Stage Senior 2016 – Livello Medium

Stampato integrale delle lezioni

Autori vari

Indice

INDUZIONE & FRIENDS - MEDIUM

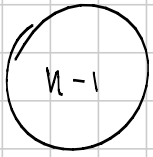
Note Title 9/1/2016

INDUZIONE
IND. FORTE
MINIMO INTERO
DISCESA INFINITA
PIGEONHOLE

→ Caso iniziale "a vuoto":

Esempio: il numero di coppie che posso fare con n oggetti è $1+2+\dots+(n-1)$

$P(n)$



$P(n) \to P(n+1)$

$n+1$ oggetti → coppie tra i primi n oggetti
↘ coppie con l'oggetto nuovo

Caso base: coppie di 0 oggetti

$$\sum_{i=1}^{0} i = 0$$

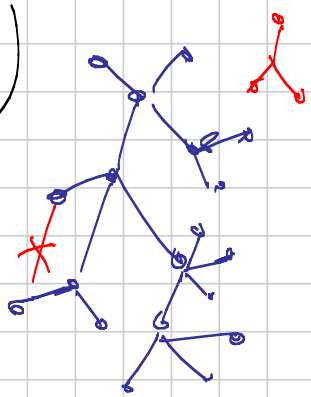
Sommatoria vuota $= 0$

Produttoria vuota = 1

Classico esempio di induzione problematica:
"Induzione su grafi aggiungendo"

Esempio: Teo: Ogni albero con n vertici $P(n)$ ha $n-1$ archi

(albero = grafo connesso, senza cicli)



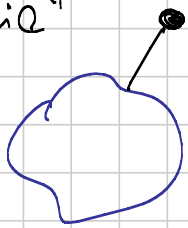
Dim: (sbagliata):
$P(n) \Rightarrow P(n+1)$
Prendo un albero con n vertici (e $n-1$ archi) Hp. ind.

Ho aggiunto 1 nodo $n \to n+1$
1 arco $n-1 \to n$

Problema: nessuno mi dice che "aggiungendo" posso raggiungere tutti gli alberi con $n+1$ nodi

Invece: devo partire da una configuraz. con $n+1$ nodi

Sia G un grafo con $n+1$ nodi, voglio mostrare che posso sempre togliere una "foglia"



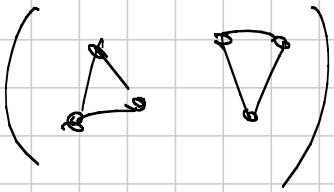
$n+1 \to n$

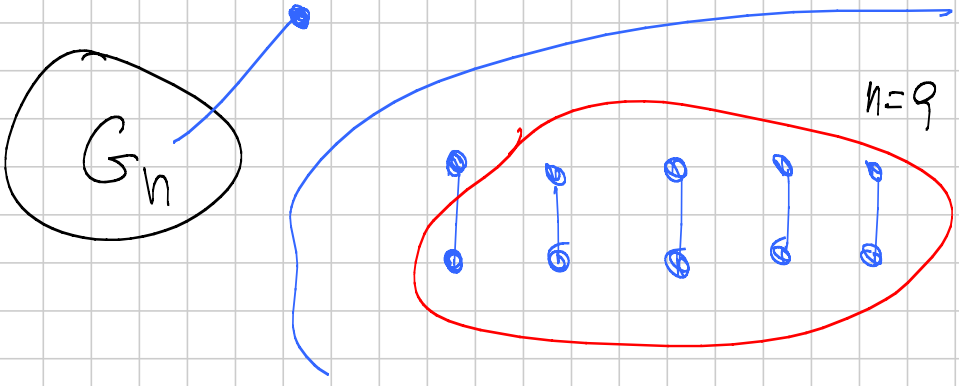
$? \to n-1$

Hp. ind. albero con n nodi

Mi serve dimostrare che ogni albero ha una foglia: se per assurdo non ci fosse foglie, parto da un vertice a caso, e "seguo la strada": dopo al max n passi, devo ripassare da un vertice già visto, assurdo.

Teo (falso): ogni grafo senza vertici isolati è connesso.





$P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow P(4) \Rightarrow P(5) \Rightarrow P(6) \dots$

Esempi di "induzione non lineare":

Dimostrazione della disuguaglianza tra le medie AM-GM

$\boxed{n=2}$ $\quad \frac{x^2+y^2}{2} \geq xy \iff (x-y)^2 \geq 0$

$P(2)$ $\quad x^2=a \quad y^2=b$

$P(n)$: $\quad \frac{a_1+a_2+\dots+a_n}{n} \geq \sqrt[n]{a_1 a_2 \dots a_n}$

$P(k), P(2) \Rightarrow P(2k)$

$$\frac{a_1+a_2+\dots+a_k+a_{k+1}+\dots+a_{2k}}{2k} = \frac{\frac{a_1+a_2+\dots+a_k}{k} + \frac{a_{k+1}+\dots+a_{2k}}{k}}{2}$$

$$\overset{P(2)}{\geq} \left(\frac{a_1+a_2+\dots+a_k}{k}\right)^{\frac{1}{2}} \left(\frac{a_{k+1}+\dots+a_{2k}}{k}\right)^{\frac{1}{2}} \overset{P(k)}{\geq}$$

$$\geq \left(a_1 a_2 \dots a_k\right)^{\frac{1}{k}\cdot\frac{1}{2}} \left(a_{k+1} \dots a_{2k}\right)^{\frac{1}{k}\cdot\frac{1}{2}}$$

$P(k+1) \Rightarrow P(k)$

Applico AM-GM a

$$\frac{a_1+a_2+\dots+a_k+\frac{a_1+a_2+\dots+a_k}{k}}{k+1} \geq \left(a_1 a_2 \cdots \frac{a_1+\dots+a_k}{k}\right)^{\frac{1}{k+1}}$$

e semplifico

Come arrivo a $P(13)$?

$$P(2) \Rightarrow P(4) \Rightarrow P(8) \Rightarrow P(16) \Rightarrow P(15) \Rightarrow P(14) \Rightarrow P(13)$$

Induzione su due variabili, es. m, n

Ad es. induzione su $m+n$ $\max(m,n)$

$P(0,0)$ $P(0,1)$ $P(0,2)$ $\cdots$

$P(1,0)$ $P(1,1)$ $P(1,2)$ $\cdots$

$P(2,0)$ $P(2,1)$ $P(2,2)$

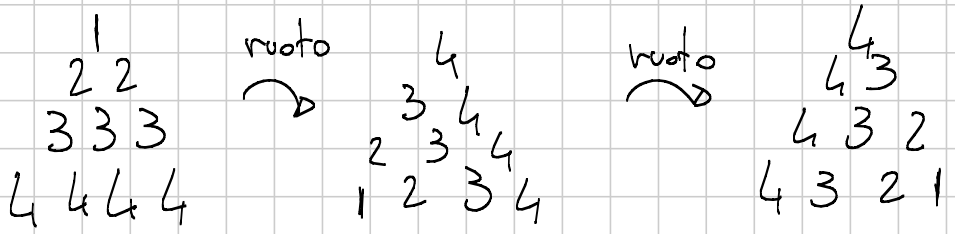
$\vdots$ $\vdots$ $\vdots$

Se dimostro $P(m,n) \Rightarrow P(m+1,n)$

$$P(m,n) \Rightarrow (m-1, n+1)$$

allora ho vinto...

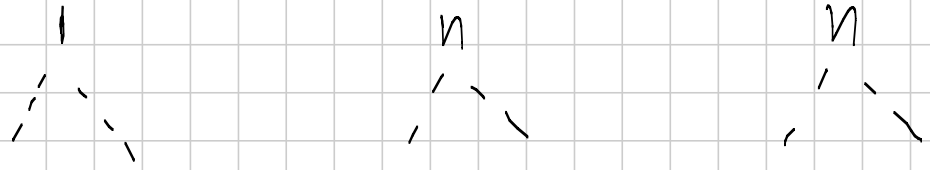
Dimostrazione "visiva" che $1^2+2^2+3^2+\dots+k^2 = \frac{k(k+1)(2k+1)}{6}$



Se sommo tutti i numeri nella stessa posizione, viene sempre $2n+1$

$$3\left(1^2+2^2+\dots+n^2\right) = (2n+1)\frac{n(n+1)}{2}$$

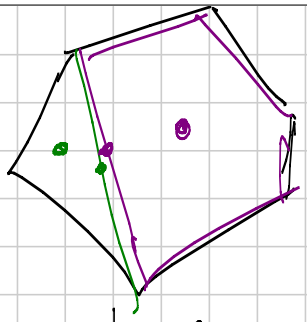
1) Se sommo quelli in cima, viene $2n+1$



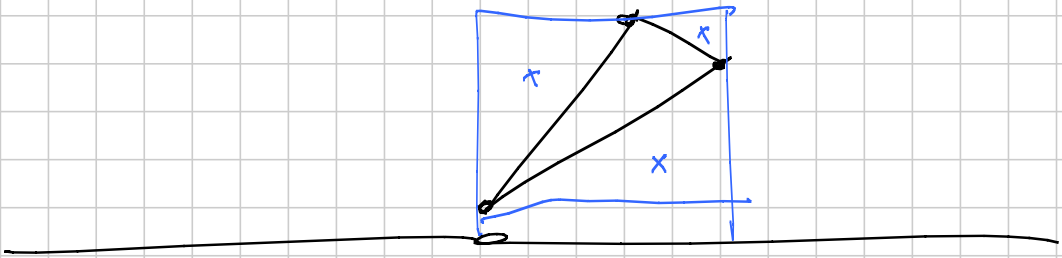
2) Se mi sposto ↗, su un triangolo sale di 1, su uno scende di 1, su uno resta uguale

3) Se mi sposto ↘

~ Pick



Mi basta dimostrarlo sui triangoli



ES: Teo: $F_{n+1}^2 + F_n^2 = F_{2n+1}$ $\quad P(n)$

$P(n+1)$: $F_{n+2}^2 + F_{n+1}^2 = (F_n + F_{n+1})^2 + F_{n+1}^2 =$

$= F_n^2 + 2F_nF_{n+1} + F_{n+1}^2 + F_{n+1}^2 = F_{2n+1} + 2F_nF_{n+1} + F_{n+1}^2$

...

$\overset{(\text{HOPE})}{=} F_{2n+3}$

Mi manca di dire che $2F_nF_{n+1} + F_{n+1}^2 = F_{2n+2}$

Provo a dimostrarlo per induzione

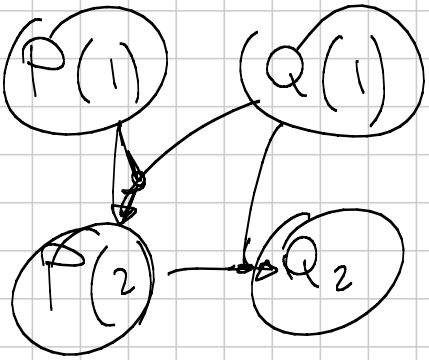
$Q(n)$: $2F_{n-1}F_n + F_n^2 = F_{2n}$

$Q(n+1)$: $2F_nF_{n+1} + F_{n+1}^2 = 2F_n(F_{n-1} + F_n) + (F_{n-1} + F_n)^2$

$= 2F_n F_{n-1} + 2F_n^2 + F_{n-1}^2 + F_n^2 + 2F_{n-1}F_n =$ (HOPE) $= F_{2n+2}$

$= 2F_{2n} + F_{n-1}^2 + F_n^2$

mi manca che $F_{n-1}^2 + F_n^2 = F_{2n-1}$? $P(n-1)$



$P(3)$ $Q(3)$

$P(4)$ $Q(4)$

Induzione "devo via qualcosa"

ES: $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{k^2} < 2$ $\frac{\pi^2}{6}$ (speranza vana)

$\frac{1}{1^2} + \dots + \frac{1}{k^2} + \frac{1}{(k+1)^2} \overset{IND}{<} 2 + \frac{1}{(k+1)^2} \dots < 2$

Invece, si riesce a dimostrare per induzione che

$$\sum_{k=1}^{n} \frac{1}{k^2} \leq 2 - \frac{1}{n} \qquad \text{(più forte)}$$

Facciamolo:

$$\sum_{k=1}^{n+1} \frac{1}{k^2} = \left(\sum_{k=1}^{n} \frac{1}{k^2}\right) + \frac{1}{(n+1)^2} \overset{\text{HP IND}}{\leq} 2 - \frac{1}{n} + \frac{1}{(n+1)^2} \qquad (*)$$

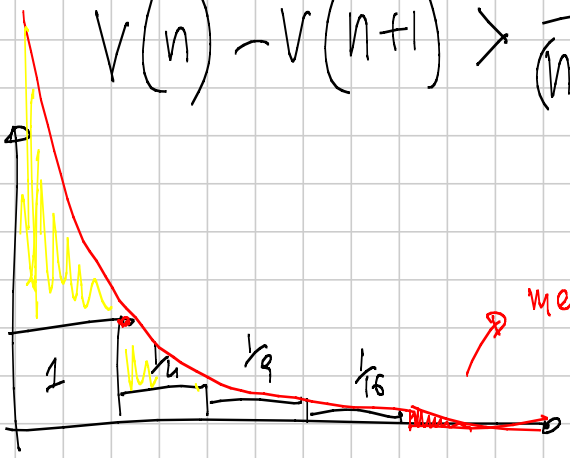
$$\text{(Hope)} \quad < 2 - \frac{1}{n+1}$$

$$\frac{1}{n} - \frac{1}{n+1} = \frac{n+1-n}{(n+1)n} = \frac{1}{n(n+1)} > \frac{1}{(n+1)^2}$$

$$\frac{1}{n} = \frac{1}{n+1} + \frac{1}{n(n+1)}$$

$$\sum_{k=1}^{n} \frac{1}{k^2} \leq 2 - V(n)$$

$$V(n) - V(n+1) > \frac{1}{(n+1)^2}$$



$$\text{mentre} \quad \int_n^{\infty} \frac{1}{x^2}\, dx = \frac{1}{n}$$

Funziona anche con altri esponenti: se devo sommare

$$\sum_{k=1}^{+\infty} \frac{1}{k^{3/2}} \leq (\text{costante})$$

cerco un "potenziale" che si comporti come

$$\int_n^{\infty} \frac{1}{x^{3/2}}\,dx = 2\,\frac{1}{x^{1/2}}$$

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \dots \to \infty$$

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \dots + \frac{1}{16} + \frac{1}{17} + \dots \quad \frac{1}{32} + \dots$$

VI: $\frac{1}{4} + \frac{1}{4} = \frac{1}{2}$ VII: $\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} = \frac{1}{2}$ VII: $\frac{8}{16} = \frac{1}{2}$

"Frazioni egizie"

$$\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}$$

$\frac{5}{6} = \frac{1}{2} + \frac{1}{3}$

$\frac{1}{6} + \frac{1}{6} + \dots + \frac{1}{6}$

Teo: ogni razionale si scrive come somme di frazioni distinte con numeratore 1

$\frac{17}{43} = \dots$

dim: (sbagliata)

$\frac{17}{43} = \frac{1}{43} + \frac{1}{43} + \dots$ $\quad \frac{1}{43}$

$= \frac{1}{44} + \frac{1}{43 \cdot 44}$ $\quad = \frac{1}{44} + \frac{1}{43 \cdot 44}$

$= \frac{1}{45} + \frac{1}{45 \cdot 46}$

Finisce questo procedimento? Mah...

dim (giusta): "greedy": metto sempre il termine più grosso che ci sta

Fase 1: $\frac{42}{13} = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{K}$

$\frac{1}{K}$ è tutti quelli che ci stanno

Arrivato al punto in cui non ci stanno più,

resto = $\frac{p_1}{q_1}$

ci metto il più grande $\frac{1}{n}$ che ci sta

$\frac{p_2}{q_2} = \frac{p_1}{q_1} - \frac{1}{n_1}$, dove n_1 è il più grande t.c. $\frac{1}{n_1} < \frac{p_2}{q_2}$

⋮

<u>Lemma</u>: se faccio questo, la successione dei numeratori $p_1, p_2, p_3, \dots$ è decrescente

$$\frac{p_{k+1}}{q_{k+1}} = \frac{p_k}{q_k} - \frac{1}{n_k} = \frac{n_k p_k - q_k}{q_k n_k}$$

$p_k > n_k p_k - q_k$ dev'essere vera altrimenti

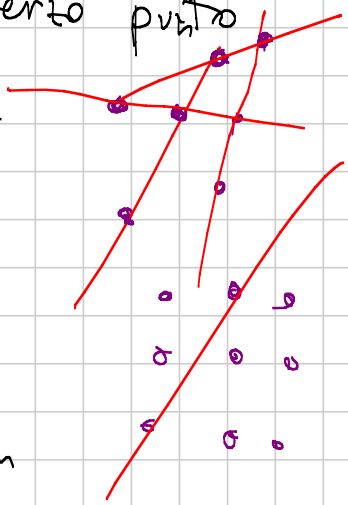
$(n_k - 1) p_k < q_k$ $\quad \frac{p_k}{q_k} < \frac{1}{n_k - 1}$, impossibile

perché ho scelto n_k = il minore che ci sta

RMM '09: variante con le arcotangenti (serve la formula della somma delle tg.)

Teo: Sylvester–Gallai

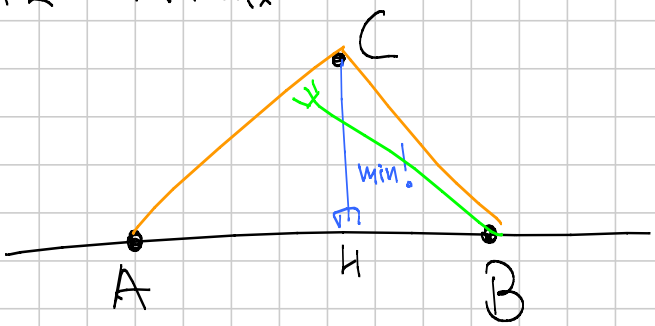
Dato un insieme S di n punti del piano, se $\forall A, B \in S$ esiste un terzo punto di S nella retta AB, allora sono tutti allineati.



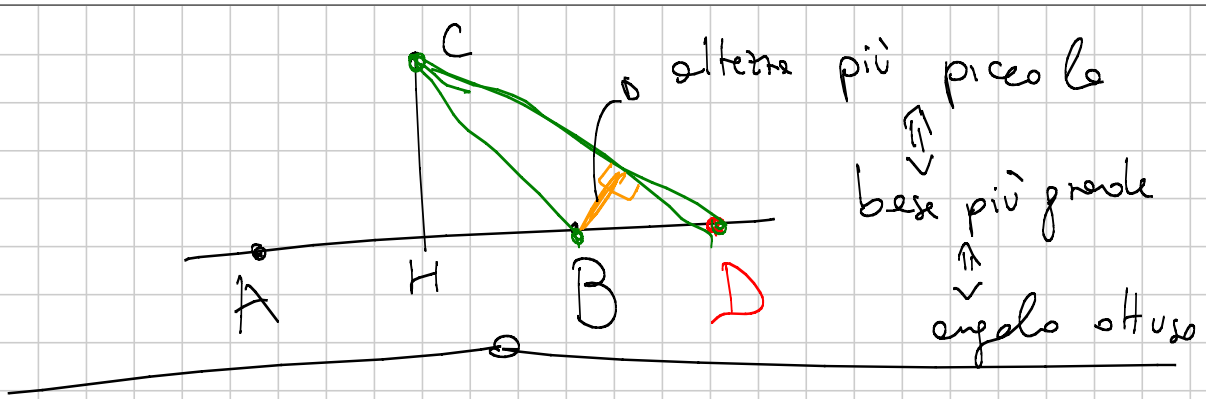
Dim:

Per induzione non viene: $S_{n+1} \Rightarrow S_n$ non si fa mantenendo l'ipotesi

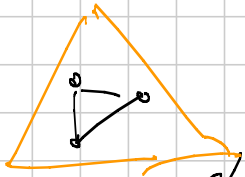
Invece viene con il principio del minimo: supponiamo non tutti allineati, e consideriamo la terna A, B, C tale che $dist(C, AB) \neq 0$ sia minima



CH altezza più piccola $\Rightarrow$ AB lato più grande



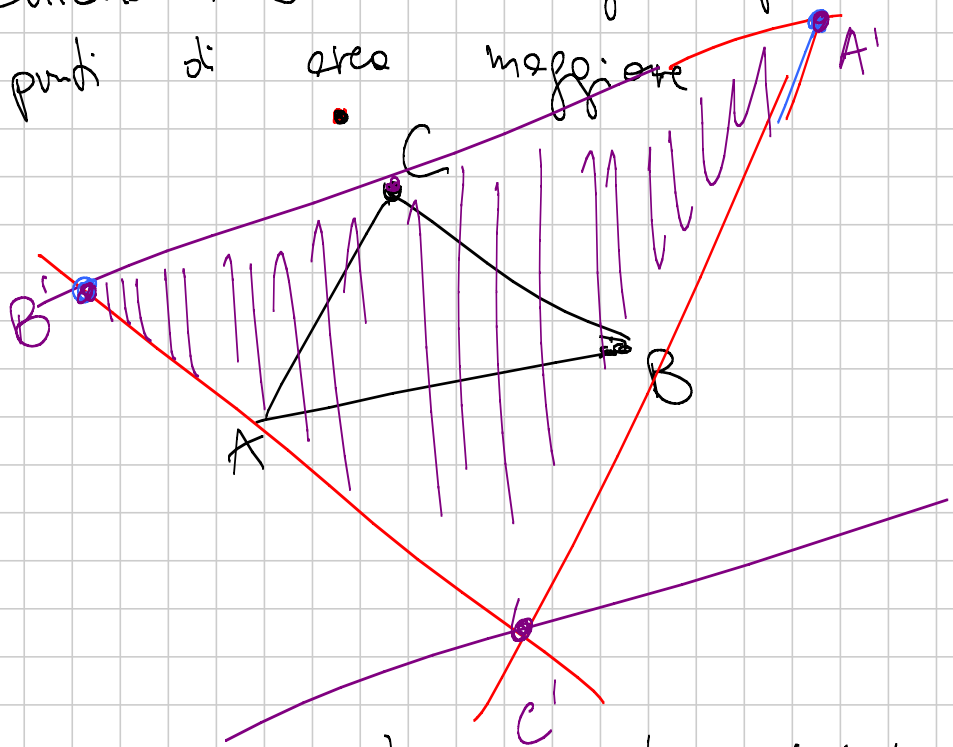
Variante.. Dato un insieme S_n di punti nel piano tali che $\forall A, B, C \in S$
$\text{Area}(ABC) < 1$



Allora stanno dentro un triangolo di area < 4

dim: cerco qualcosa di estremale...

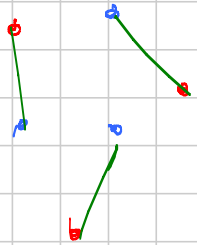
Chiamo ABC il triangolo fatto con questi punti di area massimale



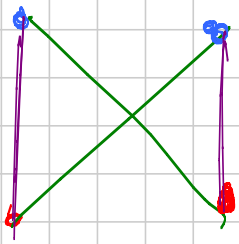
Tutti i punti stanno dentro $A'B'C'$

$$\text{Area}(A'B'C') = 4\,\text{Area}(ABC) < 1.$$

Teo: dati n punti rossi e n punti blu nel piano, esiste un modo di unirli a 2 a 2 (rosso–blu) in modo che non si intersechino.



Dim (giusta): prendo il modo di unirli con somma delle lunghezze dei segmenti minima. Se avessi



li rimpiazzo con i viola (rimpiazzo diagonali di un quadrilatero con lati).

Dim (sbagliata): parto da una configurazione a caso, se due si intersecano, li rimpiazzo, e continuo

Teo (sbagliato): 1 è il più grande

numero intero positivo.

Dim? : se il più grande fosse $M \neq 1$,

allora $M^2 > M$, assurdo

a, b, c $\quad$ $a-\varepsilon$ $b+\varepsilon$ c

≥4 PISE : DM 1° PIANO

NUOVI ≥H : MAGNA DM

ALTRI: INFORMATICA

A1 Medium Tess

Note Title 9/3/2016

Polinomi

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

Ci servono 2 proprietà sui coefficienti

ho le operazioni di $+$ e $\cdot$

un **Anello** è insieme con queste operazioni

la x non è un elemento dell'anello dei coefficienti
semplicemente distingue i coefficienti grado per grado

La **valutazione** è una funzione $p: A \to A$

$a \mapsto p(a)$

es. di Anelli: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$; $\mathbb{F}_p$ = gli interi mod p ← field

Se A è un anello, $A[x] := \{$ polinomi a coeff. in $A\}$

è ancora un anello

(se ho 2 polinomi posso sommarli e moltiplicarli)

Es: $\mathbb{Z}[x]$ è l'anello dei polinomi a coeff. interi

$\mathbb{Z}[x][y] = \mathbb{Z}[x,y]$ sono i polinomi in 2 variabili (a coeff. interi)

Se in A posso fare la divisione (inverso moltiplicativo)

chiamerò A un **campo**

es di campi: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$

non è vero che se K è un campo anche $K[x]$ lo è

Con i polinomi a coeff. in un campo avete

la **DIVISIONE EUCLIDEA**

(le operazioni usate sono solo $+, \cdot$, e si usa l'inverso del coefficiente di testa del divisore)

es: x^2+x+1 diviso $3x+1$ (in $\mathbb{Q}[x]$)

$Q = \frac{x}{3} + c$, $R = \frac{1}{9} + \frac{1}{3} + 1$

← l'inverso

Thm di Ruffini: $p(x) \in K[x]$ e $a \in K$

t.c. $p(a)=0 \Rightarrow p(x) = (x-a)q(x)$

Dim: potete fare la divisione tra $p(x)$ e $x-a$

$$p(x) = (x-a)q(x) + r(x)$$

$r(x)$: deg < 1

$\Rightarrow$ valutando in a viene $p(a) = r = 0$

Allora un polinomio non nullo di grado n ha al massimo n radici

Dim: per induzione

il passo base è che $p(x)$ non ha radici

il passo induttivo
- Ruffini
- legge di ann. del prodotto

$$p(x) = (x-a)q(x) \quad \text{(Ruffini)}$$

$q(x)$: ha grado 1 in meno di $p(x)$

una radice di p è radice di $x-a$ (legge ann. prod.) oppure di $q(x)$

Principio di identità dei polinomi

Supponete di avere $p(x)$ di grado $\leq n$ con $n+1$ radici, allora $p(x)$ è nullo

Dim: conseguenza dell'enunciato precedente

Variante se non sapete nulla sul grado di $p(x)$?

Mi bastano infinite radici.

Es: esiste un polinomio a coeff. in $\mathbb{Q}$ t.c.

$p(n) = 2^n \quad \forall\, n \in \mathbb{N}$?

No! $q(x) = p(x) - 2p(x-1)$ è un polinomio

è chiaro che $q(x)$ si annulla su $\mathbb{N}$

$\Rightarrow q(x) = 0$ (come uguaglianza sui polinomi)

$\Rightarrow p(x) = 2p(x-1)$

guardo il coeff. direttivo (= il coeff. di grado + alto)

sarà a_n:

$a_n = 2a_n \Rightarrow$ assurdo se $p(x)$ non è nullo

Altre conseguenze di Ruffini:

$a - b \mid a^n - b^n$

considero $p(a) = a^n - b^n \in \mathbb{Z}[b][a]$

$d(a) = a - b \in \mathbb{Z}[b][a]$

↑ è monico $\Rightarrow$ posso fare la DIV EUCL

$\Rightarrow$ " Ruffini

Ma $p(b)=0 \Rightarrow p(a) = (a-b)q(a)$

$\in \mathbb{Z}[b][a]$

$a-b \mid p(a)-p(b)$ (divisibilità tra interi se $p \in \mathbb{Z}[x]$)

$d(a)$ $f(a)$ (ma anche come polinomi a coeff. in $\mathbb{Z}[b]$)

$f(b)=0 \Rightarrow d(a) \mid f(a)$ per Ruffini

$a+b+c \mid a^3+b^3+c^3-3abc$

$d(a) \in \mathbb{Z}[b,c]$ $p(a) \in \mathbb{Z}[b,c][a]$

è monico!

Posso applicare Ruffini: infatti: $p(-b-c)=0$

$$p(a) = a^3 - (3bc)a + (b^3+c^3)$$

Es: IMO SL 2006 A6

$$|ab(a^2-b^2) + bc(b^2-c^2) + ca(c^2-a^2)| \le M(a^2+b^2+c^2)^2$$

determinare la migliore M che rende vera la dis.

$\forall a,b,c \in \mathbb{R}$

Oss 1 è che il termine in $|\cdot|$ si fattorizza!

Sia $p(a) \in \mathbb{Z}[b,c]$ il polinomio in $|\cdot|$

vale che $p(b) = 0$ (infatti $0 + bc(b^2-c^2) + cb(c^2-b^2) = 0$)

$\Rightarrow a-b \mid p(a)$

Ma allora $p(a,b,c)$ è multiplo di $(a-b),(b-c),(c-a)$

il quoziente $\dfrac{p(a,b,c)}{(a-b)(b-c)(c-a)}$ è ciclico in a,b,c

è di 1° grado $\Rightarrow ka+kb+kc$ per $k \in \mathbb{Z}$

viene $k=1$

IMO 2004 - 2

Determinare tutti i polinomi $p(x) \in \mathbb{R}[x]$

tali che

$$p(a-b) + p(b-c) + p(c-a) = 2p(a+b+c)$$

$\forall\, a,b,c \in \mathbb{R}$ t.c. $ab+bc+ca=0$

Oss. banale $p(0)=0$ (ponendo $a=b=c=0$)

Ponendo solo $a=b=0$

$$p(0) + p(-c) + p(c) = 2p(c)$$

$\Rightarrow \quad p(-c) = p(c) \qquad \forall\, c \in \mathbb{R}$

$\Rightarrow \quad p(-x) = p(x)$ come polinomi (principio di identità dei polinomi)

Guardando i coeff. di grado dispari

$\Rightarrow -a_{2n+1} = a_{2n+1}$ $\Rightarrow$ il polinomio ha solo termini di grado pari

Poniamo $a = 6\lambda$, $b = 3\lambda$, $c = -2\lambda$

$p(3\lambda) + p(5\lambda) + p(8\lambda) = 2\,p(7\lambda) \quad \forall \lambda \in \mathbb{R}$

$\Rightarrow$ vale l'uguaglianza dei coeff.

Guardo il termine di testa se $[x^n]\,p(x) = a_n$

$3^n a_n + 5^n a_n + 8^n a_n = 2 \cdot 7^n a_n$

$3^n + 5^n + 8^n = 2 \cdot 7^n$

$\Rightarrow$ ora so che non può essere n troppo grande

(se per esempio $8^n > 2 \cdot 7^n$ non è vera l'$=$)

(mi pare che si abbia $n < 6$)

Ora so che $p(x) = ax^4 + bx^2$

(in realtà questa è soluzione $\forall\, a, b \in \mathbb{R}$)

Supponiamo che $p(x), q(x) \in \mathbb{Z}[x]$ sono tali che

$p(n) \mid q(n) \quad \forall\, n \in \mathbb{Z}$ (mi bastano ∞ $n \in \mathbb{Z}$)

e che $p(x)$ sia monico

Allora $p(x) \mid q(x)$ (esiste $r \in \mathbb{Z}[x]$ t.c. $q(x) = p(x)r(x)$)

$\Rightarrow$ DIV EUCL.

$\forall\, q(x) = p(x)r(x) + s(x)$ con $\deg(s) < \deg(p)$

$r, s \in \mathbb{Z}[x]$

vedi: fondo pagina

Valuto x in n $\forall\, n \in \mathbb{Z}$

$$q(n) = p(n)r(n) + s(n)$$

$$\mathbb{Z} \ni \frac{q(n)}{p(n)} = r(n) + \frac{s(n)}{p(n)} \qquad \text{quindi } \frac{s(n)}{p(n)} \in \mathbb{Z}$$

hyp. $\quad \in \mathbb{Z}$

per $n \gg 0$ (n abbastanza grande)

deve essere $|p(n)| > |s(n)|$ (convincersene per esercizio)

(basta farlo quando $p(x) = x^m$)

$$\Rightarrow \left|\frac{s(n)}{p(n)}\right| < 1 \Rightarrow \frac{s(n)}{p(n)} = 0$$

$$\Rightarrow s(n) = 0 \quad \text{(ma è vero per } \infty \text{ } n\text{)}$$

(Si può dire qualcosa anche se p non è monico, anche in tal caso vale la div)

Sia $p(x,y) \in \mathbb{C}[x,y]$ t.c.

$p(t^3, t) = 0$ per ∞ $t \in \mathbb{C}$

Allora $x - y^3 \mid p(x,y)$

DIV EUCL. $x - y^3 \in \mathbb{C}[Y][X]$ è monico!

$p(x,y) = (x-y^3)q(x,y) + r(x,y)$

$\mathbb{C}[X][X]$ $\mathbb{C}[Y][X]$

La tesi è $r(x,y) = 0$

sapete già che $\deg_x(r(x,y)) < \deg_x(x-y^3)$

quindi: $r(x,y) = r(y)$

valutando $x = t^3$, $y = t$ $\forall t$ dell'ipotesi

$0 = p(t^3, t) = r(t)$

$\Rightarrow$ r è il polinomio nullo! (principio d'identità polinomi)

$p(x,y) \in \mathbb{C}[x,y]$ t.c.

$p(\sin\theta, \cos\theta) = 0$ $\forall \theta \in \mathbb{R}$

Allora $x^2+y^2-1 \mid p(x,y)$

DIV EUCL rispetto a x (x^2+y^2-1 è monico in x)

$$p(x,y) = (x^2+y^2-1)\,q(x,y) + r(x,y)$$

ora però $\deg_x(r(x,y)) < 2$

$$\Rightarrow r(x,y) = a_0(y) + x\,a_1(y)$$

l'ipotesi dice che $0 = a_0(\sin\theta) + \cos\theta\, a_1(\sin\theta)$

quindi: vorrei scrivere $0 = a_0(t) + \sqrt{1-t^2}\, a_1(t)$ e dire che è un polinomio

$$a_0^2(\sin\theta) = \cos^2\theta\, a_1^2(\sin\theta) = (1-\sin^2\theta)\, a_1^2(\sin\theta)$$

ora il polinomio $a_0^2(x) - (1-x^2)\,a_1^2(x) = 0$

$$a_0^2(x) = (1-x^2)\,a_1^2(x)$$

$$(1-x)^4(1+x)$$

conto il # di radici "1" a dx e a sx

$$\begin{matrix} \text{III} \\ 1 \pmod 2 \end{matrix} \not\equiv 0 \pmod 2$$

se a_0, a_1 sono non nulli

$$\Rightarrow a_0(y) = a_1(y) = 0$$

Es. per casa:

$a^n - b^n \mid a^m - b^m$ (come polinomi $\mathbb{Z}[a,b]$ $\mathbb{C}[a,b]$

oppure per $b \in \mathbb{Z}$ come polinomi in $\mathbb{Z}[a]$ o $\mathbb{C}[a]$

$\Downarrow$

$n \mid m$

oppure come divisibilità in $\mathbb{Z}$ (se $a, b \in \mathbb{Z}$))

Sia $p_k(a,b,c) \in \mathbb{Z}[a,b,c]$

$p_k(a,b,c) = a^k + b^k + c^k \quad \forall\, k \in \mathbb{N}$, $k > 0$

trovare tutte le coppie (n,m) t.c.

$p_n \mid p_m$

Sia $p(x,y,z) \in \mathbb{C}[x,y,z]$ t.c.

$p(\cos\alpha, \cos\beta, \cos\gamma) = 0 \quad \forall\, \alpha,\beta,\gamma$ angoli di un triangolo

[vale $\cos^2\alpha + \cos^2\beta + \cos^2\gamma + 2\cos\alpha\cos\beta\cos\gamma = 1$]

allora $x^2+y^2+z^2+2xyz-1 \mid p(x,y,z)$

Oss. sparse:

con i polinomi a coeff. in un campo potete fare il thm di Bezout ($(p,q)=1 \Rightarrow \exists\, a,b \in K[x]$ t.c. $ap+bq=1$)

avete le congruenze tra polinomi

es. dovete ottenere il resto della divisione di $x^{2016}+x^{1008}+x+1$ per x^2+x+1

vale che $x^2 \equiv -x-1 \pmod{x^2+x+1}$

$x^3 \equiv 1 \pmod{x^2+x+1}$

$x^{2016} \equiv x^{3(\cdots)} \equiv 1$

$x^{1008} \equiv 1$

$\Rightarrow$ il resto è $x+3$

Potete anche fare thm cinese su $x^2+x+1=(x-\xi)(x-\xi^2)$ con ξ 3-primitiva dell'unità

$p(x) \equiv a+b\xi \quad (x-\xi)$

$p(x) \equiv a'+b'\xi \quad (x-\xi^2)$

Interpolazioni

avete dei punti (x_0, y_0) … (x_n, y_n) con $x_i, y_i \in K$

gli x_i sono tutti diversi

volete trovare un polinomio $p(x) \in K[x]$ t.c. $p(x_i) = y_i$

Siano p_1, p_2 polinomi di grado $\leq n$

allora $p_1 = p_2$

infatti $p_1(x) - p_2(x)$ ha grado $\leq n$

con $x_0, \dots, x_n$ come radici (distinte)

$\Rightarrow$ è il polinomio nullo

Se avete un polinomio p che soddisfa, allora ce ne sono ∞

$p(x) + (x-x_0)\cdot\dots\cdot(x-x_n)\,q(x)$

soddisfa $\forall\, q \in K[x]$

Se voglio trovare p che soddisfa induzione su n

per $n=0$ voglio $p(x_0)=y_0$ ho $p(x)=y_0$

$n \Rightarrow n+1$ se p soddisfa per $x_0, \dots, x_n$

voglio p' che soddisfa per $x_0, \dots, x_{n+1}$

sarà $p'(x) = p(x) + (x-x_0)\cdot\dots\cdot(x-x_n)\,q(x)$

basta imporre $q(x) = C$ con C t.c.

$y_{n+1} = p(x_{n+1}) + (x_{n+1}-x_0)\cdot\dots\cdot(x_{n+1}-x_n)\,C$

$\neq 0$

Un altro modo è usare la linearità

osservo che se riesco a risolvere il problema

con $(x_0,1), (x_1,0), \dots, (x_n,0)$

e $(x_0,0), (x_1,1), \dots, (x_n,0)$

e $\vdots$

e $(x_0,0), (x_1,0), \dots, (x_n,1)$

allora so risolvere il problema anche per

$(x_0,y_0), (x_1,y_1), \dots, (x_n,y_n)$

Siano $L_0(x), \dots, L_n(x)$ [Si chiama metodo di Lagrange]

i polinomi che soddisfano gli $n+1$ problemi di cui sopra

allora $y_0 L_0 + y_1 L_1 + \dots + y_n L_n$ soddisfa il problema originale.

(basta valutare in $x = x_i \ \forall i$)

ad esempio

$L_0(x) = C\,(x-x_1)\cdot\dots\cdot(x-x_n)$

con C t.c. $\quad 1 = L_0(x_0) = C\,(x_0-x_1)\cdot\dots\cdot(x_0-x_n)$

$\neq 0$

Es: voglio $p(x)$ t.c. $p(n) = 2^n$ per $n = 0, 1, \dots, k$

$$p(x) = \sum_{n=0}^{k} \binom{x}{n} \qquad \binom{x}{n} := \frac{x(x-1)\cdots(x-n+1)}{n!}$$

(sto usando $\sum_n \binom{k}{n} = 2^n = (1+1)^n$)

Es bis: voglio $p(n) = \alpha^n \quad \alpha \in \mathbb{R}$ (per $n = 0, \dots, k$)

Uso $\left(1+(\alpha-1)\right)^n = \sum_{i=0}^{n} (\alpha-1)^i \binom{n}{i}$

Funzionerà $p(x) = \sum_{i=0}^{k} (\alpha-1)^i \binom{x}{i}$

Se voglio interpolare un polinomio a coeff. in $\mathbb{F}_p = \mathbb{Z}/p$

ottengo che qualsiasi funzione $f: \mathbb{Z}/p \to \mathbb{Z}/p$
è polinomiale di grado $\leq p-1$
(sto risolvendo un problema di interpolazione sui punti:
$X_i = i$ per $i = 0, \dots, p-1$)
$Y_i = f(i)$

Polinomi simmetrici
sono $p \in \mathbb{Z}[X_1, \dots, X_n]$
tali che $p = \tau p$ con $\tau = (i\,j)$ ← trasposizione
↑ cioè $p(X_0, \dots, X_{i-1}, X_j, X_{i+1}, \dots X_{j-1}, X_i, \dots)$
cioè scambio 2 variabili senza cambiare il polinomio

Es: se $n=1$, tutti
$n=2$ $a+b$, a^2+b^2, ab
$n=3$ $a+b+c$, $ab+bc+ca$, abc

Thm: fondamentale sui polinomi simmetrici in 3 variabili:

se $p \in \mathbb{Z}[a,b,c]$ simmetrico

$\Rightarrow \exists\ q \in \mathbb{Z}[x,y,z]$ t.c.

$$q(a+b+c,\ ab+bc+ca,\ abc) = p(a,b,c)$$

Eg: $a^3+b^3+c^3 = (a+b+c)^3 - 3(a+b+c)(ab+bc+ca)+3abc$

quindi: $q(x,y,z) = x^3 - 3xy + 3z$

Def: i coefficienti di

$$(x+x_1)(x+x_2)\cdots(x+x_n) \in \mathbb{Z}[x_1,\dots,x_n][x]$$

sono detti: polinomi simmetrici elementari, $e_1,\dots,e_n$

$e_1 = x_1+\dots+x_n$

Thm (fondamentale sui polinomi simmetrici)

Se $p \in \mathbb{Z}[x_1,\dots,x_n]$ è simmetrico

$\Rightarrow \exists\ q \in \mathbb{Z}[y_1,\dots,y_n]$ t.c.

$$p(x_1,\dots,x_n) = q(e_1,\dots,e_n)$$

Dim: induzione su n

$n=1$ (tutti i polinomi sono simmetrici) banale

$n \Rightarrow n+1$ So che tutti i polinomi in n variabili si scrivono ... come in tesi

voglio fare altrettanto per $n+1$ "

Posso fare così:

$p \in \mathbb{Z}[X_1, \dots, X_{n+1}]$

Oss: allora $p(X_1, \dots, X_n, 0)$ è simmetrico

$p(X_1, \dots, X_n, 0) = q(e_1, \dots, e_n)$ ← in n var.

Oss: e_i in $n+1$ variabili, se ne valuto una in 0

ottengo e_i in n variabili: ($\neq 0$ se $i = n+1$)

(segue facilmente dalla definizione degli e_i)

$r(\underline{X}) = p(X_1, \dots, X_n, X_{n+1}) - q(e_1, \dots, e_n)$ ← in $n+1$ var.

per Ruffini $(X_{n+1} - 0) \mid r(\underline{X})$

ma $r(\underline{X})$ è simmetrico in $n+1$ var. perché somma di simmetrici

quindi: $X_i \mid r(\underline{X}) \quad \forall i$

$\Rightarrow e_{n+1} \mid r(\underline{X})$

$\Rightarrow$ Concludo con induzione sul grado di p

ora $\dfrac{r(\underline{X})}{e_{n+1}}$ è simmetrico in $n+1$ variabili; ma il grado è $< p$

Naturalmente il P.B. è facile:

se fosse $\deg(p(\underline{X})) < n+1$ allora ho già ottenuto

$p(\underline{x}) = q(e_1, \dots, e_n)$ □

Es: esprimere $a^2+b^2+c^2$ in funzione delle simmetriche elementari

Sol: pongo $c=0$

$a^2+b^2 = e_1^2 - 2e_2 = q(e_1, e_2)$

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

$a^2+b^2+c^2 = e_1^2 - 2e_2$

Es per casa

Mostrare che se $q(x_1, \dots, y_n) \in \mathbb{Z}[x_1, \dots, y_n]$ tale che $q(e_1, \dots, e_n) = 0$ allora $q = 0$

(significa che $e_1, \dots, e_n$ sono indipendenti, cioè non si può esprimere qualsiasi polinomio simmetrico usando solo alcune delle simmetriche elementari)

$e_1^2 = e_2$ non si verificano

(qui $q(x,y) = x^2 - y$)

Sia $p(X_1, \dots, X_n) = \prod_{i<j} (X_i - X_j)^2$

mostrare che è simmetrico

e che se $q(e_1, \dots, e_n) = p(X)$, allora

$q(Y_1, \dots, Y_n)$ è irriducibile

(vuol dire $\nexists$ q_1, q_2 t.c. $q = q_1 \cdot q_2$ e q_1, q_2 non costanti)

Irriducibilità

Se $p(x) \in A[x]$ è irriducibile se

$\nexists$ $p_1(x), p_2(x)$ non costanti t.c.

$p(x) = p_1(x) p_2(x)$

Dipende moltissimo da A

Caso $A = \mathbb{C}$, ci sono solo polinomi di grado 1

(teorema fondamentale dell'algebra)

Caso $A = \mathbb{R}$, ci sono solo grado 1 e

grado 2 con $\Delta < 0$

(conseguenza del caso $A = \mathbb{C}$)

Casi $A=\mathbb{Q}$ e $A=\mathbb{Z}$

è vero che irriduc. su $\mathbb{Q}$ $\Rightarrow$ irriduc. su $\mathbb{Z}$

l'altra freccia è vera e si chiama lemma di Gauss

In $A=\mathbb{Z}$ ci sono alcuni criteri di irr.

ridurre mod p (ridurre i coeff.)

$q \in \mathbb{Z}[x]$ irr. di $\overline{q}$ in $\mathbb{Z}_p[x]$ $\Rightarrow$ irr di q su $\mathbb{Z}[x]$

es: x^2+x+1 mod 2 è irr.

Controllare le radici razionali

se $p(x) \in \mathbb{Z}[x]$ e r è una radice $\in \mathbb{Q}$

$r=\frac{n}{m}$ $(n,m)=1$ $\Rightarrow$ $n \mid p_0$, $m \mid p_{\deg(p)}$

$p(x)=\sum_{i=0}^{\deg p} p_i x^i$

Criterio di Eisenstein

se $p(x) \in \mathbb{Z}[x]$ ed esiste q primo t.c.

$q \mid$ tutti i coeff. di p, tranne il coeff. direttivo

e $q^2 \nmid$ il termine noto $\Rightarrow$ $p(x)$ è irriducibile.

es: $p(x)=x^{2016}-3$ è irr. per Eisenstein con $q=3$.

Senior 2016 - A2 medium - Ludo

Note Title 9/4/2016

(Disuguaglianze)

Riarrangiamento $a_1 \dots a_n$ $b_1 \dots b_n$ reali

$\sum a_i b_{\sigma(i)}$ σ permutazione

$a_1 \geq a_2 \geq \dots \geq a_n$ $\quad b_1 \geq b_2 \geq \dots \geq b_n$

$\sum a_i b_i$ è max $\quad \sum a_i b_{n+1-i}$ è min.

Se le disug. sono strette, sono uniche; altrimenti no.

