Stage Senior 2013 – Livello Advanced

Stampato integrale delle lezioni

Autori vari

Indice

SENIOR 2013 – ALGEBRA (Advanced

Titolo nota 06/09/2013

Funzioni convesse

Insiemi convessi: I è convesso se per ogni $P \in I$ e $Q \in I$ si ha che segmento PQ è tutto contenuto in $I \subseteq \mathbb{R}^n$.

$n=1$ Gli insiemi convessi sono: – intervalli } con o
– semirette } senza bordo
– tutto $\mathbb{R}$

$n>1$: ce ne sono di più.

$I \subseteq \mathbb{R}^n$ convesso $f: I \to \mathbb{R}$ è convessa se

$$f(\underbrace{\lambda P + (1-\lambda)Q}_{\in I \text{ perché } I \text{ è convesso}}) \leq \lambda f(P) + (1-\lambda) f(Q)$$

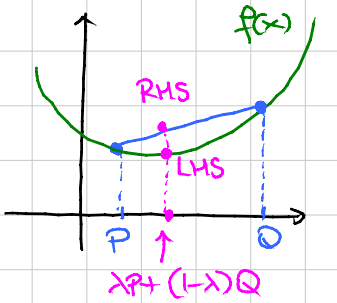
$\forall P \in I, \forall Q \in I, \forall \lambda \in [0,1]$

Oss. $\lambda P + (1-\lambda)Q$ al variare di $\lambda \in [0,1]$ è il segm. PQ

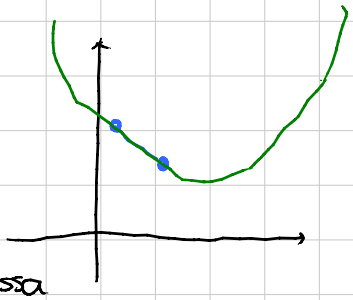
Quando vale il segno di $=$? ① $\lambda = 0$
② $\lambda = 1$
③ $P = Q$ e $\lambda \in [0,1]$

Se non ci sono altri casi di $=$, f si dice strett. convessa.

$n=1$ $f(x)$ è convessa $\Leftrightarrow$ il grafico sta sotto i segmenti secanti



Una funzione è convessa, ma non strett. convessa $\Leftrightarrow$ il grafico ha tratti "RETTILINEI"



Def. f è CONCAVA se
$LHS \geq RHS$
oppure (è lo stesso) se $-f$ è convessa

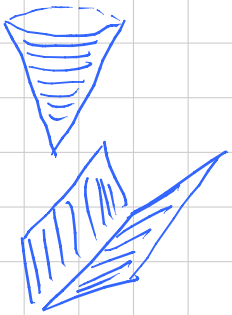
Oss. f è convessa $\Leftrightarrow$ sopragrafico è convesso come insieme di $\mathbb{R}^2$ (in gen. $\mathbb{R}^{n+1}$)

Esempi in $\mathbb{R}^2$

① $f(x)$ = distanza (x, P)
punto ↑ fissato ↑

② $f(x)$ = distanza (x, r)
retta ↑

③ $f(x) = [\text{distanza}\ (x,P)]^2$.



Oss. Sottolivello di una funzione
$\{x \in I : f(x) \leq R\} = S_R$
fissato ↑

Se f è convessa, tutti i sottolivelli sono convessi

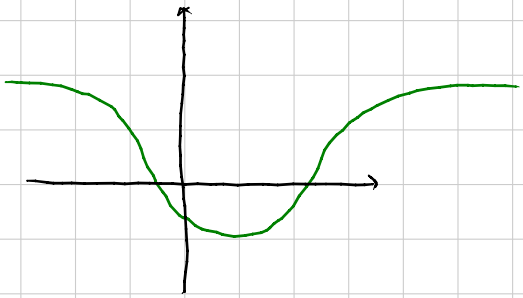
Dim. $P \in S_R \quad Q \in S_R \quad \lambda \in [0,1] \quad \lambda P + (1-\lambda)Q \in S_R$

$$f(\lambda P + (1-\lambda)Q) \leq \lambda f(P) + (1-\lambda) f(Q) = R$$

conv. $\leq R$ $\leq R$

Vale il viceversa? NO!!

Ogni funzione monotona ha i sottolivelli convessi !!



Nemmeno se i sottolivelli sono intervalli !!

$n=1$ f convessa $f(x)=0$

Se è strett. convessa, ne ha al max 2

Dim. Se ne avesse 3, prendo $a<b<c$ e in b deve stare sotto la congiungente.

Domanda: $f(x) = g(x)$ con f e g convesse

Può avere ∞ soluzioni con i grafici che si attraversano ∞ volte:

$f(x) = x^2$

$f'(x) = 2x$

$f''(x) = 2$

$g(x) = x^2 + \sin x$

$g'(x) = 2x + \cos x$

$g''(x) = 2 - \sin x \geq 1$

DISUGUAGLIANZA DI JENSEN

$I \subseteq \mathbb{R}$ convesso $\quad f: I \to \mathbb{R}$ convessa. Allora

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

combinazione convessa di $x_1, \dots, x_n$

$$\forall\, (x_1, \dots, x_n) \in I^n \qquad \lambda_i \geq 0 \qquad \lambda_1 + \dots + \lambda_n = 1$$

Dim. Induzione UP–DOWN

$n = 2$ Definizione

$n \Rightarrow 2n$ $\rightsquigarrow$ vero per 2^k

$n+1 \Rightarrow n$ $\rightsquigarrow$ completo

$n \Rightarrow 2n$

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

$\Lambda_1 = \lambda_1 + \dots + \lambda_n \qquad \Lambda_2 = \lambda_{n+1} + \dots + \lambda_{2n}$

$$= f\left(\Lambda_1 \underbrace{\left(\frac{\lambda_1 x_1 + \dots + \lambda_n x_n}{\Lambda_1}\right)}_{P} + \Lambda_2 \underbrace{\left(\frac{\dots}{\Lambda_2}\right)}_{Q}\right)$$

$$\leq \Lambda_1 f(P) + \Lambda_2 f(Q)$$

$$= \Lambda_1 f\left(\frac{\lambda_1}{\Lambda_1} x_1 + \dots + \frac{\lambda_n}{\Lambda_1} x_n\right) + \Lambda_2 f(\dots)$$

$$\leq \Lambda_1 \left(\frac{\lambda_1}{\Lambda_1} f(x_1) + \dots + \frac{\lambda_n}{\Lambda_1} f(x_n)\right) + \dots$$

↑ Ip induttiva

$n+1 \Rightarrow n$ Introduco un pto x_{n+1} con coeff. $\lambda_{n+1} = 0$.

SL – IMO 98 – A2

$x_1 \geq 1, \dots, x_n \geq 1 \Rightarrow$

$$\frac{1}{x_1+1} + \frac{1}{x_2+1} + \dots + \frac{1}{x_n+1} \geq \frac{n}{\sqrt[n]{x_1 \cdots x_n} + 1}$$

Dim. 1 Induzione UP–DOWN

$n=2$ $\quad \frac{1}{x^2+1} + \frac{1}{y^2+1} \geq \frac{2}{xy+1}$

$$(x^2+y^2+2)(xy+1) \geq 2(x^2+1)(y^2+1)$$

$$xy(x^2+y^2) + x^2 + y^2 + 2xy + 2 \geq 2x^2y^2 + 2x^2 + 2y^2 + 2$$

$$xy(x-y)^2 \overset{?}{\geq} (x-y)^2 \quad \text{Ok perché } x \geq 1 \text{ e } y \geq 1$$

$n \Rightarrow 2n$ Facile!

$n+1 \Rightarrow n$ Sono dati $x_1, \dots, x_n$ e introduco

$$x_{n+1} = \sqrt[n]{x_1 \cdots x_n} = G$$

$$\frac{1}{x_1+1} + \dots + \frac{1}{x_n+1} + \boxed{\frac{1}{G+1}} \geq \frac{n+1}{\sqrt[n+1]{x_1 \cdots x_n \cdot G} + 1}$$

$x_1 \cdots x_n \cdot G = G^n$

per ipotesi è vera per $n+1$

$$= \frac{n+1}{G+1}$$

$\Rightarrow$ Tesi $\quad \square$

Dim. 2 Provo con JENSEN direttamente.

Pongo $f(x) = \dfrac{1}{e^x+1}$

Pongo $y_1 = \log x_1, \dots, y_n = \log x_n$

Se per caso $f(x)$ fosse convessa ...

$$\frac{1}{n}\left[f(y_1)+\dots+f(y_n)\right] \geq f\left(\frac{y_1+\dots+y_n}{n}\right)$$

$$\frac{1}{n}\,\text{RHS} = \frac{1}{e^{\log \sqrt[n]{x_1\cdots x_n}}+1} \quad \text{cioè la tesi}$$

$$\frac{1}{n}(y_1+\dots+y_n) = \frac{1}{n}[\log(x_1)+\dots+\log x_n] = \log\sqrt[n]{x_1\cdots x_n}$$

$$f(x) = \frac{1}{e^x+1} \qquad f'(x) = -\frac{e^x}{(e^x+1)^2}$$

$$f''(x) = -\frac{e^x(e^x+1)^2 - 2(e^x+1)e^{2x}}{(e^x+1)^4} = -\frac{-e^{2x}+e^x}{(e^x+1)^3}$$

$$= \frac{e^x(e^x-1)}{(e^x+1)^3} \geq 0 \quad \text{per } x \geq 0$$

L'ho usata con $y_i = \log x_i$ poiché $x_i \geq 1$ ho che $y_i \geq 0$, quindi nella zona di convessità

DISUGUAGLIANZA DI KARAMATA (HARDY ?)

f convessa

$$f(x_1) + \dots + f(x_n) \geq f(y_1) + \dots + f(y_m)$$

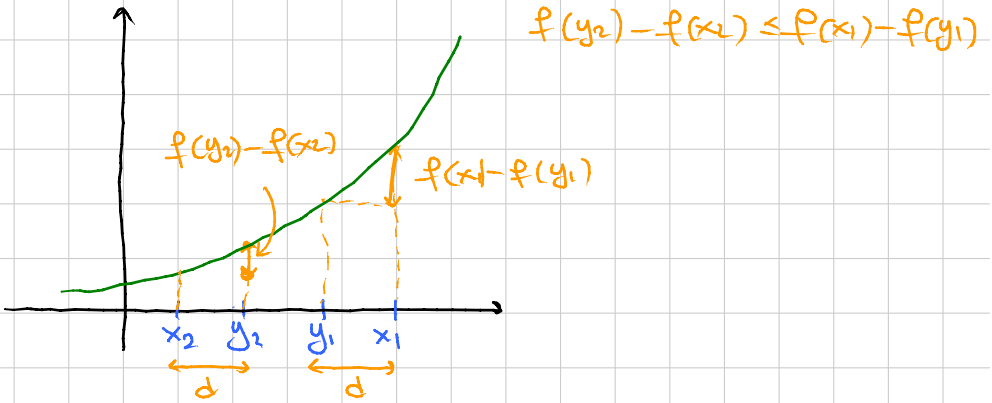
$\{x_i\} \succ \{y_i\}$

$$x_1 \geq x_2 \geq \dots \geq x_n$$
$$y_1 \geq y_2 \geq \dots \geq y_m$$
$$x_1 \geq y_1$$
$$x_1 + x_2 \geq y_1 + y_2$$
$$\vdots$$
$$x_1 + \dots + x_{n-1} \geq y_1 + \dots + y_{m-1}$$
$$x_1 + \dots + x_n = y_1 + \dots + y_m$$

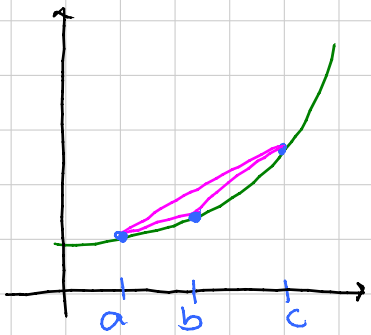
Caso banale $y_1 = y_2 = \dots = y_m = \dfrac{x_1 + \dots + x_n}{n}$

Ottengo Jensen: $\dfrac{1}{n}\left[f(x_1) + \dots + f(x_n)\right] \geq f\left(\dfrac{x_1 + \dots + x_n}{n}\right)$

Caso $n=2$ $x_1 + x_2 = y_1 + y_2 = S$



Lemma 1 (Lemma dei 3 rapporti incrementali)



f convessa
$a < b < c$

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

Dim: scrivo b come comb. convessa di a e c

$$b = \lambda a + (1-\lambda)c \qquad \lambda = \frac{b-c}{a-c}$$

Scrivo Def.: $f(b) \leq \lambda f(a) + (1-\lambda) f(c)$
$= \lambda [f(a) - f(c)] + f(c)$

$f(b) - f(c) \leq \lambda [f(a) - f(c)]$ sostituisco λ e divido e ne ottengo una...

DIM. KARAMATA

$$\sum_{i=1}^{n} f(x_i)-f(y_i) = \sum_{i=1}^{n} \frac{f(x_i)-f(y_i)}{x_i-y_i}(x_i-y_i)$$

$$= \sum_{i=1}^{n} R_i\,(x_i-y_i)$$

$A_i = x_1+\dots+x_i$
$B_i = y_1+\dots+y_i$

$$= \sum_{i=1}^{n} R_i\,(A_i-A_{i-1}-B_i+B_{i-1})$$

$$= \sum_{i=1}^{n} R_i\,(A_i-B_i) - \sum_{i=1}^{n} R_i\,(A_{i-1}-B_{i-1})$$

$$= R_n\,(A_n-B_n) + \sum_{i=1}^{n-1} R_i\,(A_i-B_i) - \sum_{i=1}^{n-1} R_{i+1}\,(A_i-B_i) - R_1\,(A_0-B_0)$$

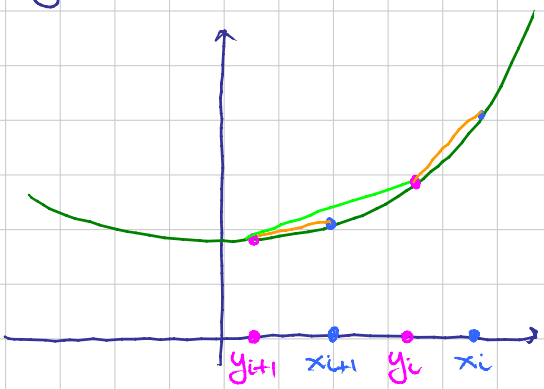
$$= R_n\,(A_n-B_n) - R_1\,(A_0-B_0) + \sum_{i=1}^{n-1} (R_i-R_{i+1})(A_i-B_i) \geq 0$$

$A_n = 0$, $B_0 = 0$; $R_i - R_{i+1} \geq 0$ Hope; $A_i - B_i \geq 0$

Hope: $R_i \geq R_{i+1}$ cioè

$$\frac{f(x_i)-f(y_i)}{x_i-y_i} \geq \frac{f(x_{i+1})-f(y_{i+1})}{x_{i+1}-y_{i+1}}$$

$R(y_{i+1}, x_{i+1}) \leq$
$R(y_{i+1}, y_i) \leq$
$R(y_i, x_i)$



Occhio: potrebbe essere che $y_i \geq x_i$: funziona ancora, ma bisogna cambiare il termine intermedio.

Oss. Se f è convessa e CRESCENTE, allora si può assumere $A_m \geq B_m$ invece di $A_m = B_m$

... tutto si riconduce a controllare $R_m(A_m - B_m)$

—o—o—

Caso speciale **POPOVICIU** f convessa

$$f(a)+f(b)+f(c)+f\left(\frac{a+b+c}{3}\right) \geq \frac{4}{3}\left[f\left(\frac{a+b}{2}\right)+f\left(\frac{b+c}{2}\right)+f\left(\frac{c+a}{2}\right)\right]$$

FORTI DEBOLE MEDI

Dim. Karamata con

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

$\frac{a+b}{2}, \frac{a+b}{2}, \frac{a+b}{2}, \frac{a+b}{2}$ e 4 volte gli altri

Si tratta di verificare le ipotesi: WLOG $a \geq b \geq c$

si distinguono i casi a seconda di Media $\geq b$ o Media $\leq b$

e si verificano le ipotesi con pazienza.

—o—o—

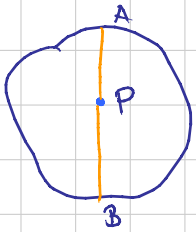
PUNTI ESTREMALI DI UN CONVESSO

I convesso in $\mathbb{R}^m$ P è estremale se non esistono segmenti in I per cui P è p.to interno.

Esempi Gli estremali di un cerchio sono la circonf.

Gli estremali di un poligono sono solo i vertici. □

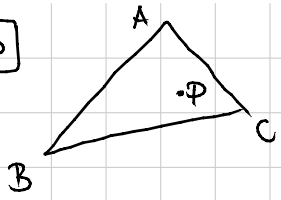
FATTO Per una funzione convessa il massimo viene assunto (anche) in uno dei pti estremali.



Dim semplice:
non può essere
$f(P) > f(A)$
$f(P) > f(B)$

FATTO 2 Se una funzione convessa assume max in un pto P non estremale, allora ha lo stesso valore costante su tutti i segmenti che contengono P come pto interno.

TST 2005
ITA



$f(P)$ = somma distanze dai lati
P interno o sul bordo

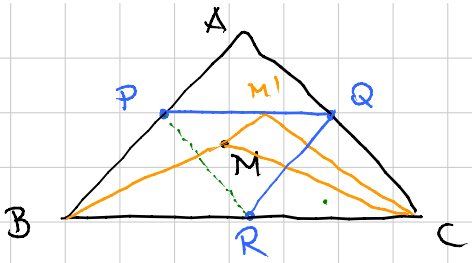
Max / min di $f(P)$

su tutto il piano

Dim.: è somma 3 funzioni convesse ⇒ max nei vertici
⇒ max = altezza + lunga

All'interno del triangolo è somma di 3 concave ⇒
minimo nei vertici ⇒ min = altezza + corta

IMO SL – 1999 – G1



$$\min\{MA, MB, MC\} + MA + MB + MC < AB + BC + CA$$

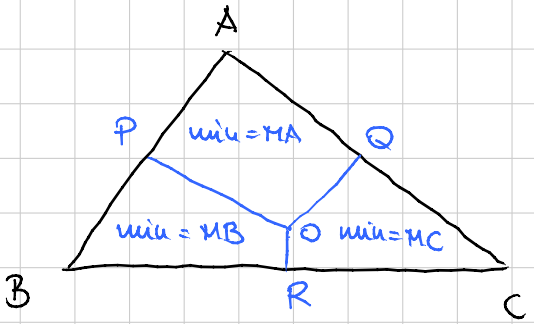
$$BM + MC < BP + PQ + QC = \frac{1}{2}(AB + BC + CA)$$
$$BM + MA < BR + RQ + QA = \frac{1}{2}(AB + BC + CA)$$

$$2BM + MC + MA < AB + BC + CA$$

A seconda della posiz. di M posso scrivere 2 o 3 di queste !!!

WLOG siamo in zona MA
Allora devo cercare il
Max di

$$2MA + MB + MC$$



È somma di 4 distanze,
quindi convessa, quindi max nei pti estremali!
controllo solo A, P, O, Q ↑ come P

Banale in A

Controllo in P $\quad \frac{3}{2}c + m_c < a+b+c$

$$2m_c < 2a+2b-c$$

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

$$2a^2+2b^2-c^2 < a^2+b^2+2c^2+2ab-2ac-2bc$$

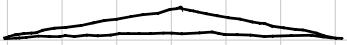
$$a^2+b^2+2ab+c^2 \geq 2ac+2bc$$

$$a^2+b^2+2ab+c^2 = (a+b)^2+c^2 \geq 2c(a+b).$$

Controllo in O $\quad 4R < a+b+c$

$$= 2R(\sin\alpha+\sin\beta+\sin\gamma)$$

$$\sin\alpha+\sin\beta+\sin\gamma > 2$$

NO!  viene circa O !!!

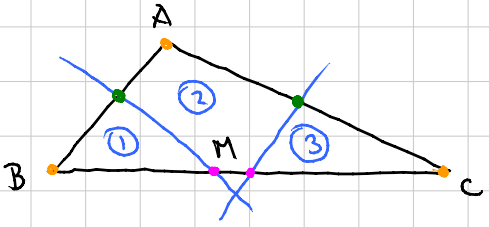
Questa ci serve solo sugli acutangoli

KARAMATA $\quad \sin x$ è concava in $[0, \frac{\pi}{2}]$

$$\left\{\frac{\pi}{2}, \frac{\pi}{2}, 0\right\} > \{\alpha, \beta, \gamma\} \qquad \text{WLOG } \alpha \geq \beta \geq \gamma$$

$$f\left(\frac{\pi}{2}\right)+f\left(\frac{\pi}{2}\right)+f(0) \leq f(\alpha)+f(\beta)+f(\gamma)$$

$MA+MB+MC+MA$
$= 3MB+MC$ OK



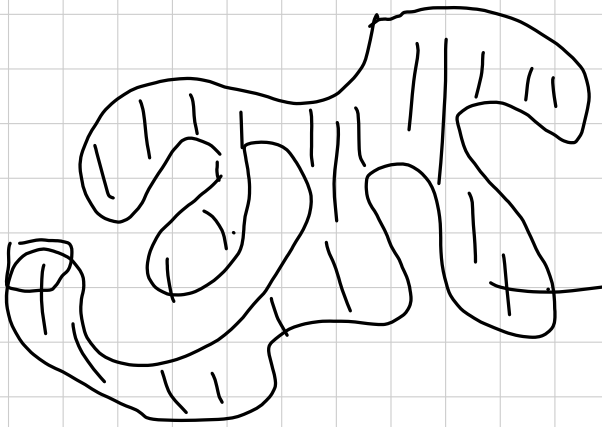
Titolo nota 03/09/2013

$2n+1$ interi distinti:

$\Sigma_{n+1} > \Sigma_n \longrightarrow$

i) each $> n^2$

ii) find all configurations where sum $= n^2+1$.



(Arc ≤ 1).

$P_1 \cup P_2 \cup \dots \cup P_J$

$1 \geq \mu\left(\bigcup_{i=1}^{J} P_i\right) \geq \sum_{i=1}^{J} \mu(P_i) - \sum_{i<j} \mu(P_i \cap P_j)$

$\sum_{i<j} \mu(P_i \cap P_j) \geq \frac{3}{2}$ (10) $\frac{J}{2}$

$\longrightarrow \mu\left(P_i \cap P_j\right) \geq \frac{3}{20}$

α_k = measure set of points which are covered by exactly k packets.

α_0, α_1

$1 = \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5$ | a

$\frac{5}{2} = \sum_{i=1}^{5} \mu(P_i) = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5$ | b

$? = \sum_{i<j} \mu(P_i \cap P_j) = \alpha_2 + 3\alpha_3 + 6\alpha_4 + 10\alpha_5 \Leftarrow$ (10)

$\begin{cases} a + 2b = 1 \\ a + 3b = 3 \end{cases} \rightarrow \begin{cases} b = 2 \\ a = -3 \end{cases}$

$-3(I) + 2(II) : (2) = -3\alpha_0 - \alpha_1 + \alpha_2 + 3\alpha_3 + 6\alpha_4 + 10\alpha_5 + 5\alpha_4 + 7\alpha_5 = -\alpha_2 - 3\alpha_5 =$

$= \sum_{i<j} \mu(P_i \cap P_j) - (3\alpha_0 + \alpha_1 + \alpha_2 + 3\alpha_5) \leq$

$\leq \sum_{i<j} \mu(P_i \cap P_j) \rightarrow \exists\, \mu(P_i \cap P_j) \geq \frac{2}{10} = \frac{1}{5}.$

~~5~~ 6 factors.

COVERINGS & PACKINGS.

DESIGN THEORY.

(v, b, k, r, λ) — BIB ($\mathcal{D}$)

balanced — block

incomplete

v elements

b varieties

subset = block. Each block has k elements

Each of the v belongs to r blocks.

Each pair — λ —.

1. $v \cdot r = bk$
2. $\lambda \cdot \frac{v(v-1)}{2} = b\frac{k(k-1)}{2}$

‖ Necessary Condition

Fisher's Inequality: $b \geq v$

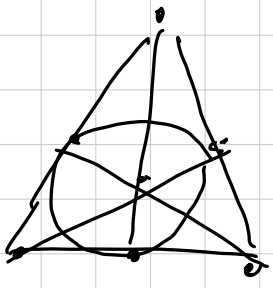
$b = v$ — BIB symmetric. (v, r, λ)

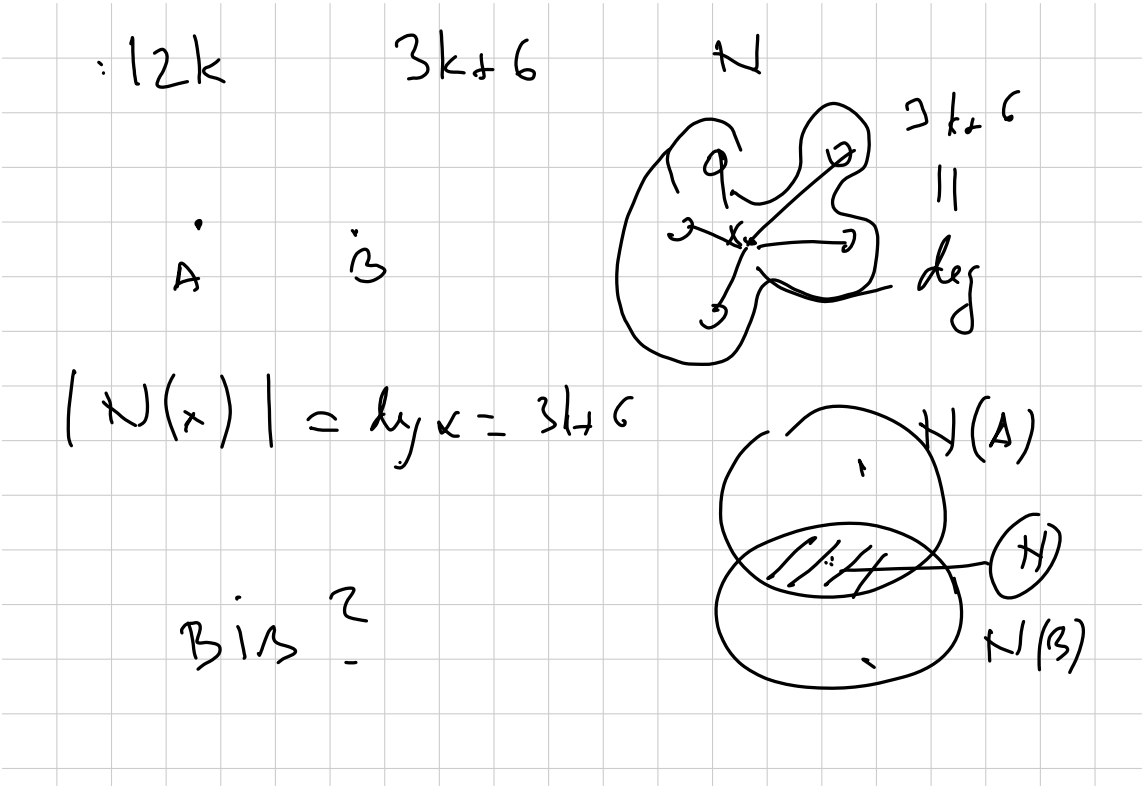
Ryser–Brooke–Chowla Theorem

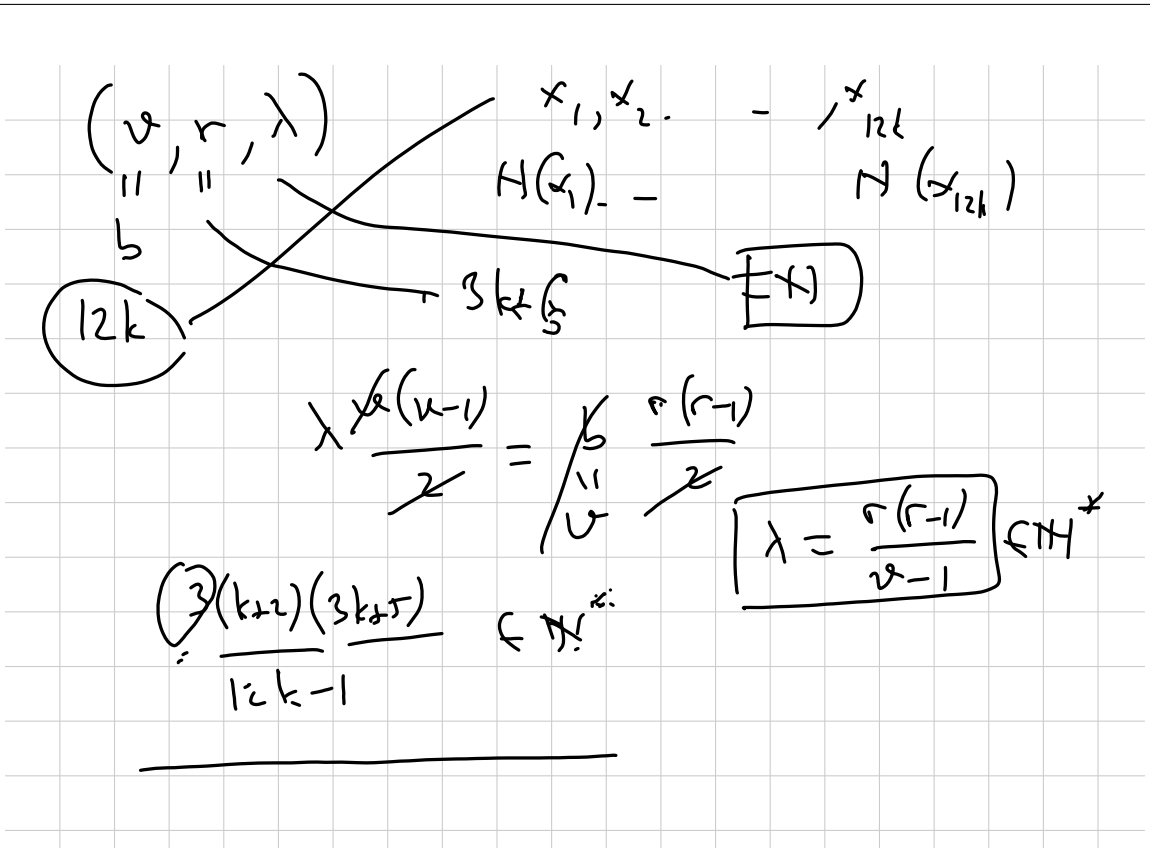
$\lambda = 1$. $\begin{cases} v = \xi^2 + \xi + 1 \\ r = \xi + 1 \end{cases}$

$\xi = p^\alpha$, p prime.

FANO




: 12k
3k+6
N
A
B
3k+6
=
deg
|N(x)| = deg x = 3k+6
N(A)
N
N(B)
Bis ?


(v, r, λ)
= =
b
12k
x1, x2 . . . x12k
N(x1) . . .
N(x12k)
3k+5
∈ N
λ v(v-1)/2 = b r(r-1)/2
v
λ = r(r-1)/(v-1) ∈ N*
3(k+2)(3k+5)/(12k-1) ∈ N!

