Stage Senior 2011 – Livello Basic

Stampato integrale delle lezioni

Autori vari

Indice

INDUZIONE - PRINCIPIO DEI CASSETTI

Titolo nota 04/09/2011

$\mathbb{N}$ = insieme dei numeri naturali $= \{1, 2, 3, \dots\}$

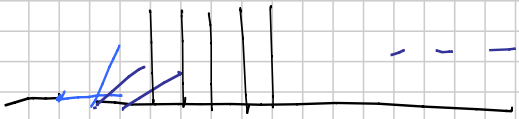
$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$

P_n = affermazione che dipende da $n \in \mathbb{N}$

$\frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}$ è un numero intero $\forall n \in \mathbb{N}$

- Dimostrare che P_1 è vera
- Dimostrare che SE P_n è vera, ALLORA è vera anche P_{n+1}

$\Rightarrow$ P_n è vera PER OGNI $\forall n \in \mathbb{N}$



- $\frac{1}{5} + \frac{1}{2} + \frac{1}{3} - \frac{1}{30} = \frac{6+15+10-1}{30} = \frac{30}{30} = 1 \in \mathbb{N}$
- $\frac{(n+1)^5}{5} + \frac{(n+1)^4}{2} + \frac{(n+1)^3}{3} - \frac{n+1}{30}$

$\frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30} + \frac{1}{5} + \frac{1}{2} + \frac{1}{3} - \frac{1}{30} + \frac{5n^4 + 10n^3 + 10n^2 + 5n}{5}$

$\in \mathbb{N}$ per ipotesi induttiva $\quad = 1 \quad \in \mathbb{N}$

$+\frac{4n^3+6n^2+4n}{2} + \frac{3n^2+3n}{3}$ Ho una somma di 5 quantità intere

$\in \mathbb{N}$ $\in \mathbb{N}$

P_n è vera $\forall n \in \mathbb{N}$

$S_n = 1+2+3+\dots+n = \frac{n(n+1)}{2}$

$S_n = \frac{n(n+1)}{2}$

$1+2+3+\dots+n-1+n = S_n$

$n+n-1+n-2+\dots+2+1 = S_n$

$(n+1)+(n+1)+(n+1)+\dots+(n+1) = 2S_n$

$n(n+1)$

- $S_1 = 1$ $\quad \frac{1(1+1)}{2} = 1$

$S_n = \frac{n(n+1)}{2}$ $\quad S_{n+1} \stackrel{?}{=} \frac{(n+1)(n+2)}{2}$

$S_{n+1} = S_n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)+2(n+1)}{2} =$

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

PROGRESSIONI ARITMETICHE

$a_i = \alpha + (i-1)\cdot r \quad i \in \mathbb{N}$

$a_1 = \alpha \quad a_2 = \alpha + r \quad a_3 = \alpha + 2r \dots$

$$a_1 + a_2 + \cdots + a_n = \sum_{i=1}^{n} a_i \stackrel{?}{=} \frac{n(2\alpha + (n-1)r)}{2}$$

- $S_1 = a_1 = \alpha$ $\qquad \frac{1 \cdot (2\alpha + (1-1)\cdot r)}{2} = \frac{2\alpha}{2} = \alpha$
- $S_{n+1} = \frac{(n+1)(2\alpha + nr)}{2}$

$$S_{n+1} = S_n + a_{n+1} = \frac{n(2\alpha + (n-1)r)}{2} + (\alpha + nr) =$$

$$\frac{n(2\alpha + (n-1)r) + 2\alpha + 2nr}{2} = \frac{2\alpha(n+1) + n(nr - r + 2r)}{2} =$$

$$= \frac{2\alpha(n+1) + nr(n+1)}{2} = \frac{(n+1)(2\alpha + nr)}{2}$$

$$S_n^{(2)} = 1^2 + 2^2 + \cdots + n^2 = \frac{n(2n+1)(n+1)}{6}$$

- $n=1$ $\quad S_1^{(2)} = 1^2 = 1$ $\qquad \frac{1 \cdot (2\cdot 1 + 1)\cdot(1+1)}{6} = \frac{1 \cdot 3 \cdot 2}{6} = 1$
- $S_{n+1}^{(2)} = S_n^{(2)} + (n+1)^2 = \frac{n(2n+1)(n+1)}{6} + (n+1)^2 =$

$$\frac{(n+1)[n(2n+1) + 6(n+1)]}{6} = \frac{(n+1)(2n^2 + 7n + 6)}{6} \quad (2n+3)(n+2)$$

$$= \frac{(n+1)(2(n+1)+1)((n+1)+1)}{6}$$

$S_n^{(k)}$ è un polinomio di grado $k+1$ nella variabile n

$S_n^{(2)} = an^3 + bn^2 + cn + d$

$S_1^{(2)} = 1^2 = 1$

$S_2^{(2)} = 1^2 + 2^2 = 5$

$S_3^{(2)} = 1^2 + 2^2 + 3^2 = 14$

$S_4^{(2)} = 1^2 + 2^2 + 3^2 + 4^2 = 30$

$$\begin{cases} a+b+c+d = 1 \\ 8a+4b+2c+d = 5 \\ 27a+9b+3c+d = 14 \\ 64a+16b+4c+d = 30 \end{cases} \qquad \begin{array}{l} a = 1/3 \\ b = 1/2 \\ c = 1/6 \\ d = 0 \end{array}$$

SOMMA DEI CUBI

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

- $S_1^{(3)} = 1^3 = 1 \qquad \left(\frac{1\cdot(1+1)}{2}\right)^2 = 1^2 = 1$

$$S_{n+1}^{(3)} = S_n^{(3)} + (n+1)^3 = \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 = (n+1)^2\left[\frac{n^2}{4} + n + 1\right]$$

$$= (n+1)^2 \frac{n^2+4n+4}{4} = \frac{(n+1)^2(n+2)^2}{4} = \left(\frac{(n+1)(n+2)}{2}\right)^2$$

PROGRESSIONE GEOMETRICA $r \neq 1$

$i=1 \quad i=2 \quad i=3$

$\alpha, \alpha r, \alpha r^2, \ldots \qquad a_i = \alpha r^{i-1}$

$$S_n^{(G)} = \sum_{i=1}^{n} a_i = \alpha \frac{r^n - 1}{r - 1}$$

$$\alpha + \alpha r + \alpha r^2 + \ldots + \alpha r^{n-1} = \alpha(1 + r + r^2 + \ldots + r^{n-1})$$

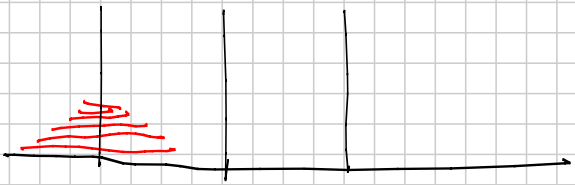
$$(r^{n+1}-1) = (r-1)(r^n + r^{n-1} + r^{n-2} + \dots + r + 1)$$

$$(r^n - 1) = (r-1)(r^{n-1} + r^{n-2} + \dots + r + 1)$$

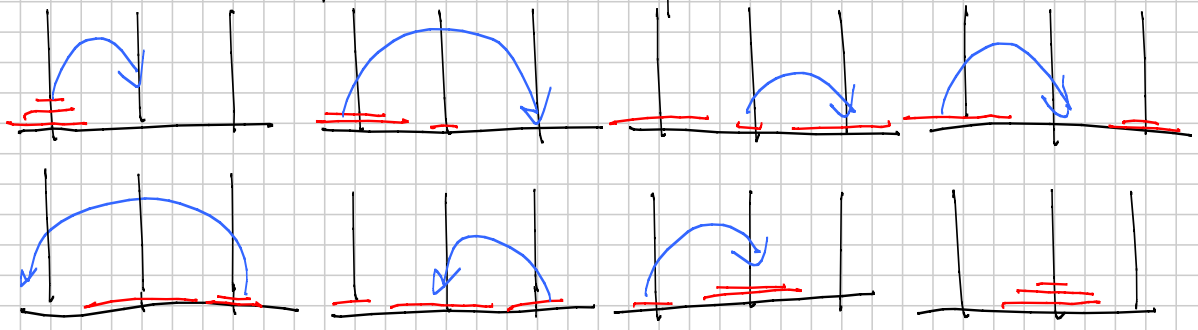
- $S_1^G = \alpha \qquad \alpha \cdot \frac{r^1 - 1}{r-1} = \alpha \frac{r-1}{r-1} = \alpha$
- $S_{n+1}^G = S_n^G + \alpha r^n = \alpha \frac{r^n - 1}{r-1} + \alpha r^n =$

$$= \alpha \frac{r^n - 1 + r^n(r-1)}{r-1} = \alpha \frac{r^{n+1} - r^n + r^n - 1}{r-1} = \alpha \frac{r^{n+1} - 1}{r-1}$$

TORRE DI HANOI



- Si può spostare 1 disco alla volta (quello superiore) da un piolo ad un altro
- Non si può mettere un disco + grande sopra uno più piccolo
- Quanto vale il numero minimo di mosse necessario per poter spostare una pila di n dischi?



$$\begin{cases} N_1 = 1 \\ N_n = 2N_{n-1} + 1 \end{cases}$$

ok

$N_1 = 2^1 - 1 = 1$

$N_1 = 1 = 2^1 - 1$

$N_2 = 3 = 2^2 - 1$

$N_3 = 7 = 2^3 - 1$

$N_4 = 15 = 2^4 - 1$

$\vdots$

$N_{n+1} = 2(2^n - 1) + 1 =$

$= 2^1 \cdot 2^n - 2 + 1 = 2^{n+1} - 1$

$N_n = 2^n - 1$?

$$f(x) = \frac{x}{x+1} \qquad x \geq 0$$

$$f(f(x)) = \frac{\frac{x}{x+1}}{\frac{x}{x+1} + 1} = \frac{\frac{x}{x+1}}{\frac{x + x + 1}{x+1}} = \frac{x}{x+1} \cdot \frac{x+1}{2x+1} =$$

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

$$f(f(f(x))) = \frac{\frac{x}{2x+1}}{\frac{x}{2x+1} + 1} = \frac{\frac{x}{2x+1}}{\frac{x + 2x + 1}{2x+1}} = \frac{x}{3x+1}$$

$$f(f(f \dots f(x) \dots)) = f^{(n)}(x) = \frac{x}{nx+1}$$

(n volte)

