{space of symbols})^n$$

Given is the fact $R_i \neq R_j$ as vectors.
Show that we may choose to remove some column, so that in the new $n \times (n-1)$ matrix, the rows are still distinct (as vectors).



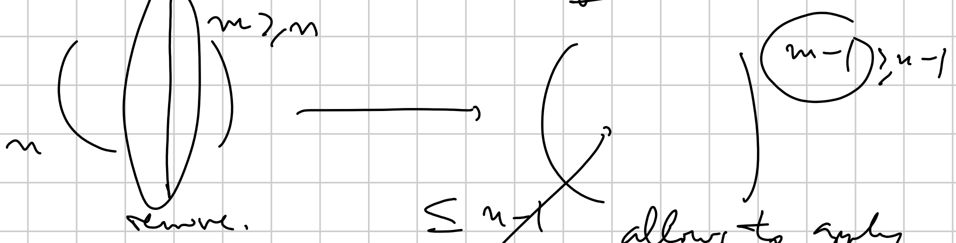
Solution 1



Matrix not square anymore ← — < — not allow induction

= — ✓

"Patch" to this obstacle: replace our problem with a more general one:



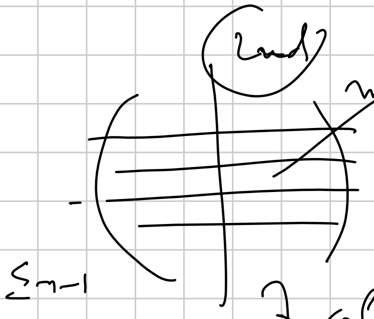
allows to apply induction.

(Check the truth thesis for "small" values. $n=1,2$)

Ind. Hyp → YES, I can remove a column s.t. remaining rows distinct.

$n = m = 1$, remove the single column → original ~~statement~~ true ?

by a vacuous argument — YES



∃ column may be removed, rows to remain distinct.

Now → we go back, remove a column from $n \times m$ matrix. $\square$.

Solution 2. (Story) Ross Honsberger.

Assume that any C_k column we remove, there appear duplicate rows: R_i and R_j.

For $k' \neq k$ → could they be the same? NO.

Build graph G: vertices R_i

edges between $R_i \overset{k}{—} R_j$

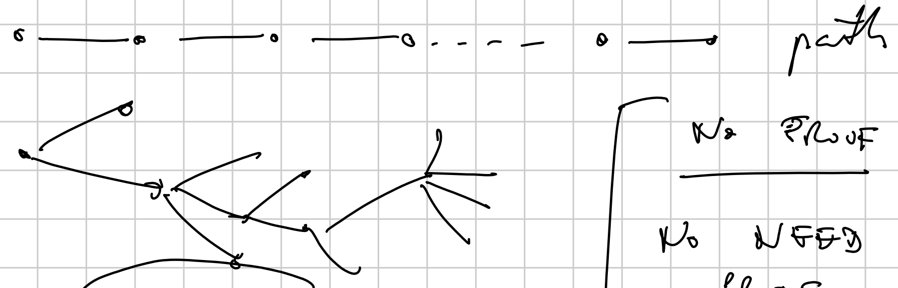
$|G| = n$, $\|G\| = n$.

What do we know about such graphs?

There must be a cycle! (YES)

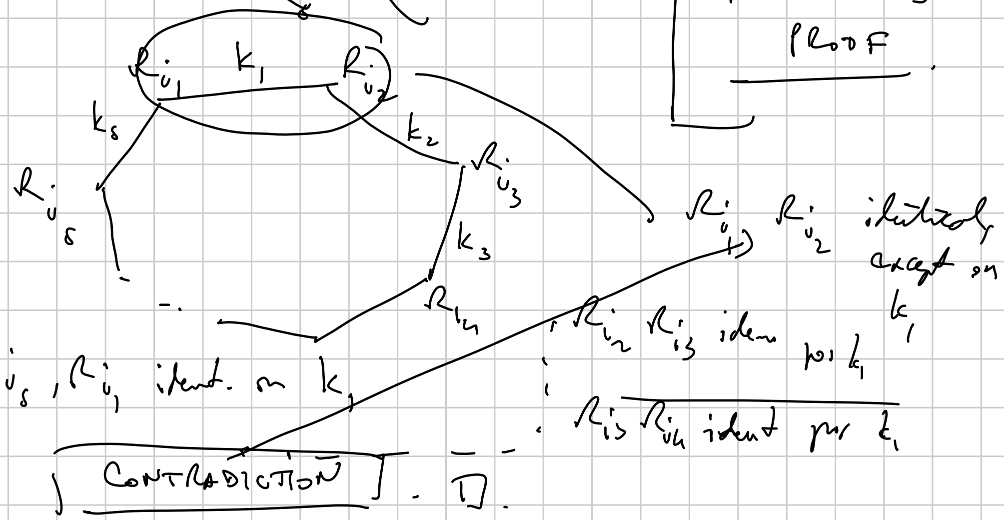
Because the largest number of edges a graph n vertices may have, so that no cycles are present — is $\boxed{n-1}$

$n-1$ the maximal # edges of an acyclic graph. Are called trees :



No PROOF

No NEED PROOF.

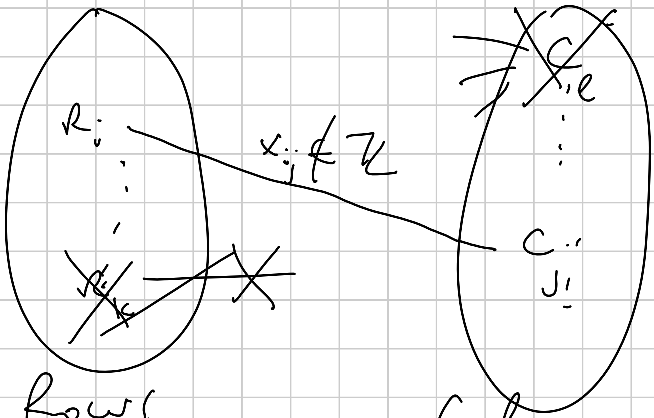


. $\square$.

Generalization. Given $m \times n$ matrix.
$m \geq n$ → we may remove $|m-n+1|$ columns → rows to remain distinct.

Problem. We have some rectangular array $m \times n$, whose entries real numbers x_{ij}.
We know that sums by rows and by columns are integer numbers.
Prove that we can replace (if need is) x_{ij} with y_{ij} integer : $y_{ij} \in \{\lfloor x_{ij} \rfloor, \lceil x_{ij} \rceil\}$, such that the sums by rows and columns stay the same.

Solution. Those $x_{ij}\in\mathbb{Z}$ do not matter.



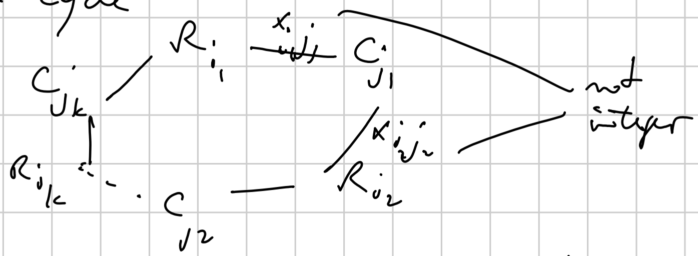
Rows

Columns.

Graph, where vertices partitioned 2 classes, and edges are only between classes. is called bipartite

$\boxed{\text{Results about bipartite graphs}}$ $\Longleftrightarrow$ Cycles are of even length.

Let's take a cycle



Let us denote by ε the least distance from any of the $x_{i_\ell j_\ell}$ to their neighboring integers.

$x_{i_1j_1}\xleftarrow{\varepsilon}$; $x_{i_2j_2}\xrightarrow{\varepsilon}$, $x_{i_3j_3}\xleftarrow{\varepsilon}$, and so on.

$x_{i_kj_k}\xrightarrow{\varepsilon}$

End $\longrightarrow$ some (≥ 1) x_{ij}'s become integer and all the conditions are obeyed.

Reverse induction $\longrightarrow$ basic algorithm (loop)
Build a new bipartite graph (strictly less edges).

Problem. Noga Alon (Combinatorial Nullstellensatz).

Consider $\{1, 2, \ldots, n\}$. Consider two permutations $\sigma, \tau \in S_n$.

$\sigma(1), \sigma(2), \ldots, \sigma(n)$ || rows of ± 1's.
$\tau(1), \tau(2), \ldots, \tau(n)$

We look at functions $f : \{1, 2, \ldots, n\} \to \{-1, +1\}$.

We look at $\sum_{k=i}^{k=j} f(\sigma(k))$ (sums of consecutive terms in the σ-sequence)

Question is? Can we find such an f, so that all these "partial sums", for both σ, and τ, they all are at most 2 in absolute value?

Solution. What if only σ was given?

choose to start $+1/-1$

$\overset{+1}{\sigma(1)}, \overset{-1}{\sigma(2)}, \ldots, \overset{+1}{\;}\overset{-1}{\sigma(n)}$

$-1 \quad + \quad -1 \qquad \pm 1$

$\underbrace{\tau(1) \quad \tau(2)}$ $\qquad \tau(n)$

$-1 \quad +1$

Subcase $\boxed{n = 2m}$ (even)

$\sigma(1) \overset{\text{red}}{—} \sigma(2) \quad \sigma(3) \overset{\text{red}}{—} \sigma(4) \quad \ldots \quad \sigma(2m-1) \overset{\text{red}}{—} \sigma(2m)$

$\tau(1) \underset{\text{blue}}{—} \tau(2) \quad \tau(3) \underset{\text{blue}}{—} \tau(4) \quad \ldots \quad \tau(2m-1) \underset{\text{blue}}{—} \tau(2m)$

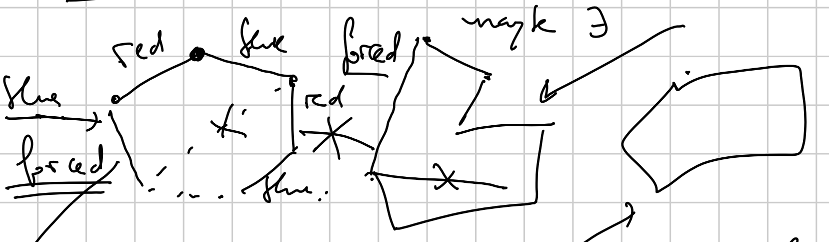
The vertices of my graph G : $\{1, 2, \ldots, n = 2m\}$

edges? $\longrightarrow$ some red, some blue.

Structure of G? $\deg(v) = 2$ (1 red + 1 blue).

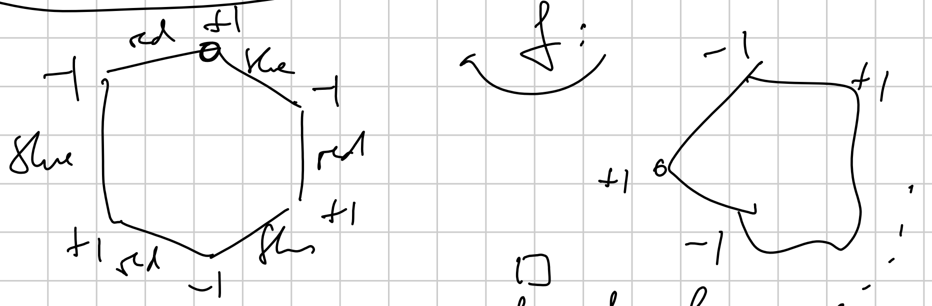
G is a 2-regular graph.

What do we know about 2-regular graphs?



$\Updownarrow$ A union of disjoint cycles

Colors come into play $\Longrightarrow$ length of the cycle is $\boxed{\text{even}}$.



□ Proved. for n even.

Kill the subcase n odd!

$= 2m+1$ ✗ reduce to $\boxed{2m}$ (ambiguous)

"enlarge"

true $\boxed{2m+2}$

$\downarrow$

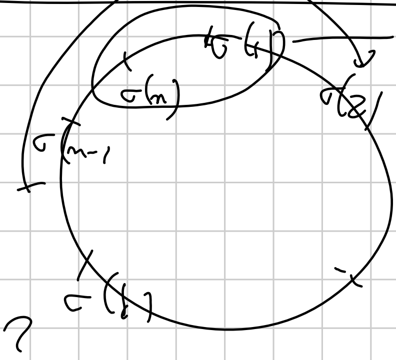
f found

Need $\tilde{\sigma}, \tilde{\tau} \in S_{2m+2}$

$\tilde{\sigma}(2m+1) = \tilde{\tau}(2m+1) = 2m+2$ (fix $2m+2$)

$\tilde{\sigma}, \tilde{\tau} \equiv \sigma, \tau$ otherwise

One last word.



become neighbours

Both σ, τ

Q: Does the result stay true?

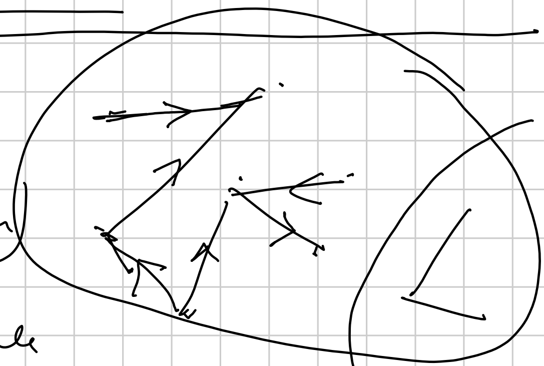
For n even — YES.

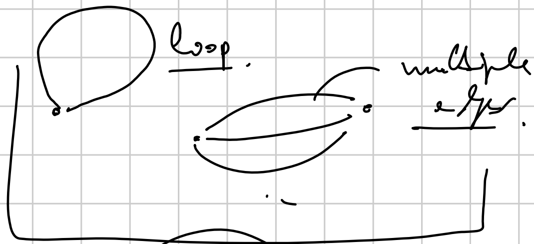
n odd — $\boxed{\text{No}}$ — Need a model.