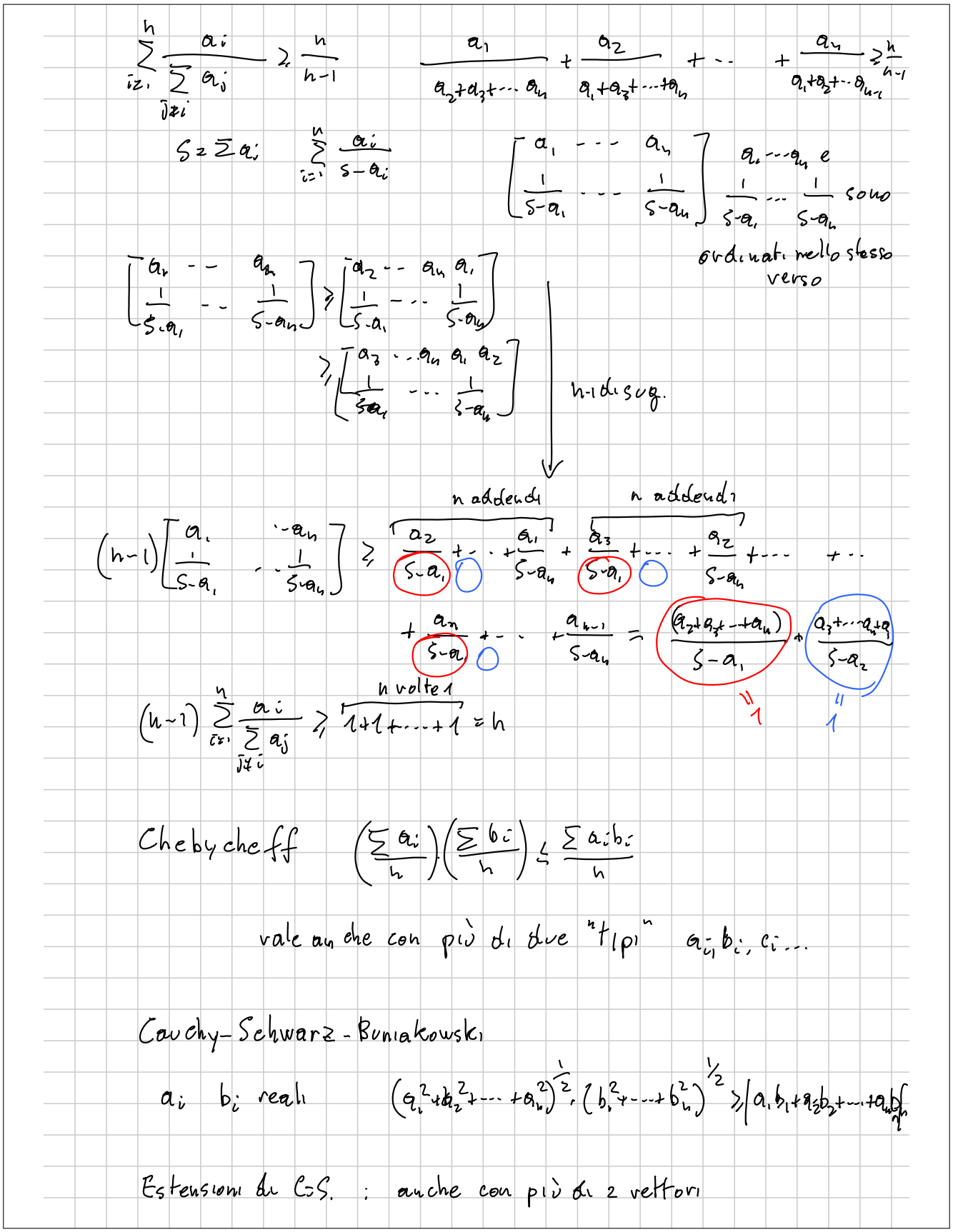
$\begin{bmatrix} a_1 & \dots & a_n \\ b_1 & \dots & b_n \end{bmatrix}$ Funziona anche con più di due "tipi".

$\begin{bmatrix} a_1 & \dots & a_n \\ b_1 & \dots & b_n \\ c_1 & \dots & c_n \end{bmatrix}$ Teo: Se a_i, b_i e c_i sono ordinate nello stesso "verso", la somma $\sum_{i=1}^{n} a_i b_{i} c_i$ è massima. Se non lo sono, il risultato è $\leq$ di questo massimo.

$a,b,c \geq 0$

$a^4+b^4+c^4 \geq a^2bc + b^2ac + c^2ba$ $\quad \begin{bmatrix} a^2 & b^2 & c^2 \\ a & b & c \\ a & b & c \end{bmatrix} \geq \begin{bmatrix} a^2 & b^2 & c^2 \\ b & a & c \\ c & b & a \end{bmatrix}$

Così, $\sum_{i=1}^{n} x_i^{n+1} \geq x_1 x_2 \dots x_n (x_1 + x_2 + \dots + x_n) \begin{bmatrix} x_1 & \dots & x_n \\ x_1 & & x_n \\ \vdots & & \vdots \\ x_1 & & x_n \end{bmatrix}_{n+1} \geq \begin{bmatrix} x_1 & x_2 & \dots \\ x_2 & x_3 & \\ x_3 & \ddots & \\ x_n & x_1 & \\ x_1 & x_2 & \end{bmatrix}$


$\sum_{i=1}^{n} \frac{a_i}{\sum_{j\neq i} a_j} \geq \frac{n}{n-1}$
$\frac{a_1}{a_2+a_3+\dots a_n} + \frac{a_2}{a_1+a_3+\dots+a_n} + \dots + \frac{a_n}{a_1+a_2+\dots a_{n-1}} \geq \frac{n}{n-1}$
$S = \sum a_i$ $\sum_{i=1}^{n} \frac{a_i}{S-a_i}$
$\begin{bmatrix} a_1 & \dots & a_n \\ \frac{1}{S-a_1} & \dots & \frac{1}{S-a_n} \end{bmatrix}$ $a_1 \dots a_n$ e $\frac{1}{S-a_1} \dots \frac{1}{S-a_n}$ sono ordinati nello stesso verso
$\geq \begin{bmatrix} a_2 & \dots & a_n & a_1 \\ \frac{1}{S-a_1} & \dots & \frac{1}{S-a_n} \end{bmatrix}$
$\geq \begin{bmatrix} a_3 & \dots & a_n & a_1 & a_2 \\ \frac{1}{S-a_1} & \dots & \frac{1}{S-a_n} \end{bmatrix}$
n-1 disug.
n addendi
n addendi
$(n-1)\begin{bmatrix} a_1 & \dots & a_n \\ \frac{1}{S-a_1} & \dots & \frac{1}{S-a_n} \end{bmatrix} \geq \frac{a_2}{S-a_1} + \dots + \frac{a_1}{S-a_n} + \frac{a_3}{S-a_1} + \dots + \frac{a_2}{S-a_n} + \dots$
$+ \frac{a_n}{S-a_1} + \dots + \frac{a_{n-1}}{S-a_n} = \frac{(a_2+a_3+\dots+a_n)}{S-a_1} + \frac{a_3+\dots+a_n+a_1}{S-a_2}$
$= 1$ $= 1$
n volte 1
$(n-1)\sum_{i=1}^{n} \frac{a_i}{\sum_{j\neq i} a_j} \geq 1+1+\dots+1 = n$
Chebycheff $\left(\frac{\sum a_i}{n}\right)\left(\frac{\sum b_i}{n}\right) \leq \frac{\sum a_i b_i}{n}$
vale anche con più di due "tipi" $a_i, b_i, c_i \dots$
Cauchy-Schwarz-Buniakowski
a_i b_i reali $(a_1^2+a_2^2+\dots+a_n^2)^{\frac{1}{2}} \cdot (b_1^2+\dots+b_n^2)^{\frac{1}{2}} \geq |a_1b_1+a_2b_2+\dots+a_nb_n|$
Estensioni di C-S. : anche con più di 2 vettori

$a_i, b_i, c_i \geq 0 \quad \left(a_1^3 + a_2^3 + \dots + a_n^3\right)^{\frac{1}{3}} \cdot \left(\sum b_i^3\right)^{1/3} \left(\sum c_i^3\right)^{\frac{1}{3}} \geq \left|\sum a_i b_i c_i\right|$

Con esponenti diversi: (Hölder) : $p, q > 0 \quad \frac{1}{p} + \frac{1}{q} = 1$

$$\left(a_1^p + a_2^p + \dots + a_n^p\right)^{\frac{1}{p}} \cdot \left(b_1^q + b_2^q + \dots + b_n^q\right)^{\frac{1}{q}} \geq \left|a_1 b_1 + a_2 b_2 + \dots + a_n b_n\right|$$

(anche questo con più di 2 vettori)

Quali altri pregi ha C.-S.? Talvolta è usata per "eliminare" frazioni o radicali.

IMO 2001/2 $a, b, c > 0 \quad \sum_{cyc} \frac{a}{\sqrt{a^2+8bc}} \geq 1$

$$\left(\frac{\sqrt{a}}{\sqrt[4]{\quad}}, \frac{\sqrt{b}}{\sqrt[4]{\quad}}, \frac{\sqrt{c}}{\sqrt[4]{\quad}}\right)\left(\sqrt[4]{\quad}, \sqrt[4]{\quad}, \sqrt[4]{\quad}\right)$$

$$\left(\sum_{cyc} \frac{a}{\sqrt{a^2+8bc}}\right) \cdot \left(\sqrt{a^2+8bc} + \sqrt{b^2+8ac} + \sqrt{c^2+8ab}\right) \geq \left(\sqrt{a}+\sqrt{b}+\sqrt{c}\right)^2$$

$$\left(\sum \frac{a}{\sqrt{a^2+8bc}}\right) \cdot \left(\sum \frac{a}{\sqrt{a^2+8bc}}\right) \cdot \left(\sum a(a^2+8bc)\right) \geq (a+b+c)^3$$

≥ 1 ?

Se $\sum a(a^2+8bc) \leq (a+b+c)^3$, ho vinto perché $\sum \frac{a}{\sqrt{a^2+8bc}}$ deve essere ≥ 1 perché valga la

$$\sum_{cyc} a(a^2+8bc) \le (a+b+c)^3$$

$$a^3+b^3+c^3 + 24abc \le a^3+b^3+c^3 + 3a^2b+3ab^2+\dots + 6abc$$

$$+2abc \qquad +2abc$$

$$8abc \le (a+b)(b+c)(c+a)$$

$$2 \quad 2 \quad 2 \qquad 4$$

IMO 2005/3 $x,y,z>0$ $xyz\ge 1$ $\sum_{cyc} \frac{x^5-x^2}{x^5+y^2+z^2} \ge 0$

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

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

$\frac{1}{x} \le yz$

$$\frac{yz+y^2+z^2}{x^2+y^2+z^2} \ge \frac{\frac{1}{x}+y^2+z^2}{x^2+y^2+z^2} \ge \frac{x^2+y^2+z^2}{x^5+y^2+z^2} + 1 - 1 = \frac{x^2+y^2+z^2-x^5-y^2-z^2}{x^5+y^2+z^2} + 1$$

$+1-1$

$$\frac{x^5-x^2}{x^5+y^2+z^2} \ge 1 - \frac{yz+y^2+z^2}{x^2+y^2+z^2} = \frac{x^2-yz}{x^2+y^2+z^2}$$

$$\sum_{cyc} \frac{x^5-x^2}{x^5+y^2+z^2} \ge \sum_{cyc} \frac{x^2-yz}{x^2+y^2+z^2} = \frac{1}{x^2+y^2+z^2} \sum_{cyc} x^2-yz \ge 0.$$

Lemma (Titu) [caso partic. di C.-S.]

$a_i, b_i > 0$ $\sum \frac{a_i^2}{b_i} \ge \frac{\left(\sum a_i\right)^2}{\sum b_i}$ $b_i = c_i^2$ $\left(\sum c_i^2\right)\left(\sum \frac{a_i^2}{c_i^2}\right) \ge \left(\sum a_i\right)^2$

$a_i > 0$ $i=1,\dots,6$ $\sum a_i = 7$ Qual è il $\min \sum_{i=1}^{6} \frac{i^2}{a_i}$?

$$\sum \frac{i^2}{a_i} \ge \frac{\left(\sum i\right)^2}{\sum a_i} = \frac{21^2}{7} = 63$$

C.-S. ha uguaglianza se $(a_i) = \lambda(b_i)$

$\left(\sqrt{a_i}\right) = \lambda\left(\frac{i}{\sqrt{a_i}}\right)$ $a_i = \lambda i$ $\sum_{7}^{a_i} = \lambda \sum_{21}^{i}$ $\lambda = \frac{1}{3}$

$a_i = \frac{i}{3}$

$\sum_{c} \frac{x^3}{(x+y)^2} \geq \frac{1}{4}$ $\quad \sum x = 1$

Lemma di Titu generalizzato:

$$\sum \frac{x_i^m}{a_i^{m-1}} \geq \frac{(\sum x_i)^m}{(\sum a_i)^{m-1}}$$

$$\sum \frac{x^3}{(x+y)^2} \geq \frac{(\sum x)^3}{\left(\sum (x+y)\right)^2} = \frac{1}{4}$$

$abc = 1$

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

$bc = x \quad ca = y \quad ab = z$

$$\sum_{cyc} \frac{b^2c^2}{a(b+c)} \geq \frac{(\sum bc)^2}{\sum a(b+c)} = \frac{(\sum x)^2}{2\sum x} \geq \frac{3\sqrt[3]{(abc)^2}}{2} = \frac{3}{2}$$

Medie

$a_1, \dots, a_n \geq 0$

$$M(s) = \left(\frac{a_1^s + \dots + a_n^s}{n}\right)^{1/s} \quad \text{se } s \neq 0$$

AM-GM, HM, QM

$$M(0) = \sqrt[n]{a_1 \cdot a_2 \cdot \dots \cdot a_n}$$

(si può fare anche pesata con $\lambda_i \leq 1$

$\left(\lambda_1 a_1^s + \lambda_2 a_2^s + \dots + \lambda_n a_n^s\right)^{1/s}$ è crescente con s

$$M_\lambda(0) = a_1^{\lambda_1} a_2^{\lambda_2} \dots a_n^{\lambda_n}$$

Weitzenböck: a, b, c lati di un triangolo di area A

$$a^2 + b^2 + c^2 \geq 4\sqrt{3}A$$

$$A = \sqrt{p(p-a)(p-b)(p-c)}$$

$$16A^2 = (a+b+c)(a+b-c)(a-b+c)(-a+b+c) \leq (a+b+c)^4$$

$$4A \leq (a+b+c)^2 = 9 \cdot \left(\frac{a+b+c}{3}\right)^2 \leq 9 \cdot \left(\frac{a^2+b^2+c^2}{3}\right)^{1/2}$$

$a+b+c=1 \quad a^a b^b c^c + a^b b^c c^a + a^c b^a c^b \leq 1.$

$$(a^a b^b c^c)^{\frac{1}{a+b+c}} \le \frac{a^2+b^2+c^2}{a+b+c}$$

$$(a^b b^c c^a)^{\frac{1}{a+b+c}} \le \frac{ab+bc+ca}{a+b+c}$$

$$(a^c b^a c^b)^{\frac{1}{a+b+c}} \le \frac{ac+ba+cb}{a+b+c}$$

$$\text{LHS} \le \frac{(a+b+c)^2}{a+b+c} = a+b+c = 1$$

(Bunching)

Schur a,b,c $\quad [3,0,0]+[1,1,1] \ge 2[2,1,0]$ $\qquad \sum_s a^3 + \sum_s abc \ge 2\sum_s a^2 b$

$$\sum_{a,c} a(a-b)(a-c) \ge 0$$

Schur $\quad [a+2b,0,0]+[a,b,b] \ge 2[a+b,b,0] \qquad a,b \ge 0$

$$[a+2b+k,k,k]+[a+k,b+k,b+k] \ge 2[a+b+k,b+k,k]$$

$$\sum \frac{x^5-x^2}{x^5+y^2+z^2}$$

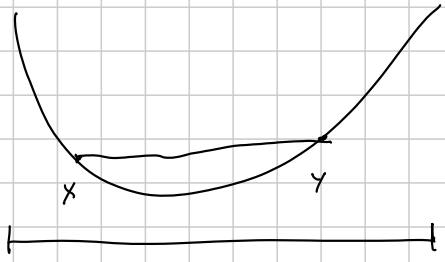
$$[10,1,1]+[6,3,3] \ge 2[8,2,2]$$

$$[9,0,0]+[5,2,2] \ge 2[7,1,1]$$

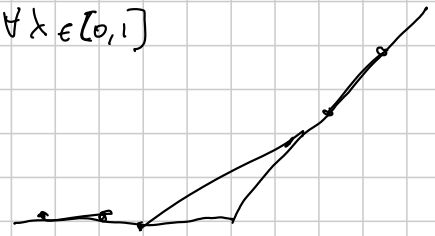
$$\ge 2[7,2,0] \ge 2[7,1,1]$$

$$[10,1,1]+4[7,5,0]+[6,3,3] \ge 2[6,5,1]+[8,2,2]+[6,5,2]+2[6,4,2]$$

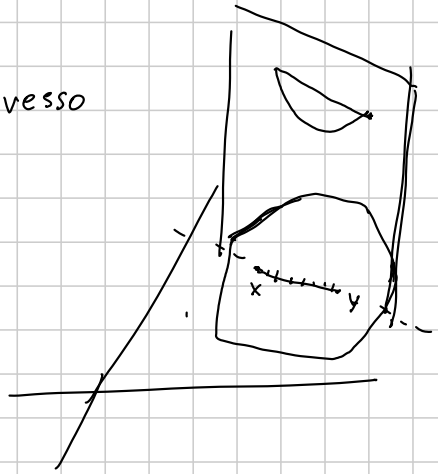
Funzioni convesse :



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



f di due variabili definita su un convesso



Dis. Jensen: $0 \leq \lambda_i \leq 1$ $\sum \lambda_i = 1$ se f è convessa,

$$f(\lambda_1 x_1 + \lambda_2 x_2 + \dots + \lambda_n x_n) \leq \lambda_1 f(x_1) + \lambda_2 f(x_2) + \dots + \lambda_n f(x_n)$$

Dis. Karamata f convessa. Supp. che $(x_i) \succcurlyeq (y_i)$

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

$\sum x_i = \sum y_i$

$x_1 \geq y_1$

$x_1 + x_2 \geq y_1 + y_2$

$x_1 + x_2 + x_3 \geq y_1 + y_2 + y_3$

$\vdots$

$x^\alpha \quad \alpha \geq 1 \quad x \geq 0$ convessa

$x^\alpha \quad 0 < \alpha < 1 \quad x \geq 0$ concava (stesse di sug. e converso opposto)

$\frac{1}{x}$, $\frac{1}{\sqrt{x}}$, $-\log x$ $\qquad \sum \lambda_i x_i \geq \prod x_i^{\lambda_i}$

$\sum \frac{a}{\sqrt{a^2+8bc}}$ $\left[\frac{1}{\sqrt{x}} \text{ convessa; pesi } a,b,c\right] \geq \frac{1}{\sqrt{\sum a(a^2+8bc)}}$

omog. $\Rightarrow$ posso supp. $a+b+c=1$

$a=\lambda_1 \quad b=\lambda_2 \quad c=\lambda_3 \quad x_1 = a^2+8bc \quad x_2 = b^2+8ac \quad x_3 = c^2+8ab \quad f(x) = \frac{1}{\sqrt{x}}$.

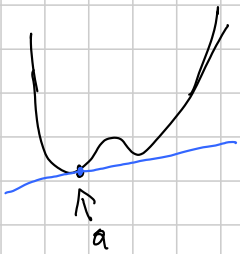
$\Leftrightarrow \sum a(a^2+8bc) \le (a+b+c)^3$

$\sum_c \frac{1}{a+b} \le \sum_c \frac{1}{2a}$ $\qquad f(x)=\frac{1}{x}$ $\qquad a\ge b\ge c$

$\sum_c \frac{a_{i+1}^3}{a_i} \ge \sum a_i^2$ $\qquad a_i = e^{\log x_i}$ $\qquad (a+b, a+c, b+c) \prec (2a, 2b, 2c)$

e^x conv. $\qquad 2a \ge a+b$

$2a+2b \ge a+b+a+c$



Trucco della tangente.

Se $f(x) \ge f(a) + f'(a)(x-a)$

$\sum f(x_i) \ge \sum [f(a)+f'(a)(x_i-a)] = n(f(a)+a\cdot f'(a)) + f'(a)\cdot \sum x_i$

Piccolo elenco di cose che non vedremo: Newton, MacLaurin, Ravi,

i) Dis. geom. : $a,b,c\ge 0$ $\qquad a+b+c=abc$ $\qquad \sum_c \frac{1}{\sqrt{1+a^2}} \le \frac{3}{2}$.

$a=\tan\alpha$
$b=\tan\beta$
$c=\tan\gamma$

$\sum_c \cos\alpha \le \frac{3}{2}$

$1+4\operatorname{sen}\frac{\alpha}{2}\operatorname{sen}\frac{\beta}{2}\operatorname{sen}\frac{\gamma}{2}$ $\qquad \log \sin x$ f. conv.

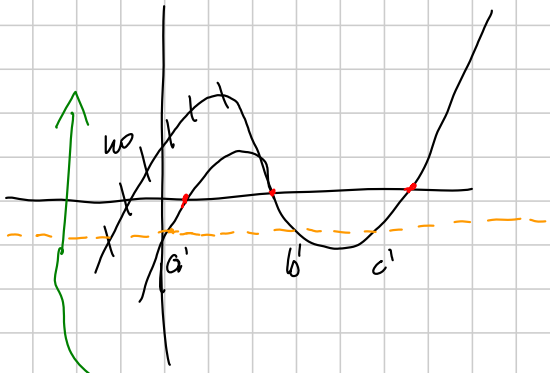
Metodo ABC (o SPQ, o PQR) $\qquad$ Tre variabili $a,b,c\ge 0$

disuguaglianza simmetrica in a,b,c. $\rightarrow$ tutto si può scrivere in termini di $S=a+b+c$, $P=abc$, $Q=ab+bc+ca$ (teo. Newton)

Una funzione simm. f di grado ≤ 5 in $a,b,c\ge 0$ ha massimo e

minimo o dove (almeno) due tra a,b,c sono uguali, o dove uno (almeno) di essi è 0, (se f è monotona in P)

Costruiamo $g(x)=(x-a)(x-b)(x-c)=x^3-Sx^2+Qx-P$



$\tilde{f}(S,Q,P)=$

$SQ+Q^2+S^4+SP$

$(a,b,c)\to(S,Q,P)$

$(a',b',c')\to(S,Q,P')$

come trovo $P'>P$ (a',b',c'), in cui f è più grande?

Traslo il grafico

$\to$ grafico di $g(x)+k$

le radici di $g(x)+k$, a',b',c', sono t.c.

$(x-a')(x-b')(x-c')=x^3-Sx^2+Qx-P+k$

$$f(a',b',c')=\tilde{f}(S,Q,P-k)=f(S,Q,P)-Sk<f(S,Q,P)$$

Quindi (a,b,c) non è minimo (e se traslo al contrario, non è massimo),

se non posso traslare, una è 0 o due sono uguali.

Così per ogni f simm. in a,b,c, di grado ≤ 8 con il coeff. di P^2 positivo. Es. $(ab+bc+ca)\left(\frac{1}{(a+b)^2}+\frac{1}{(b+c)^2}+\frac{1}{(c+a)^2}\right)\ge\frac{9}{4}$ IRAN '96.

~~(con normalizzazione)~~

Hölf-degree principle, teoria dei points of incidence.

SENIOR 2016 – ALGEBRA 3 (Max)

Note Title 05/09/2016

Algebra 3: → Successioni
→ Eq. Funzionali

SUCC. PER RICORRENZA LINEARI

Succ. di ordine

$$x_{n+1} = a x_n + b \qquad \forall n \in \mathbb{N}$$
$$x_0 \text{ DATO}$$

Obiettivo: trovare formula generale

1ª idea Boriamo pure

x_0

$x_1 = a x_0 + b$

$x_2 = a^2 x_0 + ab + b$

$x_3 = a^3 x_0 + a^2 b + ab + b$

Idea: $x_n = a^n x_0 + b(1 + a + a^2 + \dots + a^{n-1})$

$= a^n x_0 + b \frac{a^n - 1}{a - 1}$

Congettura: $\boxed{x_n = a^n x_0 + b \frac{a^n - 1}{a - 1}}$

Dimostro per induzione

↑ se $a \neq 1$, altrimenti è ancora più banale

2ª idea Facciamo finta che sia $b = 0$ $\qquad x_{n+1} = a x_n \rightsquigarrow x_n = x_0 a^n$

Cerco di ridurmi a questa situazione

Pongo $y_n := x_n + l$. Vedo cosa risolve y_n:

$$y_{n+1} = x_{n+1} + l = a x_n + b + l = a(y_n - l) + b + l = a y_n - al + b + l$$

scelgo l in modo che sia $= 0$

$l = \frac{b}{a-1}$ $\qquad y_n = y_0 a^n$ $\qquad x_n = y_n - l = y_0 a^n - l$

$\rightsquigarrow$ si conclude e si ottiene la formula di prima

3ª idea $x_{n+1} = a x_n + \text{roba}(n)$ $(n^2+2,\ 2^n,\ n^n)$

Mettiamo di conoscere per qualche motivo **UNA** succ. z_n che risolve la ricorrenza

$$z_{n+1} = a z_n + \text{roba}(n)$$

(Magari $z_0 \neq x_0$ e quindi non è la soluz. del pbm. dato)

Allora dico che **TUTTE** le soluz. della ricorrenza sono del tipo

$$x_n = \boxed{c\,a^n} + \boxed{z_n}$$

$c\,a^n$: soluzione generale se roba$(n) \equiv 0$; costante arbitraria

z_n: soluz. speciale che ho

Se questo è vero, allora posso scegliere c in modo da rispettare x_0 come voglio.

Dim. Ci sono 2 cose da dim.

① Tutte le x_n scritte sopra risolvono la ricorrenza

$$x_{n+1} = c\,a^{n+1} + z_{n+1} = c\,a^{n+1} + a z_n + \text{roba}(n) = a\overbrace{(c a^n + z_n)}^{x_n} + \text{roba}(n)$$

② Tutte le x_n che risolvono la ricorrenza si scrivono come sopra. Sia x_n che risolve, cioè

$$x_{n+1} = a x_n + \text{roba}(n)$$
$$z_{n+1} = a z_n + \text{roba}(n)$$

Chiamo

$$d_n := x_n - z_n$$

e vedo che risolve $d_{n+1} = a d_n \rightsquigarrow d_n = \underbrace{c}_{\text{do}} a^n$

$$x_n - z_n = c\,a^n \rightsquigarrow x_n = c a^n + z_n$$

Tornando a $x_{n+1} = a x_n + b$ posso cercare una z_n costante che la risolve $z_n \equiv l$

$$l = al + b \quad \rightsquigarrow \quad l = \frac{b}{1-a} = z_n$$

$$x_n = c\,a^n + \frac{b}{1-a} \qquad \text{(se conosco } x_0 \text{ trovo } c\text{)}$$

— o — o —

Esercizio $x_{n+1} = 3x_n + n^2$ $\qquad x_n = c\,3^n + z_n$

Provo con z_n = polinomio di 2° grado $\qquad z_n = an^2 + bn + c$

Sostituisco

$$\underbrace{a(n+1)^2 + b(n+1) + c}_{z_{n+1}} = \underbrace{3an^2 + 3bn + 3c}_{3z_n} + n^2$$

Espando il LHS e uguaglio i coeff. delle potenze di n

$$\begin{cases} a = 3a + 1 \\ 2a + b = 3b \\ a + b + c = 3c \end{cases} \quad \rightsquigarrow \text{trovo } a, b, c$$

Esercizio $x_{n+1} = 3x_n + 7^n$ $\qquad$ Provo $z_n = a\,7^n \rightsquigarrow a7^{n+1} = 3a7^n + 7^n$

$\rightsquigarrow 7a = 3a + 1$

Caso critico: $x_{n+1} = 3x_n + 3^n \quad \rightsquigarrow 3a = 3a + 1$ ☹

$z_n = an3^n \qquad a(n+1)3^{n+1} = 3an3^n + 3^n$

$a(n+1)3 = 3an + 1 \qquad 3a = 1$

Per approfondire: LEZIONI ANALISI 1 PER MATEMATICA

Ordine 2 (Poi l'ordine n è uguale)

$$x_{n+2} = a x_{n+1} + b x_n + \text{roba}(n)$$

Quando roba$(n) \equiv 0$ la soluzione si ottiene dal pol. caratteristico

$x^2 - ax - b = 0 \rightsquigarrow$ radici λ e $\mu \rightsquigarrow$ $\boxed{x_n = c_1 \lambda^n + c_2 \mu^n}$

Se c'è la roba la soluzione è del tipo $x_n = \boxed{c_1 \lambda^n + c_2 \mu^n}$ (sol. gen. se roba $\equiv 0$) $+ \boxed{z_n}$ (sol. speciale da trovare in qualche modo)

Ripasso: perché la formula con roba $\equiv 0$ funziona?

1ª oss. Se x_n e y_n sono 2 soluz., allora $x_n + y_n$ è ancora sol.

2ª oss. Se x_n risolve e c è una costante, allora $c x_n$ risolve

1ª + 2ª oss. Se x_n e y_n risolvono, allora $c_1 x_n + c_2 y_n$ risolve

3ª oss. Cerco delle soluz. che siano esponenziali $x_n = k^n$

$k^{n+2} = a k^{n+1} + b k^n \rightsquigarrow k^2 = ak + b \rightsquigarrow$ se k risolve eq. car. ho trovato una sol.

4ª oss. Chi mi dice che non ci sono altre soluzioni?
Fissati x_0 e x_1, posso trovare c_1 e c_2 in modo che la formula $c_1 \lambda^n + c_2 \mu^n$ rispetti la ricorrenza e le condizioni x_0 e x_1.
Tutti i valori successivi sono univoc. det. da x_0 e x_1.

—o—o—

Riassunto / generalizzazione

→ Per ricorrenze di ordine k non omogenee (cioè con roba (n)) una lineari

$$x_{n+k} = a_1 x_{n+k-1} + a_2 x_{n+k-2} + \dots + \text{roba}(n)$$

la soluzione generale è del tipo

$$x_n = y_n + z_n$$

z_n: soluzione qualunque da individuare

y_n: sol. gen. stessa ricor. ma con roba $(n) \equiv 0$

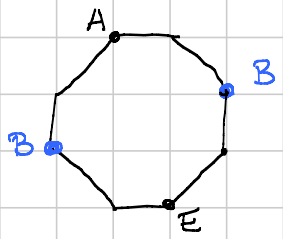
→ y_n si determina a partire dalle radici del pol. caratteristico.

→ Occhio al caso in cui ci sono radici multiple e al caso in cui la roba (n) contiene un esponenziale che ha come base una radice dell'eq. caratt.

—o—

Successioni per ricorrenza escono spesso in comb. enumerativa (vedi TI #5)

IMO 1979-6 Trovare quanti sono i percorsi lunghi n che
→ partono da A
→ arrivano in E
→ prima non sono mai stati in E



Detto P_n il numero dei percorsi, intanto $P_{2n+1} \equiv 0$

A_n = percorsi lunghi n che arrivano in A (senza mai passare da E)
B_n = " " " " " " un B (")

Osservo che A_n e B_n sono $\equiv 0$ sui dispari.

Sui pari vale $\quad A_{2m+2} = 2A_{2m} + B_{2m}$

$B_{2m+2} = 2A_{2m} + 2B_{2m}$

Tecnica dello shift

$$B_{2m+4} = 2A_{2m+2} + 2B_{2m+2} = 4A_{2m} + 2B_{2m} + 2B_{2m+2}$$

(2^a con shift inoltre; A_{2m+2} dalla 1^a)

$$= 2B_{2m+2} - 4B_{2m} + 2B_m + 2B_{2m+2}$$

(A_{2m} dalla 2^a)

Concludendo

$$B_{2m+4} = 4B_{2m+2} - 2B_{2m}$$

$x^2 - 4x + 2 = 0 \quad 2 \pm \sqrt{2}$ ... da cui la formula per B_{2m}.

Dalla formula per B_{2m} trovo quello che serve.

— o — o —

IMO 2005 – 4 $\quad a_n = 2^n + 3^n + 6^n - 1$

Per ogni primo p esiste $n \in \mathbb{N}$ t.c. $p \mid a_n$

$a_n = 2^n + 3^n + 6^n - 1^n$ Caso speciale di una ricorrenza di ordine 4 le cui radici del polinomio caratteristico sono $1, 2, 3, 6$

$$a_{n+4} = \alpha a_{n+3} + \beta a_{n+2} + \gamma a_{n+1} + \delta a_n \qquad x^4 - \alpha x^3 - \beta x^2 - \gamma x - \delta = 0$$

ha come radici $1, 2, 3, 6$

Inoltre non ho problemi a calcolare

a_0, a_1, a_2, a_3

Oss. chiave : $a_{-1} = 0$ e quindi sarà 0 modulo tutti i p

Altra osservazione: la formula modulo p è periodica se $p \neq 2, 3$ perché le potenze sono periodiche, quindi a_{-1} prima o poi ritorna

Capito questo, possiamo fare un'altra soluzione: le potenze ciclano con periodo $p-1$, quindi

$$0 \leftrightarrow p-1$$
$$-1 \leftrightarrow p-2$$

Considero $n = p-2$. $\quad a_{p-2} = 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$

Moltiplico per 6: $\quad 6\,a_{p-2} = 3\cdot 2^{p-1} + 2\cdot 3^{p-1} + 6^{p-1} - 6$

$$\equiv 3 + 2 + 1 - 6 \equiv 0 \pmod p$$

Se $p \neq 2, 3$ $\quad p \mid a_{p-2}$

Più "brutal mode" $\quad 2^{p-2} = \dfrac{2^{p-1}}{2} \equiv \dfrac{1}{2} \pmod p$

Controllare $p=2$ e $p=3$ a mano

$$a_{p-2} \equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1.$$

Oss. Le formule per le ricorrenze valgono anche modulo p, ma ovviamente le radici del pol. caratteristico vanno trovate mod p.

EQUAZIONI FUNZIONALI

EQ. CAUCHY $f(x+y) = f(x) + f(y)$

- Se cerco soluzioni $f: \mathbb{Q} \to \mathbb{R}$ trovo solo le funz. lineari

$$f(x) = \lambda x \qquad \lambda = f(1)$$

Dim.
→ $f(0) = 0$ Pongo $\lambda = f(1)$
→ $f(n) = \lambda n \quad \forall n \in \mathbb{N}$ (induzione)
→ $f(n) = \lambda n \quad \forall n \in \mathbb{Z}$ ($y = -x$ e vedo che è dispari)
→ $f(nx) = n f(x) \quad \forall n \in \mathbb{N} \quad \forall x \in \mathbb{Q}$ (induzione)
→ Se $x = \frac{p}{q}$, allora $f(q \cdot x) = q f(x)$
$f''(p)$
$''\lambda p \rightsquigarrow f(x) = \lambda \frac{p}{q}$

- Se cerco soluzioni $f: \mathbb{R} \to \mathbb{R}$, allora ce ne sono anche di orribili, ma sono soltanto le solite $f(x) = \lambda x$ se so qualcosa in più, a scelta tra
  → f è monotona
  → f è continuità
  → f è loc. limitata dall'alto o dal basso
  → esiste un rettangolo nel piano che non contiene al suo interno pti del grafico di f
  (questo dice che le altre soluzioni sono davvero orribili)

Le soluzioni orribili si ottengono con le basi di HAMEL.

BASI DI HAMEL Un sottoinsieme $B \subseteq \mathbb{R}$ si dice

- un insieme di generatori se ogni numero reale x è comb. lin. finita a coeff. in $\mathbb{Q}$ di elem. di B, cioè si scrive come

$$x = q_1 b_1 + \dots + q_k b_k \qquad q_1, \dots, q_k \in \mathbb{Q} \quad (k \text{ dipende da } x)$$
$$b_1, \dots, b_k \in B$$

- un insieme linearmente indipendente se l'unica comb. lin. di el. di B a coeff in $\mathbb{Q}$ che fa 0 è quella con tutti i coeff. nulli, cioè

$$q_1 b_1 + \dots + q_k b_k = 0 \quad \Rightarrow \quad q_1 = \dots = q_k$$

Def. Una base di Hamel è un qualunque sottoinsieme $B \subseteq \mathbb{R}$ che sia un insieme di generatori e linearmente indip.

Esercizio facile Per ogni $x \in \mathbb{R}$, la scrittura come comb. lin. di el. di B è UNICA

Dim.: se ne avessi due DIVERSE, portando dalla stessa parte avrei una scrittura di 0 non banale.

Teorema difficile Esistono delle basi di Hamel in $\mathbb{R}$.

Basi di Hamel ed eq di Cauchy Data una $B \subseteq \mathbb{R}$ base di Hamel scelgo un numero reale λ_b per ogni $b \in B$.
Dato $x \in \mathbb{R}$, lo scrivo come

$$x = q_1 b_1 + \dots + q_k b_k \quad \text{e pongo} \quad f(x) = q_1 \lambda_{b_1} b_1 + \dots + q_k \lambda_{b_k} b_k$$

Si verifica che questa risolve la Cauchy (esercizio!)

Dim $y = \bar{q}_1 b_1 + \dots + \bar{q}_k b_k$ (posso supporre di usare gli stessi b_i per scrivere x e y)

Ma allora

$$(x+y) = (q_1+\bar{q}_1) b_1 + \dots + (q_k+\bar{q}_k) b_k$$

$$f(x+y) = (q_1+\bar{q}_1)\lambda_{b_1} b_1 + \dots + (q_k+\bar{q}_k)\lambda_{b_k} b_k$$

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

—o—o—

Esercizio Le soluzioni ottenute con la base di Hamel sono tutte

—o—o—

Esercizio Esistono $f : \mathbb{R} \to \mathbb{R}$
$g : \mathbb{R} \to \mathbb{R}$
periodiche tali che

$$f(x) + g(x) = x \qquad \forall x \in \mathbb{R}$$

(Quando uno lo risolve ha capito la base di Hamel).

—o—o—

VARIANTI DELLA CAUCHY

- $f(x+y) = f(x) + f(y) + a$ (numero dato)

$$\underbrace{f(x+y)+a}_{g(x+y)} = \underbrace{f(x)+a}_{g(x)} + \underbrace{f(y)+a}_{g(y)}$$

$\rightsquigarrow \quad g(x) = \lambda x \quad \rightsquigarrow \quad f(x) = \lambda x - a$

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

$$f(\overbrace{x+a}^{z} + \overbrace{y+a}^{w} - a) = f(x+a-a) + f(y+a-a)$$

$f(z+w-a) = f(z-a) + f(w-a)$ $\quad g(x) := f(x-a)$

$\rightsquigarrow g(x) = \lambda x \rightsquigarrow f(x) = g(x+a) = \lambda(x+a) = \lambda x + \lambda a$

- $f(x+y+a) = f(x) + f(y) + b$

Metto insieme le 2 idee precedenti

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

$y = w+a \rightsquigarrow f(x+w+a) = f(x+a) + f(w+a)$
In alternativa
$x+a = w \rightsquigarrow f(w+y-a) = f(w) + f(y) \rightsquigarrow$ come prima

- $f(x+y) = f(x) \cdot f(y) \rightsquigarrow$ le soluzioni sono del tipo $f(x) = \lambda^x$ (su $\mathbb{Q}$)

[Dim.: volendo si ripercorre la strada della dim. originaria

$\rightsquigarrow$ se $f(0) = 0$ allora $f(x) = 0$, altrimenti $f(0) = 1$ e posto $f(1) = \lambda$ conquisto $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$

In alternativa dimostro in qualche modo che $f(x) > 0$ sempre e poi prendo $g(x) := \log_\lambda f(x)$

$g(x+y) = \log_\lambda f(x+y) = \log_\lambda f(x) + \log_\lambda f(y) = g(x) + g(y)$]

- $f(x \cdot y) = f(x) + f(y) \rightsquigarrow f(x) = \log_\lambda x$
- $f(xy) = f(x) \cdot f(y) \rightsquigarrow f(x) = x^\lambda$

— o — o —

NORDIC 1998 $f : \mathbb{Q} \to \mathbb{Q}$

$$f(x+y) + f(x-y) = 2f(x) + 2f(y) \qquad \forall x \in \mathbb{Q}, \forall y \in \mathbb{Q}.$$

- $P(0,0)$: $2f(0) = 4f(0) \rightsquigarrow f(0) = 0$
- $P(0,y)$: $f(y) + f(-y) = 2f(y) \rightsquigarrow f(y) = f(-y) \Rightarrow$ PARI

Pongo $\lambda = f(1)$

- $P(x,x)$: $f(2x) = 4f(x) \quad \forall x \in \mathbb{R} \quad (f(2) = 4\lambda)$
  (sembra ragionevole che le soluz. siano $f(x) = \lambda x^2$)
- $P(2x,x)$: $f(3x) + f(x) = 2f(2x) + 2f(x)$
  $= 8f(x) + 2f(x)$
  $\rightsquigarrow f(3x) = 9f(x)$

$\rightsquigarrow$ per induzione $f(nx) = n^2 f(x)$ (sistema $\mathbb{N}$ e $\mathbb{Z}$ essendo pari)

Ora uso $x = \frac{p}{q}$ e $n = q$

$$\lambda p^2 = f(p) = f\left(q \cdot \frac{p}{q}\right) = q^2 f\left(\frac{p}{q}\right) \rightsquigarrow f\left(\frac{p}{q}\right) = \lambda \left(\frac{p}{q}\right)^2.$$

— o — o —

INIETTIVITÀ E SURGETTIVITÀ Come si comportano per composizione ?

$g(f(x))$
- → Se f e g sono iniettive, allora la comp. è iniettiva
- → f e g surg, allora la composizione è surg.
- → Se $g(f(x))$ è iniettiva, allora $f(x)$ lo è
- → Se $g(f(x))$ è surgettiva, allora $g(x)$ lo è

Lo stesso vale se ho composizione di k funzioni. Da iu./surg. della comp., posso dedurre solo info. sulla + interna o esterna.

Esercizio Farsi esempi in cui f iniettiva
g non iniettiva
$g(f(x))$ iniettiva

e idem per suriettività

Esercizio $f(x+y) = f(f(x)) + f(f(y))$ $\quad f: \mathbb{Q} \to \mathbb{Q}$

$P(x,0)$: $f(x) = f(f(x)) + f(f(0))$
$P(0,y)$: $f(y) = f(f(y)) + f(f(0))$

$f(x+y) = f(x) + f(y) - 2f(f(0))$ $\rightsquigarrow$ affini
$\quad -0 \quad -0 -$

Esempio 1 $f(xf(y) + f(x)) = 2f(x) + xy$ $\quad f: \mathbb{R} \to \mathbb{R}$

Ci sono x e y fuori $\rightsquigarrow$ sfruttabili per iniett. e surg.

$P(1,y)$: $f(f(y) + f(1)) = \underbrace{2f(1) + y}_{\text{surg./iniett.}}$

$\Rightarrow f$ (pensata come esterna) è suriettiva
$\Rightarrow f$ " " interna è iniettiva

Prendo $x_0 \in \mathbb{R}$ tale che $f(x_0) = 0$

$P(x_0, y)$: $f(x_0 f(y)) = x_0 y$

$P(x, x_0)$: $f(f(x)) = 2f(x) + xx_0$

$P(x_0, x_0)$: $f(0) = x_0^2$

poco utili

$P(0,y)$: $f(f(0)) = 2f(0)$

$P(x,0)$: $f(xf(0) + f(x)) = 2f(x)$

Se uno sapesse che $f(0) = 0$ $\rightsquigarrow$ $f(f(x)) = 2f(x)$

$f(y) = 2y$

essendo f suriettiva y è un qualunque numero reale.

$P(x_0,0)$: $f(x_0 f(0)) = 0$ ma per iniettività $x_0 f(0) = x_0$

quindi $\rightarrow$ $f(0) = 1$ oppure $x_0 = 0$.

D'altra parte sapevamo che $f(f(0)) = 2f(0)$

$f(1) = 2$

$f(0) = x_0^2$. se fosse $f(0) = 1$ avremmo $x_0^2 = 1$

$\rightsquigarrow$ $x_0 = 1$ oppure $x_0 = -1$ (vedi fondo file)

ci stiamo perdendo...

— o — o —

Esercizio 2 $f(f(x) - y) = 2x + f(f(y) - x)$ $f : \mathbb{R} \to \mathbb{R}$

$P(x, f(x))$: $f(0) = 2x + f(f(f(x)) - x)$

$f(\text{mostro}) = \underbrace{f(0) - 2x}_{\text{surg.}}$ $\Rightarrow$ f suriettiva

Sia $x_0 \in \mathbb{R}$ t.c. $f(x_0) = 0$

$P(x_0, x_0)$: $f(-x_0) = 2x_0 + f(-x_0)$ $\rightsquigarrow$ $x_0 = 0$

$P(x,x)$: $f(\cancel{f(x)} - x) = 2x + f(\cancel{f(x)} - x)$

$\rightsquigarrow$ impossibile

Aggiunto dopo video: il testo corretto (facile e istruttivo) è

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

segno +

Esercizio 3 $f(f(x)+y) = f(x^2-y) + 4yf(x)$ $\quad f:\mathbb{R}\to\mathbb{R}$

Provare a rendere uguali due f: $f(x)+y = x^2-y$

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

$P\left(x, \frac{x^2-f(x)}{2}\right)$ $\quad f(\dots) = f(\dots) + 4\,\frac{x^2-f(x)}{2}\,f(x)$

$f(x)=0$ oppure $f(x)=x^2$. Bisogna escludere il "mistoue"

Supponiamo che $f(a)=0$ $\quad a\neq 0$

$f(b)=b^2$ $\quad b\neq 0$

Sostituisco e vedo che succede

$P(a,b)$: $f(b) = f(a^2-b) \rightsquigarrow f(a^2-b) = b^2$

"b^2"

Due casi $\quad 0 = b^2 \rightsquigarrow b=0$

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

$a^4 - 2a^2b + b^2 = b^2$

$a^2(a^2-2b) = 0$

$a^2 = 2b$

Se esiste un $b\neq 0$ t.c. $f(b)=b^2$, allora l'unico valore a t.c. $f(a)=0$ risolve $a^2=2b$.

Tutti i valori tranne $\pm\sqrt{2b}$ devono andare nel quadrato

Ci sono al max 3 valori di a t.c. $f(a)=0$ e questi 3 valori devono risolvere $a^2=2b$ per tutti gli altri b.

Assurdo.

— o — o —

IMO 1996 – 6 $\quad f(x-f(y)) = f(f(y)) + xf(y) + f(x) - 1$

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

$P(f(y), y)$: $\quad f(0) = 2f(f(y)) + f(y)^2 - 1$

$\rightsquigarrow f(f(y)) = \frac{f(0)+1}{2} - \frac{1}{2}f(y)^2$

$\rightsquigarrow f(x) = k - \frac{1}{2}x^2$ Potremmo farlo se fosse surgettiva

Se fosse surgettiva, sarebbe questa, ma allora non sarebbe surgettiva

$P(f(z), y)$: $f(\boxed{f(z)-f(y)}) = f(f(y)) + f(z)f(y) + f(f(z)) - 1$

$= k - \frac{1}{2}f(y)^2 + f(z)f(y) + k - \frac{1}{2}f(z)^2 - 1$

$= f(0) - \frac{1}{2}\left[\boxed{f(z)-f(y)}\right]^2$

$f(x) = f(0) - \frac{1}{2}x^2$ per ogni x che è diff. di due immagini

Resta da dim. che ogni reale è diff. di due immagini

Se $f(x) \equiv 0$ non va bene, quindi $\exists\, y_0 \in \mathbb{R}$ t.c. $f(y_0) \neq 0$

$P(x, y_0)$: $f(x - f(y_0)) = f(f(y_0)) + x f(y_0) + f(x) - 1$

$f(x - f(y_0)) - f(x) = \underbrace{f(f(y_0)) - 1 + x f(y_0)}_{\text{reale qualunque}}$

— o — o —

BMO 2007 – 2 $f(f(x)+y) = f(f(x)-y) + 4y f(x)$

$f(x) \equiv 0$ è una soluzione

$P(x, f(x))$: $f(2f(x)) = f(0) + 4f(x)^2$ $\quad f(z) = f(0) + z^2$ per ogni $z \in 2\,\text{Im}$.