- $n=1$ è ovvio $\dfrac{x}{1\cdot x+1} = \dfrac{x}{x+1} = f(x)$ ↑ 1 volta ok

$$f^{(n+1)}(x) = f\left(f^{(n)}(x)\right) = \frac{\frac{x}{nx+1}}{\frac{x}{nx+1}+1} = \frac{\frac{x}{nx+1}}{\frac{x+nx+1}{nx+1}} = \frac{x}{(n+1)x+1}$$

DISEGUAGLIANZA DI BERNOULLI

$\forall x > -1 \quad \forall n \in \mathbb{N}_0 \quad (1+x)^n \geq 1+nx$

- $(1+x)^0 \geq 1+0\cdot x$

  $1 \geq 1+0$

  $1 \geq 1$ vera

$(1+x)^{n+1} = (1+x)(1+x)^n$ ($1+x > 0$)

$\geq (1+x)(1+nx) = 1+x+nx+nx^2$

$= 1+(n+1)x+nx^2 \geq 1+(n+1)x$ ($nx^2 \geq 0$)

$(1+x)^{n+1} \geq 1+(n+1)x$

INDUZIONE FORTE

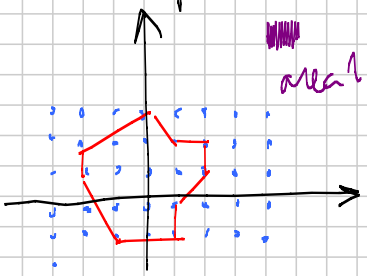
Supponiamo che un'affermazione P_n sia vera per

- tutti i valori $1, 2, 3, 4 \ldots n$ e che
- SE P_n è vera, ALLORA P_{n+1} è vera

→ P_n è vera $\forall n \in \mathbb{N}$

TEOREMA DI PICK

Supponiamo di considerare in un piano cartesiano solo i punti a coordinate intere



Se un poligono ha tutti i vertici in punti del reticolo la sua area S è data da

$$S = I + \frac{B}{2} - 1$$

I = n° di punti interni al poligono

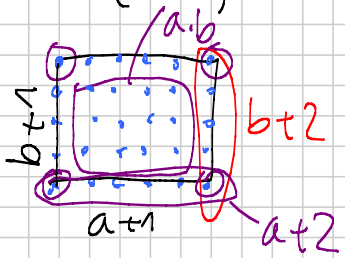
B = n° di punti sul bordo del poligono (spigoli e vertici)

Dim si dimostra a mano per i triangoli e poi si usa l'induzione forte

Rettangolo di lati di lunghezza $a+1$ e $b+1$

$S = (a+1)(b+1)$

$I = a \cdot b$



$B = 2(a+2) + 2(b+2) - 4$

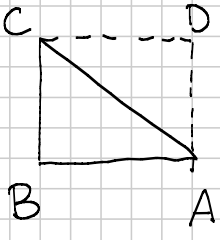
$= 2a + 2b + 4$

$$S = I + \frac{B}{2} - 1 = a \cdot b + \frac{2a+2b+4}{2} - 1 = ab + a + b + 1$$

$$= (a+1)(b+1)$$

Come si fa a vedere che funziona per un triangolo?

Tr. rettangolo coi cateti paralleli agli assi



AB ha $a+2$ punti (a senza contare gli estremi)

BC ha $b+2$ punti (b senza contare gli estremi)

AC ha $c+2$ punti (c senza contare gli estremi)

i = numero dei punti interni ad $\triangle ABC$

Quanti sono i punti interni al rettangolo

$2i + c = ab$

Quanti sono i punti di bordo di $\triangle ABC$

$$B = a+2+b+2+c+2-3 = a+b+c+3$$

$$I + \frac{B}{2} - 1 = i + \frac{a+b+c+3}{2} - 1 = \frac{\overbrace{2i+c}^{ab} + a+b+3-2}{2}$$

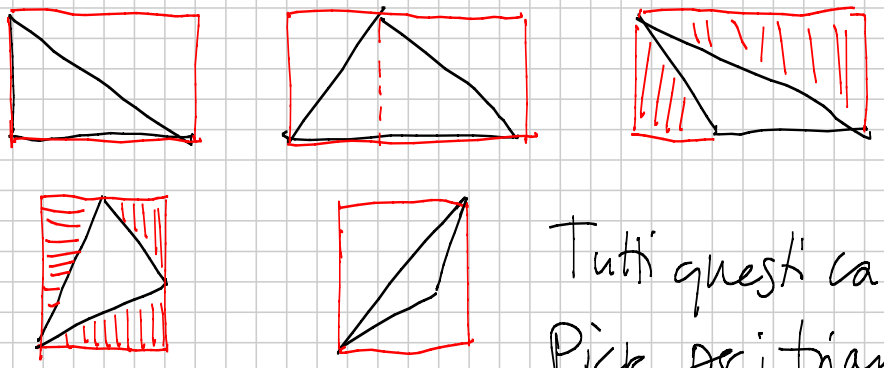
$$= \frac{ab+a+b+1}{2} = \frac{(a+1)(b+1)}{2} = \frac{S}{2}$$

Abbiamo Pick per un 

Per mostrare la validità di Pick per un triangolo qualsiasi, si divide in casi

2 lati // assi (fatto) 1 lato // assi → 2 casi

0 lati // assi (2 casi)



Tutti questi casi esauriscono Pick per i triangoli

Supponiamo che Pick sia vero per tutti i poligoni da 3 a n lati e mostriamo che è vero per poligoni con $n+1$ lati.

Si spezza il poligono P in 2 sottopoligoni che hanno ciascuno un minor numero di lati

se P è convesso basta tirare una diagonale

se P ha un angolo $> 180°$ si tracciano tutte le semirette uscenti dal vertice di quell'angolo finché non se ne trova una che batte in un vertice → ci deve essere perforza, altrimenti il poligono avrebbe area infinita

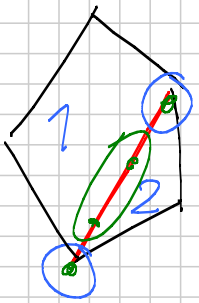
$A = A_1 + A_2$ $\qquad P_1 \cup P_2 = P$

A_1 area di P_1, A_2 area di P_2

I_1, B_1 interni e di frontiera per P_1

I_2, B_2 punti interni e di frontiera per P_2

$A_1 = I_1 + \frac{B_1}{2} - 1$ $\quad A_2 = I_2 + \frac{B_2}{2} - 1$



x = n° di punti sulla diagonale
estremi esclusi

$A_1 + A_2 = I_1 + I_2 + \frac{B_1 + B_2}{2} - 2$

$B = B_1 + B_2 - 2 - 2x$ = n° di punti di frontiera di P

$I = I_1 + I_2 + x$

$I_1 + I_2 = I - x$ $\quad B_1 + B_2 = B + 2 + 2x$

$A = A_1 + A_2 = I - x + \frac{B + 2 + 2x}{2} - 2 = I + \frac{B - 2 + 2x}{2}$

$-2 + 1 = I + \frac{B}{2} - 1$ → abbiamo Pick per
un poligono di $n+1$ lati

PRINCIPIO DEI CASSETTI

k oggetti con $k > n$

Esiste almeno un cassetto che contiene almeno due oggetti

Dimostrare che a una festa con n invitati ci sono almeno due persone che hanno dato lo stesso numero di strette di mano

n cassetti → non possono essere tutti pieni
n persone

Se è pieno il 1° cassetto, allora vuol dire che l'ultimo cassetto è vuoto e viceversa

I cassetti pieni vanno
da 0 -- a n-2 oppure
da 1 -- a n-1
quindi i cassetti pieni in tutto possono essere n-1

A questo punto scatta il principio dei cassetti.
Poiché gli invitati sono n e i cassetti sono n-1

almeno un cassetto contiene almeno due invitati
$\exists$ almeno 2 invitati che hanno dato lo stesso numero di strette di mano.

Prendiamo $n+1$ interi positivi tutti minori di $2n$
Mostriamo che ne esiste almeno uno di essi che è divisore di un altro numero di tale insieme.

$a_1, a_2 \dots a_{n+1}$

$a_1 = 2^{k_1} \cdot y_1 \quad a_2 = 2^{k_2} \cdot y_2 \dots \quad a_{n+1} = 2^{k_{n+1}} y_{n+1}$

DISPARI

$\{a_1 \dots a_{n+1}\}$

$\{y_1 \dots y_{n+1}\} \quad y_i < 2n$

$n+1$ numeri dispari $< 2n$
possono essere tutti distinti ?

$1\ 3\ 5 \dots 2n-1$
$n=1 \quad n=2 \quad n=3$
$2n=2 \quad n=4$

Devono esserci almeno 2 uguali

$i_1 \quad i_2 \qquad x_{i_1} = 2^{k_{i_1}} \cdot y_{i_1} \qquad x_{i_2} = 2^{k_{i_2}} \cdot y_{i_2}$

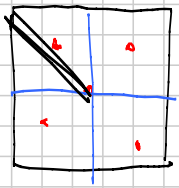
uguali

se $k_{i_1} > k_{i_2}$, x_{i_1} divide x_{i_2} $\quad 2^{k_{i_1} - k_{i_2}}$ oppure

$k_{i_2} > k_{i_2}$, x_{i_2} divide x_{i_1} $\quad 2^{k_{i_2} - k_{i_1}}$

ESEMPIO GEOMETRICO

In un quadrato di lato 1 prendiamo 5 punti. Mostriamo che ne esistono almeno 2 che distano fra loro al più $\sqrt{2}/2$



$$d_{max} = \frac{1}{2} \cdot \sqrt{2} = \frac{\sqrt{2}}{2}$$

Per il principio dei cassetti

$\exists$ almeno un quadrato che contiene almeno 2 punti $\rightarrow$ $\exists$ due punti che distano fra loro $d \leq \frac{\sqrt{2}}{2}$

SENIOR 2011 – ALGEBRA 1 (Basic)

Titolo nota 06/09/2011

NUMERI COMPLESSI

$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

$\mathbb{C} = \{ a+bi : a \in \mathbb{R}, b \in \mathbb{R} \}$ $\quad i^2 = -1$

$z = a+bi \in \mathbb{C}$, allora $a = \mathrm{Re}(z)$ $\quad b = \mathrm{Im}(z)$

Piano di Gauss: normale piano dove identifico $z = a+bi$ con il p.to di coordinate (a,b)

$z \in \mathbb{R} \iff \mathrm{Im}(z) = 0 \iff$ sta sull'asse x del piano di Gauss