$\sigma = id$. $\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ & 1 & & \end{pmatrix}$ all σ(evens) all σ(odds) $\pi = \begin{pmatrix} 1 & 2 & 3 & & n \\ a_1 & a_2 & & & a_n \end{pmatrix}$

Problem. $G = (V, E)$

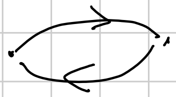
Oriented, directed, (digraph)





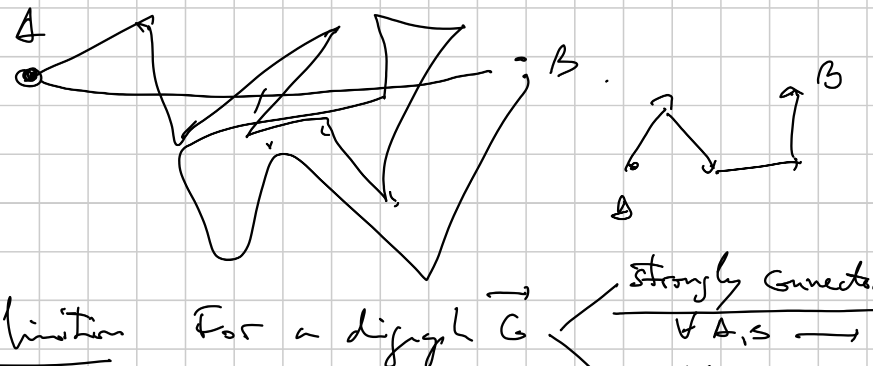
loop. multiple edges. simple

enclave (San Marino)



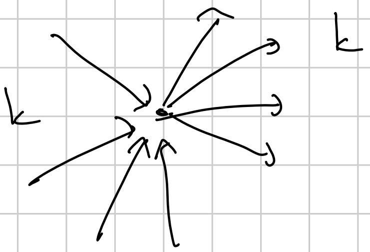
A complete digraph = tournament. (round-robin).

A graph G is called connected if any two vertices are linked by some path.

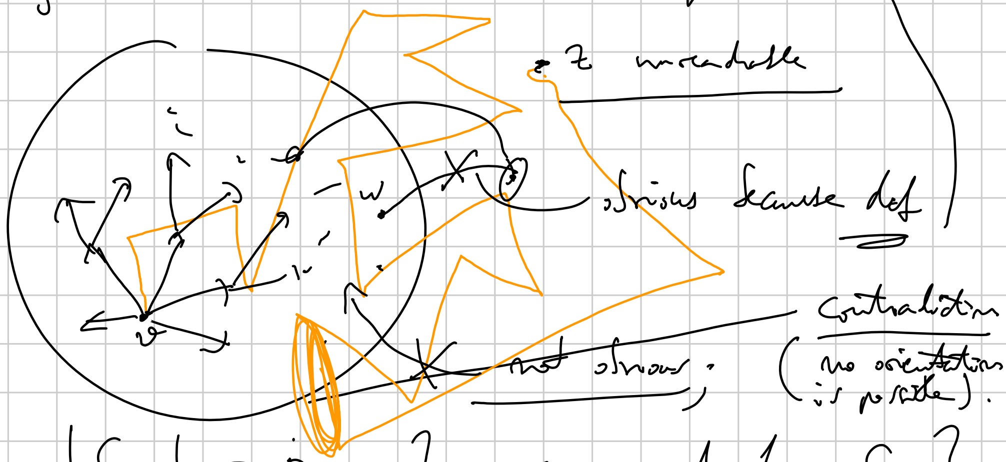


Definition For a digraph $\vec{G}$ — strongly connected if $\forall A, B \to$ path.
— weakly connected but if when ignoring the orientation, it is

Problem. Any $\boxed{k\text{-regular digraph}}$ which is weakly connected, is also strongly connected.



Solution. Start v; build the set C_v, made of all w which are reachable from v.



$|C_v| = p$; ? arrows come out of $x \in C_v$? $= pk$

? arrows coming in $x \in C_v$?

$\leq pk$ same.

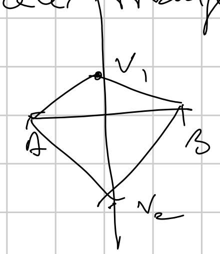
SENIOR 2010 – DAN (COMBI + LINEAR ALGEBRA)

Titolo nota 08/09/2010

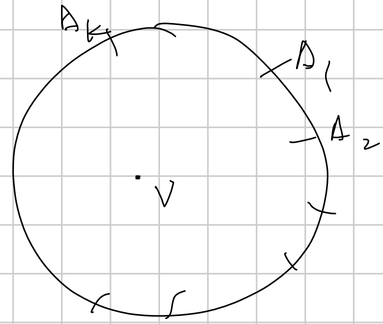
For starters IMO 1989? (double counting)
Given n, k. Given n points in the plane, no 3 collinear (in general position); for each point — there are $\geq k$ other points situated at a same distance from that point.
How large (find a bound) can k be?

Solution. Count all isosceles triangles.
$\{V, \{A, B\}\}$

1° $\binom{n}{2}$; $\underline{N \leq n(n-1)}$



2° n;



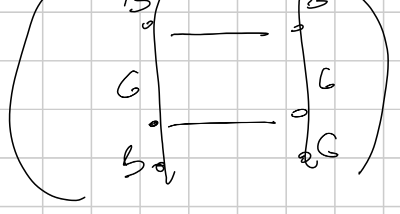
Any A_i, A_j

$\underline{N \geq n \frac{k(k-1)}{2}}$

$\square$

Problem 2 (China 2005?).

We have a $2n \times n$ array. Boys & girls.



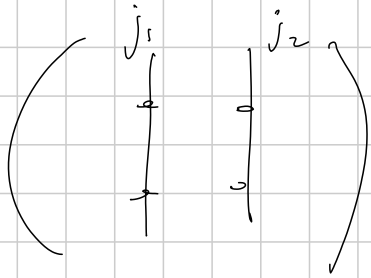
Any two columns, There are at least as many differences in gender (by row) as there are coincidences of gender.

To establish a bound for B boys!

$$i\left(\underline{\quad b_i \qquad g_i = n - b_i \quad}\right)$$

N = total # of differences of gender

$$N = \sum_{i=1}^{2m} b_i g_i \qquad \sum_{i=1}^{2m} \delta_i (n-\delta_i) \ \ldots$$



$$N \ge n\binom{m}{2} = n\frac{m(m-1)}{2}$$

$$\sum_{i=1}^{2m} \delta_i = B \qquad f(x) = x(n-x)$$

$$\sum_{i=1}^{2m} \delta_i (n-\delta_i) \le 2m\,\frac{\sum_{i=1}^{2m} \delta_i}{2m}\left(n - \frac{\sum \delta_i}{2m}\right) =$$

$$= \cancel{2m}\,\frac{B}{\cancel{2m}}\left(\frac{2mn - B}{2m}\right)$$

$$n\frac{m(m-1)}{\cancel{2}} \le N \le B\cdot\frac{2mn-B}{\cancel{2m}}$$

$$B^2 - 2mnB + n^2 m(m-1) \le 0 \qquad \Delta = \cancel{n^2m^2} - \cancel{n^2m^2} + n^2 m$$

$$mn - n\sqrt{m} \le \underbrace{B \le mn + n\sqrt{m}}.$$

$$2n = 22, \quad m = 75 \qquad \underline{mn - n\sqrt{m}} \approx$$

ELEMENTS OF LINEAR ALGEBRA.

(VECTOR)

K "body" of numbers, + (0) (1)

field $(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p)$.

of scalars.

V – set of vectors. < add, $\mathbf{0}$, $-v$; multiplication: scalar · vector.

$$\lambda(u+v) = \lambda u + \lambda v \qquad 1\cdot v = v$$

$$\lambda(\mu u) = (\lambda\mu)u \qquad 0\cdot v = \mathbf{0}$$

$$\lambda\cdot\mathbf{0} = \mathbf{0}$$

$$\sum_{i=1}^{n} \lambda_i v_i = \text{linear combination}.$$

Can it be equal to $\mathbf{0}$? without all λ_i's all v_i's being null.

$| = 0$ but not trivial = (relation)

Consider those set of vectors where there are NO relations. Such a set S linearly independent vectors. $\mathbf{0} \notin S$.

Take any l.c. $\sum_{i=1}^{n} \alpha_i v_i = u$, $v_i \in S$.

unique.

~~$\sum_{j=1}^{m} \mu_j w_j$, $w_j \in S$~~

Basis. V = lin. ind set B such that any $u \in V$ can be represented as $\sum_{i=1}^{n} \alpha_i v_i$, $v_i \in B$..

Finite $B = \{b_1, b_2, \ldots b_d\}$

$K^d = \underbrace{K \times K \times \cdots \times K}_{d} = \{(x_1, x_2, \ldots x_d) \mid x_i \in K\}$

k-plets

$\mathbf{0} = (0, 0, \ldots, 0)$

$-v = (-x_1, -x_2, \ldots -x_d)$

$\lambda v = (\lambda x_1, \lambda x_2 \ldots, \lambda x_d)$

Canonical basis: $e_1 = (1, 0, 0, \ldots 0)$
$e_2 = (0, 1, 0, \ldots 0)$
$e_d = (0, 0, \ldots 0, 1)$

$$\boxed{v = \sum_{i=1}^{d} x_i e_i}.$$

$V \simeq K^d$

isomorphic.

$b_i \longleftrightarrow e_i$

Theorem. If there exists a finite basis B with d elements, then any other basis has also d elements.

Lemma (The Exchange Lemma).

If I have two bases B, B', and chose $b' \in B'$, there exists some $b \in B$, so that $\boxed{(B \setminus \{b\}) \cup \{b'\}}$ is a basis.

Proof. Because B basis, $b' = \sum_{i=1}^{m} \lambda_i b_i$; there must be $\lambda_i \neq 0$

$$\lambda_i b_i = \sum_{j \neq i} \lambda_j b_j - b' \quad ; \text{ divide by } \lambda_i$$

$$b_i = \ldots$$

∎

B least # elem B' larger #

made of vectors B' j-th

$B' \setminus (\quad)$

$$\dim V = \dim (K^d) = d = |B| .$$

$u = (u_1, u_2, \ldots, u_d)$

$v = (v_1, v_2, \ldots, v_d)$

$$u \cdot v = \langle u, v \rangle \stackrel{\text{def}}{=} \sum_{i=1}^{d} u_i v_i \in K$$

Example: All polynomials of degree $\leq d-1$ coefficients in K

Basis $= \{1, x, x^2, \ldots, x^{d-1}\}$

$\mathbb{R}^2 =$ vectors $\mathbb{C}$

$\mathbb{R}[x]$

$\langle u_1+u_2, v\rangle = \langle u_1, v\rangle + \langle u_2, v\rangle$

$\langle \lambda u, v\rangle = \lambda \langle u, v\rangle$

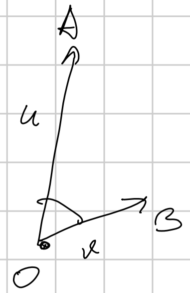
Dot product = called for a bilinear form

$\langle u, u\rangle = \sum_{i=1}^{d} u_i^2$ = square of the Euclidean distance from O to

$K = \mathbb{R}$

$\|u\|^2$

What is $\dfrac{\langle u, v\rangle}{\|u\|\cdot\|v\|} = \cos(u, v)$



Prove Cauchy–Schwarz.

(variational methods).

$0 \le \|u+\lambda v\|^2 = \langle u+\lambda v, u+\lambda v\rangle =$

$= \langle u,u\rangle + 2\lambda\langle u,v\rangle + \lambda^2\langle v,v\rangle =$

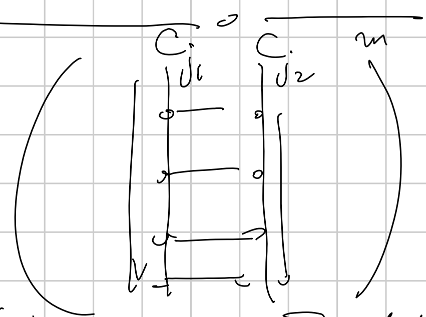
$= \|u\|^2 + 2\langle u,v\rangle\lambda + \|v\|^2\cdot\lambda^2$

$\Delta \le 0$ $\quad$ $\langle u,v\rangle^2 - \|u\|^2\cdot\|v\|^2 \le 0$ (C–S)

Back Chinese problem

Boys — $+1$

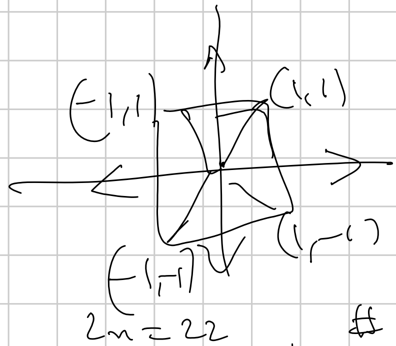
Girls — -1

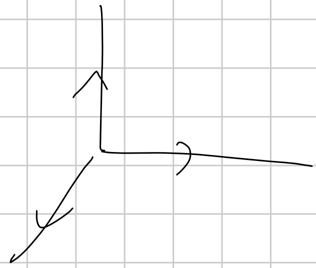


$\langle C_{j_1}, C_{j_2}\rangle = \sum_{i=1}^{2m} \ell(e_{ij})\cdot\ell(e_{ij}) \le 0$. Translates the given problem.

$\mathbb{R}^{2m}$

Result. The max. number of vectors, which 2 by 2 make $\geq \pi/2$ angle is twice the dimension of the space ($4m$)





$2n = 22$, $\# \le 44 < 75$.

Definition. $\langle u, v \rangle = 0$, orthogonal $u \perp v$

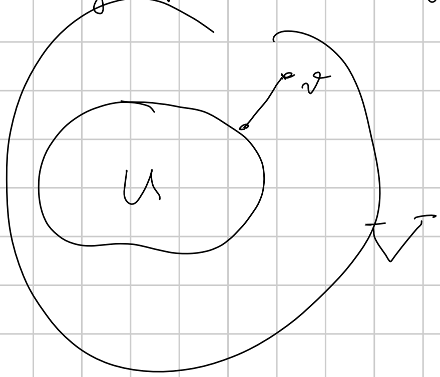
Assuming $\|u\| = 0 \iff u = 0$

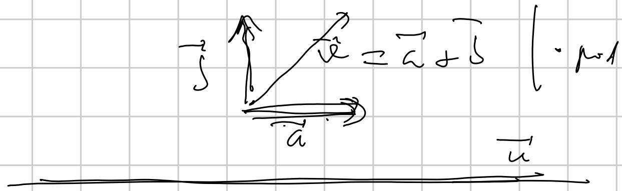
Proposition. A set of pairwise orthogonal vectors is linearly independent.

Proof. Assume $\sum_{i=1}^{n} \lambda_i v_i = 0 \quad \Big| \cdot v_j$

$$\langle v_j, \sum_{i=1}^{n} \lambda_i v_i \rangle = \lambda_j \|v_j\|^2 + \sum_{i \ne j} \lambda_i \underbrace{\langle v_j, v_i \rangle}_{=0} = \lambda_j \|v_j\|^2$$

$$0 = \lambda_j \|v_j\|^2, \quad \|v_j\|^2 \ne 0$$



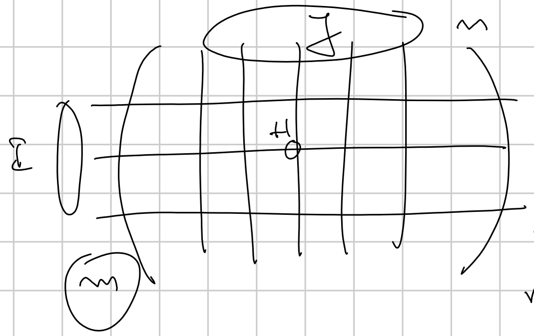


Problem (PUTNAM 2007?)