$\boxed{y = 2f(z) - f(x)}$ $\quad f(2f(z)) = f(2f(x) - 2f(z)) + 8f(z)f(x) - 4f(x)^2$

$f(0)+4f(z)^2 = f(2(f(x)-f(z))) + 8f(z)f(x) - 4f(x)^2$

$\rightsquigarrow f[2(f(x)-f(z))] = f(0) + 4[f(x)-f(z)]^2$

$\rightsquigarrow f(y) = f(0) + y^2$ per ogni y che $2(\mathrm{Im}-\mathrm{Im})$

Basta la suriettività di $\mathrm{Im}-\mathrm{Im}$.

— o — o —

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

$P(x,0) = f(x)^2 + f(0) = f(f(x))$ $\qquad f(z) = f(0) + z^2$ sull'immagine

$y = -f(z)$: $f(x)^2 - 2f(x)f(z) + f(-f(z)) = f(f(x)-f(z))$

$\Vert$ ← se fosse pari

$f(f(z))$

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

$y = -f(x)$: $f(x)^2 - 2f(x)^2 + f(-f(x)) = f(0)$

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

— o — o —

Aggiunto dopo video: BACK to esercizio 1 (più difficile del previsto)

① $P(1,y) \Rightarrow$ iniettiva e suriettiva. Sia $x_0 \in \mathbb{R}$ t.c. $f(x_0) = 1$

② $P(x_0, 0) \Rightarrow f(x_0 f(0)) = 0 \Rightarrow$ per iniettività $x_0 f(0) = x_0 \Rightarrow$ $f(0)=1$ oppure $x_0 = 0$

③ Se $x_0 = 0$, allora $f(x) = 2x$, ma questa non verifica, quindi $f(0) = 1$

④ $P(x_0, x_0) \Rightarrow x_0^2 = 1 \Rightarrow x_0 = \pm 1$

⑤ $P(0,y) \Rightarrow f(1) = 2$, quindi $x_0 = -1$

⑥ Dovrebbe potersi dimostrare che $f(z) = z+1$ per ogni $z \in \mathbb{Z}$.

⑦ $P(x,-1) \Rightarrow f(f(x)) = 2f(x) - x$

⑧ $P(x,-2) \Rightarrow f(f(x)-x) = 2(f(x)-x)$

⑨ Scelto z t.c. $f(z) = f(x) - x$, confrontando ⑦ e ⑧ ottengo che $z = 0$, quindi $f(x) = x+1$.

Senior 2016 - C1 Medium (Anér)

Note Title 9/2/2016

Permutazioni

Def Una perm. è una funzione bigettiva

$$\sigma : \{1, \dots, n\} \longrightarrow \{1, \dots, n\}$$

Composizione Se σ e τ sono permutazioni su $\{1, \dots, n\}$, anche $\sigma \circ \tau$ lo è

$$\sigma \circ \tau : \{1 \dots n\} \longrightarrow \{1 \dots n\}$$

$$\sigma \circ \tau\,(i) = \sigma\big(\tau(i)\big)$$

S_n = insieme delle perm. su $\{1, \dots n\}$

In S_n c'è l'identità, $\forall \sigma \in S_n$ c'è l'inversa di σ, vale a dire $\sigma^{-1} \in S_n$

$$\sigma^{-1}\big(\sigma(i)\big) = i \qquad \forall i \in \{1, \dots n\}$$

Esempio $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$ $n=5$

Decomposizione in cicli

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 2 & 5 & 3 & 4 \end{pmatrix} = (2\ 6\ 4\ 5\ 3)(1)$$

$\sigma(2)=6 \quad \sigma(6)=4 \quad \sigma(4)=5 \quad \sigma(5)=3$

Composizione di trasposizioni

Una trasposizione è una perm. che fissa tutti gli elementi di $\{1, \dots n\}$ tranne due, i e j, che vengono scambiati

$$\begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ 1 & 2 & \dots & j & \dots & i & \dots & n \end{pmatrix}$$

Fatto Ogni permutaz. si può ottenere componendo alcune trasposizioni

Segno di una perm

Data $\sigma \in S_n$

poniamo $\operatorname{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j} = \pm 1$

OSS $\operatorname{sgn}(\sigma \circ \tau) = \prod_{1 \le i < j \le n} \frac{\sigma\circ\tau(i) - \sigma\circ\tau(j)}{i - j} =$

$$= \prod_{1 \le i < j \le n} \left(\frac{\sigma \cdot \tau(i) - \sigma \cdot \tau(j)}{\tau(i) - \tau(j)} \quad \frac{\tau(i) - \tau(j)}{i - j} \right) =$$

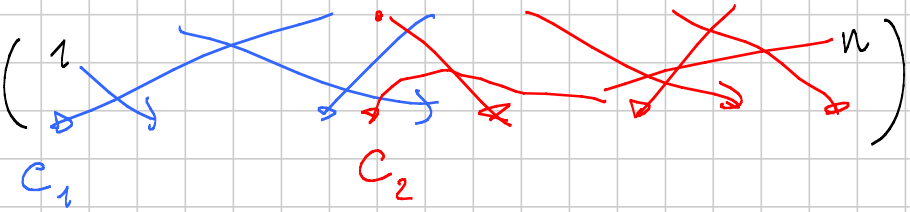
$$= \prod_{1 \le i < j \le n} \underbrace{\left(\frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \right)}_{\frac{\sigma(j') - \sigma(i')}{j' - i'}} \cdot sgn(\tau) = sgn(\sigma) \cdot sgn(\tau)$$

con $i' = \tau(i)$ $j' = \tau(j)$

non importa quale tra i' e j' è maggiore

Sia ora $\sigma = c_1 \cdot c_2 \cdot c_3 \cdot \ldots \cdot c_k$

$\sigma = \begin{pmatrix} 1 & \cdots & n \end{pmatrix}$



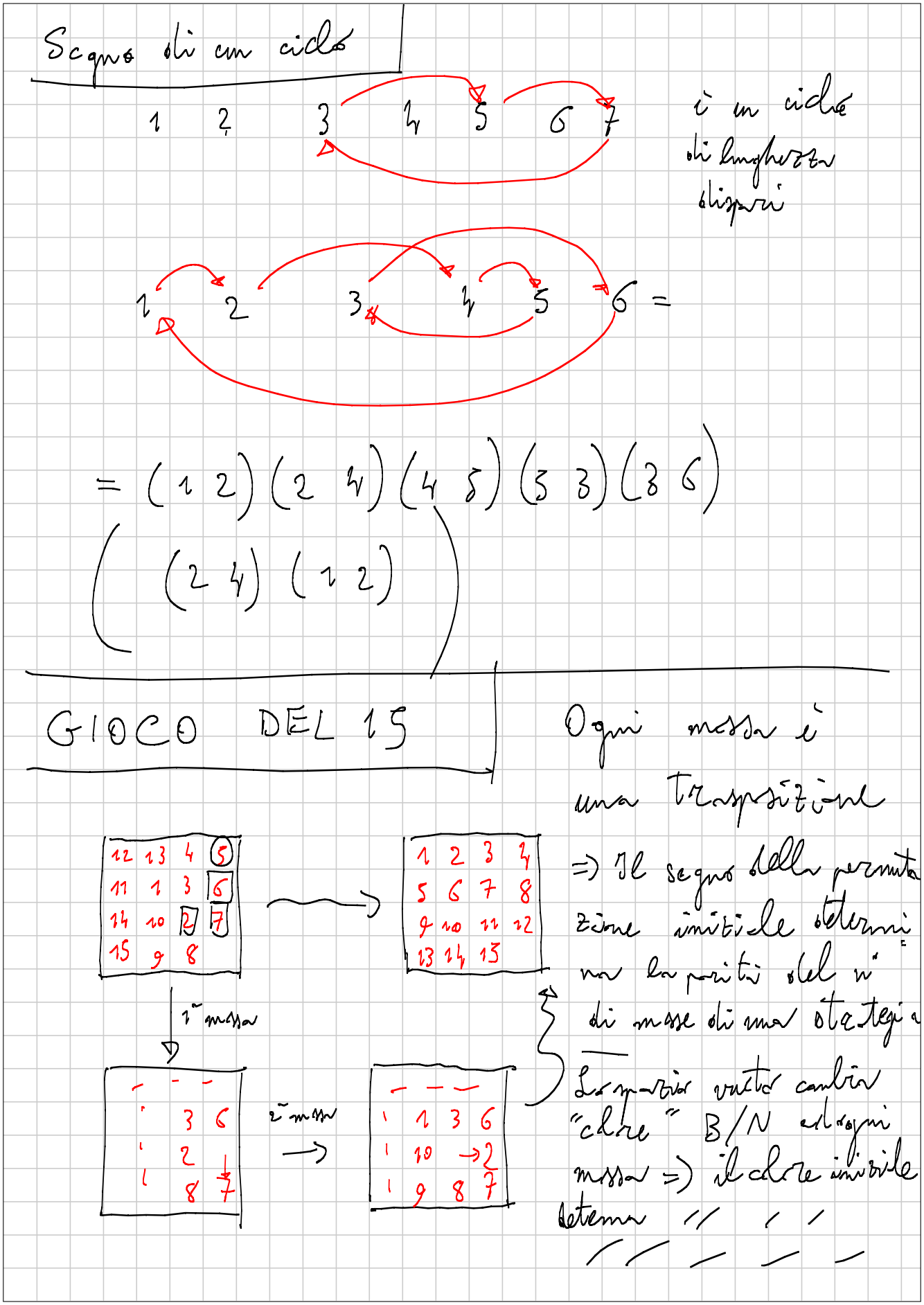
$|c_i|$ = lunghezza del ciclo c_i

$$sgn(\sigma) = \prod_{i=1}^{k} sgn(c_i) = \prod_{i=1}^{k} (-1)^{|c_i|-1} =$$

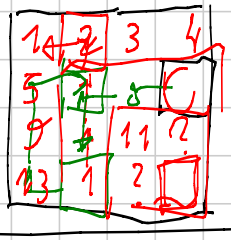
$= (-1)^{(\text{parità del numero di cicli di lungh. pari nella decomposizione})}$

Se $\sigma = \tau_1 \cdot \ldots \cdot \tau_h$ trasposizioni

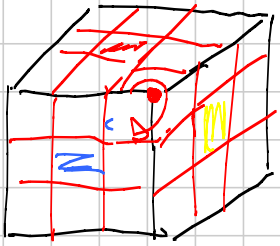
Allora $(-1)^h = sgn(\sigma)$


Segno di un ciclo
1 2 3 4 5 6 7
è un ciclo di lunghezza dispari
1 2 3 4 5 6 =
= (1 2)(2 4)(4 5)(5 3)(3 6)
((2 4)(1 2))
GIOCO DEL 15
Ogni mossa è una trasposizione
⇒ Il segno della permutazione iniziale determina la parità del n° di mosse di una strategia
La mossa vuota cambia "colore" B/N ad ogni mossa ⇒ il colore iniziale determina
1ª mossa
2ª mossa

Se i due invarianti mod 2 coincidono, esiste una strategia

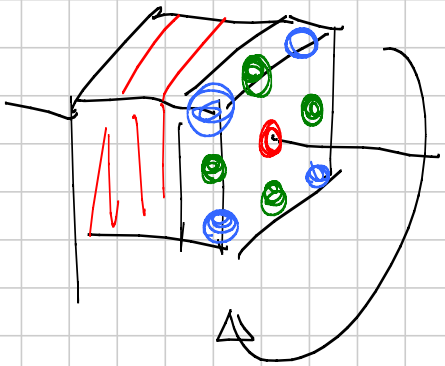


CUBO DI RUBIK



- Definisco un invariante facilmente calcolabile
- verificare che non varia durante le mosse

Una mossa del cubo di Rubik permuta i cubetti permuta anche le facce

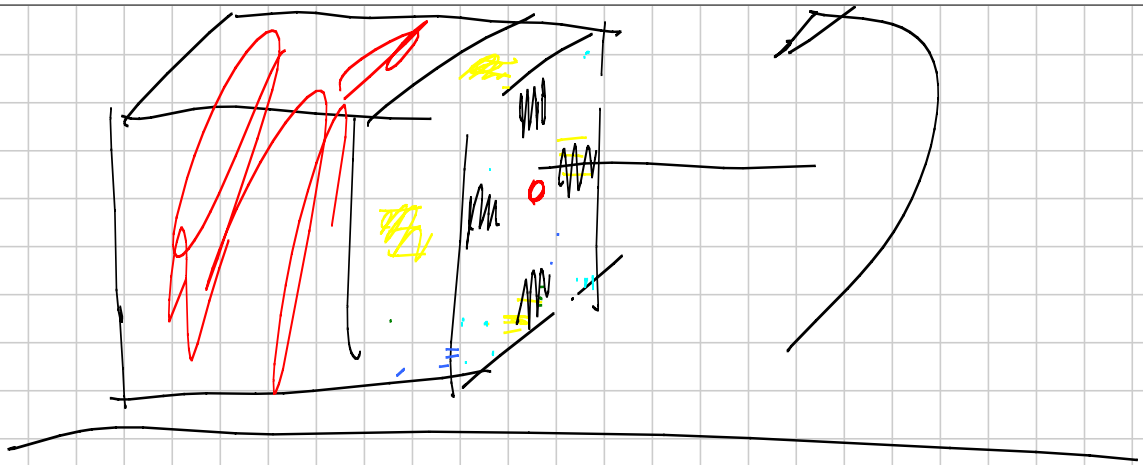


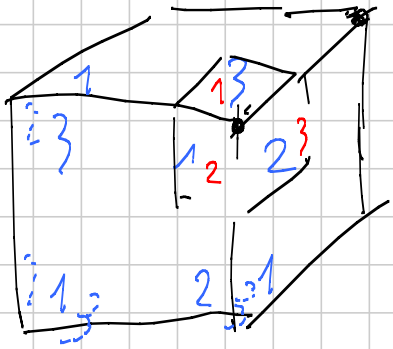
Il segno di una mossa come perm. dei (27) cubetti è +1.

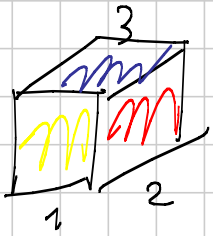
90°

è invariante Serve rispettare questo segno.

Permutazione sulle facce degli spigoli La permutazione è pari (due due cicli due)

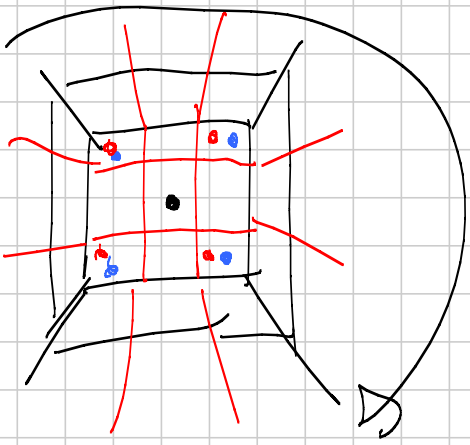






Numero le facce di ogni cubetta di angolo da 1 a 3 in senso antiorario. Numero gli angoli interni ai vertici del cubo "fantasma" da 1 a 3 in senso antiorario

In ogni vertice, ■ − ■ (mod 3) non dipende da quale delle 3 facce uso per il calcolo



NUMERI DI CATALAN

① Ho n parentesi aperte e chiuse e voglio disporle in modo che, a partire da sinistra, non ci siano mai più parentesi chiuse che aperte

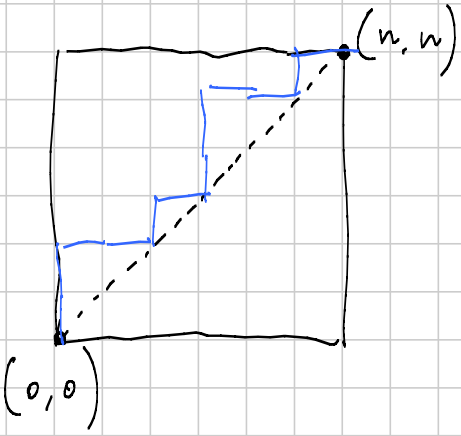
$n=4$ ()()() ok))()(() NO

In quanti modi posso disporre le parentesi?

② Formulazione 2

Quadrato $n \times n$

Andare da $(0,0)$ a (n,n) con $\uparrow$ e $\rightarrow$



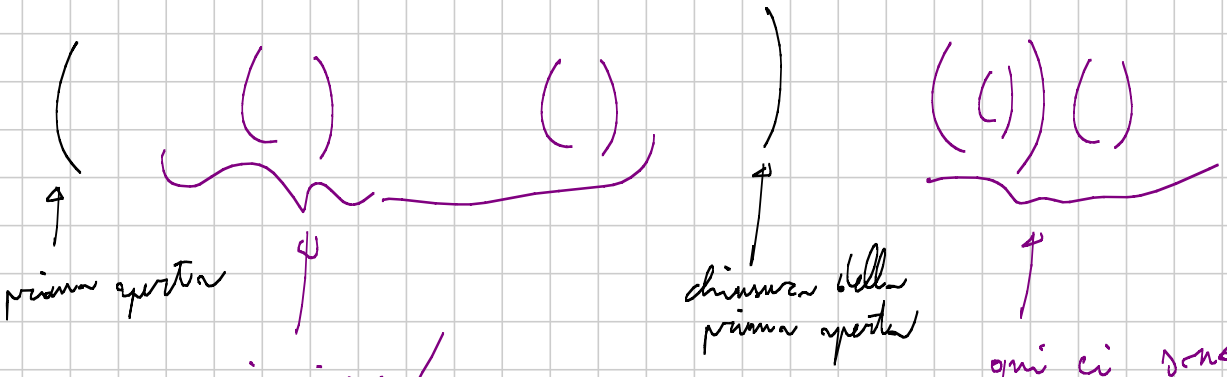
(fino ogni $\binom{2n}{n}$ modi), con l'ulteriore condizione di non scendere mai sotto la diagonale.

Chiamiamo C_n il numero cercato nei problemi (equivalenti) ① e ②.

RICORSIONE

Lavoriamo con le parentesi

La prima parentesi è necessariamente aperta.



qui ci sono i coppie complete di parentesi i cui indici vanno da 0 a $n-1$

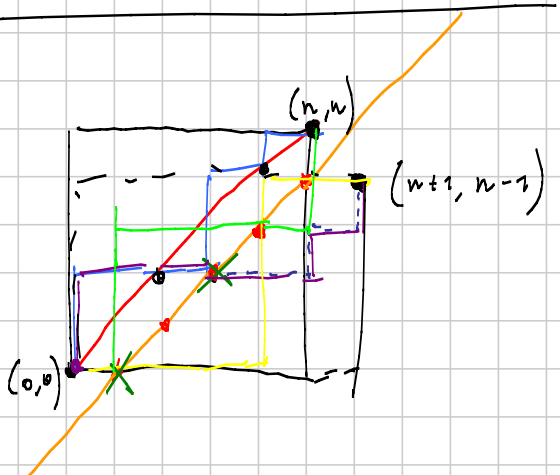
qui ci sono $n-i-1$ coppie di parentesi

Quante possibilità ho con un certo i?

$$C_i \cdot C_{n-i-1}$$

Quante in tutto? $C_n = \sum_{i=0}^{n-1} C_i \cdot C_{n-i-1}$

Altro approccio



In tutto (potendo passare sotto la diagonale) ho $\binom{2n}{n}$ possibilità.

Quante di queste sono "cattive"?

Dato un percorso cattivo, indichiamo il suo primo punto rosso (X), riflettiamo il tratto dopo X rispetto alla retta MN, e arriviamo in $(n+1, n-1)$ in uno dei

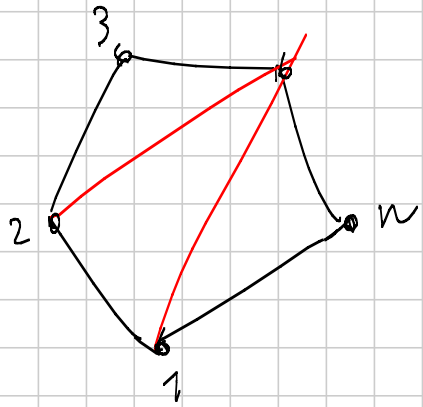
$\binom{2n}{n-1}$ modi possibili con $n+1 \to$ e $n-1 \uparrow$

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

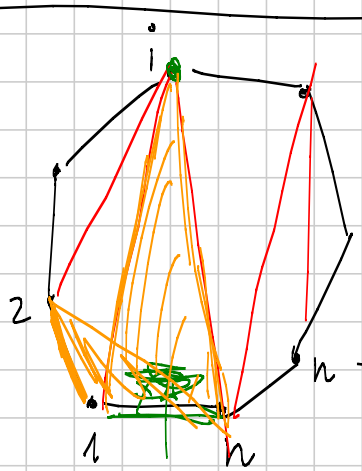
$$\binom{2n}{n} - \frac{(2n)!}{(n-1)!\,(n+1)!} = \binom{2n}{n} - \frac{(2n)!}{n!\cdot n!}\cdot\frac{n}{n+1}$$

TRIANGOLAZIONI

Abbiamo un n-agono convesso $(n \geq 3)$ e vogliamo triangolarlo, cioè tracciare $n-3$ diagonali che non si intersechino internamente tra loro e lo dividano in $n-2$ triangoli. Quanti modi?



Sia T_n la risposta



Data una triangolazione, il triangolo contenente il lato $1-n$ contiene un terzo vertice i, per un certo i tra 2 e $n-1$

Se voglio il triangolo $\overbrace{1 - i - n}$, ho $T_i \cdot T_{n-i+1}$

$T_3 = 1$ $\quad$ $T_2 = 1$ per convenzione

$$T_n = \sum_{i=2}^{n-1} T_i \cdot T_{n-i+1} \qquad i = j+2$$

j va da 0 a $n-3$

$$T_n = \sum_{j=0}^{n-3} T_{j+2} \cdot T_{n-j-1}$$

$T_n = C_{n-2}$ per induzione (controllare valori piccoli + stessa ricorsione).

Stirling (di nuovo sulle permutazioni)

Quante sono le permutazioni su n elementi con esattamente k cicli? La risposta è $\begin{bmatrix} n \\ k \end{bmatrix}$, cioè il n° di Stirling di prima specie di indici n e k.

$\begin{bmatrix} n+1 \\ k \end{bmatrix}$ = qualcosa che coinvolge i valori precedenti

Data una perm. $\sigma \in S_{n+1}$ con k cicli

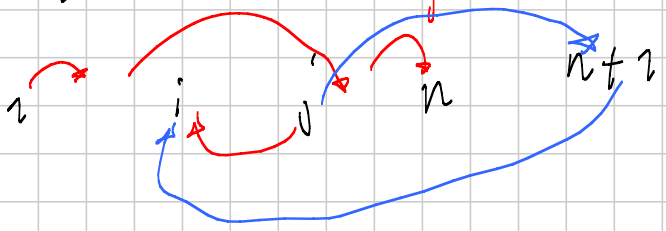
Come è fatto il ciclo di σ che contiene $n+1$?

1° caso $n+1$ è un punto fisso di σ. Allora $(n+1)$ è uno dei k cicli, $\{1, \dots n\}$ si permutano tra loro tramite $k-1$ cicli,

$\begin{bmatrix} n \\ k-1 \end{bmatrix}$ possibilità.

2° caso $\sigma(n+1) = i < n+1 \qquad \sigma^{-1}(n+1) = j < n+1$

Definisco $\tilde{\sigma}$ come σ su tutto $\{1, \dots n\}$ tranne j, e $\sigma(j) = i$. $\tilde{\sigma} \in S_n$. σ ha k cicli (sostanzialmente gli stessi di prima). Viceversa, data un $\tau \in S_n$ con k cicli, posso definire $\tilde{\tau}$ assegnando a $n+1$ un'immagine $\tilde{\tau}(n+1) = i < n+1$ e poi modifico $\tilde{\tau}(\tau^{-1}(i)) = n+1$



$n \cdot \begin{bmatrix} n \\ k \end{bmatrix}$ possibilità

$$\begin{bmatrix} n+1 \\ k \end{bmatrix} = \begin{bmatrix} n \\ k-1 \end{bmatrix} + n \begin{bmatrix} n \\ k \end{bmatrix}$$

Magia $\operatorname{sym}_\ell^h(x_1, \dots x_\ell) = \sum_{1 \le i_1 < \dots < i_h \le \ell} x_{i_1} \cdot \dots \cdot x_{i_h}$

$$\left[{n \atop k} \right] = \operatorname{sym}^{n-k}_{n-1}(1, 2, \dots, n-1)$$

Numeri di Stirling di 2ª specie.

Abbiamo un insieme con n elementi $\{1, \dots n\}$

In quanti modi possiamo partizionarlo in k sottoinsiemi (non vuoti)? In $\left\{ {n \atop k} \right\}$ modi

Prendo $\{1, \dots, n+1\}$. Ci sono 2 casi.

1° caso | $n+1$ sta da solo, gli altri n stanno in $k-1$ insiemi. $\left\{ {n \atop k-1} \right\}$

2° caso | $n+1$ non è solo. Lo tolgo e ottengo una partizione in k parti non vuote di $\{1, \dots n\}$.
Viceversa, se divido $\{1, \dots n\}$ in k parti, e scelgo in quale mettere $n+1$, ottengo una partizione in k parti di $\{1, \dots n+1\}$

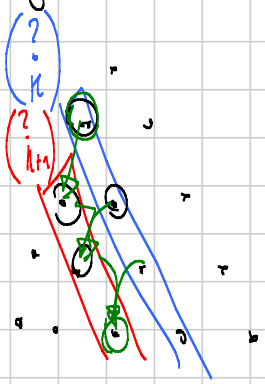
$k \cdot \left\{ {n \atop k} \right\}$

IN TOTALE $\left\{ {n+1 \atop k} \right\} = \left\{ {n \atop k-1} \right\} + k \cdot \left\{ {n \atop k} \right\}$

Curiosità $\sum_{k=1}^{n} \left\{ {n \atop k} \right\} = B_n$ l'n-esimo numero di Bell.

Calcolare "cose del tipo" $\sum_{i=1}^{n} i^k$ " $k \geq 0$, $n \geq 0$

Sarebbe più facile calcolare $\sum_{i=1}^{n} \binom{i}{k} = \binom{n+1}{k+1}$



OSS I binomiali sono polinomi (nel numeratore, fissato il denominatore)

Es $\binom{n}{k} = \dfrac{n(n-1)\cdots(n-k+1)}{k!}$ è un pol. in n di grado k.

Scrivo anche $\binom{x}{k} \in \mathbb{Q}[x]$. Se riesco a scrivere

$$x^k = a_0 \cdot \binom{x}{0} + a_1 \binom{x}{1} + \cdots + a_k \binom{x}{k}$$

Con opportuni numeri $a_0 \dots a_K$,

$$\sum_{x=1}^{n} x^K = \sum_{x=1}^{n} \sum_{h=0}^{K} a_h \binom{x}{h} = \sum_{h=0}^{K} a_h \underbrace{\binom{n+1}{h+1}}$$

è un polinomio di grado $K+1$ in n

$$x^3 = a \cdot x + b \cdot (x+1) + c \cdot 1 + d \cdot (x^3 + x^2)$$

$K = 1$ $\quad x = \binom{x}{1} = 1 \cdot \binom{x}{1} + 0 \cdot \binom{x}{0}$

$K = 3$ $\quad x^3 = 6\binom{x}{3} + 3 \cdot 2! \binom{x}{2} + 3\binom{x}{1}$

$$6\binom{x}{3} = \frac{x(x-1)(x-2)}{3!} = \frac{x^3 - 3x^2 + 2x}{6}$$

$a_K = K!$; $\boxed{K! \cdot \binom{x}{K}} + a_{K-1} \binom{x}{K-1} + a_{K-2} \left(\right.$

è a coeff. interi

contiene $b_{K-1} \cdot x^{K-1}$

deve essere $(K-1)! \cdot b_{K-1}$

è a coeff. interi

contiene $b_{k-2} \cdot X^{k-2}$

Fatto generale Se un polinomio $p(x) \in \mathbb{R}[x]$ di grado k a coeff. reali assume valori interi sugli interi (ma bastano i naturali (anche da un certo punto in poi ($k+1$ consecutivi?))) Allora $\exists\, a_0, \dots a_k$ interi per cui

$$p(x) = a_0 \binom{x}{0} + \dots + a_k \binom{x}{k}$$

(Idea: $q(x) = p(x+1) - p(x)$ ha grado $k-1$, ed ha ancora la proprietà interi $\to$ interi $\dots$)

Per ogni x intero ≥ 0

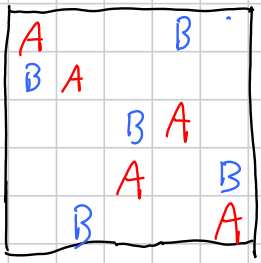
$$p(x) = p(1) + \underbrace{q(1) + \dots + q(x-1)}$$

$$q(x) = b_0 \binom{x}{0} + \dots + b_{k-1} \binom{x}{k-1}$$

Allora $p(x) = p(1) \cdot \binom{x}{0} + b_0 \binom{x}{1} + \dots + b_{k-1} \binom{x}{k}$

Senior 2016 - C2 Medium (Aner)

Note Title 9/6/2016



$n \times n$, vogliamo mettere n lettere A nelle caselle, una per ogni riga e una per colonna

Si può fare! Sulla diagonale

Possiamo aggiungere anche n lettere B con le stesse condizioni, ma in caselle diverse

Si può fare! (Una B sotto ogni A, per esempio)

Possiamo ora aggiungere n lettere C ?

Lemma dei matrimoni Abbiamo un insieme A di ragazzi, e un insieme B di ragazze. $\forall$ ragazzo $x \in A$ ad x piace un sottoinsieme $\Gamma(x) \subseteq B$. Vogliamo organizzare dei matrimoni, assegnando ad ogni ragazzo una moglie tra le ragazze che gli piacciono.

È possibile? Non sempre. Per $X \subseteq A$ chiamiamo

$$\Gamma(X) = \{\text{ragazze che piacciono ad almeno un ragazzo in } X\} = \bigcup_{x \in X} \Gamma(x)$$

Se esiste $X \subseteq A$ con $|X| > |\Gamma(X)|$, non si può

Tesi del lemma Se $\forall X \subseteq A \quad |X| \leq |\Gamma(X)|$ allora si può fare

DIM. Per induzione estesa su $n = |A|$

PASSO BASE $n=0$ tutto va bene

facciamo anche $n=1$ tutto va bene

PASSO INDUTTIVO Ci sono due possibilità:

(1) $\forall X \subseteq A$ con $X \neq \emptyset$, $X \neq A$, vale $|X| < |\Gamma(X)|$

(2) $\exists X \subseteq A$ con $X \neq \emptyset$, $X \neq A$, per cui $|X| = |\Gamma(X)|$

Nel caso (1) possiamo scegliere un ragazzo $\bar{x} \in A$ e gli assegniamo una moglie $\bar{y} \in B$ (in qualche modo).

Rimangono i ragazzi in $A \setminus \{\bar{x}\}$ e le ragazze in $B \setminus \{\bar{y}\}$. Verifichiamo le ip. del lemma per gli insiemi $A \setminus \{\bar{x}\}$, $B \setminus \{\bar{y}\}$

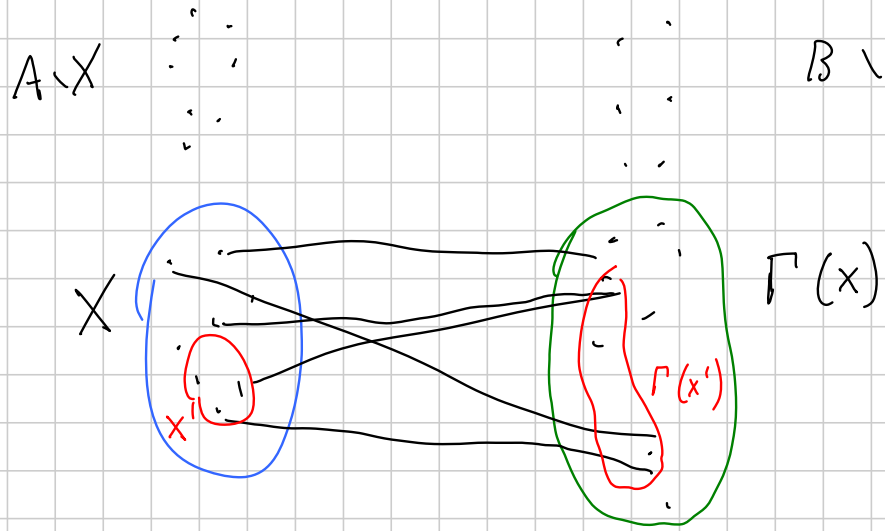
$X \subseteq A \setminus \{\bar{x}\}$, $|\Gamma(X) \setminus \{\bar{y}\}| \overset{?}{\geq} |X|$

$X = \emptyset$ è ovvio; $|X| > 0$ comunque $X \neq A \Rightarrow |X| \leq |\Gamma(X)| - 1$

$|\Gamma(X) \setminus \{\bar{y}\}|$

(2) Prendo $X \neq \emptyset, A$ $|X| = |\Gamma(X)|$

A



Vorrei spezzare il problema in 2 problemi più piccoli, con le coppie $(X, \Gamma(X))$ e $(A \setminus X, B \setminus \Gamma(X))$

Devo verificare:

- $\forall\, X' \subseteq X \quad |\Gamma(X')| \geq |X'|$ parte dell'ipotesi originale ✓
  se già che è incluso in $\Gamma(X)$

- $\forall\, X'' \subseteq A \setminus X \quad |\Gamma(X'') \setminus \Gamma(X)| \geq |X''|$

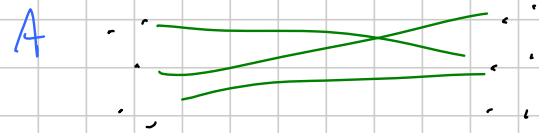
Considero l'insieme $X \cup X''$

$$|X| + |X''| = |X \cup X''| \leq |\Gamma(X'' \cup X)| = |\Gamma(X)| + |\Gamma(X'') \setminus \Gamma(X)|$$

✓

OSS Sembra un lemma difficilmente applicabile (l'ipotesi è difficile da verificare ...)

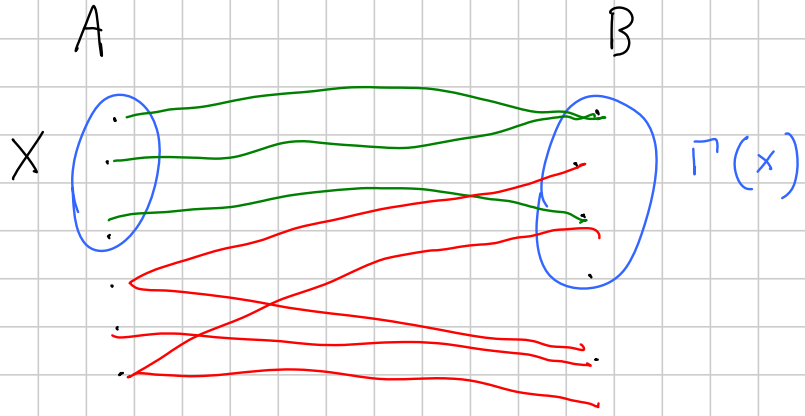
Def Un grafo si dice bipartito se i suoi vertici si possono dividere in due sottoinsiemi A e B disgiunti per cui tutti gli archi vanno da A a B



Lemma ausiliario dei matrimoni A ragazzi, B ragazze

Supponiamo che $\forall x \in A$ e $y \in B$ che si conoscono, $\deg x \geq \deg y$. Allora le ip. del lemma dei matrimoni sono verificate. (gradi dei ragazzi >0, wlog gradi delle ragazze >0)

Dim Assegniamo un peso 1 a ogni ragazza e a ogni ragazza (in cioccolato). Ogni ragazzo distribuisce equamente il suo cioccolato alle sue vicine; ogni ragazza fa lo stesso (divide il suo cioccolato tra i ragazzi a cui piace)



Sia $p(x)$ il cioccolato ricevuto da un ragazzo, $p(y)$ quello

ricevuto da una ragazza.

cioccolato ricevuto da X

$$\sum_{x \in X} p(x) \leq |\Gamma(X)|$$

$$\sum_{y \in \Gamma(X)} p(y) \geq |X|$$ vera, ma non servirà

$$\sum_{x \in X} p(x) = \sum_{\substack{x \in X \\ y \in \Gamma(x) \\ xy \text{ si conoscono}}} \frac{1}{\deg y} = \sum_{x \in X} \overbrace{\sum_{\substack{y \in \Gamma(x) \\ xy \text{ si conoscono}}} \frac{1}{\deg(y)}}^{p(x)}$$

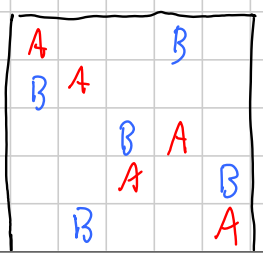
$\forall$ vale per ipotesi $\deg x \geq \deg y$ se x e y si conoscono

$$\sum_{y \in \Gamma(x)} p(y) \geq \sum_{\substack{y \in \Gamma(x) \\ x \in X \\ xy \text{ si conoscono}}} \frac{1}{\deg x} = |X|$$

vera ma non servirà

Corollario Se per ogni $x \in A$ e per ogni $y \in B$ $\deg(x) \geq \deg(y)$, a maggior ragione posso organizzare i matrimoni.

Torniamo alle scacchiere

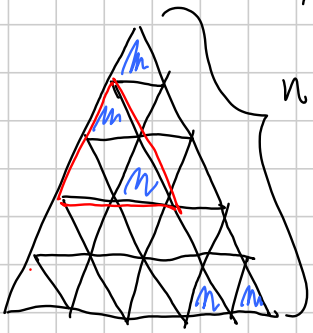


Oggiungere le C vuol dire far sposare ogni riga con una colonna. Usando il lemma ausiliario e il corollario, basta verificare $\deg(\text{riga}) \geq \deg(\text{colonna})$ $\forall$ riga e colonna

dove $\deg(\text{riga } r) = \#$ caselle libere su r

$\deg(\text{colonna } c) = \;//\;//\;/\;c$

IMO SL 2006/C6



Rimuovete n triangolini con la punta in alto; rimane una figura che volete tassellare con dei rombi 

Tesi: ciò è possibile se e solo se in ogni sottotriangolo con la punta in alto di lato k $(1 \le k \le n)$ ci sono al massimo k triangolini rimossi.

Verso il teorema di König: Supponiamo di avere

A ragazzi, B ragazze, alcuni si conoscono.

Per $X \subseteq A$, definisco $\delta(X) = |X| - |\Gamma(X)|$

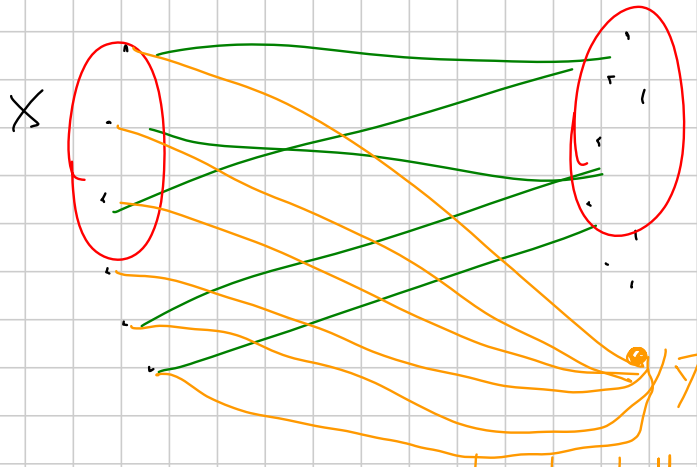
Il lemma dei matrimoni dice che se $\delta(X) \le 0$ sempre, allora posso effettuare tutti i matrimoni.

Cerchiamo di generalizzare: Supponiamo $\delta(X) \le 1$ sempre.

Cosa possiamo dire? Riusciremo a combinare tutti i matrimoni, tranne al max uno.

DIM

A B



ipotesi: per ogni $X \subseteq A$
$|\Gamma(X)| \geq |X| - 1$

Oraggiungiamo una ragazza conosciuta da tutti A

Chiamo $\tilde{B} = B \cup \{\bar{y}\}$. La coppia $(A, \tilde{B})$ soddisfa l'ipotesi del lemma dei matrimoni !!!

Ora posso creare tutti i matrimoni, ma alla fine, eventualmente, devo eliminare al massimo un matrimonio, quello di $\bar{y}$.

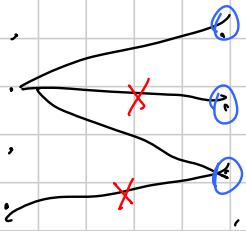
Generalizziamo $\quad \delta = \max\{\delta(X) \mid X \subseteq A\}$

allora posso creare tutti i matrimoni, salvo al più δ.

Def Un matching o accoppiamento in un grafo bipartito è un sottoinsieme M degli archi per cui due archi in M non hanno estremi in comune

Def Un covering o ricoprimento è un sottoinsieme C dei vertici (di tutti i vertici), per cui ogni arco ha almeno un estremo in C

OSS M matching, C covering $\quad |M| \leq |C|$

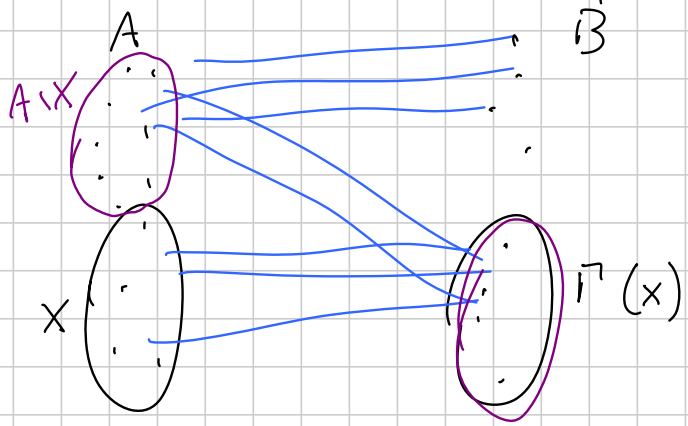


Teorema di König Esistono un accoppiamento e un ricoprimento con la stessa cardinalità.

DIM Sia $\alpha = |A|$. Sia $\delta = \max\{\delta(X) \mid X \subseteq A\}$.

- Se $\delta \leq 0$ allora sono nell'ip. del lemma dei matrimoni classico, per cui c'è un α-matching. È chiaro anche che A è un α-covering
- $\delta > 0$. Esiste un $(\alpha - \delta)$-matching.

  Sia $X \subseteq A$ tale che $\delta = |X| - |\Gamma(X)|$



Cerco un $(\alpha - \delta)$-covering

$\alpha - \delta =$

$= \alpha - |X| + |\Gamma(X)|$

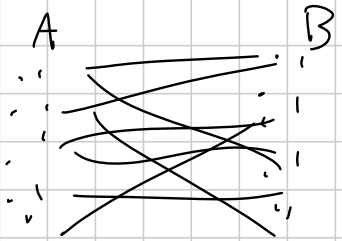
Provo $(A \setminus X) \cup \Gamma(X)$. È un covering? Sì

Problema di Turán G grafo generico, con n vertici, e archi, senza triangoli (cicli lunghi 3).

- Albero $e = n-1$ (il totale delle coppie di vertici è $\frac{n(n-1)}{2}$)
- vertice centrale + tanti cicli da 4

$$4\left\lfloor \frac{n-1}{3} \right\rfloor \sim \frac{4}{3}n$$ un po' meglio ...

- grafo bipartito completo (i cicli hanno tutti lunghezza pari)



$e = |A| \cdot |B|$ con $|A| + |B| = n$

$e = \frac{n^2}{4}$ per n pari $\quad e = \frac{(n+1)}{2} \cdot \frac{(n-1)}{2} = \frac{n^2-1}{4} = \left\lfloor \frac{n^2}{4} \right\rfloor$

questa stima è di secondo grado

Teo (Turán) Non si può fare di meglio

DIM Parto con un peso 1 su ogni vertice. Cerco di spostare i pesi e massimizzare $\sum_{\substack{v_i \text{ e } v_j \text{ sono collegati} \\ i<j}} x_i \cdot x_j = X$

$V_1, \dots, V_n$ sono i vertici di un grafo senza triangoli

x_i è il peso assegnato a V_i

All'inizio $x_i = 1$ per ogni i, quindi $X = e$

Ad ogni passaggio

1) Prendo due vertici x_i e x_j non collegati e tali che

$x_i > 0$, $x_j > 0$ (se ci sono)

2) $X = \sum_{\substack{V_k, V_h \text{ collegati} \\ k,h \neq i,j}} x_k \cdot x_h + x_i \cdot \sum_{V_e, V_i \text{ collegati}} x_e + x_j \cdot \sum_{V_m, V_j \text{ collegati}} x_m$

Cerco di modificare i valori $x_i \rightsquigarrow 0$ $\quad x_j \rightsquigarrow x_j + x_i$

oppure $x_j \rightsquigarrow 0$ $\quad x_i \rightsquigarrow x_i + x_j$

Vorremo che X aumenti (debolmente)

Scelgo opportunamente quale modifica fare

3) X aumenta o rimane invariato. Il numero di vertici con peso nullo aumenta di 1 $\Rightarrow$ prima o poi l'algoritmo finisce

---

Cosa vediamo alla fine dell'algoritmo? Alla fine tutti i vertici con peso > 0 sono collegati in tutti i modi possibili tra loro. Il nostro grafo non ha $\Delta \Rightarrow$ ci sono al massimo due vertici con peso positivo OSS: X prima si annulla

mai, quindi ha esattamente due vertici V_a, V_b per cui $X_a > 0$ $X_b > 0$ V_a e V_b sono collegati

$X = X_a \cdot X_b$ alla fine; inoltre $X_a + X_b = n$

$X \le \frac{n^2}{4}$ per AM-GM $\Rightarrow e \le \frac{n^2}{4}$ $\overset{\text{è intero}}{\Rightarrow}$ $e \le \left\lfloor \frac{n^2}{4} \right\rfloor$

(all'inizio $X = e$)

ORDINI PARZIALI Nella vita, capita di trovarsi di fronte a un insieme S, e di avere una regola infallibile per confrontare due el. di S, s e t, e dire quale dei due è "maggiore" e quale è "minore" in un opportuno senso. (esempio: un sottoinsieme di $\mathbb{R}$)

A volte invece capita un S sprovvisto di questa proprietà (es. un sottoinsieme di $\mathbb{C}$, un insieme di colori, un sottoinsieme di punti in $\mathbb{R}^3$ ...)

A volte ci sono situazioni intermedie, cioè in S alcune coppie s, t sono confrontabili, altre no.
(esempio: $\mathbb{N} = S$, $n \prec m$ se $n \mid m$)

Comunque deve valere la proprietà transitiva:

se $s \preceq t$ e $t \preceq u$ $\quad s \preceq u$

Altro non-esempio $S = \mathbb{R}^2 = \{(x,y) \mid x,y \in \mathbb{R}\}$

$(x_1,y_1) \prec (x_2,y_2)$ se $x_1 < x_2$, oppure $x_1 = x_2$ e $y_1 < y_2$

questo è un ordine totale

Altro esempio $S = \mathbb{R}^2$ $(x_1,y_1) \prec (x_2,y_2)$ se

$x_1 < x_2$ e $y_1 < y_2$

Tricotomia (volendo) ha una funzione da $S^2 \to \{\prec, \succ, \text{boh}\}$

che dice $\forall (s,t)$ se $s \prec t$, $s \succ t$ oppure non si sa

Ci noi interessano gli ordini parziali finiti

Def Una catena $C \subseteq S$ è un sottoinsieme totalmente ordinato: ogni coppia di el. di C sono confrontabili

Def Una anticatena $A \subseteq S$ è un sottoinsieme totalmente disordinato: due el. di A sono sempre inconfrontabili.