Operazioni tra numeri complessi

$z = a+bi$ $\quad w = c+di$

$$z \pm w = (a+bi) \pm (c+di) = (a \pm c) + (b \pm d)\, i$$

$$z \cdot w = (a+bi)\cdot(c+di) = ac + adi + bci + dbi^2 \quad (i^2 = -1)$$
$$= (ac - db) + (ad + bc)i$$

$$\frac{w}{z} = \frac{c+di}{a+bi} \cdot \frac{a-bi}{a-bi} = \frac{ac - cbi + adi - dbi^2}{a^2+b^2} =$$

$a^2 - (bi)^2$, $a^2 + b^2$

$$= \boxed{\frac{ac+bd}{a^2+b^2}} + \boxed{\frac{ad-cb}{a^2+b^2}}\, i$$

$\mathrm{Re}\left(\frac{w}{z}\right)$ $\qquad$ $\mathrm{Im}\left(\frac{w}{z}\right)$

Oss. $\frac{w}{z}$ esiste sempre purché $z \neq 0$ $\quad (z = 0 + 0\cdot i)$

Coniugato di z Se $z = a+bi$, allora $\bar{z} = a-bi$
(simmetrico di z rispetto all'asse x)

Modulo di z Se $z = a+bi$, allora $|z| = \sqrt{a^2+b^2}$

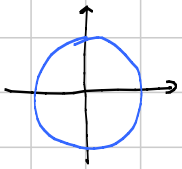
Esercizi $z\cdot\bar{z} = (a+bi)(a-bi) = a^2+b^2 = |z|^2$

$$\frac{1}{z} = \frac{\bar{z}}{|z|^2} \qquad \frac{1}{a+bi} = \frac{1}{a+bi}\,\frac{a-bi}{a-bi} = \frac{a-bi}{a^2+b^2}$$

$$\overline{z\pm w} = \bar{z}\pm\bar{w}\,, \qquad \overline{z\cdot w} = \bar{z}\cdot\bar{w}\,, \qquad \overline{\left(\frac{z}{w}\right)} = \frac{\bar{z}}{\bar{w}}$$

Quali sono tutti i complessi z t.c. $\frac{1}{z} = \bar{z}$?

$\Leftrightarrow |z| = 1 \Leftrightarrow$



$$|z\cdot w| = |z|\cdot|w|$$

Dim. Faccio i quadrati $|z\cdot w|^2 = |z|^2\cdot|w|^2$ $\quad z = a+bi$, $w = c+di$

$$(ac-bd)^2 + (ad+bc)^2 = (a^2+b^2)(c^2+d^2)$$

↑ verifica

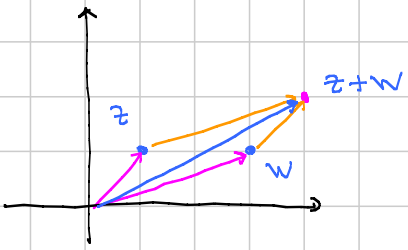
Corollario L'insieme degli interi del tipo a^2+b^2, con $a\in\mathbb{N}, b\in\mathbb{N}$ è chiuso rispetto alla moltiplicazione.

Esercizio L'insieme degli interi del tipo a^2+7b^2 con $a\in\mathbb{N}, b\in\mathbb{N}$ è chiuso rispetto alla moltiplicazione

Idea basic: $(a^2+7b^2)\cdot(c^2+7d^2) = \ldots = (\quad)^2+7(\quad)^2$

$$|a+\sqrt{7}bi|^2\cdot|c+\sqrt{7}di|^2 = |(ac-7bd)+\sqrt{7}(ad+bc)i|^2$$

Nel piano di Gauss si vedono bene somma e diff. con la regola del parallelogrammo

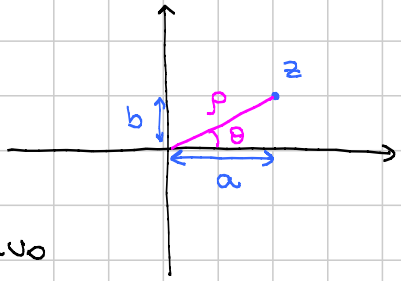


$$|z\pm w| \le |z|+|w|$$

↑ disuguaglianza triangolare

$$\left|\frac{1}{z}\right| = \frac{1}{|z|}$$

Forma trigonometrica $z = a+bi$



Per individuare z uso
- distanza ρ dall'origine $(\rho \geq 0)$
- angolo θ con il semiasse reale positivo

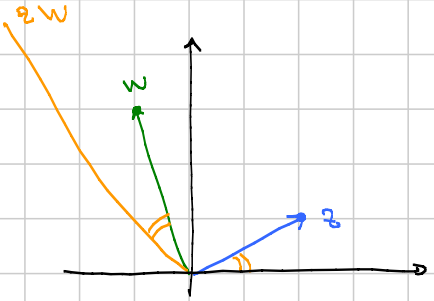
Relazioni ovvie: $\rho = |z| = \sqrt{a^2+b^2}$ $\qquad a = \rho\cos\theta \qquad b = \rho\sin\theta$

$$z = \rho\cos\theta + \rho\sin\theta\, i = \rho(\cos\theta + i\sin\theta)$$

$$z = \rho(\cos\theta + i\sin\theta) = \rho\cos\theta + i\rho\sin\theta$$
$$w = r(\cos\varphi + i\sin\varphi) = r\cos\varphi + ir\sin\varphi$$

$$z\cdot w = \rho r(\cos\theta\cos\varphi - \sin\theta\sin\varphi + i(\cos\theta\sin\varphi + \sin\theta\cos\varphi))$$
$$= \rho r(\cos(\theta+\varphi) + i\sin(\theta+\varphi))$$

ρr: modulo di $z\cdot w$ — $(\theta+\varphi)$: angolo (o argomento) del prodotto



Analogamente

$$\frac{z}{w} = \frac{\rho}{r}(\cos(\theta-\varphi) + i\sin(\theta-\varphi))$$

—o—o—

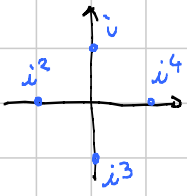
Potenza n-esima di un numero complesso

$$z = \rho(\cos\theta + i\sin\theta) \quad \Rightarrow \quad z^n = \rho^n(\cos(n\theta) + i\sin(n\theta))$$

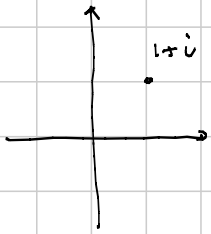
Dim.: induzione su n a partire dalla formula del prodotto.

Esercizio $(\cos\theta + i\sin\theta)^5 = \cos(5\theta) + i\sin(5\theta)$

↓ sviluppare con il binomio di Newton



Esercizio Calcolare $(1+i)^{2011}$. Passo in forma trigonometrica



$$(1+i) = \sqrt{2}\left(\cos\tfrac{\pi}{4} + i\sin\tfrac{\pi}{4}\right)$$

$$(1+i)^{2011} = (\sqrt{2})^{2011}\left(\cos\tfrac{2011}{4}\pi + i\sin\tfrac{2011}{4}\pi\right)$$

$$= 2^{1005}\sqrt{2}\left(\cos\tfrac{3}{4}\pi + i\sin\tfrac{3}{4}\pi\right) = -2^{1005} + 2^{1005}i$$

$-1+i$

Forma esponenziale: ρ e θ come nella trigonometrica

$$z = \rho \cdot e^{i\theta} \qquad w = r \cdot e^{i\varphi}$$

$$z \cdot w = \rho \cdot e^{i\theta} \cdot r \cdot e^{i\varphi} = (\rho \cdot r) \cdot e^{i(\theta+\varphi)}$$

$$\frac{1}{z} = (\rho \cdot e^{i\theta})^{-1} = \rho^{-1} \cdot e^{-i\theta}$$

Occhio: scrivere -1 in forma esponenziale: $-1 = 1 \cdot e^{i\pi}$

scrivere $-i$ in forma esponenziale: $-i = 1 \cdot e^{\frac{3\pi}{2}i}$

$$[\rho(\cos\theta + i\sin\theta)]^{-n} = \rho^{-n}(\cos(-n\theta) + i\sin(-n\theta))$$
$$= \rho^{-n}(\cos(n\theta) - i\sin(n\theta))$$

Esercizio Trovare formula per $\cos x + \cos(2x) + \dots + \cos(nx) = C$

Considero anche $i(\sin x + \sin(2x) + \dots + \sin(nx)) = iS$

$$C + iS = (\cos x + i\sin x) + (\cos(2x) + i\sin(2x)) + \dots$$
$$= z + z^2 + z^3 + \dots + z^n = z(1 + z + z^2 + \dots + z^{n-1})$$

Posto $z = \cos x + i\sin x$

$$= z\,\frac{z^n - 1}{z - 1}$$

$$C + iS = (\cos x + i \sin x)\,\frac{\cos(nx) + i\sin(nx) - 1}{\cos x + i \sin x - 1}$$

$C = \mathrm{Re}$ (Mostro)

—o—o—

Radice n-esima di un numero complesso

Dato $a \in \mathbb{C}$, trovare tutti gli $z \in \mathbb{C}$ t.c. $z^n = a$ ($n \geq 2$ intero)
Banale: se $a = 0$, allora l'unica soluzione è $z = 0$.

Teorema Se $a \neq 0$, allora esistono esattamente n numeri complessi z t.c. $z^n = a$.
Inoltre nel piano di Gauss sono i vertici di un poligono regolare di n lati con centro nell'origine.

Dim. Pongo $a = \rho(\cos\theta + i\sin\theta)$ e cerco $z = r(\cos\varphi + i\sin\varphi)$
Impongo

$$z^n = r^n(\cos(n\varphi) + i\sin(n\varphi)) = \rho(\cos\theta + i\sin\theta) = a$$

Quindi

$$\begin{cases} r^n = \rho & \text{devono avere lo stesso modulo} \\ n\varphi = \theta + 2k\pi & k \in \mathbb{Z}, \text{ stesso angolo a meno di multipli di } 2\pi \end{cases}$$

$r = \sqrt[n]{\rho}$ ← radice n-esima di un numero reale ≥ 0 (che è un unico numero reale ≥ 0)

$\varphi = \frac{\theta}{n} + \frac{2k\pi}{n}$ ← ottengo n oggetti distinti se do a k i valori $k = 0, 1, 2, \ldots, n-1$. Poi si ripete.