$12k-1 \mid 3k^2+11k+10$

$(12k^2+4k+4k+4) - k + k$

$\longrightarrow 45k+40$

$180k + 160 - 15 + 15 = 175 = 5^2 \cdot 7$

$12k-1 \in \{1, 5, 7, 25, 35, 175\}$

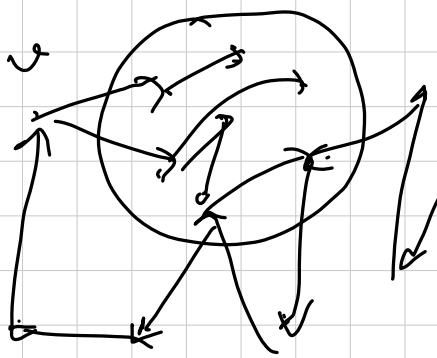
$12k \in \{2, 6, 8, 26, 36, 176\} \longrightarrow k = 3$

$(\lambda = N = 6)$

$(36, 15, 6)$ Bis ∎

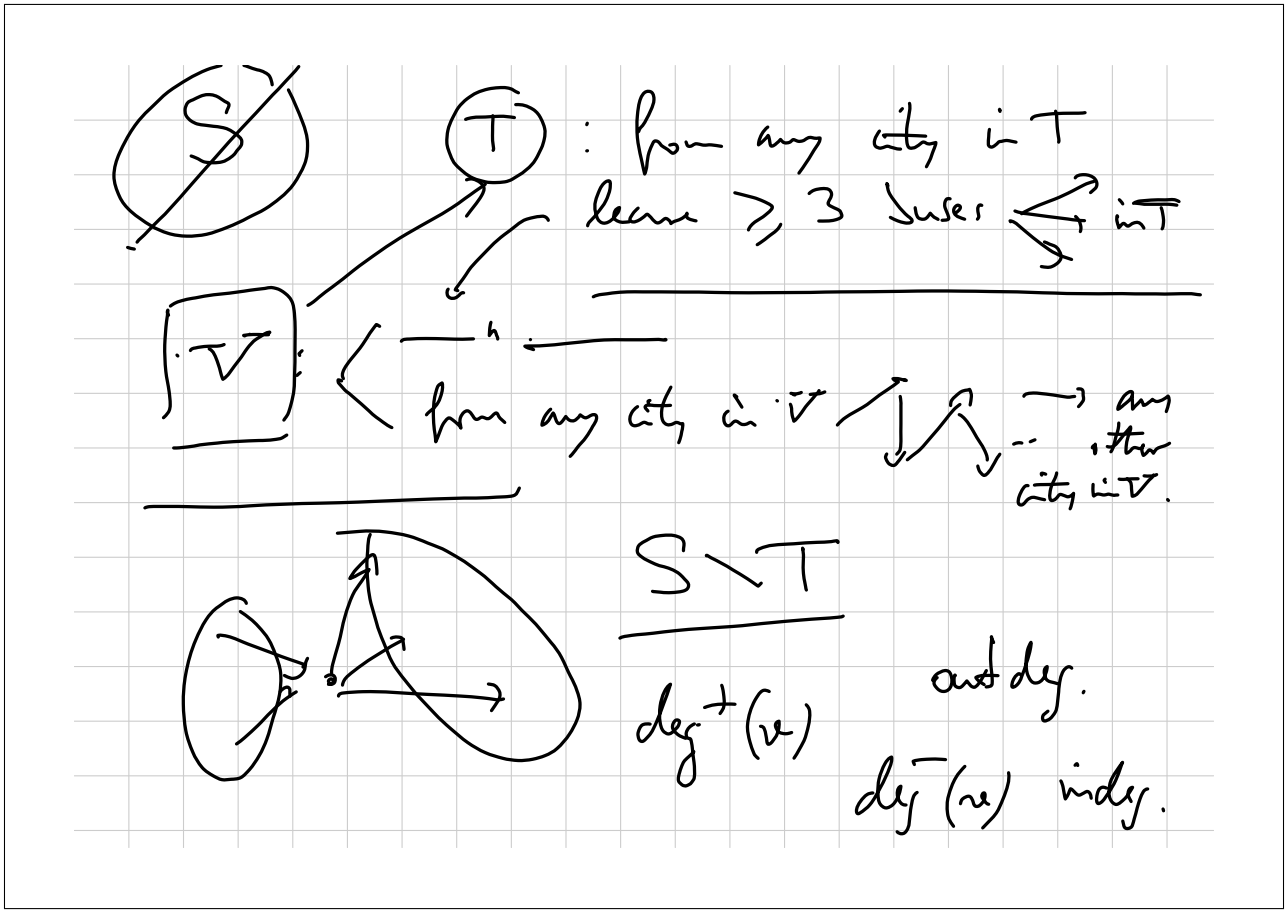
Digraph:

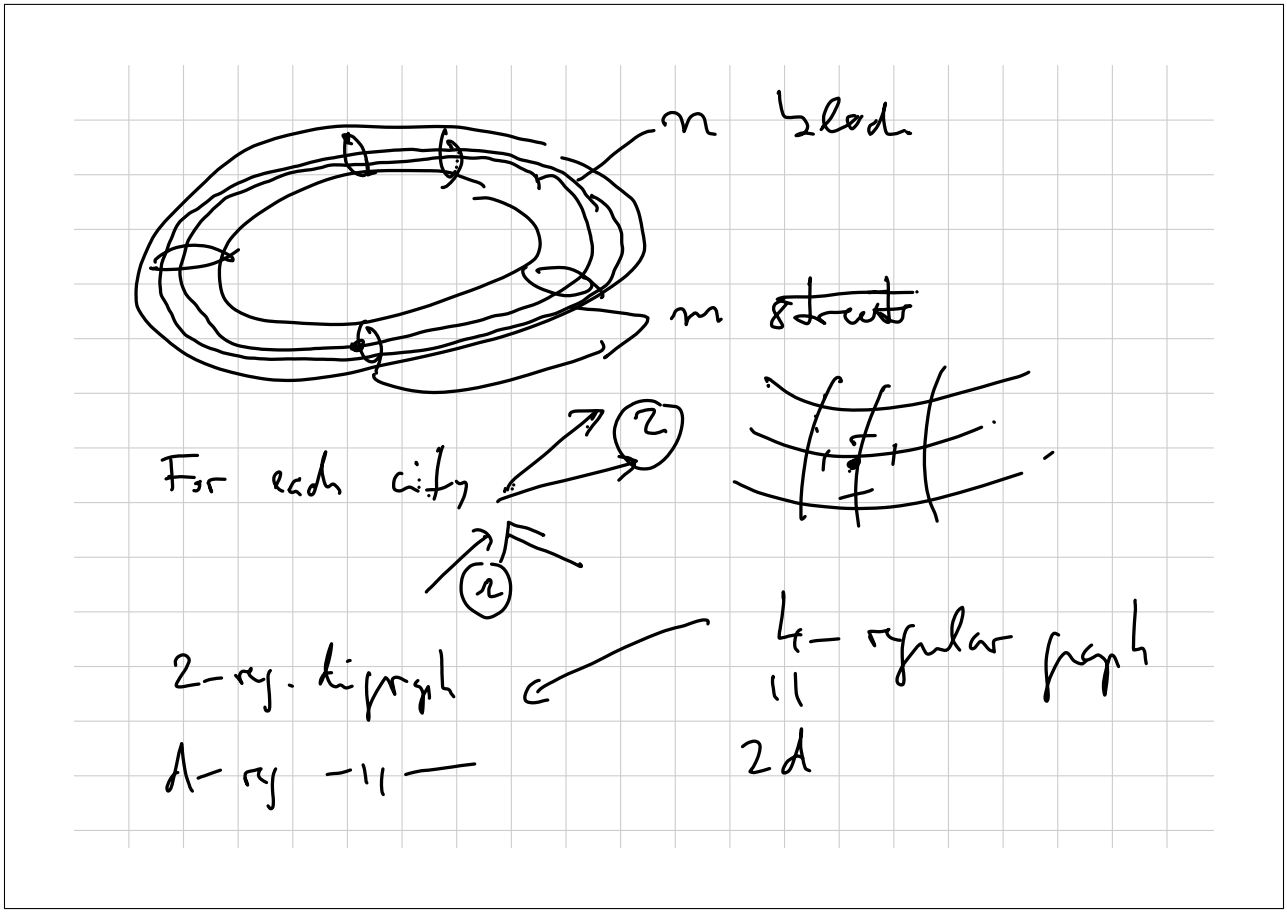
$C_v = \{$ cities w that can be reached from v $\}$

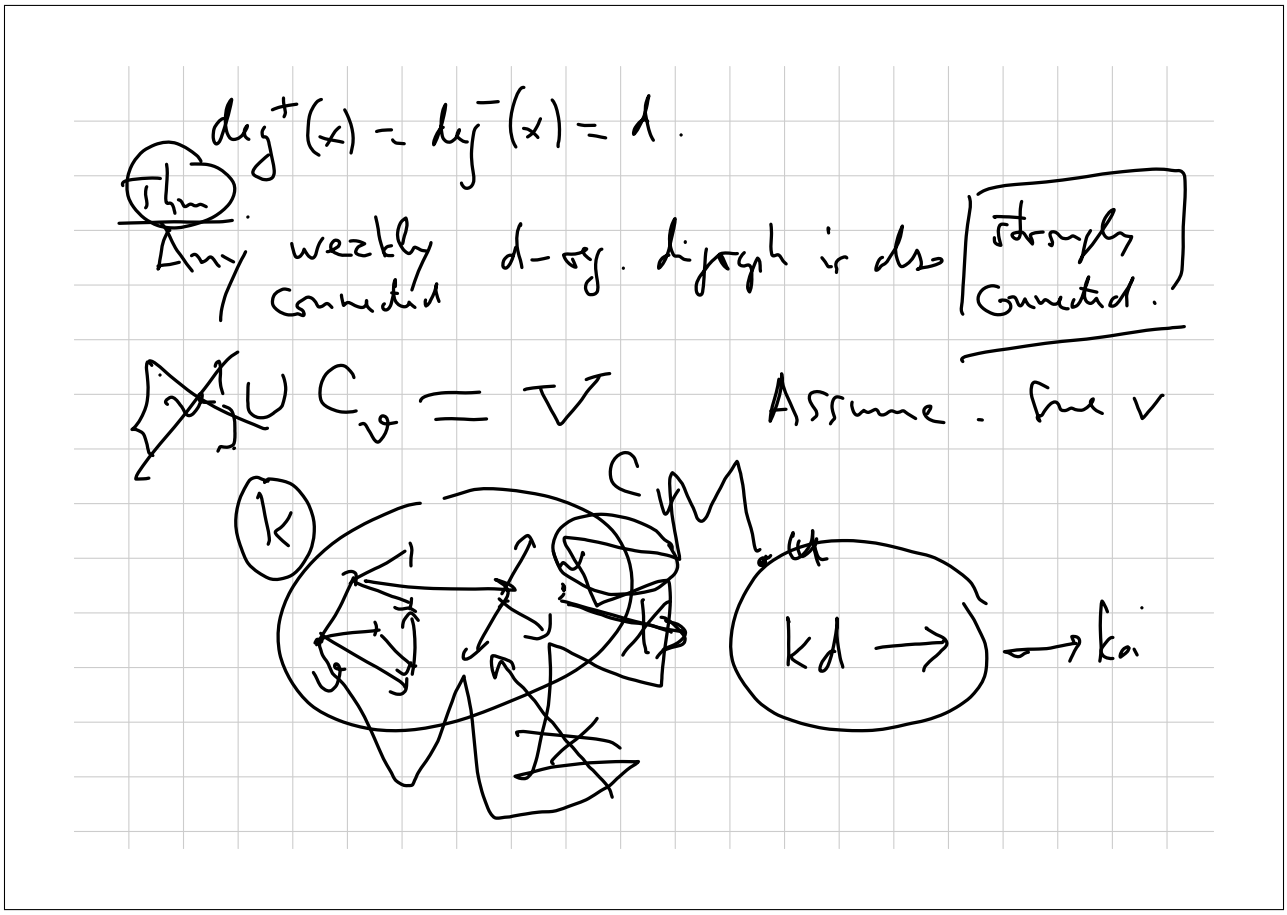


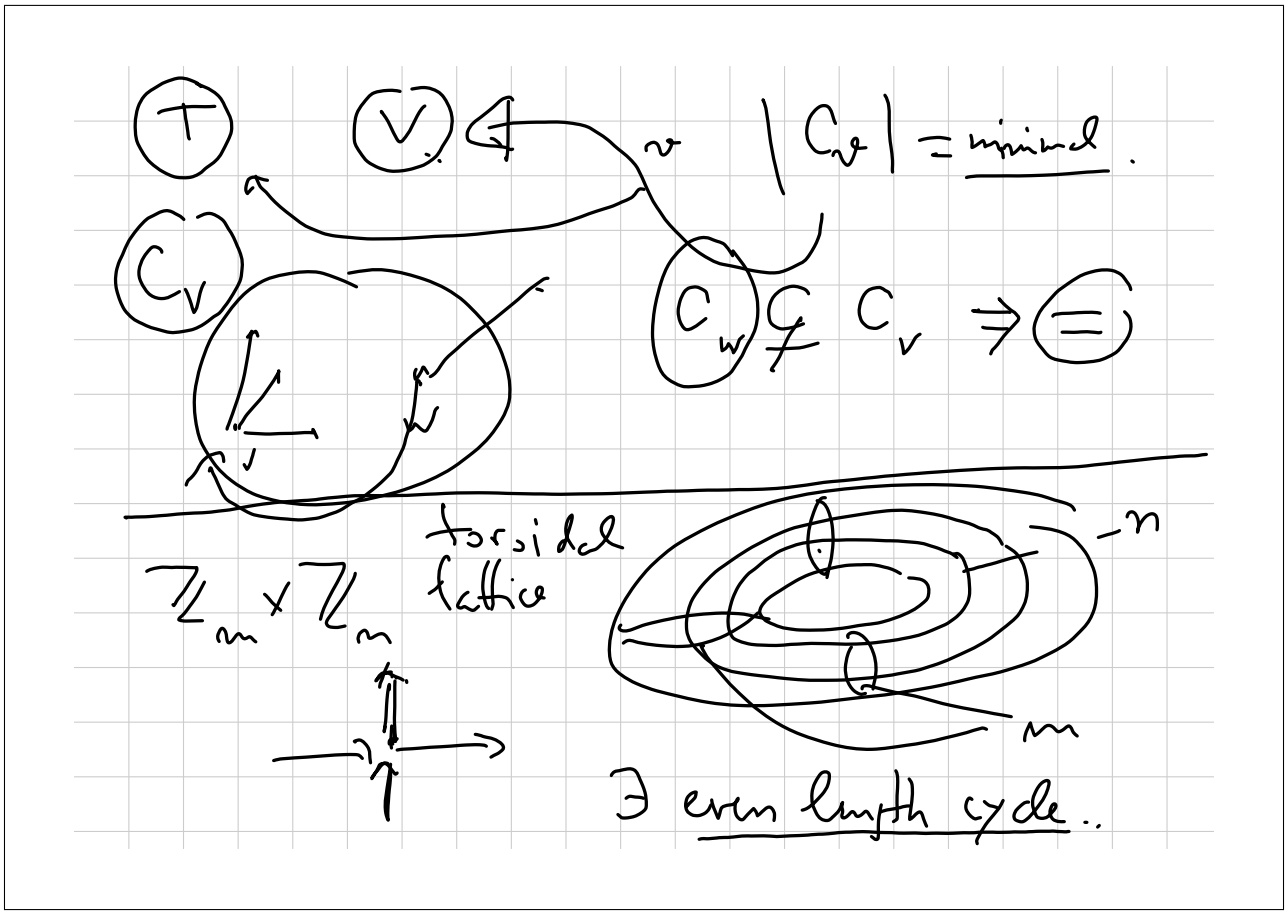
$C_u \supseteq C_v$

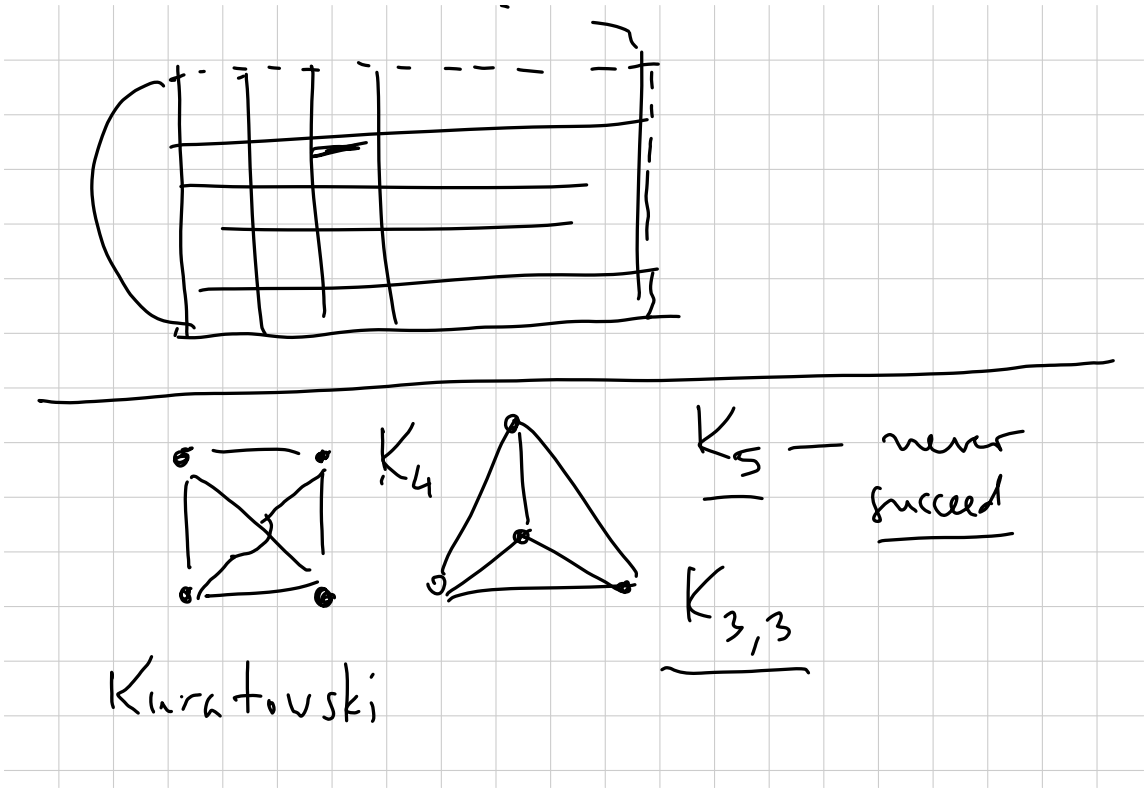
□

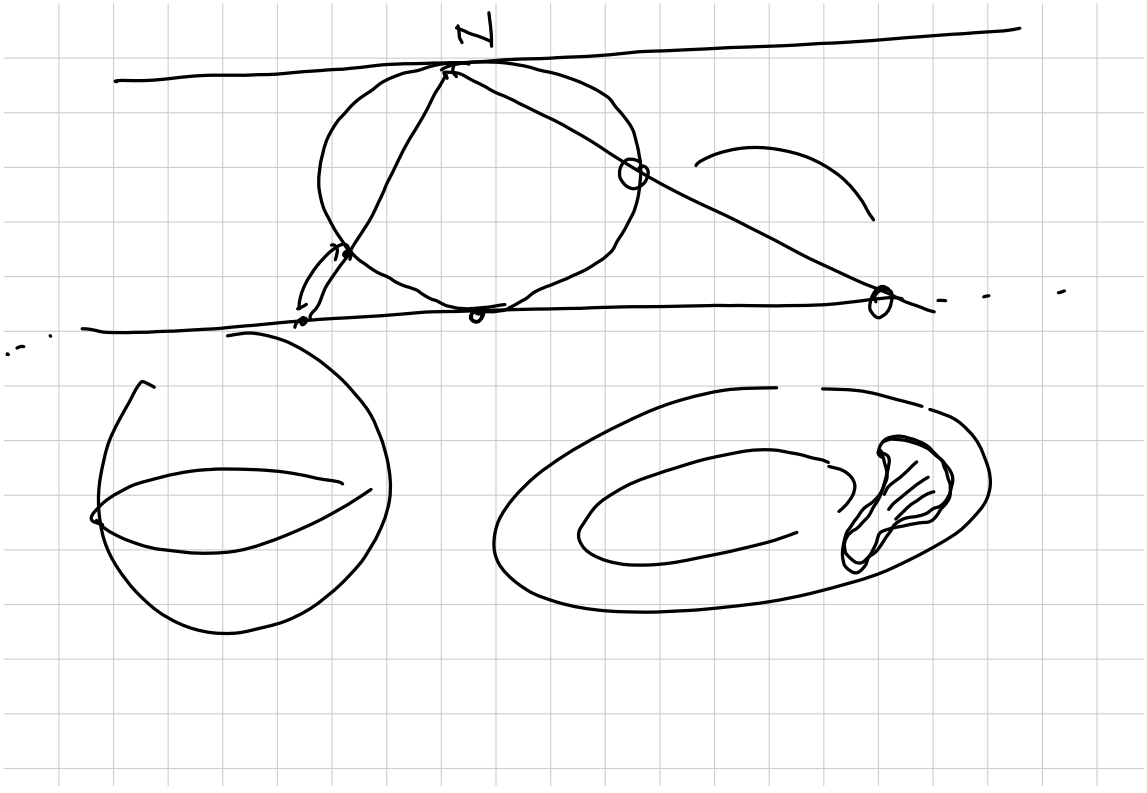

S
T
: from any city in T
leave ≥ 3 Jusers in T
V
h
from any city in V
any other city in V.
S \ T
out deg.
deg+(v)
deg−(v) indeg.

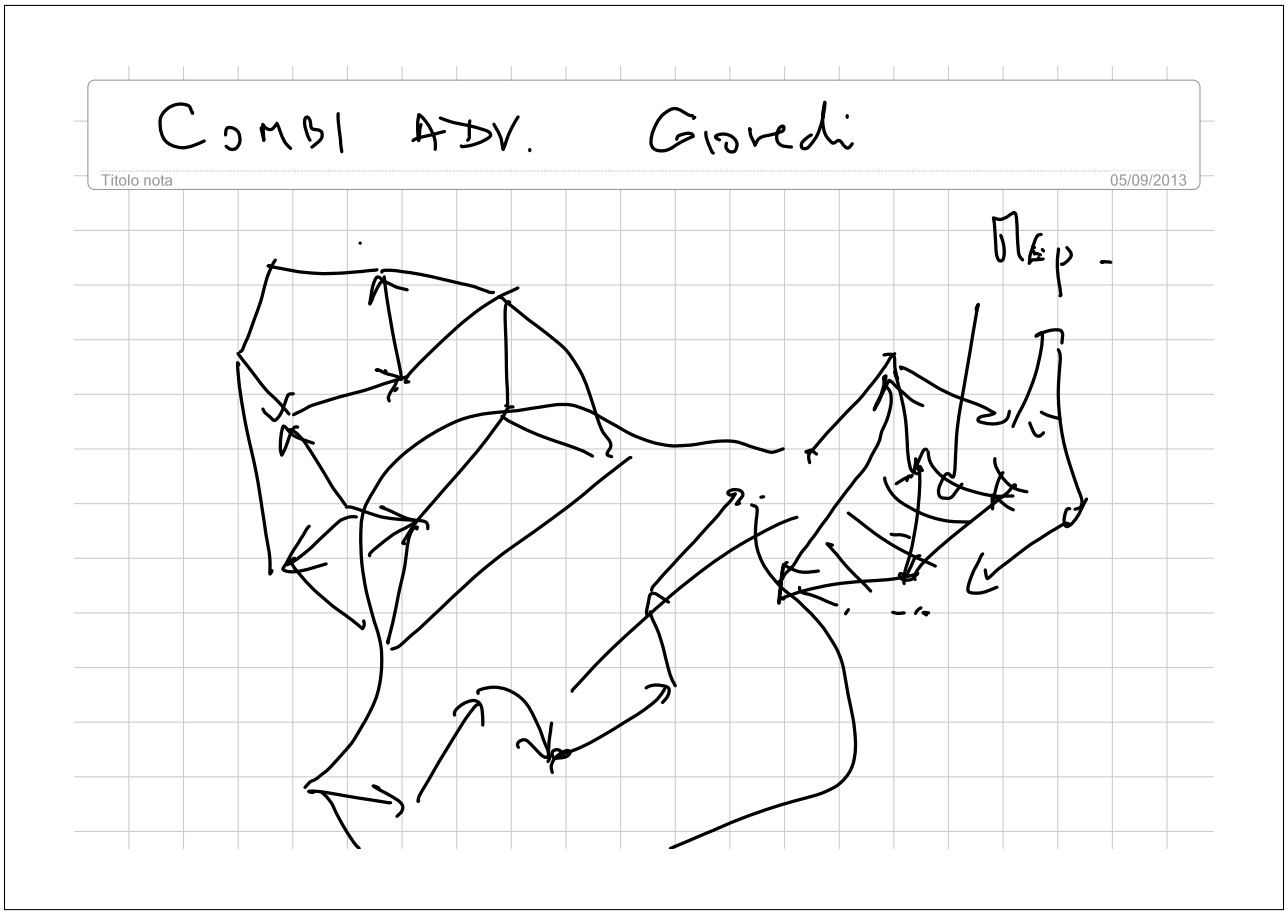

n blocks
m streets
For each city
2
2
2-reg. digraph
4-regular graph
=
2d
d-reg =

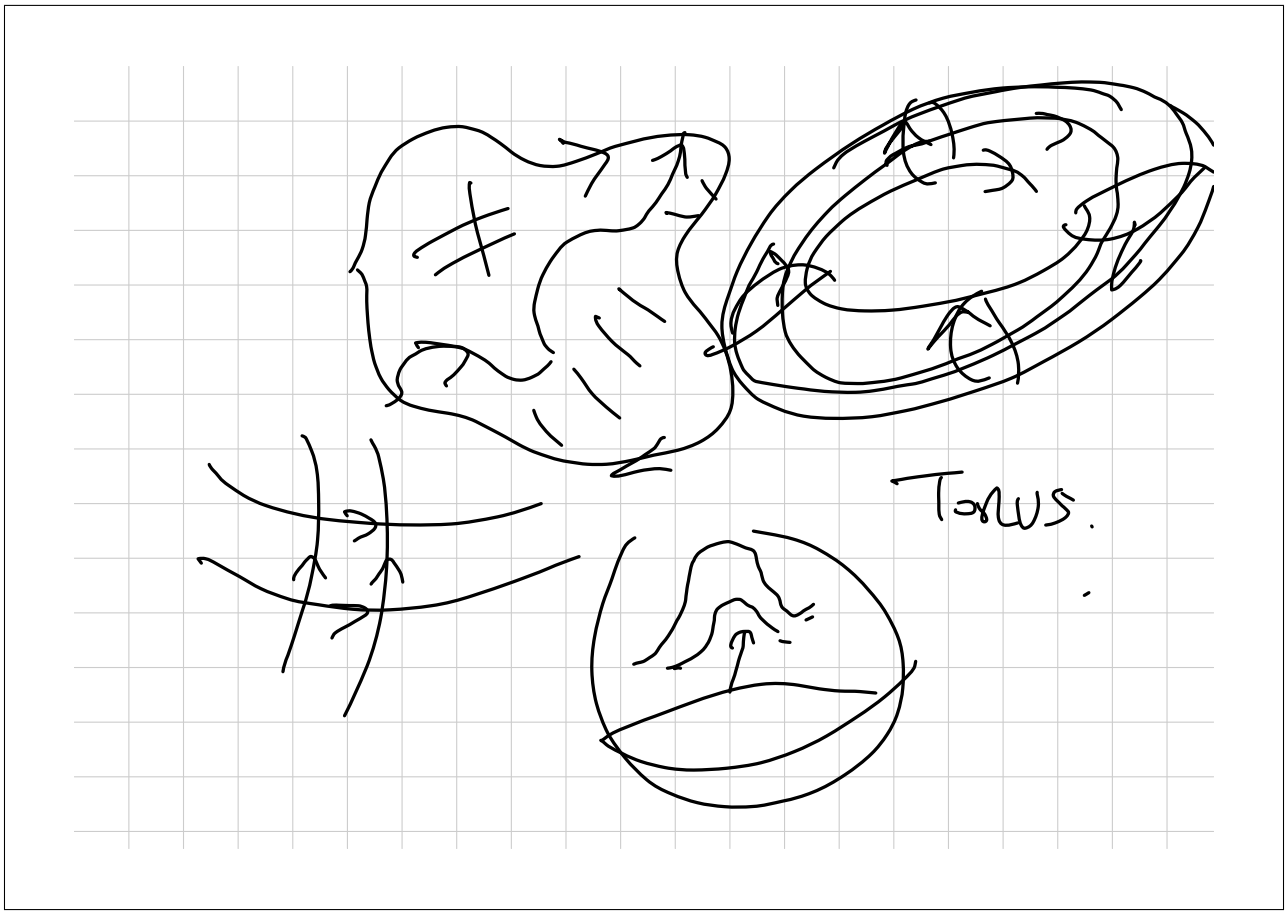

deg⁺(x) = deg⁻(x) = d.
Thm.
Any weakly connected d-reg. digraph is also strongly connected.
⋃ C_v = V
Assume. for v
C_v
k
kd →
→ ka


T
V
v
|C_v| = minimal.
C_v
C_w ⊊ C_v ⇒ ⊥
toroidal lattice
Z_m × Z_m
n
m
∃ even length cycle..

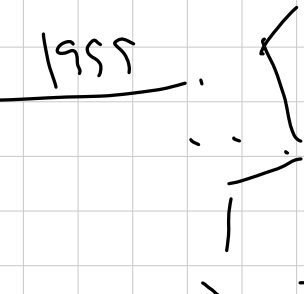

K_4
K_5 — never succeed
$K_{3,3}$
Kuratowski


N


COMBI ADV. Giovedì
Titolo nota
05/09/2013
Map -


TORUS.

China 1995



Color edges red / blue

"eccentric"

exc(v) = #

There exist A, B, s.t. exc(A) + exc(B) ≤ 4

V + F = E + 2

3 3 3

2

$V + F = E \quad (\text{torus})$

"genus" g

$V + F = E + 2(1-g)$

$E \leq 3V - 6$

$V = V_3 + V_4 + \cdots + V_k + \cdots$

$F = F_3 + F_4 + \cdots + F_k + \cdots$

$3V_3 + 4V_4 + \cdots + kV_k + \cdots = 2E$

(F)

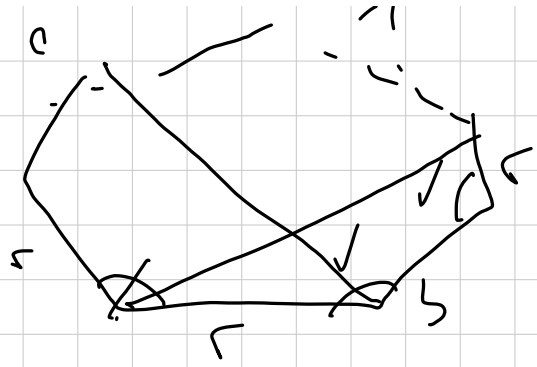
$\sum_{v} \deg(v) = 2E \leq 6V - 12$

$\deg \leq 6 - \frac{12}{V}$.

A

$exc(v) = \#$ $\quad$ $exc(f) = \#$ acc.

$\sum_{v} exc(v) = \sum_{f} exc(f)$



$F = F_3$

$exc(f) \leq 2$.

$\sum deg \leq 6V - 12$

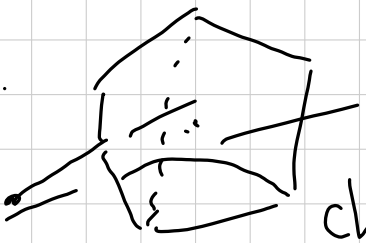
$\sum exc \leq \frac{2}{3}(\quad) = 4V - 8$

$\overline{exc} \leq 4 - \frac{8}{V} < 4$

$exc(v) =$ even. odd number.

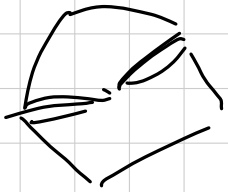
$\exists A, B, C, D$, $\sum exc(A) \leq 8$ Best!.

BMO problem 4.