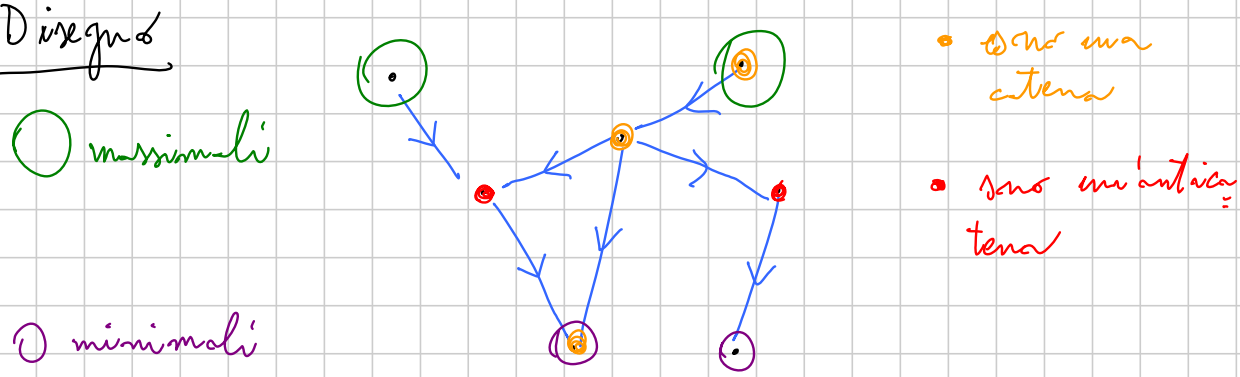
Def $m \in S$ si dice "minimale" se $\forall s \in S$, $s \neq m$

vale $m \not\succ s$, oppure m e S non sono confrontabili

Def $M \in S$ // "massimale" se //

// $M \not\prec S$, // // // // // //

Disegno



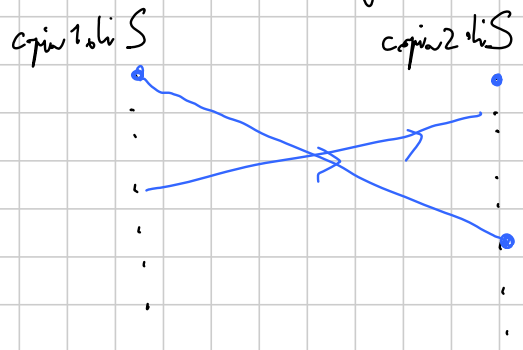
Lemma L'insieme dei minimali è un'anticatena.
Idem per i massimali.

Teorema (Dilworth) Sia S un ordine parziale finito.

① Sia K la massima cardin. di una catena in S; allora S si può scrivere come unione di K anticatene (disgiunte)

② Sia h la massima |anticatena|; allora S è unione di h catene (disgiunte).

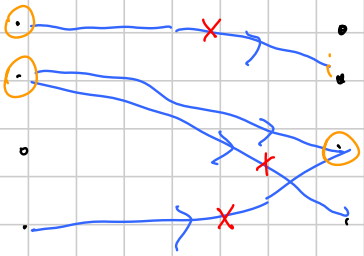
DIM ② Applichiamo König su questo grafo bipartito



Vertici = due copie di S
archi: collego s a sinistra con t a destra se $s > t$

In particolare non collego s a s

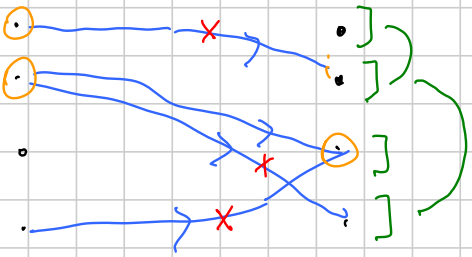
Applico König: ottengo un matching e un covering della stessa cardinalità c.

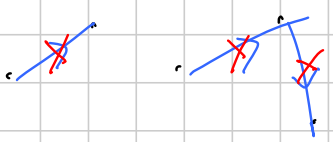


$\exists$ almeno $|S| - c$ elementi di S che non sono identici al covering né nella loro copia a sx, né in quella a dx!

Questi elementi formano un'anticatena: infatti se s, t sono fra questi e $s > t$, allora nel grafo ho un arco non coperto dal covering

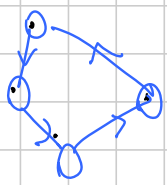
Come divido ora S in $|S| - c$ catene?





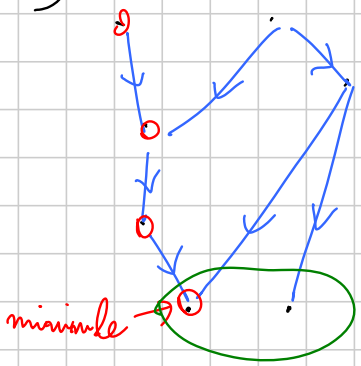
e frecce: scompongo S in "serpenti" e cicli

(ma i cicli in realtà non capitano)



Ho $|S| - c$ catene

① S



K è la massima lunghezza di una catena

OSS Una catena di lunghezza massima finisce con un minimale

Idea La prima anticatena della partizione in anticatene saranno i minimali $A_m = \{\text{minimali}\}$

- ho anche a disposizione $K-1$ anticatene per partizionare $S \setminus A_m$
- la max lunghezza di una catena in $S \setminus A_m$ è $K-1$ $\Rightarrow$ induzione

---

$m, n > 0$; abbiamo un insieme di $mn+1$ persone, tutte di età diversa e tutte di altezza diversa. Allora almeno una delle seguenti vale:

- esistono $m+1$ persone che, in ordine di età crescente, sono anche in ordine di altezza crescente
- esistono $n+1$ persone // // // sono in ordine decrescente di altezza

(poi c'è l'altra enunciata, scambiando m e n)

Definisco un ordine parziale tra le persone:

$p_1 < p_2$ se p_1 è meno anziana e meno alta di p_2

Stiamo chiedendo che esista una catena lunga $m+1$, oppure una anticatena lunga $n+1$.

Supponiamo che ogni catena sia lunga al massimo m; allora Dilworth (1) mi dice che le persone si possono raggruppare in $\leq m$ anticatene. Per pigeonhole una di queste anticatene ha almeno $n+1$ persone.

G1 Medium

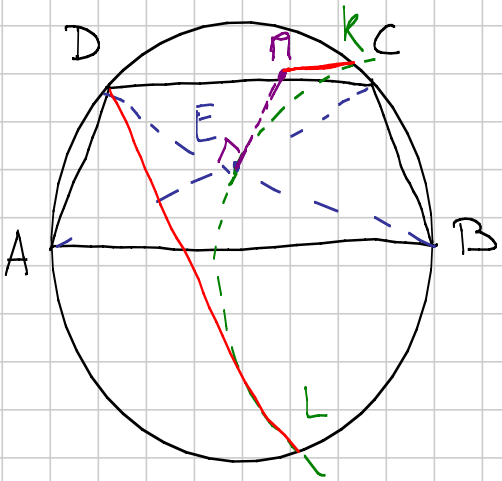
Sam

Note Title 9/2/2016

Complessi, vettori, coordinate

Es: ABCD trapezio inscritto in Γ con AB diametro
La cfr di centro B e raggio BE ($E = AC \cap BD$) incontra Γ in K e L, con K dalla stessa parte di C rispetto ad AB.
Il punto CD è t.c. $E\Pi \perp BD$. Allora $K\Pi \perp DL$. ?

[BMO 2014-3]



Per dopo

Ripasso misto su $\mathbb{C}$

Es: ABC tri; P punto generico. I simmetrici di P rispetto ai lati sono allineati se e solo se $P \in \Gamma_{ABC}$.

dim: Scriviamo P_c numero di P rispetto ad AB

$$P \longrightarrow p-a \longrightarrow \frac{p-a}{b-a} \longrightarrow \frac{\overline{p}-\overline{a}}{\overline{b}-\overline{a}} \longrightarrow \left(\frac{\overline{p}-\overline{a}}{\overline{b}-\overline{a}}\right)(b-a)+a$$

origine in A; porto B in 1; simmetria rispetto ad AB = conj $\mathbb{R}$-lin; rimetto le cose a posto

Suppongo che Γ_{ABC} sia la cfr. unitaria $(z\bar{z}=1)$

$\forall z \in \Gamma_{ABC} \quad \bar{z} = \frac{1}{z}$

$$p_c = \left(\frac{\bar{p} - \frac{1}{a}}{\frac{1}{b} - \frac{1}{a}}\right)(b-a) + a = \left(\frac{a\bar{p} - 1}{a - b}\, b\right)(b-a) + a =$$

$$= \boxed{a + b - ab\bar{p}}$$

$p_b = a + c - ac\bar{p} \qquad p_a = b + c - bc\bar{p}$

$$\frac{p_a - p_b}{p_c - p_b} = \frac{b + c - bc\bar{p} - a - c + ac\bar{p}}{a + b - ab\bar{p} - a - c + ac\bar{p}} =$$

$$= \frac{(b-a)(1 - c\bar{p})}{(b-c)(1 - a\bar{p})}$$

r, s, t allineati se

$\not\sphericalangle rst \equiv 0 \ (\pi)$ sse

$\arg\left(\frac{t-s}{r-s}\right) \equiv 0 \ (\pi)$ sse

$\frac{t-s}{r-s} \in \mathbb{R}$

voglio che sta in $\mathbb{R} = \{ z \in \mathbb{C} : z = \bar{z} \}$

$\Rightarrow$ Faccio il coniugato $\quad \frac{\bar{b} - \bar{a}}{\bar{b} - \bar{c}} \, \frac{1 - \bar{c}p}{1 - \bar{a}p} =$

$$= \frac{\frac{1}{b} - \frac{1}{a}}{\frac{1}{b} - \frac{1}{c}} \cdot \frac{1 - \frac{p}{c}}{1 - \frac{p}{a}} = \frac{a-b}{c-b} \cdot \frac{c-p}{a-p} \cdot \frac{a}{a} =$$

$$= \boxed{\frac{a-b}{c-b}} \cdot \frac{c-p}{a-p}$$

$p_a\, p_b\, p_c$ allineati sse $\quad \frac{1 - c\bar{p}}{1 - a\bar{p}} = \frac{c-p}{a-p} \iff$

$\iff a - p - ac\bar{p} + cp\bar{p} = c - p - ca\bar{p} + ap\bar{p}$

$\iff a - c = (a-c)p\bar{p} \iff p\bar{p} = 1 \iff p \in \Gamma_{ABC}$.□

Oss: H sta sulla retta per P_a, P_b, P_c. ($\text{se } P \in T_{ABC}$)

Dim: $h = a+b+c$

$$h - p_a = a+b+c - b - c + bc\bar{p} = a + bc\bar{p} = \frac{ap+bc}{p}$$

$$z = re^{i\theta} \qquad \frac{z}{\bar{z}} = \frac{re^{i\theta}}{re^{-i\theta}} = e^{i2\theta}$$

$$\frac{h-p_a}{\bar{h}-\bar{p}_a} = \frac{\frac{ap+bc}{p}}{\frac{ap+bc}{abcp}\,p} = \frac{abc}{p} \Rightarrow H \text{ sta sulla retta}$$

Cor: Le proiez di P sui lati sono allineate (retta di Simson) e tale retta passa per il pt. medio di PH.

Oss: Proiez di P su AB $\boxed{\frac{1}{2}(p+a+b-ab\bar{p})}$ per ogni P!! Non solo su T_{ABC}

Oss 2: Il pt. medio di PH, $P \in T_{ABC}$, sta sulla cfr. dei 9 punti.

dim: [omotetia, oppure] $l = \frac{a+b}{2}$, $m = \frac{b+c}{2}$, $n = \frac{a+c}{2}$

l, m, n, q sono concicliche sse

$$\sphericalangle lmn + \sphericalangle nql \equiv 0 \quad (\pi) \text{ sse}$$

$$q = \frac{1}{2}(a+b+c+p)$$

$$\arg\left(\frac{n-m}{l-m} \cdot \frac{l-q}{n-q}\right) \equiv 0 \quad (\pi) \text{ sse}$$

$$\frac{n-m}{l-m} \cdot \frac{l-q}{n-q} \in \mathbb{R} \qquad \frac{\frac{a-b}{2}}{\frac{a-c}{2}} \cdot \frac{-\frac{c-p}{2}}{-\frac{b-p}{2}} = \frac{a-b}{a-c} \cdot \frac{c+p}{b+p} = \sigma$$

$$\bar{\sigma} = \frac{\frac{1}{a}-\frac{1}{b}}{\frac{1}{a}-\frac{1}{c}} \cdot \frac{\frac{1}{c}+\frac{1}{p}}{\frac{1}{b}+\frac{1}{p}} = \frac{(b-a)(c+p)}{(c-a)(b+p)} \frac{1}{abcp} = \frac{a-b}{a-c}\,\frac{c+p}{b+p} = \sigma$$

$\Rightarrow$ OK.

Oss 3: P, P' sono diam. opposti in $\Gamma_{ABC} \Rightarrow$ le rette di Simson sono perpendicolari.

Dim: $p' = -p$ Considero le rette per i simm. di P e P'.

$p_a = b + c - bc\bar{p}$ $\quad p_a' = b + c + bc\bar{p}$ "simm di P' risp. a BC

$\sphericalangle r s \equiv \frac{\pi}{2} \ (\pi)$ se $\arg\left(\frac{t-s}{r-s}\right) \equiv \frac{\pi}{2} \ (\pi)$ se $\frac{t-s}{r-s} \in i\mathbb{R} = \{z \in \mathbb{C} : z = -\bar{z}\}$

$$\frac{h - p_a}{h - p_a'} = \frac{a + bc\bar{p}}{a - bc\bar{p}} = \tau$$

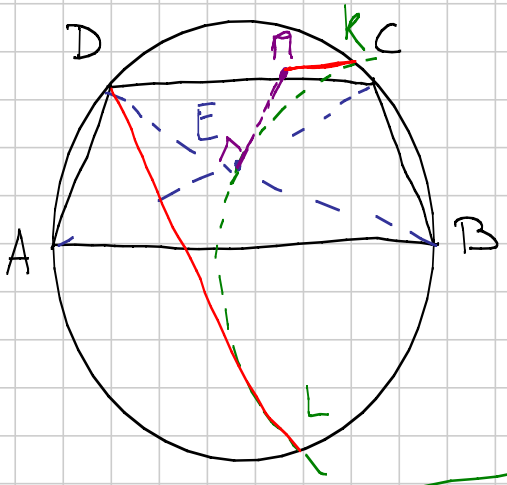
$$\overline{\tau} = \frac{\frac{1}{a} + \frac{p}{bc}}{\frac{1}{a} - \frac{p}{bc}} = \frac{bc + ap}{bc - ap} = \frac{bc\bar{p} + a}{bc\bar{p} - a} = -\tau$$

$\Rightarrow \tau \in i\mathbb{R}$

$\Rightarrow$ le rette sono perpendicolari. $\square$

Es: $ABCD$ trapezio inscritto in Γ con AB diametro
La cfr di centro B e raggio BE ($CE = AC \cap BD$) incontra Γ
in K e L, con K dalla stessa parte di C rispetto ad AB.
Π su CD t.c. $E\Pi \perp BD$. Allora $K\Pi \perp DL$. ?

[BMO 2014-3]



Strategia 1

Γ cfr. unitaria ✓
$B = 1$ $A = -1$ ✓
$D \to -\bar{c}$ ✓
$E = ix$ ✓ $x \in \mathbb{R}$ facile da calcolare
$K = \bar{e}$ ✓

1° problema: K dipende da $\sqrt{1+x^2}$ tramite funz. goniometriche inverse. ~ ✓

$\Pi = pt\ su\ CD \ (\Leftrightarrow) \ m = c + t(d-c) \quad t \in \mathbb{R}$
t.c. proiettato su DB fa E $\quad ix = \frac{1}{2}\left(-\bar{c}+1 + \bar{c}\bar{m} + m\right)$ ✓
lineare in t

$\frac{k-m}{d-\ell} \in i\mathbb{R}$ ✓
↑
Hope

Oss sintetiche sparse:
DB bisett. di $L\hat{D}K$
$\Rightarrow$ E incentro di $\triangle DKL$

Teo: Dati $a, b, c \in \Gamma = \{z\bar{z} = 1\}$ posso trovare tre numeri cplx u, v, w t.c. $a = u^2$, $b = v^2$, $c = w^2$ e quindi il punto medio degli archi

$\widehat{AB}, \widehat{BC}, \widehat{CA}$ sono $-uv, -vw, -uw$.

Da cui l'incentro è $-uv - vw - uw$.

Fisso Γ ch. un'iperbole ✓ — Strategia n. 2

Pongo $d = u^2$, $k = v^2$, $l = w^2$ ✓

$\Rightarrow$ B è dato da $-vw$ $\Rightarrow$ A è vw ✓

C è t.c. $DC \parallel AB$ e $C \in \Gamma$ $\qquad x$

$\frac{u^2 - x}{2vw} \in \mathbb{R} \iff \frac{u^2 - x}{2vw} = \frac{\frac{x - u^2}{xu^2}}{\frac{2}{vw}}$

$\Leftarrow$ $x = -\frac{v^2 w^2}{u^2}$ è C. ✓

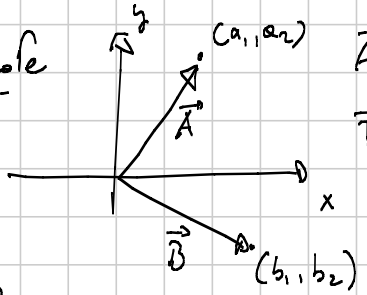
$E = -uv - vw - uw$. ✓ Π si trova come prima

Facendo i conti $\Pi = u^2 + v^2 + w^2$ e l'orocentro di DKL $\Rightarrow$ fine.

Vettori e coordinate

Prodotto scalare: $\vec{A}\cdot\vec{B} = \|\vec{A}\|\cdot\|\vec{B}\|\cdot\cos\widehat{AB}$

in 2 coordinate



$\vec{A} = (a_1, a_2)$

$\vec{B} = (b_1, b_2)$

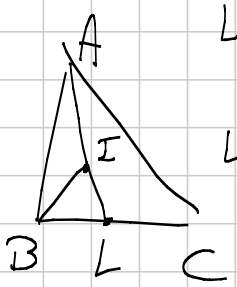
$\vec{A}\cdot\vec{B} = a_1b_1 + a_2b_2$

$\vec{e}_1, \vec{e}_2$ $\quad \vec{A} = a_1\vec{e}_1 + a_2\vec{e}_2$ ...

calcolarlo con Carnot $\quad \vec{i}, \vec{j}$

Vale in n coordinate: $\vec{A}\cdot\vec{B} = \sum_{j=1}^{n} a_j b_j$

Espressione vettoriale dell'incentro: $\vec{I} = \dfrac{a\vec{A} + b\vec{B} + c\vec{C}}{a+b+c}$



$\dfrac{BL}{LC} = \dfrac{AB}{AC}$

$\Downarrow$

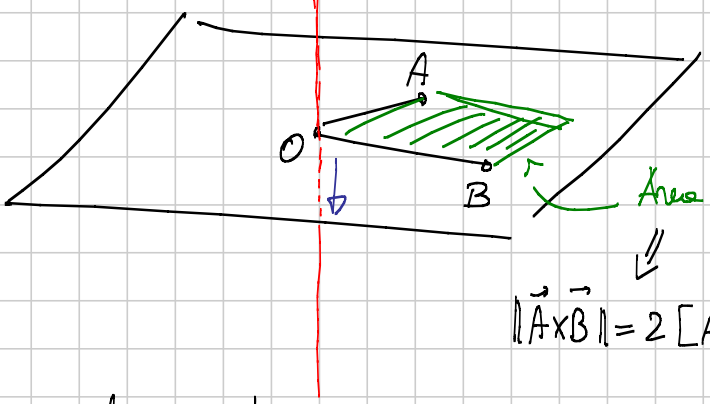
$L = \dfrac{c\vec{C} + \vec{B}}{b+c}$

Prodotto vettore (in 3 dimensioni)

$\vec{A}, \vec{B} \rightsquigarrow \vec{A}\times\vec{B}$

$\|A\times B\| = \|A\|\cdot\|B\|\cdot|\sin A\hat{O}B|$

direz. = $\perp$ al piano per A, O, B



verso = regola mano dx

Area $= \|A\|\cdot\|B\|\cdot|\sin A\hat{O}B|$

$\Downarrow$

$\|\vec{A}\times\vec{B}\| = 2\,[\hat{AOB}]$

$\vec{A}\times\vec{B}$

$\|$

$-\vec{B}\times\vec{A}$

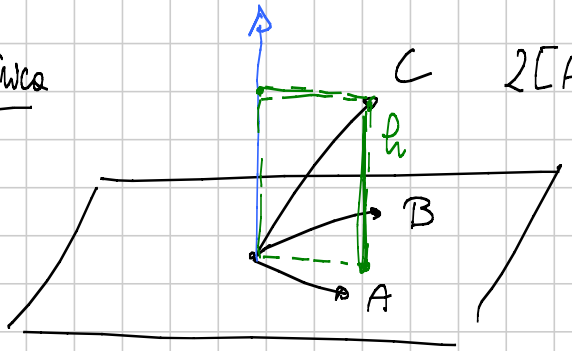
En per gli amanti

$A = (a_1, a_2, a_3)$ $\quad B = (b_1, b_2, b_3)$

$\vec{A}\times\vec{B} = (a_2b_3 - a_3b_2,\ b_1a_3 - a_1b_3,\ a_1b_2 - a_2b_1)$

Ed totality: $(\vec{A}\times\vec{B})\cdot\vec{C} = \det(A|B|C)$.

Idea geometrica



$2[A\hat{O}B]\cdot h = 6\,\mathrm{Vol}(OABC)$

$$\det(A|B|C) = c_1a_2b_3 - c_1a_3b_2 + c_2b_1a_3 - c_2a_1b_3 + c_3a_1b_2 - c_3a_2b_1$$

$$\det\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} = a_1b_2c_3 + b_1c_2a_3 + c_1a_2b_3 - c_1b_2a_3 - c_2b_3a_1 - b_1a_2c_3$$

(diagonali discendenti: alto sx → basso dx; diagonali ascendenti: alto dx → basso sx)

Regola di SARRUS.

$$\det\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} = a_1b_2 - a_2b_1$$

$\{a_{ij}\}_{i,j=1}^{n}$

$$\det(a_{ij}) = \sum_{\sigma\in S_n} (-1)^{|\sigma|}\cdot\prod_{j=1}^{n} a_{j\sigma(j)}$$

Se $\det(A|B|C) = 0$

$\Rightarrow$ almeno una delle seguenti è vera

$A = \beta B + \gamma C$

$B = \alpha A + \gamma C$

$C = \alpha A + \beta B$

$\det(2A|B|C) = ?$

$\det(A|C|B) = ?$

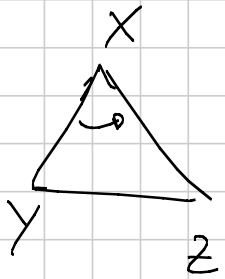
$\det(A+A'|B|C) = ?$

Teo: ABC triangolo, P punto. Allora $\exists!\ \alpha,\beta,\gamma \in \mathbb{R}$ t.c.

1) $\alpha+\beta+\gamma = 1$
2) $\alpha\vec{A}+\beta\vec{B}+\gamma\vec{C} = \vec{P}$

$[XYZ] > 0$ se XYZ sono in senso antiorario.

<u>Dim</u>: $\alpha = \dfrac{[PBC]}{[ABC]}$, $\beta = \dfrac{[PAC]}{[BAC]}$, $\gamma = \dfrac{[PAB]}{[CAB]}$



Se $P = \alpha A+\beta B+\gamma C$ $\quad [PBC] =$

$= (C-B)\times(P-B) = k\cdot[ABC]$
$\qquad\qquad\qquad\quad \| \qquad\qquad \|$
$\qquad\qquad\qquad (B-A)\times(C-A)$

$(\vec{Y}-\vec{X})\times(\vec{Z}-\vec{X})$

--- □

<u>Oss</u>: $P = \alpha A+\beta B+\gamma C$

$Q = \rho A+\sigma B+\tau C$

pt. med tra P e Q
$\|$
$\dfrac{P+Q}{2} = \left(\dfrac{\alpha+\rho}{2}\right)A + \left(\dfrac{\beta+\sigma}{2}\right)B + \left(\dfrac{\gamma+\tau}{2}\right)C$

<u>Oss 2</u>: Posso rimuovere alla condizione i), sostituendola con $\alpha+\beta+\gamma \neq 0$

e $P = \dfrac{\alpha A+\beta B+\gamma C}{\alpha+\beta+\gamma}$

<u>Coord baricentriche rispetto ad ABC</u> (A)

$P = [p:q:r]$ sse $\vec{P} = \dfrac{p\vec{A}+q\vec{B}+r\vec{C}}{p+q+r}$

se $p+q+r = 1$ si dicono <u>normalizzate</u>

Oss: $p = k\cdot[PBC]$ $q = k\cdot[APC]$ $r = k\cdot[ABP]$ $k \in \mathbb{R}\setminus\{0\}$

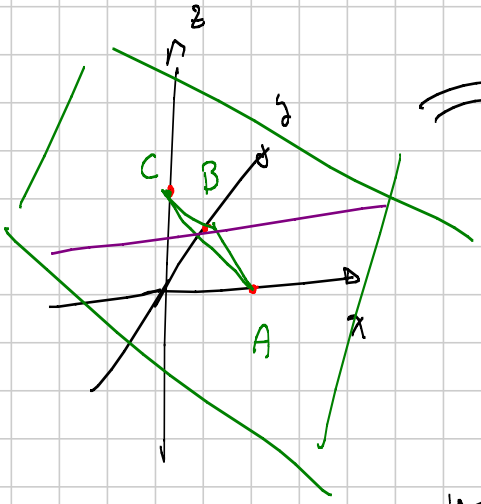
Es: $\{[x:y:z] \text{ t.c. } lx+my+nz=0\}$ $l,m,n \in \mathbb{R}$ non tutti nulli.

è una retta. $x=0$, $y=0$, $z=0$ lato di ΔABC

Es: $A=[1:0:0]$ $B=[0:1:0]$ $C=[0:0:1]$

R = pt. medio di AB $= \left[\frac{1}{2}:\frac{1}{2}:0\right] = [1:1:0]$

Idea 3-dim:



$\Rightarrow$ P, Q, R sono allineati

$\| \quad \| \quad \|$

$p_i \quad q_i \quad r_i$

se i corrisp. vett. 3-dim sono complanari

se $\det(PQR)=0$

$\det\begin{pmatrix} p_1 & q_1 & r_1 \\ p_2 & q_2 & r_2 \\ p_3 & q_3 & r_3 \end{pmatrix} = 0.$

Condiz di allineamento in coord. baricentriche

Es: **Mediana:** $M=[1:1:0]$
$C=[0:0:1]$

$\det\begin{pmatrix} 1 & 0 & x \\ 1 & 0 & y \\ 0 & 1 & z \end{pmatrix} = 0 \iff \boxed{x-y=0}$

Rette parallele: Due piani per l'origine

$$\begin{cases} xl + ym + zn = 0 \\ xl' + ym' + zn' = 0 \end{cases}$$

$\rightsquigarrow \mathcal{L}_1, \mathcal{L}_2$ danno due rette in $x+y+z=1$.

Questi due piani si intersecano in una retta r.

$$r \cap \{x+y+z=1\} = \mathcal{L}_1 \cap \mathcal{L}_2$$

$$(A \cap C) \cap (B \cap C) \quad \| \quad (A \cap B) \cap C$$

$\Rightarrow$ $\mathcal{L}_1$ e $\mathcal{L}_2$ sono $\parallel$ sse $r \subseteq \{x+y+z=0\}$

$\Leftrightarrow$ tutte le sol di $\begin{cases} xl + ym + zn = 0 \\ xl' + ym' + zn' = 0 \end{cases}$ sono t.c. $x+y+z=0$

Oss: $xl + ym + zn = 0$

$\Downarrow$

$(x,y,z) \cdot (l,m,n) = 0 \iff \{P \text{ t.c. } \overrightarrow{OP} \perp (l,m,n)\}$

$$\{P : \vec{P} \perp (l,m,n)\} \cap \{P : \vec{P} \perp (l',m',n')\}$$

$$= \{P : \vec{P} = k\,(l,m,n) \times (l',m',n') \quad k \in \mathbb{R}\}$$

$$\begin{cases} lx + my + nz = 0 \\ l'x + m'y + n'z = 0 \end{cases}$$

in coord baricentriche

$$[(l,m,n) \times (l',m',n')] =$$

$$= [mn' - nm' : l'n - ln' : lm' - l'm]$$

Oss: $\mathcal{L}_1, \mathcal{L}_2$ parallele sse $(l,m,n) \times (l',m',n') \in \{x+y+z=0\}$

se $\boxed{mn' - nm' + l'n - ln' + lm' - l'm = 0}$ sse

$\boxed{\det \begin{pmatrix} l & l' & 1 \\ m & m' & 1 \\ n & n' & 1 \end{pmatrix} = 0}$ condizione di parallelismo.

1) retta per $[p_1 : p_2 : p_3]$ $[q_1 : q_2 : q_3]$

$$\det \begin{pmatrix} p_1 & q_1 & x \\ p_2 & q_2 & y \\ p_3 & q_3 & z \end{pmatrix} = 0$$

2) intersezione tra $lx + ym + nz = 0$ e $l'x + m'y + n'z = 0$

$$[(l, m, n) \times (l', m', n')]$$

3) rette parallele $\iff$ $\det \begin{pmatrix} l & l' & 1 \\ m & m' & 1 \\ n & n' & 1 \end{pmatrix} = 0$

Alcuni punti

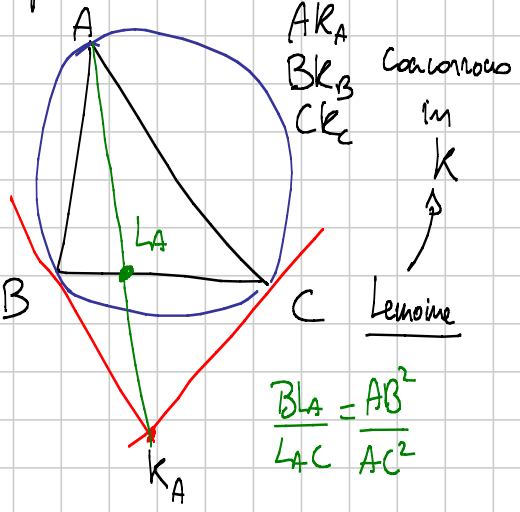
$G = [1:1:1]$

$I = [a:b:c]$ $\quad L = [0:b:c]$ piede bisett. da A

$I_A = [-a:b:c]$ e cicliche

$H = [\tan A : \tan B : \tan C]$

$O = [\sin 2A : \sin 2B : \sin 2C]$



Teo di Ceva + : $[0:q_1:r_1]$, $[p_2:0:r_2]$, $[p_3:q_3:0]$

$D \in BC$ $E \in CA$ $F \in AB$

domanda : quando AD, BE, CF concorrono?
e dove?

$$AD: \det\begin{pmatrix} 1 & 0 & x \\ 0 & q_1 & y \\ 0 & r_1 & z \end{pmatrix} = \boxed{zq_1 - yr_1 = 0}$$

$$\begin{cases} -r_1 y + q_1 z = 0 \\ -r_2 x + p_2 z = 0 \\ -q_3 x + p_3 y = 0 \end{cases}$$

ha una sol. non banale se e solo se le rette concorrono $\iff \det\begin{pmatrix} 0 & -r_1 & q_1 \\ -r_2 & 0 & p_2 \\ -q_3 & p_3 & 0 \end{pmatrix} = 0$

$$r_1 p_2 q_3 - q_1 r_2 p_3 = 0 \iff p_2 q_3 r_1 = q_1 r_2 p_3 \iff \frac{r_1}{q_1} \cdot \frac{q_3}{p_3} \cdot \frac{p_2}{r_2} = 1$$

[Ceva]

$$D = \frac{q_1 B + r_1 C}{q_1 + r_1} \iff \frac{BD}{DC} = \frac{r_1}{q_1}$$

P = punto di concorrenza $(0, -r_1, q_1) \times (-r_2, 0, p_2) =$

$$= (-r_1 p_2, -r_2 q_1, -r_1 r_2)$$

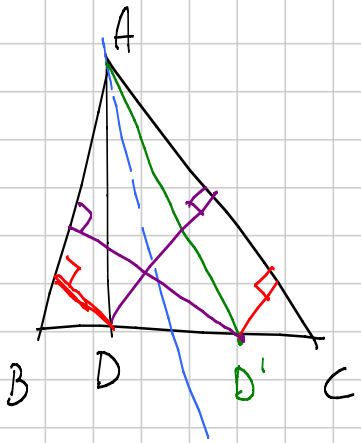
$P = [r_1 p_2 : r_2 q_1 : r_1 r_2]$ $\rightsquigarrow$ c'è un modo di rendere ciclica l'espressione.

$P = [p:q:r]$ i piedi delle ceviane $[0:q:r]$, $[p:0:r]$, $[p:q:0]$.

Punto di Lemoine: $L_A = [0 : b^2 : c^2] \rightsquigarrow K = [a^2 : b^2 : c^2]$

Esercizio per casa: $P = [p : q : r] \rightsquigarrow$ coniugato isogonale

$$P' = \left[\frac{a^2}{p} : \frac{b^2}{q} : \frac{c^2}{r}\right]$$



K è il coniug isog di G

$$G_e = \left[(s-b)(s-c) : (s-c)(s-a) : (s-a)(s-b)\right]$$

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

Es: ABC tri, K pt. dove la circ. inscritta è tg a BC

$IO \parallel BC \Rightarrow AO \parallel HK$

$$\det\begin{pmatrix} a & \sin 2A & x \\ b & \sin 2B & y \\ c & \sin 2C & z \end{pmatrix} = 0$$

$$x\underbrace{(b\sin 2C - c\sin 2B)}_{\alpha_1} - y\underbrace{(a\sin 2C - c\sin 2A)}_{\alpha_2} + z\underbrace{(a\sin 2B - b\sin 2A)}_{\alpha_3} = 0$$

$x = 0$

$$\det\begin{pmatrix} \alpha_1 & 1 & 1 \\ \alpha_2 & 0 & 1 \\ \alpha_3 & 0 & 1 \end{pmatrix} = 0 \iff \alpha_2 - \alpha_3 = 0$$

il resto per casa (può essere comodo scrivere tutto con a, b, c)

BTN 2015 – 2 ABC scaleno, ω circoscritta.

AI, BI, CI incontrano di nuovo ω in D, E, F.

Le parallele a BC, CA, AB per I incontrano EF, DF, DE in K, L, Π.

$\Rightarrow$ K, L, Π allineati.

$$D = [-a^2 : b(b+c) : c(b+c)]$$

Parallela a BC per I: $lx + my + nz = 0$

1) passaggio per I $\quad la + mb + nc = 0$

2) parallela a BC $\quad \det\begin{pmatrix} ! & l \\ 0 & m \\ 0 & n \end{pmatrix} = 0 \iff m - n = 0$

$$\begin{cases} la + mb + nc = 0 \\ m - n = 0 \end{cases} \qquad \begin{matrix} la + m(b+c) = 0 \\ [b+c; -a; -a] \end{matrix}$$

$$\{(b+c)x - ay - az = 0\}$$

G2M - Sam - Metodi Proiettivi Sintetici

Note Title 9/4/2016

0. Rapporti con segno

$\frac{AB}{BC}$ B interno al segmento $AC \iff > 0$

B esterno al segmento $AC \iff < 0$

$\frac{AC}{CB} = \lambda$

$C \xrightarrow{f} \frac{AC}{CB} \in \mathbb{R}$

$AC = \lambda CB$ $\quad CB = \frac{a}{1+\lambda}$

$AC + CB = a$

$\lambda > 0$

$\lambda < 0$ definisco i due pezzi ok

$f : \mathbb{R} \setminus \{B\} \to \mathbb{R} \setminus \{-1\}$ è bigettiva.

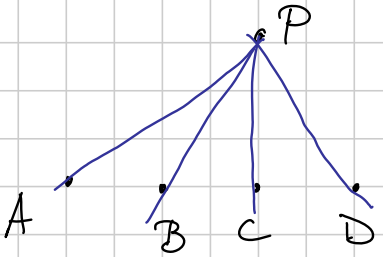
1. Birapporti

$$(A,B;C,D) = \frac{\frac{AC}{CB}}{\frac{AD}{DB}}$$

Oss: $(A,B;C,D) = (A,B;C,E) \Rightarrow D = E$

Dim: $\frac{\frac{AC}{CB}}{\frac{AD}{DB}} = \frac{\frac{AC}{CB}}{\frac{AE}{EB}} \Rightarrow \frac{AD}{DB} = \frac{AE}{EB}$

$\Longrightarrow D = E.$

Prop: 

$(A,B;C,D)$ dipende solo dagli angoli formati in P (P qualsiasi punto fuori dalla retta per A,B,C,D).

Dim: $AC = \dfrac{CP}{\sin C\hat{A}P} \cdot \sin A\hat{P}C$ (↑ Teo dei seni nel $\triangle ACP$), $CB = \dfrac{CP}{\sin C\hat{B}P} \cdot \sin C\hat{P}B$

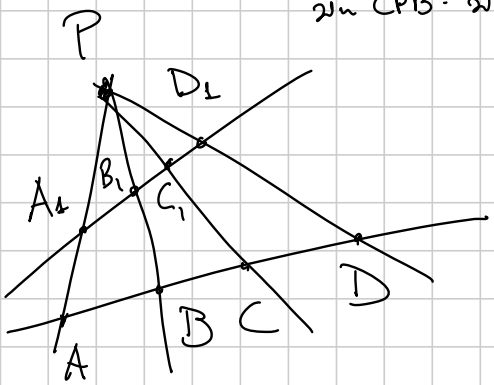
Attenzione: uso angoli orientati!

$AD = \dfrac{DP \cdot \sin A\hat{P}D}{\sin D\hat{A}P}$ $\quad DB = \dfrac{DP}{\sin D\hat{B}P} \cdot \sin D\hat{P}B$

$$\frac{AC}{CB} = \frac{\cancel{CP} \cdot \dfrac{\sin A\hat{P}C}{\sin C\hat{A}P}}{\cancel{CP} \cdot \dfrac{\sin C\hat{P}B}{\sin C\hat{B}P}} \qquad \frac{AD}{DB} = \frac{\cancel{DP} \cdot \dfrac{\sin A\hat{P}D}{\sin D\hat{A}P}}{\cancel{DP} \cdot \dfrac{\sin D\hat{P}B}{\sin D\hat{B}P}}$$

$$\frac{\frac{AC}{CB}}{\frac{AD}{DB}} = \frac{\sin A\hat{P}C}{\sin C\hat{P}B} \cdot \frac{\cancel{\sin C\hat{B}P}}{\cancel{\sin C\hat{A}P}} \cdot \frac{\sin D\hat{P}B}{\sin A\hat{P}D} \cdot \frac{\cancel{\sin D\hat{A}P}}{\cancel{\sin D\hat{B}P}} =$$

$$= \frac{\sin A\hat{P}C \cdot \sin D\hat{P}B}{\sin C\hat{P}B \cdot \sin A\hat{P}D} \quad \blacksquare$$

Cor: 

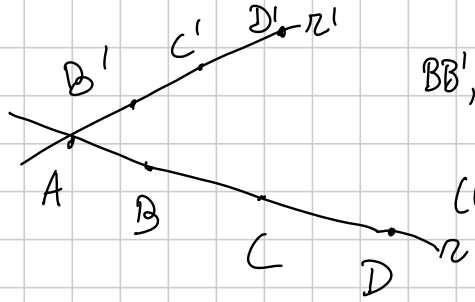
$(A,B;C,D) = (A_1,B_1;C_1,D_1)$

Def: r_1, r_2, r_3, r_4 rette concorrenti in P

$(r_1, r_2; r_3, r_4) = (r_1 \cap \ell, r_2 \cap \ell; r_3 \cap \ell, r_4 \cap \ell)$

ℓ non per P e non parallela a nessuna di loro.

Prop:



BB', CC', DD' concorrono sse $(A,B;C,D) = (A,B';C',D')$

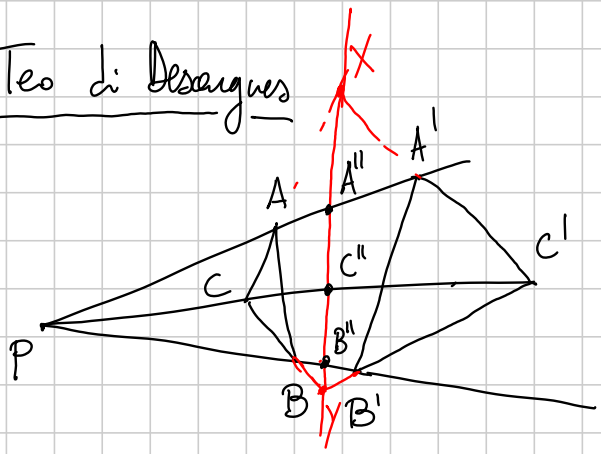
Dim: $\Leftarrow$ sia $P = BB' \cap CC'$, intersezione con r' $r' \cap PD$

allora $(A,B;C,D) = (PA,PB;PC,PD) = (A,B';C',X)$

$(A,B';C',D)$ — ipotesi, per def.

$(A,B';C',D') = (A,B';C',X) \Rightarrow D' = X$ ∎

Teo di Desargues



AA', BB', CC' concorrono $\Leftrightarrow$

$AB \cap A'B'$, $BC \cap B'C'$, $AC \cap A'C'$ sono allineati

Dim: $AC \cap A'C' = X$ $CB \cap C'B' = Y$

Voglio dim che $XY, AB, A'B'$ concorrono

$(P,C,C',C'') = (P,A,A',A'')$ (proiett. da X)

XY =

proiett. da Y $\rightarrow$ =

(P,B,B',B'')

$\Rightarrow AB, A'B', A''B''$ concorrono. ∎

Es: $AB \cap A'B'$, $AC \cap A'C'$, $BC \cap B'C'$ allineati $\Rightarrow AA', BB', CC'$ concorrenti.

Oss:

$r \setminus \{A\} \ni D \longrightarrow (A,B;C,D) \in \mathbb{R}$

$C = D \rightsquigarrow 1$

$B = D \rightsquigarrow 0$

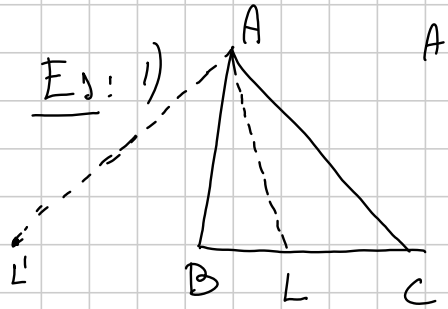
positivo se C, D sono entrambi: esterni o entrambi interni a AB.

$\frac{AC}{CB} / \frac{AD}{DB}$

$r \setminus \{A\} \to \mathbb{R} \setminus \{-\frac{AC}{CB}\}$

biiettivo

Es: 1)

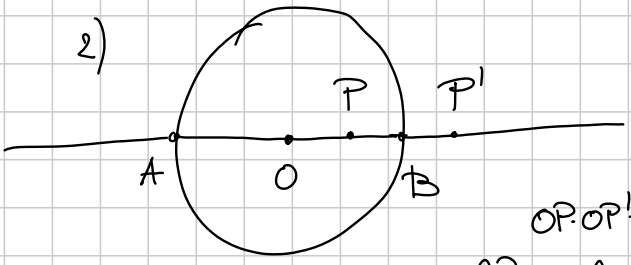


AL bisett. int. AL' bisett. esterna

$(B,C;L,L') = -1$

$\frac{BL}{LC} = \frac{AB}{AC} \quad \frac{BL'}{L'C} = -\frac{AB}{AC}$

2)



P' inverso circolare di P AB diametro.

$(A,B;P,P')$

$OP \cdot OP' = R^2$

$\frac{AP}{PB} = \frac{AO+OP}{PO+OB} \qquad \frac{AP'}{P'B} = \frac{AO+OP'}{P'O+OB}$

segmenti orientati

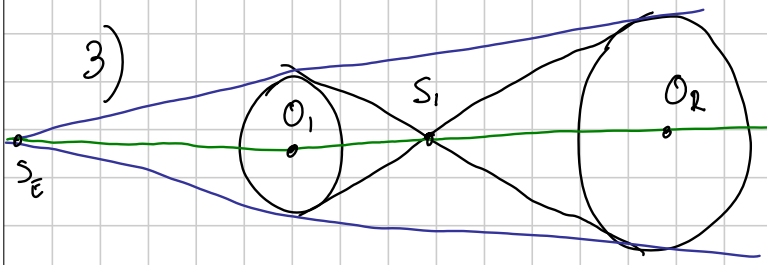
$OP \cdot OP' = AO \cdot OB \qquad \frac{AP'}{P'B} = \frac{AO + \frac{AO \cdot OB}{OP}}{\frac{AO \cdot OB}{PO} + OB} =$

$= -\frac{AO}{OB}\left(\frac{OP+OB}{AO+PO}\right)$

$$\frac{AP}{PB} \Big/ \frac{AP'}{P'B} = \frac{AO+OP}{PO+OB} \Big/ -\left(\frac{OP+OB}{AO+PO}\right) = \qquad AO = OB$$

$$= - \frac{AO+OP}{PO+OB} \Big/ \frac{OP+AO}{OB+PO} = -1$$

3)



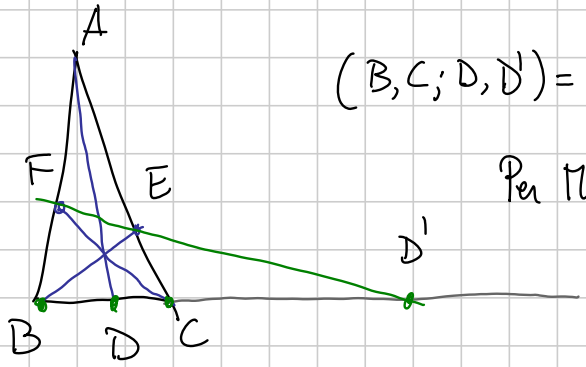
$(O_1, O_2; S_I, S_E) = ?$

$$\frac{O_1 S_I}{S_I O_2} = \frac{R_1}{R_2}$$

$$\frac{O_1 S_E}{S_E O_2} = -\frac{R_1}{R_2}$$

$(O_1, O_2; S_I, S_E) = -1$

4)



$(B, C; D, D') = ?$

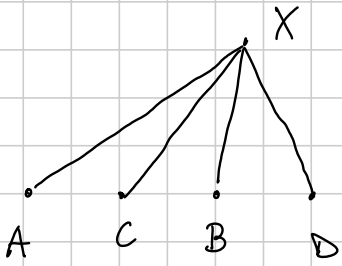
Per Menelao, F, E, D' allineati

$$\Rightarrow \frac{BF}{FA} \cdot \frac{AE}{EC} \cdot \frac{CD'}{D'B} = -1$$

Per Ceva $\frac{BF}{FA} \cdot \frac{AE}{EC} \cdot \frac{CD}{DB} = 1$

$\Rightarrow (B, C; D, D') = -1.$

Prop:



Due delle seguenti implicano la terza

(i) $(A, B; C, D) = -1$

(ii) XC bisca $A\hat{X}B$

(iii) $XC \perp XD$

Dim: (ii) + (iii) $\Rightarrow$ (A, B; C, D) = −1 (i)

↑ bisett int/est.