Esempio Calcolare le radici cubiche di $-8i$

Soluzione con la formula: $-8i$ ha $\rho = 8$ e $\theta = \frac{3\pi}{2}$

Quindi $r = \sqrt[3]{8} = 2$ $\quad \theta = \left(\frac{3\pi}{2}\right)\frac{1}{3} + \frac{2k\pi}{3}$

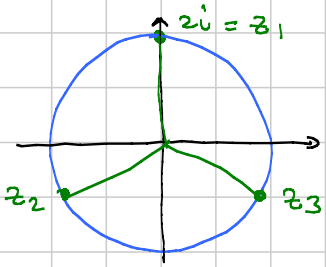
$= \frac{\pi}{2} + \frac{2k\pi}{3}$ $\quad k=0 \ \frac{\pi}{2}$ $\quad k=1 \ \frac{7\pi}{6}$ $\quad k=2 \ \frac{11\pi}{6}$

Quindi le 3 soluzioni sono $z_1 = 2\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right) = 2i$

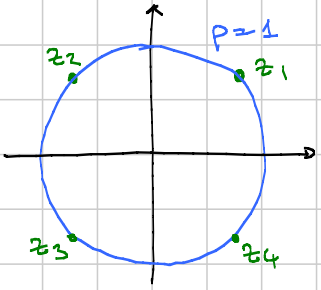
$z_2 = 2\left(\cos\frac{7\pi}{6} + i\sin\frac{7\pi}{6}\right) = -\sqrt{3} - i$

$z_3 = 2\left(\cos\frac{11\pi}{6} + i\sin\frac{11\pi}{6}\right) = \sqrt{3} - i$

Alternativa: $z^3 = -8i$. Una soluzione è $z = 2i$. Le altre due devono completare il triangolo equilatero



Esercizio $z^4 = -1$



$z_{1,2,3,4} = \frac{\sqrt{2}}{2}(\pm 1 \pm i)$

POLINOMI $\quad p(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0$

a_i = coeff. del polinomio $(\in \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C})$
Si intende che $a_k \neq 0$ e $k = \deg(p(x))$ è il grado del polinomio.

Funzione polinomiale: ad ogni x associo $p(x)$

Principio di identità dei polinomi. Se due polinomi coincidono per ogni valore di x, allora i due polinomi hanno gli stessi coefficienti.
(In realtà, per polinomi di grado $\leq k$, basta sapere che coincidono in $k+1$ valori di x).

Possibilità di assegnare $(k+1)$ valori.
Siano $x_0, x_1, \dots, x_k$ $(k+1)$ numeri reali distinti
Siano $a_0, a_1, \dots, a_k$ " " " qualunque.
Allora esiste un unico polinomio $p(x)$, a coeff. reali, di grado $\leq k$, tale che

$$p(x_i) = a_i \quad \text{per ogni } i = 0, 1, \dots, k.$$

DIM 1 Impongo le condizioni $p(x) = b_0 + b_1 x + \dots + b_k x^k$.
Le incognite sono i coeff. $b_0, b_1, \dots, b_k$.

$$\begin{cases} b_0 + x_0 b_1 + \dots + x_0^k b_k = a_0 \\ b_0 + x_1 b_1 + \dots + x_1^k b_k = a_1 \\ \dots \\ b_0 + x_k b_1 + \dots + x_k^k b_k = a_k \end{cases}$$

Sistema lineare di $k+1$ equazioni in $k+1$ incognite

Non sarebbe obbligato ad avere soluzioni, ma in questo caso lo ha perché la tabella (matrice) dei coefficienti è

$$\begin{pmatrix} 1 & x_0 & x_0^2 & \dots & x_0^k \\ 1 & x_1 & x_1^2 & \dots & x_1^k \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_k & x_k^2 & \dots & x_k^k \end{pmatrix}$$

WANDERMONDE

DIM 2 "DIVIDE ET IMPERA". Risolvo il caso in cui tutti gli a_i sono 0, tranne uno che è uguale ad 1.

WLOG: $a_0 = 1$, $a_1 = \dots = a_k = 0$

Sto chiedendo $\underbrace{p(x_1) = p(x_2) = \dots = p(x_k) = 0}_{\alpha (x-x_1)(x-x_2)\cdot\dots\cdot(x-x_k)}$ e $p(x_0) = 1$

↑ scelgo α in modo da sistemare $p(x_0) = 1$, cioè

$$\alpha = \frac{1}{(x_0-x_1)(x_0-x_2)\cdot\dots\cdot(x_0-x_k)}$$

Come si risolve il caso generale? Considero

$p_0(x)$ la soluzione con $a_0 = 1$ e gli altri nulli

⋮

$p_i(x)$ la soluzione con $a_i = 1$ e gli altri nulli.

Allora

$$a_0 p_0(x) + a_1 p_1(x) + \dots + a_k p_k(x) = p(x)$$

Il polinomio $p(x)$ così costruito vale a_i in x_i per ogni $i = 0, 1, \dots, k$ (ogni volta si annullano tutti gli addendi tranne 1)

— o — o —

Oss. La possibilità di assegnare $(k+1)$ valori vale su $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, ma non vale su $\mathbb{Z}$.

— o — o —

Divisione di polinomi Dati $A(x)$ e $B(x)$ esistono unici $Q(x)$ ed $R(x)$ t.c.

$$A(x) = B(x) \cdot Q(x) + R(x) \qquad \deg(R(x)) < \deg(B(x))$$

Dim: induzione sul grado di $A(x)$.

Oss. La divisione vale a coeff. in $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$.
Vale su $\mathbb{Z}$ se $B(x)$ è MONICO (coeff. grado max = 1)

Oss. C'è un BEZOUT sui polinomi.

Teorema di RUFFINI Se divido un certo $A(x)$ per $B(x) = (x-\alpha)$, allora $R(x)$ ha grado 0, quindi $R(x)$ è un numero, e questo numero è $A(\alpha)$.

$$A(x) = (x-\alpha)\,Q(x) + A(\alpha)$$

Corollario Se $A(\alpha) = 0$, cioè se α è una radice di $A(x)$, allora $A(x)$ è divisibile per $(x-\alpha)$, cioè resto $= 0$.

Corollario Un polinomio di grado d può avere al max d radici.

Dim. Formalmente è induzione su d. Praticamente: se avesse $d+1$ radici avrebbe $d+1$ fattori ed il grado sarebbe superiore.

Sia $P(x)$ un polinomio, e sia α una radice, cioè $P(\alpha) = 0$.
Si dice molteplicità di α il più grande esponente k t.c. $(x-\alpha)^k$ divide $P(x)$.

Detto bene: un pol. di grado d ha al più d radici, se contate con molteplicità.

Back to principio identità polinomi. Siano $P(x)$ e $Q(x)$ di grado $\leq k$. Supponiamo che coincidano in $x_0, x_1, \dots, x_k$ distinti. Allora $P(x) - Q(x)$ avrebbe $(k+1)$ radici, il che è impossibile a meno che non sia il polinomio nullo.

Teorema fondamentale dell'algebra Un polinomio di grado d a coeff. complessi ha esattamente d radici complesse, se contate con molteplicità.

Oss. Basta dimostrare che ne ha almeno una, poi è fatta.

Corollario Ogni polinomio a coeff. complessi si scrive come prodotto di fattori di 1° grado, eventualmente ripetuti

$$p(x) = a\,(x-x_1)\cdot\ldots\cdot(x-x_d)$$

$x_1, \ldots, x_d$ sono le radici complesse, ripetute con molteplicità

— o — o —

Polinomi a coeff. reali. Un pol. a coeff. reali si può sempre scrivere come prodotto di pol. a coeff. reali di grado 1 o 2 (e i fattori di grado 2 hanno $\Delta < 0$, cioè non si scompongono)

Corollario Se il grado è dispari, almeno un fattore è di grado 1, quindi c'è almeno 1 radice reale.

Idee della dim. ① Scrivo sui complessi come prod. di fattori di grado 1. I fattori corrispondenti a radici reali vanno già bene.

② Se $\alpha \in \mathbb{C}$ è radice di $P(x)$ a coeff. reali, allora $\bar{\alpha}$ è anche lei radice con la stessa molteplicità. Infatti $P(\bar{\alpha}) = \overline{P(\alpha)}$.

③ Se tra i fattori c'è $x-a-bi$ ($x-\alpha$), ci sarà anche $x-a+bi$ ($x-\bar{\alpha}$)

e $(x-a-bi)(x-a+bi) = x^2 - 2ax + (a^2+b^2)$ REALE !!!

— o — o —

Oss. Un polinomio a coeff. reali ha, per x grandi o molto negativi, lo stesso segno del termine di grado max.

POLINOMI A COEFF. INTERI

Esempio $p(x)$ a coeff. interi. So che $p(1)=3$, $p(3)=7$.
Cosa posso dire di $p(9)$?

Se $p(1)=3$, allora $p(x)-3$ ha $x=1$ come radice, quindi

$$p(x)-3=(x-1)\,q(x)$$

cioè $$p(x)=3+(x-1)\,q(x)$$

Impongo $p(3)=7$:

$$7=3+2\,q(3) \Rightarrow q(3)=2$$

Ma allora, come prima, $q(x)=2+(x-3)\,r(x)$, quindi

$$\begin{aligned} p(x) &= 3+(x-1)\{2+(x-3)\,r(x)\} \\ &= 3+2(x-1)+(x-1)(x-3)\,r(x) \\ &= 1+2x+(x-1)(x-3)\,r(x) \end{aligned}$$

Mettendo $x=9$ trovo $p(9)=19+48\,r(9)$ (intero), quindi

$$p(9)\equiv 19 \pmod{48}$$

Può essere qualunque cosa perché $r(9)$ può essere un qualunque intero.

—o—o—

Sapendo che $p(3)=2011$, cosa posso dire di $p(20)$?

$$p(x)=2011+(x-3)\,q(x) \Rightarrow p(20)=2011+17\,q(20)$$

$$\Rightarrow p(20)\equiv 2011 \pmod{17}$$

—o—o—

Fatto generale Se $P(x)$ ha coeff. interi, allora $(a-b)\mid(P(a)-P(b))$

Dim. Dato $P(a)$ ho che $P(x)=P(a)+(x-a)\,Q(x)$.
Sostituisco $x=b$ e ho che $P(b)=P(a)+(b-a)\,Q(b)$
Porto $P(a)$ dall'altra parte.