Given a $m \times n$ array whose entries are ± 1.

Look for the $+1$. Find some rows, columns I J

= subarray made of just $+1$'s.



Prove $\boxed{|I|\cdot|J| \leq \boxed{m}}$

We know that for any two rows R_i, R_j $\underline{\sum_{k=1}^{m} x_{ik}\cdot x_{jk} = 0}$

$\langle R_i, R_j\rangle = 0$; $\boxed{R_i \perp R_j}$.

$\underline{m=1}$ $(1, 1, \text{— —}, 1)$

$n = 2m'$

$$\begin{pmatrix} \boxed{\begin{matrix} +1 & \text{—} & +1 \\ +1 & \text{—} & +1 \end{matrix}} & \begin{matrix} +1 & \text{—} & +1 \\ -1 & -1 & -1 \end{matrix} \end{pmatrix}$$

$n=2$

Solution. My rows = vectors, n-dimensional.

Assume I, J, $R = \sum_{i\in I} R_i$;

$\|R\|^2 = \langle R, R\rangle = \langle \sum_{i\in I} R_i, \sum_{i\in I} R_i\rangle =$

$= \sum_{i\in I} \|R_i\|^2 = \underline{m|I|}$.

$\|R\|^2 = \sum_{1}^{m} (\text{coordinate})^2 = \sum_{j\in J} (\ )^2 + \sum_{j\notin J} (\ )^2$

$\geq \sum_{j\in J} (\ )^2 = |I|^2\cdot|J|$

$m\cancel{|I|} \geq |I|^{\cancel{2}}\cdot|J| \rightarrow \boxed{|I|\cdot|J| \leq m}$ $\square$

Problem. Set $|A| = n$, $A_1, A_2, \dots, A_m \subseteq A$

$|A_i| = \text{odd}$, $|A_i \cap A_j| = \text{even}$, $i \neq j$.

Prove $\underline{m \leq n}$. Trivial example if we take all $\underline{\text{singletons}}$.

$B \subseteq A$, $\chi_B : A \longrightarrow \{0,1\} = \mathbb{Z}_2$

$|A| = n$ $\qquad \chi_B(a) = \begin{cases} 0 & \text{if } a \notin B \\ 1 & \text{if } a \in B \end{cases}$

$\chi_B : (\underset{1^{st}}{0/1}, \underset{2^{nd}}{0/1}, \dots, \underset{n^{th}}{0/1}) \longrightarrow$

$B \longrightarrow \chi_B = (\qquad) \in \mathbb{Z}_2^n$

$\underline{C}$

$B \Delta C = (B \cup C) \setminus (B \cap C)$

$(B \setminus C) \cup (C \setminus B)$

$\chi_B + \chi_C = \chi_{\boxed{B \Delta C}}$

$A, \left(\mathcal{P}(A), \Delta, \cap\right)$ Boolean ring.

$A_1, A_2, \dots, A_m$ —— $\chi_{A_1}, \chi_{A_2}, \dots, \chi_{A_m}$

$|A_i| = \text{odd} \iff \|\chi_{A_i}\|^2 = 1$

$|A_i \cap A_j| = \text{even} \iff \langle \chi_{A_i}, \chi_{A_j} \rangle = 0$

$\{\chi_{A_i}\}$ $\boxed{\text{linearly independent}}$ $\subset \mathbb{Z}_2^n$ – $\underline{n\text{-dimensional}}$

$m \leq n$.

$\underline{\text{Problem}}$. ("baby" Lindstrom). (China)

Again $|A| = n$, $A_1, A_2, \dots, A_{n+1} \subseteq A$ non-empty.

Prove there exist $I, J \subseteq \{1, 2, \dots, n+1\}$, $I \cap J = \emptyset$, ~~there~~

such ~~that~~ $\bigcup_{i \in I} A_i = \bigcup_{j \in J} A_j$.

Counterexample for n subsets: $\underline{\text{all singletons}}$.

Solution. $A_i \to X_{A_i}$ vectors. $\boxed{n+1 \text{ such}}$.

$\cap$ $\mathbb{R}^n$ (same $\mathbb{Z}_2^n$)

Applying Lin. Alg. n-dimensional vector space

$\Longrightarrow$ There must exist a nontrivial relation between $n+1$ vectors: $\sum_{i=1}^{n+1} \lambda_i X_{A_i} = 0$, without all λ_i's being null. all not null

$\Rightarrow$ (there must be ≥ 2 such not-null scalar λ_i's)

$$\Longrightarrow \quad \sum_{i \in U} \lambda_i X_{A_i} = \sum_{j \in V} (-\lambda_j) X_{A_j}$$

$U, V \subset \{1, 2, \dots, n+1\}$ disjoint.

positive λ_i negative λ_j

I J

$$\boxed{\bigcup_U A_i \overset{?}{=} \bigcup_V A_j}$$

$\square$

Problem (Lindström). $A_1, A_2, \dots, A_{n+2}$

one can find I, J sets of indices, disjoint, s.t.

$\bigcup_{i \in I} A_i = \bigcup_{j \in J} A_j$, but also $\bigcap_{i \in I} A_i = \bigcap_{j \in J} A_j$.

Solution. Counterexample: all singletons, and A.

2 approaches. 1^{st} $A_i \to (X_{A_i}, X_{\overline{A_i}})$ $2n$-vector

$(\underbrace{x_1, x_2, \dots, x_n}, 1-x_1, 1-x_2, \dots, 1-x_n) \in \mathbb{R}^{2n}$

(set of vectors $S \subset V$; consider all $\sum_{i=1}^{t} \lambda_i x_i$, $x_i \in S$

$\langle S \rangle \subseteq V$ a linear space generated by S.

$|A| = n$, all $B \subseteq A$ — $\left(\chi_B \mid \chi_{\bar B} \right)_{2n} \subset \mathbb{R}^{2n}$

$\dim \langle S \rangle \geq n$? generate a copy of $\mathbb{R}^n$

$= \boxed{n+1}$

There must be a non-trivial relation. $\boxed{\sum_{i=1}^{n+2} \lambda_i (\chi_{A_i} \chi_{\bar A_i}) = 0}$

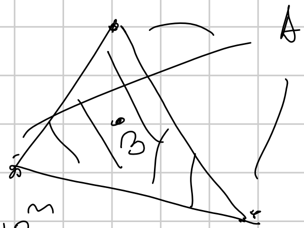
We separate $\underbrace{\text{positive } \lambda\text{'s}}_{U} = \underbrace{\text{negative } \lambda\text{'s}}_{-V}$

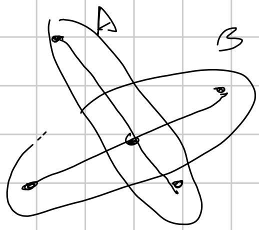
2nd — <u>Helly's Theorem</u>. If a (finite) collection of convex sets intersect 3 by 3, then they all have a common point.

$\mathbb{R}^n$, need to intersect in groups of $n+1$

<u>Radon's Theorem</u> If $n+2$ points in $\mathbb{R}^n$ then there is at least one way to partition them into two nonempty sets A, B. such that $\boxed{\operatorname{conv}(A) \cap \operatorname{conv}(B) \neq \emptyset}$

$\mathbb{R}^2$: $\boxed{n+2 = 4}$:





$\in \mathbb{R}^n$

x_{A_i} $1, 2, \ldots, n+2$ can be partitioned. A, B

$x \in \operatorname{conv}(A) \cap \operatorname{conv}(B) \neq \emptyset$.

$$\| \quad \sum_{i\in A} \lambda_i x_{A_i} = \sum_{j \in B} \mu_j x_{A_j}$$

I J

x writes in Conv(A) x writes conv.(B)

→ not just linear combinations.
they are convex combinations

affine combination. (sum scalars is 1)

$\boxed{\text{scalars} \begin{cases} \geq 0 \\ \text{their sum} = 1 \end{cases}}$

R Memento → How many points, (N)
(no 3 collinear), can one have in the plane,
such that for any three → at least one distance equal to 1

N ≥ 6

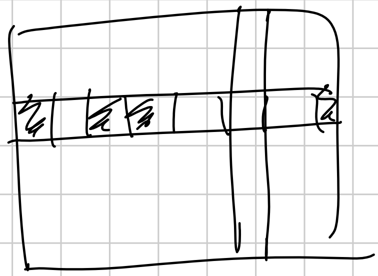
$\boxed{N = 7}$ find model
more & cannot (B)

ADVANCED - 2010 - COMBINATORICS MISCELLANEA

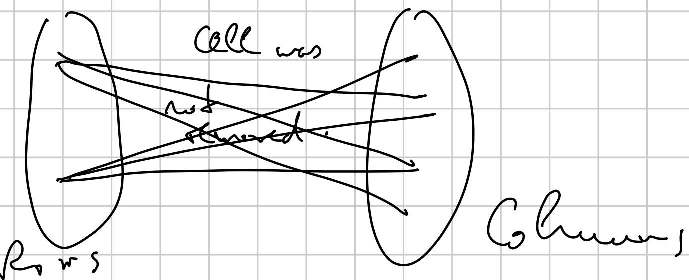
Titolo nota 10/09/2010

Problem 1. A $2n \times 2n$ chessboard; remove at will cells, but not more than n on any row or column.

Prove that one can still place $2n$ rooks so that they do not attack each other



Solution. If no cells removed $(2n)!$ ways.



Answer = perfect matching

Marriage Theorem. Bipartite graph $|A|=|B|$, if for any $S \subseteq A$, $|S| \leq |\Gamma(S)|$.

$\Rightarrow$ Yes, there is a perfect matching.

If $|S| \leq n$, ok: even one row $R \in S$ $|\Gamma(R)| \geq n$

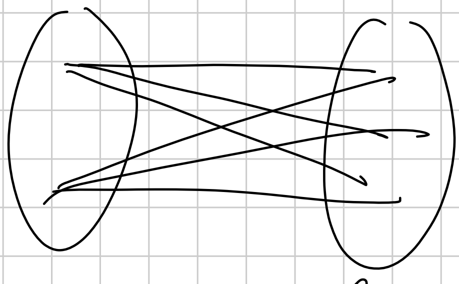
If $|S| > n$, $|\underbrace{\Gamma(S)}_{= B}| = 2n$

By M.T. $\longrightarrow$ Perfect matching can be done.

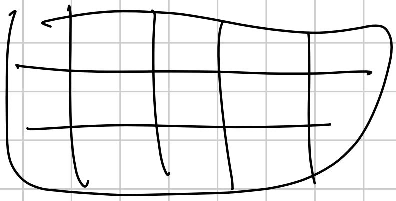
Particular case

K-regular

A



B



Set (finite) = mk elements

π partition into m classes of k elements each.

π' —— " ——

Find m elements which represent both partitions.

G group, H subgroup index n

$$G = \bigsqcup_{i=1}^{n} \underbrace{Hx_i}_{\pi_i} = \bigsqcup_{i=1}^{n} \underbrace{y_i H}_{\pi'_i}$$

Problem 2. (AMM) Island A, n families.

Ministry Agriculture: partitioned A into n equal

—"— Hunting: —"—

Ministry Family: we should allocate to each family one each so that they intersect

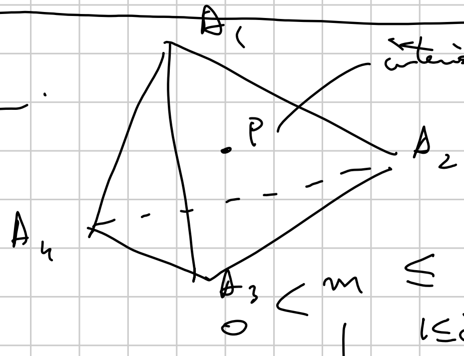
they succeeded!

Ministry Religion: declared a miracle!

a) Math. Institute: → refuted: it could always be done!

b) Find the fraction λ of area A island, so that by a clever allocation, each family receives a $|C_i \cap H_i| \geq \lambda$.

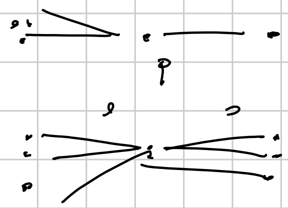
GEOMETRY



$$0 < m \leq \sum_{1 \leq i < j \leq 4} \measuredangle A_i P A_j \leq M < 6\pi$$

Claim

3π $\qquad$ 4π



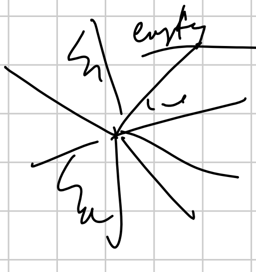
$\Sigma \approx 3\pi + 3 \cdot 0 = 3\pi$

$\Sigma \approx 2 \cdot 0 + 4 \cdot \pi = 4\pi$.

Convex polyhedron

Σ angles $< 2\pi$

"Cut" along edges → put on a plane



$2\pi - \Sigma$ angles $=$ "defect"

$\sum$ defect $= ?\ \boxed{4\pi}$.

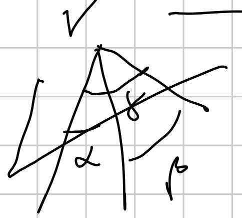
Polyhedra

$\Uparrow$

Euler: $V + F = E + 2$.

Proof. $\sum_{\text{around a vertex}}$ angles $< 2\pi$

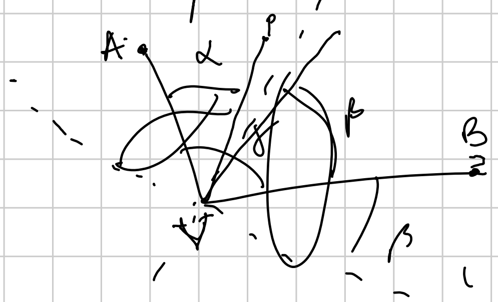
show **Lemma**. Vertex of a ~~tetra~~hedron.



α, β, γ have the "triangular" ineq. property

$$\alpha+\beta \geq \gamma, \quad \beta+\gamma \geq \alpha, \quad \gamma+\alpha \geq \beta$$

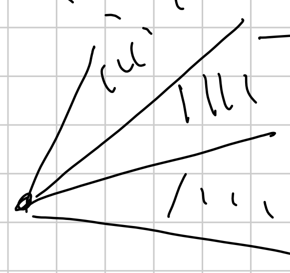
In the plane draw the layout of γ:



Assume $\alpha+\beta < \gamma$.

Locus in $\mathbb{R}^3$ of points P s.t. $\angle PVA = \alpha$?