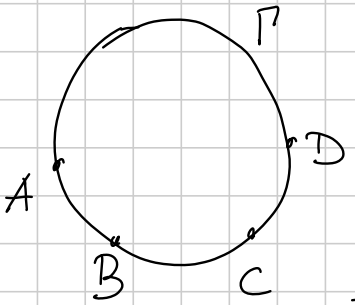
(i) + (ii) $\Rightarrow$ (iii) ovvia

(i) + (iii) $\Rightarrow$ (ii) per esercizio

Oss: $(A,B;C,D) = \lambda \qquad (A,C;B,D) = 1-\lambda$

$$\left(\lambda,\ \frac{1}{\lambda},\ 1-\lambda,\ \frac{\lambda}{1-\lambda},\ \frac{1-\lambda}{\lambda},\ \frac{1}{1-\lambda}\right)$$

Birapporto su una circonferenza

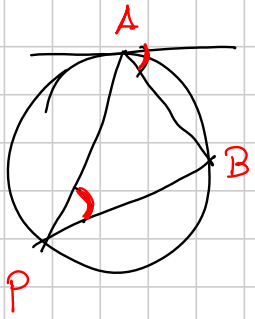


$(A,B;C,D)_\Gamma = (PA,PB;PC,PD)$

$P \in \Gamma$ qualsiasi

notazione: $AA = tg$ a Γ in A

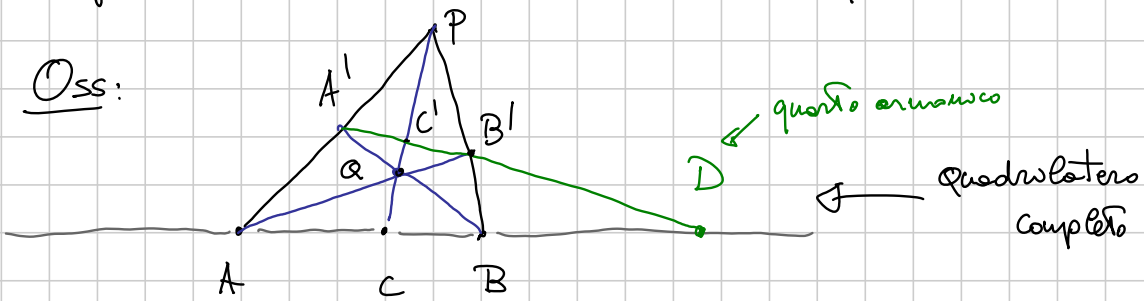
ben definito perché dipende solo dai semi degli angoli in P



PA, PB
AA, AB

Def: $(A,B;C,D) = -1$ A,B,C,D sono una quaterna armonica

Oss:



$$(A,B;C,D) = (A',B';C,D) = (B,A;C,D) = \frac{1}{(A,B;C,D)}$$

↑ proiett. da P ↑ proiett. da Q

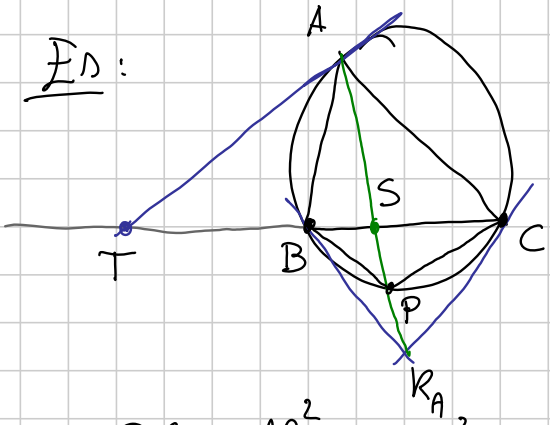
$(A,B;C,D) = \begin{cases} +1 & \text{solo se } C=D \text{ impossibile} \\ -1 & \end{cases}$

Prop: A,B,C,D quaterna armonica, O = pt. medio di AB

1) $\frac{2}{AB} = \frac{1}{AC} + \frac{1}{AD}$ 2) $CA \cdot CB = CO \cdot CD$

3) $OC \cdot OD = OA^2 = OB^2$ 4) $\frac{OC}{OD} = \left(\frac{AC}{AD}\right)^2 = \left(\frac{BC}{BD}\right)^2$

Es:

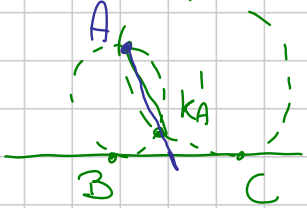


$(B,C;S,T) = -1$

Divagazione: AS è la simmediana

dim: Inversione di centro A e raggio $\sqrt{AB \cdot AC}$ + simm. nella bisettrice di $B\hat{A}C$.

$B \to C$
$C \to B$
$T \to BC$
$BK_A \to$ ch. per B,A tg a BC
$CK_A \to$ ch per C,A tg a BC



$AS \to AS'$ sim di AS rsp alla bisettrice

$AS' = AK_A'$. □

$$\frac{BS}{SC} = \frac{AB^2}{AC^2} = \frac{BP^2}{PC^2}$$

$$\left|(B,C;P,A)_\Gamma\right| = \left|\frac{BP}{PC} \Big/ \frac{BA}{AC}\right| =$$

$$= 1$$

$(B,C;P,A)_\Gamma = -1$

$\Vert$ ← proietto da A

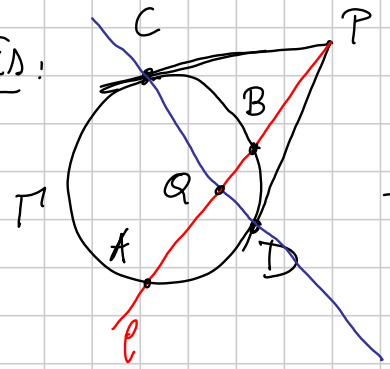
$(AB, AC; AP, AA)$

$\Vert$ ← intersco con BC

$(B,C;S,T) = -1$ ∎

Def: $ACBD$ ciclico con $(A,B,C,D)_\Gamma = -1$ si dice quadrilatero armonico.

ED:



$(A,B;C,D)_\Gamma = -1$

Lem: $\triangle PDB \sim \triangle PAD$ $\quad \triangle PBC \sim \triangle PCA$

$\frac{BD}{AD} = \frac{PB}{PD}$ $\quad \frac{BC}{AC} = \frac{PB}{PC}$

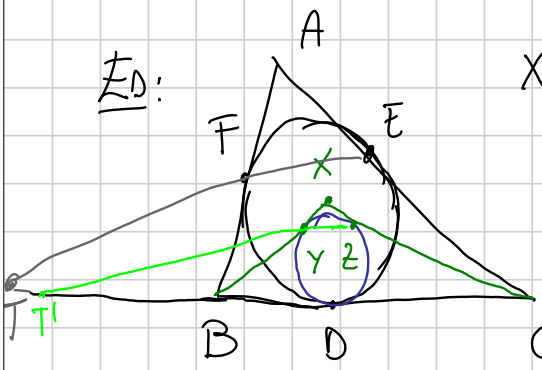
$\frac{BD}{AD} = \frac{BC}{AC} \Longrightarrow (A,B;C,D)_\Gamma = -1.$

↑ perché i pt sono nell'ordine giusto

Cor: Proietto da $C \Rightarrow (CA, CB; CC, CD) = -1$

interseco con $\ell \Rightarrow (A, B; P, Q) = -1.$

ED:



$TE \cdot TF = TD^2$

$TZ \cdot TY = TD^2$

X t.c. la circ inscritta in XBC tange BC in D e XB, XC in Y, Z.

Allora $EZYF$ è ciclico.

Dim: 1) AD, BE, CF concorrono nel pt di Gergonne di ABC

$\Rightarrow (B,C;D,T) = -1$

2) XD, BZ, CY concorrono nel pt di Gergonne di BCX

$\Rightarrow (B,C;D,T') = -1$

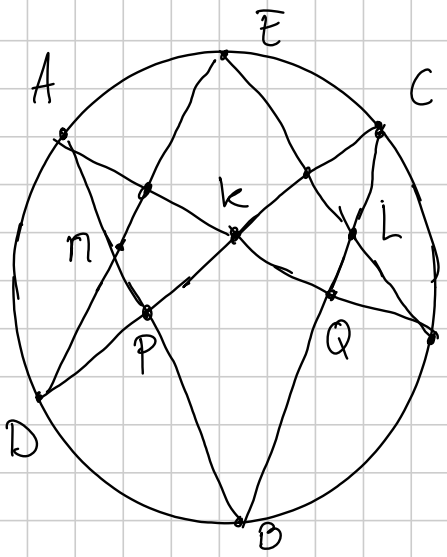
3) $\Rightarrow T = T' \Rightarrow$ ok.

Teo di Pascal

Γ circ, $ABCDEF$ esagono ciclico

$\Rightarrow AB \cap DE,\ BC \cap EF,\ CD \cap FA$ sono allineati

$AB \cap DE = M$, $BC \cap EF = L$, $CD \cap FA = K$



Lem: Veglio Π, K, L allineati.

$$(C, L; Q, B) \underset{F}{=} (C, E; A, B)_{\Pi} =$$

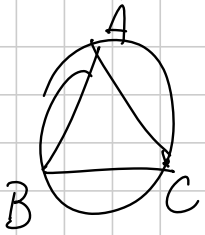
$$\underset{D}{=} (P, \Pi; A, B) \underset{K}{=} (C, \Pi K \cap CB; Q, B)$$

$$\Rightarrow \Pi K \cap BC = L$$

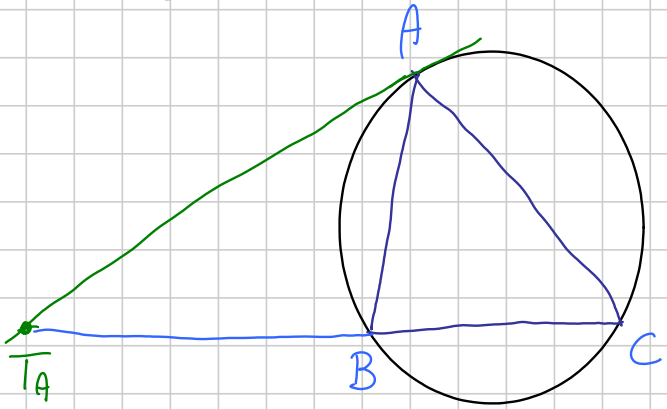
Oss 1: Posso permutare i 6 punti ottenendo 720 diverse terne ordinate di pt. allineati. $\Rightarrow$ 120 rette diverse.

Oss 2: Si può usare pascal anche con punti coincidenti. In quel caso si considereno le tangenti.

Es:



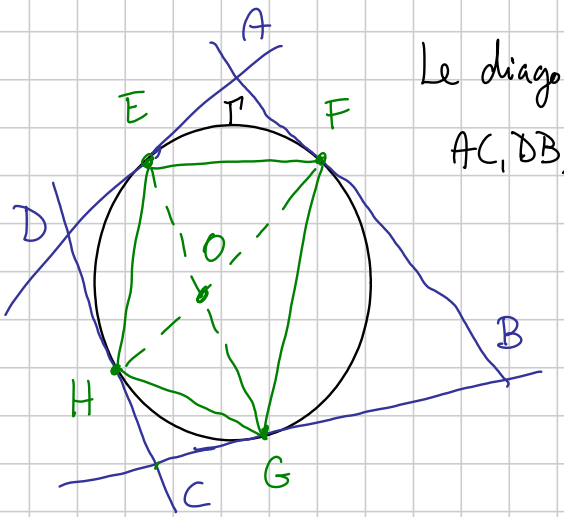
$AABBCC$ $AA \cap BC$, $AB \cap CC$, $BB \cap CA$ sono allineati



T_A, T_B, T_C allineati.

(asse di Lemoine)

Teo di Newton



Le diagonali concorrono
AC, DB, EG, FH

dim: $O = EG \cap FH$ $X = EH \cap GF$

Pascal su EGGFHH ⇝ $EG \cap FH = O$, $GG \cap HH = C$, $GF \cap HE = X$ allineati

Pascal su EEHFFG ⇝ $EE \cap FF = A$, $EH \cap FG = X$, $HF \cap EG = O$ allineati.

A, O, C, X allineati ⇒ $O \in AC$

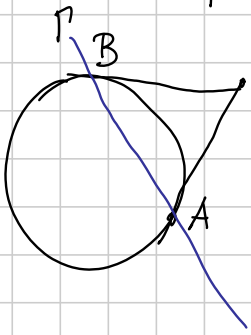
$Y = EF \cap HG$ ⇝ D, O, B, Y allineati ⇒ $O \in BD$. ∎

BRIANCHON

Teo (Brianchon): ABCDEF esagono circoscritto a Γ. Allora AD, BE, CF concorrono.

2) Poli e Polari

Γ circonferenza, P pt. esterno



$pol_\Gamma(P)$ = retta AB polare di P risp. a Γ

PA, PB tg a Γ

equivalente: ⊙ $\mathrm{pol}_\Gamma(P)$ = retta $\perp PO$ che passa per l'inverso di P in Γ.

⊙ funziona anche per P interno o per $P \in \Gamma$!

Oss: $P \in \Gamma \Rightarrow \mathrm{pol}_\Gamma(P) = $ tg a Γ in P

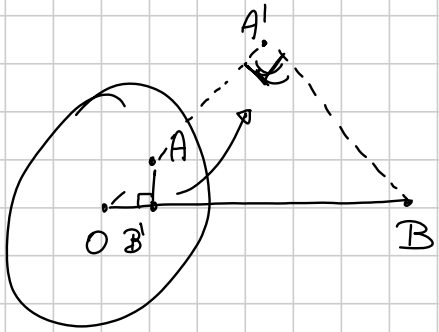
Def: Γ cfr, r retta $\mathrm{pol}_\Gamma(r) = P$ **polo di r rispetto a Γ**
t.c. $OP \perp r$ e $OP \cap \{r\} = P'$ con P' inverso di P in Γ.

Prop: 1) $A \in \mathrm{pol}_\Gamma(B) \iff B \in \mathrm{pol}_\Gamma(A)$

2) $\mathrm{pol}_\Gamma(r \cap s) =$ retta per $\mathrm{pol}_\Gamma(r)$, $\mathrm{pol}_\Gamma(s)$

3) $\mathrm{pol}_\Gamma(A) \cap \mathrm{pol}_\Gamma(B) = \mathrm{pol}_\Gamma(AB)$

dim: 1)



$A\hat{B'}B = \frac{\pi}{2} \iff A \in \mathrm{pol}_\Gamma(B)$

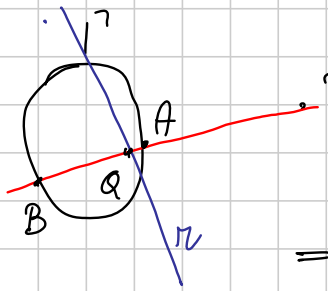
$\Updownarrow$

$O\hat{B'}A = \frac{\pi}{2} \iff O\hat{A'}B = \frac{\pi}{2} \iff B \in \mathrm{pol}_\Gamma(A)$

2, 3) affari vostri

Oss: $\mathrm{pol}_\Gamma(P) = \{\mathrm{pol}_\Gamma(r) \mid P \in r\}$

Prop:



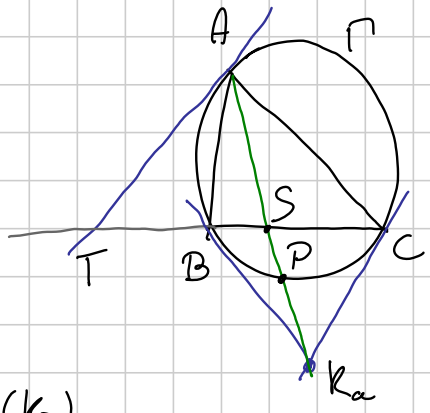
$r = \mathrm{pol}_\Gamma(P)$

$l =$ retta per P

$A, B = l \cap \Gamma$ $Q = l \cap r$

$\Rightarrow (A, B; P, Q) = -1$.

Es:



$(B,C;S,T)$

$BC = pol_\Gamma(K_a)$ $T \in BC$

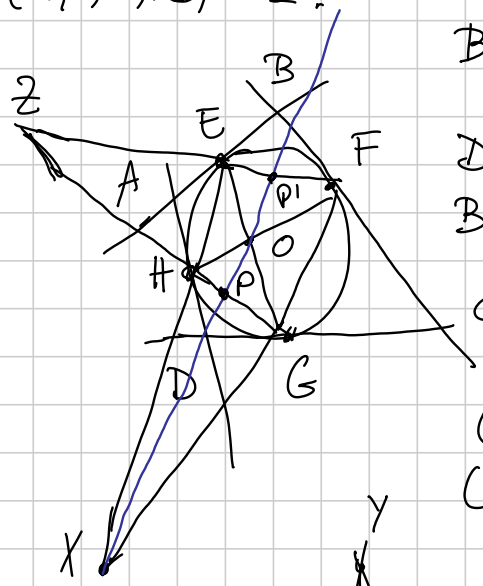
$K_a \in pol_\Gamma(T)$ $\Rightarrow K_aA = pol_\Gamma(T)$

$A \in pol_\Gamma(T)$ $\Rightarrow (B,C;S,T) = -1$

$BC = pol_\Gamma(K_a)$

$\rightarrow (A,P;S,K_a) = -1$.

Es:



B, D, O, X sono allineati

$D = pol_\Gamma(HG)$

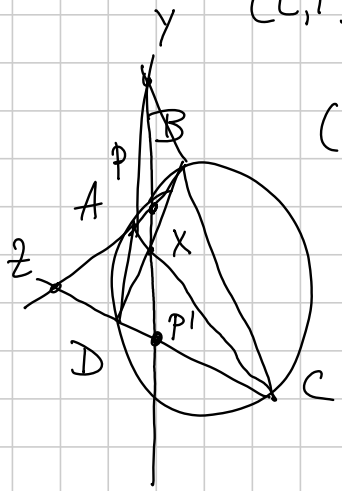
$B = pol_\Gamma(EF)$

$Z = pol_\Gamma(BD)$

$(H,G;Z,P) = -1$

$(E,F;Z,P') = -1$

Oppure:



$(A,B;Z,P) =$

$= (C,D;Z,P') = -1.$

Oss: $\Gamma_A = \{P : PB/PC = AB/AC\}$. N_A centro di Γ_A

$\Rightarrow N_A$ è pt. medio di LL'

L = piede bisettr. interna

L' = " " esterna

$N_A = pol_\Gamma(AK_A)$

3) L'infinito

Proiettivo = **Piano** + centri dei fasci impropri $= r_\infty$

ω

A_∞, B_∞

PA_∞ = retta per P che appartiene al fascio di centro A_∞

$r \cap s = A_\infty \Rightarrow r, s \in$ fascio di centro $A_\infty \Rightarrow r \parallel s$

$A_\infty B_\infty$ = ?? è l'insieme di tutti questi centri. $= r_\infty$

$r \cap r_\infty$ = centro del fascio improprio che contiene r

Posso definire il birapporto su tutto il proiettivo

$$(A, B; C, D_\infty) = (PA, PB; PC, PD_\infty)$$

$D_\infty \in AB$

A_1, B_1, C_1, D_∞ sono allineati.

Posso definire $\text{pol}_\Gamma(r_\infty) = O$, $\text{pol}_\Gamma(A_\infty) = r$

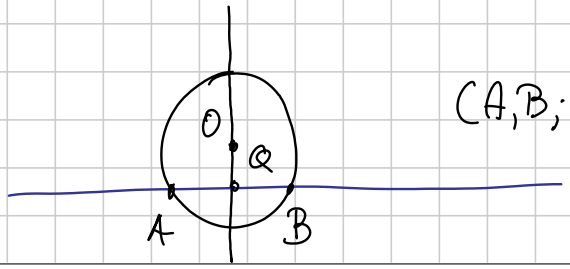
$r \perp OA_\infty$

$O \in r$

Oss: A M B M pt. medio di AB

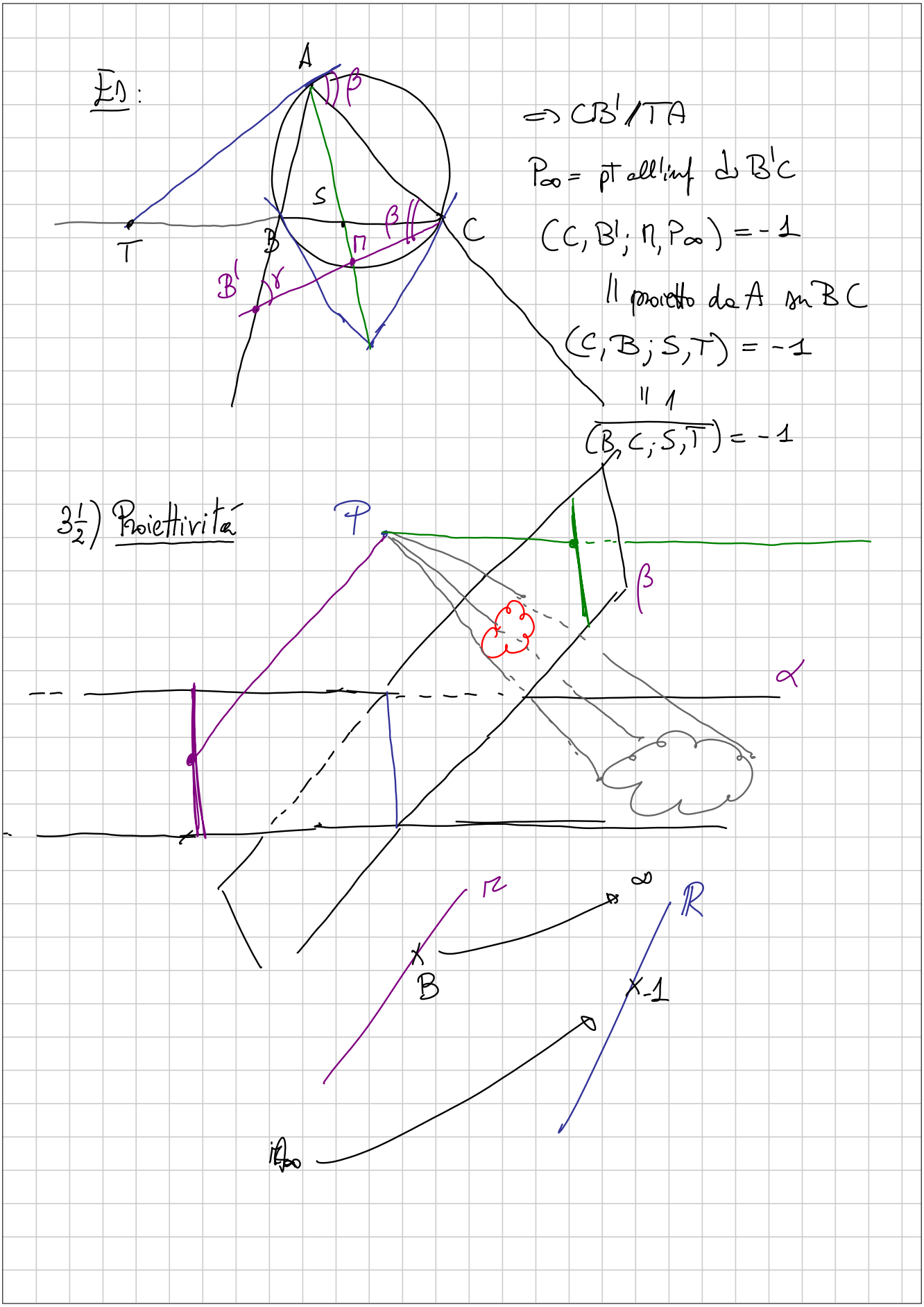
$(A, B; M, P_\infty) = -1$ P_∞ = pt. all'infinito di AB.

Oss:



$(A, B; Q, A_\infty) = -1$ $\Longrightarrow A_\infty$

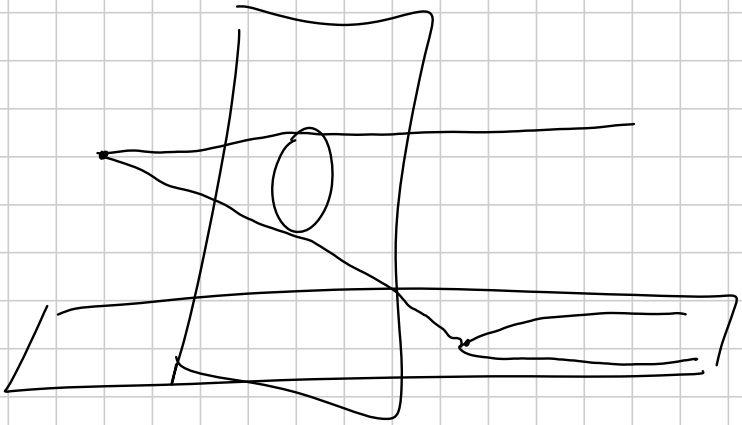
$\hat{}$ lemma della polare


ED:
A
T
B
C
S
B'
β
γ
η
$\Rightarrow CB' \parallel TA$
P_∞ = pt all'inf di $B'C$
$(C, B'; \eta, P_\infty) = -1$
Il proietto di A su BC
$(C, B; S, T) = -1$
$\| \; 1$
$(\overline{B}, C; S, \overline{T}) = -1$
$3\frac{1}{2}$) Proiettività
γ
β
α
r
∞
R
B
X
X-1
i_{∞}

Aggiungendo le rette all'infinito, ho una trasf

Proiettivo $\longrightarrow$ Proiettivo bigettiva

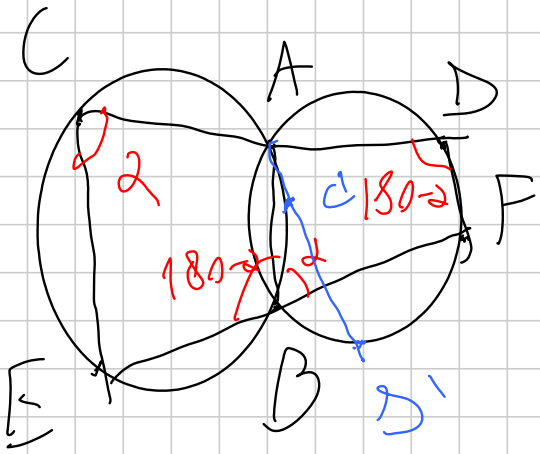
1) rette in rette
2) conserva l'incidenza
3) preserva i birapporti
4) permette di definire poli e polari x le coniche



S16 M-G 3

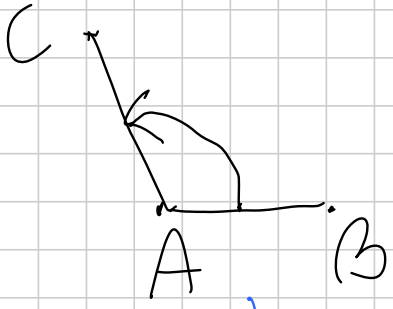
Note Title 9/6/2016

PROBLEMA 1 (TED REIM)



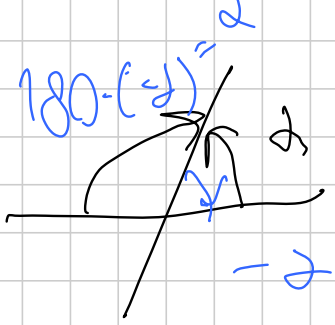
Th CE // DF

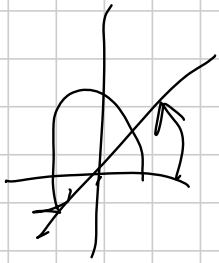
ANGOLI ORIENTATI



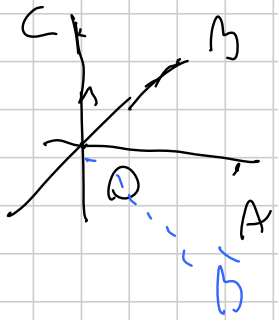
$\measuredangle BAC = (\widehat{BAC}) = \measuredangle(BA, AC)$

$\measuredangle BAC = -\measuredangle CAB$





1) $\angle BAC = -\angle CAB$

2) 

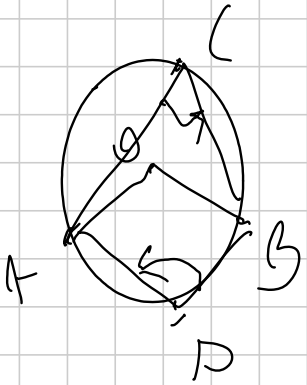
$\angle AOC = \angle AOB + \angle BOC$

3) 

$\angle, A, D$ allineati

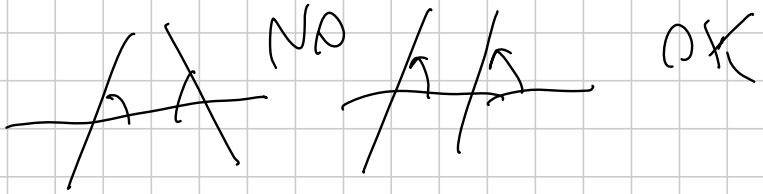
$\Downarrow$

$\triangle ADC$ $\quad \angle BAC = \angle BAD$

4) 

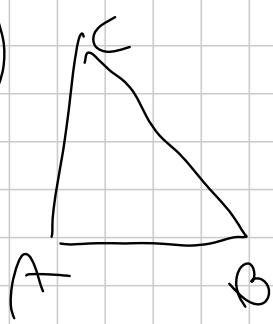
$\angle AOB = 2\angle ACB = 2\angle ADB$

5) $r_1 \parallel r_2 \iff \angle(r_1, r_3) = \angle(r_2, r_3)$



6) $r_1 \perp r_2 \iff \angle(r_1 r_2) = \angle(r_2, r_1)$

7)



$\angle ABC + \angle BCA + \angle CAB = 0 \quad (180)$

8)

$\triangle ABC \sim \triangle DEF$

$\Updownarrow$

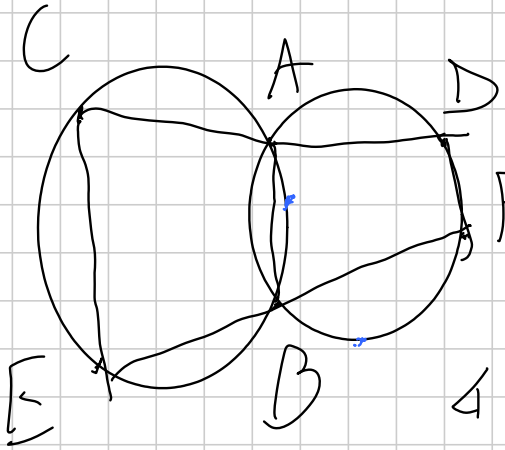
$\angle BAC = \angle EDF$

$\angle ACB = \angle DFE$

$\angle CBA = \angle FED$

- Scrivo tutto normalmente, ma ho fatto a mano un disegno di angoli in senso antiorario
- Scrivo usando le proprietà di sopra

— O — O —



$\angle ECA = \angle EBA$

$\angle EBA = \angle FBA$

$\angle FBA = \angle FDA$

$\angle ECD = \angle FDC$

ESERCIZI X CASA

1) DIMOSTRARE TUTTE LE PROPRIETÁ

2) $\forall\, \Gamma_i$: $1 \le i \le 4$ $\quad \bigcap_{i=1}^{4} \Gamma_{i,1}\, A_i', B_i'$

Th: $A_1A_2A_3A_4$ ciclico $\Leftrightarrow$ $B_1B_2B_3B_4$ è ciclico

3) P punto, A, B, C allineati: O_{BCP}, O_{ACP}, O_{ABP}
(centri in) $\quad$ " X $\quad$ " Y $\quad$ " Z

Th: XYZP è ciclico

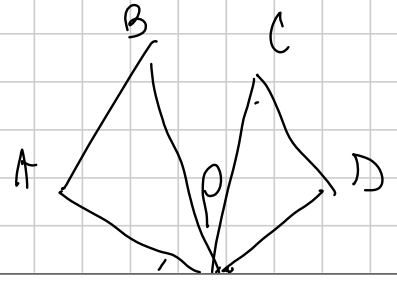
4) P punto, A, B, C $\triangle$ O_{BCP} ha centro in X
e ciclico.

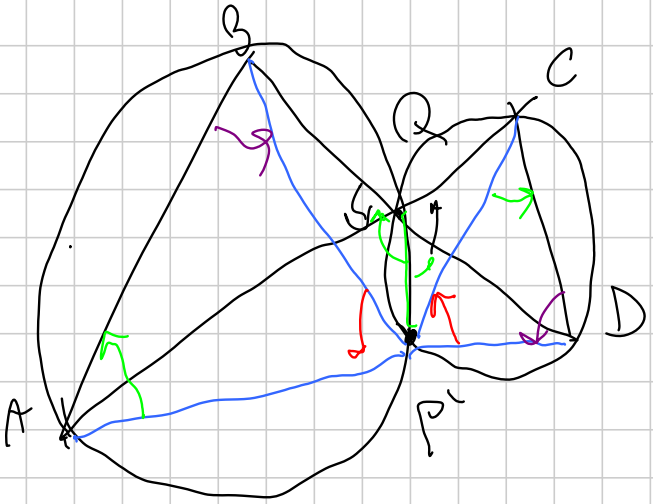
O_{XBC}, O_{ZAB}, O_{AC_1} si intersecano in Q

— O — O —

LEMMA OMOTETIA

$\exists!\, P$ t.c. $\triangle PAB \sim \triangle PCD$





$\odot_{ABQ}$ $\odot_{CQD}$

$(Q = AC \cap BD)$

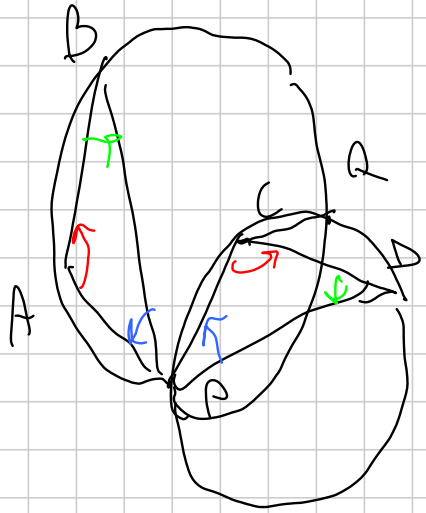
Considero $P'AB$, $P'CD$

$\angle BP'A = \angle BQA = \angle DQC = \angle DP'C$

$\angle P'AB = \angle P'AB = \angle P'QD = \angle P'CD$

$\Delta P'AB$, $\Delta P'CD$ hanno angoli uguali $\Rightarrow$ sono simili

2ª FRECCIA il punto P è unico



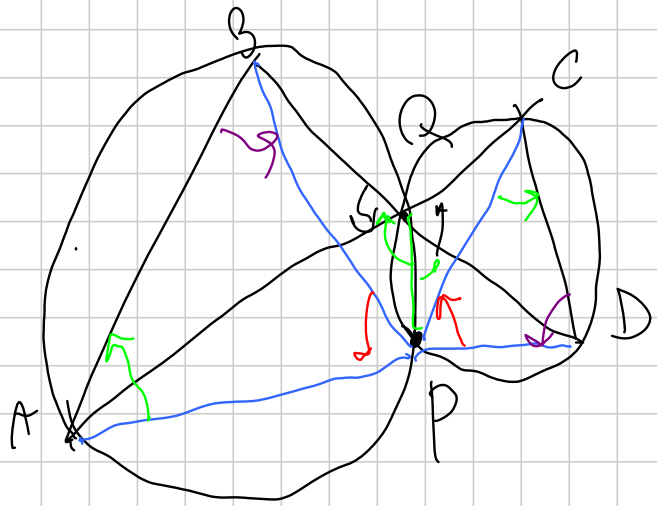
$\odot_{ABP} \cap \odot_{PCD} = Q$

$\angle CDP = \angle CQP$

$\angle ABP = \angle AQP$ $\Rightarrow A, Q, C$ allineati

Analogamente $BQD \Rightarrow P = P'$

$\Rightarrow \exists P$ ed è unico. C.V.D.



OSS. ANCHE

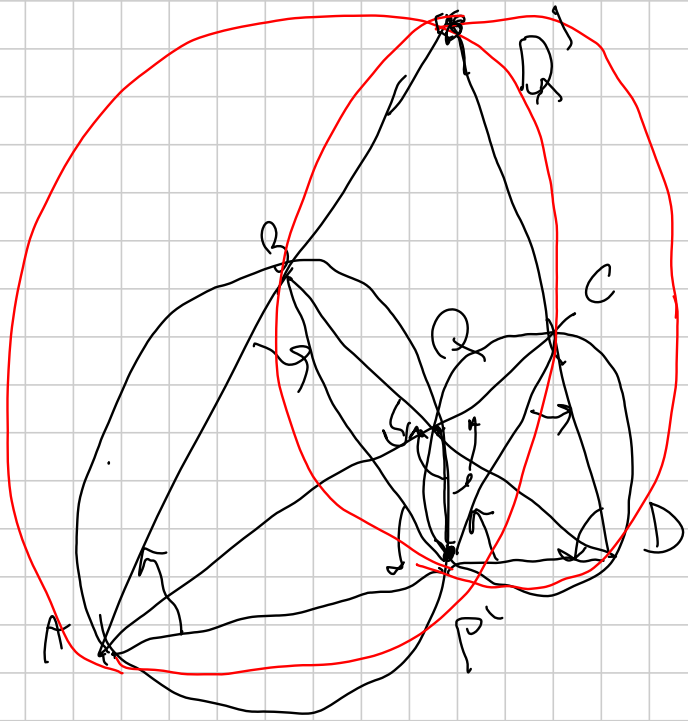
$\triangle PAC \sim \triangle PBD$

$\frac{PA}{PB} = \frac{PC}{PD} \Leftrightarrow \frac{PA}{PC} = \frac{PB}{PD}$

$\angle CPA = \angle CPB + \angle BPA = \angle CPB + \angle DPC$

$= \angle DPB$ C.V.D.

OSS. 2. APPLICO il lemma inverso della potenza a $\triangle PAC, \triangle PBD$



A, C , BD $\exists P$ t.c.

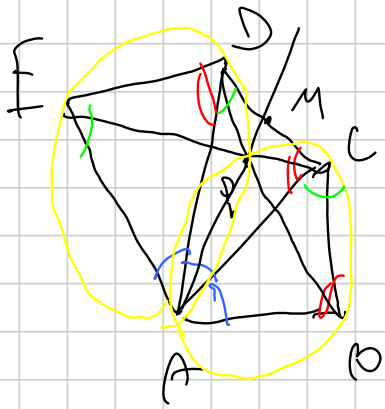
$\Downarrow$

$\exists Q = AB \cap CD$

t.c. $QACP$, $QBPD$ non ciclici

PROBLEMA 2 $\angle BAC = \angle CAD = \angle DAE$

$\angle CBA = \angle DCA = \angle EDA$

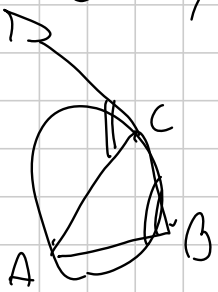


$P = BD \cap EC$

$AP \cap DC = M$

Th: $CM = DM$

Per il lemma della stomachia, il centro di omotetia che manda $BC \to DE$ è l'intersezione delle circonf. $\odot BCP, DPE \Rightarrow A \in \odot_{BCP}, \odot_{DEP}$



$\Rightarrow DC$ tange $\odot BCA$

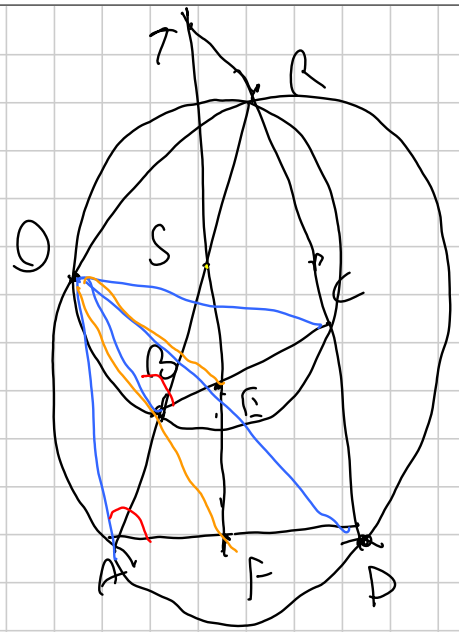
Analogamente DC tange $\odot DEA$

$MC^2 = MP \cdot MA = MD^2 \Rightarrow MC = MD$ C.V.D.

— o — o —

PROBLEMA 3 $R = BA \cap CD$, $T = CD \cap EF$

$S = AB \cap EF$



$E \in BC$, $F \in AD$

E.c. $\frac{BE}{EC} = \frac{AF}{FD}$ $\left(\frac{a}{b} = \frac{c}{d} \Rightarrow \frac{a}{a+b} = \frac{c}{c+d}\right)$

Th $\bigcirc_{SEB}$, $\bigcirc_{SAF}$, $\bigcirc_{TEC}$, $\bigcirc_{TFD}$ concomm.

$\triangle OBC \sim \triangle OAD$

$\Downarrow$

$\frac{OB}{BC} = \frac{OA}{AD}$ $\rightarrow$ Ipotiz. $\frac{BE}{BC} = \frac{AF}{AD}$

$\rightarrow \frac{OB}{BE} = \frac{OA}{AF}$ $\left(\frac{OB}{OA} = \frac{BC}{AD} = \frac{BE}{AF}\right)$

$\Downarrow$

$\angle OBE = \angle OAF$ $\rightarrow$ $\triangle OBE \sim \triangle OAF$

Il centro di omotetia $BE \to AF$ è l'intersezione di $\bigcirc_{CES}$, $\bigcirc_{AFS}$

$\Downarrow$

$O \Rightarrow \bigcirc_{BES}$, $\bigcirc_{AFS}$ c.d.d.

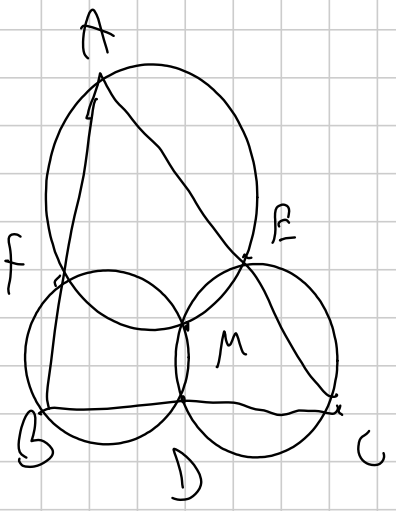
Per analogia (Scambio B e C, A e D)

$\bigcirc_{CET}$, $\bigcirc_{DFT}$ c.d.d.

$\mathcal{C}_{BES}, \mathcal{C}_{AFS}, \mathcal{C}_{CET}, \mathcal{C}_{DFT}$ concorrono in O C.V.D.

— O — O —

MIQUEL



$D, E, F \in BC, AC, AB$ a caso

$\mathcal{C}_{CDE}, \mathcal{C}_{AFE}, \mathcal{C}_{FBD}$

Th concorrono in punto M

DIM $M' = \mathcal{C}_{CED} \cap \mathcal{C}_{BFD}$

Voglio $M' \in \mathcal{C}_{AFE}$

$\angle EM'F = \angle EM'D + \angle DM'F = \angle ECD + \angle DBF =$

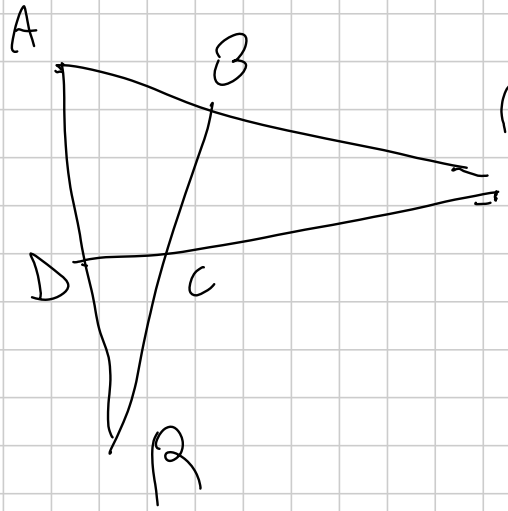
(per le cicliche)

$= 180 - \angle BAC = -\angle BAC = \angle CAB = \angle EAF$

$\Rightarrow EMAF$ ciclico

— O —

MIQUEL ++



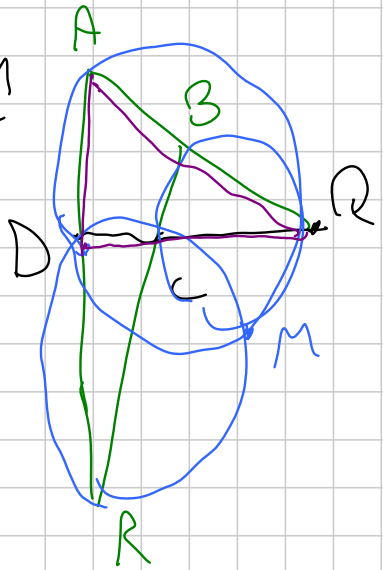
$Q = ABA'CD$

$R = ADA'BC$

$\bigcirc_{DCR}, \bigcirc_{ABR}, \bigcirc_{ADQ}, \bigcirc_{BCQ}$

concorrono in M

DIM



Per m'qual $\triangle$ su ABR

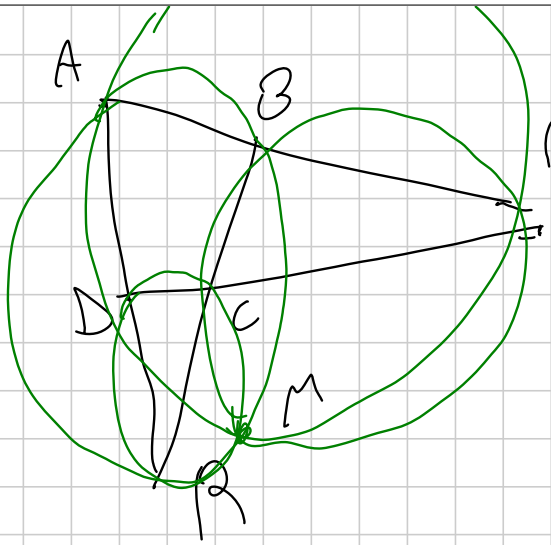
$\bigcirc_{RDC}, \bigcirc_{BCQ}, \bigcirc_{ADQ}$

concorrono in M

m'qual su $ADQ \Rightarrow \bigcirc_{BCQ}, \bigcirc_{ABR}, \bigcirc_{DCR}$

concorrono in M'

Unendo i due fatti, $M = M' \Rightarrow$ le 4 circonferenze concorrono.



RD, SQ

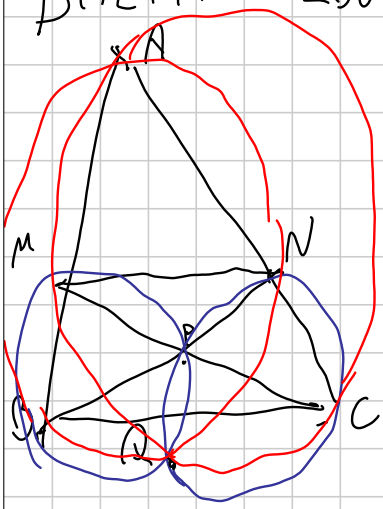
Per il lemma della mantellina

$\triangle MDR \sim \triangle MRB$

$\triangle MRB \sim \triangle MSQ$ e simili

— ○ —

BALKAN 2009/2



$MN \parallel AC$ $MC \cap BN = P$

$\bigcirc_{BMP} \cap \bigcirc_{PNC} = Q$

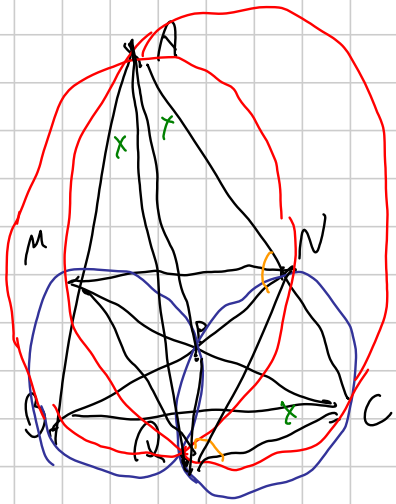
Th: $\angle BAQ = \angle PAC$

1) Inversione + simmetria: Circ A, raggio $\sqrt{AN \cdot AB}$, bisettrice di BAC (X STASERA)

2) Notiamo che è la configurazione del quadrilatero completo

$\angle ABQ = \angle MPQ = \angle CPQ = \angle CNQ = \angle ANQ$

$\Rightarrow ABQN, AMQC$ ciclici



$\angle BAP = \angle BNP = \angle PCP$

$\angle PQC = \angle PNC = \angle PNA$

Se t_{en} i vez, $\triangle PQC \sim \triangle PNA$

$\Downarrow$

prvo o dimostrato.