Esercizio $P(x)$ ha coeff. interi. $P(P(3)) = 3$, $P(0) = 2011$

Pongo $P(3) = a$, quindi $P(a) = 3$, quindi

$$P(x) = 3 + a - x + (x-3)(x-a)\,Q(x)$$

Metto $x = 0$

$$2011 = 3 + a + 3a\,Q(x)$$

$$2008 = a\,(1 + 3Q(x))$$

Quindi $a \mid 2008$, e $a \equiv 1 \pmod 3$

$P(1) = 1$, $P(2) = 8$, $P(3) = 27$

$$P(x) = x^3 + (x-1)(x-2)(x-3)\,Q(x)$$

RELAZIONI RADICI – COEFFICIENTI

$$P(x) = x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_1 x + a_0$$

$P(x)$ ha k radici complesse $r_1, \dots, r_k$ contate con molteplicità. Allora

$$-a_{k-1} = r_1 + r_2 + \dots + r_k = \sum_{1 \le i \le k} r_i$$

$$a_{k-2} = \sum_{1 \le i < j \le k} r_i r_j \quad \text{(somma dei prodotti a 2 a 2)}$$

$$-a_{k-3} = \sum_{1 \le i < j < l \le k} r_i r_j r_l \quad \text{(prodotti a 3 a 3)}$$

e così via fino a

$$(-1)^k a_0 = r_1 \cdot r_2 \cdot \dots \cdot r_k$$

Se non è monico, basta dividere per il coeff. di x^k e diventa monico con le stesse radici.

Esempio 1 $x^3 - 3x^2 + 7x + 5$ a, b, c radici complesse

Allora

$$S = a+b+c = 3$$
$$Q = ab+bc+ca = 7$$
$$P = abc = -5$$

Quindi fa $a^2+b^2+c^2 = (a+b+c)^2 - 2(ab+bc+ca)$
$= 3^2 - 2\cdot 7 = -5$

$\Rightarrow$ le radici sono 1 reale e 2 complesse coniugate

Teorema funzioni simmetriche Ogni polinomio simmetrico nelle variabili a, b, c si scrive come polinomio nelle variabili S, Q, P. Stessa cosa vale in k variabili usando le k funzioni simmetriche elementari (cioè quelle coinvolte nelle relazioni radici-coefficienti).

Esempio $a^2b^2+b^2c^2+c^2a^2 = (ab+bc+ca)^2 - 2(a^2bc+ab^2c+abc^2)$
$= Q^2 - 2SP.$

—o—

Dim. relazioni: segue immediatamente dalla fattorizzazione

$$(x-r_1)(x-r_2)(x-r_3) = x^3 - x^2(r_1+r_2+r_3) + x(r_1r_2+r_2r_3+r_3r_1) - r_1r_2r_3$$

—o— o —

Fatti generali $P(x) = x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_1x + a_0$

$$r_1^2 + r_2^2 + \dots + r_k^2 = [a_{k-1}]^2 - 2a_{k-2}$$
$$\frac{1}{r_1} + \frac{1}{r_2} + \dots + \frac{1}{r_k} = -\frac{a_1}{a_0}$$
$$P\left(\frac{1}{x}\right) = \frac{1}{x^k} + a_{k-1}\frac{1}{x^{k-1}} + \dots = \frac{1 + a_{k-1}x + a_{k-2}x^2 + \dots + a_1x^{k-1} + a_0x^k}{x^k}$$

Ora $\frac{1}{r_1}, \frac{1}{r_2}, \dots, \frac{1}{r_k}$ sono le radici del numeratore.

—o—o—

Radici razionali $P(x) = a_k x^k + \dots + a_0$ a coeff. interi

Se $P(x)$ ha una radice razionale del tipo $\frac{m}{n}$, allora $m \mid a_0$ e $n \mid a_k$

con $MCD(m,n)=1$

Corollario Se è monico allora le radici razionali sono per forza intere.

Dim. Brutale sostituzione

$$a_k \frac{m^k}{n^k} + a_{k-1} \frac{m^{k-1}}{n^{k-1}} + \dots + a_1 \frac{m}{n} + a_0 = 0$$

$$\frac{a_k m^k + a_{k-1} n m^{k-1} + \dots + a_1 n^{k-1} m + a_0 n^k}{n^k} = 0$$

Tutti i termini al num, tranne il 1°, sono multipli di n, quindi anche $a_k m^k$ deve esserlo, quindi $n \mid a_k$ (non potendo dividere m)
Idem per l'ultimo termine.

— o — o —

IMO 1988-4 Disequazione

$$\frac{1}{x-1} + \frac{2}{x-2} + \dots + \frac{70}{x-70} \geq \frac{5}{4}$$

L'insieme delle soluzioni è unione di intervalli di ampiezza complessiva pari a 1988.

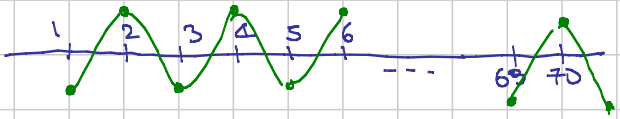
Dim. $P(x) = (x-1) \cdot \dots \cdot (x-70)$ $\quad P_i(x) = \frac{P(x)}{x-i}$

Disequazione $\Leftrightarrow$ $\frac{4[P_1(x) + 2P_2(x) + \dots + 70P_{70}(x)] - 5P(x)}{4P(x)} \geq 0$

Il numeratore ha deg = 70 con termine di grado max $= -5x^{70}$, quindi è negativo per x molto grandi e molto negativi
Inoltre
$\text{Num}(1) = 4P_1(1) = \text{neg.}$

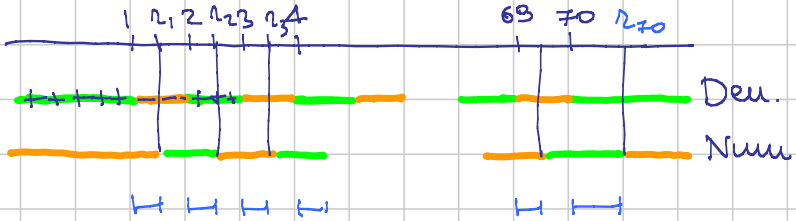
$Num(2) = 8P_2(2) = pos.$

$Num(3) = 12P_3(3) = neg.$



Quindi il numeratore ha 70 radici, tutte reali,

$r_1 < r_2 < \dots < r_{70}$ e $i < r_i < i+1$ per ogni $i = 1, \dots, 69$



La disequazione ha come soluzione l'unione dei 70 intervalli

$[i, r_i]$

quindi la lunghezza totale è $L = \sum_{i=1}^{70} (r_i - i) =$

$= \sum_{i=1}^{70} r_i - (1+2+\dots+70)$

Per calcolare $\sum r_i$, mi servono i coeff. di x^{70} e x^{69} nel num.

$Num = -5x^{70} + \underbrace{4x^{69}(1+2+\dots+70)}_{\text{viene fuori dai } P_i(x)} + \underbrace{5x^{69}(1+2+\dots+70)}_{\text{viene fuori da } P(x)}$

$\sum_{i=1}^{70} r_i = \frac{9}{5}(1+2+\dots+70)$

$L = \left(\frac{9}{5} - 1\right)(1+2+\dots+70) = \frac{4}{5} \cdot 71 \cdot 35 = 1988$!!!

— o — o —

IMO 1974 – 6 $P(x)$ a coeff. interi di grado d.
Allora $[P(x)]^2 = 1$ ha al max $d+2$ soluzioni distinte intere

$P(x) = 1$ oppure $P(x) = -1$ Quindi le sol. sono al max $2d$

Quindi ok banalmente per $d = 1$ e per $d = 2$.

Lemma Se esistono 4 interi distinti tali che
$P(a) = P(b) = P(c) = P(d) = 1$
allora $P(x) = -1$ non ha soluzioni intere

Dim. Pongo $Q(x) = P(x) - 1$. Allora
$$P(x) - 1 = Q(x) = (x-a)(x-b)(x-c)(x-d)R(x)$$
Supponiamo che $P(e) = -1$. Allora ponendo $x = e$

$$-2 = \underbrace{(e-a)(e-b)}_{\text{potrebbero essere } \pm 1}(e-c)(e-d)\underbrace{R(e)}_{\text{potrebbe essere } 1}$$

-2 non può essere divisibile per il prodotto di 4 interi distinti

Dato il lemma si divide il problema. Se $d \geq 4$ e avessi più di $d+2$ soluzioni, ne avrei almeno 7, quindi almeno 4 pti in cui vale $+1$ o vale -1. Quindi vale addirittura con d invece di $d+2$. Il caso $d = 3$ si fa a mano con la fattorizzazione.

—o—o—

Lemma $P(x)$ a coeff. interi. Considero
$$P^{(k)}(x) = P(P(P(\dots))) \quad k \text{ volte}$$

Sia x intero. Allora $P^{(k)}(x) = x \Rightarrow P(P(x)) = x$.
(se si torna indietro in k passaggi, allora o si è stati fermi sempre, o si torna indietro ogni 2 passaggi).

Dim. Si usa ripetutamente $a - b \mid P(a) - P(b)$

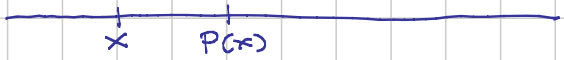
$$a-b \mid P(a)-P(b) \mid P(P(a))-P(P(b)) \mid \dots$$

La uso con $a = P(x)$ e $b = x$

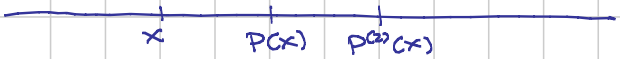
$P(x)-x \mid P(P(x))-P(x) \mid \dots \mid P^{(k+1)}(x)-P^{(k)}(x)$

$P(x) \quad - \quad x$

Quindi tutte le differenze sono uguali a meno del segno



$P^{(2)}(x)$ può essere x (e siamo a posto) o dall'altra parte.
Per assurdo sia dall'altra parte



Ogni volta faccio avanti o indietro della stessa quantità e dopo k passaggi torno in x

Se voglio tornare ad x devo fare un passo da $P(x)$ ad x.
La regola di passaggio è sempre la stessa, quindi da $P(x)$ non si può andare una volta avanti e una indietro

(From IMO 2006-5 : Se $P(x)$ ha grado d, allora
$P^{(k)}(x) = x$ ha al più d radici)

Sui complessi avrebbe d^k soluzioni, perché $\deg(P^{(k)}) = d^k$
Grazie al lemma ci si riduce a d^2 soluzioni.