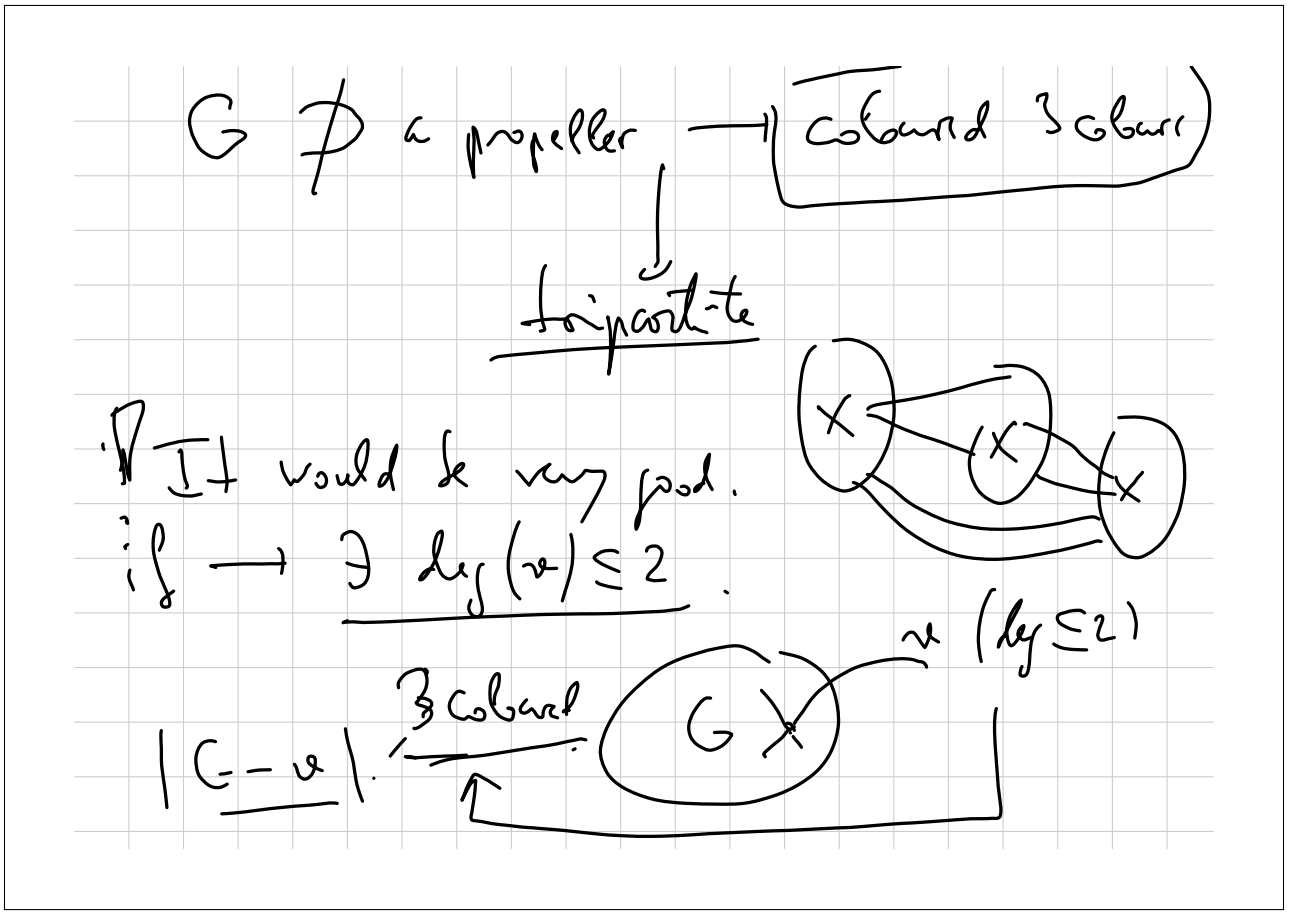


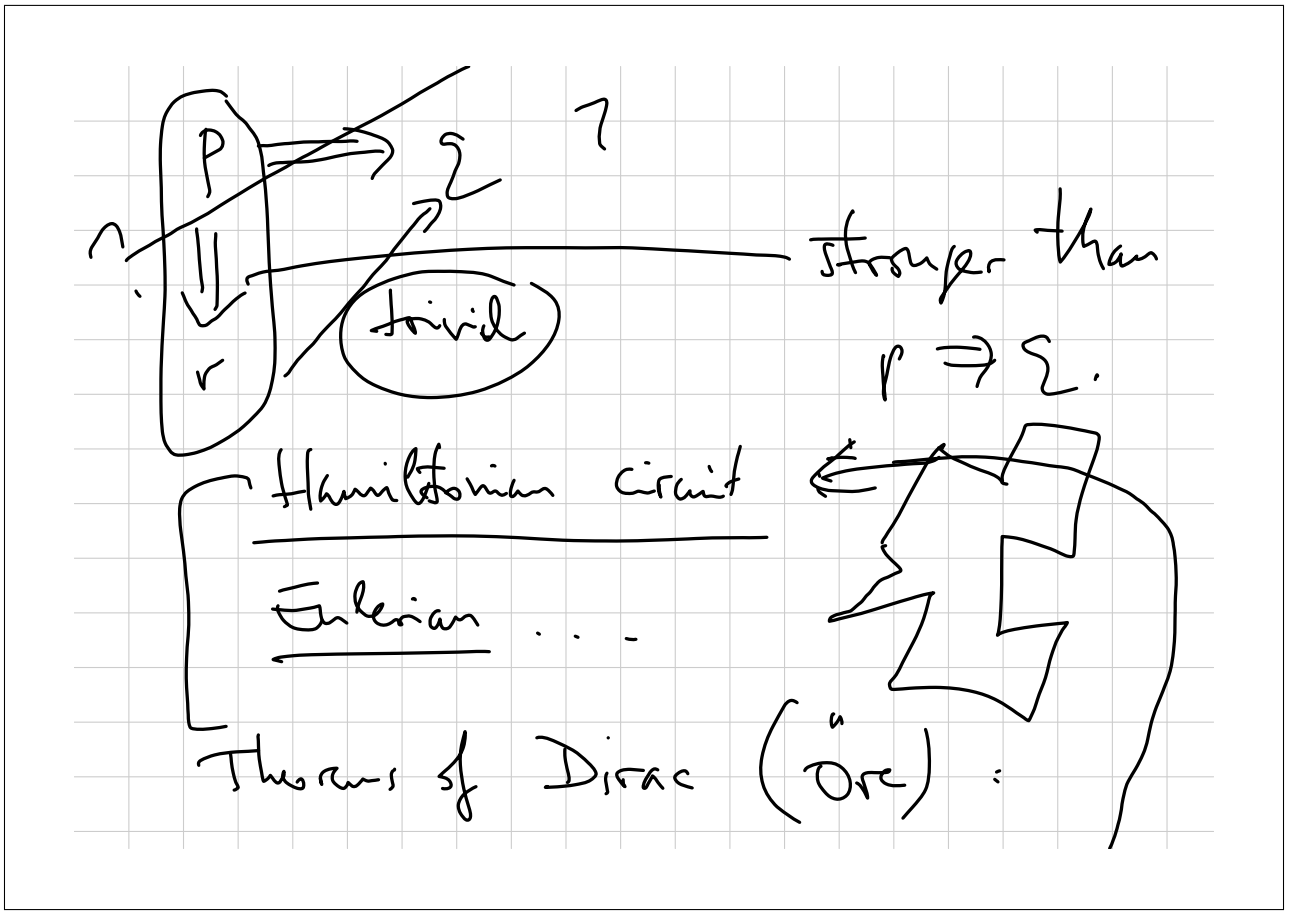
cycle

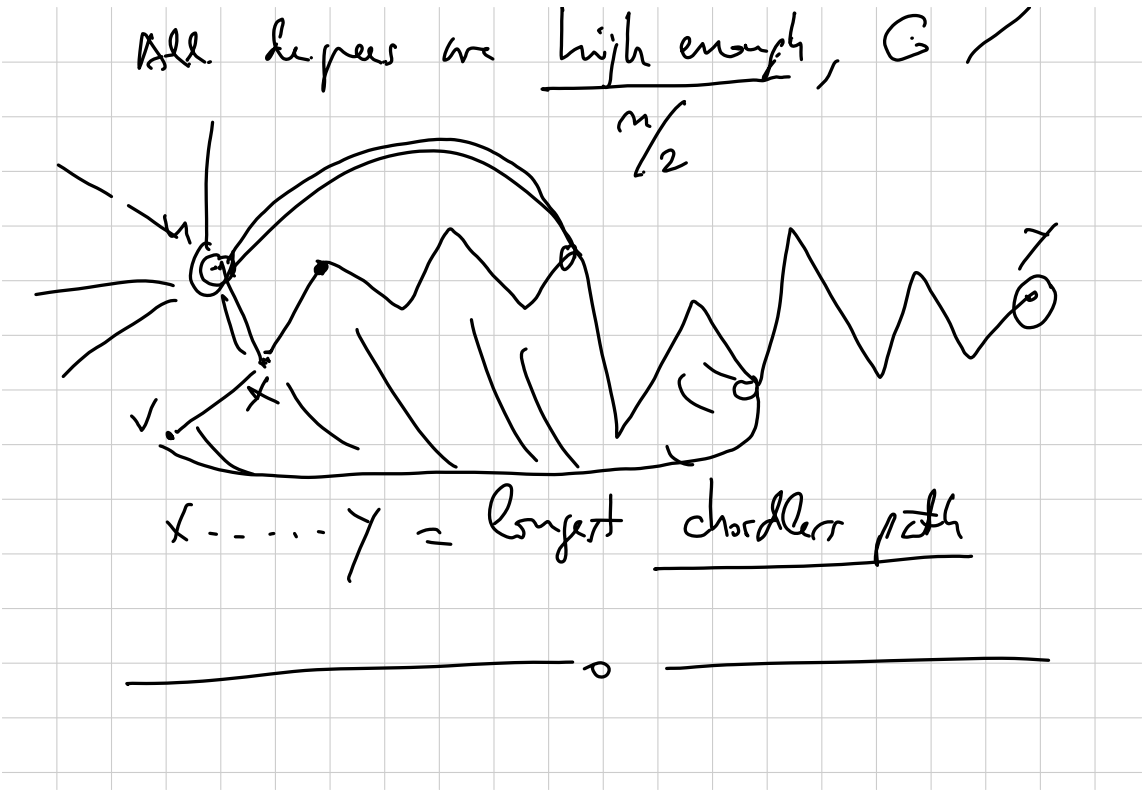
chordless

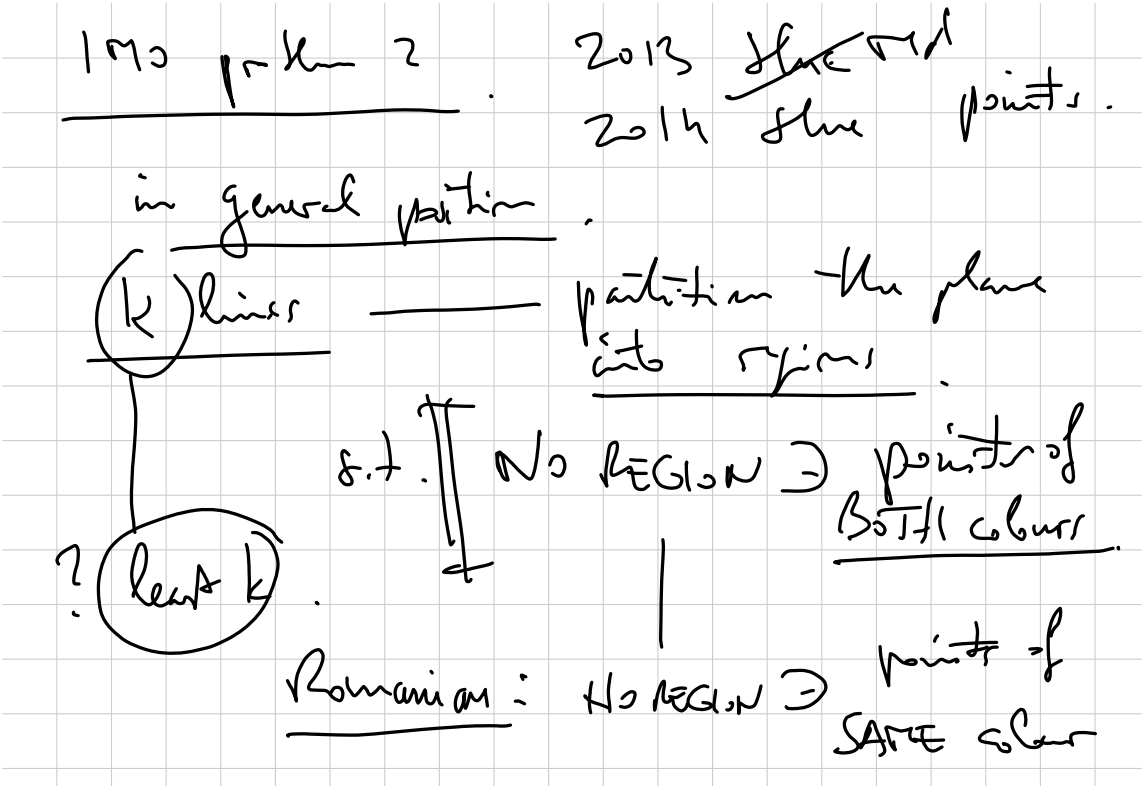


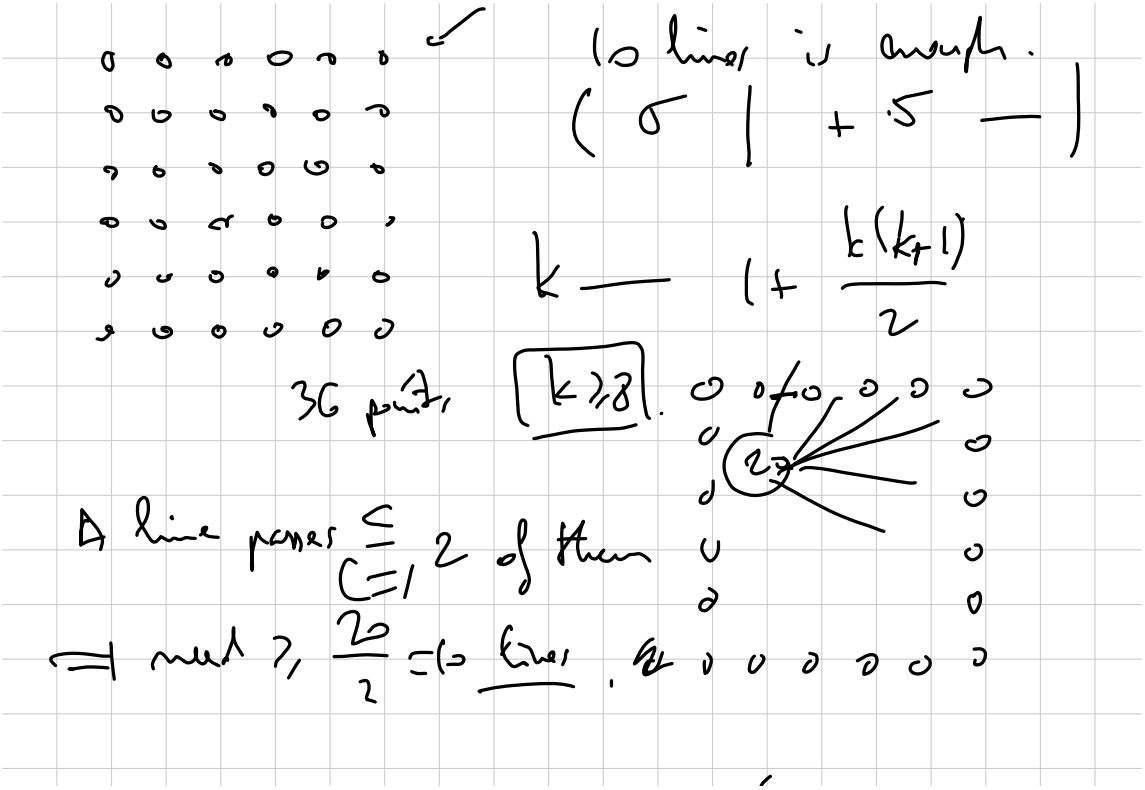
"propeller" 4

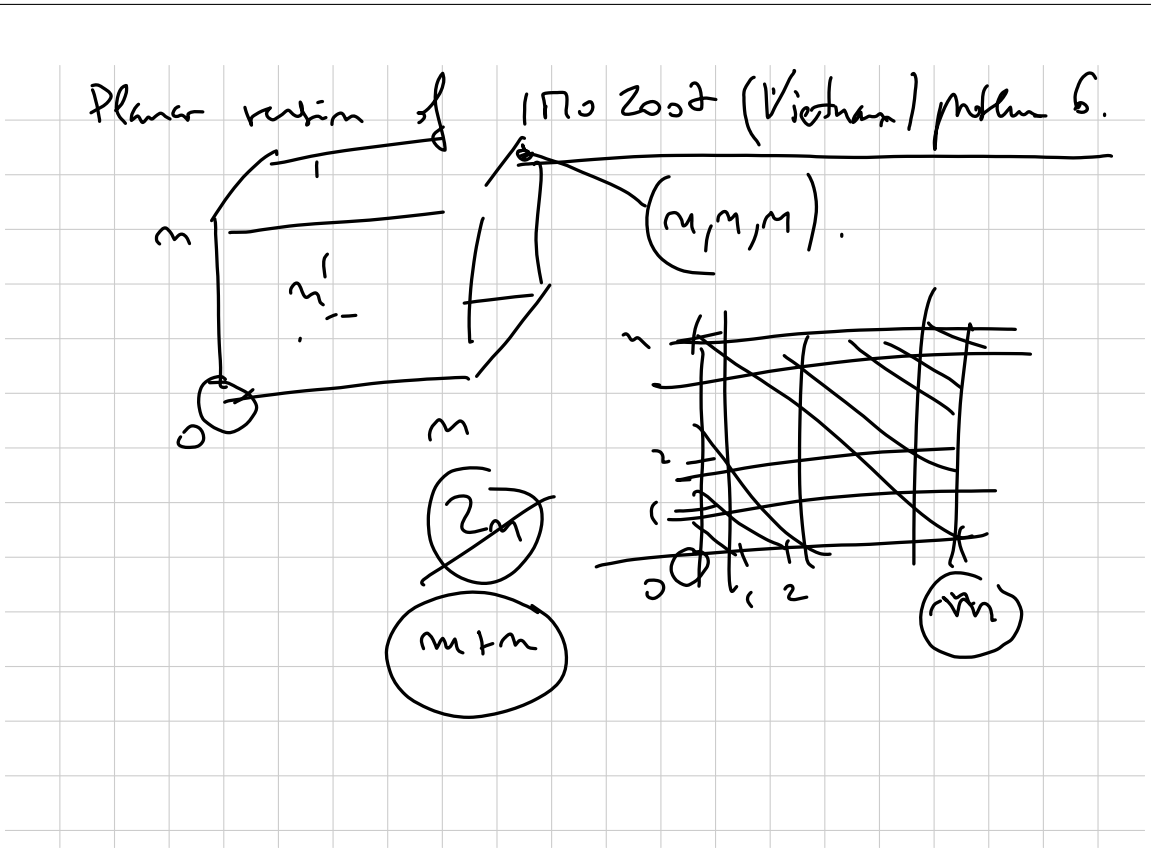

G ⊅ a propeller
coloured 3colour
tripartite
It would be very good.
if → ∃ deg(v) ≤ 2.
X
X
X
v (deg ≤ 2)
|G − v|.
3colour
G

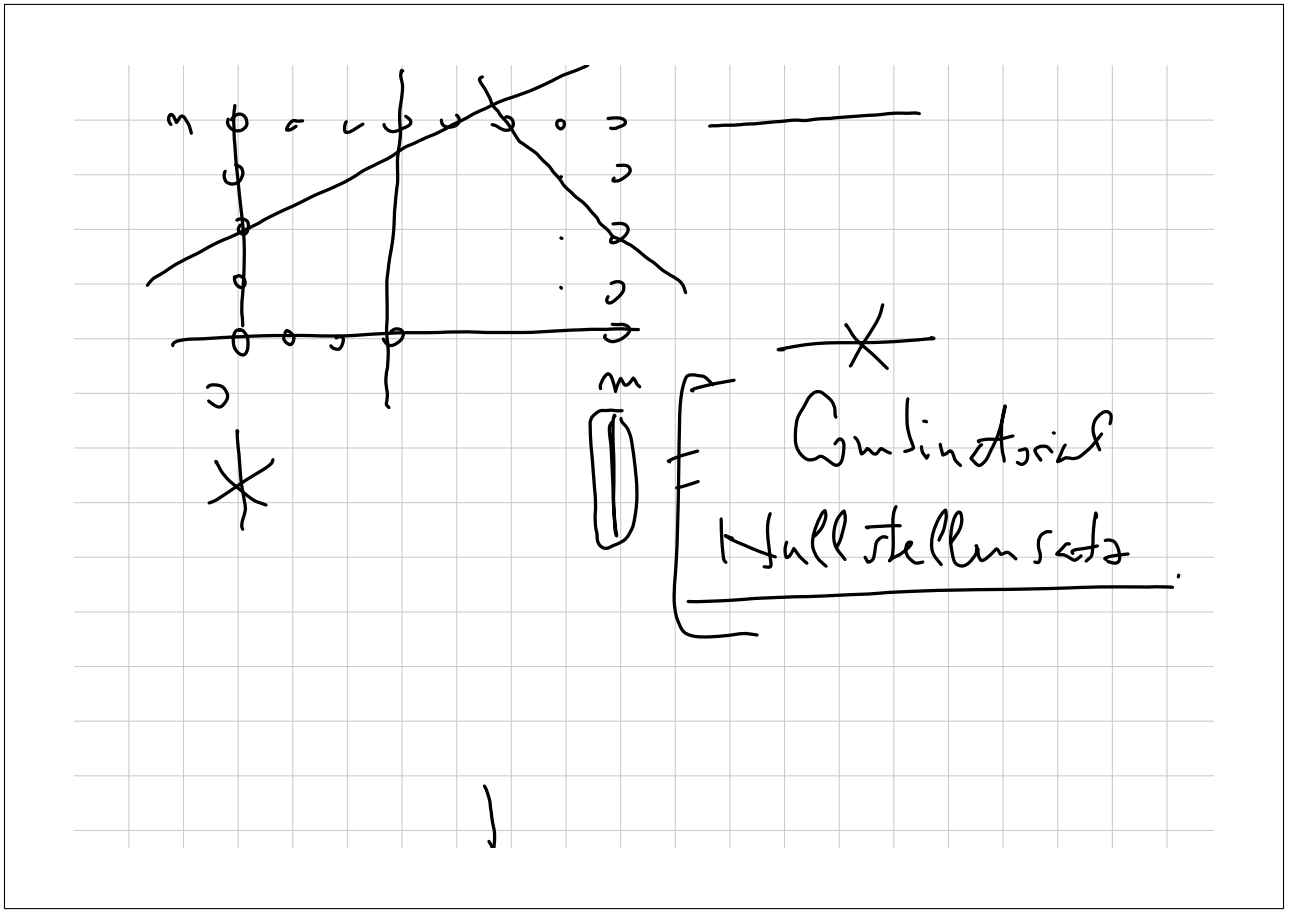

P
Q
?
r
trivial
stronger than
P ⇒ Q.
Hamiltonian circuit
Eulerian . . .
Theorem of Dirac (Ore):

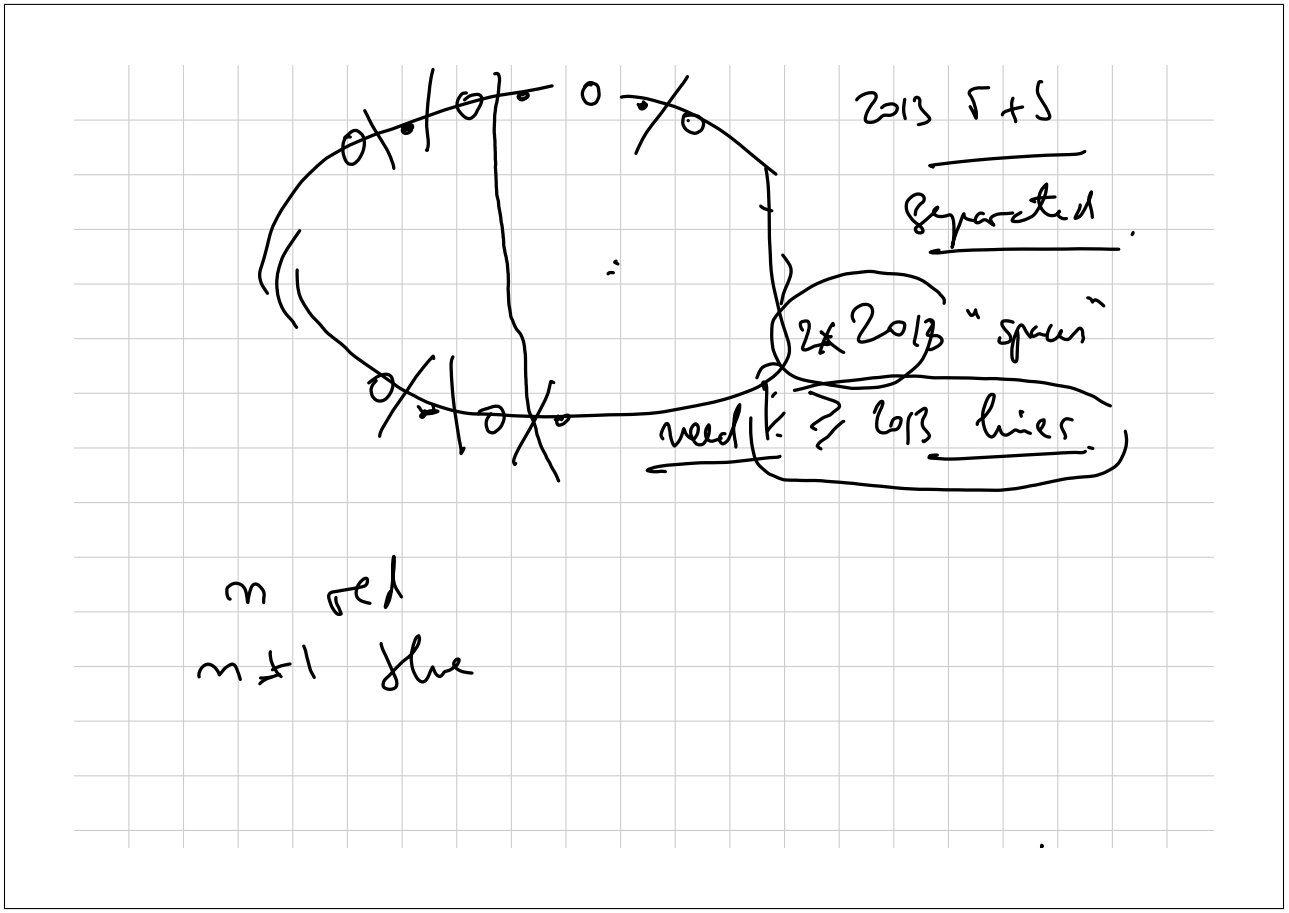

All degrees are high enough, G ✓
n/2
x
y
x ..... y = longest chordless path

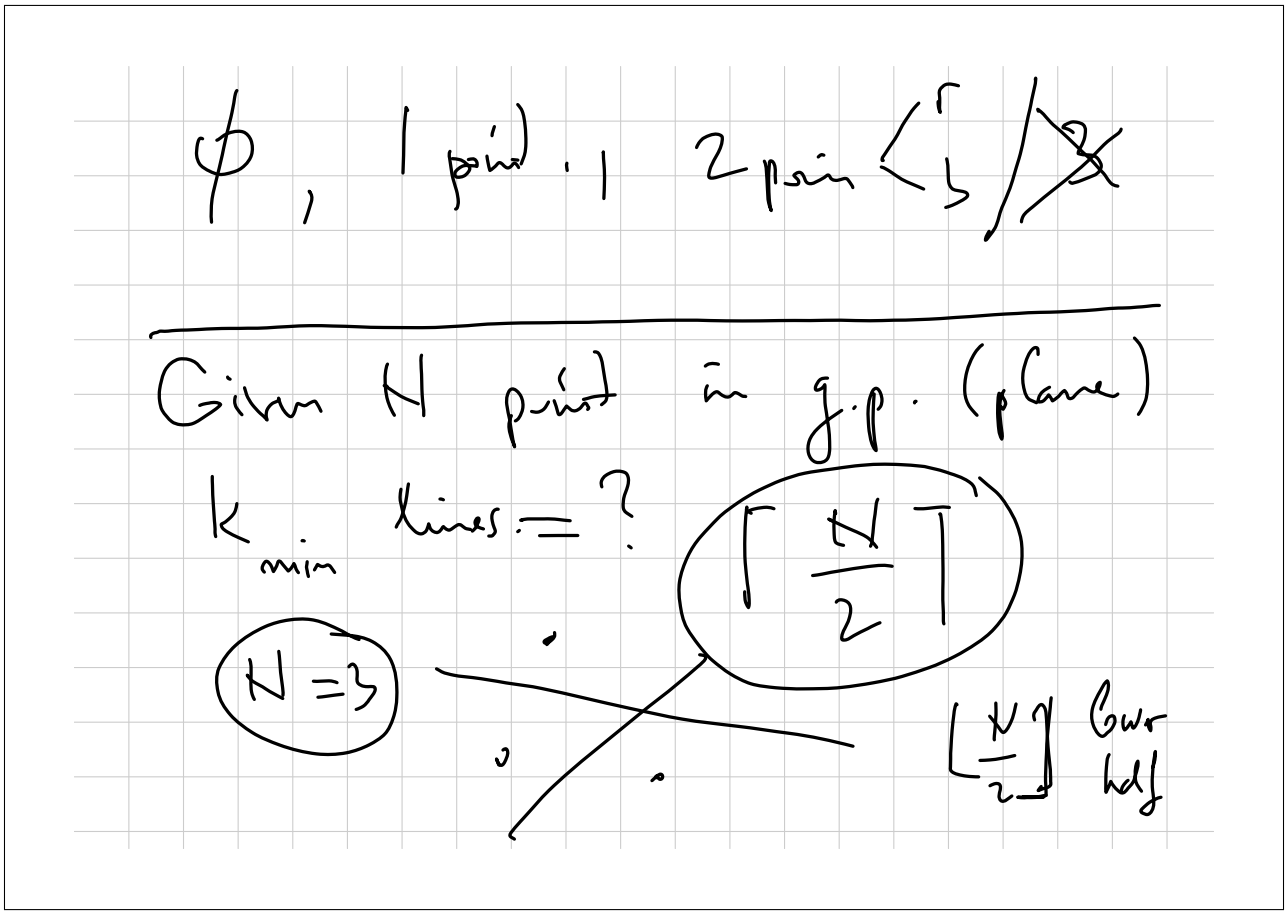

IMO problem 2
2013
2014 plane points.
in general position.
k lines
partition the plane into regions.
s.t. NO REGION ∋ points of BOTH colours.
? least k.
Romanian: NO REGION ∋ points of SAME colour

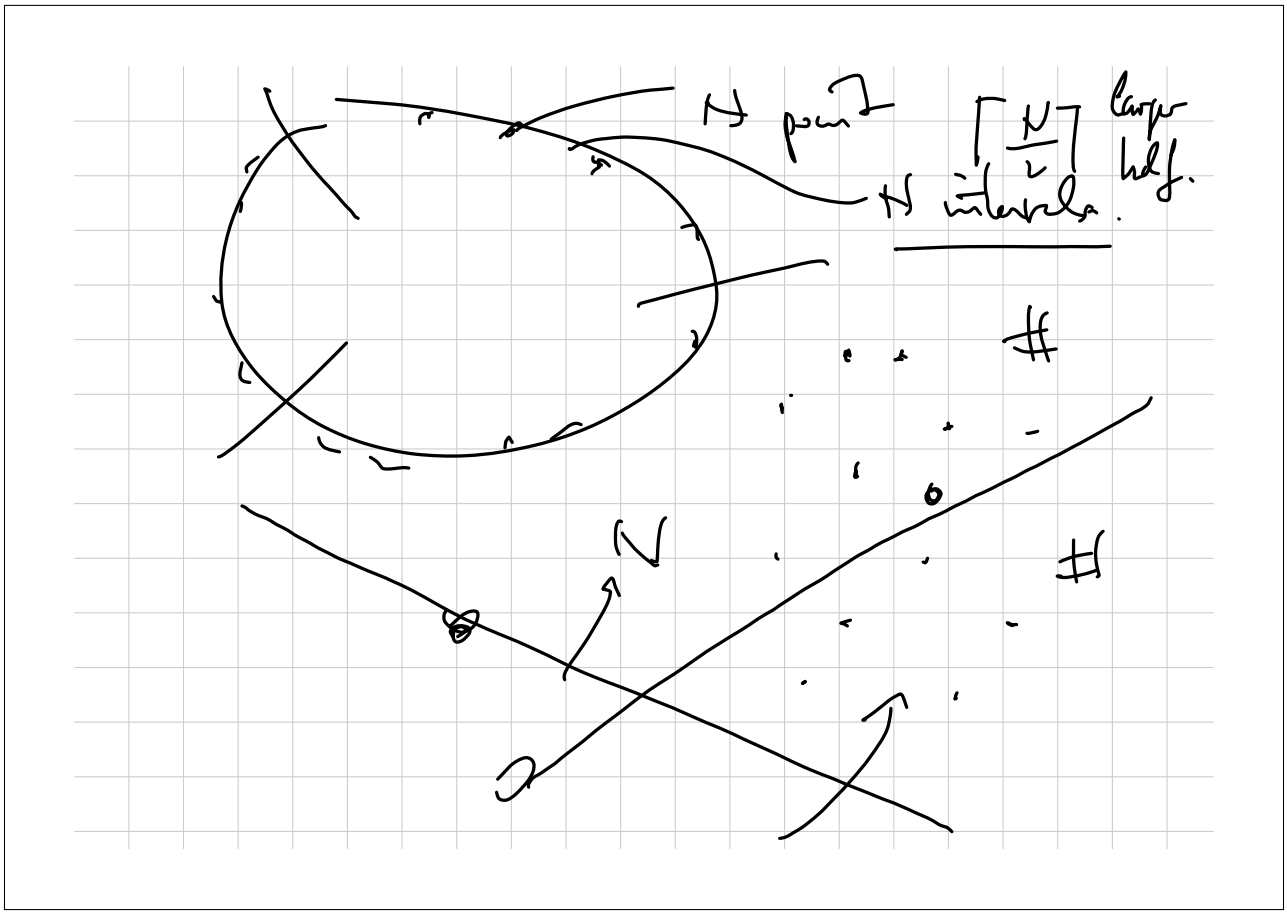

15 lines is enough.
36 points
k ≥ 8.
A line passes ≤ 2 of them
⇒ need ≥ 20/2 = 10 lines.

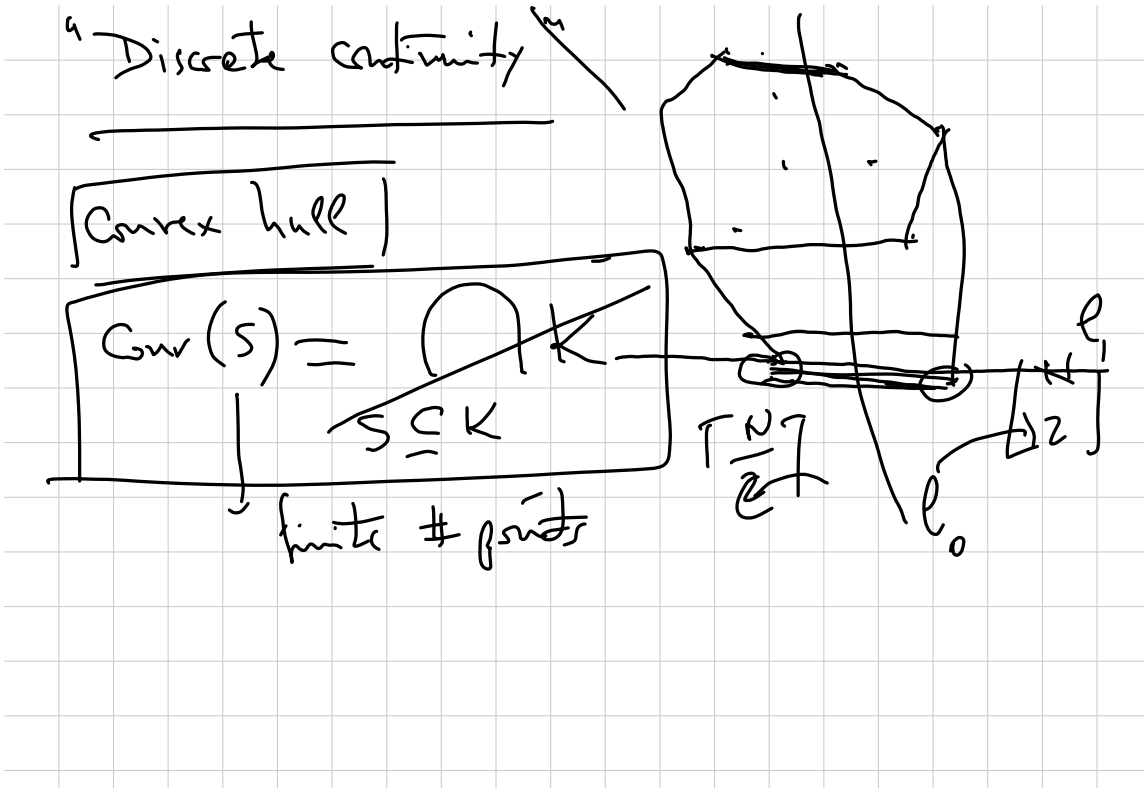

Planar version of IMO 2002 (Vietnam) problem 6.
(n,n,n).
n
n!
0
n
2n
n+n
n
2
1
0
1, 2
n!