Mi basta $\frac{PN}{NA} = \frac{PQ}{QC} \Rightarrow \frac{PN}{PQ} = \frac{AN}{QC}$

$\parallel$

$\frac{AM}{MQ}$

$MN \parallel BC$

$\downarrow$

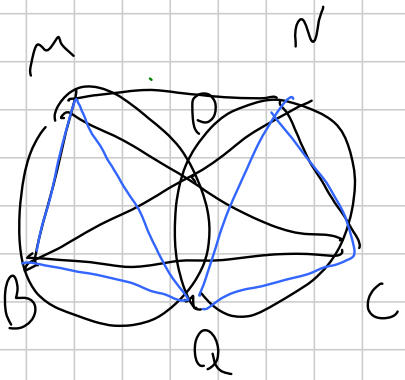
Per lo ten, mi basta $\frac{AM}{MQ} = \frac{AN}{QC} \Leftrightarrow \frac{MQ}{QC} \overset{?}{=} \frac{AM}{AN} = \frac{AB}{AC} = \frac{MB}{NC}$

$\frac{MB}{MQ} = \frac{NC}{CQ}$ Guardo $\triangle MBQ, \triangle NCQ$, è la configurazione

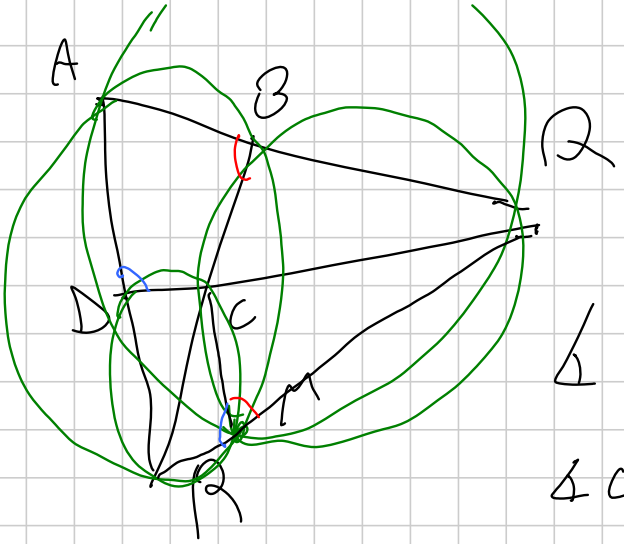
della dimostrata $\Rightarrow \triangle MBA \sim \triangle NCQ$

$\Downarrow$

Ten



— O —



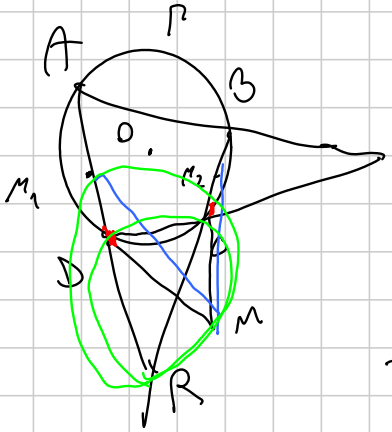
Quant'è di R, Q, M non allineati?

$\angle CMR = \angle CDR = \angle CDA$ (1)

$\angle CMQ = \angle CBQ = \angle CBA$ (1)

$M \in RQ \iff \angle CDA = \angle CBA \iff ABCD$ è ciclico

Da ora in poi, $ABCD$ è ciclico.



O il centro di P

Th: $OM \perp QR$

DIM Sia M_1 pt medio di AD

Sia M_2 ..... BC

$\triangle MAD$, $\triangle MBC$ non simili (per ipotesi)

$\angle MDA = \angle MCB$ $\quad \frac{AD}{DM} = \frac{BC}{CM}$ $\quad \left(\frac{AD}{M_1D} = \frac{BC}{M_2C} = 2\right)$

Segue $\frac{M_1D}{DM} = \frac{M_2C}{CM}$ e $\angle M_1DM = \angle M_2CM$

Sono simili e hanno M in comune $\Rightarrow$ $\exists$ rotomotetia di centro M che manda

$M_1D \to M_2C \qquad M_1M_2 \to DC$

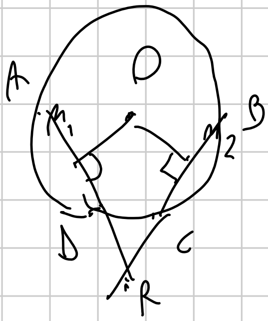
$\exists$ rotazione di centro M: $M_1M_2 \to DC \Rightarrow R = M_1D \cap M_2C$

sta sulle circonferenze

$\bigcirc_{MRDC}$, $\bigcirc_{MRM_1M_2}$

Supponiamo M_1M_2RM ciclico.

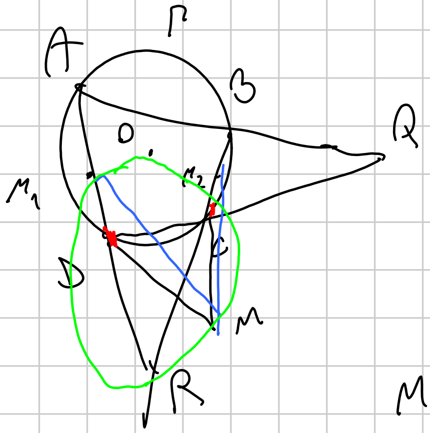
MA! M_1M_2RO è ciclico



$\Rightarrow \bigcirc_{M_1M_2R}$ passa per O, M

$\Downarrow$

M_1M_2ROM ciclico



$\measuredangle OMR = \measuredangle OM_2R = 90°$

$\measuredangle OMR = 90°$

$M \in RQ \Rightarrow OM \perp RQ$

— o — o —

OSS: $ACOM$, $BODM$ sono ciclici

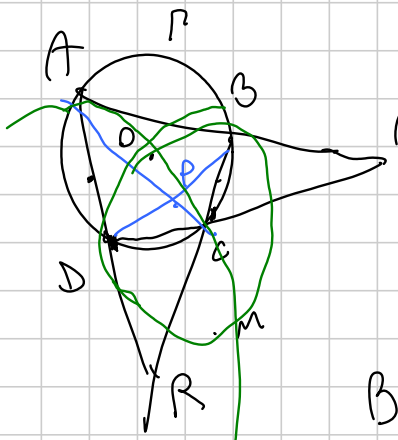
$\measuredangle AOC = 2\measuredangle ABC = 2\measuredangle ADC$

$\measuredangle AMC = \measuredangle AMR + \measuredangle RMC = \measuredangle ABR + \measuredangle RDC = \measuredangle ABC + \measuredangle ADC = \angle AOC$

(dove $\measuredangle ABC = \frac{1}{2}\angle AOC$ e $\measuredangle ADC = \frac{1}{2}\angle AOC$)

Siccome $ABMR$ è ciclico $\Rightarrow \measuredangle AMR = \measuredangle ABR$

" " $CMDR$ " $\Rightarrow \measuredangle RMC = \measuredangle RDC$



P, M inversi rispetto a Γ

DIM

Γ inverto in Γ

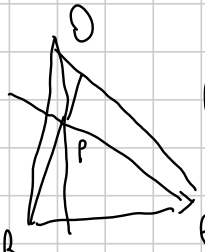
$BD \Rightarrow O_{BOD}$ $AC \Rightarrow O_{AOC}$

Adesso dimostriamo che ADCM, BODM sono cicl

$P' = (AC \cap BD)' = (AC)' \cap (BD)' = O_{AOC} \cap O_{BDO} = M$

CONSEGUENZA: OPM allineati $OM \perp RQ \Rightarrow OP \perp RQ$

$pol_\Gamma(P) = RQ$, $pol_\Gamma(Q) = RP$, $pol_\Gamma(R) = PQ$ e che $OR \perp PQ$, $OQ \perp RP$



Nel $\triangle PRQ$, O è ortocentro

ESERCIZIO CASA

IMO 1985/5; CHINA 1992/4, RUSSIA 1997/GRADE 8 ES 7

TST 15/2 ABCD ciclico $AC \cap BD = P$ $AD \cap BC = E$

$O_{APD} \cap O_{BPC} = Q$ M pt medio di AD

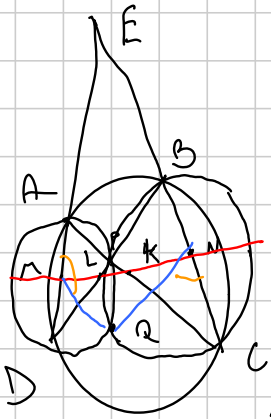
N ~~~ BC

$MN \cap AC = K \quad MN \cap BD = L$

Th: a) $EMNQ$ ciclico

b) $AMKQ$, $BLQN$ ciclici

c) O_{AMK}, O_{BLC}, AB concorrono



DIM: $\triangle PBE \Rightarrow Q$ è Miquel

$\Downarrow$

$\triangle ADQ \sim \triangle CBQ \Rightarrow \triangle AMQ \sim \triangle CNQ$

$\angle EMQ = \angle AMQ = \angle CNQ = \angle ENQ \Rightarrow EMNQ$ ciclico

a) ✓

b) $\triangle AMQ \sim \triangle CNQ \Rightarrow \angle AQM = \angle CQN$

HOPE: $\angle AKM = \angle AQM = \angle CQN$

$\angle CKN$

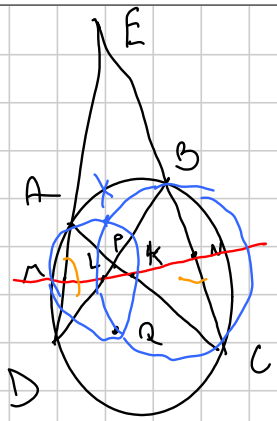
Applichiamo la notevole su AM, $NC \Rightarrow$ centro di notevole $=$

$O_{AMK} \cap O_{KNC} = Q \Rightarrow AKMQ$, $NKAC$ ciclo

$BLNQ$

c) O_{AKM}, O_{BLC}, AB concorrono

$O_{AKM} \cap O_{BLC} = X$



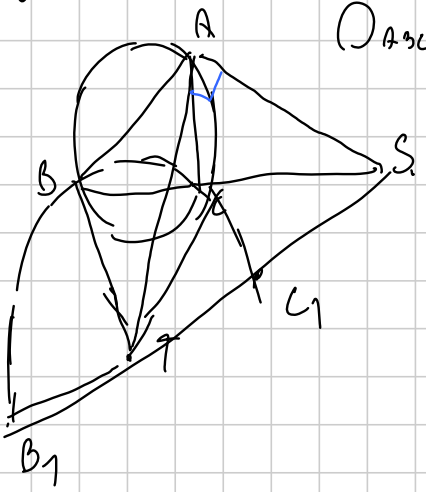
$\angle AXQ = \angle AKQ = \angle CKQ = \angle CNQ = \angle BNQ$

$= \angle BXQ$ perché $BLNQ$ ciclico

$\angle AXQ = \angle BXQ \Rightarrow AXB$ allineati

— O —

USA TST 2007



$\Omega_{ABC} = \Gamma$, BT, CT tangono Γ. Sia $S \in BC$ t.c. $\angle SAT = 90°$

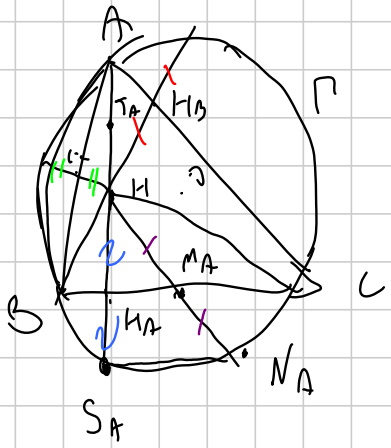
ω la circ. di centro T e raggio BT

$B_1 = ST \cap \omega$ $C_1 = ST \cap \omega$

$\Delta ABC \sim \Delta AB_1C_1$ (LLA)

— O — O —

Un po' di cose note (si spera)



Omotetia di fattore $\frac{1}{2}$ in H

$S_A \to H_A$ $\Gamma \to$ circonferenza per

$N_A \to M_A$ • punti medi dei lati

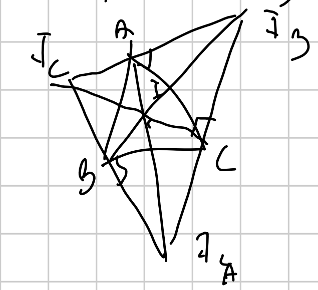
$A \to T_A$ • piedi delle altezze

• punti medi AH e circ.

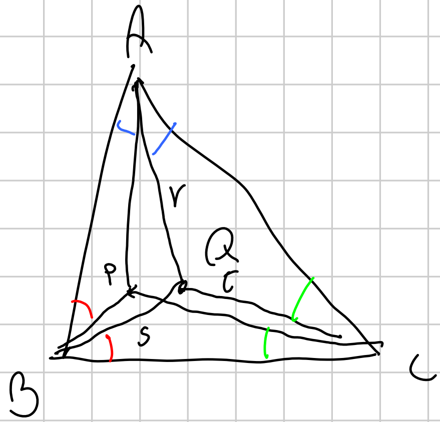
ed è Feuerbach.

$\Rightarrow$ Centro $\in$ retta di Euler = pt medio di OH

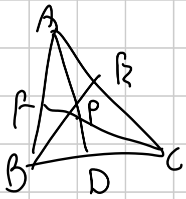
Feuerbach tange incerchio (nel punto di Feuerbach) e gli excerchi.
(SAPEVATELO!)



→ $I_C C \perp I_B I_A$ · $I_B I_C I_A$ ha ortocentro I.
La sua Feuerbach è proprio Γ (passa per i piedi delle altezze, ovvero A, B, C)



Ceva:



$\frac{BD}{DC} \cdot cyc = 1$

$\frac{\sin BAD}{\sin DAC} \cdot cyc = 1$

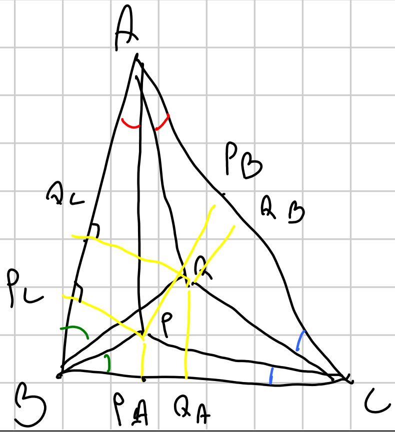
$\frac{[BAD]}{[DAC]} \cdot cyc = 1$

⇓

AP, BP, CP concorr.

$$\frac{\sin BAP}{\sin PAC} = \frac{\sin (r, AC)}{\sin (BA, r)} \Rightarrow \text{per Ceva } r, s, t \text{ concorrono}$$

P e Q vengono detti CONIUGATI ISOGONALI



P_A, P_B, P_C proiezioni di P sui lati
Q_A, Q_B, Q_C .... Q ....

Th $P_A P_B P_C Q_A Q_B Q_C$ sono conciclici

$\triangle BPP_A \sim \triangle BQQ_C$ $\quad \angle PBP_A = \angle Q_CBQ$ e $\angle QQ_CB = \angle PP_AB = 90$ $\Rightarrow$ Sono simil.

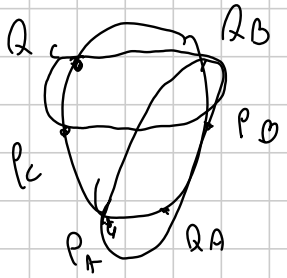
Analogamente $\triangle BQR_A \sim \triangle BPP_C$

$\frac{BP}{BP_A} = \frac{BQ}{BQ_C}$; $\frac{BP}{BP_C} = \frac{BQ}{BR_A} \Rightarrow \frac{BP_A}{BQ_C} = \frac{BP}{BQ} = \frac{BP_C}{BQ_A}$

$\Rightarrow BP_A \cdot BR_A = BP_C \cdot BQ_C \Rightarrow P_AR_AP_CQ_C$ è ciclo ω_B

Ripeto il ragionamento per $A, C \Rightarrow P_AR_AP_BQ_B$ è ciclo ω_C

$P_BR_BQ_CP_C$ è ciclico ω_A



Presuppongo le tesi false $\Rightarrow$ sono 3 circonferenze distinte.

Asse rad. $\omega_A \omega_B = AB$

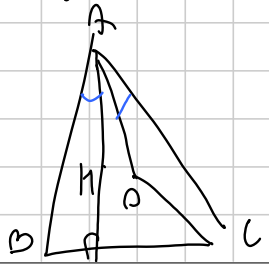
$\omega_A \omega_C = AC$

$\omega_B \omega_C = BC$

Gli assi radicali di 3 circonferenze concorrono $\Rightarrow$ ASSURDO

$\Rightarrow P_AR_AP_BR_BP_CR_C$ è ciclico

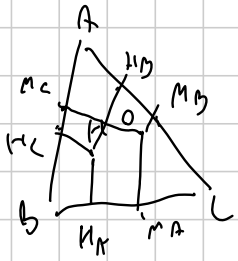
OSS.



H e O sono coniugati isogonali.

$\angle BAH = 90 - B$

$\angle ACO = \frac{1}{2}(180 - \angle AOC) = 90 - \frac{1}{2}(2\angle ABC) = 90 - B$

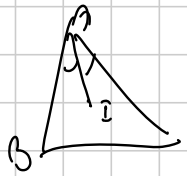


Per il teorema dei cerchi circoscritti

$H_A M_A H_B M_B H_C M_C$ è ciclico

M_a è Feuerbach.

— O —



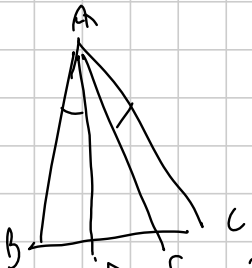
I è cerchio circoscritto di riferimento

G è cerchio circoscritto di Lemoine. (pt di concorrenza delle simmediane)

AT_A è simmediana.

Se simmediane concorrono in L.

ES CASA (TEOREMA DEI RAPPORTI DI STEINER)

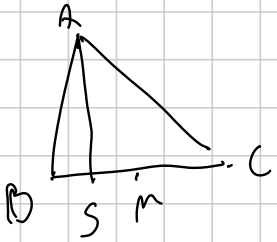


ABC D, $D, E \in BC$ $\angle BAD = \angle EAC$

AD, AE cerchi

Th: $\frac{AB^2}{AC^2} = \frac{BD \cdot BE}{CD \cdot CE}$ (DIM: Ceva dei rapporti in ABD, ACD, ABE, ACE)

CASO PARTICOLARE

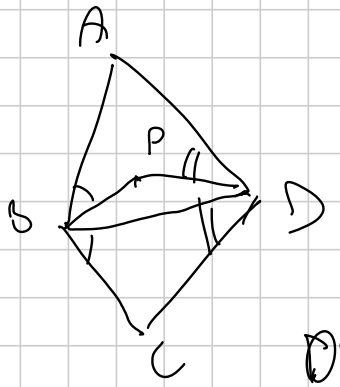


$\frac{BS}{CS} = \frac{AB^2}{AC^2}$

Fine digressione

— O — O —

IMO 2014/5



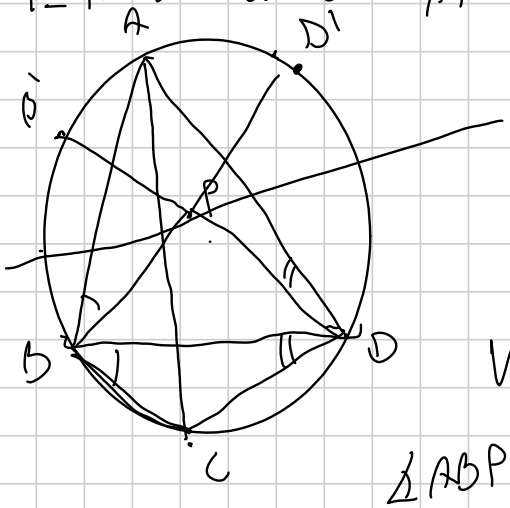
P all'interno del quadrilatero ABCD tale che

$\angle ABP = \angle DBC$ e $\angle CDB = \angle PDA$

Ter: ABCD ciclico $\Leftrightarrow$ AP = CP

OSS: in $\triangle BPD$, A e C sono coniugati isogonali

1° = Freccia ciclico $\Rightarrow$ AP = CP



Ter $\Leftrightarrow$ P $\in$ one di AC

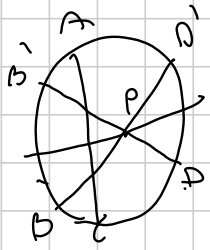
B', D' simmetrici di B, D rispetto all'one di AC

Voglio dimostrare BPD' allineati ($C \leftrightarrow A$)

$\angle ABP = \angle DBC = \angle AB'D' =$

$= \angle ABD'$ $\Rightarrow$ BPD' allineati

Analogamente B'PD allineati

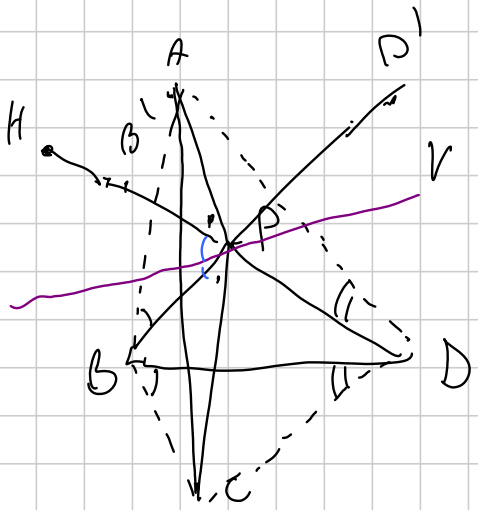


Basta la simmetria rispetto all'one di AC

$B \to B'$ $D \to D'$ $\Rightarrow$ $BD' \to B'D$

$P \to P'$ $\Rightarrow$ P $\in$ one di AC ✓

2° FRECCIA. AP = CP $\Rightarrow$ ciclico



Perché A, C sono coniugati in $\triangle BPD$

$\Downarrow$

$\angle APH \cong \angle BPC$

Considero la bisettrice esterna di $\angle BPD$

$\Rightarrow$ è bisettrice (interna) di APC

MA APC è isoscele $\Rightarrow$ bisettrice è anche altezza $\Rightarrow$ è $\perp AC \Rightarrow$ è il suo asse

$r \perp AC$

B', D' simmetrici di B, D rispetto a $r \Rightarrow B' \in PD$, $D' \in PB$

$\angle ABD' \cong \angle ABP \cong \angle DBC \cong \angle AB'D'$ (per la simmetria)

$AB'D$ è ciclico

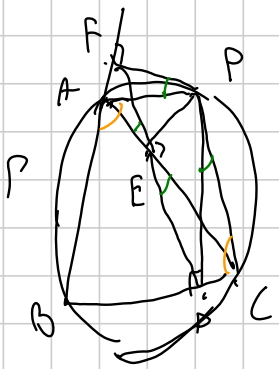
$\Rightarrow ABB'DD'$ ciclico

Analogamente $ADD'B$ è ciclico

Poiché la simmetria rispetto a $r \Rightarrow$ la circonferenza passa anche per $C \Rightarrow ABCD$ ciclico $\Rightarrow$ Tesi C.V.D.

— ○ — ○ —

Retta di Simson



$P \in \Gamma = O_{ABC}$

D, E, F proiezioni di P sui lati

Allora D, E, F sono allineati.

DIM. Noto che $\angle PDC = \angle PEC = 90° \Rightarrow PEDC$ è ciclico

$\angle PEA = \angle PFA = 90 \Rightarrow PAFE$ è ciclico

$\angle PDB = \angle PFB = 90° \Rightarrow PDBF$ è ciclico

Per la tesi mi basta $\triangle CED \overset{?}{=} \triangle AEF$

$\angle CED = \angle CPD = 180 - \triangle PDC - \triangle DCP = 90 - \triangle DCP = 90° - \triangle BCP =$

$= 90° - \triangle BAP = 90° - \triangle PAR = 90° - (180 - 90 - \triangle FPA) = \triangle FPA = \triangle FEA$

$\Rightarrow DEF$ non allineati C.V.D.

— o — o —

SIMSON 1,5

D, E, F t.c. $\triangle PDB = \triangle PEC = \triangle PFA$ con $D \in AB$ vecchio

$\Rightarrow$ D, E, F non allineati

Teoria dei Numeri

Note Title 9/3/2016

Livello ~~Brocat~~

RIEPILOGO

WILSON p PRIMO $\Rightarrow (p-1)! \equiv -1 \ (p)$

EULERO $(n,x)=1 \quad x^{\varphi(n)} \equiv 1 \ (n)$

$\text{ord}_n(x) \mid \varphi(n)$

LTE

SIA $p>2$ PRIMO E SIANO a,b INTERI TALI CHE

$(a,p)=1 \quad (b,p)=1$ E $p \mid a-b$

$$\nu_p(a^n - b^n) = \nu_p(a-b) + \nu_p(n)$$

$\nu_p(x)$ = "NUMERO DI FATTORI p CHE COMPAIONO IN x"

$$x = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \qquad \nu_{p_j}(x) = \alpha_j$$

$\nu_p(a^n - b^n)$

SUGGERIMENTO: PROVIAMO CON n PRIMO E POI CERCHIAMO DI GENERALIZZARE

i) $n = q$ primo $\neq p$

$$v_p(a^q - b^q) = v_p(a-b) + \underbrace{v_p(q)}_{\| \; 0 \; p \nmid q}$$

$v_p(a^q - b^q) = v_p(a-b)$ È VERO

SE $\dfrac{a^q - b^q}{a-b}$ NON È UN MULTIPLO DI p

$\underbrace{a^{q-1} + a^{q-2}b + \dots + ab^{q-2} + b^{q-1}}_{q \text{ TERMINI}}$

SONO TUTTI $\equiv$ MOD p

PERCHÉ $a \equiv b \pmod p$

$$a \equiv b \pmod p$$

$$a^{q-1} \equiv a^{q-2} \cdot a \equiv a^{q-2} \cdot b \pmod p$$

$$a^{q-i-1} \cdot b^i \equiv a^{q-1} \pmod p$$

$$a^{q-1} + \dots + b^{q-1} \equiv q \cdot a^{q-1} \pmod p$$

$$!!! \quad 0 \; !$$

$$a^{q-1} \not\equiv 0 \pmod p \Leftarrow p \nmid a$$

$$q \not\equiv 0 \pmod p \Leftarrow q \neq p$$

$$\frac{a^q - b^q}{a-b} \not\equiv 0 \pmod p \rightarrow v_p\left(\frac{a^q-b^q}{a-b}\right) = 0$$

$$v_p(a^q - b^q) = v_p(a-b) \qquad \square$$

ii) $n = p$

$$v_p(a^p - b^p) = v_p(a-b) + v_p(p) =$$
$$= v_p(a-b) + 1$$

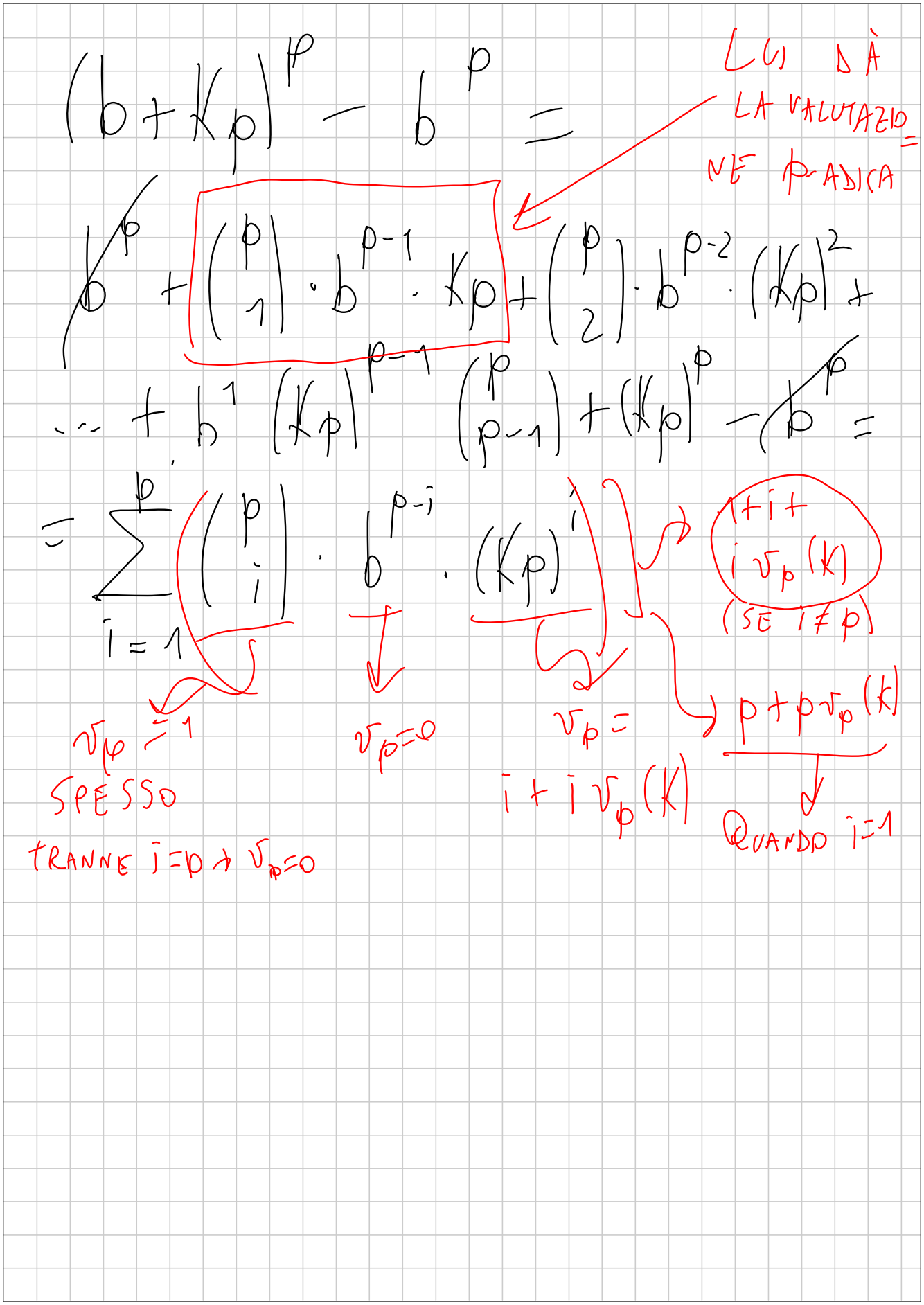
FARE IL RAPPORTO: VIENE MA È UN PO' LABORIOSO

Hp. $p \mid a-b$ $\Leftarrow$ $\boxed{a = b + kp}$ (SPESSO RITORNA)

$$v_p(a^p - b^p) = v_p(a-b) + 1$$

$$v_p((b+kp)^p - b^p) = v_p(kp) + 1$$

→ SVILUPPIAMO


$(b+kp)^p - b^p =$
LA 1 DÀ LA VALUTAZIONE p-ADICA
$b^p + \binom{p}{1} b^{p-1} \cdot kp + \binom{p}{2} b^{p-2} \cdot (kp)^2 +$
$\cdots + b^1 (kp)^{p-1} \binom{p}{p-1} + (kp)^p - b^p =$
$= \sum_{i=1}^{p} \binom{p}{i} \cdot b^{p-i} \cdot (kp)^i$
$1+i+i v_p(k)$ (SE $i \neq p$)
$p+p v_p(k)$
QUANDO $i=1$
$v_p = i + i v_p(k)$
$v_p = 1$ SPESSO
$v_p = 0$
TRANNE $i=0 \Rightarrow v_p=0$

$v_p(k)$ È MINIMO PER $i=1$.

(INOLTRE CON $i=1$ È MINORE DI $i=p$

$$2+v_p(k) < p+p v_p(k)$$

(RICORDIAMO: $p>2$) → SE $p=2$ È $v_2(k)=0$

$$2+v_p(k) = v_p\left((b+kp)^p - b^p\right)$$

$$\| \cdot v$$

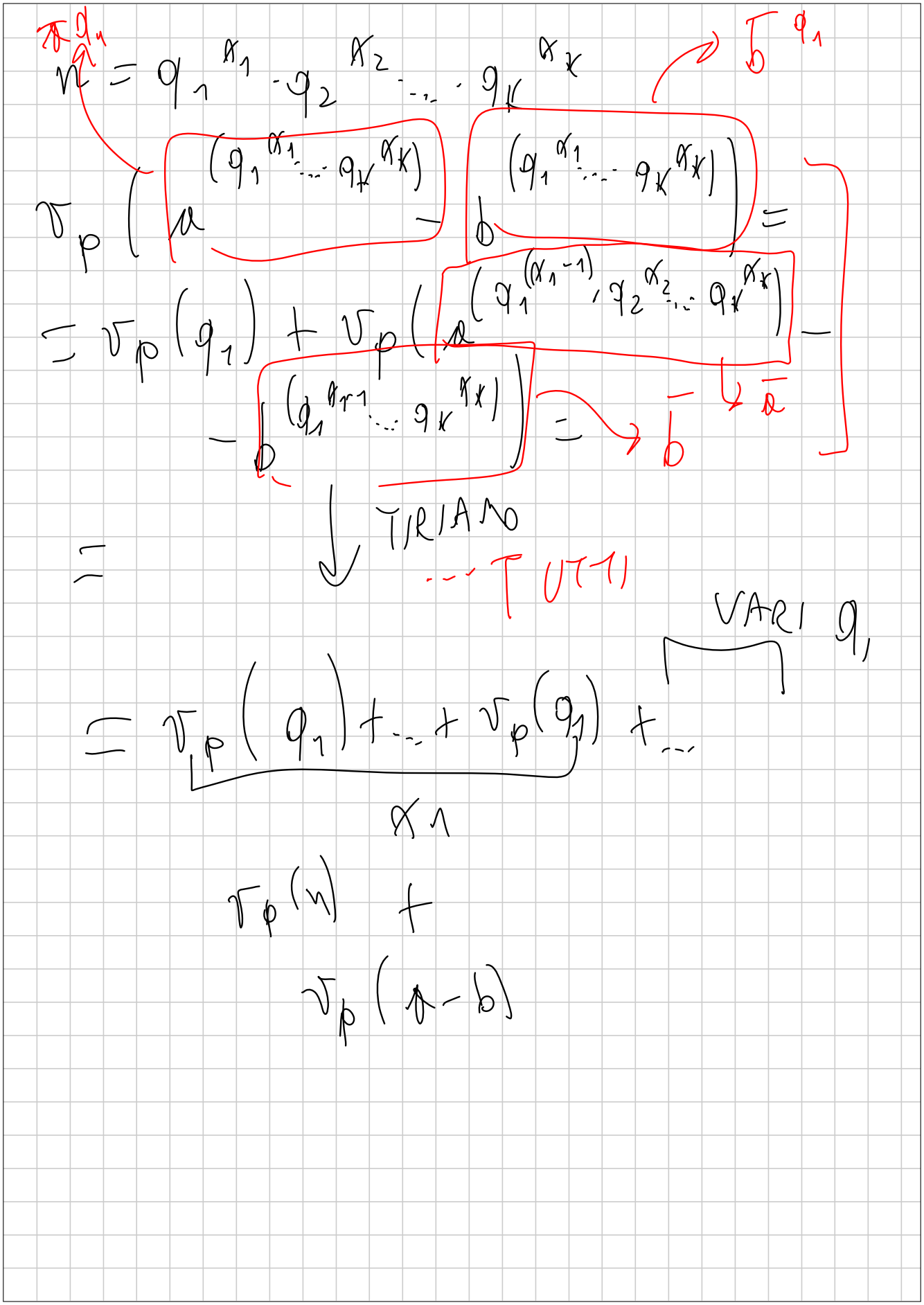
$$1+v_p(kp)$$

$$\| \qquad \| \qquad \|$$

$$1+\left(v_p(k)+v_p(p)\right)$$

$$v_p(a^n-b^n) = v_p(a-b)+v_p(n)$$

VALE PER n PRIMO


TIRIAMO
VARI q_1

LTE CON IL 2 (a,b) DISPARI

$$v_2(a^n - b^n) = v_2(a-b)$$

SE n È DISPARI

$$v_2(a^n - b^n) = v_2(a^2 - b^2) + v_2(n) - 1$$

SE n È PARI

(SI FA UGUALE)

ESERCIZIO (OLIFORUM) DIMOSTRARE CHE ESISTONO INFINITI INTERI POSITIVI n TALI CHE $n^2 \mid 3^n + 2^n$

LTE CON $a=3$ $b=-2$

L'UNICO PRIMO CHE POSSO PRENDERE È 5

LEMMA DEL GUADAGNO DI UN PRIMO

$(a,b)=1$

SIA $p \geq 2$ PRIMO. ALLORA SPESSO

$\frac{a^p - b^p}{a-b}$ HA UN DIVISORE PRIMO CHE NON HA $a-b$

SE $p=2$ È FALSO MOLTISSIME VOLTE

$a+b \quad (3,1) \to 4 \quad$ E 2

$a+b = 2^k \qquad a-b=2$

$(a,b)=1$ MA HANNO GLI STESSI FATTORI PRIMI

$p=3 \qquad a=2 \qquad b=-1$

$\frac{a^3-b^3}{a-b}=3 \qquad a-b=3$

LTE!

$a^p - b^p$ E $a-b$

SUPPONIAMO CHE NON ESISTA NESSUN PRIMO CHE DIVIDE a^p-b^p E NON $a-b$.

SIA q UN DIVISORE PRIMO DI $a-b$

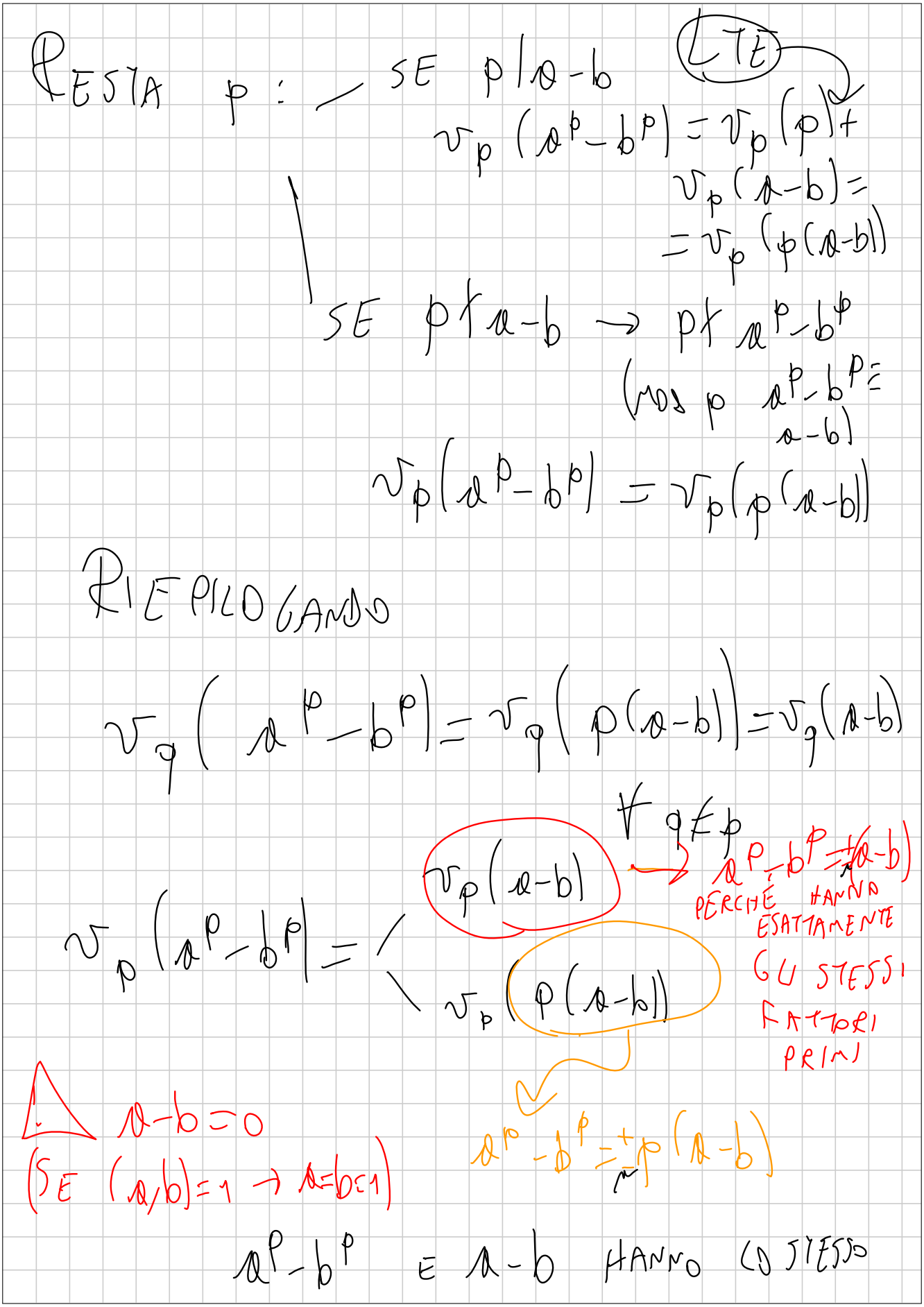
ALLORA $v_q(a^p-b^p) = v_q(a-b) + v_q(p) =$

$= v_q(p(a-b))$

VERO SE $q \nmid a-b$.

SE $q \mid a-b$ E $q \neq p$ $\quad v_q(a^p-b^p) =$

$q \mid a^p-b^p$ PER IPOTESI $\quad \not\downarrow \quad = v_q(p(a-b)) \neq 0$


TESTA p: — SE p | a-b
LTE
v_p(a^p - b^p) = v_p(p) + v_p(a-b) =
= v_p(p(a-b))
SE p ∤ a-b → p ∤ a^p - b^p
(mod p a^p - b^p ≡ a-b)
v_p(a^p - b^p) = v_p(p(a-b))
RIEPILOGANDO
v_q(a^p - b^p) = v_q(p(a-b)) = v_q(a-b)
∀ q ≠ p
v_p(a^p - b^p) = { v_p(a-b) v_p(p(a-b))
a^p - b^p ≠ p(a-b)
PERCHÉ HANNO ESATTAMENTE GLI STESSI FATTORI PRIMI
a^p - b^p = p(a-b)
a-b = 0
(SE (a,b) = 1 → a = b = 1)
a^p - b^p E a-b HANNO LO STESSO

SEGNO!

SE $a-b>0 \iff a>b \iff a^p>b^p \iff a^p-b^p>0$

$a^p - b^p$ / $p(a-b)$, $(a-b)$

$(1,0)$
$(1,-1)$
1
p

$$\boxed{a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \dots + b^{p-1}}$$

SE SONO TUTTI CONCORDI (OVVIO)

SE HANNO SEGNI OPPOSTI

$$a^{p-2}(a-b) + a^{p-4}b^2(a-b) + \dots + b^{p-3}(a-b) + b^{p-1}$$

ECCEZIONE CON p

$$a^{p-1} + a^{p-2}b + \dots + b^{p-1} = p$$

$a=2 \quad b=-1 \quad p=3$

$n^2 \mid 2^n + 3^n$

PASSIAMO DA UNA SOLUZIONE ALL'ALTRA ATTRAVERSO IL LEMMA DEL GUADAGNO DI UN PRIMO.

$n=1$ ✓ $\quad 1 \mid 2^1 + 3^1$ ($= 5$)

$n=5$ ✓ $\quad 25 \mid 2^5 + 3^5$

$275 = 5^2 \cdot 11$

$11^2 \mid 2^{11} + 3^{11}$ NO!

$11 \mid 2 + 3 \ (11)$

$55^2 \mid 2^{55} + 3^{55} = (2^5)^{11} + (3^5)^{11}$ ✓

$v_p(2^{55} + 3^{55}) = v_p(11) + v_p(2^5 + 3^5)$

$p = 5, 11$ $\qquad$ 11 $\qquad$ $5^2 \cdot 11$

SIA $a_0 = 1$, $a_1 = 5$ E DEFINIAMO

$a_{n+1} = p \cdot a_n$, DOVE p È UN PRIMO CHE DIVIDE $3^{a_n} + 2^{a_n}$ MA NON $3^{a_{n-1}} + 2^{a_{n-1}}$. TALE PRIMO ESISTE PER IL LEMMA DI GAUSS PERCHÉ

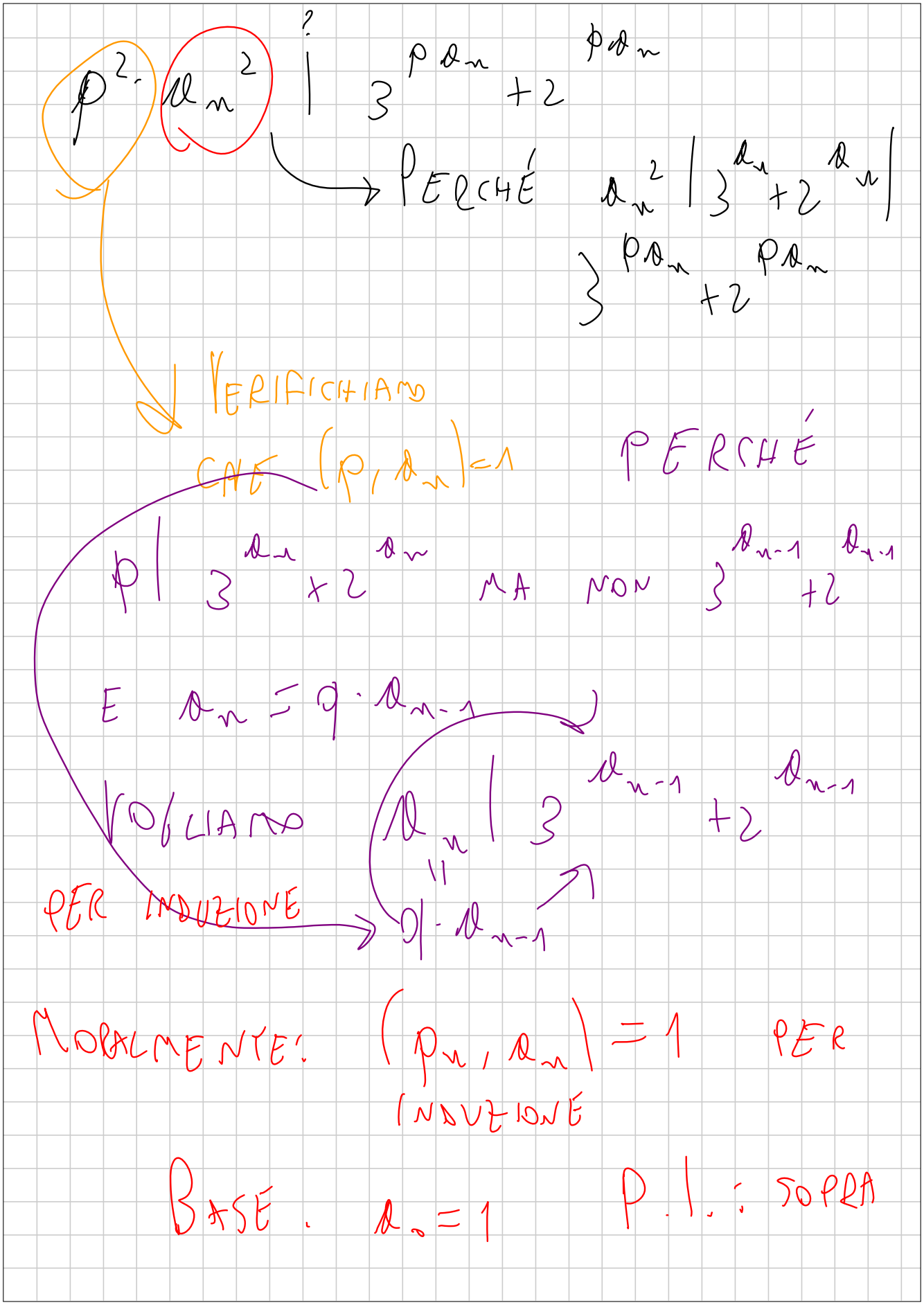
$a_n = a_{n-1} \cdot q$, CON q PRIMO

VERIFICHIAMO PER INDUZIONE CHE 6 LI FUNZIONANO

$a_0 = 1$ ✓ $\quad 1^2 \mid 5$

$a_{n+1} = p \cdot a_n$

$a_{n+1}^2 \mid 3^{a_{n+1}} + 2^{a_{n+1}}$?