Q

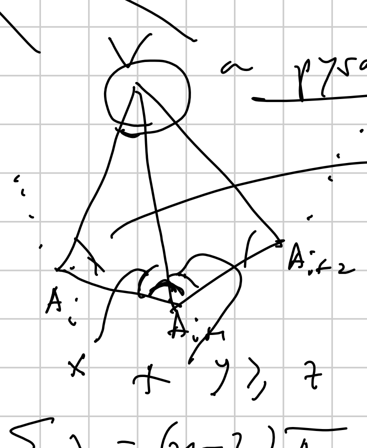


π

$= \beta$

$\sum_{i=1}^{n} \alpha_i$

a pyramid.



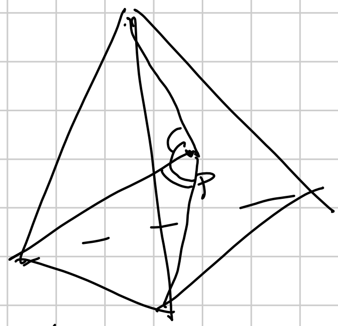
π

$\sum$ along all lateral faces $= n\pi$

$x + y \geq z$

$\sum z = (n-2)\pi$

$\sum^{6} \measuredangle A_i P A_j \le 4\pi$



$\sum^{3} \le 2\pi$

for all groups of 3 out of the 4 vertices

Four times $\cancel{2}\sum^{6} \le \frac{\cancel{8}\pi}{\cancel{4}}$.

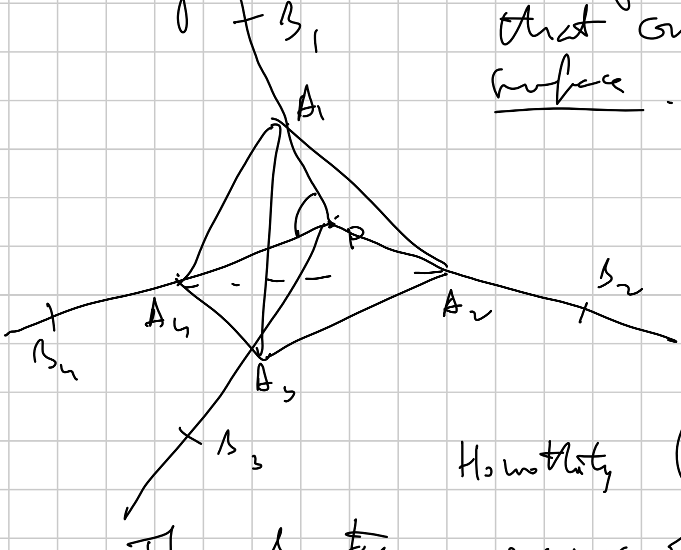
$3 \le \sum^{6} \underset{2\pi}{\le} \widehat{A_1PA_3} + \widehat{A_3PA_4} + \widehat{A_4PA_2} + \widehat{A_2PA_1}$

$(1,3,4,2)$

Lateral. Why is this happening (is it?).

One way → you do a nice drawing on a sphere.

"geodesic" = "arc" of minimal length that connects 2 points on a surface.

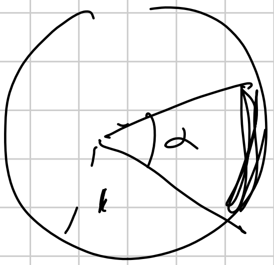


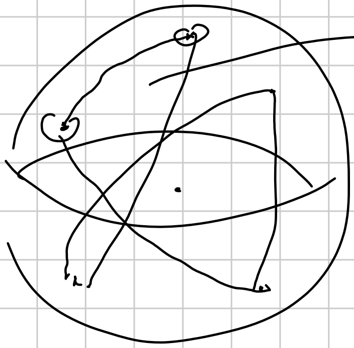
Can take B_i such that PB_i = equal.

P center of the sphere △ $B_1B_2B_3B_4$ inscribed.

Homothety $(=1,$

The advantage: measure of $\measuredangle$ (radians) = length of the arc great circle "subtended".

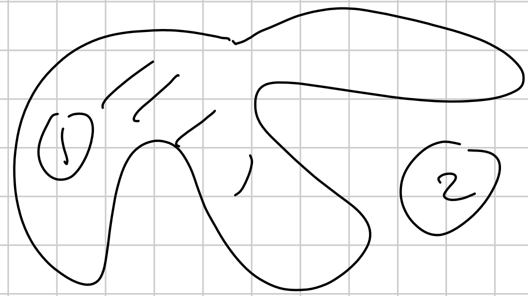


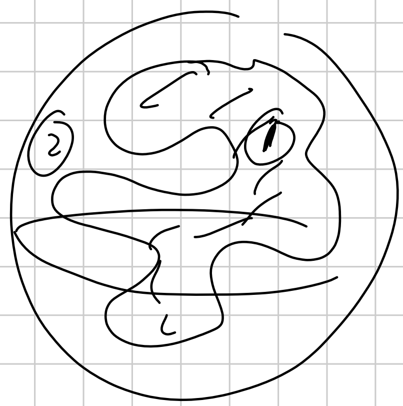


length of
L arc $\geq 2\pi$.

WRONG
PICTURE

Combi fact 1. If on surface of sphere of radius 1, curve γ simple (does not autointersect), closed, rectifiable (its length can be calculated). And if such a curve, divides surface of sphere into 2 regions, equal area, Then length $\lambda(\gamma) \geq 2\pi$.





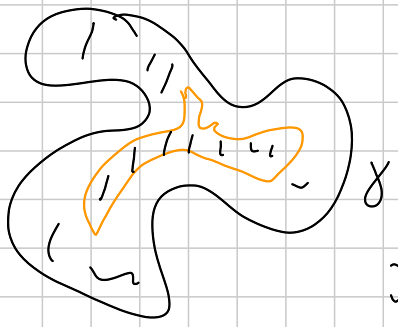
Torus (doughnut)

Proof. $\varphi : S^2 \longrightarrow S^2$

$p \longrightarrow p' =$ antipode

$\varphi(\gamma) =$ curve. γ blue

$\varphi(\gamma)$ red



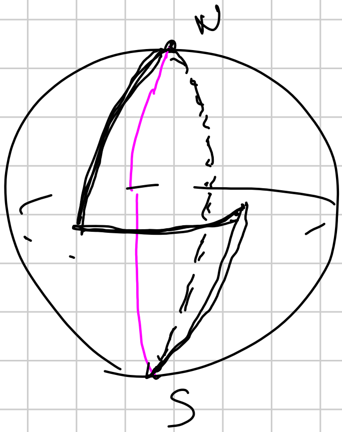
$|\gamma \cap \varphi(\gamma)| \geq 2$ (pairs)
P

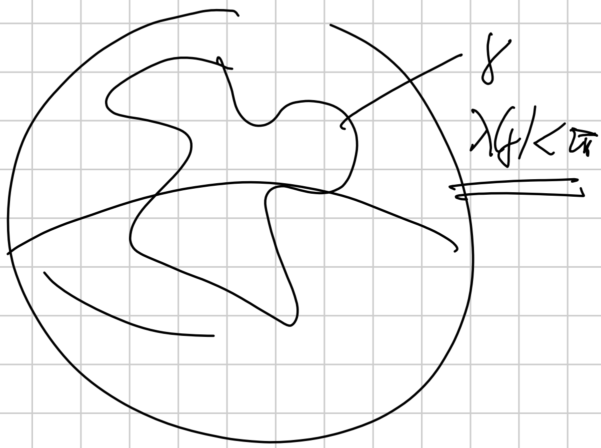
$P, P' \in \gamma$ $(\varphi(\gamma))$

$\lambda(\gamma) = \widehat{PP'} + \widehat{P'P} \geq \frac{1}{2}$ circle $+ \frac{1}{2}$

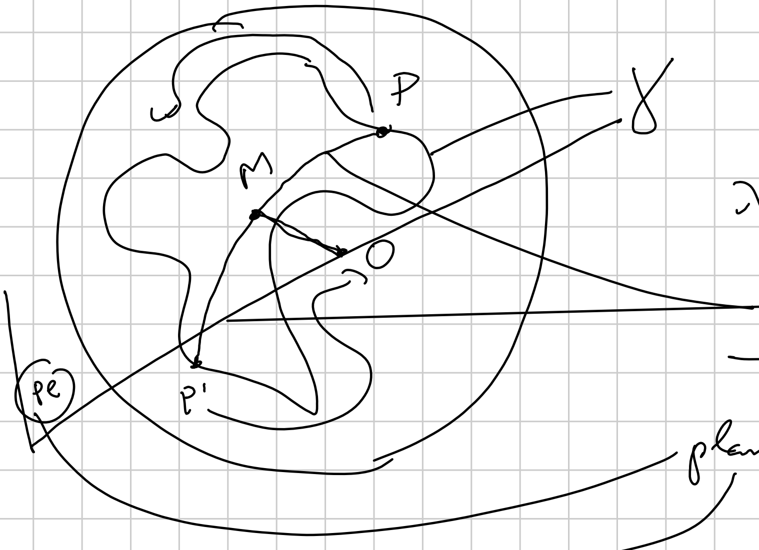
$=$ full great circle $= 2\pi$

$\square$





γ ⊂ Hemisphere.



$\exists!\, P'$

$\lambda(PP') = \lambda(P'P)$

~~arc of great circle PP'~~

plane ⊥ OM
"middle"

γ ⊂ Hemispl.

Assume not.

Either PP' $P'P$ ∩ "equator"

equat $\cap$ $\rho\rho'$ $\longrightarrow$ symmetric with respect to O$\cap$

X $\longrightarrow$ arc $\subset$ S

same length $= \frac{1}{2}\lambda(\gamma)$

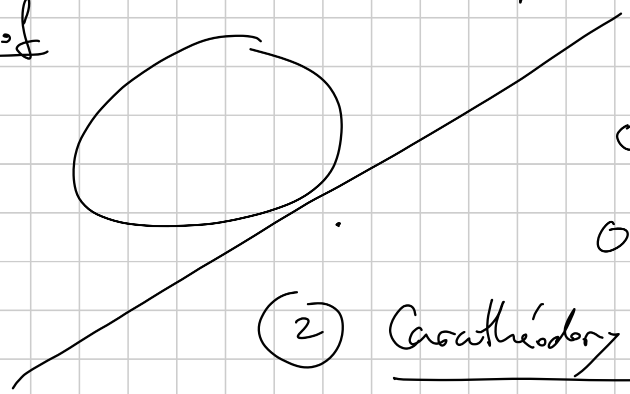
X' $\cup$ also on equator (opposite)

Instead looking at γ : ($\underbrace{\rho\rho' \cup \text{symmetric arc}}_{=\lambda(\gamma)}$)

contains X, X' $= \lambda(\gamma)$

My solution : (1) The fact that a set $S \subset S^2$ is not contained in ANY hemisphere $\Longleftrightarrow$ Conv(S) $\ni$ O.

Proof



O $\notin$ Conv(S)

O $\in$ Conv(S)

(2) Carathéodory Theorem $\in \gamma$

There must be de some $A_1, A_2, A_3, A_4 \ni$ O

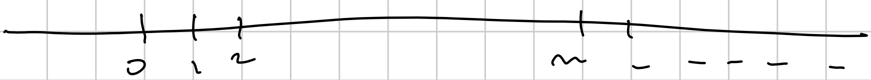
(3)

o o

Monty Python : And now, on a different ...

Problems with hats, names _ _ _

(1) $\longrightarrow$



Establish an equivalence relation among infinite binary "words"

wwwwwww. . . — — — —

$X \sim Y \overset{def}{\iff}$ they differ only in finitely many positions.

Agree on a representative $X \in \hat{X}$ (Axiom of choice)

Each one → write the color on the position that he occupies.

Finite variations $1 \to n$

$1, 2, \ldots n$ → as they write down a color, they also pronounce it.

The n persons again not allowed to speak

But instead →

n people, n colors of hats

Strategy 1st give themselves some number $1 - n$

2nd give the colors some code $1 - n$

Each will write: $\left[\left(\sum \text{colors he sees}\right) - \text{his position}\right] (\text{mod } n)$

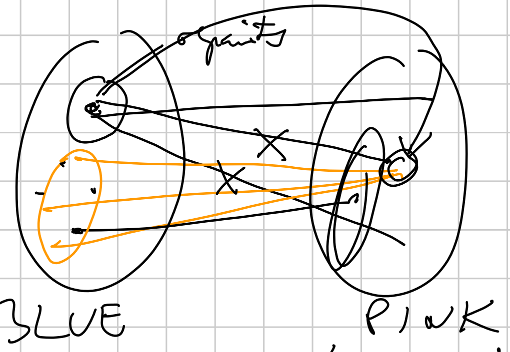
$= \sum_{\text{colors}}^{\text{all}} -$ the color of first person hat

constant

In a forest there n dwarves: blue, pink hat

Each one, in turn, visits all his friends.
If strictly > 1/2 his friends have a ~~lower~~ different color than his → he repaints.
Show, after some time → there is no need to repaint.

Sikinia.



The number of edges between B/P is ↓ strictly

The (2n) dwarves — game:

In cabin there are 2n boxes, each containing the name of one dwarf.

One by one, each enters cabin, allowed to open $\leq n$ boxes → finding his name.

They win if ALL find their names.
What strategy to maximize the chance to win?

From the "idiot" → $\left(\frac{1}{2}\right)^{2n}$ chance
a $\frac{1}{n}$ chance by improvement

Sketch: k → opens box k — if i
if not open box i

1	2	– – –	2n
$\sigma(1)$	$\sigma(2)$		$\sigma(2n)$

$$\sigma = \left(1, \sigma(1), \sigma(\sigma(1)) \ldots\right)\left(3, \sigma(3) \ldots\right)\left(k\right) =$$

$$\Rightarrow \sigma = \prod_{i=1}^{s} \gamma_i \,, \quad \sum \lambda(\gamma_i) = 2n \,.$$

They win game if $\lambda(\gamma_i) \le n, \ \forall i$.

Estimate $\dfrac{\#\,\sigma \text{ with cycles} \le n}{\#\text{ perm} = (2n)!}$.

Count N of σ which do have cycles of $\lambda > n$

$n+1$ —
$n+2$ —
$\vdots$
$2n$ —

Let's count $\# N_k$ of σ with a cycle $\lambda = n+k$, $k = 1, 2, \ldots, n$

$(\quad)_{n+k}$ (rest) arbitrary $(n-k)!$

$$\binom{2n}{n+k} \cdot (n+k-1)! \cdot (n-k)! = \frac{2n!}{n+k}$$

$$\bar{p} = \frac{\bar{N}}{(2n)!} = \frac{1}{n+1} + \frac{1}{n+2} + \ldots \frac{1}{2n} \approx \ln 2$$

$$p = 1 - \ln 2 = 0.7 \quad \approx 30\%$$

$\boxed{\text{LAST}} \rightarrow$ (Martin GARDNER)

You are given N folded papers, each a real number distinct.