— o — o —

A2 - BASIC DISUGUAGLIANZE (un po' di)

Titolo nota 08/09/2011

1) Medie
2) Riarrangiamento
3) Cauchy - Schwarz
4) Convessità

1. Medie

$$A(x_1, \dots, x_n) = \frac{1}{n} \sum_{i=1}^{n} x_i$$

$$G(x_1 \cdots x_n) = \sqrt[n]{x_1 \cdot \dots \cdot x_n}$$

$$Q(x_1 \cdots x_n) = \sqrt{\frac{\sum_i x_i^2}{n}}$$

- omogeneità $\lambda > 0$

$$A(\lambda x_1, \dots, \lambda x_n) = \lambda A(x_1 \cdots x_n)$$

idem per le altre

$$M_p(x_1, \dots, x_n) = \sqrt[p]{\frac{1}{n} \sum_{i=1}^{n} x_i^p}$$

$$H(x_1, \dots, x_n) = M_{-1}(x_1 \cdots x_n) = \left[\frac{1}{n} \left(\frac{1}{x_1} + \cdots + \frac{1}{x_n} \right) \right]^{-1}$$

$$= \frac{n}{\frac{1}{x_1} + \cdots + \frac{1}{x_n}}$$

$x_1, \dots, x_n \geq 0$

$M_{-1}(x_i)$ (H) $M_0(x_i)$ (G) $M_1(x_i)$ (A) $M_2(x_i)$ (Q) (P) $M_p(x_i)$

$H(x_i) \leq G(x_i) \leq A(x_i) \leq Q(x_i) \leq M_p(x_i)$

$=: M_0(x_i)$

ok $\min(x_i) =: M_{-\infty}(x_i)$

$p \geq 2$ in ok

$M_{+\infty}(x_i) = \max(x_i)$

e se vale anche una sola $=$

allora $x_1 = x_2 = \dots = x_n$

- omogeneità (cosa succede se $x_i \to \lambda x_i$)
- ottimalità ($\exists$? casi di $=$)
- caratterizzazione dei casi di $=$

Come si ricordano?

(P)

$p < q \Rightarrow M_p(x_i) \leq M_q(x_i)$

Studio qualitativo di una disuguaglianza in p per $p \to$ valore

Per esempio, fissati $x_1, \dots, x_n > 0$

si può mostrare che $M_p(x_i) \xrightarrow[p\to\infty]{} \max(x_i)$

$\Rightarrow$

SIGNIFICA: fissati gli x_i si può rendere $M_p(x_i)$ vicino quanto vogliamo a $\max(x_i)$ per di prendere p abbastanza grande ($p \gg 0$)

es $\sqrt[p]{\frac{x^p+y^p}{2}} \xrightarrow{p\gg 0} X$

Supp. $X > y > 0$

$X \sqrt[p]{\frac{1+(y/x)^p}{2}}$ si avvicina a X quando $p \gg 0$

$(y/x)^p \to 0$ perché $y/x < 1$

$\frac{1+0}{2} \to \frac{1}{2}$

$\sqrt[p]{\frac{1}{2}} \to 1$

Analogamente potete provare a mostrare:

$$M_p(x_i) \xrightarrow[p \to 0^+]{} G(x_i)$$

$$M_p(x_i) \xrightarrow[p \to +\infty]{} \min(x_i)$$

(da fare per esercizio).

Tutte le disuguaglianze tra medie seguono da:

(R) RIARRANGIAMENTO
(CS) CAUCHY-SCHWARZ
(C) CONVESSITÀ

(R) DISUGUAGLIANZA DI RIARRANGIAMENTO

Siano $a_1 \le a_2 \le \dots \le a_n$ e $b_1 \le b_2 \le \dots \le b_n$

Sia $\sigma: \begin{pmatrix} 1 \\ \vdots \\ n \end{pmatrix} \to \begin{pmatrix} \sigma(1) \\ \vdots \\ \sigma(n) \end{pmatrix}$

Allora: $\sum_{i=1}^{n} a_i b_{n+1-i} \le \sum_{i=1}^{n} a_i b_{\sigma(i)} \le \sum_{i=1}^{n} a_i b_i$

Cosa succede nel caso di $=$? Caratterizzazione?

* dimostrazione di (R)

Supp. che σ sia la permutazione per la quale si ottiene il massimo M

$M = a_1 b_{\sigma(1)} + \dots + a_i b_{\sigma(i)} + \dots + a_j b_{\sigma(j)} + \dots + a_n b_{\sigma(n)}$

$a_1 b_{\sigma(1)} + \dots + a_i b_{\sigma(j)} + \dots + a_j b_{\sigma(i)} + \dots + a_n b_{\sigma(n)}$

se $\sigma \neq id$

$\exists\, i < j$

$\sigma(i) > \sigma(j)$

$a_i (b_{\sigma(i)} - b_{\sigma(j)}) + a_j (b_{\sigma(j)} - b_{\sigma(i)}) \ge 0$

$(a_i - a_j)(b_{\sigma(i)} - b_{\sigma(j)}) \ge 0$

$(a_i - a_j)(b_{\sigma(i)} - b_{\sigma(j)}) \geq 0$

≤ 0 $\quad$ ≥ 0

l'unica possibilità è che dia 0

$a_i = a_j$ $\qquad$ $b_{\sigma(i)} = b_{\sigma(j)}$

Morale (1) se gli a_i $\uparrow$, b_i $\uparrow$ strettamente crescenti

la permutazione σ che dà il numero è id

(2) se gli a_i $\uparrow$, b_i $\uparrow$ debolmente crescenti

$\Downarrow$

σ è una permutazione che può scambiare $i \hookrightarrow j$ solo se $a_i = a_j$

ex

1	2	2	3	4	$= (a_i)$
5	6	7	8	8	$= (b_i)$

1	2	2	4	3
5	7	6	8	8

Applicazioni – esempi di (R)

1) a, b, c qualsiasi

$$ab + bc + ca \leq a^2 + b^2 + c^2$$

$(a\ b\ c)$

$(b\ c\ a)\ (a\ b\ c)$

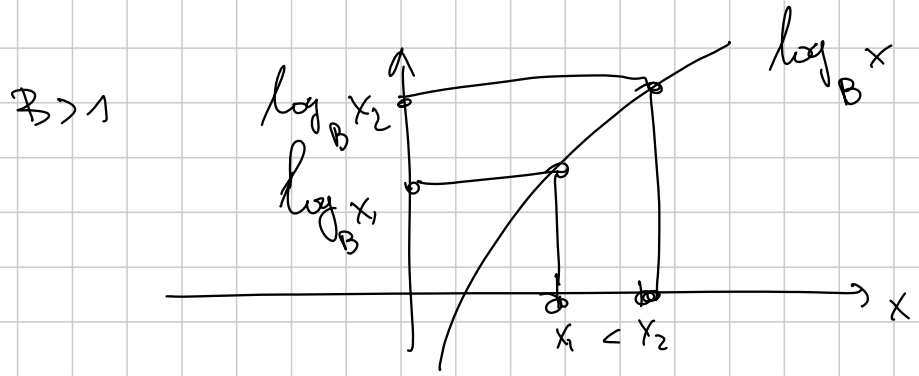
2) a, b, c positivi

$$a^a \cdot b^b \cdot c^c \geq a^b\ b^c\ c^a$$

$a \log a + b \log b + c \log c$ $\quad b \log a + c \log b + a \log c$

$a, b, c \nearrow \Rightarrow \log a, \log b, \log c \nearrow$

$\boxed{B>1}$ $\log_B x$ è il numero a cui deve essere elevato B per ottenere x



3) Somma di quozienti ciclici

$a_1, a_2, \dots, a_n$ positivi

(non necessariamente ≥ 1)

$$\frac{a_1}{a_2} + \frac{a_2}{a_3} + \frac{a_3}{a_4} + \dots + \frac{a_n}{a_1} \geq n$$

$a_1 \quad \dots \quad a_n$ non ordinati

$1/a_1 \quad \dots \quad 1/a_n$ non ordinati

Se σ è l'ordinamento decrescente degli a_i

$$a_{\sigma(1)} \leq a_{\sigma(2)} \leq \dots \leq a_{\sigma(n)}$$

$$\frac{1}{a_{\sigma(1)}} \geq \frac{1}{a_{\sigma(2)}} \geq \dots \geq \frac{1}{a_{\sigma(n)}}$$

$$\sum_{i=1}^{n} a_i / a_{i+1} \geq \underbrace{1 + \dots + 1}_{n} = n$$

Altro modo di farla:

se $0 \le a_1 \le a_2 \le \dots \le a_n$

allora $a_1/a_{\sigma(1)} + \dots + a_n/a_{\sigma(n)} \ge n$

$\forall$ permutazione σ

4) $G(x_1, \dots, x_n) \le A(x_1, \dots, x_n)$

$x_1, \dots, x_n$ positivi

$G_i = G(x_i)$

$a_1 = G/x_1$

$a_2 = G^2/x_1x_2$

$\vdots$

$a_n = G^n/x_1 \cdots x_n = 1$

Non ne conosco l'ordinamento

$a_i \le a_{i+1}$?

$\Rightarrow \dfrac{G^i}{x_1 \cdots x_i} \le \dfrac{G^{i+1}}{x_1 \cdots x_{i+1}}$

$\Leftrightarrow x_{i+1} \le G$

$a_1/a_2 + a_2/a_3 + \dots + a_n/a_1 \ge n$

$a_i / a_{i+1} = x_{i+1} / G$

$a_n / a_1 = x_1 / G$

$x_2/G + x_3/G + \dots + x_1/G \geq n$

$\frac{1}{n} \sum_{i=1}^{n} x_i \geq G$

Dimostriamo che se $G(x_i) = A(x_i) \Rightarrow x_1 = x_2 = \dots x_n$
(il caso di uguaglianza) $\leq$
Con un'altra tecnica.