PERCHÉ
VERIFICHIAMO
CHE
PERCHÉ
MA NON
E
VOGLIAMO
PER INDUZIONE
NORMALMENTE:
PER
INDUZIONE
BASE:
P.I.: SOPRA

(1 MANCA $p^2 \mid 3^{a_{n+1}} + 2^{a_{n+1}} =$

$= \} \quad + 2^{p a_n} \quad p a_n$

$v_p\left(3^{p a_n} + 2^{p a_n}\right) = v_p(p) + v_p\left(3^{a_n} + 2^{a_n}\right)$

$\geq 1 \qquad\qquad \geq 1$

$\mathbb{F}_p$: $\longrightarrow$ PER QUANTI INTERI IN $\{0, 1, \dots, (p-1)\}$ PUÒ ANNULLARSI?

UN POLINOMIO MOD p QUANTE RADICI PUÒ AVERE MODULO p?

~~X~~ $+1$ IN CHE VALORI SI ANNULLA

SOLO IN -1,

$X + 1 \equiv 0 \ (p) \iff X \equiv -1 \ (p)$

$$x^2+1 \equiv 0 \pmod{p}$$

TRE TIPI
- 0: $x^2+1 \equiv 0 \pmod 3$
- 1: $x^2+1 \equiv 0 \pmod 2$
- 2: $x^2+1 \equiv 0 \pmod 5$

FATTO: SE $f(x)$ È UN POLINOMIO MONICO DI GRADO k HA AL PIÙ k RADICI MODULO p.

MOD 15: $x(x-1)(x-2)$

HA COME RADICI.

0, 1, 2, 5, 6, 7, 10, 11, 12

PERCHÉ È VERO IL FATTO?

IN $\mathbb{Z}$ I POLINOMI HANNO AL PIÙ k RADICI.

$a \cdot b = 0 \rightarrow a = 0 \vee b = 0$

$a \cdot b \equiv 0 \pmod{p} \rightarrow a \equiv 0 \pmod{p} \vee b \equiv 0 \pmod{p}$

$3 \cdot 5 \equiv 0 \pmod{15} \not\rightarrow 3 \equiv 0 \pmod{15} \vee 5 \equiv 0 \pmod{15}$

SIA $f(x)$ UN POLINOMIO MONICO DI GRADO k E SUPPONIAMO CHE ABBIA $k+1$ RADICI.

PER INDUZIONE, SE $g(x)$ HA

GRADO $k-1$, HA AL PIÙ $k-1$ RADICI.

PASSO BASE: GRADO 0

1 NON HA RADICI MOD p.

PASSO INDUTTIVO.

$f(x)$ HA $\alpha_1, \dots, \alpha_{k-1}$ COME RADICI.

VORREMMO SCRIVERE $f(x) =$

$g(x) \cdot (x - \alpha_1)$

$f(x) = x^2 + 1 \qquad \alpha_1 = 2 \qquad p = 5$

$x^2 + 1 = (x-2) \cdot g(x)$

$(x+2) =$

$x^2 - 4 \qquad (5)$

Polinomi modulo p

I coefficienti dei polinomi sono guardati modulo p.

Modulo 5: $x^6 - 3x^2 + 17x \equiv$

$\equiv x^6 + 2x^2 + 2x \pmod 5$

α è radice di f se $f(\alpha) \equiv 0 \pmod p$

Def. finale: $\alpha(x)$ e $\beta(x)$ sono uguali modulo p se i coefficienti sono uguali modulo p.

Oss. $x^5 \equiv x \pmod 5$ il pol.

$x^5 - 1 \overset{?}{\equiv} x - 1 \pmod 5$

$x^5 - 1 \equiv (x-1)^5 \pmod 5 \rightarrow$ 5 RADICI

$x - 1 \pmod 5 \rightarrow$ 1 SOLA RADICE

$x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 1$

$f(x)$ E VORREMMO $f(x) = (x - \alpha_1) \cdot g(x) \pmod p$

$f(\alpha_1) \equiv 0 \pmod p$ PER IPOTESI

IL POLINOMIO $f(x) - 0 \pmod p$ HA UNA (NO) RADICE INTERA, IN $\mathbb{R}$.

PER RUFFINI $\boxed{f(x) - 0 \equiv (x - \alpha_1) \cdot g(x) \pmod p}$ (g di grado $x-1$)

VALE ANCHE MODULO p

$f(x) \equiv (x - \alpha_1) \cdot g(x) \pmod p$

α_1
$\alpha_2, \dots, \alpha_{k+1}$ → distinti mod p

$f(\alpha_2) \equiv 0 \not\equiv 0$

$\equiv (\alpha_2 - \alpha_1) \cdot g(\alpha_2) \pmod p$

$\not\equiv 0 \pmod p$

Allora $g(x)$ ha k radici.

↳ ha grado $k-1$

Qualunque polinomio mod p in cui il termine di testa non sia considerato nullo

$0 \cdot x \not\equiv 0 \pmod p$

GRADO DI UN POLINOMIO MOD p:

IL GRADO DEL MONOMIO NON NULLO MOD p MAGGIORE

$$3x^2 + 2 \equiv 0 \pmod 5$$

$$\updownarrow \text{ HA LE STESSE}$$

$$2(3x^2 + 2) \equiv 2 \cdot 0 \pmod 5$$

$$x^2 + 4 \equiv 0 \pmod 5$$

PRENDIAMO TUTTI I POLINOMI MODULO p DI GRADO MINORE DI p.

QUELLI DI GRADO k SONO:

$(p-1) \cdot p^k$

$$\underbrace{A_k}_{p-1} x^k + \dots + \underbrace{A_0}_{p \text{ MOD L'UNO}}$$

IN TOTALE $\sum_{i=0}^{p-1} (p-1)\cdot p^i = p^p - 1$

METTIAMOCI PURE LO 0 : p^p

PRENDIAMO $f(X)$ E $g(X)$ TRA QUESTI.
POSSONO COINCIDERE MODULO p
PER OGNI X INTERO?

SE $\underbrace{f(X) - g(X)}_{h(X)} \equiv 0 \pmod p \quad \forall X$

$h(X)$ HA p RADICI MODULO p.

↳ HA GRADO $< p$ E NON È 0 SE $f \neq g$

$h(X)$ HA p RADICI: $h(X) \equiv X \cdot h_1(X) \equiv$

$$x(x-1)\cdot h_2(x) \equiv x(x-1)(x-2)\cdot h_3(x) + \dots$$

TRA I p^p POLINOMI NON CE NE SONO DUE CHE COINCIDONO IN OGNI INTERO MODULO p.

HO UNA FUNZIONE f DA $\{0,\dots,p-1\} \to \{0,\dots,p-1\}$ SONO p^p.

DATO CHE DUE POLINOMI DIVERSI SONO DUE FUNZIONI DIVERSE, ALLORA OGNI FUNZIONE È RAPPRESENTATA DA UN POLINOMIO, POICHÉ SONO NELLO STESSO NUMERO (FINITO).

$$f: \{0,\dots,p-1\} \to \{0,\dots,p-1\}$$

$$f(x) \equiv \sum_{i=0}^{p-1} \left(\left(1-(x-i)^{p-1}\right) \cdot f(i) \right)$$

SE $x \equiv i$ $\quad 1 - (x-i)^{p-1} \equiv 1$

$x \not\equiv i$ $\quad 1 - (x-i)^{p-1} \equiv 0$

$\hookrightarrow 1$

$x^{p-1} - 1 \equiv (x-1)\dots(x-(p-1)) \pmod p$

HA $p-1$ RADICI

SONO DUE POLINOMI MONICI DI GRADO $p-1$ CON ESATTAMENTE LE STESSE $p-1$ RADICI

VALUTO IN 0: $-1 \equiv (-1)\cdot(-2)\cdot\dots\cdot(-(p-1)) \pmod p$

(T.N. UGUALI) $\quad (-1)^{p-1}\cdot(p-1)! \pmod p$

RADICI DI $x^k - 1$ MODULO p

1 SEMPRE

$x^{\frac{p-1}{2}} - 1$. AL MASSIMO $\frac{p-1}{2}$

SE $x = a^2 \pmod p \Rightarrow x^{\frac{p-1}{2}} \equiv a^{2\cdot\frac{p-1}{2}} \equiv 1 \pmod p$

↳ sono $\frac{p-1}{2}$

ESCURSUS SUI RESIDUI QUADRATICI

(CHIAMIAMO x R.Q. SE $\exists\, a$ T.C. $a^2 \equiv x \pmod p$

I RESIDUI QUADRATICI $\neq 0$ SONO $\frac{p-1}{2}$.

PERCHÉ $\left\{1, \dots, \frac{p-1}{2}\right\}$

SE $x^2 \equiv y^2 \pmod p \Rightarrow (x-y)(x+y) \equiv 0 \pmod p$

$\equiv 0$ $\quad$ $0 < x < p$

QUINDI

$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ SONO DISTINTI MODULO p

VICEVERSA $a^2 \equiv (-a)^2 \pmod p$

$\parallel$

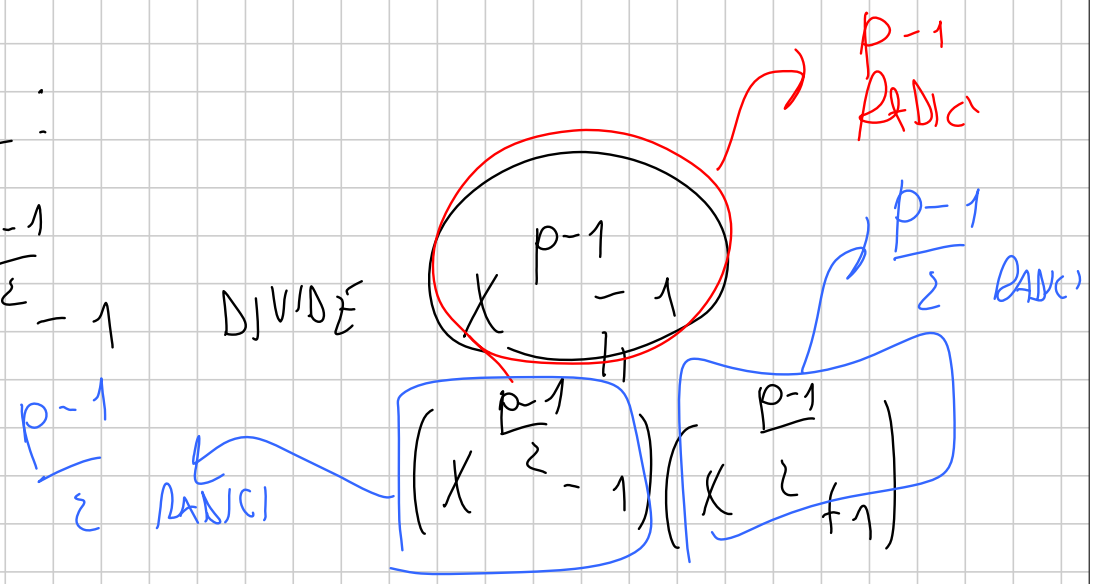
a^2

$X^{\frac{p-1}{2}} - 1$ HA AL MASSIMO $\frac{p-1}{2}$ RADICI E I R.Q. SONO SUE RADICI.

Modo 1: CI SONO $\frac{p-1}{2}$ R.Q. V

Modo 2:

$X^{\frac{p-1}{2}} - 1$ DIVIDE $X^{p-1} - 1$



CRITERIO DI EULERO:

a R.Q. $\Leftrightarrow$ $a^{\frac{p-1}{2}} \equiv 1 \pmod p$

a N.Q. $\Leftrightarrow$ $a^{\frac{p-1}{2}} \equiv -1 \pmod p$

AD ESEMPIO: QUANDO -1 È R.Q.

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p \iff p \equiv 1 \pmod 4$$

$$\left(\frac{p-1}{2}\right)! \equiv \underbrace{\left(\frac{p+1}{2}\right)\cdot\ldots\cdot(p-1)}_{\left(\frac{p-1}{2}\right)!\cdot(-1)^{\frac{p-1}{2}}} \pmod p$$

$1 \equiv -(p-1)$
$2 \equiv -(p-2)$
$\ldots \equiv -$
$\left(\frac{p-1}{2}\right) \equiv -\left(\frac{p+1}{2}\right)$

SE $p \equiv 1 \pmod 4$ I — SONO PARI

PROD. DI TUTTI $(p-1)! \equiv -1 \pmod p$

$$\left(\left(\frac{p-1}{2}\right)!\right)^2$$

$p = 13$

$\{1, 2, 3, 4, 5, 6\}$

$(13-1) \equiv (-1)\cdot 1$
$(13-2) \equiv (-1)\cdot 2$
$(13-3) \equiv (-1)\cdot 3$
$\ldots$
$(13-6) \equiv (-1)\cdot 6$

$\{7, 8, 9, 10, 11, 12\}$

$\cdot (-1)^6 = 1$

ESERCIZIO

- VEDIAMO (PER QUALI) QUANDO $(x^2+1)^{\frac{p-1}{2}} \equiv 1 \ (p)$

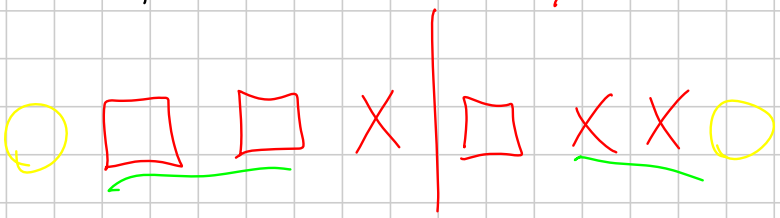
  x^2+1 È R.Q.

- È QUANDO 2 È R.Q. MODULO p

SE $p \equiv 3 \ (4)$

□ R.Q.

X N.Q.



SIMMETRIA INVERSA

$p \equiv 1 \ (4)$

SIMMETRIA GIUSTA

VOGLIAMO CONTARE QUANDO

$\sum_{\#\square (\square-1)}$ [□ + 1 = □] SE $p \equiv 3(4)$ SONO UGUALI

[X + 1 = X]

$\sum_{\#\triangle (\triangle-1)}$ [□ + 1 = X] SE $p \equiv 1(4)$ SONO UGUALI

[X + 1 = □]

QUANTI SONO $\square + 1 = \square$

$x^2 + 1 \equiv y^2 \pmod p$ È (CIRCA) 4 VOLTE

SUPPONIAMO $x, y \neq 0$ (SE $x=0$ O $y=0$)

$(x-y)(x+y) \equiv -1 \pmod p$

a b $ab \equiv -1 \pmod p$

$\frac{a+b}{2} \equiv x \pmod p$

$\frac{b-a}{2} \equiv y \pmod p$

$a \not\equiv b \pmod p$

$a \not\equiv -b \pmod p$

$a^2 \equiv -1 \pmod p$ $a^2 \equiv 1 \pmod p$

TOGLIAMO

$a \equiv i \pmod p$ $b \equiv i \pmod p$

$a \equiv -i \pmod p$ $b \equiv -i \pmod p$

$a \equiv 1 \pmod p$ $b \equiv -1 \pmod p$

$a \equiv -1 \pmod p$ $b \equiv 1 \pmod p$

$ab \equiv -1 \pmod p$

$ab \equiv -1 \pmod p$ SONO $p-1$:

$a \equiv -\frac{1}{b} \pmod p$ PER OGNI $b \neq 0$ C'È ESATTAMENTE UNA SOLUZIONE.

SOLUZIONI: $p-1$

SE $p \equiv 1 (4)$ $\rightarrow \frac{p-5}{4}$ BUONE

$p \equiv 3 (4)$ $\rightarrow \frac{p-3}{4}$ BUONE

$p \equiv 3 (4)$

$\square + 1 = \square$ $\frac{p-3}{4}$

$\triangle + 1 = \triangle$ $\frac{p-3}{4}$

$\square + 1 = \triangle$ $\frac{p+1}{4}$

$\triangle + 1 = \square$ $\frac{p-3}{4}$

$p \equiv 1 (4)$

$\square + 1 = \square$ $\frac{p-5}{4}$

$\triangle + 1 = \triangle$ $\frac{p-1}{4}$

$\square + 1 = \triangle$ $\frac{p-1}{4}$

$\triangle + 1 = \square$ $\frac{p-1}{4}$

2 è R.Q. $\iff$ $\left(\frac{p+1}{2}\right)$ è R.Q.

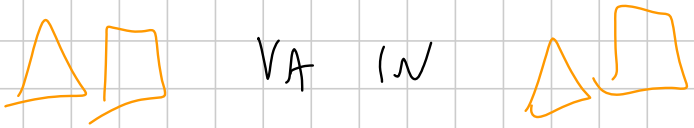
$2^{\frac{p-1}{2}} \equiv 1 \ (p) \iff \left(\frac{p+1}{2}\right)^{\frac{p-1}{2}} \equiv 1 \ (p)$

SE $\left(\frac{p+1}{2}\right)^{\frac{p-1}{2}} \equiv -1 \ (p)$

$-1 \equiv 2^{\frac{p-1}{2}} \cdot \left(\frac{p+1}{2}\right)^{\frac{p-1}{2}} \equiv 1^{\frac{p-1}{2}} \ (p)$

?

IN $p \equiv 3 \ (4)$



VA IN

$\left(\frac{p-1}{2}, \frac{p+1}{2}\right)$ È L'UNICA COPPIA FISSA:

È DEL TIPO DISPARI

ANALOGO PER $p \equiv 1 \pmod 4$.

IN GENERALE

2 R.Q. $p \leftrightarrow p \equiv \pm 1 \pmod 8$

GENERATORI

IDENTITÀ

$$\sum_{d \mid n} \varphi(d) = n$$

$\frac{1}{15}$ $\frac{2}{15}$ $\frac{3}{15}$ $\frac{4}{15}$ $\frac{5}{15}$ $\frac{6}{15}$ $\frac{7}{15}$ $\frac{8}{15}$ $\frac{9}{15}$ $\frac{10}{15}$ $\frac{11}{15}$

$\frac{12}{15}$ $\frac{13}{15}$ $\frac{14}{15}$ $\frac{15}{15}$

LE FRAZIONI SONO n:

QUELLE CON DENOMINATORE

15: 8

5: 4

3: 2

1: 1

d SONO $\phi(d)$, OVVERO TUTTE QUELLE DEL TIPO $\frac{a}{d}$ CON $a<d$ E $(a,d)=1$

– DELLE n FRAZIONI RESTANO FRAZIONI DEL TIPO $\frac{a}{d}$, CON $d \mid n$ E NE RESTANO $\varphi(d)$ ESATTAMENTE.

POLINOMI IN $\mathbb{Z}[x]$:

POLINOMI A COEFFICIENTI INTERI.

UN POLINOMIO MONICO $f(x)$ SI DICE IRRIDUCIBILE SE NON ESISTONO POLINOMI NON COSTANTI TALI CHE $f(x)=p(x)\cdot q(x)$

– OGNI POLINOMIO MONICO A COEFFICIENTI INTERI È PRODOTTO DI IRRIDUCIBILI:

$$f(x)=f_1(x)\cdot f_2(x)=f_1(x)\cdot f_2(x)\cdot f_3(x)=\dots$$

NON POSSO ANDARE AVANTI ALL'INFINITO

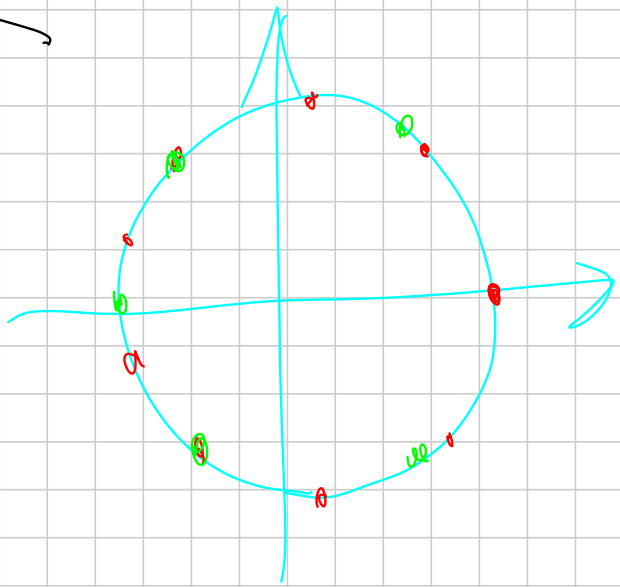
$X^n - 1 \mid X^m - 1$

$\rightarrow$ SE $n \mid m$ ALLORA

$m = kn$

$X^m - 1 = X^{kn} - 1 = (X^n - 1)(X^{n(k-1)} + \dots + 1)$

$\swarrow$



g b

SE $n \nmid m$,

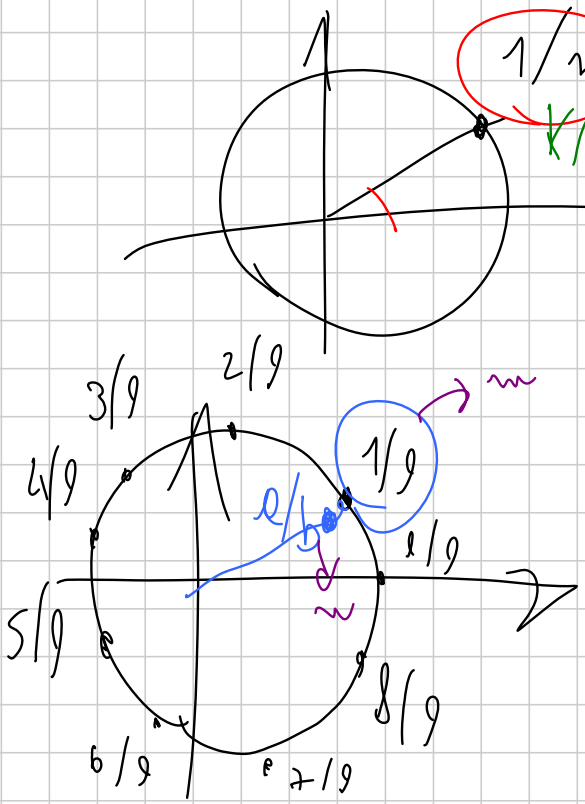
$\exists\, d$ t.c.

$\frac{d}{m}$ · n NON

È INTERO

$d = 1$

SE $n \nmid m \rightarrow$ LA RADICE n-ESIMA PRIMITIVA "PIÙ VICINA" A 1 NON È RADICE DI $X^n - 1$



$$\left(X^m - 1,\ X^n - 1\right) = X^{(m,n)} - 1$$

PER INDUZIONE SU $|m \cdot n|$

SE $m > n$

$$\left(X^m - 1,\ X^n - 1\right) = \left(X^m - 1 - X^{m-n}\left(X^n - 1\right),\ X^n - 1\right) =$$

$$= \left(X^{m-n} - 1,\ X^n - 1\right) = X^{(m-n,n)} - 1 =$$

$$= X^{(m,n)} - 1$$

$$x^m - 1 = f_1(x) \cdot f_2(x) \cdot \ldots \cdot f_k(x)$$

OGNI $x^n - 1$ CONTIENE UN POLINOMIO CHE LO DIVIDE NUOVO.

$\Phi(1)$

1: $\Phi(1)$ $x-1$ $\Phi(2)$ $\varphi(1)$

2: $(x-1)(x+1)$ $\Phi(2)$ $\varphi(2)$

3: $(x-1)(x^2+x+1)$ $\Phi(3)$ $\varphi(3)$

4: $(x-1)(x+1)(x^2+1)$ $\Phi(4)$ $\varphi(4)$

5: $(x-1)(x^4+x^3+x^2+x+1)$ $\Phi(5)$ $\varphi(5)$

6: $(x-1)(x+1)(x^2+x+1)(x^2-x+1)$ $\Phi(6)$ $\varphi(6)$

IN $x^n - 1$ CI SONO GLI IRRIDUCIBILI DEI DIVISORI d DEL $x^d - 1$

SE $\Phi(k)$ STA IN $x^n - 1$ E $k \nmid n$ ALLORA APPARE PURE IN $x^{(n,k)} - 1$: ASSURD! $(n,k) < k$

PER INDUZIONE:

SUPPONIAMO $\deg\left|\Phi(k)\right| = \phi(k) \quad \forall k \le n-1$

$\Phi(n)$

$$x^n - 1 = \Phi(n) \cdot \left(\prod_{d \mid n,\, d<n} \Phi(d) \right)$$

NIENTE: OGNI POLINOMIO O È NUOVO, O STA IN $\Phi(d)$

OPPURE STA IN $\Phi(k)$ CON $k<n$:

ASSURDO

QUINDI $\deg(x^n-1) = n$

$$= \deg\left|\Phi(n)\right| + \deg\left|\prod_{d \mid n,\, d<n} \Phi(d)\right| =$$

$$= \deg\left|\Phi(n)\right| + \sum_{d \mid n,\, d<n} \varphi(d)$$

$$n - \varphi(n)$$

$$\Phi_n(X) = \prod_{(d,n)=1,\ d<n} \left(X - \omega^d\right)$$

con ω radice primitiva n-esima

Prendiamo $x^{p-1} - 1 \equiv 0 \ (p)$

Ha p radici.

$\Phi_n(X) \equiv 0 \ (p)$

$\deg \Phi_n = \varphi(p-1)$ $\quad \Rightarrow$ Ha $\varphi(p-1)$ radici ≥ 1

Def. di $\Phi_n(X)$: prodotto degli irriducibili che dividono $x^n - 1$ ma non $x^m - 1$ $\forall m < n$

Sia y una sua radice.

$\Rightarrow \operatorname{ord}_p(y) = d \mid p-1$

y è radice di $X^d - 1$

SE $d < p-1$, $\Phi_{p-1}(X) \cdot (X^d - 1)$ DIVIDE $X^{p-1} - 1$

↳ PRODOTTO DI ALTRI CICLOTOMICI

↝

ASSURDO! $X^{p-1} - 1$ NON HA RADICI DOPPIE.

DUNQUE $\mathrm{ord}_p(g) = p-1$

$$\sum_{i=1}^{p-1} i^K \equiv \begin{cases} 0 & \text{SE } p-1 \nmid K \\ -1 & \text{SE } p-1 \mid K \end{cases}$$

$$\{1, \dots, p-1\} \longleftrightarrow \{g, 2g, \dots, g(p-1)\}$$

PERMUTAZIONE MODULO p

$$\sum_{i=1}^{p-1} i^K \equiv \sum_{j=1}^{p-1} (gj)^K \equiv g^K \sum_{i=1}^{p-1} i^K \pmod p$$

$$0 \equiv (\underbrace{g^K - 1}_{\neq 0}) \cdot \sum_{i=1}^{p-1} i^K \pmod p \quad \to \equiv 0$$

SE $p-1 \nmid k \to y^k \not\equiv 1 \pmod p$ PERCHÉ $\mathrm{ord}_p(y) = p-1$

SE $p-1 \mid k \to i^k \equiv 1 \pmod p \to \sum_{i=1}^{p-1} 1 \equiv p-1 \pmod p$

CONTIAMO PER QUANTI (x, y)

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

x^2+1 È $\square \iff (x^2+1)^{\frac{p-1}{2}} \equiv 1 \pmod p$

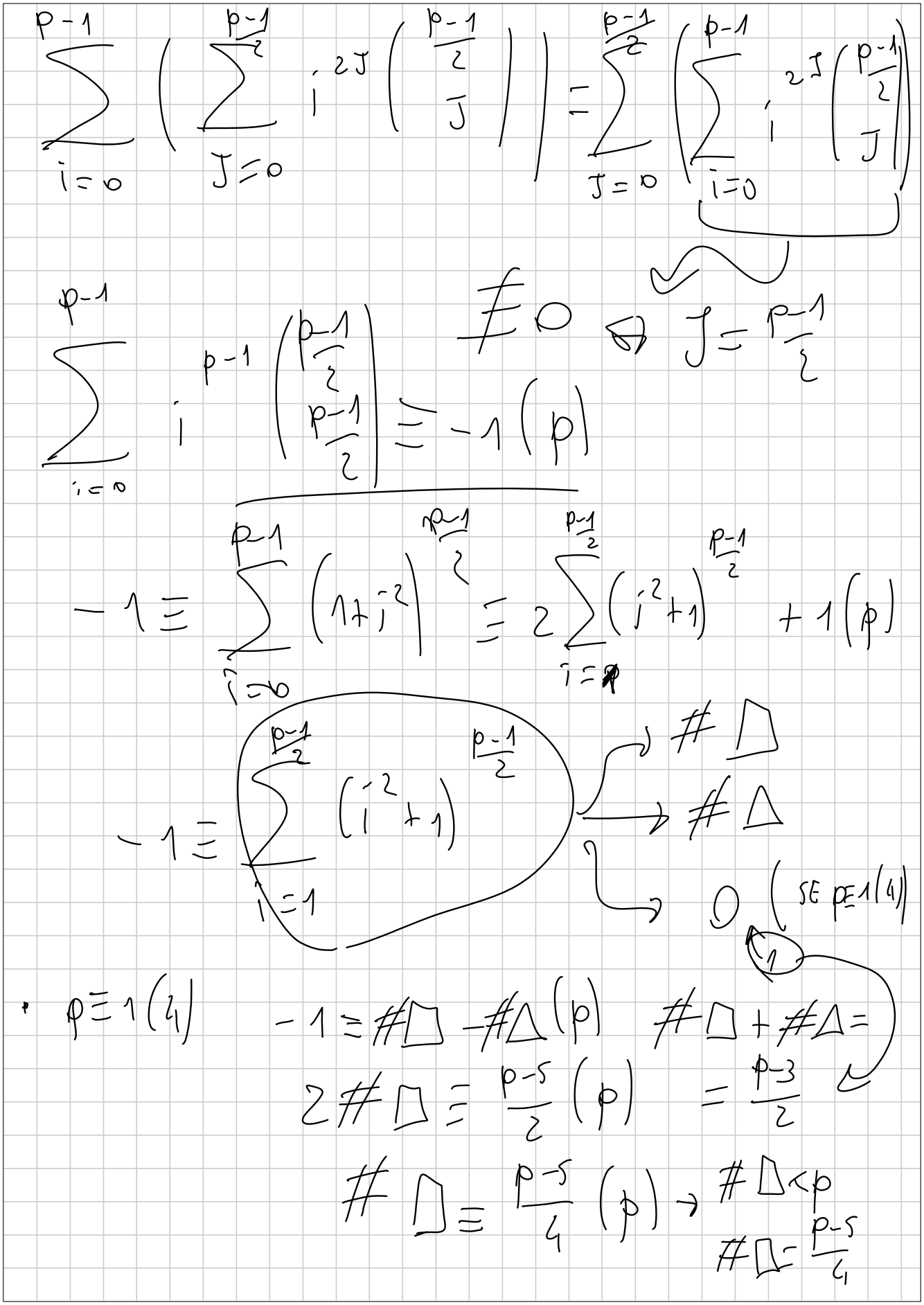
x^2+1 È $\triangle \iff (x^2+1)^{\frac{p-1}{2}} \equiv -1 \pmod p$

$x^2+1 \equiv 0 \pmod p \iff (x^2+1)^{\frac{p-1}{2}} \equiv 0 \pmod p$

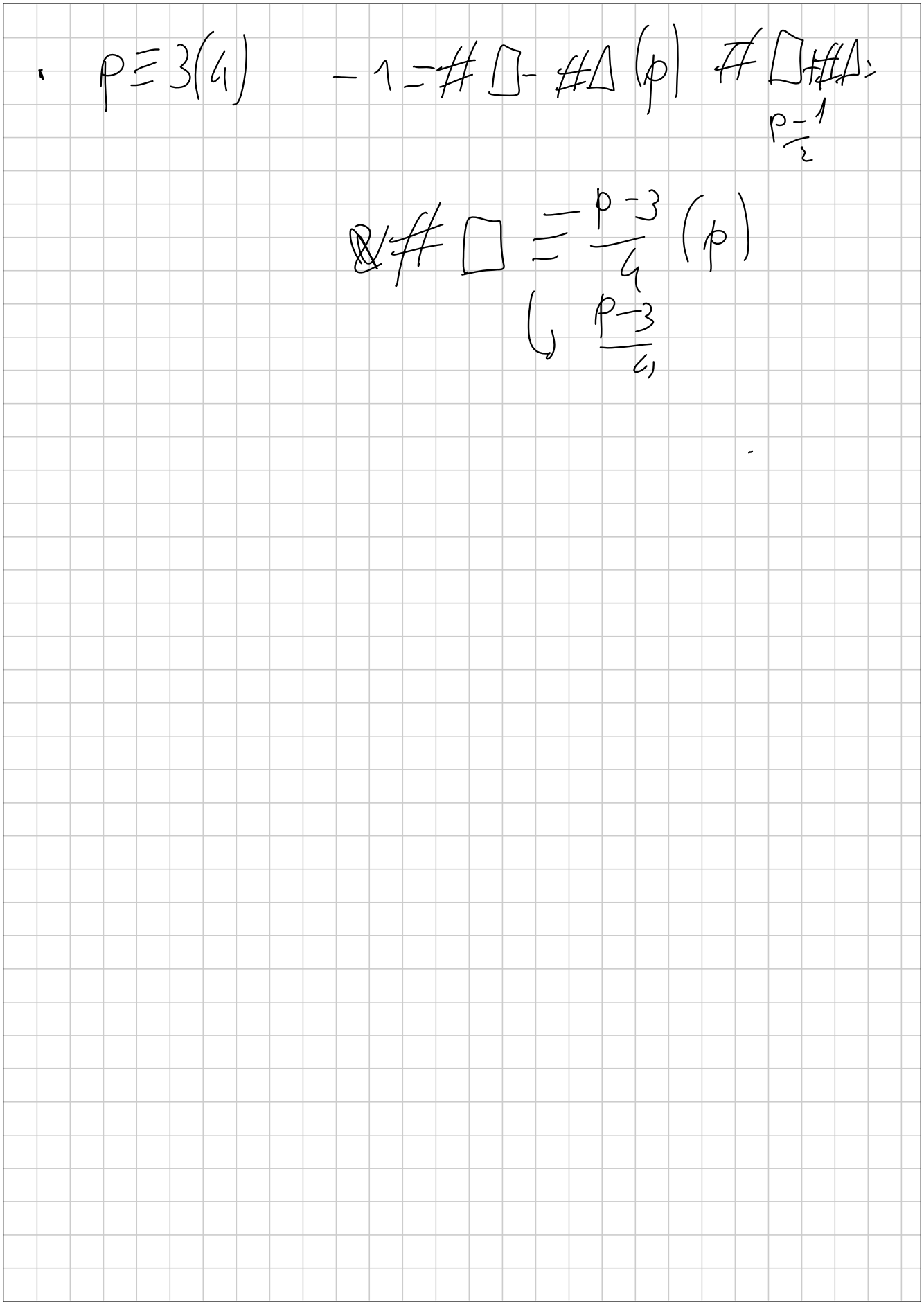
$\sum_{i=0}^{\frac{p-1}{2}} (i^2+1)^{\frac{p-1}{2}} \to \#\square - \#\triangle$

$\to$ MEGLIO DI $p-1$

$\sum_{i=0}^{p-1} (i^2+1)^{\frac{p-1}{2}} = 2 \sum_{i=1}^{\frac{p-1}{2}} (i^2+1)^{\frac{p-1}{2}} + 1$



Teoria dei Numeri 1 (Medium) – Francesco Ballini



Teoria dei Numeri

Note Title 9/5/2016

Medium 2

Trolleito brOOtal

$\mathbb{Z}[i]$ ← INTERI DI GAUSS

$a+ib$ CON $a,b \in \mathbb{Z}$ $(i^2=-1)$

$+, \cdot$ EREDITATI DA $\mathbb{C}$

$$(a+ib)+(c+id)=(a+c)+i(b+d)$$

$$(a+ib)\cdot(c+id)=(ac-bd)+i(bc+ad)$$

$(ib)\cdot(id)=-bd$

$\mathbb{Z}[i]$ AMMETTE UNA STRUTTURA LEGATA AI PRIMI (MOLTIPLICATIVA) MOLTO SIMILE A QUELLA DI $\mathbb{Z}$.

$\mathbb{Z}$: FATTORIZZAZIONE UNICA A MENO DEL $\pm$

$\mathbb{Z}[i]$: FATTORIZZAZIONE UNICA A MENO DI $\pm 1, \pm i$

EL. INVERTIBILI: POSSO SCRIVERE $1 = ab$ CON

$a \in \{1, -1, i, -i\}$

$1 \cdot 1 = 1 \quad (-1)\cdot(-1) = 1 \quad i \cdot (-i) = 1$

$(-i)\cdot i = 1$

QUALI SONO I PRIMI DI $\mathbb{Z}[i]$?

$N(a+ib) = a^2+b^2 \in \mathbb{N}$

$N((a+ib)(c+id)) =$

$N((ac-bd)+i(ad+bc)) =$

$= (ac-bd)^2 + (ad+bc)^2 =$

$= a^2c^2 + b^2d^2 - 2abcd +$

$+ a^2d^2 + b^2c^2 + 2abcd =$

$= (a^2+b^2)(c^2+d^2) =$

$= N(a+ib) \cdot N(c+id)$

LA NORMA N È MOLTIPLICATIVA.

Th. (che non dimostriamo)

In $\mathbb{Z}[i]$ esistono dei numeri primi e ogni elemento di $\mathbb{Z}[i]$ si scrive in modo unico (a meno di $1, -1, i, -i$) come prodotto di tali primi.

Quali interi possono essere primi in $\mathbb{Z}[i]$?

Quelli composti no! Perché si possono scomporre anche in $\mathbb{Z}[i]$.

(i restanti i primi.

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

↳ NON È PRIMO

$3 = (a+ib)(c+id)$

IDEA FURBA: NORMA!

$N(3) = N(a+ib) \cdot N(c+id)$

$9 = (a^2+b^2)(c^2+d^2)$

1 0 3 0

FATTO DA EVITARE: $a+ib$ PUÒ ESSERE UN INVERTIBILE

NON VANNO BENE $(1,0)$ $(0,1)$ $(-1,0)$ $(0,-1)$

a^2+b^2 $\begin{cases} 1 \\ 3 \\ 9 \end{cases}$ NO: SAREBBE INVERTIBILE

VORREMMO CHE FOSSE 3

NO: $c^2+d^2=4$

$0,1$ $0,1$

$a^2+b^2=3$ NON HA SOLUZIONE

MODULO 4.

3 È UN PRIMO IN $\mathbb{Z}[i]$

SE $p\equiv 3(4)$ COSA SUCCEDE?

$p=(a+ib)(c+id)$

$\downarrow$ NORMA

$p^2=(a^2+b^2)(c^2+d^2)$

a^2+b^2 $\begin{cases} 1 & \text{NO} \\ p & \text{NO } (\text{mod } 4) \\ p^2 & \text{NO} \end{cases}$

QUINDI $p\equiv 3(4)$ È PRIMO IN $\mathbb{Z}[i]$

SE $p \equiv 1 (4)$

SE $p = a^2 + b^2$ ALLORA

$p = (a+ib)(a-ib) = a^2 + b^2 + \cancel{ab}$

LEMMA OGNI $p \equiv 1 (4)$ SI SCRIVE COME SOMMA DI DUE QUADRATI.

SE $p \equiv 1 (4)$ $\exists\, k \in \mathbb{Z}$ TALE CHE $k^2 \equiv -1 (p)$.

CONSIDERIAMO I NUMERI DELLA FORMA $a + bk$ CON $0 \le a, b \le \lfloor \sqrt{p} \rfloor$ E $(a,b) \neq (0,0)$

QUANTE SONO? $(\lfloor \sqrt{p} \rfloor + 1)^2 - 1$

(N LO POSSO PRENDERE IN $1 + \lfloor \sqrt{p} \rfloor$ MODI)

↳ (0,0)

↳ IDEM

SAPÀ CIRCA p. ANZI, ALMENO p

$$(\lfloor \sqrt{p} \rfloor + 1)^2 - 1 \overset{?}{\geq} p$$

$$\lfloor \sqrt{p} + 1 \rfloor \overset{?}{\geq} \sqrt{p} + 1$$

p NON È UN □

p

n^2 $(n+1)^2$

$\lfloor \sqrt{p} \rfloor = n$ $\quad n + 1 \overset{?}{\geq} \sqrt{p} + 1$

VERA PERCHÉ $p + 1 \leq (n+1)^2$ PERCHÉ

$n^2 < p < (n+1)^2$

QUINDI GLI $a+bk$ SONO ALMENO p

CE NE SONO DUE CONGRUI?

(SE FOSSERO $p+1$)

- CE N'È UNO $\equiv 0 \ (p)$
- CE NE SONO $2 \equiv$ ↺ (p)

HO p NUMERI: SE NESSUNO $\equiv 0 (p)$

CI POSSO METTERE SOLO IN $\{1, \dots, p-1\}$:

p SIGEON NASCE

—

$a+kb \equiv 0 \ (p)$ $\quad k^2 \equiv -1 \ (p)$

$a \equiv -kb \ (p)$ $\quad a^2 \equiv -b^2 \ (p)$

$p \mid a^2+b^2$

$(a,b) \neq (0,0) \to a^2+b^2 \neq 0$

$a^2+b^2 < \quad (a,b \leq \lfloor\sqrt{p}\rfloor < \sqrt{p})$

$p+p = 2p \to a^2+b^2 = p$

$a_1+b_1 i \equiv a_2+b_2 i \pmod{p}$

$(a_1-a_2) \equiv (b_2-b_1)\, i \pmod{p}$

$(a_1-a_2)^2 + (b_2-b_1)^2 \equiv 0 \pmod{p}$

$a_1-a_2 \neq 0 \quad o \quad b_2-b_1 \neq 0$

↳ ALMENO UNA DELLE DUE È VERA, ALTRIMENTI $(a_1,b_1) = (a_2,b_2)$ MA LO AVEVO DUE COPPIE DISTINTE.

A PRIORI b_2-b_1 PUÒ ESSERE NEGATIVO

CONSIDERO $|a_2 - a_1| \in |b_2 - b_1|$

$\Leftrightarrow |a_2 - a_1|, |b_2 - b_1| \leq \sqrt{p}$?

b_2 E b_1 STANNO IN $[0, \sqrt{p}]$:

LA DIFFERENZA DEV'ESSERE AL PIÙ LA LORO DISTANZA, DUNQUE $|b_2 - b_1| < \sqrt{p}$

$(|a_2 - a_1|)^2 + (|b_2 - b_1|)^2$ È MULTIPLO DI p, NON È 0, È $< 2p$: È p. □

$p \equiv 1 \pmod 4$ $\quad p = a^2 + b^2 = (a+ib)(a-ib)$

↳ NON È PRIMO IN $\mathbb{Z}[i]$

$a+ib$ È PRIMO

$a+ib = (x_1+iy_1)(x_2+iy_2)$

$\downarrow$ NORMA

$p = a^2+b^2 = (x_1^2+y_1^2)(x_2^2+y_2^2)$

$\hookrightarrow$ WLOG È 1:

DUNQUE x_1+iy_1 $\begin{matrix}1\\-1\\i\\-i\end{matrix}$ $\leftrightarrow$ INVERTIBILE.

IN EFFETTI $a+ib$ È PRIMO

RAGIONEVOLMENTE $a-ib$ È PRIMO

SE $p \equiv 1 \pmod 4$, $a+ib$ E $a-ib$ SONO PRIMI DIVERSI.