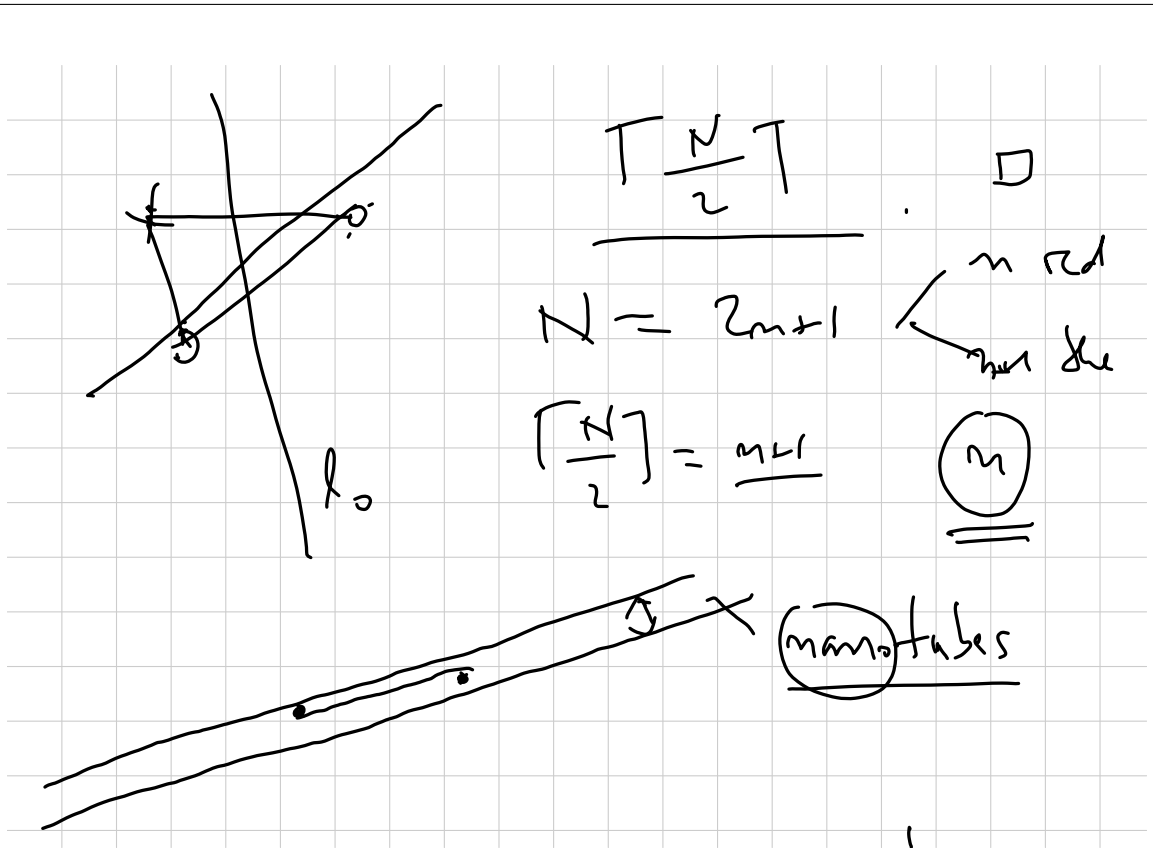

Combinatorial
Hall stellensatz

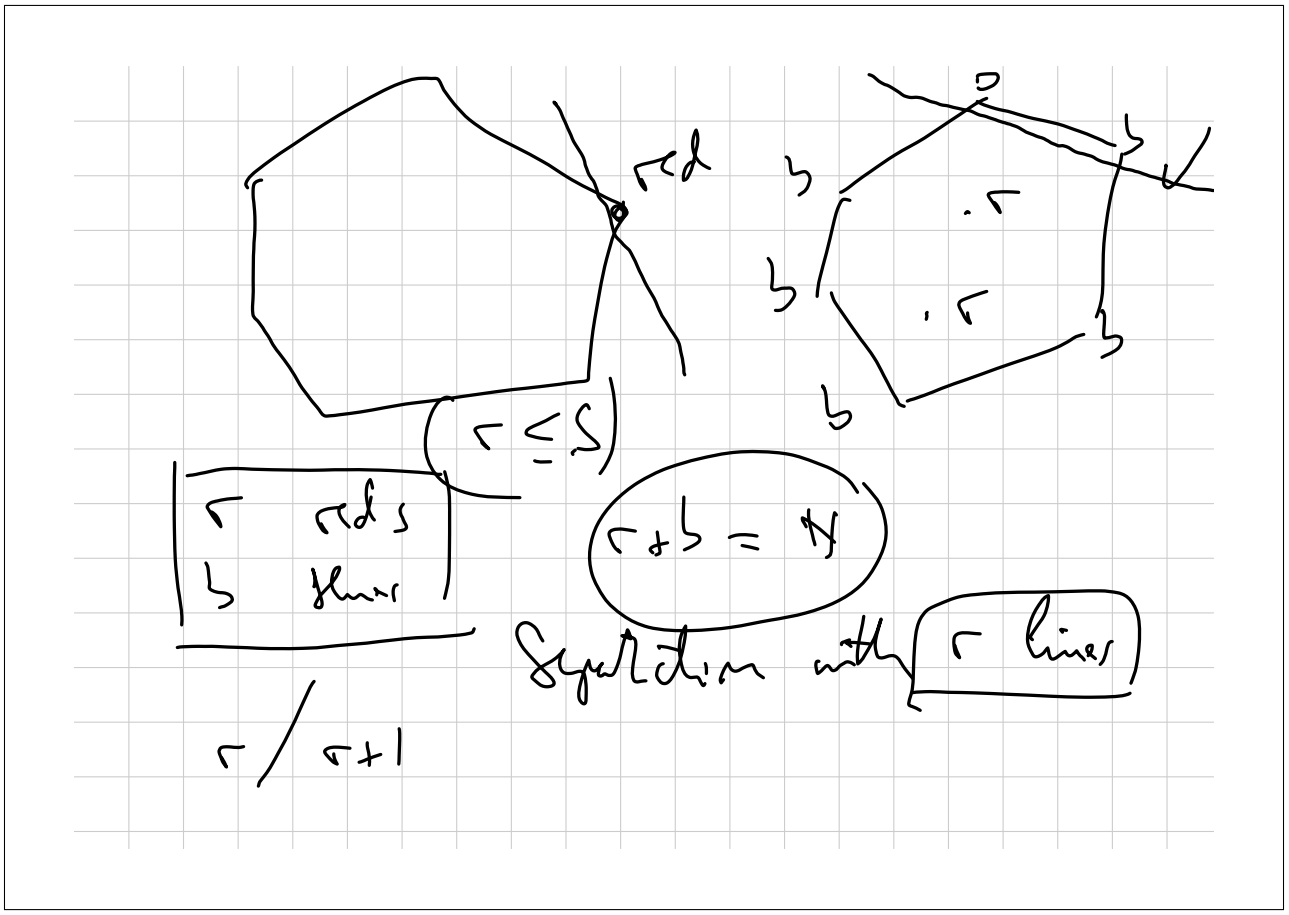

2013 5+5
separated
2x2013 "spurs"
need ≥ 2013 lines
n red
n+1 blue

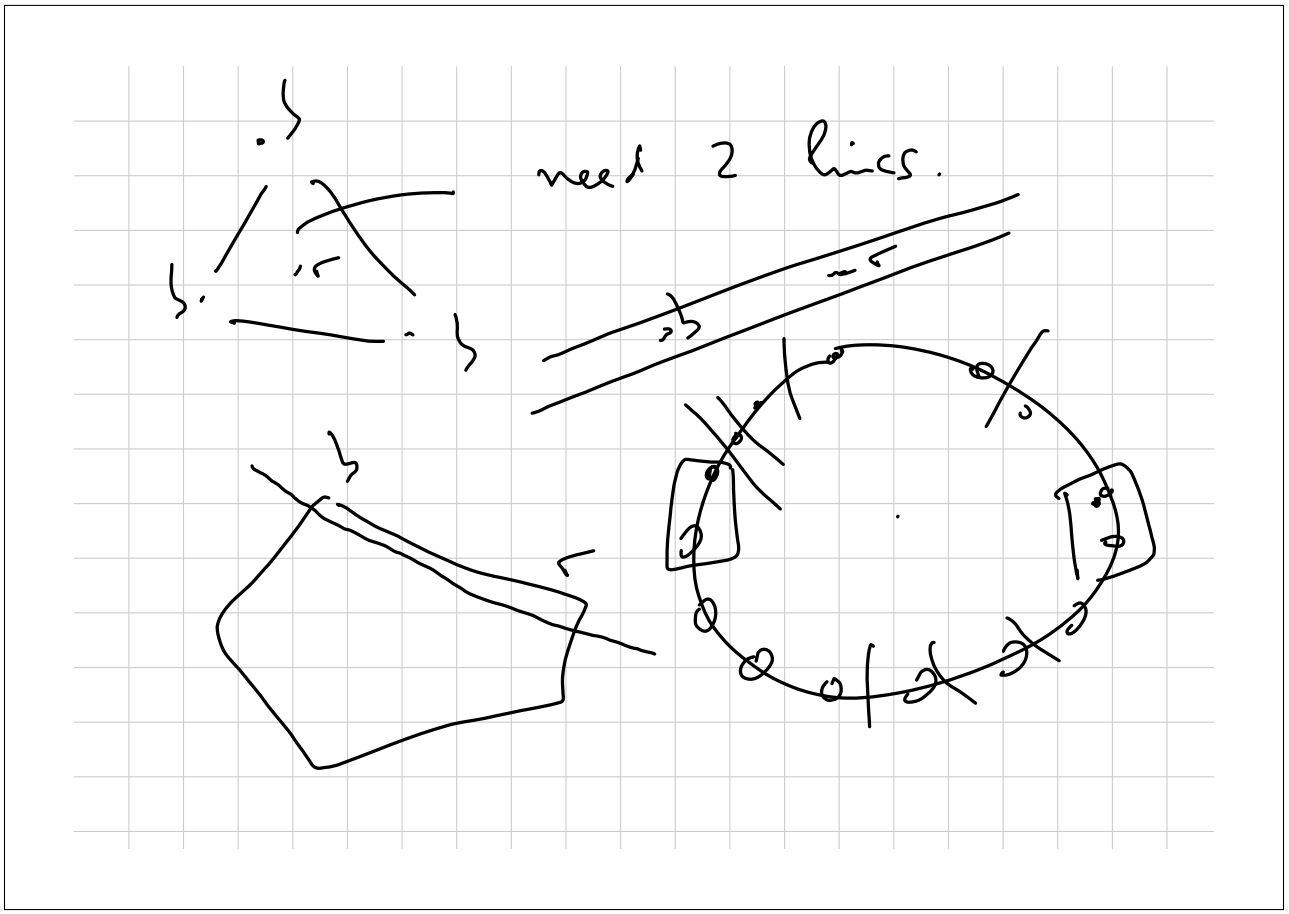

0 , 1 point . 1 2 points
Given N point in g.p. (please)
k_{min} lines := ?
N = 3
$\lceil \frac{N}{2} \rceil$
$\lfloor \frac{N}{2} \rfloor$ Cour hdf

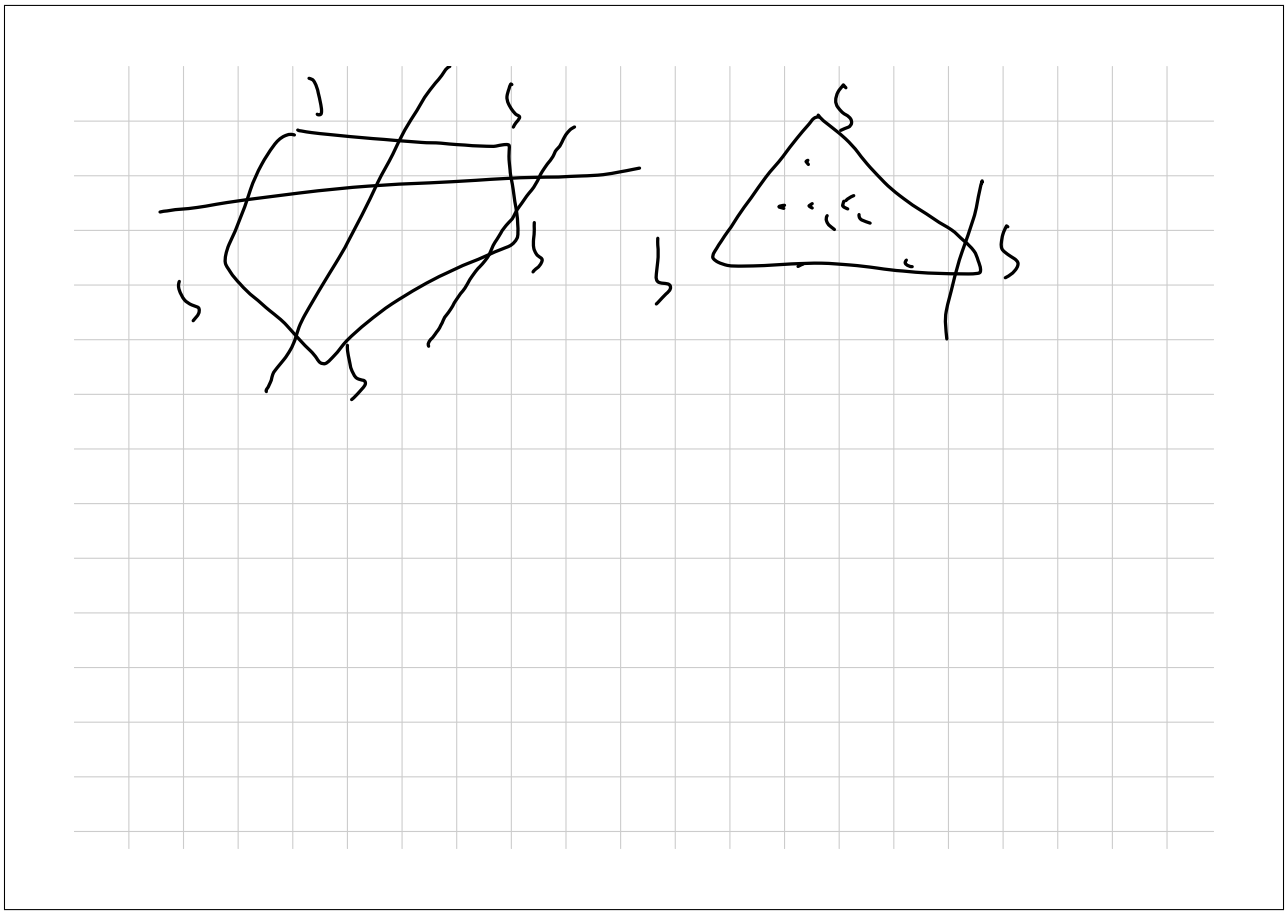

N point
$\lceil \frac{N}{2} \rceil$ large hdf.
N intervals.
N
#
#

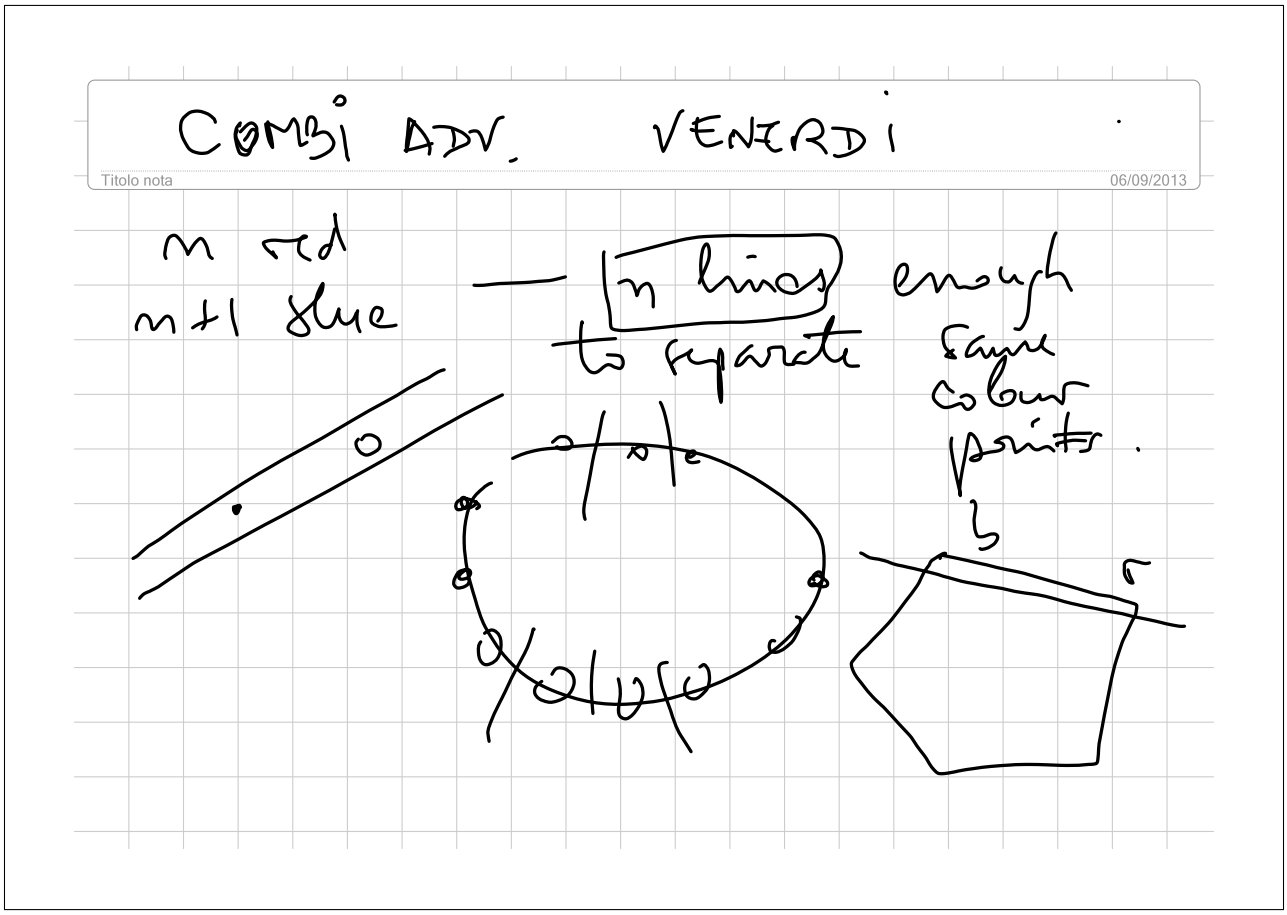

"Discrete continuity"
Convex hull
Conv(S) = ∩ K
S ⊆ K
finite # points
⌈N/2⌉
ℓ0
ℓ1
2

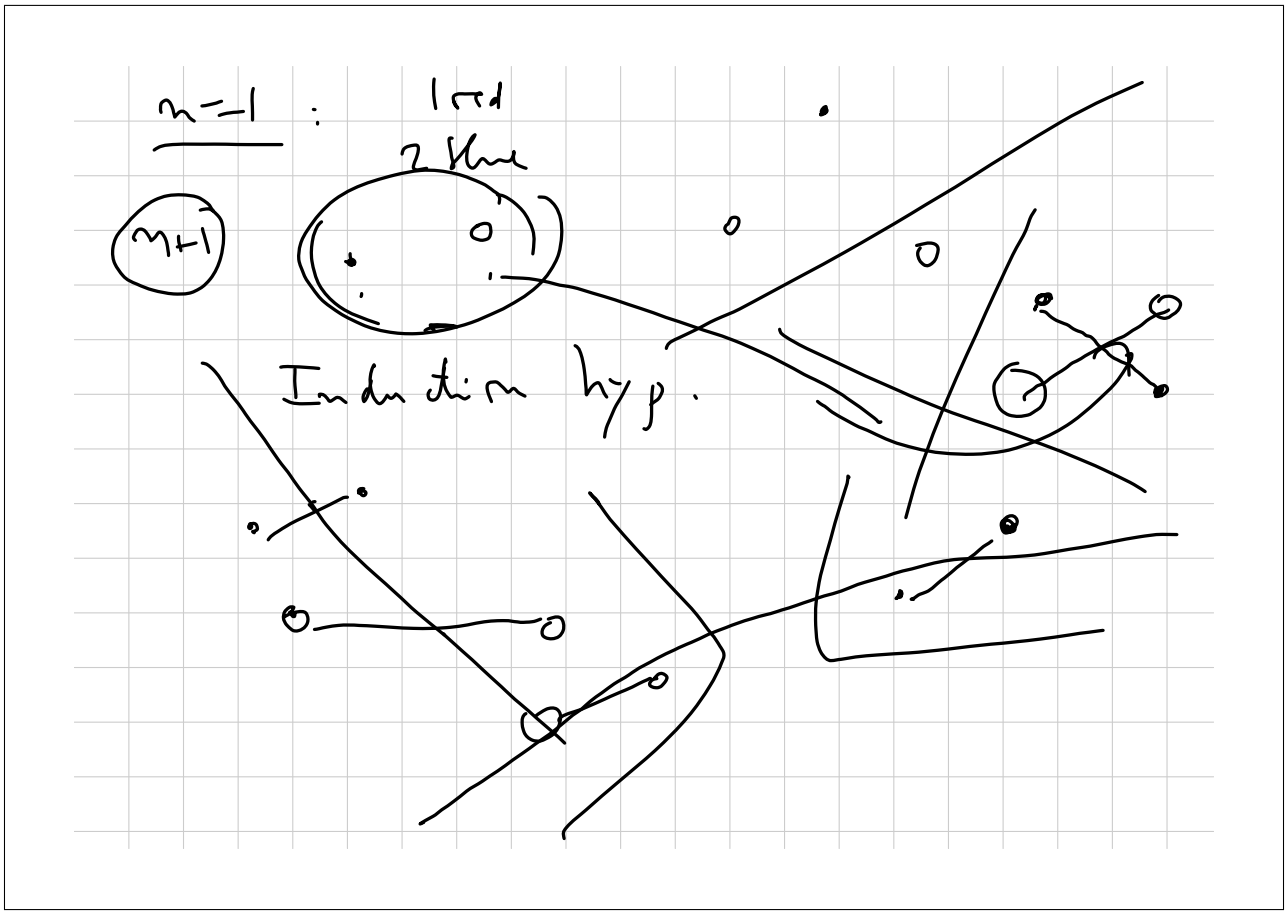

⌈N/2⌉
N = 2m+1
⌈N/2⌉ = m+1
m
ℓ0
nanotubes

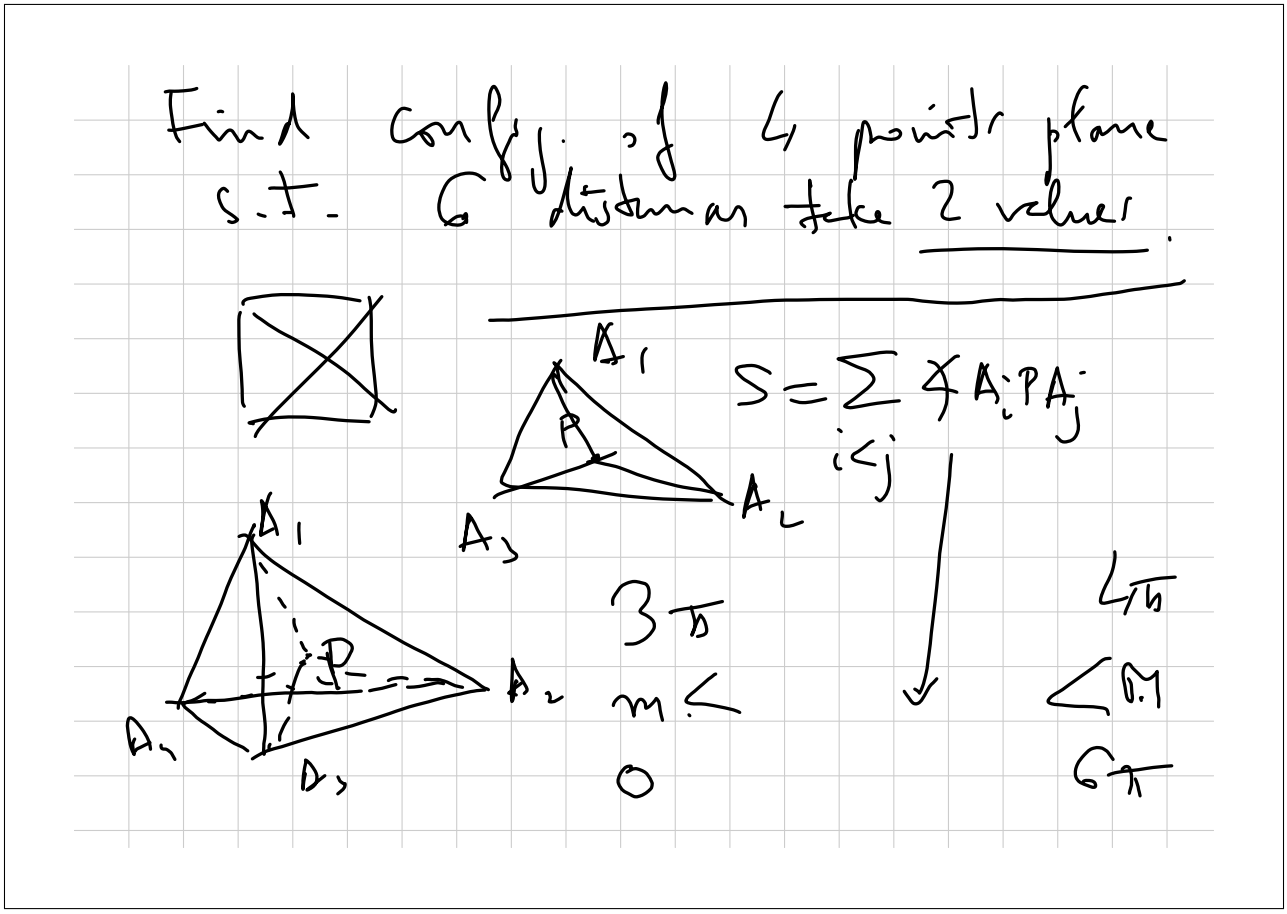


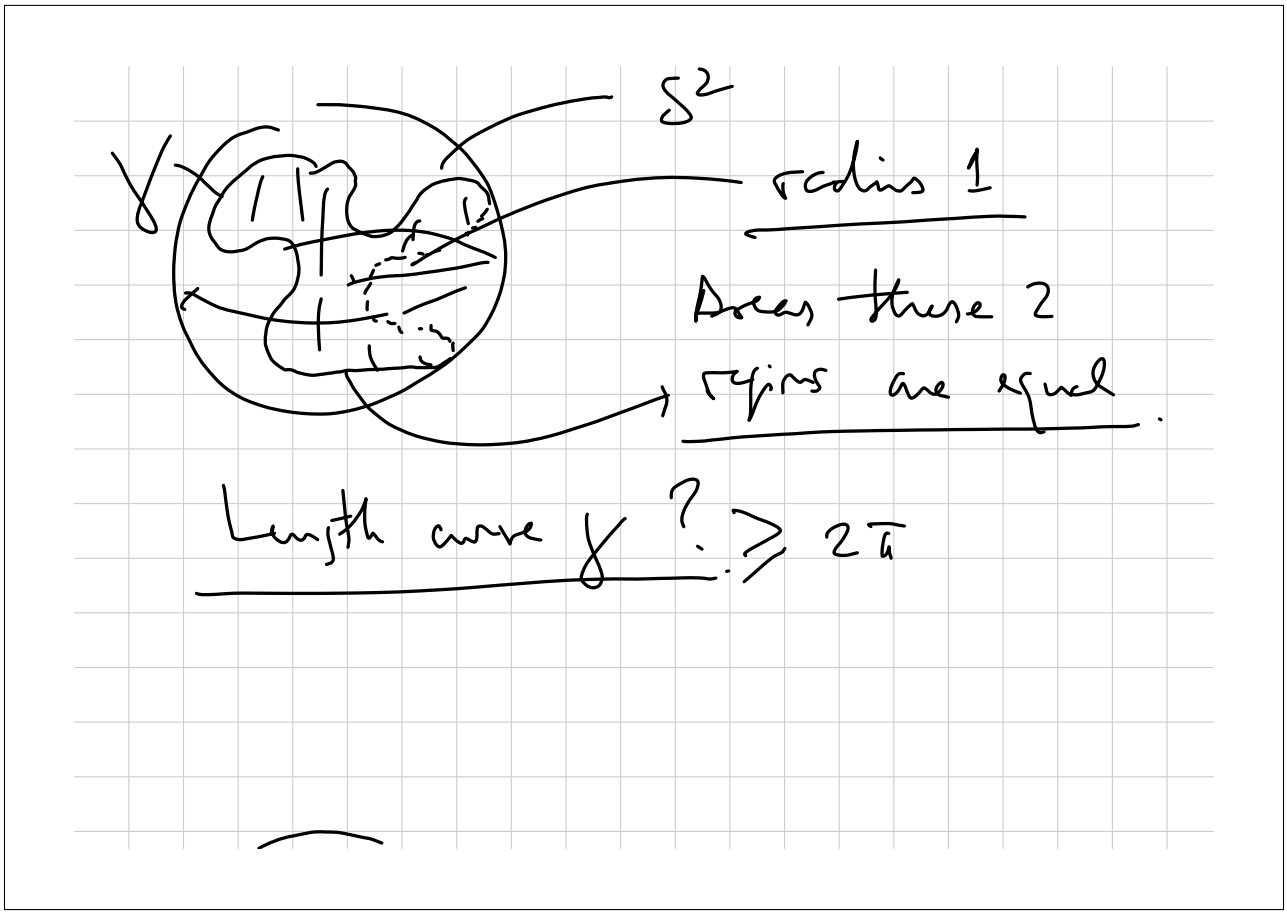

need 2 lines.

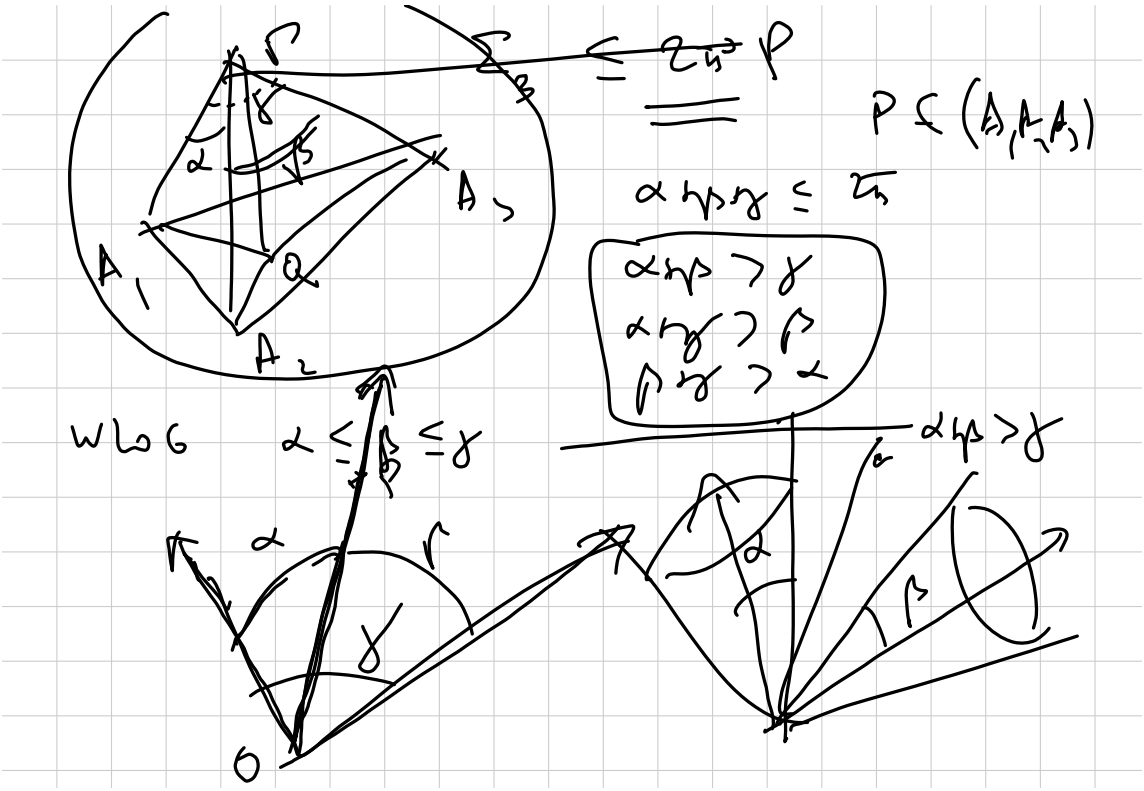


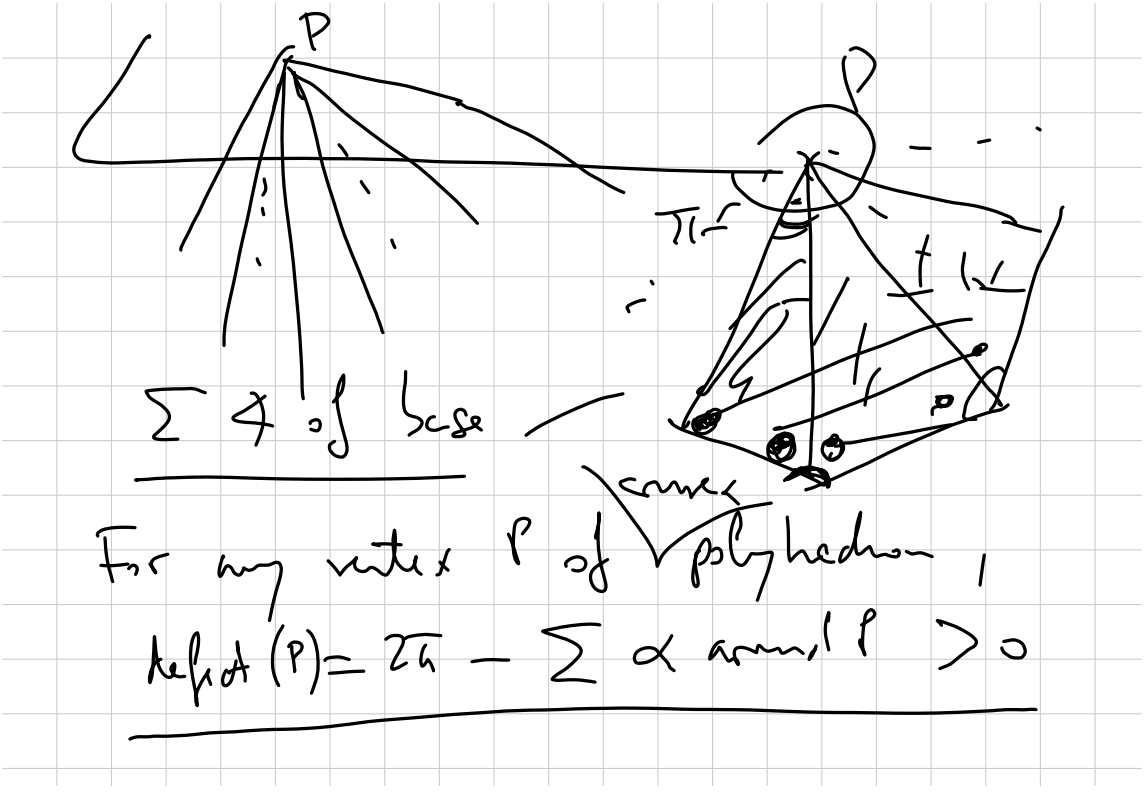

COMBI ADV. VENERDI
Titolo nota
06/09/2013
n red
n+1 blue
n lines enough
to separate
same
colour
points.


n=1 : 1 red
2 blue
n+1
Induction hyp.