Caso $n=2$ $\quad \sqrt{xy} \leq \frac{x+y}{2}$

e vale = se e solo se $x=y$

infatti $0 \leq (x-y)^2 = x^2 + y^2 - 2xy$

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

$+2xy \qquad +2xy$

$(x+y)^2 \geq 4xy$

$\frac{x+y}{2} \geq \sqrt{xy}$

vale = se $(x-y)^2 = 0$ i.e. $x=y$

caso n qualsiasi

Supponiamo $\sqrt[n]{x_1 \cdot \dots \cdot x_n} \overset{(\leq)}{=} \frac{x_1 + x_2 + \dots + x_n}{n}$

se gli x_i non sono tutti uguali

avremo $x_1 \neq x_2$

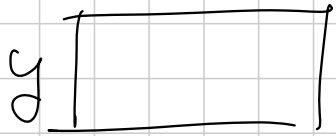
Allora chiamo $x_i' = x_i \quad i \neq 1,2$

x_1', x_2' t.c. $\begin{cases} x_1' x_2' = x_1 x_2 \\ x_1' + x_2' < x_1 + x_2 \end{cases}$

OSS la disuguaglianza $G(x,y) \leq A(x,y)$ fatta per $n=2$

ci dice che $\min\{x+y \mid xy = c\}$

è ottenuto per $x = y = \sqrt{c}$



cioè tra tutti i rettangoli di area $xy = c$ fissata

il quadrato è quello che minimizza il perimetro

$$\frac{x+y}{2} \geq \sqrt{xy} = \sqrt{c}$$

$$x + y \geq 2\sqrt{c}$$

ed è minima per $x = y = \sqrt{c}$

perché è un'uguaglianza

Ora però trovo:

$$\sqrt[n]{x_1 \cdot \dots \cdot x_n} = \sqrt[n]{x_1' \cdot \dots \cdot x_n'} \leq \frac{x_1' + \dots + x_n'}{n} \leq \frac{x_1 + \dots + x_n}{n}$$

assurdo gli x_i non verificavano l'ug. $G(x_i) = A(x_i)$.

EX. (Chebychëff) Mostrare:

$a_1 \leq a_2 \leq \dots \leq a_n$ qualsiasi

$b_1 \leq b_2 \leq \dots \leq b_n$

$$\Rightarrow \frac{1}{n}\sum_{i=1}^{n} a_i b_{n+1-i} \leq \left(\frac{1}{n}\sum_{i=1}^{n} a_i\right)\left(\frac{1}{n}\sum_{i=1}^{n} b_i\right) \leq \frac{1}{n}\sum_{i=1}^{n} a_i b_i$$

$$A(a_i b_{n+1-i}) \leq A(a_i)A(b_i) \leq A(a_i b_i)$$

Suggerimento $\sum_{i,j} a_i b_j$

$$\left(\frac{\sum a_i}{n}\right)\left(\frac{\sum b_i}{n}\right) = \frac{1}{n^2}\sum_{i,j} a_i b_j \leq \frac{1}{n^2}\cdot n \sum a_i b_n$$

$$a_1 b_1 + a_2 b_2 + \dots + a_n b_n = \sum a_i b_n$$
$$a_1 b_2 + a_2 b_3 + \dots + a_n b_1 \leq \sum a_i b_n$$
$$a_1 b_3 + \dots + a_n b_2 \leq$$
$$\vdots$$
$$a_1 b_n + \dots + a_n b_{n-1} \leq$$

EX. Calcolare $\text{MIN}\{x+2y+3z \mid x^3y^2z = 1\}$ con $x,y,z>0$

Somma di a_i — prodotto

con $\sum a_i \sim x+2y+3z$

$\prod a_i \sim x^3y^2z$

$a_1 = x$, $a_2 = y$, $a_3 = 3z$

$\sum a_i = ok$

$\prod a_i = x \cdot y \cdot 3z \neq x^3y^2z$

$$x+2y+3z = \frac{x}{3}+\frac{x}{3}+\frac{x}{3}+y+y+3z \quad (6)$$

$$\prod a_i = x^3y^2z \cdot \left(\frac{1}{3^3}\cdot \dots \cdot 3\right) \quad \leftarrow a_i$$

$$\frac{x+2y+3z}{6} \geq \sqrt[6]{\frac{1}{9}\underbrace{x^3y^2z}_{=1}} = \frac{1}{3\sqrt{3}}$$

$=$

Se $\frac{x}{3} = y = 3z$ t.c. $x^3y^2z = 1$

$x = 3y$, $z = y/3$, $y = ?$ $\quad (3y)^3 y^2 \left(\frac{y}{3}\right) = 1$

$\downarrow$ y

il minimo è $1/3\sqrt{3} \cdot 6$

EX Calcolare $\min\{x^2+y^4+z^6 \mid xyz = n\}$ $\quad x,y,z > 0$, n fissato

Sugg trovare a_i t.c. $\sum a_i \sim x^2+y^4+z^6$

$\prod a_i \sim (xyz)^\alpha$

3) Cauchy–Schwarz

$x_1, \dots, x_n$ qualsiasi

$y_1, \dots, y_n$

$$\Rightarrow \quad |x_1 y_1 + \dots + x_n y_n| \le \left(\sum_{i=1}^{n} x_i^2\right)^{1/2} \left(\sum_{i=1}^{n} y_i^2\right)^{1/2}$$

$$(x_1 y_1 + \dots + x_n y_n)^2 \le \left(\sum x_i^2\right)\left(\sum y_i^2\right)$$

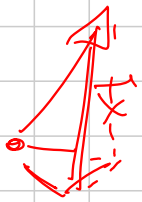
$\vec{X} = (x_1, \dots, x_n)$

$\vec{Y} = (y_1, \dots, y_n)$

$\vec{X} \cdot \vec{Y} = x_1 y_1 + \dots + x_n y_n$ PRODOTTO SCALARE

$|\vec{X}| = \sqrt{\sum x_i^2}$ NORMA O LUNGHEZZA DI $\vec{X}$

se $\vec{X} = (x_1, x_2, x_3)$



$$|\vec{X} \cdot \vec{Y}| \le |\vec{X}| \cdot |\vec{Y}|$$

Vale l'$=$ se e solo se $\vec{X} = \lambda \vec{Y}$

cioè $\exists \lambda \in \mathbb{R}$ t.c. $x_i = \lambda y_i$

oppure $y_1 = y_2 = \dots = y_n = 0$

* dimostrazione (tramite somma di quadrati)

$$\left(\sum_i a_i^2\right)\left(\sum_i b_i^2\right) - \left(\sum_i a_i b_i\right)^2 \geq 0 \quad ?$$

$$\sum_{i,j} a_i^2 b_j^2 - \sum_i a_i^2 b_i^2 - \sum_{i \neq j} a_i b_i a_j b_j \geq 0 \quad ?$$

$$\sum_{i \neq j} a_i^2 b_j^2 + \sum_{i \neq j} a_i^2 b_j^2$$

$$\sum_{i \neq j} (a_i b_j - a_j b_i)^2 \quad \overset{?}{\geq} 0$$

Vale l'= $\Rightarrow$ $a_i b_j = a_j b_i \quad \forall i,j$ diciamo

Graficamente $a_i / b_i = a_j / b_j = \lambda \quad \forall i,j$

cioè $a_i = \lambda b_i \quad \forall i$

Scrivendo bene:

- se $b_i = 0 \ \forall i \rightarrow \vec{b} = 0$ ok
- se $\exists b_i \neq 0$: $b_j = 0 \rightarrow a_j = 0$

  $b_j \neq 0 \rightarrow \frac{a_i}{b_i} = \frac{a_j}{b_j}$ ¶

Significato geometrico di Cauchy-Schwarz:

(almeno per $n=2,3$)

legge del coseno $|\vec{x}\cdot\vec{y}| = |\,|\vec{x}|\,|\vec{y}|\cos\vartheta\,|$

lunghezza col segno della proiezione di $\vec{y}$ su $\vec{x}$

Cosa vol dire se ho $=$?

$\vec{y} \parallel \vec{x}$

$\leq |\vec{x}|\,|\vec{y}|$.

Applicazione di Cauchy-Schwarz

1) $A(x_1 \dots x_n) \leq Q(x_1, \dots x_n)$

applico Cauchy-Schwarz a $\vec{x} = (x_1, \dots x_n)$

$\vec{y} = \vec{1} = (1, \dots, 1)$

$$\left(\sum_i x_i\right)^2 = \left(\sum_i x_i \cdot 1\right)^2 \leq \sum_{i=1}^n x_i^2 \cdot \underbrace{\sum_{i=1}^n 1^2}_{n}$$

$/n^2$

$$\frac{1}{n^2}\left(\sum_1^n x_i\right)^2 \leq \frac{1}{n}\sum x_i^2$$

$$\underbrace{\frac{1}{n}\sum_1^n x_i}_{A(x_i)} \leq \underbrace{\sqrt{\frac{\sum x_i^2}{n}}}_{Q(x_i)}$$

Vale $=$? $\iff x_1 = x_2 = \dots = x_n$.

Ex. Mostrare:

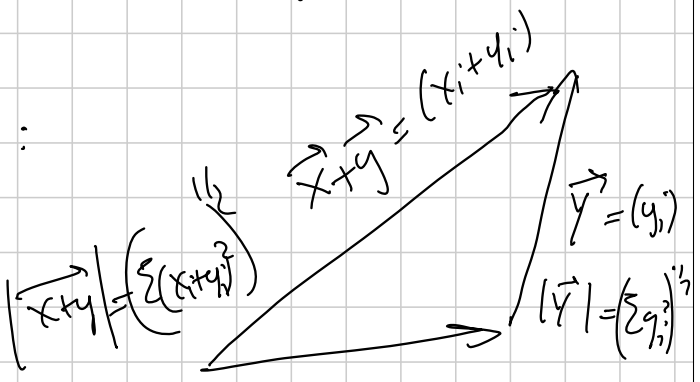
$$\sqrt{\sum_{i=1}^{n}(x_i+y_i)^2} \leq \sqrt{\sum_{i=1}^{n} x_i^2} + \sqrt{\sum_{i=1}^{n} y_i^2}$$

(Minkowsky o triangolare) $p=2$

Suggerimento: usare Cauchy-Schwarz

Significato geometrico:

$n=2,3$

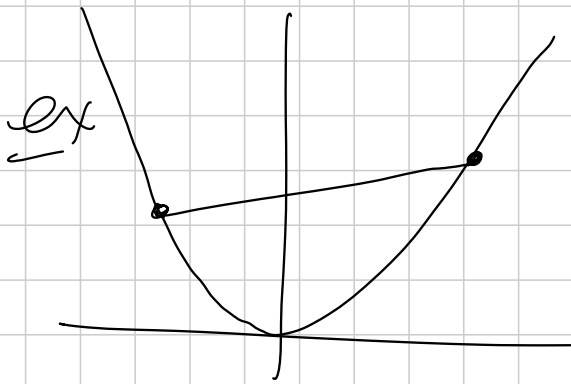


$\vec{x}=(x_i)$

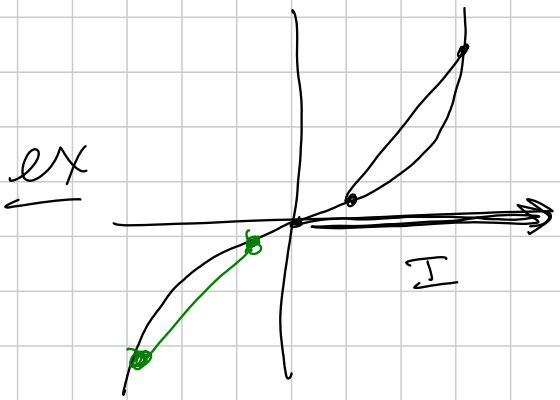
$|\vec{x}|=\left(\sum x_i^2\right)^{1/2}$