You pick the $\boxed{\text{largest}}$

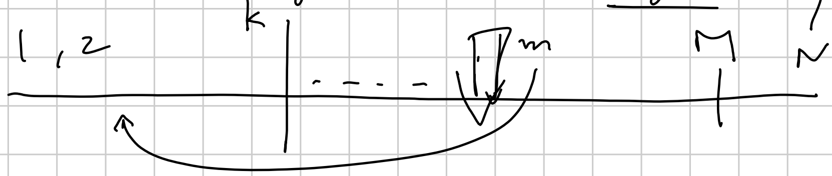
The "idiot" — pick one $1/N$

the only possible strategy is:

— pick $1 \le k \le N-1$

— open k papers — put them aside.

— start opening, until hit one larger than those rejected



$k \longmapsto p_k$ = probability of winning.

find which k max

$k \approx \frac{N}{e}$, $p_k \approx \frac{1}{e}$.

1...2...3, SCAPPATE!!!! XD

MA MENO MALE CHE CI SONO I CANNONI

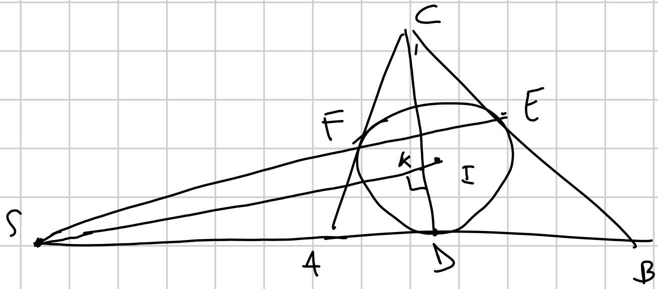
"PUÒ BACIARE LA SPOSA!"

"MA È UN LUPO!!!"

"NO! PRENDIAMO X, E MÒ NON LA FAI LA PROIETTIVITÀ CHE MANDA P ALL'INFINITO!

Titolo nota 10/09/2010

1. ABC triangolo, I incentro, D, E, F punti di tangenza, $S = EF \cap BA$. Th: $SI \perp CD$

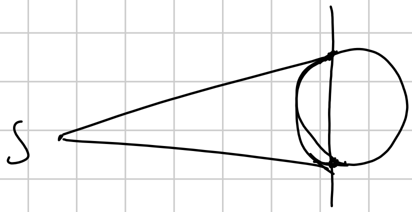


$D \in pol(S)$

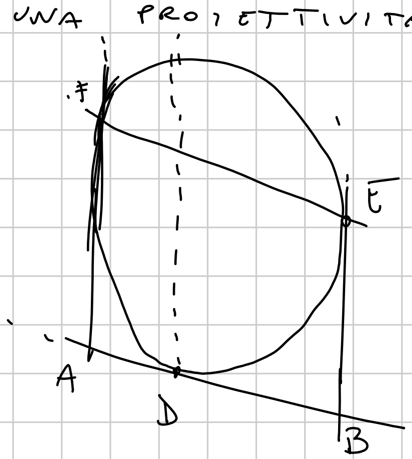
$S \in pol(C) \Rightarrow$

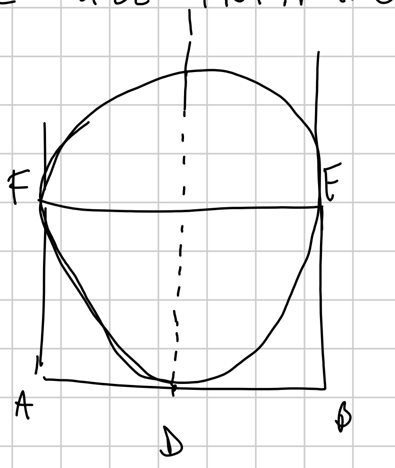
$C \in pol(S)$

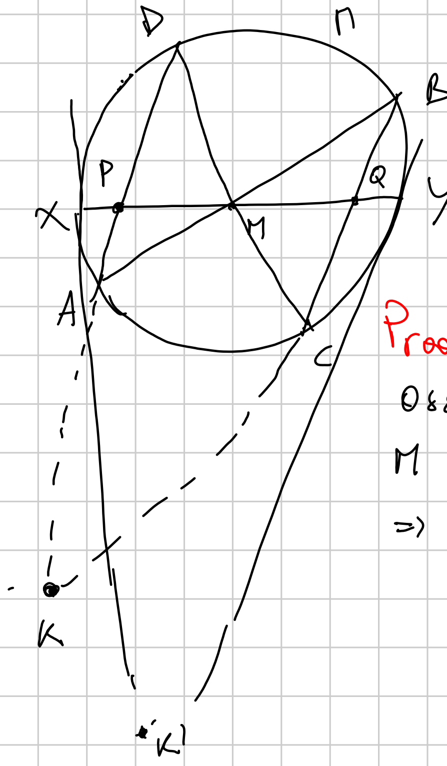
$\Rightarrow \quad pol(S) = CD$



2ª SOL. MANDO LA RETTA SC ALL'INFINITO CON UNA PROIETTIVITA'







Butterfly theorem

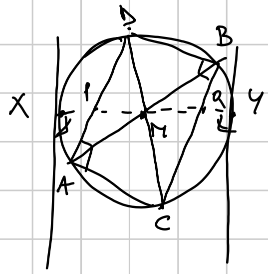
Hp: $XM = MY$ ⇝ X, M, Y, ∞ quat. armonica

Th: $PM = MQ$ ⇝ P, M, Q, ∞ quat. armonica

Proof: Mando la retta KK' all'infinito

Osservo CAF è la polare di M $\Rightarrow$ $KK' \cap \Gamma = \emptyset$

$\Rightarrow$ Γ si può mantenere cfr.



$pol(M) \perp OM$

$OM \perp XY$

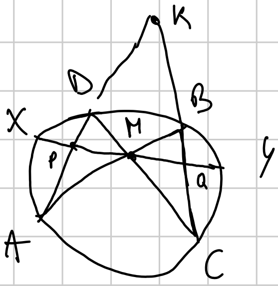
$\Rightarrow pol(M) \parallel XY$

$\Rightarrow \infty \in pol(M)$

Nel disegno nuovo:

- le tangenti in X e Y a Γ sono parallele
  $\Rightarrow$ XY è diametro di Γ
- X, M, Y, ∞_{XY} rimane una quaterna armonica
  $\Rightarrow$ $MX = MY$ $\Rightarrow$ M è il centro di Γ
- $M \in DC$ $\Rightarrow$ DC è diametro $\Rightarrow$ $C\hat{A}D$ è retto
  e similmente gli altri angoli di $ACBD$
- Ora la figura risulta simmetrica $\Rightarrow$ $PM = MQ$
  $\Rightarrow$ P, M, Q, ∞_{XY} è quaterna armonica
  $\Rightarrow$ Thesis!!

□.



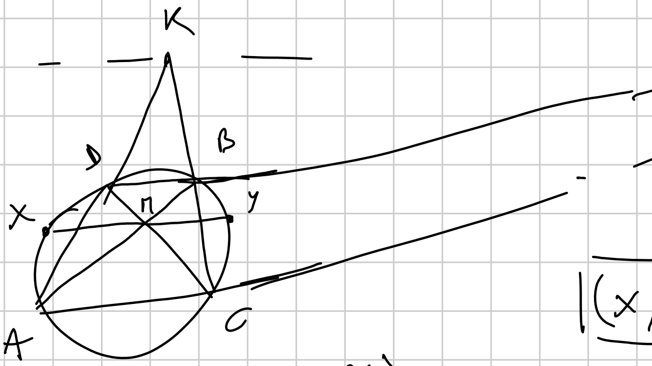
Birapporto X, B, D, Y

proiettando da C ottengo

$$(X, B, D, Y) = (X, Q, M, Y)$$
$$= (X, M, P, Y)$$

$$\frac{\cancel{XM}\cdot QY}{\cancel{XY}\cdot QM} = \frac{XP\cdot \cancel{MY}}{\cancel{XY}\cdot MP}$$

$\Rightarrow$ Q, P dividono due segmenti uguali (XM e MY) nella stessa proporzione $\Rightarrow$ $PM = MQ$



$KJ = \mathrm{pol}(M)$

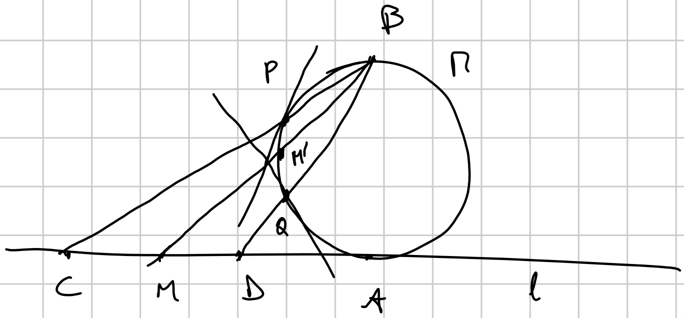
$KJ \cap XY = J'$

$\boxed{(X, Y, M, J') = -1}$??

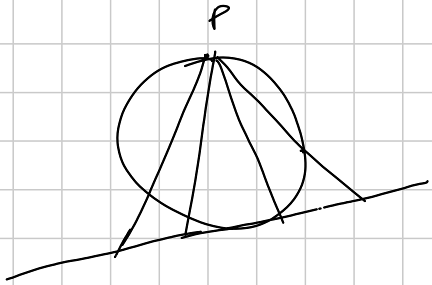
COSÌ DIMOSTRO $KJ \parallel XY$

$C, M, D, A \in l$ $\quad CM = MD \quad$ ω tange l in A

B diam. opp. ad A in ω



tangente in P
tangente in Q } Concorrono
BM



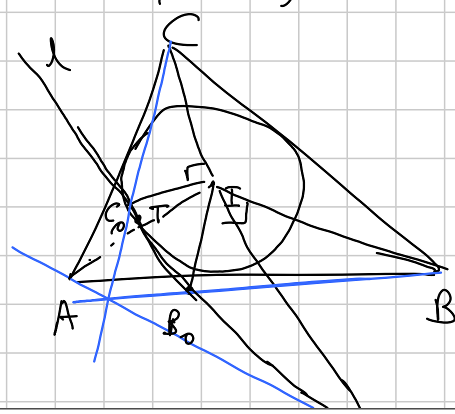
1. inverto in B dimodochè
P va in C (di raggio BA)
$R \Leftrightarrow l$
$\boxed{BCD \sim BQP}$
BM è simmediana
$\Rightarrow$ Lemma simmediana

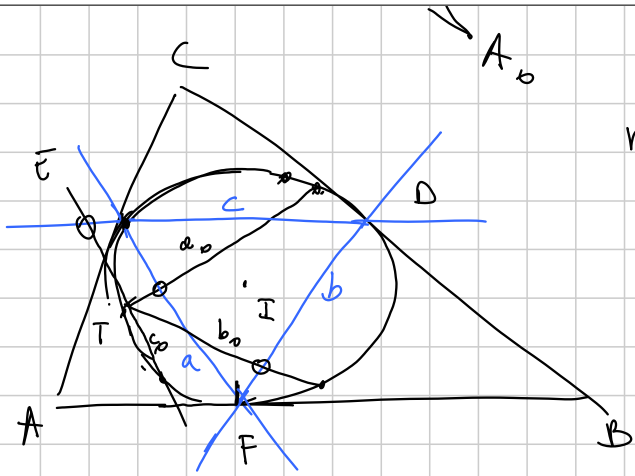
$BPM'Q$ è quadrilatero armonico
$\Rightarrow$ tangenti e diagonale concorrono

— o —

18. ABC triangolo I incentro. Sia l tangente all'incerchio. Siano $A_0, B_0, C_0 \in l$ tali che $A\hat{I}A_0 = B\hat{I}B_0 = C\hat{I}C_0 = 90^\circ$

Th. AA_0, BB_0, CC_0 concorrenti





retta di Simson

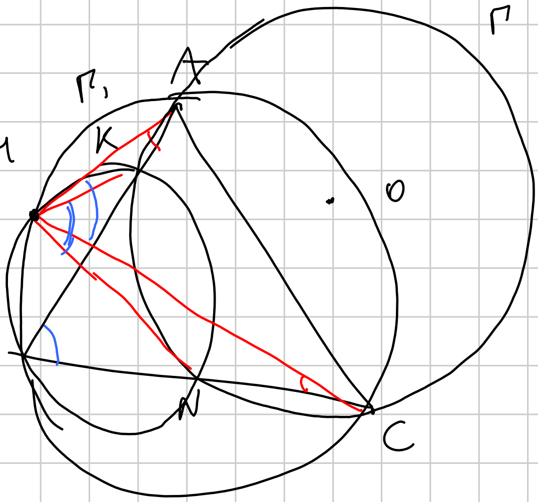
$c \perp c_0$

$a \perp a_0$

$b \perp b_0$

$T \in \Gamma \Rightarrow$ triangolo pedale è degenere $\Rightarrow$ i punti sono allineati

(IMO 1985)



Th: $OM \perp MB$

KN, MB, AC concorrono (assi radicali)

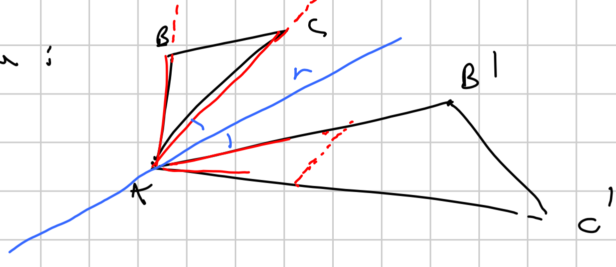
Angoli su Γ_1 $\rightsquigarrow$ $M\hat{A}K = M\hat{C}N$

Angoli su Γ_2 $\rightsquigarrow$ $K\hat{M}N = K\hat{B}N$

Angoli su Γ $\rightsquigarrow$ $A\hat{B}C = A\hat{M}C$

$\Rightarrow \overset{\triangle}{MAK} \sim \overset{\triangle}{MCN}$

Lemma:



$\overset{\triangle}{ABC} \sim \overset{\triangle}{AB'C'}$

$\Rightarrow \exists$ inv. in A composta con una sim. assiale che manda $B \rightsquigarrow C'$ e C in B'

Prendo raggio^2 $= AB \cdot AC' \overset{\text{sim.}}{=} AC \cdot AB'$

Simetria wrt r fa esattamente quello che vogliamo.

Γ rimane dunque in se stessa.

1. poiché il raggio rimane lo stesso $\Gamma \rightsquigarrow \Gamma$ con l'inversione.

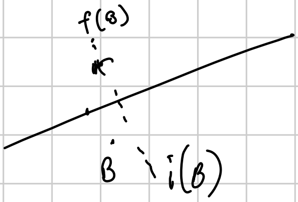
2. $\Gamma \rightsquigarrow \Gamma$ con la riflessione $\Rightarrow O \in r$

B dove va? $B = \Gamma_1 \cap \Gamma_2$

$$i(B) = i(\Gamma_1) \cap i(\Gamma_2) = i(A)i(C) \cap i(K)i(N)$$

$$f(B) = f(A)f(C) \cap f(K)f(N) = NK \cap CA \in MB$$

$\Rightarrow f(B)$ è su MB. ma si vede $i(B) \in AB$



$\Rightarrow i(B)f(B) \cap r = M$

$i(B)f(B) \perp r$

$r \perp i(B)M = BM$

$OM \perp BM$

$\square$.