Find config. of 4 points s.t. 6 distances take 2 values.
A_1
P
A_3
A_2
$S = \sum_{i<j} \angle A_i P A_j$
3π
$m <$
0
4π
$< 6\cdot\pi$
6π

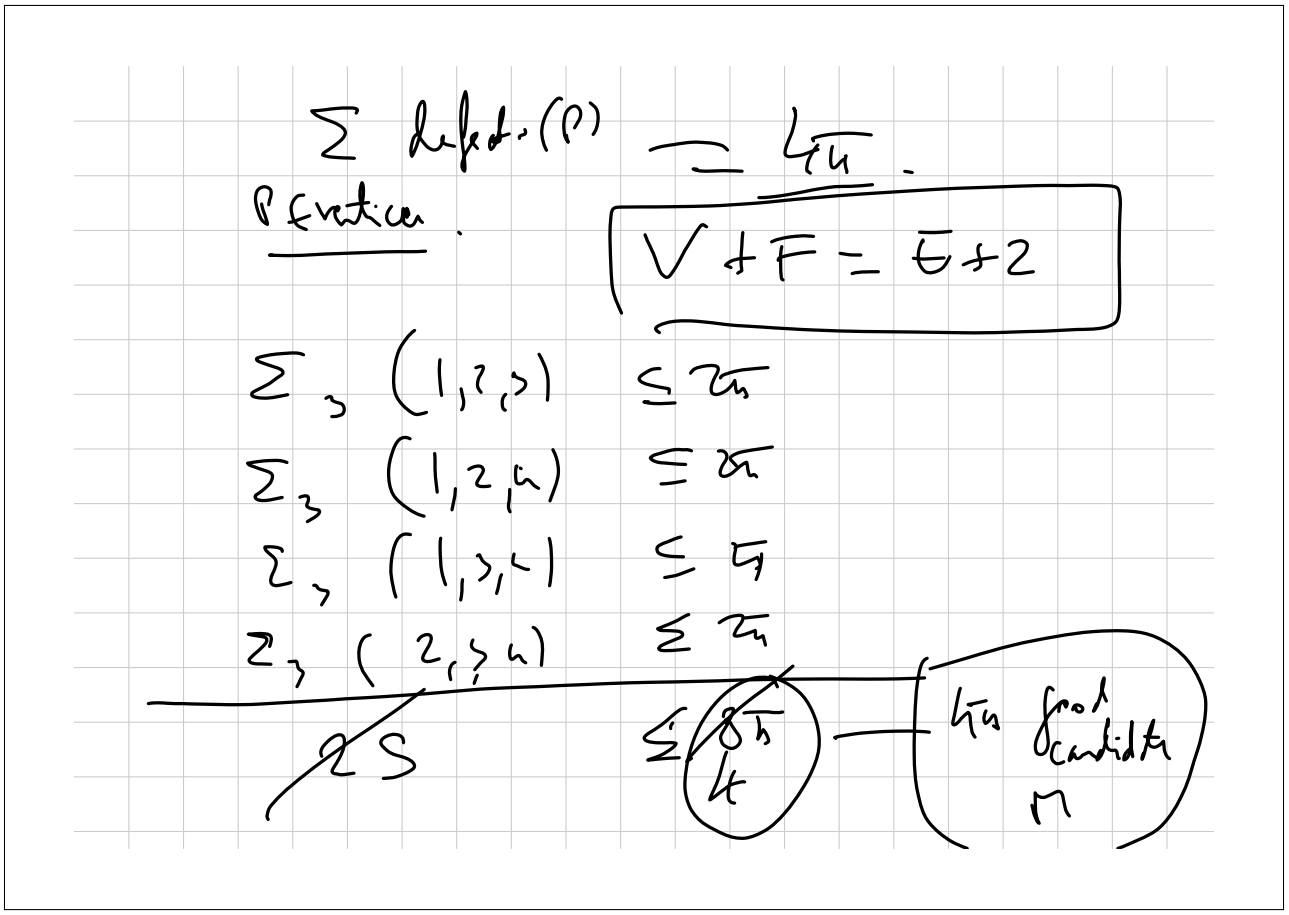

S^2
radius 1
Areas these 2 regions are equal.
Length curve γ ? $\geq 2\pi$

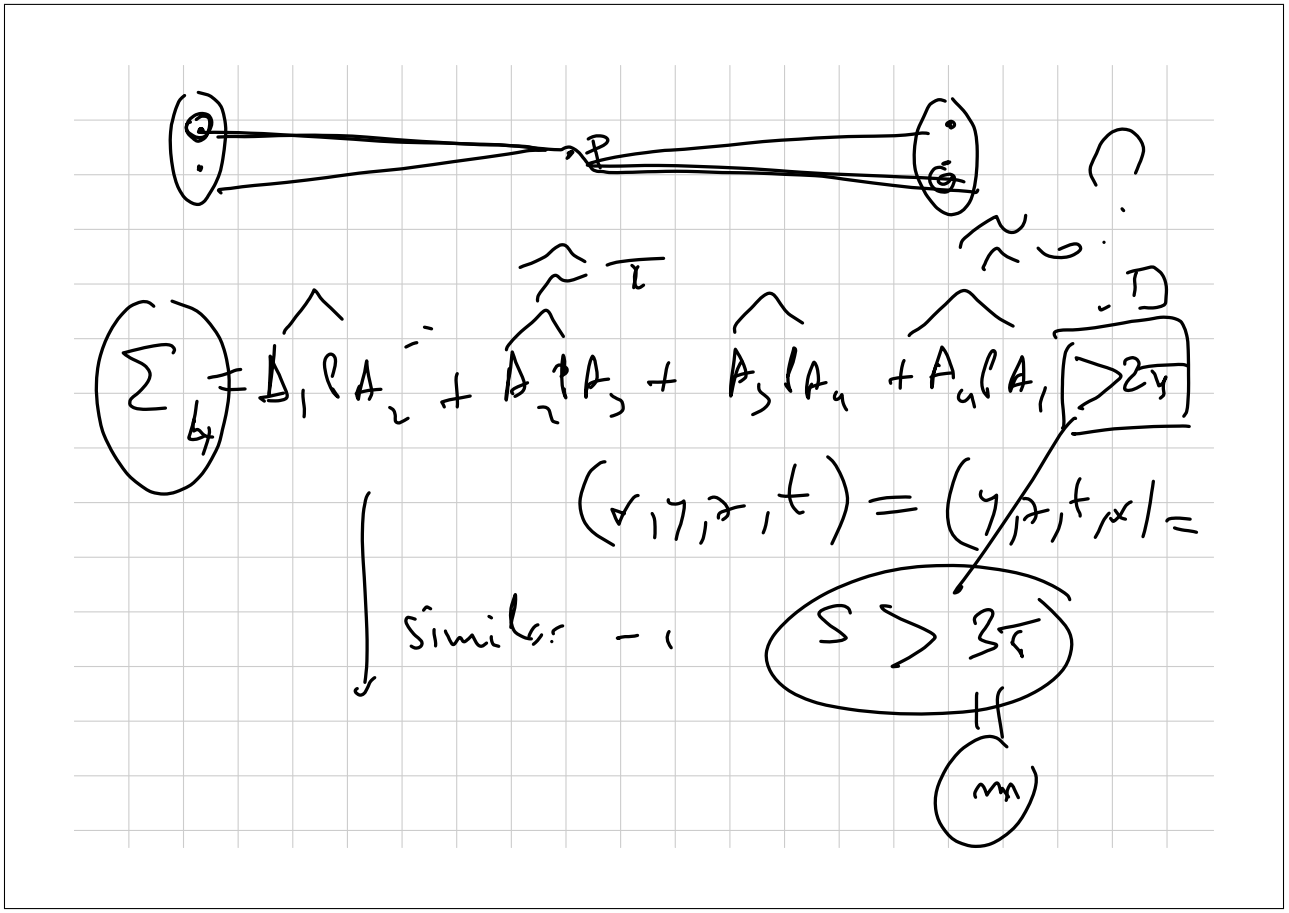


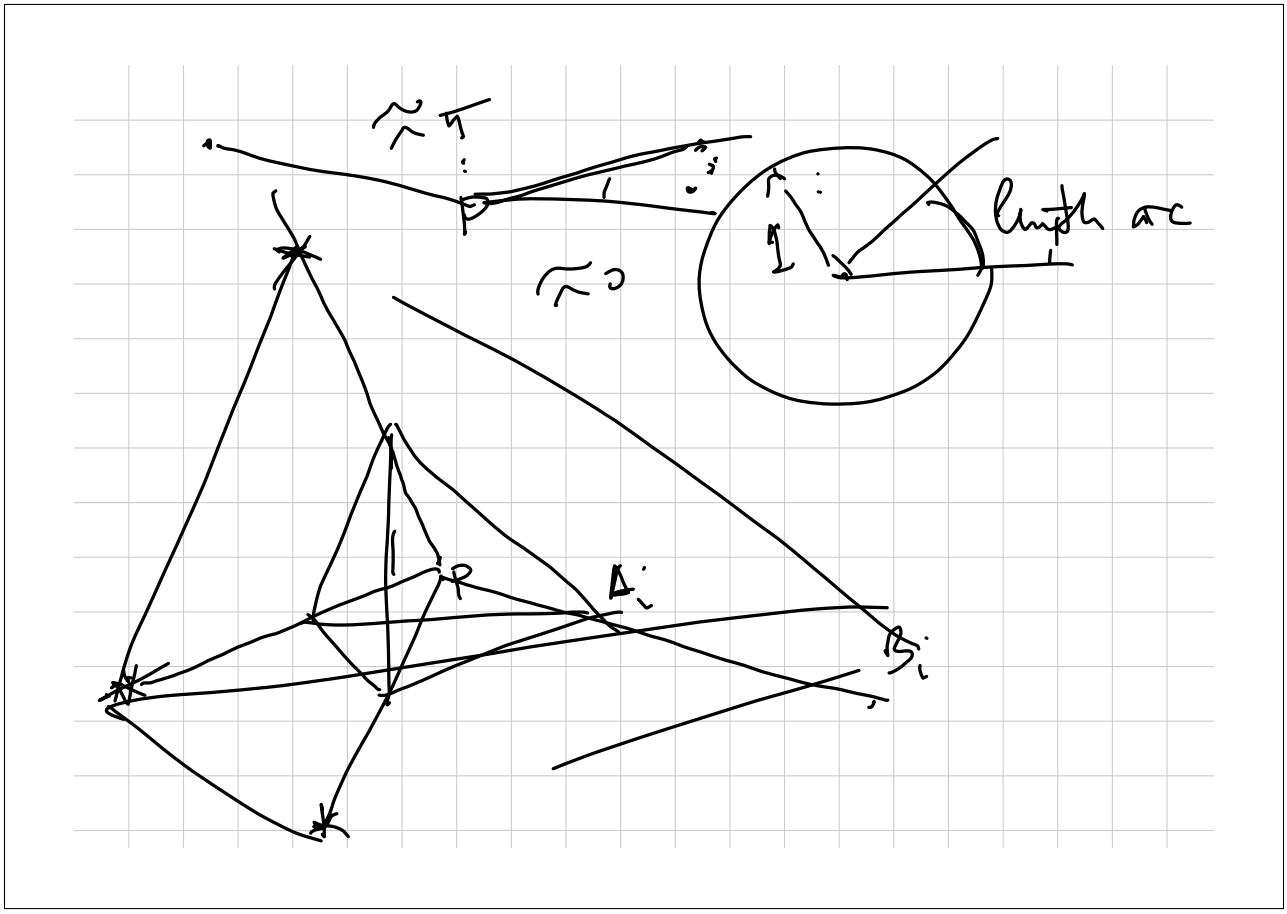


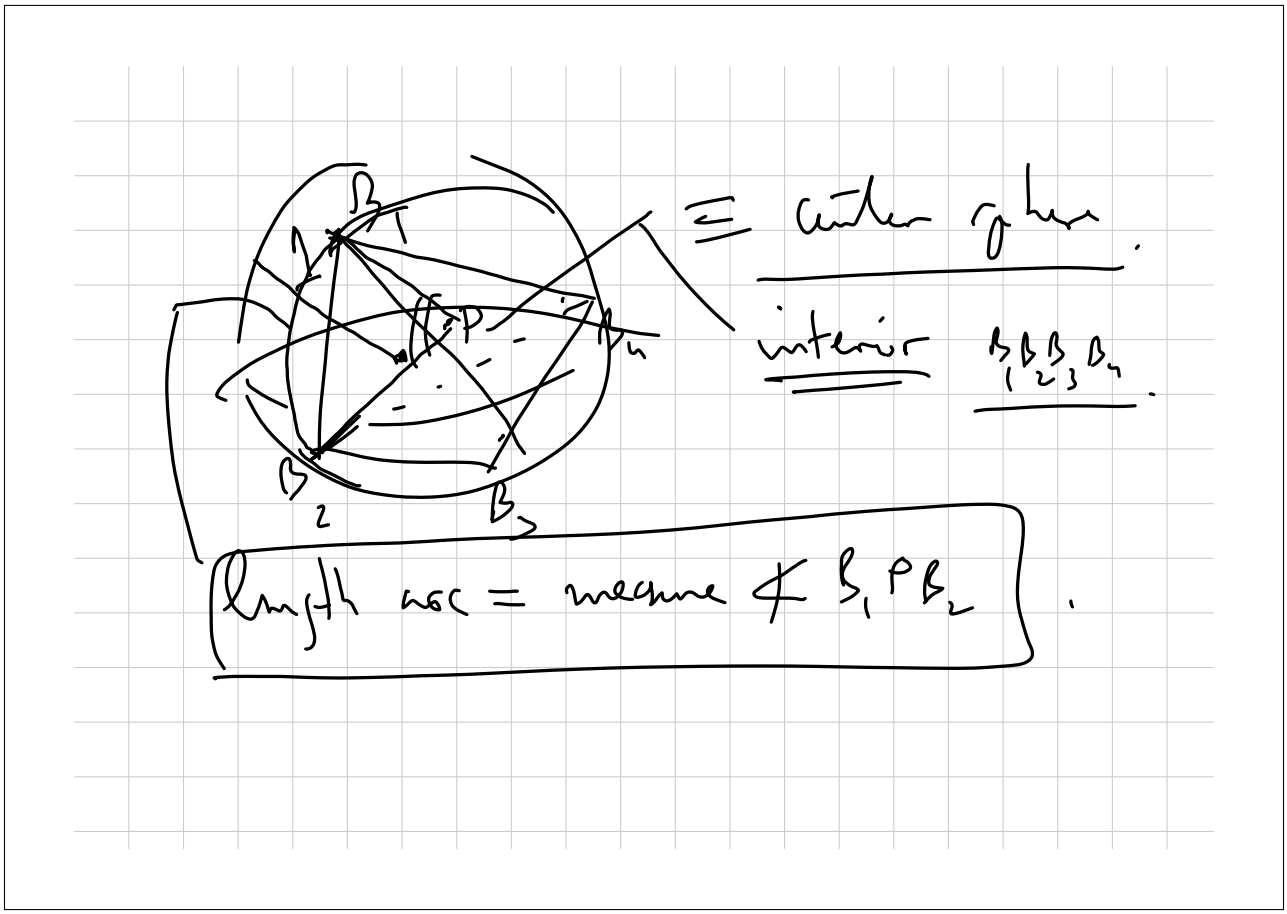
For any vertex P of a polyhedron,

$$\text{defect}(P) = 2\pi - \sum \alpha \text{ around } P > 0$$


Σ defect (P) = 4π.
Platonica.
V + F = E + 2
Σ3 (1,2,3) ≤ 2π
Σ3 (1,2,4) ≤ 2π
Σ3 (1,3,4) ≤ 4π
Σ3 (2,3,4) ≤ 4π
2S
≤ 8π
4
4π good candidate
M

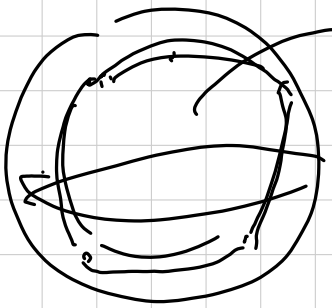

P
Q
Σ4 = A1A2 + A2A3 + A3A4 + A4A1
> 2π
(x,y,z,t) = (y,z,t,x) =
similar
S > 3π
m

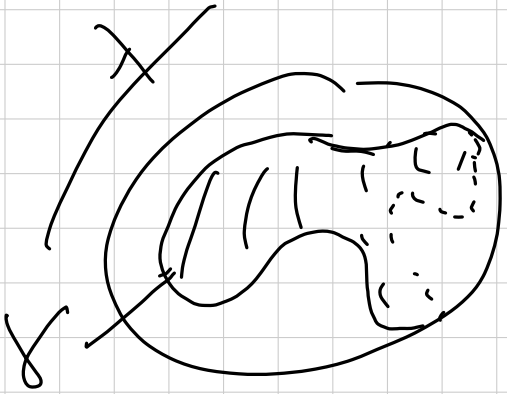

length arc
P
Δ_i
B_i


B_1
B_2
B_3
B_4
P
= center of the
interior $B_1B_2B_3B_4$.
length arc = measure of $\angle B_1PB_2$.

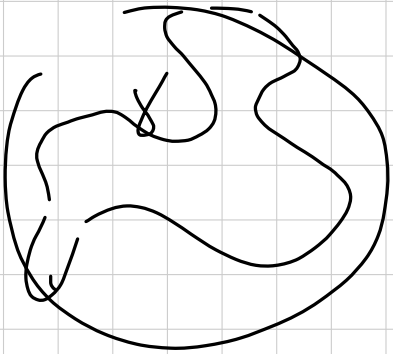
$\sum_4$ angles $= \sum_4$ lengths $\leq 2\pi$

why length $\geq 2\pi$?





Thm If length $\lambda < 2\pi \Rightarrow \gamma$ Chemin Sphere.

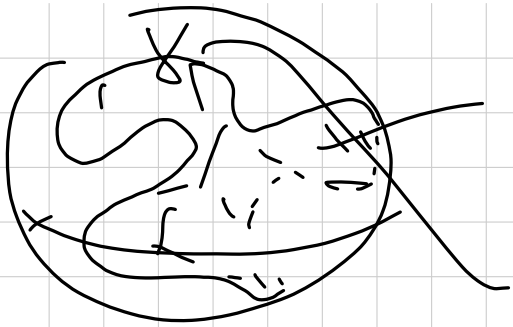


$0 \in \text{conv}(\gamma)$

$\exists x_1, x_2 - x_4$

$0 \in x_1 x_2 x_3 x_4$.

Carathéodory Theorem. Rado's Helly's.



1/2 area sphere

$\lambda \geq 2\pi$.

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

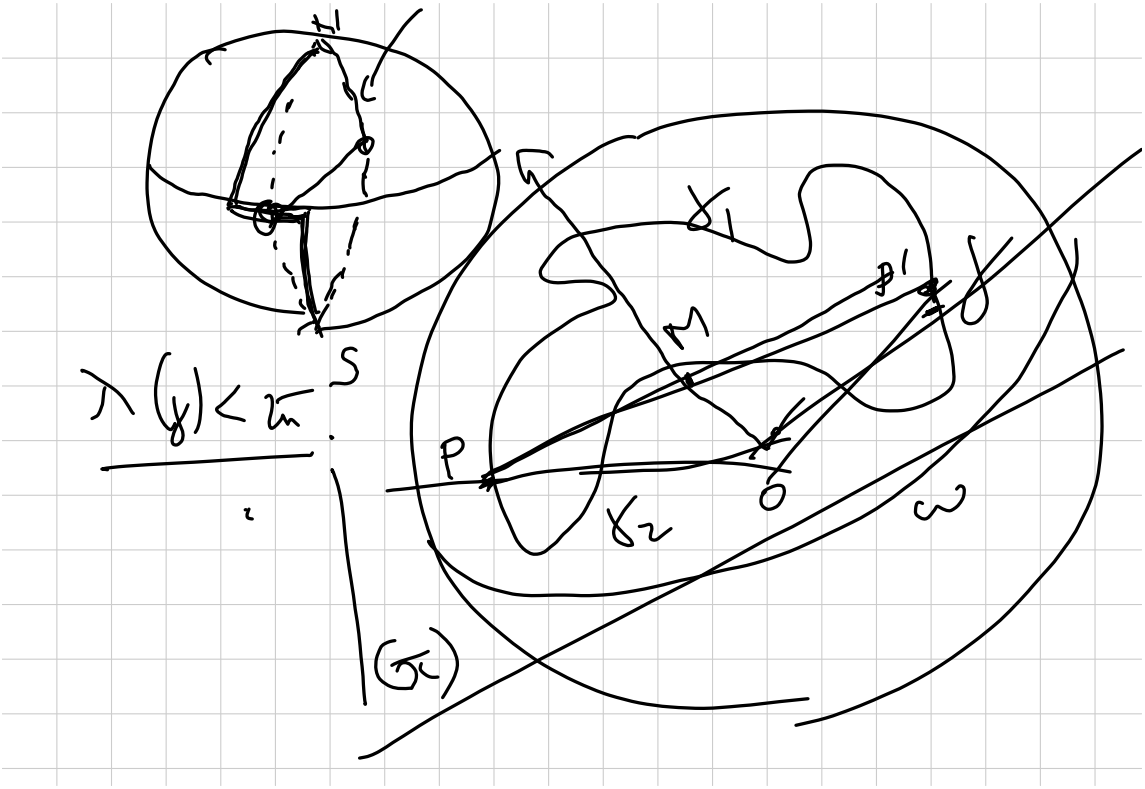
$P \longrightarrow$ antipodal point.

$\varphi^2 = id$.

γ colored red. $\varphi(\gamma)$ blue

red

$\gamma \cap \varphi(\gamma) \neq \emptyset$ ($\geq$ 2 points)



$\gamma_1 \cap \omega \neq \phi$ — X

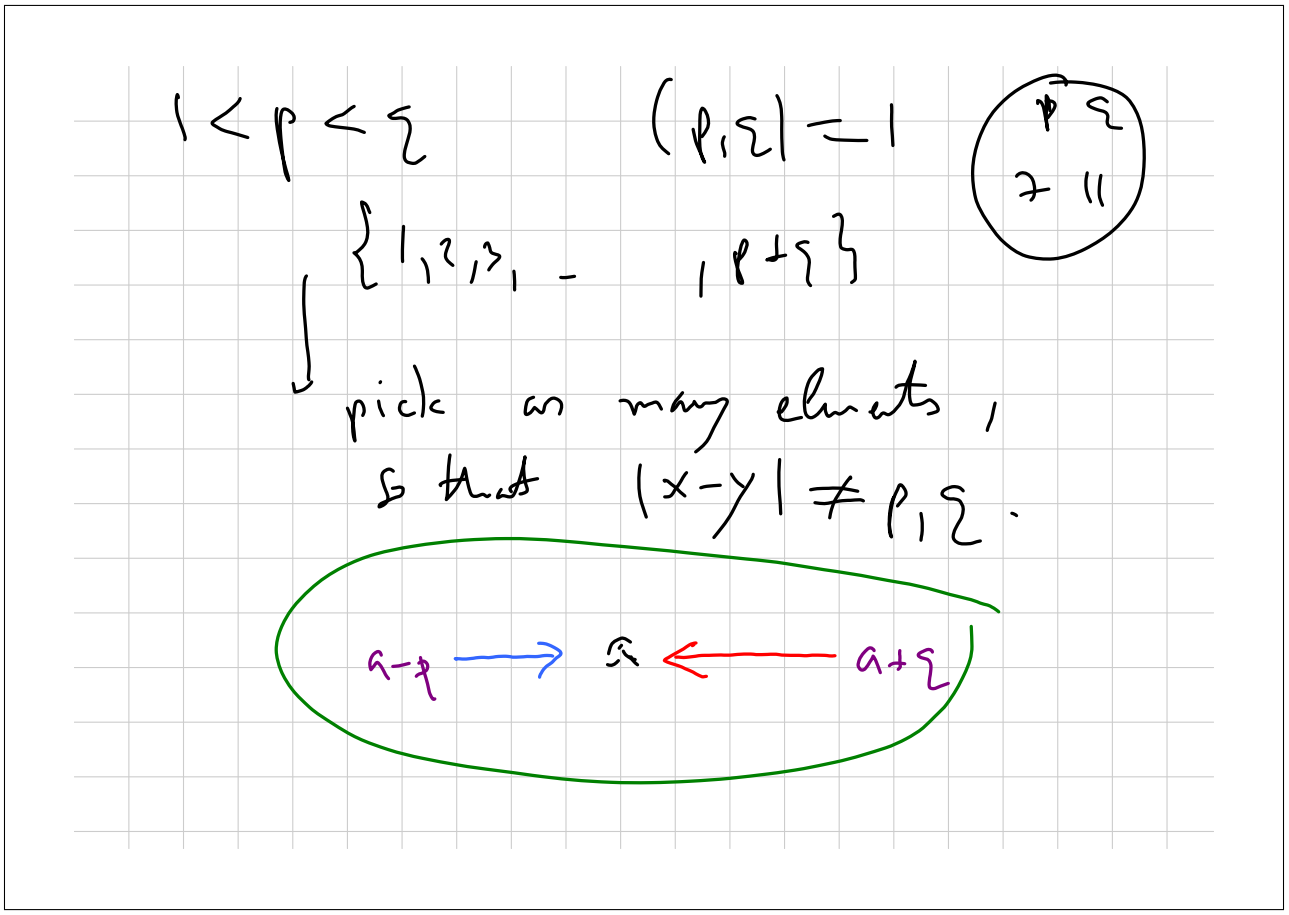
↓ sym. wrt ω — $\gamma_1' \neq \gamma_2$

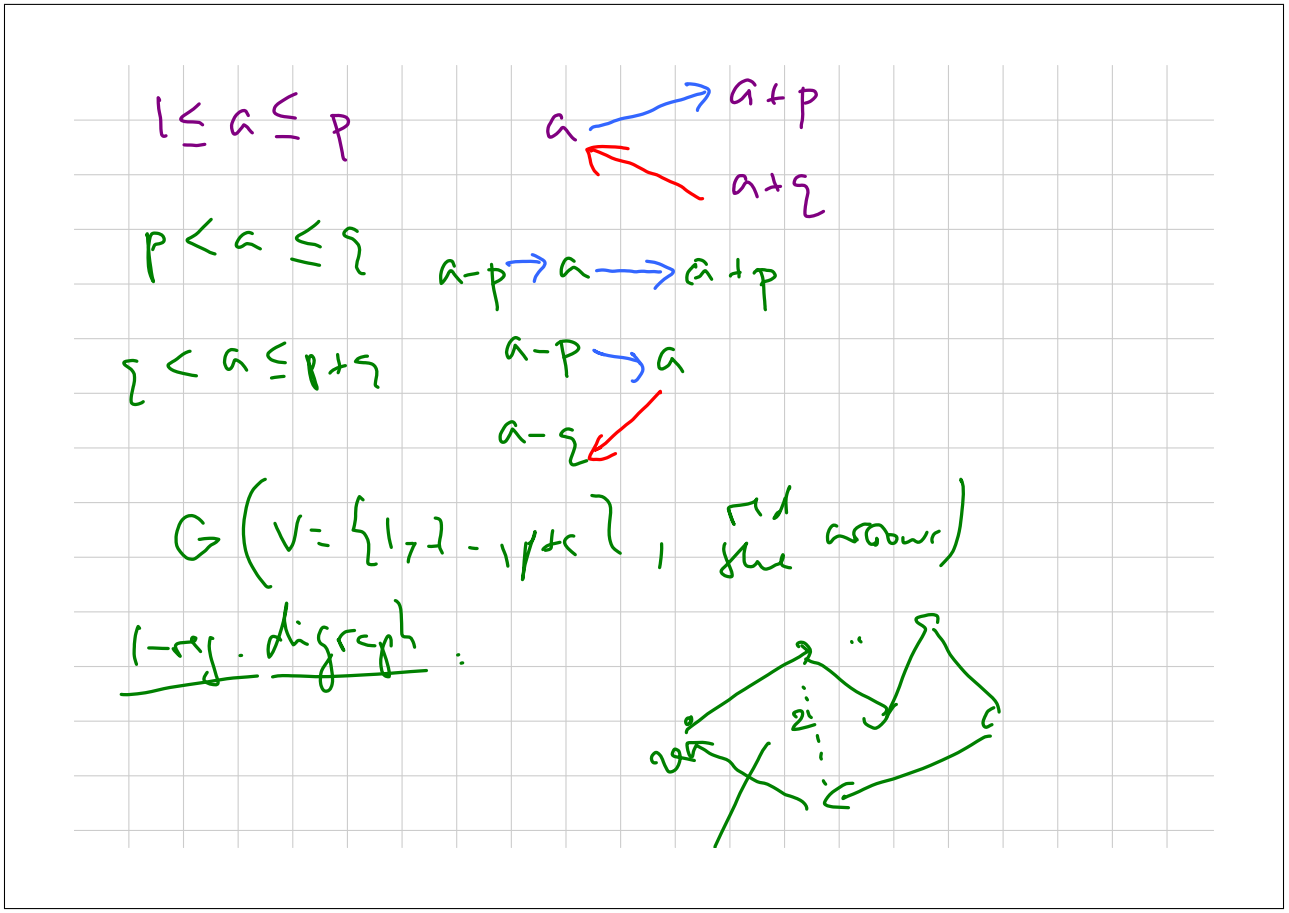
$\lambda(\gamma_1') = \lambda(\gamma_1) = \frac{1}{2}\lambda(\gamma)$

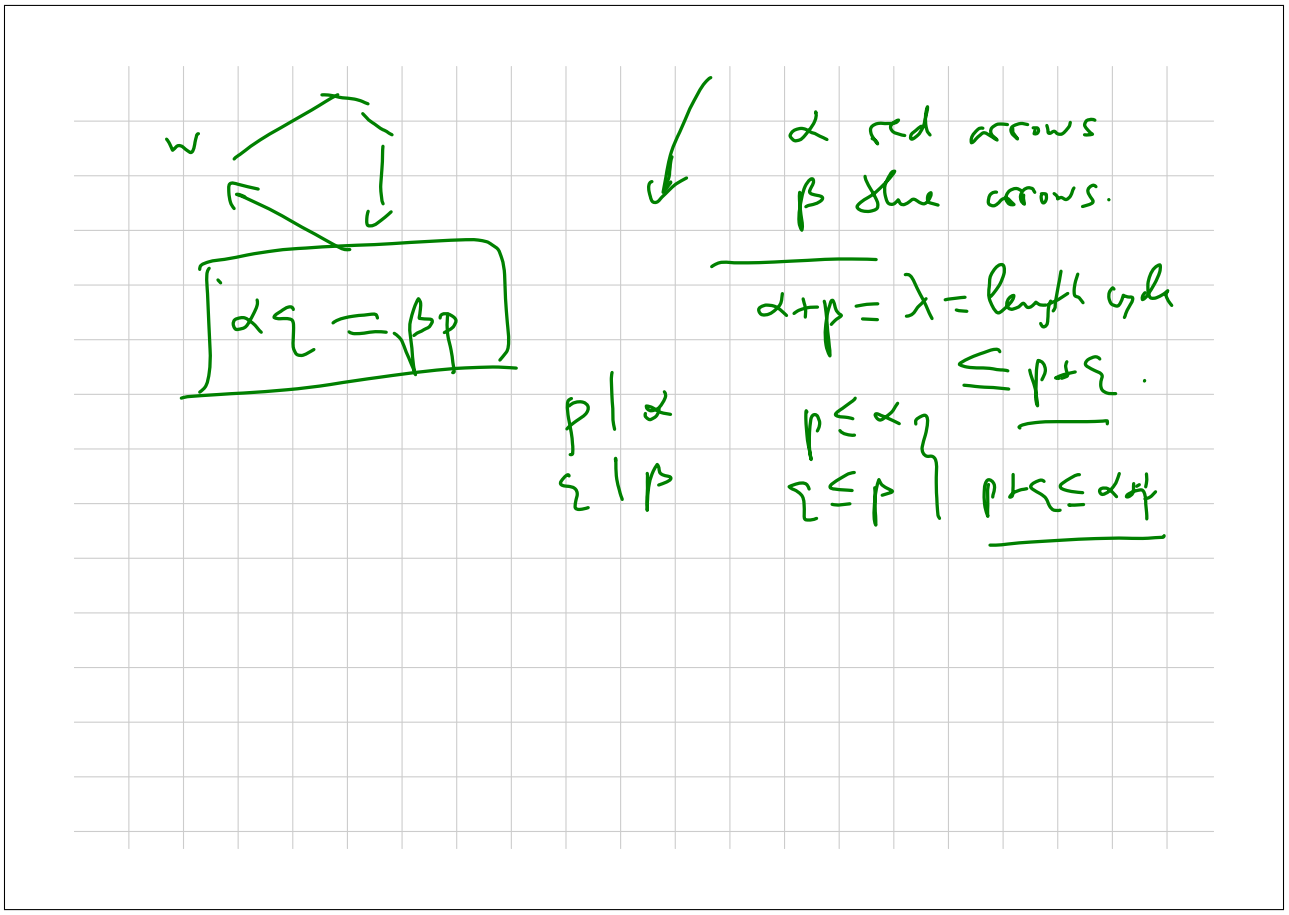
$\gamma_1' \cap \omega \neq \phi$ — X' are opposite (antipodes)

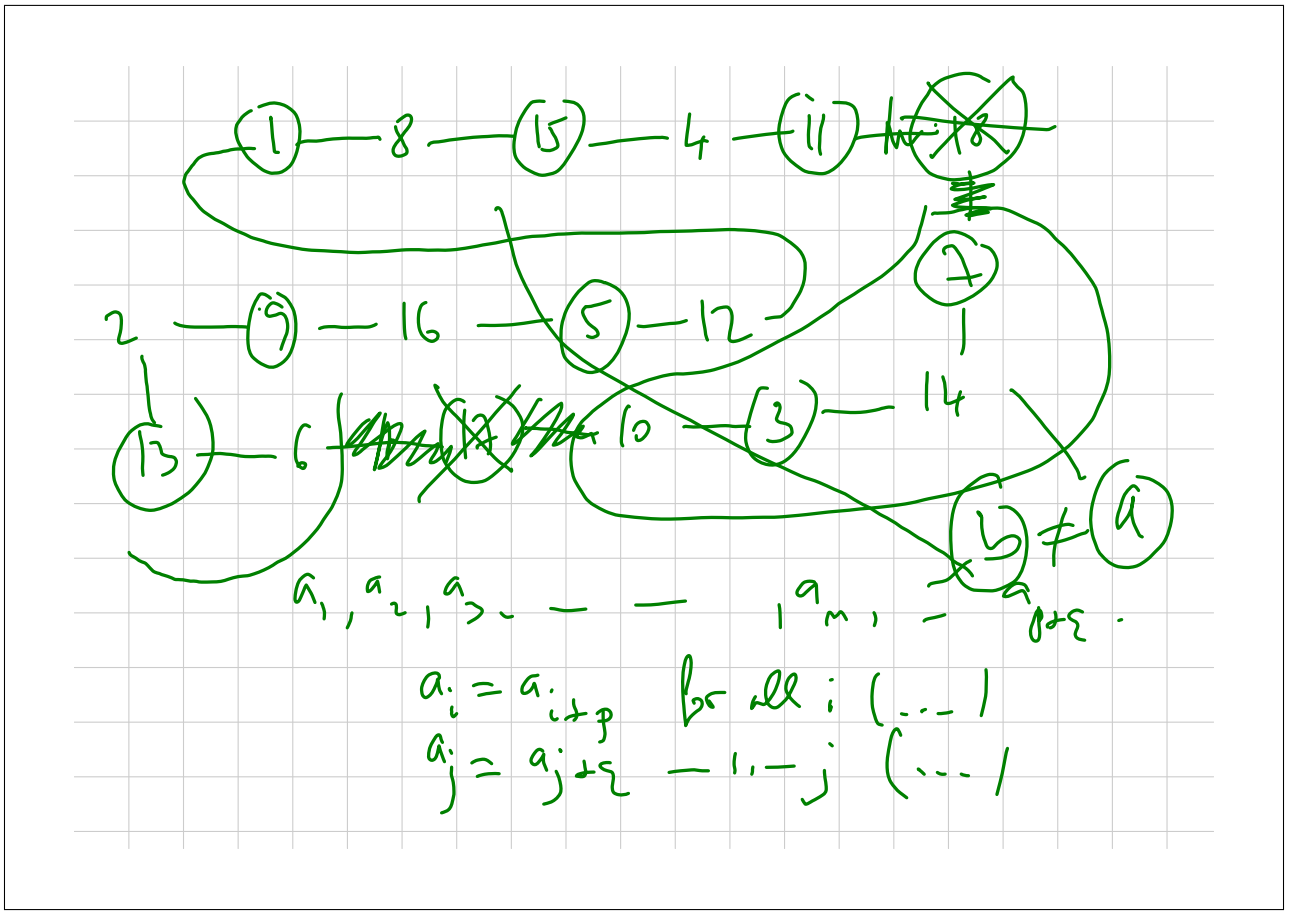
$\gamma_1 \cup \gamma_1' = \gamma'$ — $\lambda(\gamma') = \lambda(\gamma) < \pi$

containing a pair of


1 < p < q
(p,q) = 1
{1, 2, 3, ... , p+q}
pick as many elements,
s.t. that |x-y| ≠ p, q.
a-p
a
a+q


1 ≤ a ≤ p
a
a+p
a+q
p < a ≤ q
a-p
a
a+p
q < a ≤ p+q
a-p
a
a-q
G (V = {1, 2, ... , p+q}, the arrows)
1-reg. digraph.


w
$\alpha\xi = \beta\rho$
α red arrows
β blue arrows.
$\alpha+\beta = \lambda$ = length cycle
$\leq \rho+\xi$.
$p \mid \alpha$
$\xi \mid \beta$
$p \leq \alpha$
$\xi \leq \beta$
$\rho+\xi \leq \alpha+\beta$


$a_1, a_2, a_3, \ldots, a_m, \ldots$ $\rho+\xi$.
$a_i = a_{i+\rho}$ for all i (...)
$a_j = a_{j+\xi}$ — i, — j (...)

For $1 < p, q$, $(p, q) = 1$

i) There is no sequence of $pq-1$ terms (or longer) periodic of both p and q, s.t. $\neq$ constant.

ii) For $pq-2$ terms there exists and. a sequence. (using 2 values for terms).

Wilf–Fine Theorem.

$x_1, x_2, \ldots, x_n$ — numbers.

— sum of any consecutive (7) > 0 ?

— sum of any — " — (11) < 0.