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

$1+i$ E $1-i$ SONO PRIMI DISTINTI:

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

UNICA ECCEZIONE: $1+i$ È LO STESSO PRIMO DI $\overline{1+i} = 1-i$

ALTRIMENTI NO: SONO PRIMI DISTINTI:

$a+ib = \begin{cases} 1\,(a-ib): & -b = b \to b = 0 \\ i\,(a-ib): & a = b,\ b = a \\ -1\,(a-ib) & -a = a,\ b = b \\ -i\,(a-ib) & -a = b,\ -b = a \end{cases}$

$a+ib = K(1+i)$

$= K(1-i)$

$K = \pm 1$

SE $K > 1$: $K(1+i) = K \cdot (1+i)$

NESSUNO INVERTIBILE

- $b=0 \rightarrow a$ È PRIMO

  $\overline{a}=a \rightarrow$ ENTRAMBI PRIMI

  $(a \rightarrow p \equiv 3 \ (4))$

- $a=0 \rightarrow ib$ È PRIMO

  $\downarrow$

  b È PRIMO

ib PRIMO $\Leftrightarrow \overline{ib}=-ib$ PRIMO

PERCHÉ $3+4i$ NON È PRIMO

$N(3+4i)=25$ NON È PRIMO

HOPE: $a+ib$ È PRIMO SE E SOLO SE

$N(a+ib) \begin{cases} p^2 \text{ CON } p \equiv 3 \ (4) \\ p \text{ CON } p \equiv 1 \ (4) \end{cases}$

$a^2+b^2 \equiv p^2, \quad p \equiv 3 \pmod 4$

Se $0 < a, b < p$

$a^2+b^2 \equiv 0 \pmod p \to a^2 \equiv -b^2 \pmod p$

$\equiv 1$

$a^2 \cdot (b^2) \equiv -1 \pmod p$

$(a \cdot b^{-1})^2 \equiv -1 \pmod p$ MA $p \equiv 3 \pmod 4$

Dunque $(a,b) = (0,p) = (p,0)$

Se $N(a+ib) = p^2, \quad p \equiv 3 \pmod 4$

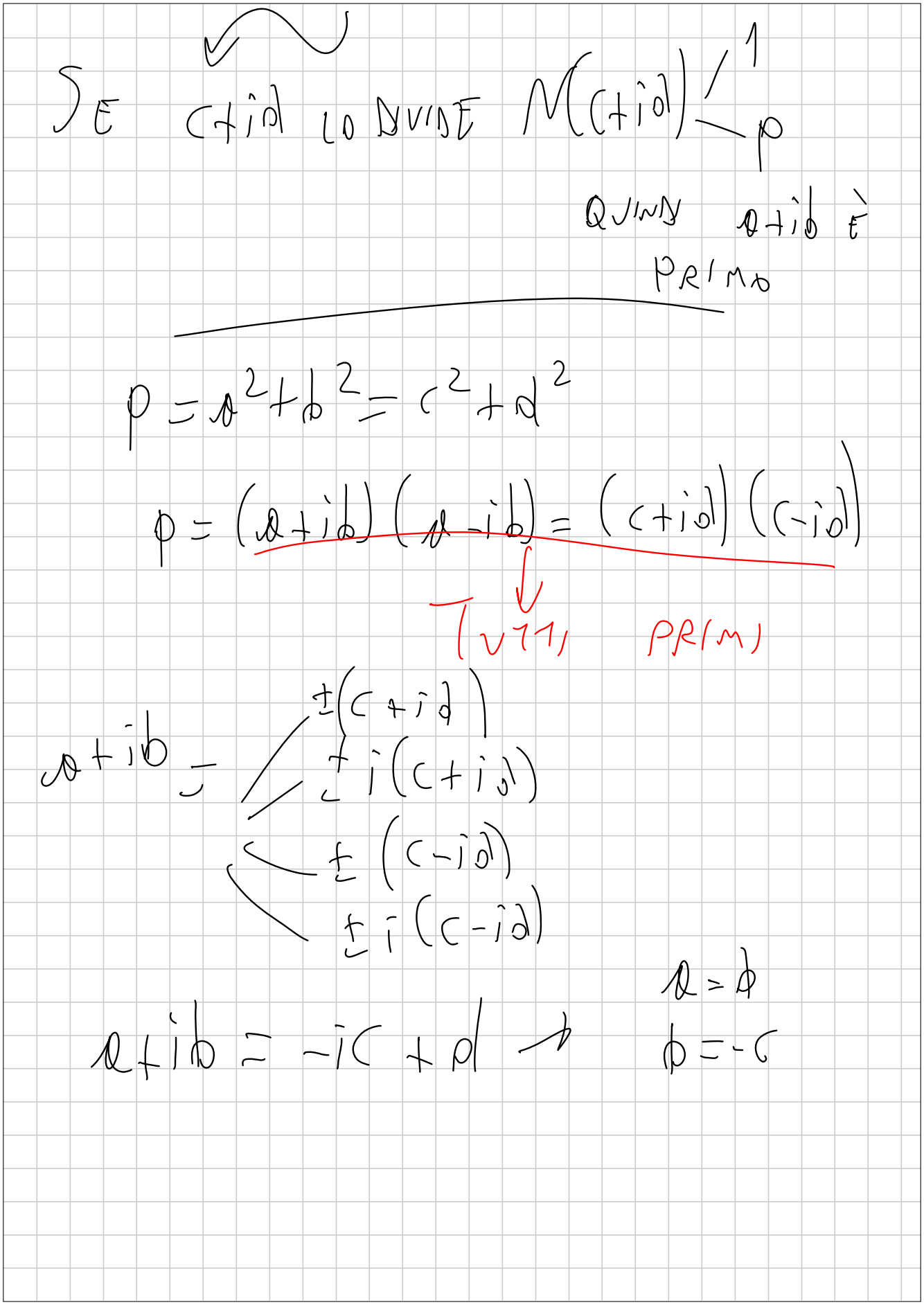
p

$a+ib \mid p$

$= i \cdot p$

$= -i \cdot p$

$N(a+ib) = p \quad (\equiv 1 \pmod 4)$


SE c+id LO DIVIDE N(c+id)^1/p
QUINDI a+ib È PRIMO
p = a^2+b^2 = c^2+d^2
p = (a+ib)(a-ib) = (c+id)(c-id)
TUTTI PRIMI
a+ib = ±(c+id)
±i(c+id)
±(c-id)
±i(c-id)
a+ib = -ic+d
a = b
b = -c

SE $N(a+ib) \neq$ p^2 $\equiv 3 \pmod 4$, p $\equiv 1 \pmod 4$

$\Rightarrow$? $\Rightarrow$ ~~$p \equiv 3 \pmod 4$~~

$N(a+ib)$ NON È UN p^2 O UN p

$\downarrow$

CONE PRODOTTO DI DUE INTERI

$N(a+ib) = qX$ CON q PRIMO

$(a+ib)$ DIVIDE qX

$(a-ib)$ DIVIDE qX

$$qX = \prod_{j=1}^{k} (m_j + i n_j)$$

$$a+ib = \prod_{j=1}^{R} (m_j + i n_j)$$

A PRIORI PUÒ ESSERE 1

$$a-ib = \prod_{j=1}^{R} (m_j - i n_j)$$

$$a^2+b^2 = \prod_{j=1}^{R} (m_j^2 + n_j^2) =$$

$$\| \quad \prod_{j=1}^{R} (m_j + i n_j)(m_j - i n_j)$$

$$N(a+ib) = q \cdot X$$

$$q = \prod_{j=1}^{V_+} (m_j + i n_j) \cdot \prod_{j=1}^{V_-} (m_j - i n_j)$$

$$K = \prod_{j=1}^{U_+} (m_j + i n_j) \cdot \prod_{j=1}^{U_-} (m_j - i n_j)$$

$a+ib$ È PRIMO $\rightarrow$ AL PIÙ 2 PRIMI CHE SONO PER PRIMO $a+ib$ È $a-ib$

$q \equiv 1 \ (4)$

$q = \prod (m+in)$ $= (a+ib)(a-ib)$ $a^2+b^2=p$

$x = \prod (n+in)$ → 0 PRIMI

I DUE PRIMI CHE AVEVO $(a+ib$ E $a-ib)$ STANNO IN q → $x=1$

$N(a+ib) = q$

$p \equiv 3 \ (4)$

$q = \prod (m+in)$ 1 PRIMO $a+ib$

$x = \prod (m+in)$

$a=0 \vee b=0$

$q = \pm n / \pm i \ (a+ib)$

$x = \pm 1 / \pm i \ (a+ib)$

WLOG $b>0$ $\rightarrow$ $q = \prod_{a+b} (a+ib) =$

$x = q$ $\qquad x = \prod_{a-b} (a+ib) =$

$N(a+ib) = xq = q^2$, con $q \equiv 3 \pmod 4$

ORA ABBIAMO TUTTI I PRIMI $p^2 p \equiv 3 \pmod 4$

$a+ib$ t.c. $N(a+ib)$ / $p,\ p \equiv 1 \pmod 4$

TROVARE PER QUALI $(x,y) \in \mathbb{Z}^2$ VALE

$x^2 + y^2 = 13 q^2$

$N(3+2i) \in \mathbb{P}$: non si scompone

$(x+iy)(x-iy) = 13^4 = (3+2i)^4 (3-2i)^4$

$(x+iy) = (3+2i)^{\alpha} (3-2i)^{\beta}$

$(x-iy) = (3+2i)^{4-\alpha} (3-2i)^{4-\beta}$

$$(3-2i)^{\alpha}(3+2i)^{\beta}$$

$$(3-2i)^{\alpha}(3+2i)^{\beta} = (3+2i)^{4-\alpha}(3-2i)^{4-\beta}$$

$$\boxed{\alpha+\beta=4}$$

$$x+iy = (3+2i)^{\alpha}(3-2i)^{4-\alpha}$$

$\alpha = 0, 1, 2, 3, 4$

CONIUGATI

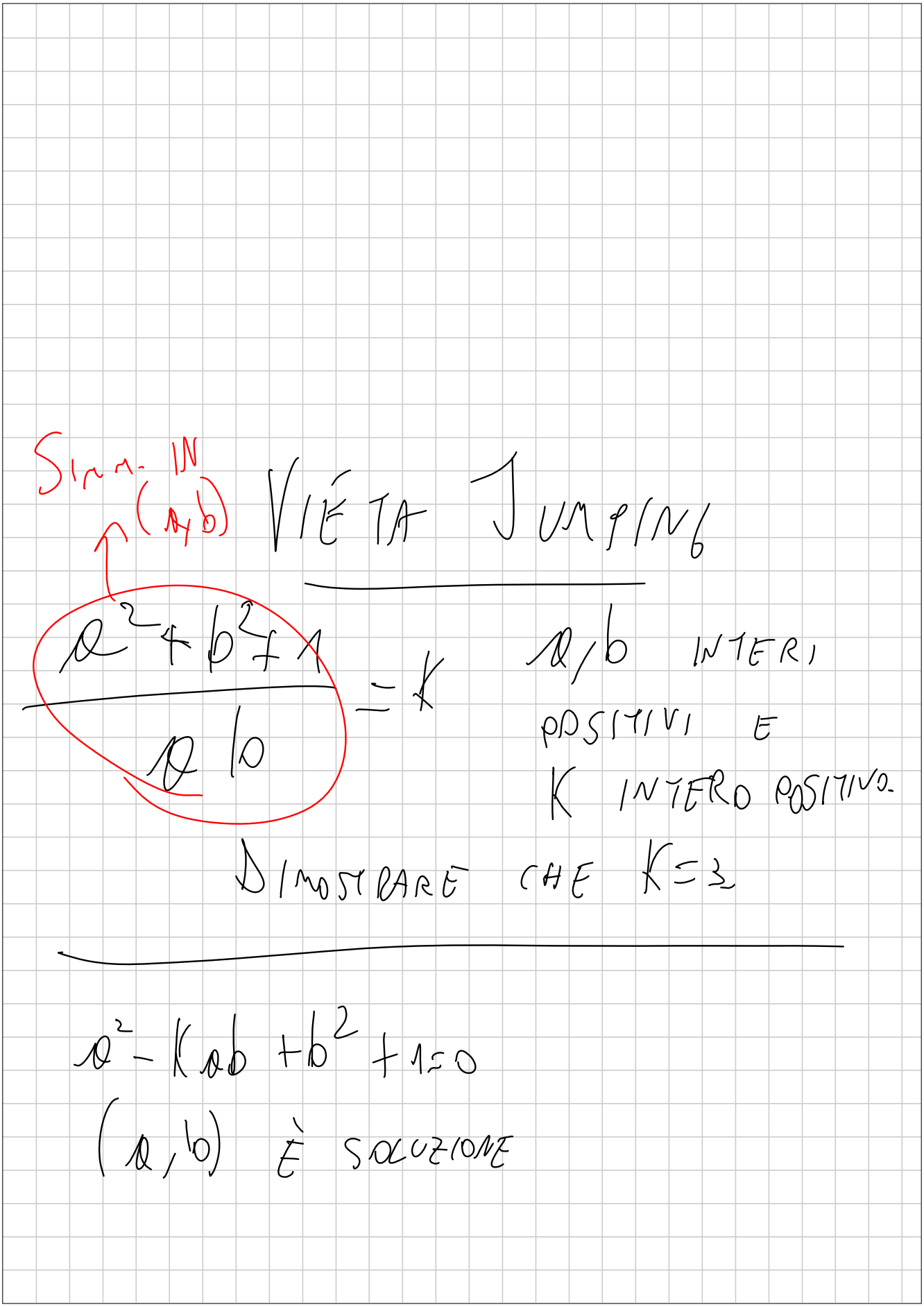
$(3+2i)^3(3-2i) =$

$\Rightarrow (3+2i)(3-2i)^3$

$$x+iy = (3+2i)^4 = -119+120i$$

$$x+iy = (3+2i)^3(3-2i) = 13(5+12i)$$

$$x+iy = (3+2i)^2(3-2i)^2 = 13^2 = 169$$


Sia n: (a,b)
VIÈTA JUMPING
$\frac{a^2+b^2+1}{ab} = k$
a, b INTERI POSITIVI E
k INTERO POSITIVO.
DIMOSTRARE CHE $k=3$
$a^2 - kab + b^2 + 1 = 0$
(a,b) È SOLUZIONE

$x^2 - mx + q = 0$ HA α COME SOLUZIONE. L'ALTRA SOLUZIONE È $m - \alpha$ (OPPURE q/α.)

$a^2 - (kb)a + (b^2+1) = 0$

a È SOLUZIONE $\rightarrow$ $kb - a$ È SOLUZIONE

$(a, b) \longrightarrow (kb - a, b)$

(b, a)

(a, b) $\nearrow$ $(kb - a, b)$

(a, b) $\searrow$ $(ka - b, a)$

UNO SPERA CHE SE $a > b$ ALLORA

$Ka - b$ O $Kb - a$ SIANO $< b$ E

> 0.

$$\frac{a^2+b^2+1}{ab} = K$$

$$\frac{(Kb-a)^2+b^2+1}{(Kb-a)b} \stackrel{?}{=} \frac{K^2b^2-2Kab+a^2+b^2+1}{Kb^2-ab} =$$

$$= \frac{K^2b^2-Kab}{Kb^2-ab} + \frac{-Kab+a^2+b^2+1}{Kb^2-ab}$$

K $\qquad -Kab+a^2+b^2+1=0$

$$K = \frac{a^2+b^2+1}{ab}$$

(a,b) SOLUZIONE CON $a \geq b > 1$.

QUALI COPPIE RESTANO?

- $b > a$ (SIMMETRIA)
- $a = b$
- $b = 1$

$a = b \rightarrow \dfrac{a^2+a^2+1}{a^2} = 2 + \dfrac{1}{a^2}$

$a > 1 \rightarrow K = 3$

$a = b = 1 \rightarrow K = 3$

$b = 1 \rightarrow \dfrac{a^2+1+1}{a} = a + \dfrac{2}{a}$

$a = 2 \rightarrow a = 2, b = 1, K = 3$

$a = 1 \rightarrow a = 1, b = 1, K = 3$

Con $a > b \geq 1$

$a^2 - a(kb) + (b^2+1)$

$(a,b) \to (b, kb-a)$

RAPPORTO ✓

$kb - a \overset{?}{<} b \qquad kb \overset{?}{<} a+b$

$\frac{(a^2+b^2+1)b}{ab} \overset{?}{<} a+b$

$a^2b + b^3 + b \overset{?}{<} a^2b + ab$

$b^2 + 1 \overset{?}{<} ab$

$1 \overset{?}{<} b(a-b)$

$1 \geq 1 \qquad a-b \geq 1$

PERCHÉ $Kb-a$ NON È NEGATIVO,
ANZI, PERCHÉ È ≥ 1

$$(Kb-a)\cdot a = (b^2+1)$$

LE 2 RADICI DI $x^2 - x(Kb) + (b^2+1)$

$$(a,b) \to (b, Kb-a)$$

$a > b > 1$ $\quad b > Kb-a \geq 1$ $\quad \geq 1$, $= 1$ ✓

$a > b > 1$ ↓ $b > Kb-a > 1$ ↓ VADO AVANTI...

K SI CONSERVA

UNA SUCCESSIONE DI INTERI POSITIVI DECRESCENTE È FINITA: IL MECCANISMO FINISCE QUANDO ARRIVO A 1

QUINDI K DEVE RISOLVERE ALMENO UNA SOL. ESTREMALE $\Rightarrow$ $K=3$.

QUALI (a,b)?

PASSAGGIO AL CONTRARIO

$(a,b) \to (b, 3b-a)$

(x, y)

$(3x-y, x)$

RISALIRE È SCEGLIERE FISSANDO L'ALTRA DELLE DUE

ALG. SU $a>b \to$ SCENDO

ALG. SU $a<b \to$ SALITO

METTIAMO CHE (a,b) CON $(a<b)$

SCEMA: $(a,b) \to (b,c)$

SE FACCIO IL PASSAGGIO AL CONTRARIO SU (b,c) SCENDO

$(1,1) \qquad (2,1)$

$(y, x) \mapsto (3y - x, y)$

$(x_{n+1}, x_n) \mapsto (3x_{n+1} - x_n, x_{n+1})$

$x_{n+2} = 3x_{n+1} - x_n$

SI RISOLVE

1 1 2 5 13 34 ...

EQ. DI PELL

$x^2 - dy^2 = 1 \qquad (x, y)$ INTERI

SE $d = \square$ $\rightarrow$ $(x+\alpha y)(x-\alpha y) = 1$

$\downarrow$

$x = 1,\ y = 0$

SE $\Delta < 0$ VABBÈ

$x^2 - dy^2 = 1, \qquad d \neq \square$

CI SONO SEMPRE ∞ SOLUZIONI.

ES.

$2a^2 + 27a + 91 = b^2$

(a/b) SONO INFINITE

$x^2 + x$ HA SENSO SCRITTO COME $\left(x + \frac{1}{2}\right)^2 - \left(\frac{1}{2}\right)^2$

$2a^2 + 27a + 91 = \frac{1}{2}\left(4a^2 + 54a + 182\right) =$

$= \frac{1}{2}\left(\left(2a + \frac{27}{2}\right)^2 - \frac{1}{4}\right) =$

$$\frac{1}{8}\left(4a+27\right)^2 - \frac{1}{8} = b^2$$

$$\left(4a+27\right)^2 - 1 = 8b^2$$

$$\left(4a+27\right)^2 - 8b^2 = 1$$

$x^2 - 8y^2 = 1$ (SO CHE HA INFINITE SOLUZIONI).

↳ DISPARI

VORREI $x = 4a+27$ ∞ VOLTE

$x \equiv 3 \ (4)$ ∞ VOLTE

$x \equiv 1, 3 \ (4)$

$x \equiv 3 \ (4)$ ✓

$x \equiv 1 \ (4) \rightarrow -x \equiv 3 \ (4)$

$x^2 - d y^2 = 1$ HA INFINITE SOLUZIONI.

$(1, 0)$

SUPPONIAMO CI SIA UNA SOL. NON BANALE (a, b).

$$a^2 - d b^2 = 1$$

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

$$\left((a^2 + b^2 d) + (2ab)\sqrt{d}\right)\left((a^2 + b^2 d) - (2ab)(\sqrt{d})\right) = 1$$

$$(a^2 + b^2 d)^2 - d\,(2ab)^2 = 1$$

$$(a, b) \to (a^2 + b^2 d,\ 2ab)$$

MOLTO GROSSA

$(a,b)\quad (x,y) \to (ax+by\sqrt{d},\ bx+ay)$

$(a+b\sqrt{d})(x+y\sqrt{d}) = (ax+by d)+(bx+ay)\sqrt{d}$

$x^2-3y^2=1 \qquad (2,1) \qquad (2+\sqrt{3})^n = a+b\sqrt{3}$

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

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

$$(a+b\sqrt{d})(x+y\sqrt{d}) = u+v\sqrt{d}$$

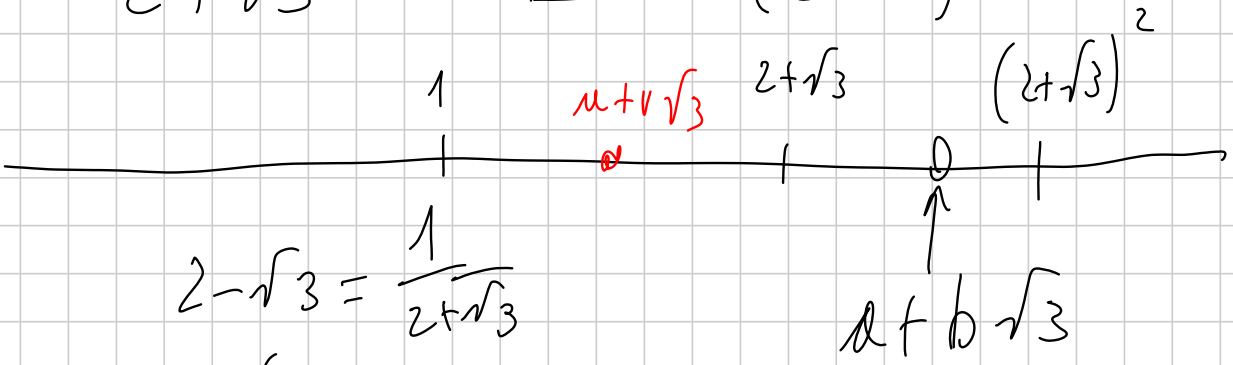
$$u = ax+bdy$$
$$v = bx+ay$$

$$(ax+bdy)^2 - d(bx+ay)^2 =$$
$$= a^2x^2 + 2abdxy - db^2x^2 -$$
$$+b^2y^2d^2 - 2abxy - da^2y^2 =$$
$$= (a^2 - b^2d)(x^2 - y^2d) = 1$$

$$(a+b\sqrt{d})(x+y\sqrt{d}) = u+v\sqrt{d}$$
$$(a-b\sqrt{d})(x-y\sqrt{d}) = u-v\sqrt{d}$$
$$(a^2-db^2)(x^2-dy^2) = u^2-dv^2$$

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

$2+\sqrt{3}$ $\quad$ Hope: $(2+\sqrt{3})^n$

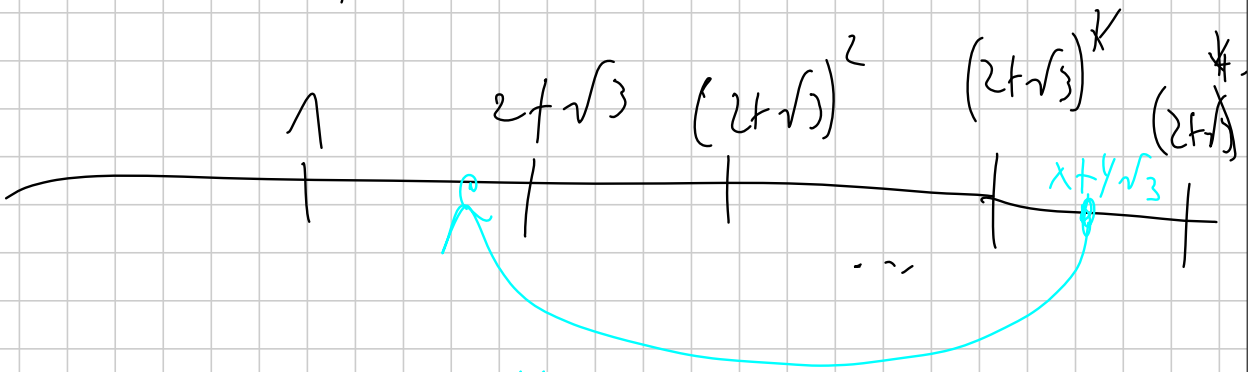


$$2-\sqrt{3} = \frac{1}{2+\sqrt{3}}$$

$$(a+b\sqrt{3})(2-\sqrt{3}) = u+v\sqrt{3}$$

$$(a-b\sqrt{3})(2+\sqrt{3}) = (u-v\sqrt{3})$$

$\|1$ $\quad$ $\|1$ $\quad$ $u^2 - 3v^2 = 1$



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

$$\downarrow$$

$$u^2 - 3v^2 = 1$$

$$1 < u + v\sqrt{3} < 2 + \sqrt{3}$$

$$u^2 - 3v^2 = 1$$

$$\| $$

$$(u + v\sqrt{3})(u - v\sqrt{3}) = 1$$

$$2 - \sqrt{3} < u - v\sqrt{3} < 1$$

$$0 < 3 - \sqrt{3} < 2u < 3 + \sqrt{3} < 6$$

$u = 1, 2$

$u = 1 \to v = 0$

$u = 2 \to v = \pm 1$

$u = 2 \quad v = -1 \quad 2 - \sqrt{3} < 1$ ASSURDO

$u = 2 \quad v = 1 \quad 2 + \sqrt{3}$ È LA SOL. BASE

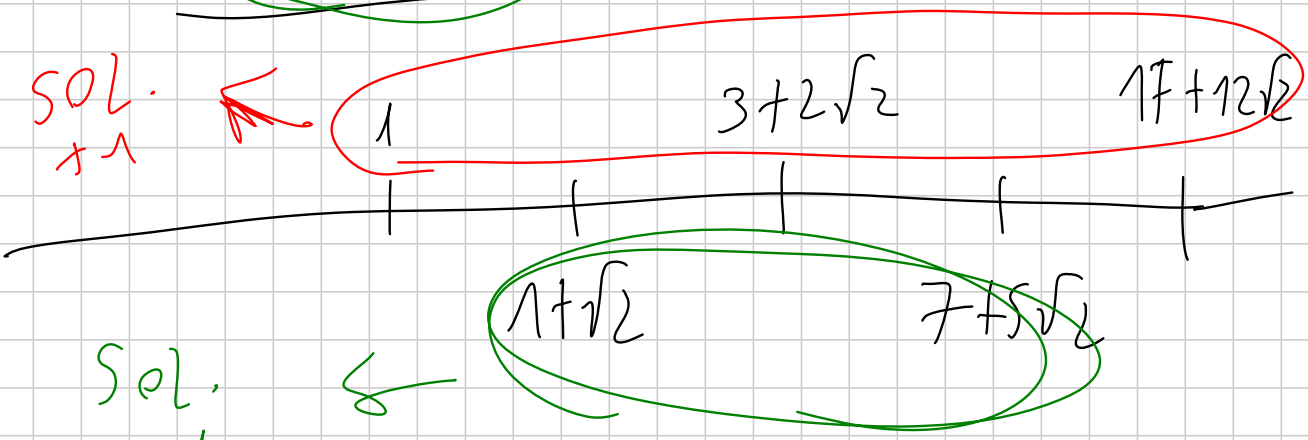
CON $x^2 - dy^2 = -1$ È MOLTO PIÙ PROBLEMATICO CAPIRE COSA SUCCEDE.

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

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

$(1+\sqrt{2})^2$

$3+2\sqrt{2}$



LE SOL. DI $x^2 - dy^2 = 1$ SONO SEMPRE POTENZE DELLA SOL. MINIMA

$x^2 - y^2 d = 1$ HA SOLUZIONE?

SIANO a_1, b_1 t.c. $a_1^2 - b_1^2 d = m$

a_2, b_2 t.c. $a_2^2 - b_2^2 d = m$

$$\frac{(a_1 + b_1\sqrt{d})}{(a_2 + b_2\sqrt{d})} = \frac{(a_1 + b_1\sqrt{d})(a_2 - b_2\sqrt{d})}{m} =$$

$= x\,m$ $\qquad = y\,m$

$$\frac{(a_1 a_2 - d\, b_1 b_2) + \sqrt{d}(a_2 b_1 - a_1 b_2)}{m}$$

$x^2 - d y^2 = ?$

$$\frac{1}{m^2}\left((a_1 a_2 - d\, b_1 b_2)^2 - d\,(a_2 b_1 - a_1 b_2)^2 \right) =$$

... CONTI

$$\frac{1}{m^2}\left((a_1^2 - d b_1^2)(a_2^2 - d b_2^2) \right) = 1$$

VOREI CHE m DIVIDESSE

$a_1a_2 - d b_1 b_2$ E $a_2 b_1 - a_1 b_2$

SE $a_1 \equiv a_2 \pmod m$ E $b_1 \equiv b_2 \pmod m$

$\equiv a_1^2 - d b_1^2 = m \equiv 0 \pmod m$

$a^2 - d b^2 \equiv 0 \pmod m$

$\equiv 0 \pmod m$

$ab - ab \equiv 0 \pmod m$

PER TROVARE UNA SOLUZIONE A $x^2 - dy^2 = 1$ CE NE BASTANO DUE A $x^2 - dy^2 = m$ CON $x_1 \equiv x_2 \pmod m$ E $y_1 \equiv y_2 \pmod m$.

ORA: SE HO ∞ SOLUZIONI A $x^2 - dy^2 = m$, DI SICURO, TRA LE COPPIE (a,b) DI SOL. MOD m, CE NE SONO 2 UGUALI.

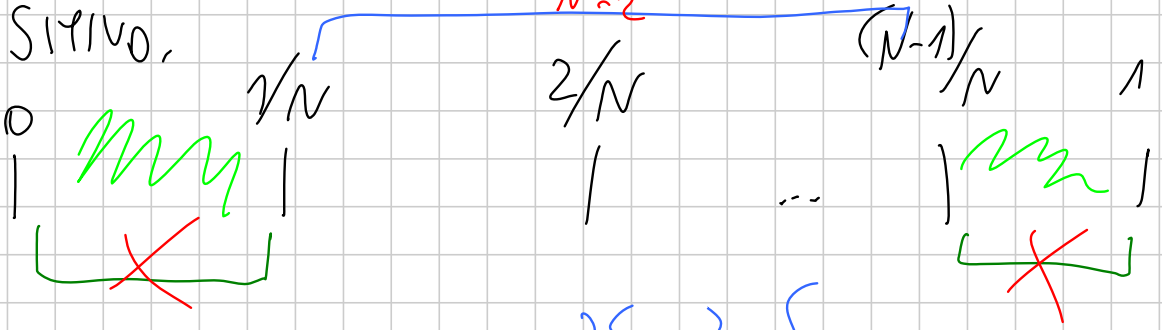
QUINDI ORA VOGLIO TROVARE ∞ SOLUZIONI

LEMMA (DIRICHLET)

SIA $\alpha > 0$ UN NUMERO IRRAZIONALE, ALLORA ESISTONO INFINITI INTERI POSITIVI p, q TALI CHE

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

PER DIMOSTRARLO, SIA N UN INTERO POSITIVO.



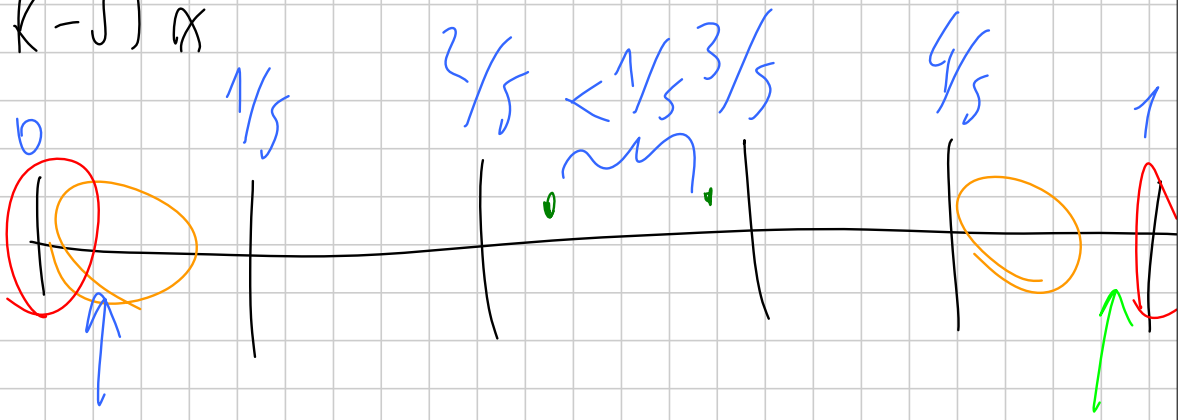
E CONSIDERIAMO $\{\alpha\}, \{2\alpha\}, \ldots, \{(N-1)\alpha\}$

POICHÉ SONO IRRAZIONALI NON SONO i/N

PER PIGEON HOLE DUE SONO NELLO STESSO INTERVALLO. SE $K\alpha$ E $J\alpha$ SONO

NELLO STESSO INTERVALLO $(K > J)$

$(K-J)\alpha$



C'È N'È UNO IN UNO DEGLI

$$|\alpha K - k| \leq \frac{1}{N} \rightarrow \left|\alpha - \frac{k}{K}\right| < \frac{1}{NK} <$$

$K < N$

$$< \frac{1}{K^2}$$

$$\left|\alpha - \frac{k}{K}\right| < \frac{1}{NK}$$

SUPPONIAMO CHE GLI K_i, K_j SIANO FINITI. ALLORA

$\left|\alpha - \frac{K_i}{K_j}\right|$ HA UN MINIMO > 0 PERCHÉ α È IRRAZIONALE

SE SCELGO N TALE CHE $\frac{1}{N}$ SIA $<$ DEL MIN

AVREI $\left|\alpha - \frac{k}{K}\right| < \frac{1}{KN} < \min$

ASSURDO

LEMMA SU $\sqrt{d}$

$$\left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{q^2}$$

$$\left|q\sqrt{d} - p\right| < \frac{1}{q}$$

$$\left(q\sqrt{d} + p\right)\left|q\sqrt{d} - p\right| < \frac{q\sqrt{d} + p}{q}$$

$$\left|p^2 - d q^2\right| < \sqrt{d} + \frac{p}{d} < \sqrt{d} + \sqrt{d} + \frac{1}{q^2} \leq 2\sqrt{d} + 1$$

$|p^2 - d q^2| < 2\sqrt{d} + 1$

INFINITE VOLTE

CI SARANNO A SOL. A $x^2 - dy^2 = m$

CON $|m| < 2\sqrt{d} + 1$

$m \neq 0$ DENNO' $x^2 = dy^2 \to d = \square$

QUALCOSA DI ANALITICO

COSA VUOL DIRE CHE UNA SOMMATORIA DI TERMINI POSITIVI DIVERGE? O CONVERGE

$$\sum_{i=1}^{+\infty} \frac{1}{i^2} = \frac{\pi^2}{6}$$

$$\sum_{i=0}^{+\infty} a_i = C \iff$$

$$\forall \varepsilon > 0 \quad \exists N \text{ t.c. } \sum_{i=0}^{N} a_i > C - \varepsilon$$

$$\forall N \quad \sum_{i=0}^{N} a_i \leq C$$

$$\sum_{n=1}^{+\infty} \frac{1}{n} \quad \text{DIVERGE} \quad (\text{VA A INFINITO})$$

$$1 \geq \frac{1}{2} = \frac{1}{2}$$

$$\frac{1}{2} \quad \frac{1}{3} \geq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

$$\frac{1}{4} \quad \frac{1}{5} \quad \frac{1}{6} \quad \frac{1}{7} \geq \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} = \frac{1}{2}$$

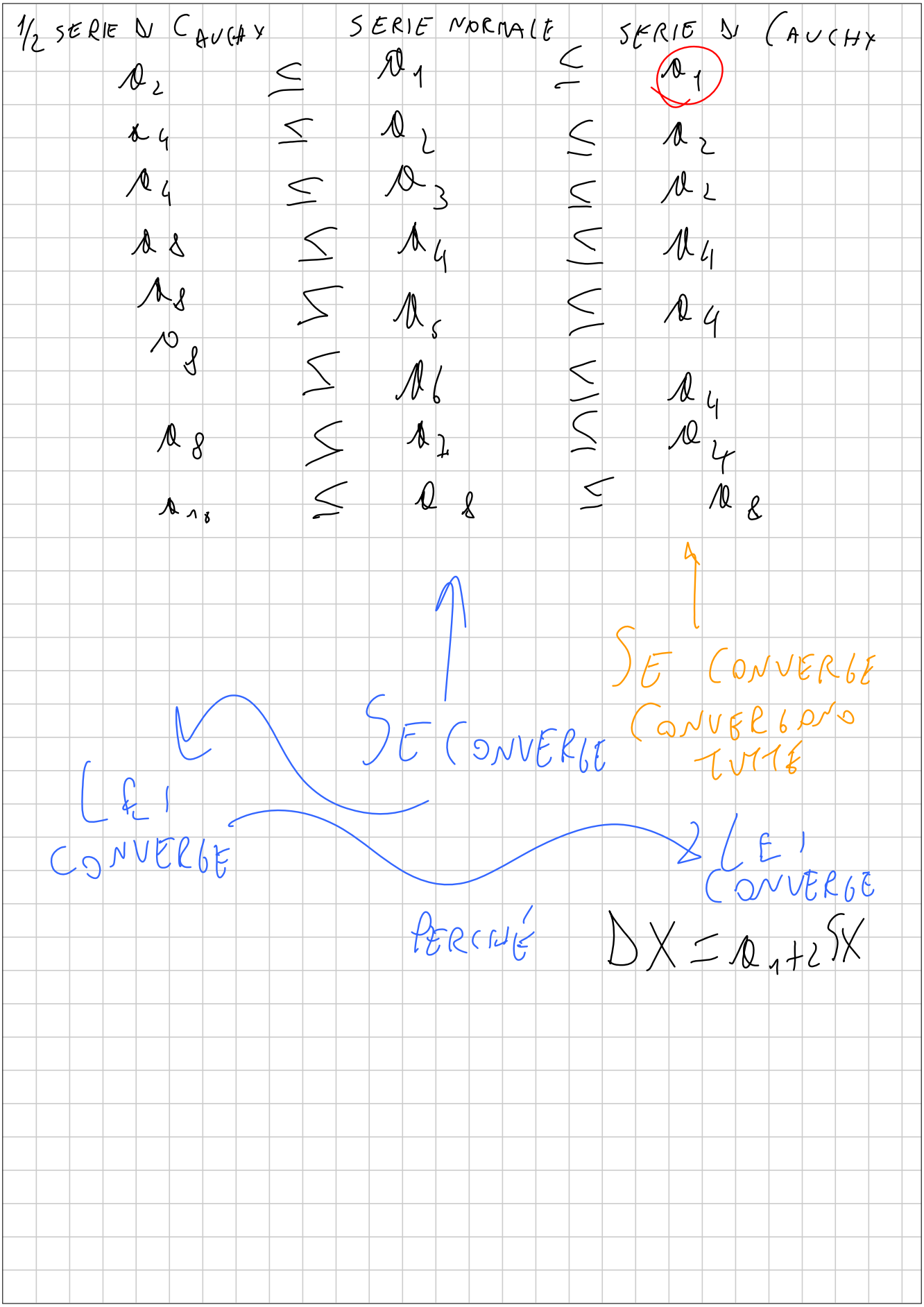
$$\sum_{i=1}^{2^K-1} \frac{1}{i} \geq \frac{K}{2}$$

$$\forall N \quad \exists K \text{ t.c. } \sum_{i=1}^{K} \frac{1}{i} > N$$

CONDENSAZIONE DI CAUCHY — **DIVERGE**

DATA UNA SUCCESSIONE DEBOLMENTE DECRESCENTE DI REALI POSITIVI $a_1, a_2, \ldots$ ALLORA

$$\sum_{n=1}^{+\infty} a_n \text{ CONVERGE} \Leftrightarrow \sum_{n=1}^{+\infty} 2^{n-1} \cdot a_{2^n} \text{ CONVERGE}$$


1/2 SERIE DI CAUCHY
SERIE NORMALE
SERIE DI CAUCHY
SE CONVERGE
SE CONVERGE CONVERGONO TUTTE
LE I CONVERGE
LE I CONVERGE
PERCHÉ
DX = a1 + 2SX

$\sum_{n=1}^{+\infty} \frac{1}{n^s}$ CONV. $s>0$

CONV. (SE E SOLO SE $s>1$)

$\sum_{n=1}^{+\infty} 2^n \cdot \frac{1}{(2^n)^s}$ CONV.

$\sum_{n=1}^{+\infty} \left(2^{1-s}\right)^n$

SE $x<1$

$\sum_{i=0}^{+\infty} x^i = 1 + x + x^2 + \dots = \lim_{n\to+\infty} \frac{x^n - 1}{x-1} = \frac{1}{1-x}$

SE $x<1$

$\sum_{i=0}^{n} x^i = \frac{x^{n+1}-1}{x-1} = \frac{1-x^{n+1}}{1-x}$

VICINO AD 1 QUANTO VOGLIO

$\frac{1}{1-x} \cdot \left(1-x^{n+1}\right) < \frac{1}{1-x}$

$$\sum_{i=0}^{+\infty} x^i \geq \sum_{i=0}^{+\infty} 1 = +\infty \qquad x \geq 1$$

$$\sum_{n=1}^{+\infty} \left(2^{1-s}\right)^n \quad ! \quad \text{CONV.} \Leftrightarrow 2^{1-s} < 1 \Leftrightarrow s > 1$$

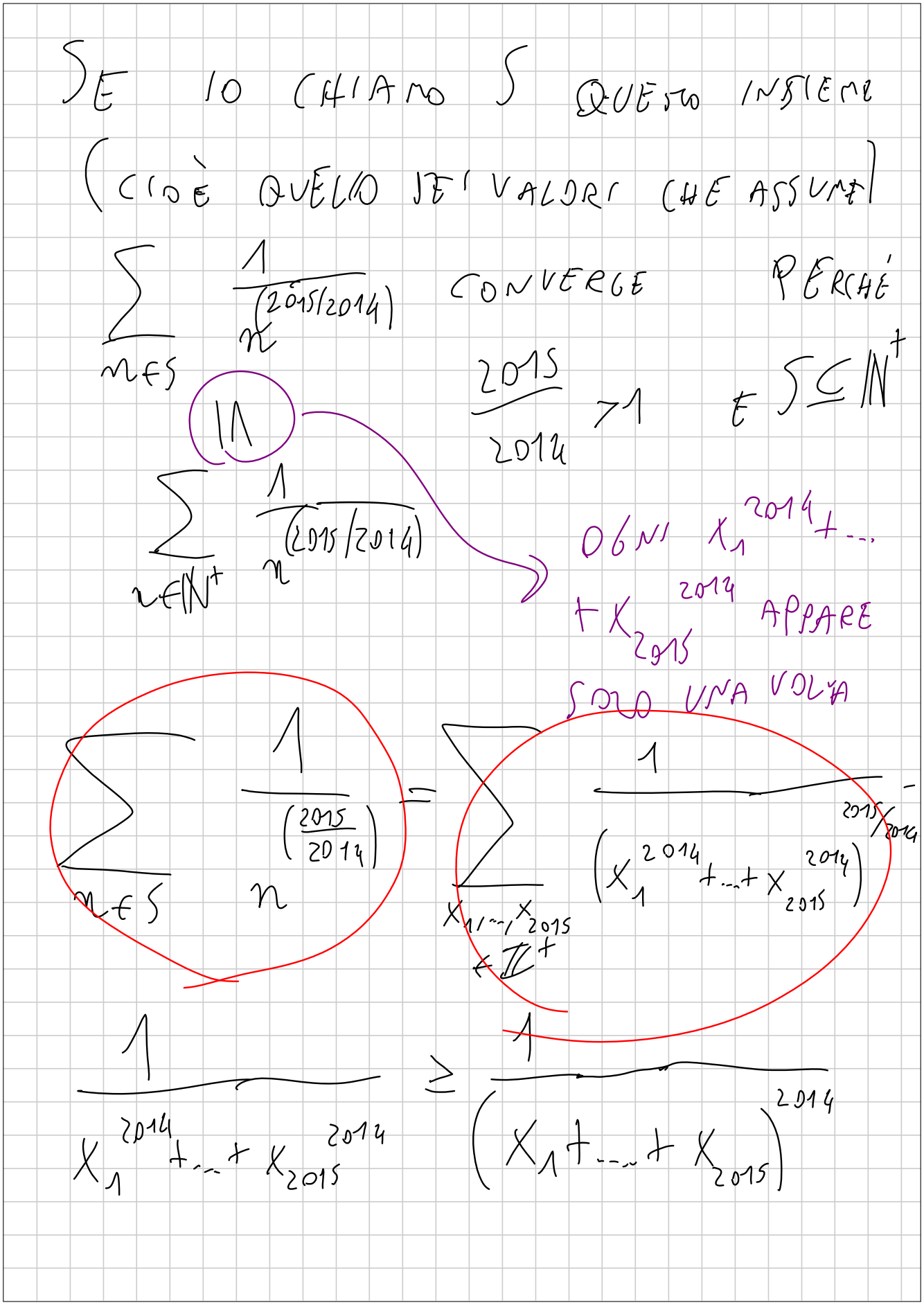
ESENATICO 5, 2014

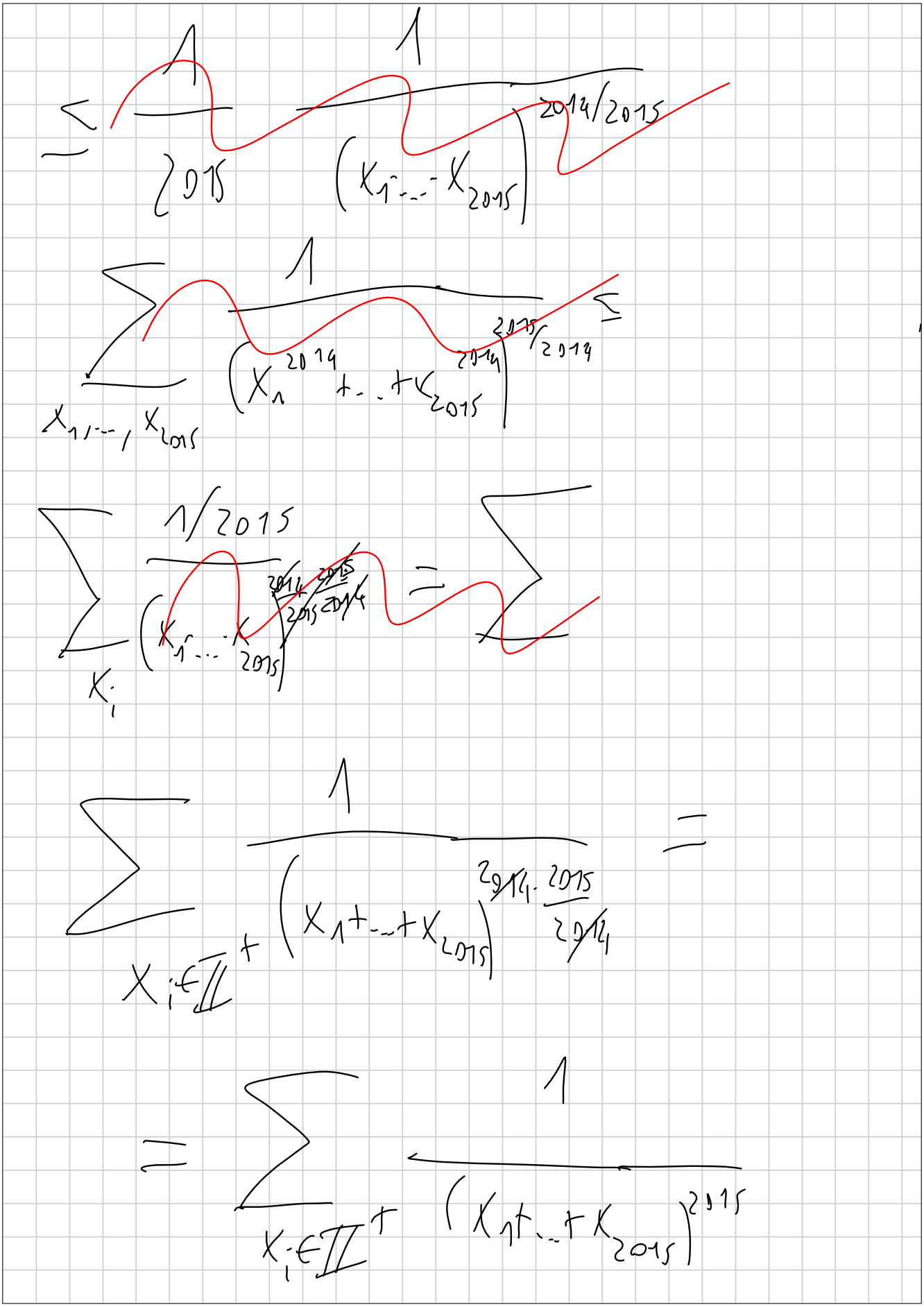
s È L'INSIEME DEI VALORI CHE ASSUME

$x_1^{2014} + \ldots + x_{2015}^{2014}$ ASSUME LO STESSO VALORE PER DUE 2015-UPLE DISTINTE DI INTERI POSITIVI.

SUPPONIAMO CHE GLI $x_1^{2014} + \ldots + x_{2015}^{2014}$ SIANO TUTTI DIVERSI.

(È UN SOTTOINSIEME DEGLI INTERI POSITIVI)


SE LO CHIAMO S QUESTO INSIEME
(CIOÈ QUELLO DEI VALORI CHE ASSUME)
CONVERGE PERCHÉ
2015/2014 > 1 E S ⊆ ℕ⁺
OGNI x_1^{2014} + ...
+ x_{2015}^{2014} APPARE
SOLO UNA VOLTA
$x_1, \dots, x_{2015}$
+ ∞⁺



K LO POSSO OTTENERE IN $K_1 + \dots + K_{2015}$ IN

$$\binom{K}{2015} \quad \text{MOD}$$

$$\sum_{x_i \in \Pi^+} \frac{\binom{K-1}{2014}}{K^{2015}}$$

$$\binom{K-1}{2014} \text{ HA GRADO } 2014$$

$$\sum_{x_i \in \Pi^+} \frac{\alpha K^{2014} + \text{ROBA}}{K^{2015}} \sim \sum_{K \in \Pi^+} \frac{1}{K^2}$$

$$> +\infty$$