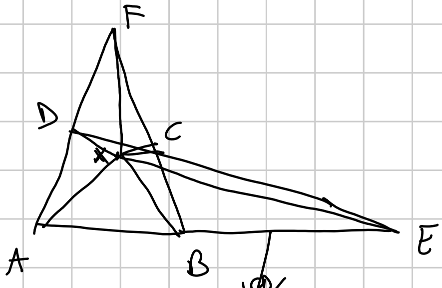
$i(P) =$ immagine di P secondo l'inversione

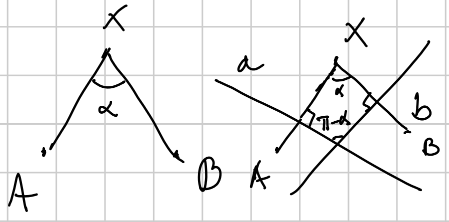
$f(P) =$ immagine di P secondo inversione + riflessione

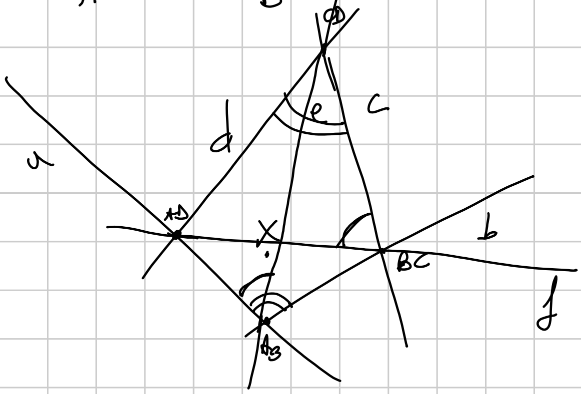
ROBA DI VERTECHI: http://veluca.altervista.org/olimpiadi/

Yufei Zhao (billzhao su ML). (fonte degli esercizi)

14. ABCD quadrilatero convesso. $AB \cap CD = E$, $AD \cap BC = F$
Esiste X (dentro il quad.) t.c. $A\hat{X}E = C\hat{X}F$. Th: $A\hat{X}B + C\hat{X}D = 180°$





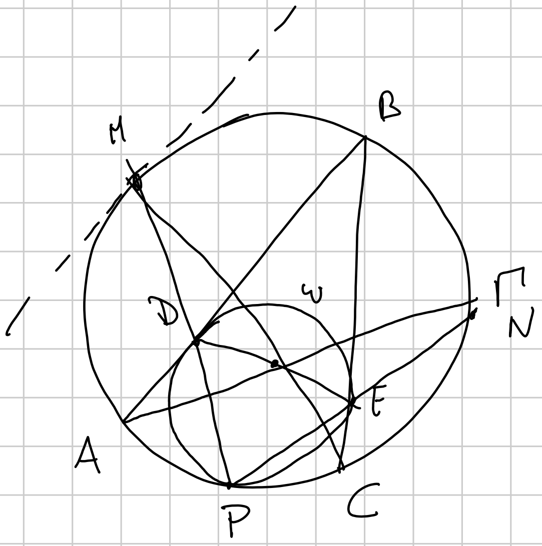


$A\hat{X}F = 180° - C\hat{X}F$

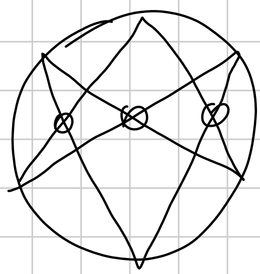
⇓ X interno + ciclicità

$A\hat{X}B = 180° - C\hat{X}D$

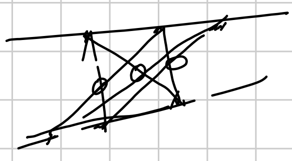
□



Th: p.to medio di DE e' l'incentro di ABC



Pappo-Pascal



Pascal: D, E, $CM \cap AN$
sono allineati

M, N punti medi degli archi ⇒ CM e AN
sono bisettrici in ABC ⇒ $CM \cap AN = I$

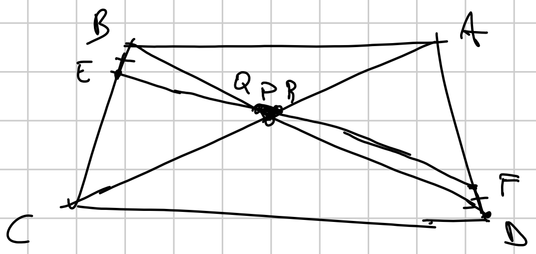
D, I, E allineati. Considero DBF, isoscele, dunque I è punto medio di DF.

ABCD q. convesso $BC = AD$ ma $BC \not\parallel AD$

$E \in BC$ $F \in AD$ t.c. $BE = DF$.

$AC \cap BD = P$, $BD \cap EF = Q$, $EF \cap AC = R$

Considero PQR al variare di E ed F. Dimostrare che tutti i circocerchi hanno un punto in comune diverso da P



TEORIA DEI NUMERI 3

Titolo nota 09/09/2010

· GRUPPO

$G \times G \to G \qquad f(a,b) = a \cdot b$

$\exists$ ELEMENTO NEUTRO

$e \in G: \quad a \cdot e = e \cdot a = a \quad \forall a \in G$

- ASSOCIATIVA: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $\exists$ INVERSO: $\forall a \, \exists b: \; ab = ba = e$

$b = a^{-1}$

COMM. $\quad ab = b \cdot a$

ANELLO COMMUTATIVI

A 2 operazione

A è un gruppo rispetto al +

prodotto:

- ASSOCIATIVO
- DISTRIBUTIVO $\quad a(b+c) = ab + ac$
- COMMUTATIVO $\quad ab = b \cdot a$

A ANELLO CON UNITÀ

se $\exists \, e: \quad a \cdot e = e \cdot a = a \quad \forall a \in A$

- EL NEUTRO SOMMA = 0
- EL NEUTRO PRODOTTO = 1

DOMINI DI INTEGRITÀ

A anello è un dominio

se $\forall a, b \neq 0$, $a \cdot b \neq 0$

a PUÒ NON AVERE INVERSO MOLTIPLICATIVO

$ab = ac \not\Rightarrow b = c$

$2 \cdot 4 = 2 \cdot 1$ $\mathbb{Z}_6$

VERA NEI DOMINI

$ab = ac \Rightarrow ab - ac = 0 \Rightarrow a \cdot (b - c) = 0$

$a \neq 0$, $\vee$ $b = c$

CAMPI $\mathbb{K}$

- SOMMA GRUPPO ABELIANO
- PRODOTTO $\mathbb{K} \setminus \{0\}$ $\mathbb{K}^*$

GRUPPO ABELIANO COMMUTATIVO

$a \cdot (b + c) = ab + ac$

I CAMPI SONO DOMINI.

DOMINI EUCLIDEI D

ESISTE UNA FUNZIONE (GRADO)

$g: D \setminus \{0\} \to \mathbb{N}$

$\forall\, m, n \in D \quad \exists\, k, r \in D:$

$\boxed{m = kn + r}$ E $g(r) < g(n)$

DIVISIONE CON RESTO OPPURE $r = 0$

$\forall\, a, b \neq 0$

$g(ab) \geq g(a)$

CON L'UGUAGL

SSE b INVERT.

ESERCIZIO

GRUPPO $\mathbb{Z}_n$ RISPETTO ALLA SOMMA

ANELLO $\mathbb{Z}_n\ +, \cdot$ ANELLO CON UNITÀ

$\mathbb{Z}_n, +, \cdot$ NON È UN DOMINIO

$n \mid ab \quad n \nmid a \wedge n \nmid b \quad n$ COMPOSTO

PRIMO $\neq$ IRRIDUCIBILE

$n \mid ab \Rightarrow n \mid a \vee n \mid b$

IRRIDUCIBILE SE NON SI FATTORIZZA

$n = a \cdot b \qquad a = \pm 1 \vee b = \pm 1$

$n \mid ab \quad n \mid a \vee n \mid b$

$\Downarrow\ \mathbb{Z}_p$ È UN DOMINIO

DOMINIO FINITO $\Rightarrow$ CAMPO

$\mathbb{Z}_p, +, \cdot$ È UN CAMPO, p PRIMO

FATTORIZZAZIONE UNICA (DOMINIO D)

def: $u \in D$ SI DICE UNITÀ SE È INVERTIBILE
SE $\exists\, u^{-1}$ $u \cdot u^{-1} = 1$

def: DOMINIO D È A FATT. UNICA (UFD)
SE OGNI $d \in D$ SI ESPRIME COME
PRODOTTO DI PRIMI IN MODO UNICO
(A MENO DI UNITÀ).

RISOLVERE DIOFANTEE CI SERVE!!

– DOMINI EUCLIDEI SONO UFD!!

1) PRIMO $\Leftrightarrow$ IRRIDUCIBILE

PRIMO $\Rightarrow$ IRRIDUCIBILE

$p \in D$ PRIMO NON IRRIDUCIBILE

$p = a \cdot b$ a, b NON SONO UNITÀ

$p \mid p \Rightarrow p \mid a \cdot b$ $p \mid a$ $a = p \cdot c$

$p = p \cdot c \cdot b$ $1 = c \cdot b$

2) IRRIDUCIBILE $\Rightarrow$ PRIMO

$d \in D$ IRRIDUCIBILE

SUPPONIAMO $d \mid ab$ $d \nmid a \wedge d \nmid b$

$d \nmid a$ $\exists\, s, k \in D :$ $sd + ak = 1$

$I = \{ na + md \mid n, m \in D \}$

(a, d) è L'ELEMENTO DI I A GRADO MINORE

$a \in I$ $d \in I$

$\forall\, i \in I$, $c \mid i$

$c = sa + kd$ $s, k \in D$

$i = s_1 a + k_1 d$

$i = q \cdot c + r$ $g(r) < g(c)$ $\vee$ $r = 0$

$g(r) < g(c)$

$s_1 a + k_1 d = q(sa + kd) + r$

$a(s_1 - qs) + d(k_1 - kq) = r \in I$ $g(r) < g(c)$

<u>ES</u> VIEN FUORI LO STESSO E A MENO DI UNITÀ

$a, d \in D$ EUCL. $\exists\, s, k$ $\underset{(a,d)}{sa + kd} \mid a$ $sa + kd \mid d$

(a, d) SIA TALE CHE:

$e \mid a \quad \vee \quad e \mid d \Rightarrow e \mid (a, d)$

$(a, d) \mid a \qquad (a, d) \mid d$

$d \mid ab \qquad \boxed{d \nmid a \wedge d \nmid b}$

$e_1 = \boxed{J_1 d + K_1 a}$

$e_1 \mid d \qquad \boxed{e_1 \mid a}$

$d = e_1 \cdot c \qquad e_1 = d \cdot c^{-1} \Rightarrow \boxed{d \mid e_1} \Rightarrow d \mid a$

e_1 INVERTIBILE $\exists\, e_1^{-1}$

$e_1^{-1}(J_1 d + K_1 a) = e_1 \cdot e_1^{-1}$

$\boxed{e_1^{-1} J_1}\, d + \boxed{e_1^{-1} \cdot K_1}\, a = 1$

d IRR. $\qquad d \nmid a \qquad d \nmid b$

$\Rightarrow \exists\, m_1, n_1 : \quad m_1 d + n_1 a = 1$

$m_2 d + n_2 b = 1$

$(m_1 d + n_1 a)(m_2 d + n_2 b) = 1$

$m_1 m_2 d^2 + m_1 d \cdot n_2 b + n_1 a \cdot m_2 d + n_1 n_2 \cdot ab = 1$

$d \mid ab \Rightarrow d \mid 1$ ASSURDO

PRIMO $\Leftrightarrow$ IRRIDUCIBILE

$d \in D$ INDUCO SU $g(d)$

$g(a) < g(d)$ $\quad a = \prod_{i=1}^{n} q_i$ $\quad q_i$ IRR.

$d = a \cdot b$ $\quad a, b$ NON UNITARI!

$g(d) > g(a), \quad g(d) > g(b)$

$a = \prod_{i=1}^{n} q_i \qquad b = \prod_{i=1}^{m} p_i$

$ab = \left(\prod_{i=1}^{n} q_i\right)\left(\prod_{i=1}^{m} p_i\right)$

OGNI d SI FATTORIZZA IN PRIMI

$d = \prod_{i=1}^{n} q_i = \prod_{i=1}^{m} p_i$

$q_n \mid p_j \qquad q_n \cdot u = p_j$

SEMPLIFICO E HO CONTROESEMPIO + PICCOLO!!

$g(ab) = g(a) \iff b$ INV.

$\implies$

$a = k\,ab + r \qquad g(r) \geq g(a) \qquad r = 0$

$a = kab \qquad 1 = kb$

ESEMPIO

$g(n) = |n|$ $\qquad |mn| \geq |m|$ ✓

$\mathbb{Z}[i] = \{ a+bi \mid a, b \in \mathbb{Z} \}$

$\overline{a+bi} = a - bi$ $\qquad z \in \mathbb{Z}[i] \quad \bar{z}$

$|z| = z \cdot \bar{z}$

$A \xrightarrow{f} B$

omom. $\begin{cases} f(a+b) = f(a) + f(b) & f(0) = 0 \\ f(a \cdot b) = f(a) \cdot f(b) & f(-a) = -f(a) \end{cases}$

ISOMORFISMO = OMOMORFISMO BIGETTIVO

$f \ , \ f^{-1}$

$$\overline{(a+bi) + (c+di)} = \overline{(a+bi)} + \overline{(c+di)}$$

$$\overline{(a+bi)(c+di)} = \overline{(ac - bd + bci + adi)}$$
$$= (ac - bd - bci - adi)$$
$$= (a-bi)(c-di)$$

$|a+bi| = (a+bi)(a-bi) = a^2 + b^2$

$w, z \qquad |wz| = wz \cdot \overline{wz} = w \cdot z \cdot \overline{w} \cdot \overline{z}$

$= w\overline{w} \cdot z \cdot \overline{z}$

$g(wz) \geq g(w)$

$a \neq 0$

$b \neq 0$

$m + ni$ DIVIDERLO $a+bi$

$(m+ni) = (a+bi)\boxed{(\alpha+\beta i)}$ α, β NON INTERI

$\alpha \quad \exists A : |\alpha - A| \leq \frac{1}{2}$

$A + Bi$

$|(m+ni) - (a+bi)(A+Bi)| =$

$= |(a+bi)(\alpha+\beta i) - (a+bi)(A+Bi)| =$

$= |(a+bi)((\alpha-A) + (\beta-B)i)| < |a+bi|$

$|a+bi| \, |(\alpha-A) + (\beta-B)i| < |a+bi|$

$|(\alpha-A) + (\beta-B)i| < 1$

$(\alpha-A)^2 + (\beta-B)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1$

$x^2 + 1 = y^3 \qquad x, y \in \mathbb{Z}$

$(x+i)(x-i) = y^3$

$(x+i, x-i) = (x+i, 2i)$

$p \in \mathbb{Z}[i]$ $|p| = q$ PRIMO IN $\mathbb{Z}$

p PRIMO $p = a \cdot b$ $|p| = |a| \cdot |b|$

$q = \mathbf{1} \cdot q$

3 $\quad$ 9

$2 = -i(1+i)^2$ $\quad (1+i)(1-i)$ $\boxed{1+i \text{ PRIMO}}$

$p \mid n^2+1 = (n+i)(n-i)$

$a \mid b$ $\quad \exists c \in D : ac = b$

$\exists a, b$ $\quad p(a+bi) = n+i$

$p = (a+bi)(c+di)$

$(a+bi)(c+di) \in \mathbb{R}$.