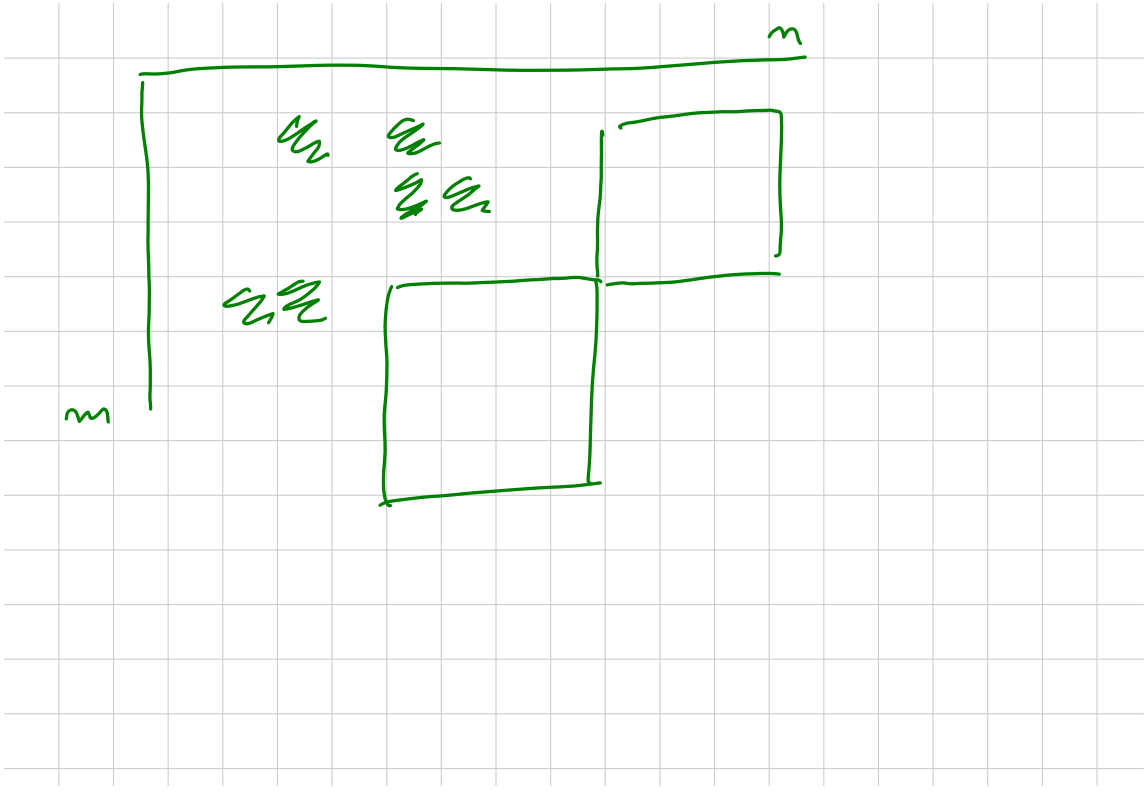
Cannot $n = pq-1$ (or larger)

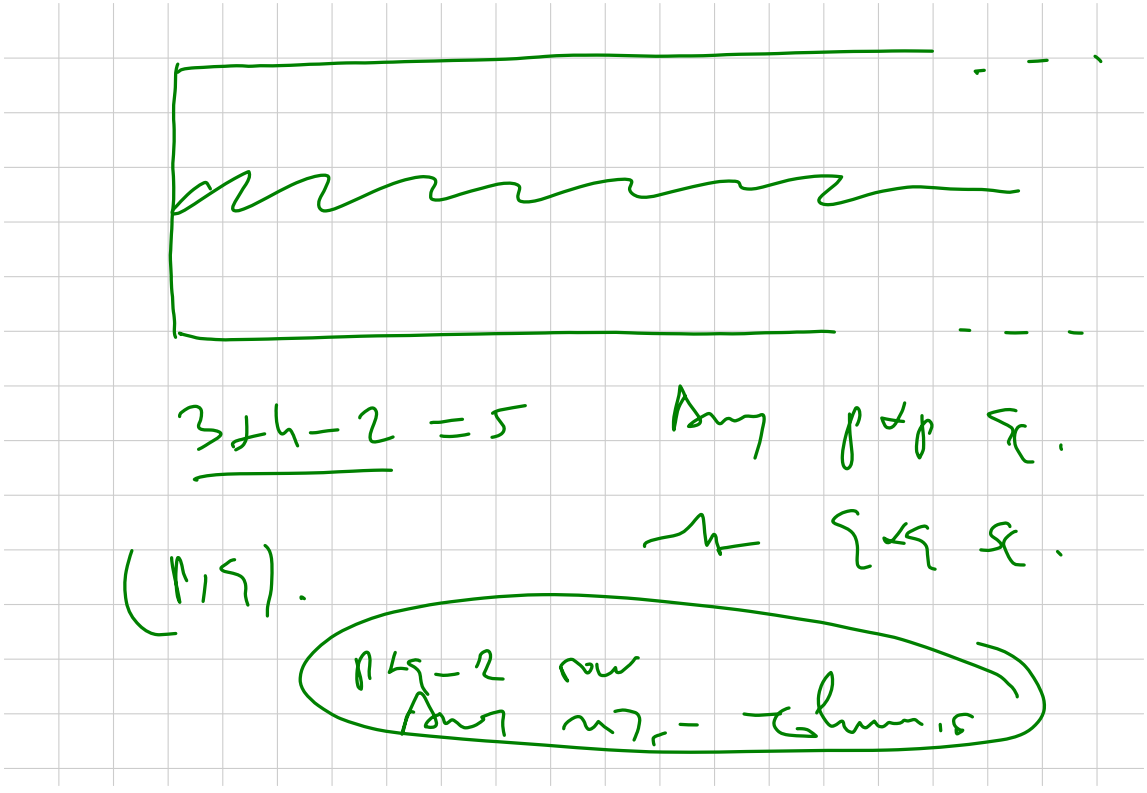
But can $n = pq-2$.

~~$a = x$~~ ~~$b = y$~~

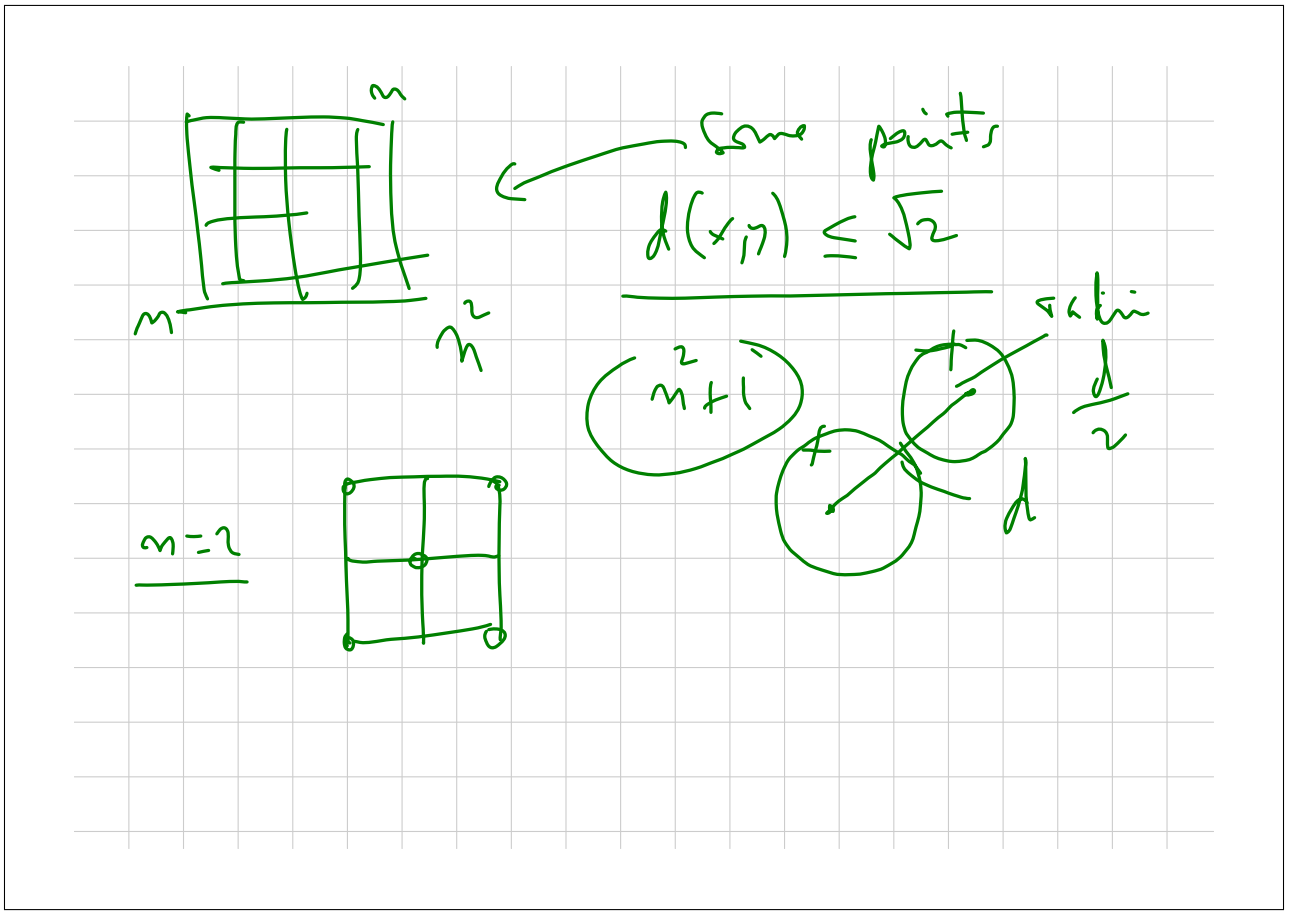
Some elem. $= a$

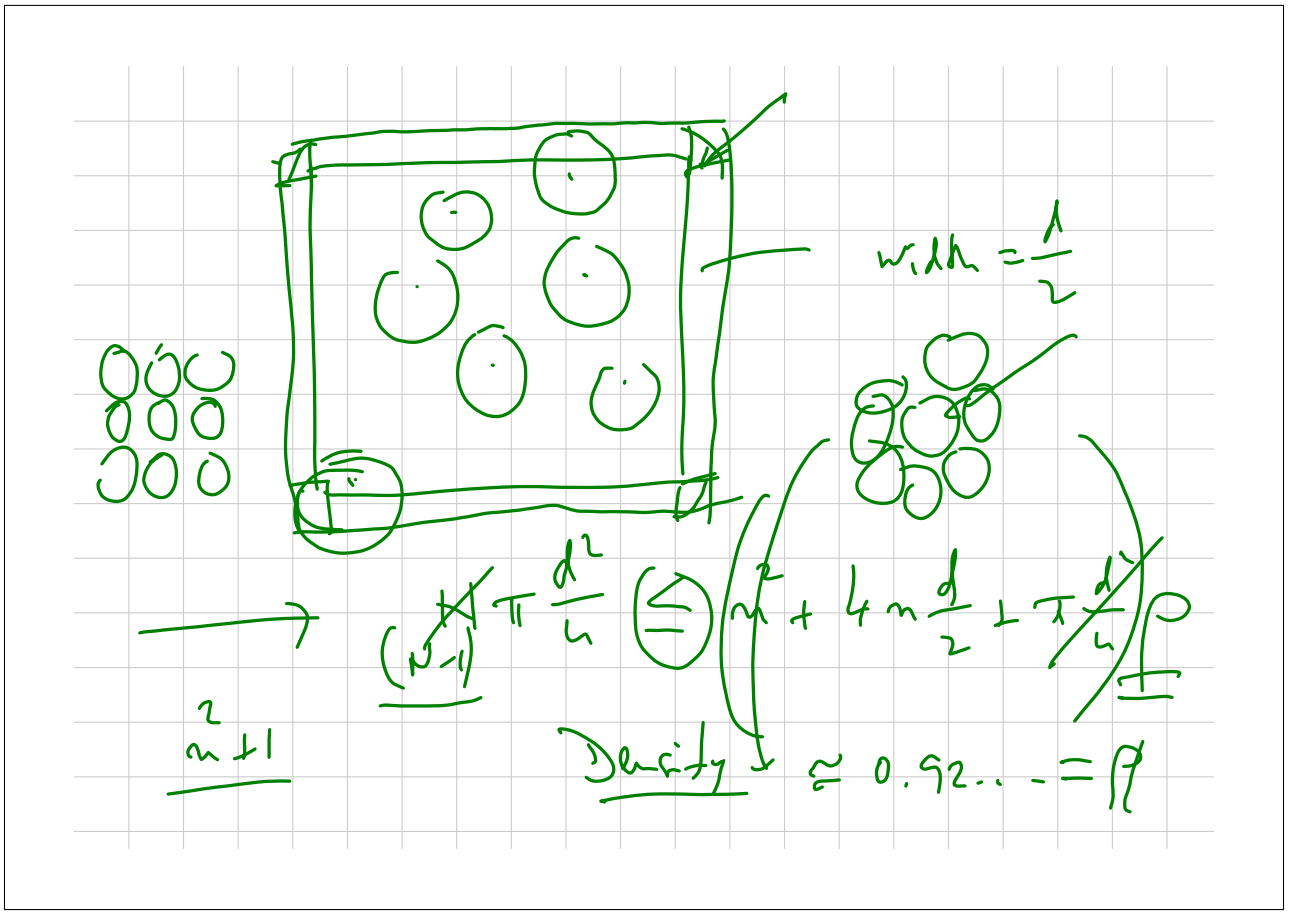
rest $= b$

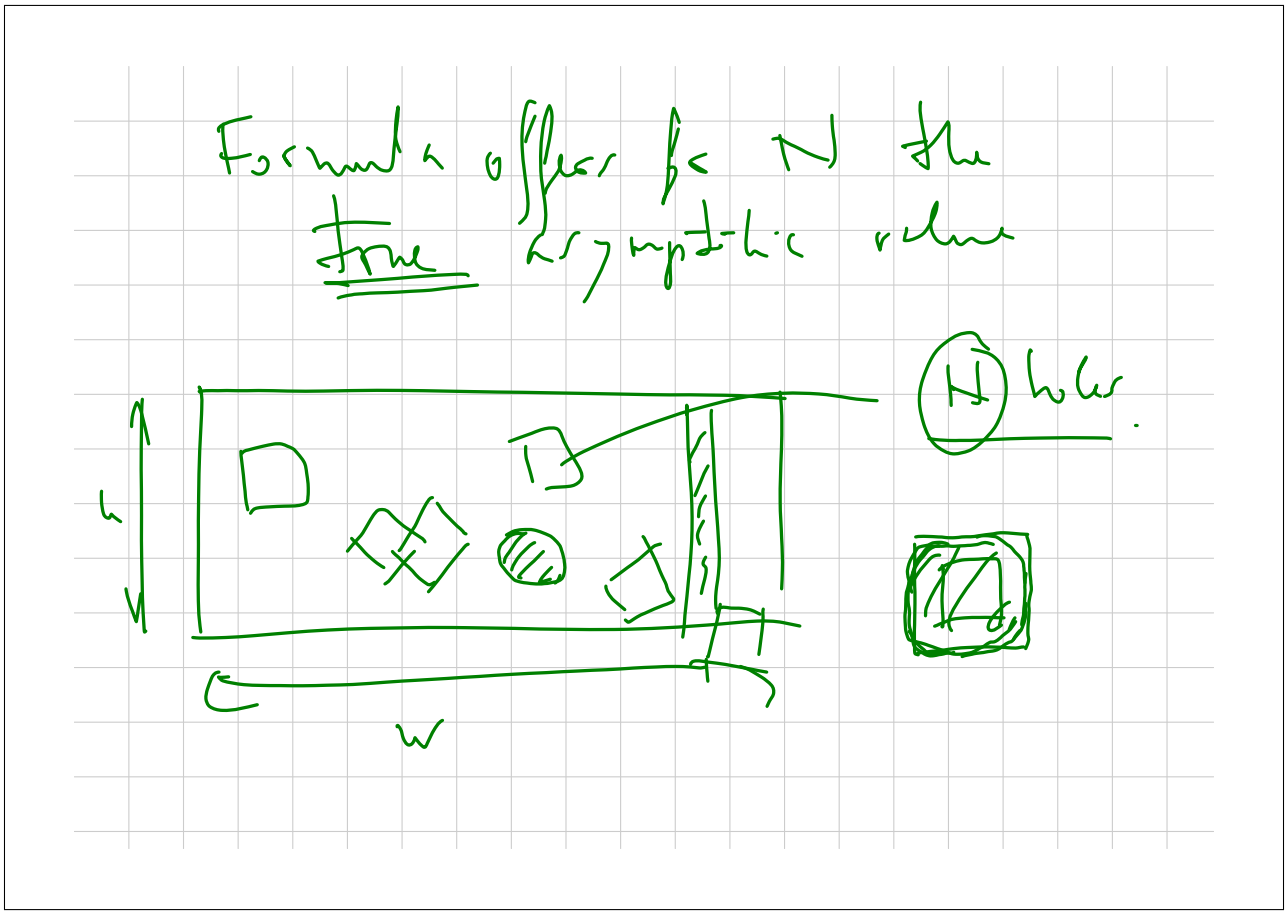




Combinatoria 3 (Advanced) – Dan Schwarz


n
n
n²
Some points
d(x,y) ≤ √2
n²+1
d/2
d
n=2


width = 1/2
(n-1)π d²/4 ≤ n² + 4n d/2 + π d²/4
n²+1
Density ≃ 0.92... = β


Formula offers for N the
true asymptotic value
H holes.
h
w

G1 - Advanced - BARICENTRICHE & co.

Titolo nota 02/09/2013

$$\mathbb{R}^n = \{(x_1, \dots, x_n) \mid x_1, \dots, x_n \in \mathbb{R}\}$$

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$

$$\lambda \cdot (x_1, \dots, x_n) = (\lambda x_1, \dots, \lambda x_n) \qquad \lambda \in \mathbb{R}$$

Oss: $\mathbb{K}$ somma, prodotto, ogni el. ha un opposto e ogni el $\neq 0$ ha un inverso [e le due operazioni di $+, \cdot$ sono commutative e associative] ($\mathbb{K}$ si chiama CAMPO)

$$\mathbb{K}^n = \{(x_1, \dots, x_n) \mid x_1, \dots, x_n \in \mathbb{K}\}$$

Es: $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$,

$\mathbb{F}_p = \{$ classi di resto mod $p\}$ p primo.

Oss: $\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}^2 = \{(x, y) \mid x, y \in \mathbb{Q}\}$

$(\mathbb{Q}[\sqrt{2}])^1 \quad a + \sqrt{2}b \longleftrightarrow (a, b)$

$$F : \mathbb{Q}[\sqrt{2}] \longrightarrow \mathbb{Q}^2$$

$$F\left((a+\sqrt{2}b) + (c+\sqrt{2}d)\right) = F((a+c)+\sqrt{2}(b+d)) =$$

$$= (a+c, b+d) = F(a+\sqrt{2}b) + F(c+\sqrt{2}d)$$

$q \in \mathbb{Q}$

$$F(q(a+\sqrt{2}b)) = (qa, qb) = q \cdot F(a+\sqrt{2}b)$$

$$F\left((a+\sqrt{2}b)(c+\sqrt{2}d)\right) = F(ac+2bd+\sqrt{2}(bc+ad)) =$$

$$= (ac+2bd, bc+ad)$$

$$\mathbb{Q}[\sqrt{2}]^5 \longrightarrow \mathbb{Q}^{10}$$

$\uparrow$

$$F : \mathbb{K}^n \longrightarrow \mathbb{K}^m$$

1) $F((x_1,\dots,x_n) + (y_1,\dots,y_n)) = F(x_1,\dots,x_n) + F(y_1,\dots,y_n)$

2) $F(\lambda(x_1,\dots,x_n)) = \lambda F(x_1,\dots,x_n)$

F lineare

Es: $f: \mathbb{R} \to \mathbb{R}$ lineare $\iff f(x) = ax$

$g(x) = ax + b$

$g(\lambda x) = a\lambda x + b \neq \lambda g(x) = \lambda a x + \lambda b$

In generale: $F: \mathbb{R}^3 \to \mathbb{R}^2$ lineare

$$F(x_1, x_2, x_3) = (a_{11}x_1 + a_{12}x_2 + a_{13}x_3,\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3)$$

Con $a_{ij} \in \mathbb{R}$

$$F\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 \end{pmatrix}$$

e_j = n-upla di zeri ed uno formata da tutti 0 e uno 1 in pos. j-esima

$\mathbb{Q}^5$ $\begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix}$ $\begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix}$ $\begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix}$ $\begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix}$ $\begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix}$

$\mathbb{Q}^5$ e_1 e_2 e_3 e_4 e_5

$\Downarrow$

$x = q_1 e_1 + q_2 e_2 + q_3 e_3 + q_4 e_4 + q_5 e_5$

scrittura unica

Base = ins. di vettori $v_1, \dots, v_k$ t.c. ogni altro v si scrive

$$v = \lambda_1 v_1 + \dots + \lambda_k v_k$$

in maniera unica!

Fatto: due basi dello stesso sp. vett. hanno la stessa cardinalità.

Def: $v_1, \dots, v_k$ sono linearmente dipendenti se $\exists\, \lambda_1, \dots, \lambda_k$ non tutti nulli t.c.

$$\lambda_1 v_1 + \dots + \lambda_k v_k = 0.$$

Es: $\exists\, a(x), b(x), c(x), d(x)$ t.c.

$$1 + xy + x^2y^2 = a(x)c(y) + b(x)d(y) \;?$$

$y=0 \qquad 1 = a(x)c(0) + b(x)d(0)$

$y=1 \qquad 1+x+x^2 = c(1)a(x) + d(1)b(x)$

$y=-1 \qquad 1-x+x^2 = c(-1)a(x) + d(-1)b(x)$

$$1 = \lambda a(x) + \mu b(x)$$
$$x = \ell a(x) + m b(x)$$
$$x^2 = L a(x) + \Pi b(x)$$

$\lambda, \mu, \ell, m, L, \Pi \in \mathbb{R}$

$\{p(x) \in \mathbb{R}[x],\ \deg p \le 2\} \cong \mathbb{R}^3$

<u>Fatto</u>: in $\mathbb{K}^n$ ogni base ha n elem.

Se ho $m < n$ vettori $\Rightarrow$ non posso scrivere <u>tutti</u> gli altri in funzione di loro.

Se ho $m > n$ vettori $\Rightarrow$ sono lin. dip.

— ∘ —

<u>Es</u>: n abitanti m società sportive.
Ogni società ha num. dispari di membri.
2 ogni società hanno in comune un num. pari di membri. $\Rightarrow m \le n$

1. numeriamo gli abitanti da $1 .. n$
2. società $\longleftrightarrow$ ($\begin{matrix} 1 \\ \vdots \\ 1 \text{ se } j \in \text{società} \\ \vdots \\ 0 \text{ se } j \notin \text{società} \end{matrix}$) $\in \mathbb{F}_2^n$

1 se $j \in$ somma

$s \in \mathbb{F}^n \qquad s \cdot s = 1$ (prodotto scalare $x \cdot y = \sum x_i y_i$)

$s, s' \in \mathbb{F}^n$

$s \neq s' \qquad s \cdot s' = 0$

$s^1, \dots, s^m \qquad s^i \cdot s^i = 1$

$s^i \cdot s^j = 0$

Se $m > n$, allora $\exists\, c_1, \dots, c_m \in \mathbb{F}_2$ t.c. (non tutti nulli)

$c_1 \cdot s^1 + \dots + c_m s^m = 0$

$0 = s^j \cdot (c_1 s^1 + \dots + c_m s^m) = c_j \qquad \forall j$

$\Rightarrow$ assurdo $\Rightarrow m \leq n$.

$(x_1, y_1) \in \mathbb{R}^2 \qquad \|(x_1, y_1)\| = \sqrt{x_1^2 + y_1^2}$

$(x_2, y_2) \in \qquad \|(x_2, y_2)\| = \sqrt{x_2^2 + y_2^2}$

$\frac{1}{2}\left((x_1 - x_2)^2 + (y_1 - y_2)^2 - x_1^2 - x_2^2 - y_1^2 - y_2^2\right)$

$= -x_1 x_2 - y_1 y_2 = -\|\bullet\| \cdot \|\bullet\| \cdot \cos\widehat{\ }$

$\mathbb{R}^{10}$ $\quad V = \{(x, y, 0, \dots, 0) \mid x, y \in \mathbb{R}\}$

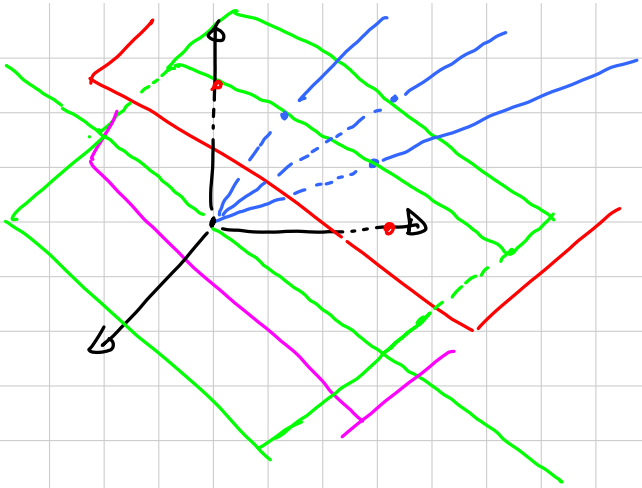
Coord. omogenee

$[x, y, z] = \{(kx, ky, kz) \in \mathbb{R}^3, k \in \mathbb{R}^*\}$

Terne omogenee

$(x, y, z) \neq (0, 0, 0)$

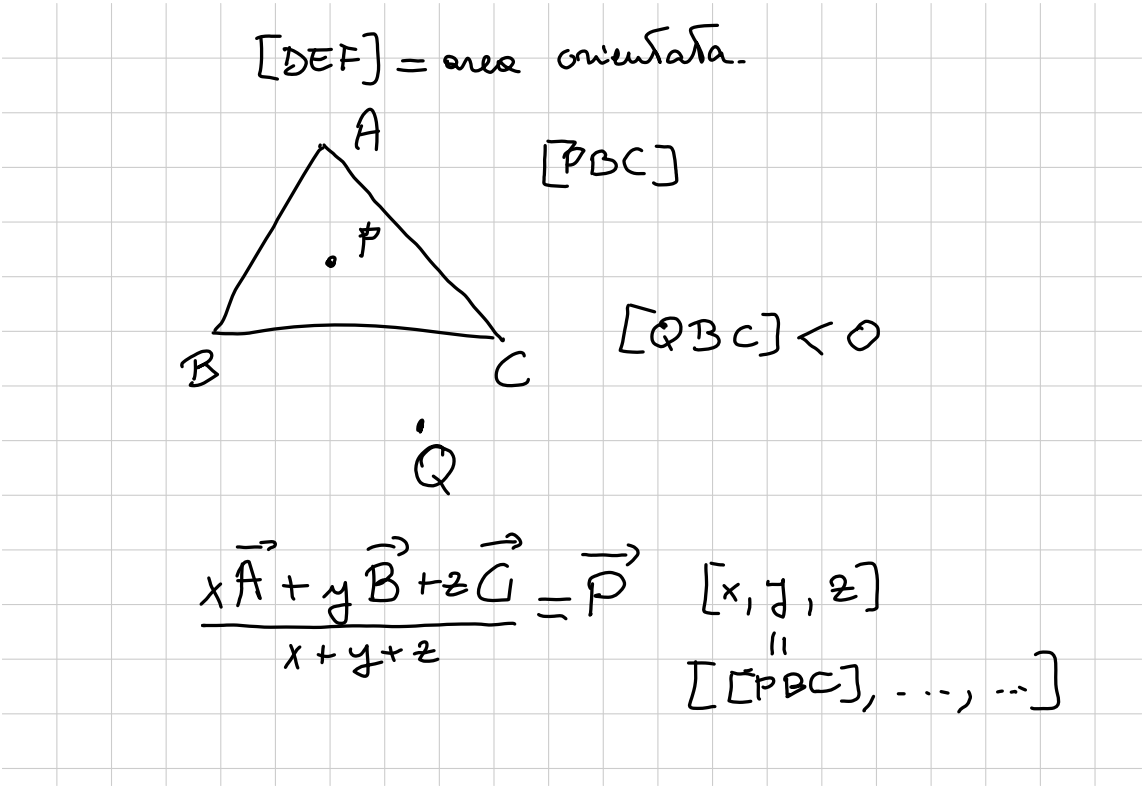
$\{[x, y, z], (x, y, z) \in \mathbb{R}^3 \setminus \{0\}\}$



Coord. baricentriche

ABC triangolo

$P \longrightarrow [[PBC], [APC], [ABP]]$


[DEF] = area orientata.
A
P
B
C
Q
[PBC]
[QBC] < 0
$\frac{x\vec{A} + y\vec{B} + z\vec{C}}{x+y+z} = \vec{P}$
[x, y, z]
=
[[PBC], ..., ...]

G2 Advanced – Sam

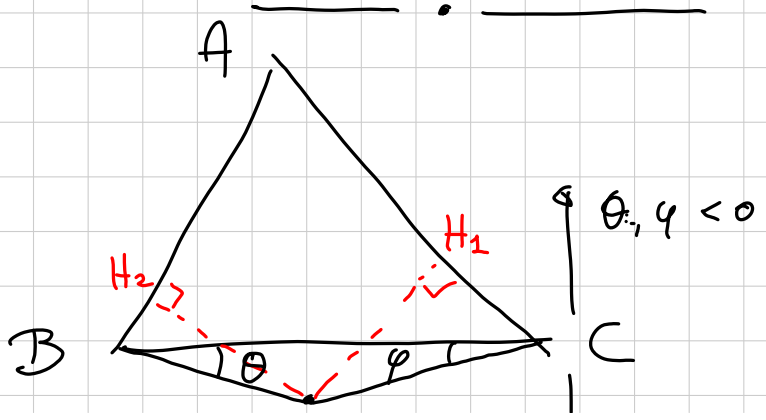
Titolo nota 03/09/2013

- Algebra lineare
  - $\mathbb{R}^n$
  - $T: \mathbb{R}^k \to \mathbb{R}^m$ lineare
  - Prodotto righe × colonne
  - Basi & indip. lineare
  - Determinante
- Coord. baricentriche
  - Vari punti
  - Rette
  - Circonferenze

$[-1:-1:-1] = [1:1:1]$

$[-1:1:1] = [1:-1:-1]$

$[ABP] + [APC] + [PBC] = [ABC]$



P PH_2 $\theta, \varphi > 0$

$$[ABP] = c \cdot \overbrace{BP \cdot \sin(\beta+\theta)}^{PH_2} \qquad \frac{BP}{CP} = \frac{\sin\varphi}{\sin\theta}$$

$$[APC] = b \cdot \underbrace{CP \cdot \sin(\gamma+\varphi)}_{PH_2}$$

$$\frac{[ABP]}{[APC]} = \frac{c}{b} \cdot \frac{BP}{CP} \cdot \frac{\sin(\beta+\theta)}{\sin(\gamma+\varphi)} =$$

$$= \frac{\sin\gamma}{\sin\beta} \cdot \frac{\sin\varphi}{\sin\theta} \cdot \frac{\sin\beta\cos\theta + \cos\beta\sin\theta}{\sin\gamma\cos\varphi + \cos\gamma\sin\varphi} =$$

$$= \frac{\cot\theta + \cot\beta}{\cot\varphi + \cot\gamma}$$

$$\frac{[ABP]}{[PBC]} = \frac{c \cdot BP \cdot \sin(\beta+\theta)}{a \cdot BP \cdot \sin\theta} = \frac{\sin\gamma}{\sin\alpha} \cdot \frac{\sin\beta\cos\theta + \cos\beta\sin\theta}{\sin\theta} =$$

$$= -\frac{\sin\gamma\sin\beta}{\sin\alpha}(\cot\beta + \cot\theta)$$

$$\frac{[APC]}{[PBC]} = -\frac{\sin\gamma\sin\beta}{\sin\alpha}(\cot\gamma + \cot\varphi)$$

$$\left[\frac{-\sin\alpha}{\sin\gamma\sin\beta},\ \cot\gamma+\cot\varphi,\ \cot\beta+\cot\theta\right]=P$$

$$2[ABC]\frac{\sin\alpha}{\sin\gamma\sin\beta}=\cancel{2}\cdot\frac{1}{\cancel{2}}bc\sin\alpha\frac{\sin\alpha}{\sin\beta\sin\gamma}=$$

$$=2R\cdot 2R\cdot\sin\alpha\cdot\sin\alpha=a^2$$

$S=2[ABC]$ (Attenti!! 2 volte l'area)

$$P=[-a^2,\ S\cot\gamma+S\cot\varphi,\ S\cot\beta+S\cot\theta]$$

$$S\cot\gamma=ab\sin\gamma\cdot\cot\gamma=ab\cos\gamma=\frac{a^2+b^2-c^2}{2}$$

$S_\theta=S\cot\theta$ $\quad S_\alpha, S_\beta, S_\gamma$

$$P=[-a^2,\ S_\gamma+S_\varphi,\ S_\beta+S_\theta]$$

Oss: 1) $S_\alpha+S_\beta=c^2$

2) $S_\alpha S_\beta+S_\beta S_\gamma+S_\gamma S_\alpha=S^2$

$$0 = tg(\alpha+\beta+\gamma) = \frac{tg(\alpha)+tg(\beta+\gamma)}{1-tg\alpha\, tg(\beta+\gamma)} =$$

$$= \frac{tg\alpha + \frac{tg\beta+tg\gamma}{1-tg\beta tg\gamma}}{1-tg\alpha\frac{tg\beta+tg\gamma}{1-tg\beta tg\gamma}} = \frac{tg\alpha+tg\beta+tg\gamma-tg\alpha tg\beta tg\gamma}{1-tg\beta tg\gamma-tg\alpha tg\beta-tg\alpha tg\gamma}$$

$$tg\alpha+tg\beta+tg\gamma = tg\alpha tg\beta tg\gamma$$

$$\frac{1}{tg\beta tg\gamma}+\frac{1}{tg\beta tg\alpha}+\frac{1}{tg\alpha tg\gamma}=1$$

$$\cot\beta\cot\gamma+\cot\beta\cot\alpha+\cot\alpha\cot\gamma=1$$

$$\boxed{S_\beta S_\gamma + S_\beta S_\alpha + S_\alpha S_\gamma = S^2}$$

Punti più o meno notevoli

$$H = [tg\alpha, tg\beta, tg\gamma] = \left[\frac{1}{S_\alpha}, \frac{1}{S_\beta}, \frac{1}{S_\gamma}\right] =$$

$$= [S_\beta S_\gamma, S_\alpha S_\gamma, S_\alpha S_\beta]$$

$$O = [a^2 S_\alpha, b^2 S_\beta, c^2 S_\gamma] =$$

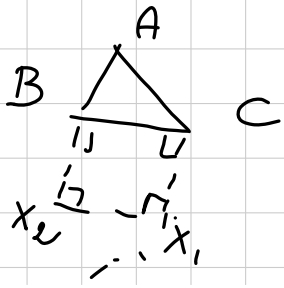
$$\sin 2\alpha = 2\sin\alpha\cos\alpha =$$