$c+di = \lambda(a-bi)$ $\quad \lambda \in \mathbb{R}$

$(a+bi)(c+di) = |a+bi| \cdot \lambda$

$p = (a+bi)(a-bi) \cdot n$

$p^2 = |a+bi| \, |a-bi| \cdot |n|$ $\quad p$

$p^2 = (|a+bi| \, n)^2$ $\quad p = |a+bi| \cdot n'$

$p = (a+bi)(a-bi)$

$p \equiv 1 \ (4)$ $\quad \exists a, b \in \mathbb{Z} : p = a^2 + b^2$

$p \equiv 3 \ (4)$ SONO IRRIDUCIBILI $\Rightarrow$ PRIMI

$(a+bi)(a-bi) = m \cdot n$ $\quad (a,b) = 1$

$\boxed{\text{WLOG}}$ $a+bi \mid m$ $\quad \nmid (a-bi)$

$m = (a+bi)(c+di) = l \cdot (a+bi)(a-bi)$

$m = l \cdot m \cdot n$

$y^3 \equiv 2 \ (4)$

$(x+i)(x-i) = y^3$ $\quad x^2+1 = y^3$

$(x+i, x-i) = (x+i, 2) = (x+i, (1+i)^2)$

$\quad = (i, 2)$

$1 = 1^3$

$-1 = (-1)^3$

$(x+i) = (a+bi)^3$ $\quad i = (-i)^3$

$-i = i^3$

$x+i = a^3 + 3a^2bi - 3ab^2 - ib^3$

$1 = 3a^2b - b^3$ $\quad b \mid 1$ $\quad b = \pm 1$

$1 = 3a^2 - 1$ $\quad 0^2+1 = 1^3$

$1 = -3a^2 + 1 \Rightarrow a = 0$

p PRIMO ≥ 3

x PARI

$x^2+1=y^p$

$(x+i)(x-i)$

$(x+i, x-i)=1$

$y^p=(a+bi)^p(a-bi)^p$

$(x+i)=(a+bi)^p$

$y^p=(a^2+b^2)^p$

$p-2k>0$

$$i=\sum_{k=0}^{\frac{p-1}{2}} a^{2k}(bi)^{p-2k}\cdot\binom{p}{2k}$$

$b \mid 1$

$b=\pm 1$

$$\cancel{i}=\cancel{(\pm i)}^p+(\pm i)^{p-2}\cdot a^2\binom{p}{2}+\dots$$

$$0=\sum_{k=1}^{\frac{p-1}{2}} a^{2k}(\pm i)^{p-2k}\binom{p}{2k} \quad a \qquad a$$

$k>1$

$$v_2\left(a^{2k}\binom{p}{2k}\right)>v_2\left(a^2\binom{p}{2}\right)$$

$$a^{2(k-1)}\frac{(p-2)!\ 2!}{(2k)!\,(p-2k)!}=a^{2(k-1)}\cdot\binom{p-2}{2k-2}\cdot\frac{2}{2k\cdot(2k-1)}$$

$$v_2\left(a^{2(k-1)}\binom{p-2}{2k-2}\frac{\cancel{2}}{\cancel{2}k\cancel{(2k-1)}}\right)>0$$

$$v_2\left(a^{2(k-1)}\binom{p-2}{2k-2}\right)>v_2(k)$$

$$\geq v_2\left(a^{2(k-1)}\right)\geq 2(k-1)$$

È POSSIBILE CHE $v_2(k)\geq 2(k-1)$?

$4^{k-1} \mid k$ $\quad k \le 1$ $\quad$ ASSURDO!

ω ~~RADICE 3ª DI 1~~

$$\boxed{\mathbb{Z}[\sqrt{-2}],\ \mathbb{Z}[\omega],\ \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]}$$

$\mathbb{Z}[\sqrt{-5}]$ $\quad 1+\sqrt{-5},\ 1-\sqrt{-5}$ $\quad (1+\sqrt{-5})(1-\sqrt{-5}) = 2\cdot 3$

UFD, EUCLIDEI

PRIMI $\quad \dots \quad |p|$ PRIMA IN $\mathbb{Z}$

$p \in \mathbb{Z}$ PRIMI IN $\mathbb{Z}$ $\quad q(x)$ NON HA RADICI mod p

$\alpha \quad \mathbb{Z}[\alpha] \quad a + b\alpha + c\alpha^2 + \dots$

$a_0 + a_1 x + \dots + a_n x^n \quad q(x)$ POL.

$\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] = \mathbb{Q}(\sqrt{-7}) \cap$ INT. ALG. (ESERCIZIO)

$\mathbb{Z}[\alpha] \quad (x-\alpha)(x-\bar{\alpha}) \quad |z| = z\cdot\bar{z}$

$a + b\alpha \to a + b\bar{\alpha}$ $\quad$ ISOMORFISMO!!!

$x^2 + 2 = y^3$

$(x+\sqrt{-2})(x-\sqrt{-2}) = y^3$

$\sqrt{-1},\ \sqrt{-2},\ \frac{1+\sqrt{-3}}{2},\ \frac{1+\sqrt{-7}}{2}$

$\frac{1+\sqrt{-19}}{2},\ \frac{1+\sqrt{-47}}{2},\ \frac{1+\sqrt{-163}}{2}$

$(x+\sqrt{-2}, \cancel{x}-\sqrt{-2}) = (x+\sqrt{-2}, 2\sqrt{-2}) = (x+\sqrt{-2}, \sqrt{-2}^3)$

$x+\sqrt{-2} = (a+b\sqrt{-2})^3$

$= a^3+3a^2b\sqrt{-2}-6ab^2-2b^3\sqrt{-2}$

$b \mid 1 \qquad b=\pm 1$

$1 = 3a^2-2 \qquad 3=3a^2 \qquad a=1$

$1 = -3a^2+2 \quad (\bmod 3)$

$a=1 \qquad b=-1 \qquad -5$

$(1-\sqrt{-2})^3 =$

$5^2+2=27$

$a^2+2=3^b$

$(a+\sqrt{-2})(a-\sqrt{-2}) = (1+\sqrt{-2})^b(1-\sqrt{-2})^b$

$(1+\sqrt{-2})^b = \pm(a\pm\sqrt{-2})$

$\mathrm{Im}\,(1+\sqrt{-2})^b = \pm 1$

$b=1$

$\dfrac{(1+\sqrt{-2})^b-(1-\sqrt{-2})^b}{(1+\sqrt{-2})-(1-\sqrt{-2})} = \pm 1 \qquad 5^2+2=3^3$

$(1-\sqrt{-2})^2 = 1-2-2\sqrt{-2} = -\boxed{(1+2\sqrt{-2})}$

$2\sqrt{-2}$

$$(1+\sqrt{-2})^h - (1-\sqrt{-2})^h = \pm\left[(1+\sqrt{-2}) - (1-\sqrt{-2})\right]$$

$$(1+\sqrt{-2})^h \equiv \pm(-1) \quad (\mathrm{mod}\ 1+2\sqrt{-2})$$

$$(-1+2\sqrt{-2})^h \equiv 1$$

$$(-2)^h \equiv 1 \quad (\mathrm{mod}\ 1+2\sqrt{-2})$$

$$1+2\sqrt{-2} \mid (-2)^h - 1$$

$$9 \mid (-2)^h - 1$$

$$a+b\sqrt{-2} \mid n \Rightarrow \frac{|a+b\sqrt{-2}|}{(a,b)} \mid n$$

$$3 \mid h$$

$$a^2+2 = 3^{3h}$$

$$\frac{(1+\sqrt{-2})^h - (1-\sqrt{-2})^h}{(1+\sqrt{-2}) - (1-\sqrt{-2})}$$

$a_0 = 0$

$a_1 = 1$

$$a_{n+2} = K a_{n+1} + J \cdot a_n$$

$a_0 = 0$

$a_1 = 1$

$$(a_n, a_m) = a_{(n,m)}$$

m' + picc. int. $a \mid a_m$

$$\Rightarrow \boxed{a \mid a_n \Leftrightarrow m \mid n}$$

$a_n = 3^K$ $\qquad a_n = \dfrac{a^n-1}{a-1}$

$a_0 = 0 \qquad a_1 = 1 \qquad a_{n+2} = K a_{n+1} + J a_n$

$(K, J) = 1$

$a_n = \dfrac{\alpha^n - \bar{\alpha}^n}{\alpha - \bar{\alpha}} \qquad (x-\alpha)(x-\bar{\alpha}) = x^2 - Kx - J$

$\mathbb{Z}[\alpha]$

$a + b\alpha$

$\| \quad \alpha^{n-1} + \alpha^{n-2}\bar{\alpha} + \dots + \bar{\alpha}^{n-1}$

LA SCIATA FISSA DAL CONIUGIO

$m = Kn$

$a_n \mid a_m \qquad \overline{\alpha^n} = \bar{\alpha}^n$

$\dfrac{\alpha^{Kn} - \bar{\alpha}^{Kn}}{\alpha^n - \bar{\alpha}^n} \in \mathbb{Z} \qquad F_n \mid F_{Kn}$

$n = dx \qquad m = dy \qquad d = (n, m)$

$b_i = \dfrac{a_{di}}{a_d} = \dfrac{\alpha^{di} - \bar{\alpha}^{di}}{\alpha^d - \bar{\alpha}^d} \in \mathbb{Z} \qquad x^2 - cx - e = 0$

$(c, e) = 1$

$(\alpha\bar{\alpha}, \alpha + \bar{\alpha}) = 1$

$a_{(n,m)} \mid (a_n, a_m) \qquad ((\alpha\bar{\alpha})^d, (\alpha+\bar{\alpha})^d) \neq 1$

$\Downarrow$

$\left(\dfrac{a_n}{a_{(n,m)}}, \dfrac{a_m}{a_{(n,m)}}\right) = 1 \qquad (\alpha\bar{\alpha}, (\alpha+\bar{\alpha})^d) \neq 1$

$\|$

$b_n \qquad b_0 = 0 \qquad b_1 = 1 \qquad (\alpha\bar{\alpha}, \alpha+\bar{\alpha}) \neq 1$ ASSURDO

$b_{n+2} = c b_{n+1} + e b_n.$

PER INDUZIONE: $(b_n, b_{n+1}) = 1$

$n = dx$

$m = dy$

$(x,y)=1$

$p \mid \left(\frac{a_n}{a_d}, \frac{a_m}{a_d}\right) \quad p \mid a_x$

$p \mid b_y \qquad p \mid b_{kx} \quad p \mid b_{jx} \ \forall j$

$kx+1 = jy$ ASSURDO!! $p \mid b_{kx} \quad \cancel{p} \mid b_{kx+1}$

$x_0 = 2 \qquad x_{n+1} = 2x_n^2 - 1$

$(n, x_n) = 1$

$$\cosh(\theta \cdot 2^n) = \frac{(e^\theta)^{2^n} + (e^\theta)^{-2^n}}{2}$$

$e^\theta = 2+\sqrt{3}$

$$x_n = \frac{(2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}}{2}$$

p DISP. $\quad p \mid x_n \qquad \left(\frac{3}{p}\right) = 1 \qquad p \mid x_n$

$\sqrt{3}$ ESISTE IN $\mathbb{Z}_p \qquad \Downarrow$

$a \quad \frac{1}{a} \quad 2^{n+2} \mid p-1$

$a^{2^n} \equiv -a^{-2^n} \qquad a^{2^{n+1}} \equiv -1$

$\left(\frac{3}{p}\right) = -1 \qquad \mathrm{ord}(a) = 2^{n+2}$

$$\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}_p\} = \mathbb{Z}_p[\sqrt{3}]$$

$$\left|\mathbb{Z}_p[\sqrt{3}] \setminus \{0\}\right| \mid p^2-1$$

$$p \mid \frac{(2+\sqrt{3})^{2^n}+(2-\sqrt{3})^{2^n}}{2}$$

$$(2+\sqrt{3})^{2^n} = -(2-\sqrt{3})^{2^n} \qquad \mathrm{ord}(2+\sqrt{3}) = 2^{n+2}$$

$$(2+\sqrt{3})^{2^{n+1}} = -1 \qquad 2^{n+2} \mid p^2-1$$

$$2^{n+1} \mid p-1 \ \vee\ 2^{n+1} \mid p+1$$

$2^n-1 \mid X_{n-2} \iff 2^n-1$ È PRIMO

Equazioni tipo Pell

$$\mathbb{Z}[\sqrt{d}] = \{ a + b\sqrt{d} : a \in \mathbb{Z}, b \in \mathbb{Z} \}$$

$z = a + b\sqrt{d}$ $\qquad \bar{z} = a - b\sqrt{d}$

$N(z) = a^2 - db^2 = z\bar{z}$ (moltiplicativa:

$\qquad N(z_1 z_2) = N(z_1) N(z_2)$)

$(x + \sqrt{d}\, y)(a + \sqrt{d}\, b) = 1$

$x^2 - dy^2 = 1$ $\qquad$ (d non quadrato)

$\exists$ una soluzione $z_0 = x_0 + y_0\sqrt{d}$ $\quad N(z_0) = 1$

con z_0 minima tra le soluzioni $N(z) = 1$

e $z > 1$, con la proprietà che ogni altra

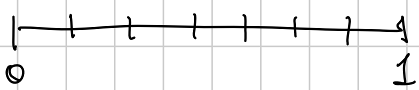
si scrive $\pm z_0^n$, $n \in \mathbb{Z}$

Teo (Dirichlet) $\forall\, \alpha$ irrazionale, $\exists$ infiniti

$p/q \in \mathbb{Q}$ t.c. $|\alpha - p/q| < 1/q^2$

Idea $\quad |\alpha - p/q| < \dfrac{1}{q(n+1)}$ $\qquad |\alpha q - p| < \dfrac{1}{n+1}$

$(q \le n)$ $\qquad 0, \{\alpha\}, \{2\alpha\}, \ldots, \{n\alpha\}, 1$



$$\left|\sqrt{d} - p/q\right| < \frac{1}{q^2}$$

$$p^2 - dq^2 = (p + q\sqrt{d})\underbrace{(p - q\sqrt{d})}_{} =$$

$$\leq q \cdot \frac{1}{q^2}(p + q\sqrt{d}) \leq (p/q + \sqrt{d}) \leq 2\sqrt{d} + 1$$

$\exists$ un $M \leq 2\sqrt{d}+1$ t.c.

$$x^2 - dy^2 = M \leftarrow$$

ha ∞ soluz.