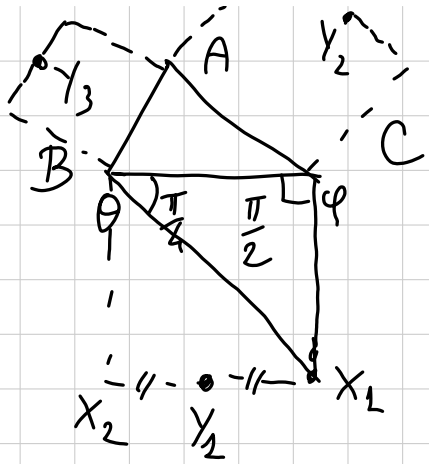
$= [S_\alpha S_\beta + S_\alpha S_\gamma, \dots, \dots] = 2\sin^2\alpha \cot\alpha$

$N = \frac{1}{2}(\vec{O}+\vec{H}) = \left[\frac{S_\alpha S_\beta + S_\alpha S_\gamma}{2} + S_\beta S_\gamma, \dots, \dots\right] =$

$= \left[\frac{S^2}{2} + \frac{S_\beta S_\gamma}{2}, \dots, \dots\right] = [S^2 + S_\beta S_\gamma, \dots, \dots]$

Esempi:





$X_2 = [-a^2, S_\gamma + \cancel{S_\varphi}, S_\beta + S_\theta]$ (11 S)

$X_1 = [-a^2, S_\gamma, S_\beta + S]$

$X_2 = [-a^2, S_\gamma + S, S_\beta]$

$Y_1 = [-a^2, S_\gamma + \frac{S}{2}, S_\beta + \frac{S}{2}]$

$Y_2 = [S_\gamma + \frac{S}{2}, -b^2, S_\alpha + \frac{S}{2}]$ $Y_3 = [S_\beta + \frac{S}{2}, S_\alpha + \frac{S}{2}, -c^2]$

Es: AY_1, BY_2, CY_3 concorrono

$$AY_1 = \left\{ \left(S_\beta + \frac{S}{2}\right) y = \left(S_\gamma + \frac{S}{2}\right) z \right\}$$

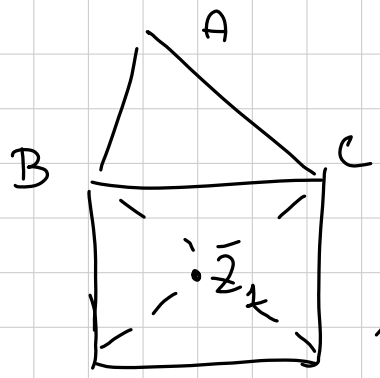
$[\bullet, r, q] \longrightarrow yq = rz$

$[r, \bullet\bullet\bullet, p] \longrightarrow xp = rz$

$[q, p, \bullet] \longrightarrow xp = yq$

le rette si incontrano in $\left[\frac{1}{p}, \frac{1}{q}, \frac{1}{r}\right]$

$$\left[\frac{1}{S_\alpha + \frac{S}{2}}, \frac{1}{S_\beta + \frac{S}{2}}, \frac{1}{S_\gamma + \frac{S}{2}}\right]$$



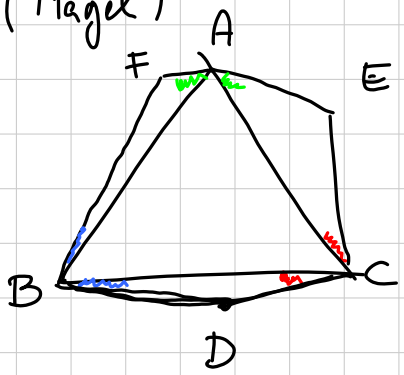
$$Z_1 = \left[-a^2, S_C + S, S_B + S\right]$$

AZ_1 BZ_2 CZ_3 concorrono in $V = \left[\frac{1}{S_A + S}, \frac{1}{S_B + S}, \frac{1}{S_C + S}\right]$

(primo) punto di Vecten (esterno)

$(AZ_1 \perp Z_2 Z_3)$

Pensata (Nagel)



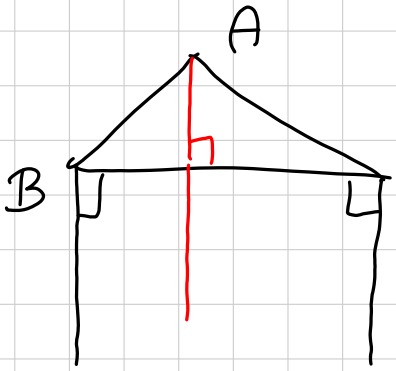
AD, BE, CF concorrono.

$$D = [-a^2, S_\gamma + S_{rosso}, S_\beta + S_{blu}]$$

$$E = [S_\gamma + S_{rosso}, -b^2, S_\alpha + S_{verde}]$$

$$F = [S_\beta + S_{blu}, S_\alpha + S_{verde}, -c^2]$$

Oss:



$$H_\infty = [-a^2, S_\gamma, S_\beta]$$

$$\det \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{S_\alpha} & \frac{1}{S_\beta} & \frac{1}{S_\gamma} \\ -a^2 & S_\gamma & S_\beta \end{pmatrix} =$$

H_∞

$= 1 - 1 = 0.$

$$[x,y,z] = \{ (kx,ky,kz) \in \mathbb{R}^3 \mid k \in \mathbb{R}^* \}$$
$$(x,y,z) \neq (0,0,0)$$

$$\mathbb{RP}^2 = \{ [x,y,z] \mid (x,y,z) \neq (0,0,0) \}$$

retta proiettiva: $\{ [x,y,z] \in \mathbb{RP}^2 \mid \ell x + my + nz = 0 \}$
per qualche $(\ell, m, n) \neq (0,0,0)$.

Passaggio da $\mathbb{RP}^2$ a $\mathbb{R}^2$

Basta togliere una retta

$$\{ \ell x + my + nz = 0 \} = r$$

$$\mathbb{RP}^2 \setminus r = \{ [x,y,z] \in \mathbb{RP}^2 \mid \ell x + my + nz \neq 0 \}$$

se $[x,y,z] \in \mathbb{RP}^2 \setminus r$

allora posso considerare $\left(\frac{x}{\ell x+my+nz}, \frac{y}{\ell x+my+nz}, \frac{z}{\dots} \right)$

$= (\tilde{x}, \tilde{y}, \tilde{z})$ $\quad \tilde{x}\ell + \tilde{y}m + \tilde{z}n = 1$

$$\mathbb{RP}^2 \setminus r = \{ [x,y,z] \in \mathbb{RP}^2 \mid \ell x + my + nz = 1 \}$$

$[x,y,z] \in \mathbb{RP}^2 \setminus \ell \longrightarrow (\tilde{x},\tilde{y},\tilde{z}) \in \mathbb{R}^3$

da sul piano

biiezione che manda rette in rette.

$\{ax+my+nz=1\}$ in $\mathbb{R}^3$

Coord. baricentriche $\cong \{x+y+z=[ABC]\}$

ES: $r = \{z=0\}$ $\quad \mathbb{RP}^2 \setminus r = \{[x,y,z] \mid z=1\}$

$[x,y,z] \longrightarrow \left(\frac{x}{z}, \frac{y}{z}, 1\right)$

Proiettività

$T: \mathbb{RP}^2 \longrightarrow \mathbb{RP}^2$

$T([x,y,z]) = [a_{11}x+a_{12}y+a_{13}z,\ a_{21}x+a_{22}y+a_{23}z,$
$a_{31}x+a_{32}y+a_{33}z] =$

$= \left[\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} \right]$

A

T è iniettiva $\Updownarrow$ T è surjettiva

Teo: Dati 4 punti A, B, C, D a 3 a 3 non allineati, $\exists\, T: \mathbb{RP}^2 \longrightarrow \mathbb{RP}^2$ t.c.

$T([1,0,0]) = A \quad T([0,0,1]) = C$

$T([0,1,0]) = B \quad T([1,1,1]) = D.$

T è biiettiva $\Leftrightarrow$ $\det A \neq 0$.

Dim: $A = [a_1, a_2, a_3]$ B, C, D analoghi

$$M = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$$

$$M \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \quad M \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} \quad M \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}$$

$$M_{hkj} = \begin{pmatrix} ha_1 & kb_1 & jc_1 \\ ha_2 & kb_2 & jc_2 \\ ha_3 & kb_3 & jc_3 \end{pmatrix} \quad M_{hkj} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} ha_1 + kb_1 + jc_1 \\ ha_2 + kb_2 + jc_2 \\ ha_3 + kb_3 + jc_3 \end{pmatrix}$$

$$\begin{cases} ha_1 + kb_1 + jc_1 = d_1 \\ ha_2 + kb_2 + jc_2 = d_2 \\ ha_3 + kb_3 + jc_3 = d_3 \end{cases} \qquad \det \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} \neq 0.$$

$\Leftrightarrow$

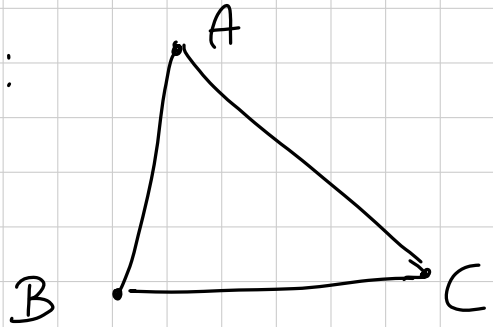
$\exists\, h, k, j$ che risolvono. unici.

$\Rightarrow T([x,y,z]) = \left[M_{hkj} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \right]$. $\square$

Oss: Inverso di una proiettività è una proiettività.

Oss 2: Date due quaterne di pt. a 3 a 3 non allineati: ∃ proiettività che manda l'una nell'altra

Es:



$\mathbb{RP}^1 = \{[x,y] \mid (x,y) \in \mathbb{R}^2 \setminus \{0\}\}$

$T : \mathbb{RP}^1 \to \mathbb{RP}^1$ proj.

$T([x,y]) = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}\right]$

Quando 3 quaterne pt. distinti in 3 altre quaterne pt. distinti

---

$\mathcal{Y} = \{\text{rette per } A\} = \{\{\lambda y = \mu z\},\ (\lambda,\mu) \neq (0,0)\}$

$f : \mathbb{RP}^1 \longrightarrow \mathcal{Y}$ bigettiva.

$[\lambda,\mu] \longrightarrow \{\lambda y = \mu z\}$

$S : \mathcal{Y} \to \mathcal{Y}$ simmetria rispetto alla bisettrice interna.

$S(\{cy = bz\}) = \{cy = bz\}$ $\quad \{cy'' = bz\}$

$S(\{cy = -bz\}) = \{cy = -bz\}$

$S(\{y = 0\}) = \{z = 0\}$

$$\begin{array}{ccc} \mathcal{Y} & \xrightarrow{S} & \mathcal{Y} \\ f \uparrow & & \downarrow f^{-1} \\ \mathbb{RP}^2 & \xrightarrow{T} & \mathbb{RP}^1 \end{array}$$

$T([\lambda,\mu]) = ?$

$T([c,b]) = [c,b]$

$T([c,-b]) = [c,-b]$

$T([1,0]) = [0,1]$

$T([0,1]) = [1,0]$

$\begin{pmatrix} 0 & h \\ k & 0 \end{pmatrix}\begin{pmatrix} c \\ b \end{pmatrix} = \begin{pmatrix} bh \\ ck \end{pmatrix} \Longleftarrow \text{“}\begin{pmatrix} c \\ b \end{pmatrix}$

$h = \frac{c}{b}$

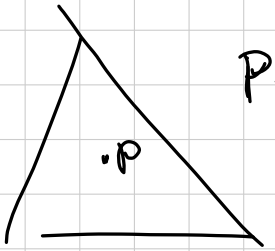
$k = \frac{b}{c}$

$\begin{pmatrix} 0 & \frac{c}{b} \\ \frac{b}{c} & 0 \end{pmatrix}\begin{pmatrix} c \\ -b \end{pmatrix} = \begin{pmatrix} -c \\ b \end{pmatrix}$

Data la retta $\{\lambda y = \mu z\}$ la sua antiv. rsp. alla bisettrice è

$$\left\{\frac{c}{b}\mu y = \frac{b}{c}\lambda z\right\} = \left\{c^2\mu y = b^2\lambda z\right\} =$$

$$= \left\{\frac{c^2}{\lambda} y = \frac{b^2}{\mu} z\right\}$$



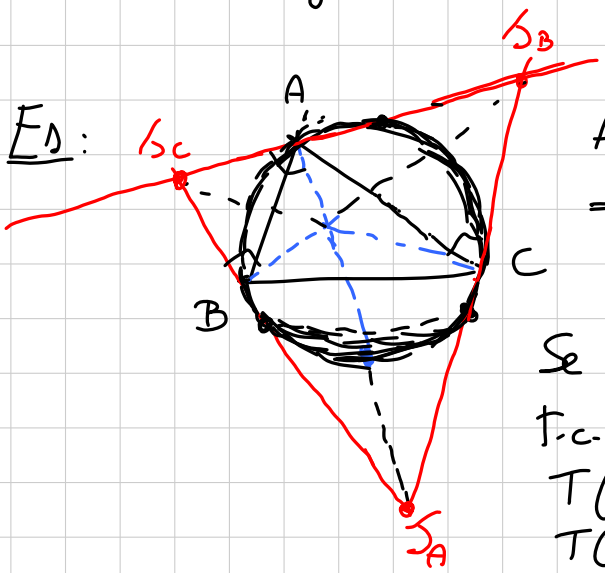
$P = [u, v, w]$

$wy = zv \longrightarrow \frac{c^2}{w} y = \frac{b^2}{v} z$

$wx = zu \longrightarrow \frac{c^2}{w} x = \frac{a^2}{u} z$

$vx = yu \longrightarrow \frac{b^2}{v} x = \frac{a^2}{u} y$

$\Rightarrow$ coord. isog. di P è $\left[\frac{a^2}{u}; \frac{b^2}{v}, \frac{c^2}{w}\right]$.



Es: ABC tri. ortico di $\gamma_A\gamma_B\gamma_C$
$\Rightarrow O$ è centro della circ. di Feuerbach di $\gamma_A\gamma_B\gamma_C$.

Se ho una proiettività t.c.
$T([1,0,0]) = [-a, b, c]$
$T([0,1,0]) = [a, -b, c]$
$T([0,0,1]) = [a, b, -c]$

$T(H) = I$
$T(O) \stackrel{?}{=} N$

Fatto: Le proiettività conservano il birapporto.

Es: $\mathcal{F} = \{\text{rette per } A\}$ $P: \mathcal{F} \to \mathcal{F}$
$r \to$ retta $\perp r$

è una proiettività?

$[c, b] \to [c, -b]$
$[c, -b] \to [c, b]$

altezza da A $\left\{\frac{u}{s_\gamma} = \frac{z}{s_\beta}\right\}$
Caso speciale $\{x = 0\}$

$[1,-1] \mapsto \left[\frac{1}{S_\gamma}, \frac{1}{S_\beta}\right] \Rightarrow$ p. all'∞ $\in [0,1,-1]$

$\parallel$ a BC per A $\{y=-z\}$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} c \\ b \end{pmatrix} = \begin{pmatrix} a_{11}c + a_{12}b \\ a_{21}c + a_{22}b \end{pmatrix} = \lambda\begin{pmatrix} c \\ -b \end{pmatrix}$$

$$\begin{pmatrix} a_{11}c - a_{12}b \\ a_{21}c - a_{22}b \end{pmatrix} = \mu\begin{pmatrix} c \\ b \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & -a_{12} \\ a_{21} & -a_{22} \end{pmatrix} = \nu\begin{pmatrix} S_\beta \\ S_\gamma \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} c^2S_\beta - b^2S_\gamma & a^2b^2 \\ c^2a^2 & c^2S_\beta - b^2S_\gamma \end{pmatrix}$$

$\lambda y = \mu z \longrightarrow (\lambda c^2 S_\beta - \lambda b^2 S_\gamma + \mu a^2 b^2) y =$

$= (\lambda c^2 a^2 + \mu c^2 S_\beta - \mu b^2 S_\gamma) z$

———— o ————

Rette.

•) Asse di BC: passa per $[0,1,1]$ e $[-a^2, S_\gamma, S_\beta]$

$\{x(S_\beta - S_\gamma) - a^2 y + a^2 z = 0\}$

$O = [a^2 S_\alpha, \dots]$

$$a^2 S_\alpha S_\beta - a^2 S_\alpha S_\gamma - a^2 b^2 S_\beta + a^2 c^2 S_\gamma =$$
$$= a^2 \left(S_\alpha S_\beta - S_\alpha S_\gamma - (S_\alpha + S_\gamma) S_\beta + (S_\beta + S_\alpha) S_\gamma \right) \equiv 0.$$

1) Retta di Euler: passa per $[1,1,1]$ e $[\bar{a}^2 S_\alpha, \dots, \dots]$

$$(c^2 S_\gamma - b^2 S_\beta) x + \dots + \dots = 0$$

$c^2 = S_\alpha + S_\beta$, $b^2 = S_\alpha + S_\gamma$ $\rightarrow$ $S_\alpha S_\gamma - S_\alpha S_\beta = S_\alpha (S_\gamma - S_\beta)$

$$\sum_{cyc} S_\alpha (S_\gamma - S_\beta) x = 0$$

- Retta per I, O: $[a,b,c]$, $[a^2 S_\alpha, \dots]$

$$\sum_{cyc} (b c^2 S_\gamma - c b^2 S_\beta) x = 0$$

$$\sum_{cyc} \frac{c S_\gamma - b S_\beta}{a} x$$

Tri pedali

$P = [u, v, w]$ $\quad \ell // AH$, $P \in \ell$

$$\pi = \{ (S_\beta v - S_\gamma w) x - (S_\beta u + a^2 w) y + (S_\gamma u + a^2 v) z = 0 \}$$

$$\begin{pmatrix} u & v & w \\ -a^2 & S_\gamma & S_\beta \\ x & y & z \end{pmatrix} \qquad \pi \cap \{x=0\} = P_A$$

$P_A = [0 : S_\gamma u + a^2 v : S_\beta u + a^2 w]$ $\quad a^2(v+w) + u(S_\beta + S_\gamma)$, $a^2 \Sigma u$

$P_B = [S_\gamma v + b^2 u : 0 : S_\alpha v + b^2 w]$ $\quad b^2 \Sigma u$

$P_C = [S_\beta w + c^2 u : S_\alpha w + c^2 v : 0]$ $\quad c^2 \Sigma u$

Teo: Due rette con punto all'∞ sono $\perp$
$[f,g,h] \perp [f',g',h']$

$\Leftrightarrow$ e $\Leftrightarrow$ $S_\alpha f f' + S_\beta g g' + S_\gamma h h' = 0$.

Es: $A0 \quad [1,0,0] \quad [aS_\alpha, \dots]$

$\Leftrightarrow \{ c^2 S_\gamma y = b^2 S_\beta z \}$

$[-b^2 S_\beta - c^2 S_\gamma, b^2 S_\beta, c^2 S_\gamma]$

$$\begin{cases} S_\alpha (b^2 S_\beta + c^2 S_\gamma) l - b^2 S_\beta^2 m - c^2 S_\gamma^2 n = 0 \\ l + m + n = 0 \end{cases}$$

$-m(b^2 S_\alpha S_\beta + c^2 S_\alpha S_\gamma - b^2 S_\beta^2) = n(b^2 S_\alpha S_\beta + c^2 S_\alpha S_\gamma + c^2 S_\gamma^2)$

$-m(b^2 S_\beta c^2 + c^2 S_\alpha S_\gamma) = n(b^2 S_\alpha S_\beta + c^2 S_\gamma b^2)$

$$m = -b^2(S_\alpha S_\beta + c^2 S_\gamma)$$
$$n = c^2(S_\alpha S_\gamma + b^2 S_\beta)$$
$$\ell = -m-n = b^2 S_\alpha S_\beta + b^2 c^2 S_\gamma - c^2 S_\alpha S_\gamma - c^2 b^2 S_\beta =$$
$$= S_\alpha(b^2 S_\beta - c^2 S_\gamma) + c^2 b^2 (S_\gamma - S_\beta) =$$
$$= S_\alpha^2 (S_\beta - S_\gamma) + c^2 b^2 (S_\gamma - S_\beta)$$
$$[\ell, m, n] \quad [1, 0, 0]$$
$$n_y = n_z$$

Circonferenze

$$a^2 yz + b^2 xz + c^2 xy + (x+y+z)(px+qy+rz) = 0.$$
$$Ax^2 + By^2 + Cz^2 + 2Dxy + 2Exz + 2Fyz = 0.$$
$$(x \ y \ z) \begin{pmatrix} A & D & E \\ D & B & F \\ E & F & C \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$
$$M$$

Per ogni punto $P \in \mathbb{RP}^2$ considero la retta
$$\{ {}^t P \cdot M \cdot X = 0 \}$$

$P = [u, v, w]$ $\quad {}^tP = (u, v, w)$

$$X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

$${}^tP \cdot \Pi = (u \; v \; w) \begin{pmatrix} A & D & E \\ D & B & F \\ E & F & C \end{pmatrix} =$$

$$= (Au + Dv + Ew, \; Du + Bv + Fw, \; Eu + Fv + Cw)$$

Tale retta si chiama POLARE di P rispetto alla conica e si indica con $pol(P)$

$P \in pol(P) \iff {}^tP \cdot \Pi \cdot P = 0 \iff P \in$ conica

$P \in pol(Q) \iff {}^tQ \cdot \Pi \cdot P = 0 = {}^tP \cdot \Pi \cdot Q \iff Q \in pol(P)$

$P \in$ conica $\iff pol(P)$ è Tangente alla conica.

[Conica è "non" (=) (irriducibile) $\iff \det \Pi \neq 0$]

$P \in$ conica $\iff p \in pol(P)$ e $\exists Q \neq P, Q \in$ conica t.c. $Q \in pol(P) \Rightarrow pol(P) = PQ$

$Q \in$ conica $\Rightarrow Q \in pol(Q)$

$Q \in pol(P) \Rightarrow P \in pol(Q) \Rightarrow pol(Q) = PQ$

${}^t P \cdot \Pi \cdot X = 0$ sono la stessa
${}^t Q \cdot \Pi \cdot X = 0$

${}^t P \cdot \Pi = {}^t Q \cdot \Pi$

$({}^t P - {}^t Q) \cdot \Pi = 0$

$\Pi \cdot (P - Q) = 0$

$\exists (a,b,c) \in \mathbb{R}^3 \setminus \{(0,0,0)\}$ t.c. $\Pi \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix} = 0$

$\det \Pi \neq 0$ assurdo.

$\Rightarrow$ conica $\cap$ $pol(P) = \{P\}$

$\Rightarrow$ $pol(P)$ è Tg. alla conica.

Es: $a^2yz + b^2xz + c^2xy = 0$

$A = [1,0,0]$

$$\begin{pmatrix} 0 & c^2 & b^2 \\ c^2 & 0 & a^2 \\ b^2 & a^2 & 0 \end{pmatrix} = \Pi$$

$${}^t A \cdot \Pi \cdot X = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & c^2 & b^2 \\ c^2 & 0 & a^2 \\ b^2 & a^2 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & c^2 & b^2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = c^2 y + b^2 z$$

Oss: La polarità è una DUALITÀ.

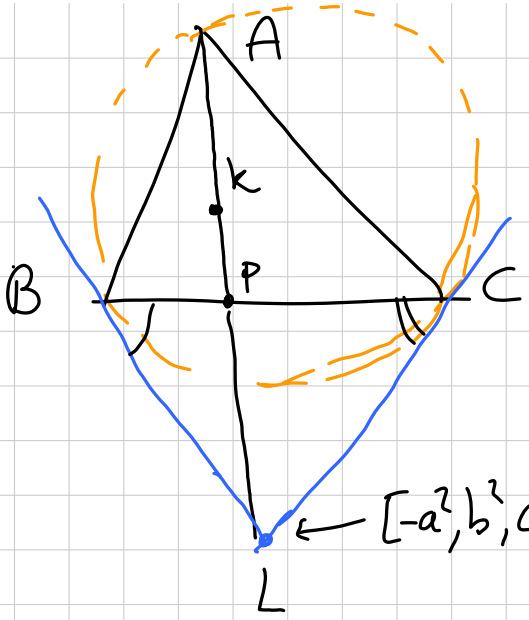
Se A, B, C sono allineati, $pol(A), pol(B), pol(C)$ concorrono.

$pol(r) = P \iff pol(P) = r$

Es: $c^2y + b^2z = 0$ $\quad r_y$ in A

$c^2x + a^2z = 0$ $\quad r_y$ in B

si intersecano in $[a^2, b^2, -c^2]$.

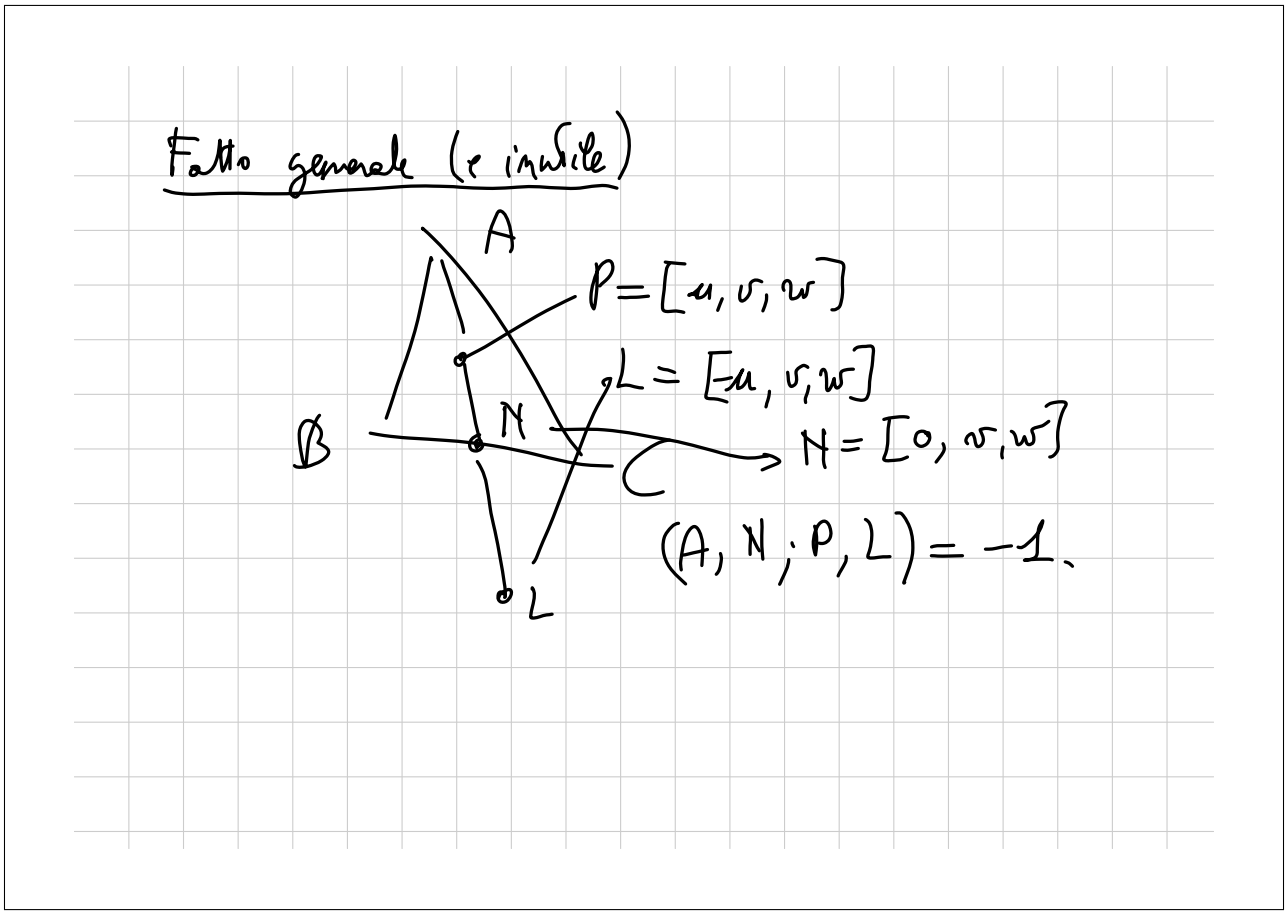


$K = [a^2, b^2, c^2]$

$b^2z = c^2y$

$\frac{AK}{KP} = -\frac{AL}{LP}$

$\leftarrow [-a^2, b^2, c^2]$ $\quad (A, P; K, L) = -1$


Fatto generale (e inutile)
A
P = [u, v, w]
L = [-u, v, w]
B
N
C
N = [0, v, w]
(A, N; P, L) = -1.
L

Teoria dei Numeri (Advanced?)

Titolo nota 04/09/2013

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

$\mathbb{Z}/6\mathbb{Z}$ è un anello, ma non è { un dominio integro / d. integrità

$$(5) = (2+i)(2-i)$$

Irriducibili vs Primi

Primo p se $p \mid ab \Rightarrow p \mid a$ o $p \mid b$
e p non è invertibile

Dividere? $ab = p \cdot (\text{qualcos'altro})$

Irriducibile $p = a \cdot b \Rightarrow a$ è invertibile o b è invertibile
p non invertibile

Negli interi di Gauss, $1+i = i\cdot(1-i)$

$3+4i$ non è invertibile in $\mathbb{Z}[i]$, perché

$(3+4i)^{-1} = \dfrac{3-4i}{25}$ non è un intero di Gauss

Es (invertibili in $\mathbb{Z}[i]$)

$(a+bi)$ è invertibile? Il suo inverso (in $\mathbb{C}$) è $\dfrac{a-bi}{a^2+b^2}$, che sta in $\mathbb{Z}[i]$ $\Leftrightarrow$

$$\frac{a}{a^2+b^2} \in \mathbb{Z}, \quad -\frac{b}{a^2+b^2} \in \mathbb{Z}$$

$\Leftrightarrow$ $a=0$, $b=\pm 1$ oppure $a=\pm 1$, $b=0$

SEMPRE: primo $\Rightarrow$ irriducibile

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

$p = b\cdot K\cdot p$

dominio $\Longrightarrow$ $1 = b\cdot K$

ATTENZIONE! Il contrario è falso: lavoriamo in $\mathbb{Z}[\sqrt{-5}]$ ed osserviamo che

$$2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

- 2 è irriducibile $a+b\sqrt{5}$

  Se potessi scrivere $2 = (a+b\sqrt{-5})(c+d\sqrt{-5})$,

  otterrei $4 = (a^2+5b^2)(c^2+5d^2)$

  $\Rightarrow$ $b=0$ e $d=0$

$\Rightarrow$ $2 = a \cdot c$ dove $a, c \in \mathbb{Z}$

- 2 non è primo: $2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5})$

  ma $2 \nmid 1+\sqrt{-5}$, $2 \nmid 1-\sqrt{-5}$: l'equazione

$$1+\sqrt{-5} = 2(a+b\sqrt{-5})$$

non ha soluzioni

$$x^2+1 = y^3$$

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

Domanda zero: $x+i$ e $x-i$ sono primi tra loro?

Oss: x è pari, altrimenti assurdo mod 4

y è dispari

Prendiamo un divisore comune di $x+i$, $x-i$.

Lo chiamo δ.

$$\delta \mid (x+i) - (x-i) = 2i$$

$\delta \mid 2i \iff \delta \mid 2$

$2i = \alpha \cdot \delta$ $\qquad$ $2 = \beta \cdot \delta$

$2 = (-i\alpha)\cdot\delta$

LE UNITÀ NON CONTANO NEI RAGIONAMENTI DI DIVISIBILITÀ

D'altro canto $\delta \mid (x+i)(x-i) = y^3$

$\delta \mid 2$

$$\begin{cases} \text{Norma}(\delta) \mid \text{Norma}(y^3) = y^6 \\ \text{Norma}(\delta) \mid N(2) = 4 \end{cases}$$

Siccome y è dispari, $N(\delta) = \pm 1$, e anzi fa $+1$, perché sicuramente $N(\delta) \geq 0$

NORMA • $N(a+bi) = a^2 + b^2$

• $\alpha \mid \beta \implies N(\alpha) \mid N(\beta)$

Perché? Se $\beta = \alpha\gamma$, prendendo i moduli (come numeri complessi) trovo $|\beta| = |\alpha| \cdot |\gamma|$ e facendo il quadrato $N(\beta) = N(\alpha) \cdot N(\gamma)$

• $N(3+4i) = 25$

FATTO Se $N(\alpha) = 1$, α è invertibile

Infatti

$$1 = N(\alpha) = \alpha \cdot \overline{\alpha}$$

e $\overline{\alpha}$ è ancora un intero di Gauss

Quindi $(x+i, x-i) = 1$, e quindi ognuno è un cubo

Ma se $(x+i)$ è un cubo, $\exists\, a+bi$:

$$x+i = (a+bi)^3$$

Confrontando le parti immaginarie,

$$1 = 3a^2b - b^3$$
$$= b(3a^2 - b^2),$$

dunque $b = \begin{cases} +1 \\ -1 \end{cases}$ $\Rightarrow$ non riesco a trovare a

$\Rightarrow a = 0$

Quindi $x+i = (-i)^3$, cioè $x=0$

$x+i$ è un cubo <u>a meno di unità</u>, ma in $\mathbb{Z}[i]$ tutte le unità sono cubi: $(-i)^3 = i$

COS'È LA FATTORIZZAZIONE UNICA?

Si dice che un anello ha fatt. unica se ogni suo elemento si scrive in modo unico come prodotto di irriducibili A MENO DI UNITÀ

Es $2 = (1+i)(1-i) = -i(1+i)^2$

Fatto α è un'unità in $\mathbb{Z}[\sqrt{-d}]$ se e solo se $N(\alpha)=1$.

Se $\alpha \cdot \alpha^{-1} = 1$

$N(\alpha) \cdot N(\alpha^{-1}) = 1$

Siccome $N(\alpha)$, $N(\alpha^{-1})$ sono interi >0,

$N(\alpha)=1$

Viceversa, $1 = N(\alpha) = \alpha \cdot \overline{\alpha}$

Perché in $\mathbb{Z}$ irriducibile $\Rightarrow$ primo?

Sia p irriducibile, $p \mid ab$, vogliamo dimostrare $p \mid a$ oppure $p \mid b$.

Per assurdo questo non succede.

$(a,p)=1$ $\qquad$ $(b,p)=1$ } Bézout

$ha+kp=1$ $\qquad$ $h'b+k'p=1$

Moltiplicando membro a membro,

$$p(\dots) + \underbrace{hh'ab}_{\text{divisibile per } p} = 1$$

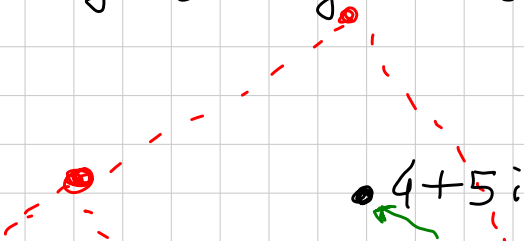
e quindi $p \mid 1$, assurdo.

Come si dimostra Bézout? Con Euclide.

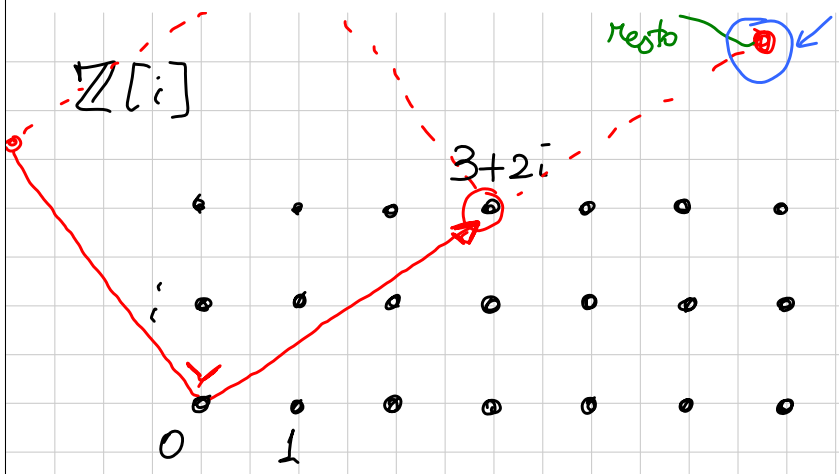
La divisione con resto vuol dire che ho una certa quantità ("la grandezza"

delle cose in gioco) e per ogni a e b so scrivere $a = kb + r$ con il resto che è o zero o più piccolo di b.

Sostengo che $\mathbb{Z}[i]$ ha la divisione euclidea con "funzione grandezza" la norma



vertice più vicino a $4+5i$



Dividiamo $4+5i$ per $3+2i$

Lato dei quadrati rossi $= N(3+2i)^{1/2}$

Se prendo il vertice del reticolo rosso più vicino alla cosa che sto dividendo, la distanza fra questi due punti è $\leq \dfrac{N(3+2i)^{1/2}}{\sqrt{2}}$

E se non c'è la fattorizzazione unica?

$$y^2 = x^3 - 26$$

$x = 3$ e $y = 1$

$$(y + \sqrt{-26})(y - \sqrt{-26}) = x^3$$

Saranno coprimi? Se $\delta \mid (y + \sqrt{-26},\ y - \sqrt{-26})$: allora

$$\delta \mid 2\sqrt{-26} \implies N(\delta) \mid 8 \cdot 13$$

D'altro canto, $\delta \mid x^3 \implies N(\delta) \mid x^6$

Congruenze mod 13^k e mod 4 dicono che

$$(x, 26) = 1,$$ da cui $N(\delta) = 1$

$N(a + b\sqrt{-26}) = a^2 + 26b^2$, quindi $N = 1$

$\iff a = \pm 1,\ b = 0$

Quindi $y + \sqrt{-26} = (a + b\sqrt{-26})^3$ e quindi

$$1 = 3a^2b - 26b^3$$

Allora $b = \pm 1$ e

$b = 1$ $\quad a = \pm 3$

$b = -1$ $\quad$ assurdo

$$y = a^3 + 3a(-26b^2) = 27 - 78 \cdot 3$$
$$= -207$$

$x = 35$

Usando la fattorizzazione unica, che però è falsa, abbiamo

* trovato la soluzione $(35, \pm 207)$ OK

* dimostrato che è l'unica MALE

La dimostrazione è, naturalmente, completamente falsa.

Esempio $x^2+2=3^n$, n dispari

Fatto $\mathbb{Z}[\sqrt{-2}]$ ha fattorizz. unica

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

$\delta \mid x+\sqrt{-2}$, $\delta \mid x-\sqrt{-2} \Rightarrow \delta \mid 2\sqrt{-2}$

$N(\delta) \mid 8$

$N(\delta) \mid 3^{2n} \Rightarrow N(\delta)=1$, δ è una unità

Tutte le unità sono potenze n-esime.

$\| \{\pm 1\}$

$1+\sqrt{-2}$ è primo? Siccome c'è fatt. unica, è suff. vedere che è irriducibile.

Supponiamo $1+\sqrt{-2} = \alpha \cdot \beta$. Allora

$$3 = N(1+\sqrt{-2}) = N(\alpha)\cdot N(\beta),$$

e quindi (WLOG) $N(\beta) = 1$.

Le cose di norma 1 sono unità, quindi la fattorizzazione era falsa

In generale $N(\alpha) = p$ primo $\Rightarrow \alpha$ irrid.

Quindi $x \pm \sqrt{-2} = (1 \pm \sqrt{-2})^n$ (non necess. con lo stesso segno)

Attenzione ai segni! ($x \mapsto -x$ se serve)

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

Lavoriamo modulo $(1-\sqrt{-2})$.

Troviamo $\pm 2\sqrt{-2} \equiv (1+\sqrt{-2})^n \pmod{1-\sqrt{-2}}$

cioè $\pm 2 \equiv 2^n \pmod{1-\sqrt{-2}}$

$\Rightarrow 4 \equiv 2^{2n} \pmod{1-\sqrt{-2}}$

$(1-\sqrt{-2}) \mid (4^n - 4)$

Quindi $4^n - 4 = (1-\sqrt{-2})\alpha$, da cui

$4^n - 4 = (1+\sqrt{-2})\overline{\alpha}$,

e cioè $4^n \equiv 4 \pmod{1+\sqrt{-2}}$

COPRIMI

$\begin{cases} (1+\sqrt{-2}) \mid 4^n - 4 \\ (1-\sqrt{-2}) \mid 4^n - 4 \end{cases} \Rightarrow (1+\sqrt{-2})(1-\sqrt{-2}) \mid 4^n - 4$

$\Rightarrow 3 \mid 4^n - 4$

Ci è andata male. Proviamo mod $(1-\sqrt{-2})^2$.

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

$\pm 2\sqrt{-2} \equiv (1+\sqrt{-2})^n \pmod{(1-\sqrt{-2})^2}$

$(1-\sqrt{-2})^2 = -2\sqrt{-2} - 1$ (Suppongo $n \geq 2$)

$\mp 1 \equiv (1+\sqrt{-2})^n \pmod{(1-\sqrt{-2})^2}$

$1 \equiv (2\sqrt{-2}-1)^n$ ($\sim$)

$1 \equiv (-2)^n \pmod{(\ )^2}$

Grazie alla divisibilità per il compl. coniug.,

$1 \equiv (-2)^n \pmod{9}$

$\mathrm{ord}_9(-2) = 3$, quindi $3 \mid n$

Ma se $3 \mid n$ tanto vale risolvere

$$x^2 + 2 = y^3$$

Questa si fa come prima... $x = 5$, $y = 3$

I MALEFICI $\mathbb{Z}\left[\frac{\sqrt{n}+1}{2}\right]$

$\mathbb{Z}[\sqrt{n}]$

Gli $n \equiv 1 \pmod 4$ sono problematici.

$n = 5$ $\qquad (1+\sqrt{5})(1-\sqrt{5}) = -4$

$= -2 \cdot 2$

$\varphi = \frac{1+\sqrt{5}}{2}$ $\qquad \varphi^2 - \varphi - 1 = 0$

Norma $(a+b\sqrt{n}) = (a+b\sqrt{n})(a-b\sqrt{n})$

$N(\alpha\beta) = N(\alpha)N(\beta)$

$N\left(\frac{1+\sqrt{n}}{2}\right) = \frac{1-n}{4} \in \mathbb{Z}$ se $n \equiv 1 \ (4)$

$\frac{1+\sqrt{n}}{2} + \frac{1-\sqrt{n}}{2} = 1$

Se $n \equiv 1 \ (4)$, $\mathbb{Z}[\sqrt{n}]$ non è MAI a fattorizzazione unica.

Quello che ha speranze è $\mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right] =$

$$= \left\{ a + b\,\frac{1+\sqrt{n}}{2} \mid a, b \in \mathbb{Z} \right\}$$

$\mathbb{Z}[\sqrt{-3}]$ non è a fatt. unica

$$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \mathbb{Z}[\zeta_6] = \mathbb{Z}[\zeta_3]$$

$= \mathbb{Z}[\omega]$ è a fatt. unica

"interi di Eisenstein"

Cose a fatt. unica

$n < 0$ $\quad n = -1, -2, -3, -7, -11,$

$-19, -43, -67, -163$

$$\mathbb{Z}[i],\ \mathbb{Z}[\zeta_3],\ \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right], \ldots$$

$n > 0$ $\quad n = 2, 3, 5, 6 \ldots$?

Eq. di RAMANUJAN $x^2 + 7 = 2^n$

$\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ ha fatt. unica

$n \leq 2$ o n pari ve la fate.

$$\frac{x^2+7}{4} = 2^y$$

$$\| $$

$$\left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right)$$

Campi finiti

Titolo nota 05/09/2013

K campo $(K, 0, 1, +, \cdot)$

$\mathbb{Z}/p\mathbb{Z}$ .... $\mathbb{F}_p$ $\qquad$ $\mathbb{R}[x]/I$ $\quad I=(p(x))$

$\mathbb{R}[x]/I$ = "polinomi modulo $p(x)$".

$\mathbb{R} \longrightarrow \mathbb{F}_p$ $\qquad$ $\mathbb{F}_p[x]/(a(x))$ $\qquad$ $(a(x)) = \{ \text{multipli di } a(x) \}$

$a(x)$ non irriducibile $\longrightarrow$ $\mathbb{F}_p[x]/(a(x))$ non è dominio d'integrità.

$a(x)$ irriducibile è campo?

$\exists$ inverso di $b(x)$? Sì per Bézout.

$\Rightarrow$ quanti elementi ha $\mathbb{F}_p[x]/(a(x))$?

$0, 1, \ldots, p-1$
$\times\ 2x \ldots (p-1)x$
$x^2 \ldots$
$\vdots$ $x^{\deg(a(x))-1} \ldots$

+ tutte le somme = $\{$pol. di grado $< \deg(a(x)) = n\}$

$\Rightarrow$ p^n elementi.

Se esiste un pol. irriducibile di grado n in $\mathbb{F}_p[x]$, esiste un campo con p^n elementi.

$\mathbb{F}_4$ $\quad x^2+x+1$ è irriducibile

$\mathbb{F}_2[x]/(x^2+x+1) \to \{0, 1, x, x+1\} \doteq \mathbb{F}_4$ $\quad +, \cdot, \dots$

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

$\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ $\quad \alpha^2+\alpha+1=0$

$\mathbb{F}_{p^2}$ $\quad x^2+ax+b$ irriducibile

x^2+b $\quad -b$ non residuo quadratico

(0 $\quad x \to y+1$ $\quad y^2+2y+b+1$)

$\mathbb{F}_p(\alpha)$ $\quad \alpha^2 = -b$ $\quad mx+n$

$(mx+n, x^2+b) = 1 \Rightarrow$

$\ell(x)(mx+n) + h(x)(x^2+b) = 1$

in $\mathbb{F}_p(\alpha)$, $\ell(\alpha)$ è inverso di $mx+n$.

$\mathbb{F}_{24} = \mathbb{F}_{16}$ $\quad x^4+x+1$ è irr. $\begin{cases} \text{non ha radici in } \mathbb{F}_2 \\ (x^2+x+1)^2 = x^4+x^2+1 \end{cases}$

$\mathbb{F}_2[x]/(x^4+x+1) \to \mathbb{F}_2(\alpha)$ $\quad \alpha^4 = \alpha+1$ $\quad \#_{x^4+x+1}$

$0 \quad 1 \quad \alpha \quad \alpha+1$

$\alpha^2 \quad \alpha^2+1 \quad \alpha^2+\alpha \quad \alpha^2+\alpha+1$

$\alpha^3 \quad \alpha^3+1 \quad \alpha^3+\alpha \quad \alpha^3+\alpha+1$

$\alpha^3+\alpha^2 \quad \alpha^3+\alpha^2+1 \quad \alpha^3+\alpha^2+\alpha \quad \alpha^3+\alpha^2+\alpha+1$

$\{ l_1\alpha^3 + l_2\alpha^2 + l_3\alpha + l_4 \mid l_i \in \mathbb{F}_2 \} =$ sp. vett. su $\mathbb{F}_2$ di dim. 4.

Il prodotto non è quello di $\mathbb{Z}/16\mathbb{Z}$! (neanche la somma)

Tutti gli $\alpha \in \mathbb{F}_{16}$ sono t.c. $\alpha+\alpha=0$

invece in $\mathbb{Z}/16\mathbb{Z}$ bisogna arrivare a 16

Invece gli $a \in \mathbb{Z}/16\mathbb{Z}$ dispari sono t.c. $a^4 \equiv 1$

invece in $\mathbb{F}_{16}$ $\quad \alpha^4 = \alpha+1 \neq 1$

$\alpha^5 \to \alpha \cdot \alpha^4 = \alpha \cdot (\alpha+1) = \alpha^2+\alpha$

$(\alpha^2+\alpha+1)(\alpha^3+\alpha^2) = \alpha^2+\alpha+\alpha+1+\alpha^3+\alpha+1+\alpha^3+\alpha^2 =$

$= \alpha.$

$\mathbb{F}_8$ $\quad x^3+x+1$ è irr. (non ha radici)

$\longrightarrow \mathbb{F}_2(\alpha) \quad \alpha^3+\alpha+1=0$

Si può fare un campo con un numero di elementi $\neq p^k$?

Caratteristica di un campo: $0 \neq x \in K$

se $x+x+x-\dots = n\cdot x$ non fa mai $0 \rightarrow$ $\operatorname{char} K = 0$

se $x+x+\dots+x = n\cdot x = 0$ $\operatorname{char} K =$
$= \min\{n \mid n\cdot x = 0\} \in \mathbb{N}$

Se $y \neq x$ $y \neq 0$, $y+y-\dots+y = n\cdot y =$

$= \left(\frac{y}{x}\right)(x+x-\dots+x)$

quindi o tutti sono t.c. $\underbrace{x+x-\dots+x}_{n\cdot x} = 0$
o nessuno

Se il campo è finito, $\operatorname{char} K \neq 0$.

Ma $\operatorname{char} K$ è un numero primo:

$n = p\cdot q \quad n\cdot x = 0 \quad p\cdot q\cdot x = 0 =$

$= (\underbrace{1+1-\dots+1}_{p \text{ volte}})\cdot(qx)$ / $p \neq 0$ $\exists \frac{1}{p} \Rightarrow qx = 0$ $\quad 0<q<n$ ass.

\ $p = 0$ ass.

Ma allora $K \supset \mathbb{F}_p = (0, 1, \dots, p-1)$

Ma se $K \supset L$ K è sp. vett. su $L \Rightarrow$ ha p^k el.

$\mathbb{F}_{27}$?

Oss. in $\mathbb{F}_p$ o $\mathbb{F}_{p^k}$ o char $K = p$

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

$\mathbb{F}_p$

$$Q(x) = x^{p^k} - x = x \cdot (x^{p^k - 1} - 1)$$

$$Q(x) = \prod_{i=1}^{N} q_i(x) \qquad q_i \text{ irr.}$$

Posso costruire $\dfrac{\mathbb{F}_p[x]}{(q_i(x))} \to \mathbb{F}_p(\alpha)$ dove $q_i(x)$ ha una radice,

in $\mathbb{F}_p(\alpha)[x]$, $Q(x) = \prod q_i^{\alpha}(x)$ $\quad q_i^{\alpha}$ irr.

$\to \dfrac{\mathbb{F}_p(\alpha)[x]}{(q_i^{\alpha}(x))} \to \mathbb{F}_p(\alpha)(\beta) \to$

$\to \quad - \quad - \quad - \quad \mathbb{F}_p(\alpha)(\beta) \dots (\omega)$ in cui

$Q(x)$ si spezza in fattori di grado 1

$K \subset \mathbb{F}_p(\alpha)(\beta)(\gamma)\dots(\omega)$

$K = \{\lambda \in \dots \mid \lambda^{p^k} = \lambda\}$

Oss. K è un campo!

$$(\lambda_1 + \lambda_2)^{p^k} = \lambda_1^{p^k} + \lambda_2^{p^k} = \lambda_1 + \lambda_2$$

$$(\lambda_1 \lambda_2)^{p^k} = \lambda_1^{p^k} \lambda_2^{p^k}$$

$$\lambda_1^{p^k} = 1 \qquad \left(\frac{1}{\lambda_1}\right)^{p^k} = \frac{1}{\lambda_1^{p^k}} = 1$$

Quanti el. ha K? Sono le radici di

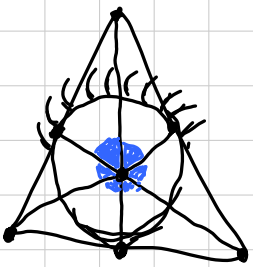
$x^{p^k} - x$ in $\mathbb{F}_p(\alpha)(\beta)\dots(\omega)$.

$\left(x^{p^k} - x\right)' = -1 \Rightarrow$ le radici sono distinte

e in $\mathbb{F}_p(\alpha)\dots(\omega)$ c'erano tutte $\Rightarrow p^k$.

$\Rightarrow |K| = p^k$. e K è il <u>campo di spezzamento</u> di $Q(x)$,

cioè il più piccolo campo $(\supset \mathbb{F}_p)$ dove $Q(x)$ si spezza in fattori di grado 1.



FANO
WAS
HERE

grado di L su K $\doteq$ dim di L su K come sp. vett.

$[L:K]$

$\alpha^4 = \alpha + 1$

$\alpha^2+\alpha \in \mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ $\quad (\alpha^2+\alpha)^2 + (\alpha^2+\alpha) + 1 =$

$\mathbb{F}_4 = \mathbb{F}_2(\alpha^2+\alpha)$ $\quad = \alpha^4 + \alpha^2 + \alpha^2 + \alpha + 1 =$

$= \alpha + 1 + \alpha^2 + \alpha^2 + \alpha + 1 = 0$!

(anche $\alpha^2+\alpha+1$ va bene)

$[\mathbb{F}_{16} : \mathbb{F}_2] = 4 \quad [\mathbb{F}_4 : \mathbb{F}_2] = 2 \quad [\mathbb{F}_{16} : \mathbb{F}_4] = ?$ ②

$K < L < E$

$[E:K] = [E:L][L:K]$.

$\mathbb{F}_{16} = \mathbb{F}_2(\alpha) = \mathbb{F}_4(\beta)$

$\mathbb{F}_2(\gamma) \overset{\mathbb{F}_4}{=} \gamma^2+\gamma+1=0$

$\hookrightarrow \mathbb{F}_{16} \quad \gamma \longrightarrow \alpha^2+\alpha$ $\quad \mathbb{F}_2(\gamma)[x]$

in $\mathbb{F}_{16}$ $\quad \alpha^2+\alpha=\gamma$ $\quad \mathbb{F}_4[x]$ $x^2+x-\gamma$ è irr.!

$K < K(\alpha)$ $\quad [K(\alpha):K]$ è il grado del minimo polinomio soddisfatto da α.

$1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{k-1}$ sono indip.:

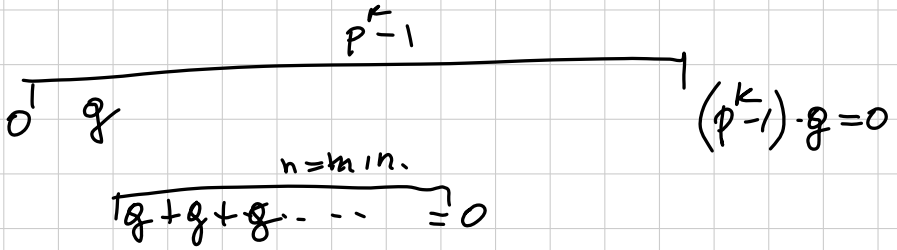
se $\alpha^k = \lambda_{k-1}\alpha^{k-1} + \dots + \lambda_1\alpha + \lambda_0$

$\Rightarrow x^k - \lambda_{k-1}x^{k-1} - \dots - \lambda_1 x - \lambda_0$ è il polinomio minimo di α su K

$x^4+x+1 = (x^2+x-\gamma)(\dots)$ in $\mathbb{F}_4[x]$

$|K| = p^k$ el., $K^* = K \setminus \{0\}$ è un gruppo molt. di ordine $p^k - 1$. $a^{p^k-1} = 1 \quad \forall a \in K$.

$\Rightarrow$ gli el. soddisfano $x^{p^k} = x$.



posso dividere i p^k-1 el. in classi di equiv. rispetto ai multipli di $g \Rightarrow n \mid p^k-1 \Rightarrow$

$\Rightarrow (p^k-1)\cdot g = 0$,

$\Rightarrow K =$ c. spezz di $x^{p^k} - x$.

Di più: $\mathbb{F}_{p^k}^*$ è ciclico.

Dim. ha p^k-1 elem. $p^k-1 = q_1^{\alpha_1} \cdot \ldots \cdot q_h^{\alpha_h}$

$x^{\frac{p^k-1}{q_i}} - 1$ ha al più $\frac{p^k-1}{q_i}$ radici in $\mathbb{F}_{p^k}^*$

$\Rightarrow \exists\, b_i$ non radice di

$\tilde{b}_i = b_i^{\frac{p^k-1}{q_i^{\alpha_i}-1}}$ $\qquad \tilde{b}_1 \cdot \tilde{b}_2 \cdot \ldots \cdot \tilde{b}_h = g$

Dico che g è un generatore.

$g^{p^k-1}=1$ se $g^h=1$ h min. $h<p^k-1 \Rightarrow h \mid p^k-1$

$\Rightarrow h \mid \frac{p^k-1}{q_i}$ per un certo i Ma allora

$g^{\frac{p^k-1}{q_i}} = 1 \cdot b_i \cdot 1 \cdot 1 \cdots = b_i \neq 1$ $\quad b_j^{\frac{p^k-1}{q_i}}=1$ $j \neq i$

□

$\mathbb{F}_{p^k}^* = \langle g \rangle$ non è detto che $\mathbb{F}_{p^k} = \mathbb{F}_p(g)$, $g=\alpha$

$\mathbb{F}_9$ x^2+1 $\mathbb{F}_3(\alpha)$ $\alpha^2+1=0$ $\mathbb{F}_9^* = \mathbb{Z}/8\mathbb{Z}$

ma $\alpha^4=(\alpha^2)^2=(-1)^2=1$

$$Q(x)=x^{p^k}-x = \prod \{ q_i(x) \text{ (monici) irriducibili di grado } d \mid k \text{ tutti} \}$$

se $q_i(x)$ irr. $q_i(x) \mid Q(x)$ il campo di spezz. di $q_i(x)$ è $L_i \subset \mathbb{F}_{p^k}$

$[\mathbb{F}_{p^k} : L_i][L_i : \mathbb{F}_p] = k$

ma $\deg q_i$ divide $[L_i : \mathbb{F}_p]$.

se α radice di q_i, $L_i \supset \mathbb{F}_p(\alpha) \supset \mathbb{F}_p$ ($\deg q_i$)

$\Rightarrow \deg q_i \mid k$.

$q_i(x)$ compaiono una volta sola perché $\mathbb{Q}(x)$ non ha radici multiple.

α radice di $q(x)$ irr. su $\mathbb{F}_p$.

$$q(x) = \sum_{i=0}^{d} \lambda_i x^i \qquad \mathbb{F}_p(\alpha)$$

$$\sum \lambda_i \alpha^i = 0$$

$$\alpha \longmapsto \alpha^p$$

$$\sum \lambda_i (\alpha^p)^i = \sum \lambda_i (\alpha^i)^p = \sum \lambda_i^p (\alpha^i)^p =$$

$$= \left(\sum \lambda_i \alpha^i\right)^p = 0 \Rightarrow \alpha^p \text{ è ancora radice!}$$

Ma $\alpha^p = \alpha$? no se no sarebbe radice di $x^p - x$ che ha già p radici in $\mathbb{F}_p$

$\alpha \quad \alpha^p \quad (\alpha^p)^p \quad \dots \quad \alpha^{p^{d-1}}$ sono radici di q

$\alpha^{p^i} = \alpha^{p^j} \qquad \alpha^{p^{j-i}} = 1$

$\Phi : \alpha \longmapsto \alpha^p$ omomorfismo di Frobenius

$\mathrm{Fix}\,\Phi = \mathbb{F}_p \qquad \mathrm{Fix}\,\Phi^{(k)} = \mathbb{F}_{p^k}$

$p^k = \sum_{d \mid k} d \cdot N_d(p)$ #pol. irr. d, grado d su $\mathbb{F}_p$

$x^{p^k} - x = \prod q_i(x)$

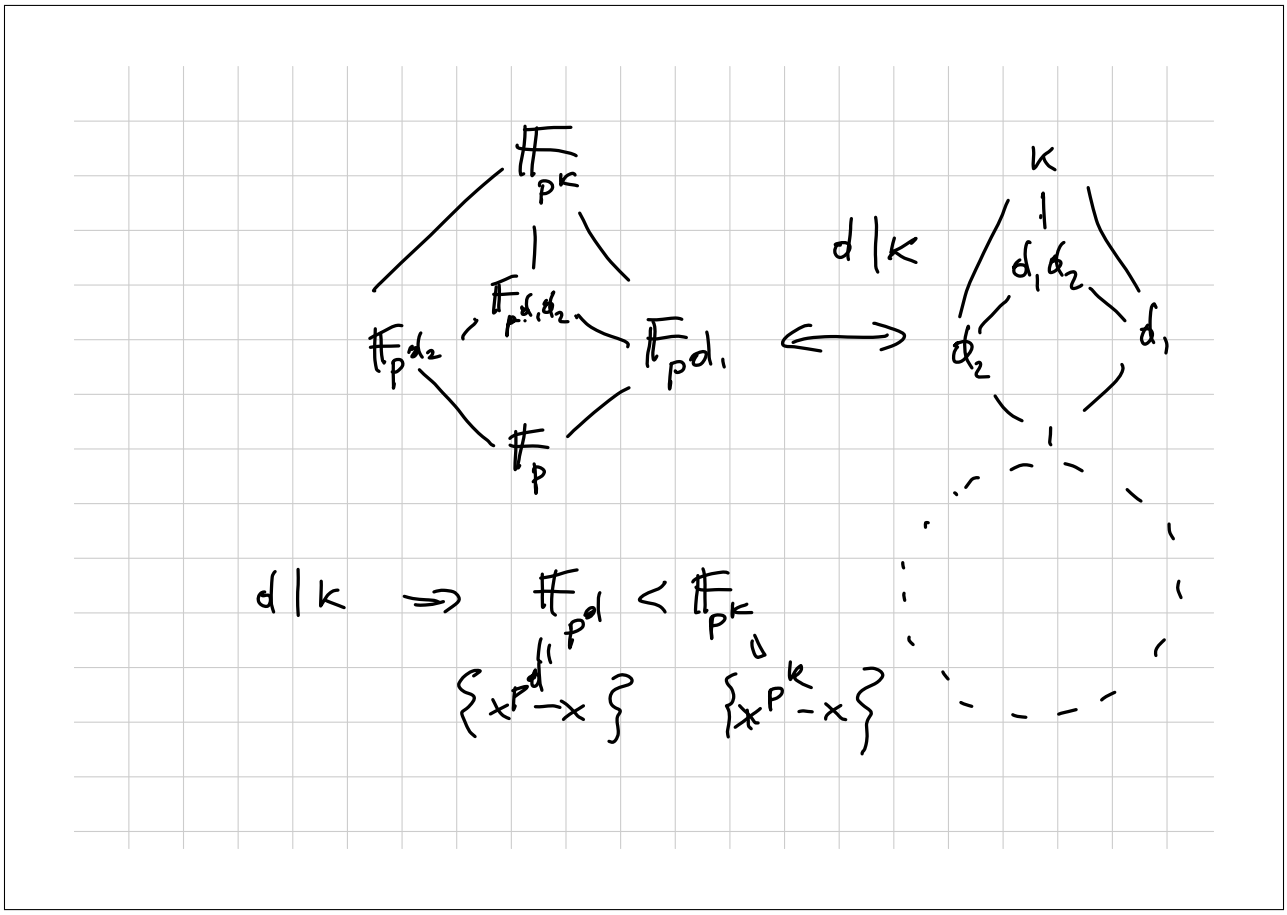
$N_n = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d =$

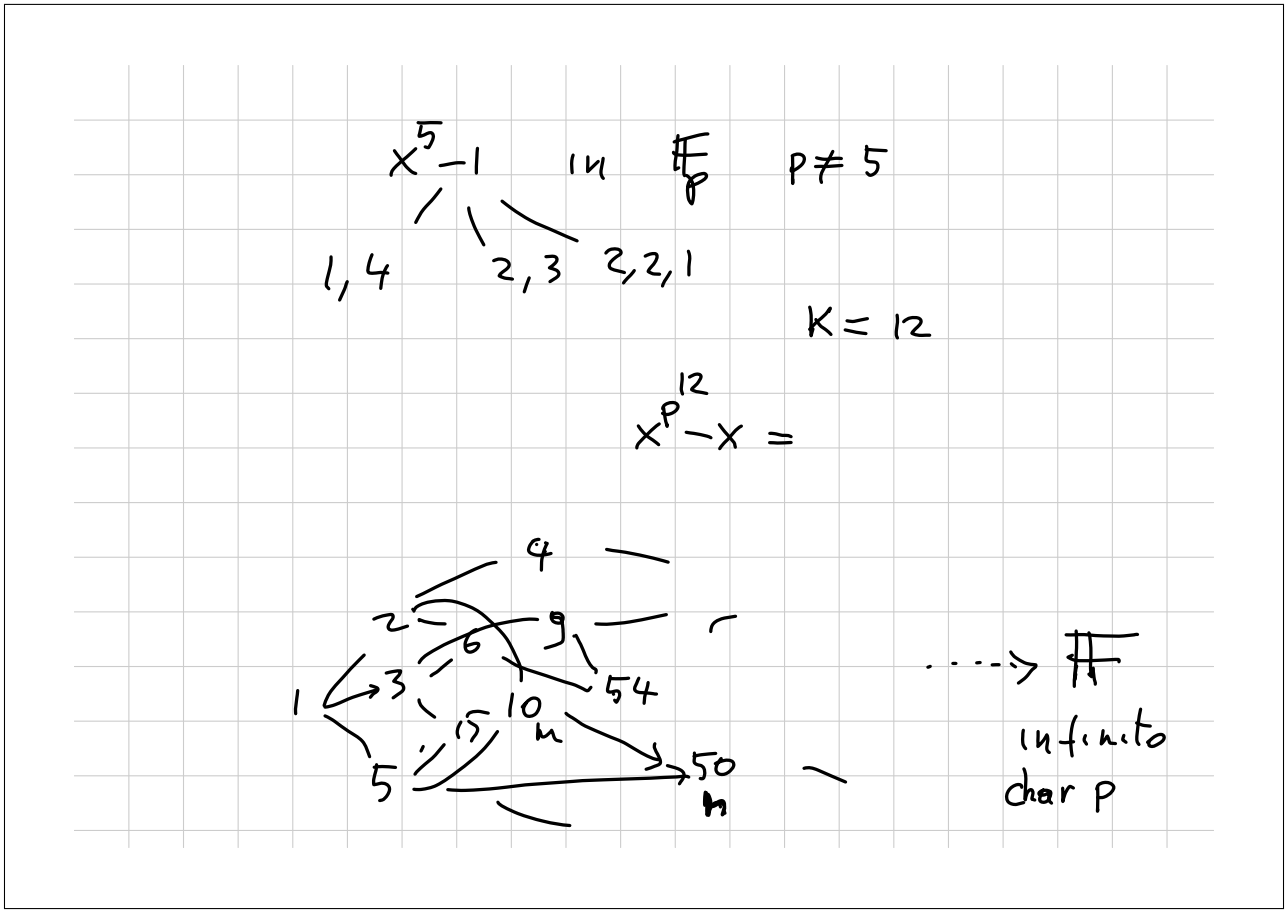
$= \frac{1}{n} \sum_{d \mid n} \mu(d)\, p^{\frac{n}{d}}$

$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = p_1 \cdots p_k \\ 0 & p^2 \mid n \end{cases}$

$f * g(n) = \sum_{d \mid n} f(d)\, g\left(\frac{n}{d}\right)$

$\mu * 1 = 1$ mi pare...


$\mathbb{F}_{p^k}$
$\mathbb{F}_{p^{d_1}}$
$\mathbb{F}_{p^{d_2}}$
$\mathbb{F}_{p^{d_1,d_2}}$
$\mathbb{F}_p$
$d \mid k$
k
$d_1 d_2$
d_1
d_2
1
$d \mid k \Rightarrow \mathbb{F}_{p^d} < \mathbb{F}_{p^k}$
$\{x^{p^d} - x\}$
$\{x^{p^k} - x\}$


$x^5 - 1$ in $\mathbb{F}_p$ $p \neq 5$
1, 4
2, 3
3, 2, 1
$K = 12$
$x^{p^{12}} - x =$
4
2
6
9
1
3
10
54
15
5
50
infinito
char p

$m \to n$

$\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$ $\qquad \mathbb{F} = \text{“}\bigcup\text{”}\, \mathbb{F}_{p^k}$

$p(x)$ a coeff. in $\mathbb{F}$ $\qquad$ m.c.m.

$c_i \in \mathbb{F}_{p^{k_i}} \subset \mathbb{F}_{p^{[k_1,\dots,k_n]}}$

$p(x)$ avrà radici in $\mathbb{F}_{p^{[\dots]}} \subset \mathbb{F}$

p.es. N = m.c.m dei gradi dei fattori irr. di p

$\mathbb{F}$ è <u>algebricamente chiuso</u> $\qquad \Phi_{\mathbb{F}} : \mathbb{F} \to \mathbb{F}$

$\mathbb{F}_{p^k} = F_1 \times \left(\Phi_{\mathbb{F}}^{(k)}\right)$

IMO 98/3 $\qquad d(n$

Trovare gli $m \in \mathbb{Z}^+$ per cui $\exists\, a \in \mathbb{N}$ t.c.

$$\frac{d(a^2)}{d(a)} = m.$$

$a = \prod p_i^{\alpha_i}$

$$m = \prod_i \frac{2\alpha_i + 1}{\alpha_i + 1} = \prod_i \left(2 - \frac{1}{\alpha_i + 1}\right) \qquad \alpha_i + 1 = b_i$$

$m = 1$ ok

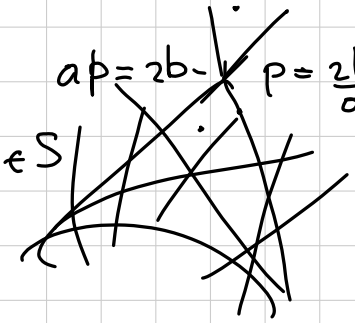
$b_1 = 3,\ b_2 = 5 \to 3$

m_1, m_2 ok $\longrightarrow m_1 \cdot m_2$ ok

$$p = \frac{(a)p}{\frac{ap+1}{2}}$$

$ap = 2b - 1 \quad p = \frac{2b}{a} - \frac{1}{a}$

$b, a \in S$



disp.

$m = 4k-1 \qquad \frac{12k-3}{6k-1} \cdot \frac{6k-1}{3k} \cdot k$

$m = 2^t k + 1 \qquad m \cdot (2^t - 1)$

$$m = \frac{2^t(2^t-1)k \cdot (2^t-1)}{2^{t-1}(2^t-1)k - (2^{t-1}-1)} \cdots \frac{4(2^t-1)k-3}{2(2^t-1)k-1} \frac{2(2^t-1)k-1}{(2^t-1)k} \cdot k$$

2000 SL N 5

$$\left|\left\{ n \in \mathbb{N} \mid n \text{ non è } \sum \text{ quadrati distinti} \right\}\right| \text{ è finito.}$$