(p, q) mod M ha M^2 possibilità

$p_1 \equiv p_2 \ (M)$, $q_1 \equiv q_2 (M)$, $p_i^2 - dq_i^2 = M$

$N(p_1 + \sqrt{d}\, q_1) = M$, $N(\ ---) = M$

$$\frac{p_1 + \sqrt{d}\, q_1}{p_2 + \sqrt{d}\, q_2} \cdot \frac{p_2 - \sqrt{d}\, q_2}{p_2 - \sqrt{d}\, q_2} = \frac{(p_1 p_2 - dq_1 q_2) + \sqrt{d}(q_1 p_2 - q_2 p_1)}{M}$$

$\circledast$ $q_1 p_2 \equiv q_2 p_1 \ (M)$

$\circledast$ $p_1 p_2 \equiv d q_1 q_2 \ (M) \iff M = p_1^2 - dq_1^2 \equiv 0 \ (M)$

$z_0 = \min\{z \text{ t.c. } N(z) = 1,\ z > 1\}$

Prendiamo una soluzione a $N(z) = 1$.

Osserviamo che $N(z \cdot z_0) = N(z)\, N(z_0) = 1 \cdot 1 = 1$

$z_0 = x_0 + y_0\sqrt{d} \longrightarrow \overline{z_0} = z_0^{-1}$

$$(x_0 + y_0\sqrt{d})(x_0 - y_0\sqrt{d}) = 1$$

$$1 \leq \underbrace{z \cdot z_0^{-k}}_{\text{Soluzione della Pell}} < z_0 \rightarrow \text{è } 1$$

$$z = z_0^k$$

$$z = \pm z_0^k$$

$$x^2 - dy^2 = m$$

Caso $m = -1$

Ha soluz. $\Longleftrightarrow$ z_0 è un quadrato in $\mathbb{Z}[\sqrt{d}]$.

Se $z_0 = z_1^2$, allora $N(z_1) = -1$

$$\begin{cases} (N(z_1))^2 = N(z_1^2) = N(z_0) = 1 \\ z_1 < z_0 \longrightarrow N(z_1) \neq 1 \end{cases}$$

Viceversa, se z_1 è t.c. $N(z_1) = -1$, allora $N(z_1^2) = 1$

Tutte le soluzioni: $z = \pm z_1 \cdot z_0^n \qquad k = n$

$$= \pm z_1^{2k+1}$$

Caso $x^2 - dy^2 = m$ generico

Esistono al più $\varphi(|m|)$ soluzioni,

$z_1, z_2, \dots, z_\ell$ con $\ell \leq \varphi(|m|)$

con la proprietà che z è soluzione prim. $\Leftrightarrow$

$$z = \pm z_k \cdot z_0^{\,n} \qquad k \in \{1, \dots, \ell\}, \quad n \in \mathbb{Z}$$

z si dice primitiva se $(z = x + \sqrt{d}\,y)$ si ha

$(x, y) = 1$

$$s(z = x + \sqrt{d}\,y) = x y^{-1} \pmod{m}$$

1) $s(z \cdot z_0^{\,n}) = s(z)$

$$z \cdot z_0^{\,n} = (x + y\sqrt{d})(a + b\sqrt{d}) \qquad N(a+b\sqrt{d}) = 1$$

$$= (ax + bdy) + \sqrt{d}\,(ay + bx) \qquad a^2 - b^2 d = 1$$

$$\frac{ax + bdy}{ay + bx} \cdot \frac{ax - bdy}{ax - bdy} = \qquad a^2 = 1 + db^2$$

$$= \frac{a^2x^2 - b^2d^2y^2}{a^2xy + abx^2 - abdy^2 - b^2dxy} = \frac{db^2(x^2 - dy^2) + x^2}{xy + Nab}$$

xy

$$= \frac{Ndb^2 + x^2}{Nab + xy} \equiv x/y \ (N)$$

Se $s(w_1) = s(w_2)$, $\frac{w_1}{w_2} \in \mathbb{Z}[\sqrt{d}]$

$$N\left(\frac{w_1}{w_2}\right) = \frac{N(w_1)}{N(w_2)} = 1 \longrightarrow w_2 = w_1 \cdot z_0^n$$

Remark Se $z \in \mathbb{Z}[\sqrt{d}]$, $N(z) = m$,

$$x = \frac{z+\bar{z}}{2}, \qquad y = \frac{z-\bar{z}}{2\sqrt{d}}$$

$z = z_0^n \longrightarrow x, y$ rispettano relaz. per ricorrenza

$$x_0 = 1, \quad y_0 = 0$$

$$x_{n+2} = (z_0 + \bar{z}_0)\, x_{n+1} - (z_0 \bar{z}_0)\, x_n$$

Bound sulle soluzioni

Se $x^2 - dy^2 = m$ ha una soluzione, allora ne ha una in cui $|x| \leq \frac{1+z_0}{2\sqrt{z_0}} \sqrt{|m|}$

Moltiplicando per z_0^n opportuno, troviamo una soluzione $\in \left[\sqrt{\frac{m}{z_0}}, \sqrt{m \cdot z_0}\right)$ che chiamo w

$$2|x| = |w + \overline{w}| = |w + m/w| \leq$$

$$\leq \max_{w \in \left[\sqrt{\frac{m}{z_0}}, \sqrt{m \cdot z_0}\right]} \left| w + \frac{m}{w} \right| \qquad (m>0)$$

$$= \sqrt{|m| \cdot z_0} + \sqrt{\frac{|m|}{z_0}} = \sqrt{|m|} \, \frac{z_0 + 1}{\sqrt{z_0}}$$

Trovare z_0 + successioni di Farey

FAREY

$$\mathcal{F}_n = \left\{ \frac{a}{b} : (a,b)=1,\ 0<b\leq n,\ 0\leq \frac{a}{b} \leq 1 \right\}$$

$$\frac{0}{1} \quad \frac{1}{1}$$

$$\frac{0}{1} \quad \frac{1}{2} \quad \frac{1}{1}$$

$$\frac{0}{1} \quad \frac{1}{3} \quad \frac{1}{2} \quad \frac{2}{3} \quad \frac{1}{1}$$

Algoritmo: * $\frac{n}{1} < \sqrt{D} < \frac{n+1}{1}$

* Ad ogni passo, se $\frac{a}{b} < \sqrt{D} < \frac{c}{d}$,

calcolate $\frac{a+c}{b+d}$.

- Se $x=(a+c)$, $y=(b+d)$ e' soluzione Pell → FINE
- Altrimenti, $\frac{a}{b} < \sqrt{D} < \frac{a+c}{b+d}$ o

$$\frac{a+c}{b+d} < \sqrt{D} < c/d$$

Lavoriamo in $\mathcal{F}_n$. Diciamo che $\frac{a}{b} < \frac{c}{d}$ siano consecutive. Allora

i) $b+d > n$ iii) $bc - ad = 1$

ii) $(a,c) = (b,d) = 1$

i) $\dfrac{a}{b} < \underbrace{\dfrac{a+c}{b+d}}_{\leq n} < \dfrac{c}{d}$ ASSURDO

ii) Segue da iii + Bézout

iii) Induzione su n. $\dfrac{a}{b} < \dfrac{c}{d}$ in $\mathcal{F}_n$

* o $\dfrac{a}{b}$, c/d restano consecutive in $\nearrow \mathcal{F}_{n+1}$
* o $\dfrac{a}{b} < \dfrac{M}{n+1} < c/d$

$$\frac{M}{n+1} - \frac{a}{b} = \frac{K_1}{b(n+1)}, \qquad \frac{c}{d} - \frac{M}{n+1} = \frac{K_2}{d(n+1)}$$

$$\frac{1}{bd} \stackrel{ii}{=} \frac{c}{d} - \frac{a}{b} = \frac{K_1 d + K_2 b}{bd(n+1)}$$

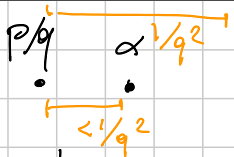
$$\underbrace{-b-d+n+1}_{\leq 0} = K_1 d + K_2 b - b - d$$

$$= d(K_1 - 1) + b(K_2 - 1) \longrightarrow K_1 = K_2 = 1$$

Teo (Hurwitz) α irraz.

$$\exists \infty \ p/q \ \text{ t.c. } \ |\alpha - p/q| < \frac{1}{\sqrt{5}\,q^2}$$

$\dfrac{a}{b} < \alpha < \dfrac{c}{d}$ una tra a/b, c/d, $\dfrac{a+c}{b+d}$ va bene nel Teo. Hurwitz



$$\alpha - p/q < 1/q^2$$

Esisterà a/b t.c. $\alpha > a/b > p/q$, e $b \leq q$?

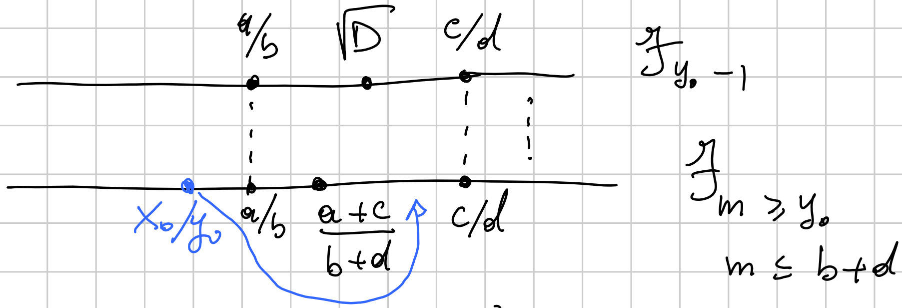
$$\frac{a}{b} - p/q \geq \frac{1}{bq} \geq 1/q^2$$

Se $x + y\sqrt{d}$ risolve la Pell, $x^2 - dy^2 = 1$

$$x/y > \sqrt{d}$$

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

Sia x_0, y_0 la più piccola soluz. Pell; x_0/y_0 starà in una $\mathcal{F}_n = \mathcal{F}_{y_0}$.



Sappiamo $\left|x_0/y_0 - \sqrt{D}\right| < \frac{1}{2y_0^2}$. Se $\frac{x_0}{y_0} \notin \left(\frac{a}{b}, \frac{c}{d}\right)$

succede che a/b è un'approx di $\sqrt{D}$ migliore di x_0/y_0 (IMPOSSIBILE, perché $b \leq y_0$)

$$\frac{c}{d} - \frac{a+c}{b+d} = \frac{cb + \cancel{cd} - ad - \cancel{cd}}{d(b+d)} = \frac{1}{d(b+d)}$$

Esempio $a^2 = 19n+1$ e $b^2 = 95n+1$ sono quadrati

$b^2 = 5a^2 - 4$ $\qquad$ $b^2 - 5a^2 = -4$

$\varphi(|4|) = 2$ $\qquad$ $b \equiv a \ (4)$

$b \equiv 3a \ (4)$

$(1 + \sqrt{5} \cdot 1)(1 - \sqrt{5} \cdot 1) = -4$

$(11 + 5\sqrt{5})(11 - 5\sqrt{5}) = -4$

Mancano: $*$ non primitive $\qquad$ $x^2 - 5y^2 = -1$

$*$ z_0 $\qquad$ $x^2 - 5y^2 = 1$ $\qquad$ $\frac{2}{1} < \sqrt{5} < \frac{3}{1}$

$\frac{2}{1} < \sqrt{5} < \frac{5}{2}$ $\qquad$ $7/3 > \sqrt{5}$

$\frac{2}{1} < \sqrt{5} < 7/3$ $\qquad$ $9/4$

Non primitive: $(2+\sqrt{5})^{2k+1}$

$(1+\sqrt{5})(9+4\sqrt{5})^k$, $\qquad$ $(11+5\sqrt{5})(9+4\sqrt{5})^k$

$(2+\sqrt{5})^{2k+1}$ $\qquad$ $\varphi^2 = \varphi + 1$

$(1+\sqrt{5})^2 = 6 + 2\sqrt{5}$

$(1+\sqrt{5})^3 = 16 + 8\sqrt{5} = 8(2+\sqrt{5})$

$(2+\sqrt{5})^2 = 9 + 4\sqrt{5} = \left(\frac{1+\sqrt{5}}{2}\right)^6$

$$(1+\sqrt{5})^5 = 16\,(3+\sqrt{5})(2+\sqrt{5}) = 16\,(11+5\sqrt{5})$$

$$11+5\sqrt{5} = 2\left(\frac{1+\sqrt{5}}{2}\right)^5$$

$$z = 2\left(\frac{1+\sqrt{5}}{2}\right)^{2k+1}$$

$$y = \frac{\cancel{2}\left(\frac{1+\sqrt{5}}{2}\right)^{2k+1} - \cancel{2}\left(\frac{1-\sqrt{5}}{2}\right)^{2k+1}}{\cancel{2}\sqrt{5}} = F_{2k+1}$$

$$F_{2k+1}^2 - 1 \equiv 0 \ (19) \qquad \left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = 1$$

<u>Es</u> $3^n - 2 = X^2$ $\qquad$ X dispari $\to$ n dispari

$$3y^2 - 2 = X^2$$

$$X^2 - 3y^2 = -2 \qquad (1+\sqrt{3})$$

$$X^2 - 3y^2 = 1 \qquad (2+\sqrt{3})$$

$$y_n = \frac{(1+\sqrt{3})(2+\sqrt{3})^n - (1-\sqrt{3})(2-\sqrt{3})^n}{2\sqrt{3}} = (\star)$$

$$(1+\sqrt{3})^2 = 4+2\sqrt{3} = 2(2+\sqrt{3})$$

$$(\star)\quad \frac{(1+\sqrt{3})^{2n+1} - (1-\sqrt{3})^{2n+1}}{2^{n+1}\sqrt{3}}$$

$$9 \mid y_n \iff n \equiv 4 \ (9)$$

$$y_4 = 153 = 9 \cdot 17$$

$$b_{2n+1} = 2^n y_n = \frac{(1+\sqrt{3})^{2n+1} - (1-\sqrt{3})^{2n+1}}{2\sqrt{3}}$$

$$(b_{2n+1}, b_9) = b_{(9,2n+1)} = b_9 \equiv 0 \ (17)$$

$$17 \mid 2^n y_n \qquad 17 \mid y_n$$