4) DISUGUAGLIANZE DI CONVESSITÀ

def. Una funzione f si dice CONVESSA (CONCAVA) in un certo intervallo I se il segmento che congiunge due qualsiasi punti del grafico di f in I sta AL DI SOPRA (AL DI SOTTO) del grafico

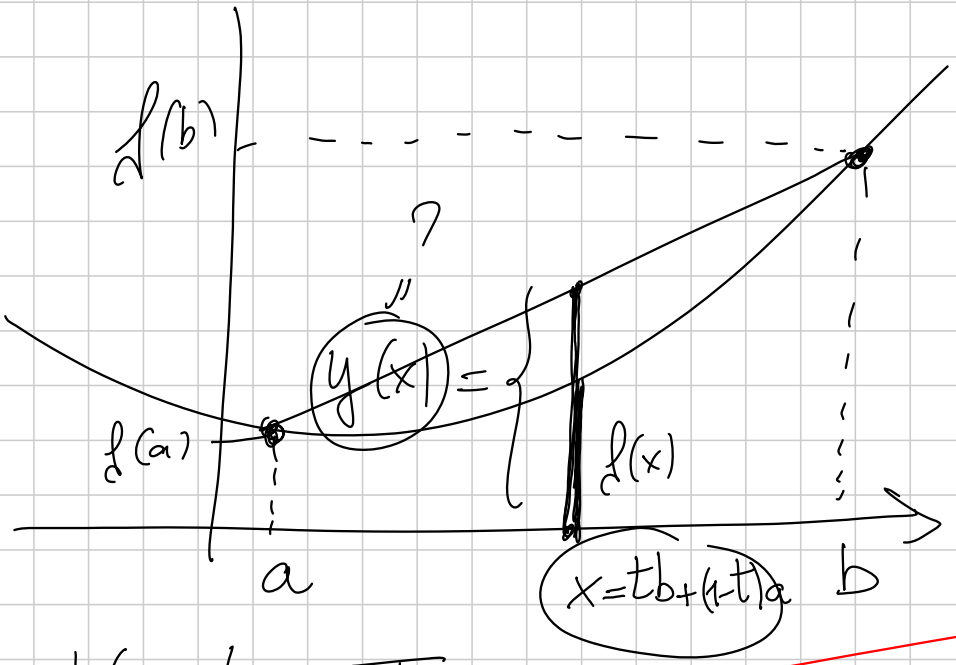


$f(x) = x^2$ è convessa in $I = \mathbb{R}$



$f(x) = x^3$ è convessa in $\mathbb{R}_+$
è concava in $\mathbb{R}_-$

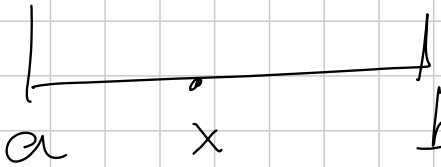
Come si scrive analiticamente la condizione di convessità di f in I



$\forall a, b \in I$ e $\forall x \in (a,b)$ ho $\boxed{y(x) \geq f(x)}$?

$x = tb + (1-t)a$

dove $t \in [0,1]$



$x = a + t(b-a) = tb + (1-t)a$

$0 < t < 1$

retta r passante per $(a, f(a))$ e $(b, f(b))$:

$$r: \quad \frac{y - f(a)}{x - a} = \frac{f(b) - f(a)}{b - a}$$

$$y(x) = \left[\frac{f(b) - f(a)}{b - a}\right](x - a) + f(a)$$

$x \to tb + (1-t)a$

$$= \left(\frac{f(b) - f(a)}{b - a}\right)\underbrace{\left(tb + (1-t)a - a\right)}_{t(b-a)} + f(a)$$

$$= \left(f(b) - f(a)\right)t + f(a)$$

$$= t f(b) + (1-t) f(a)$$

Convessità di f in I:

$$f(tb + (1-t)a) \leq t f(b) + (1-t) f(a)$$

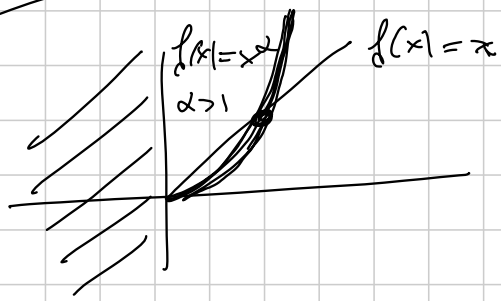
$\forall a, b \in I$ e $\forall t \in [0,1]$

Cosa dentra tutto ciò con le disuguaglianze?

ogni volta che ho f convessa e $t \in [0,1]$

$\rightsquigarrow$ disuguaglianza

ex: $f(x) = x^\alpha \quad \alpha > 1 \quad I = \mathbb{R}_+$



f convessa se $\alpha > 1$ in $\mathbb{R}_+$

$t = \frac{1}{2} \in (0,1)$

$$f\left(\frac{1}{2}a + \frac{1}{2}b\right) \leq \frac{1}{2}f(a) + \frac{1}{2}f(b)$$

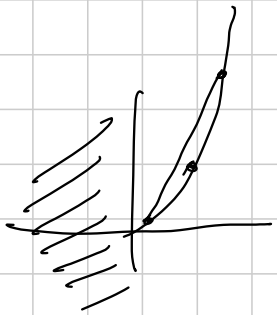
$$\frac{1}{2^\alpha}(a+b)^\alpha \leq \frac{1}{2}(a^\alpha + b^\alpha)$$

$$A(a,b) = \frac{a+b}{2} \leq \sqrt[\alpha]{\frac{a^\alpha + b^\alpha}{2}} = M_\alpha(a,b)$$

$$M_p(a_1,\dots,a_n) \le M_q(a_1,\dots,a_n)$$

$$p<q$$

Lo faccio per $n=2$:



prendo $f(x) = x^{(q/p)} \geq 1$

Convessa in $I = \mathbb{R}_+$

applico la dis di Convessità

per $t=\frac{1}{2}$ e ad x_1^p, x_2^p

$$f\left(\frac{1}{2}(x_1^p+x_2^p)\right) \le \frac{1}{2}\left(f(x_1^p)+f(x_2^p)\right)$$

$$\left(\frac{x_1^p+x_2^p}{2}\right)^{q/p} \le \frac{1}{2}\left((x_1^p)^{q/p}+(x_2^p)^{q/p}\right)$$

prendo $\sqrt[q]{\ }$

$$\left(\frac{x_1^p+x_2^p}{2}\right)^{1/p} \le \left(\frac{x_1^q+x_2^q}{2}\right)^{1/q}$$

Come si trovano le funzioni convesse (CONCAVE)?

(i) $f(tx+(1-t)y) \overset{(\leq)}{\leq} tf(x)+(1-t)f(y)$

$\forall t \in [0,1]$, $\forall x, y \in I$

(ii) [Se f è continua] $f\left(\frac{x+y}{2}\right) \overset{(\leq)}{\leq} \frac{1}{2}\left(f(x)+f(y)\right)$

(iii) [se f ha derivate seconde] $f''(x) \geq 0$ su I $(\leq)$

(IV) [Jensen, $\times$ induzione da (i)]

se ho $d_1, \dots, d_n \in [0,1]$

$\sum_i d_i = 1$

pensare a $\frac{1}{2}, \frac{1}{2}$ $t, (1-t)$ $\frac{1}{3}, \frac{2}{3}$

$f(d_1x_1+\dots+d_nx_n) \overset{(\leq)}{\leq} d_1f(x_1)+\dots+d_nf(x_n)$

$\forall x_1, \dots, x_n \in I$

tutte condizioni eq. alla convessità

ex $f(x) = x^\alpha$ $\quad \alpha > 1$

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

$f''(x) = \alpha(\alpha-1) x^{\alpha-2} > 0 \quad x \in \mathbb{R}_+$

$\longrightarrow$ f è convessa

ex $M_p(x_1, \dots, x_n) \le M_q(x_1, \dots, x_n)$ $\quad p < q$

applico la (iv) a $f(x) = x^{q/p}$

e ai pesi $\lambda_1 = 1/n, \dots, \lambda_n = 1/n$

e a $x_1^p, \dots, x_n^p$

$$f\left(\frac{1}{n}(x_1^p + \dots + x_n^p)\right) \le \frac{1}{n}\left[f(x_1^p) + \dots + f(x_n^p)\right]$$

$$\left(\frac{x_1^p + \dots + x_n^p}{n}\right)^{q/p} \le \frac{(x_1^p)^{q/p} + \dots + (x_n^p)^{q/p}}{n}$$

prendo $\sqrt[q]{\ }$ $\rightsquigarrow$ $M_p \le M_q$.

ex (YOUNG) $\boxed{AB \le \frac{1}{p}A^p + \frac{1}{q}B^q}$

per $A, B > 0$

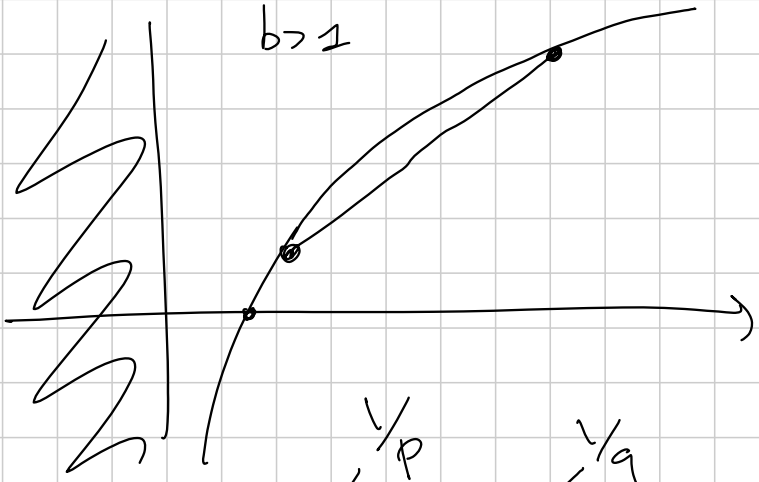
$\frac{1}{p} + \frac{1}{q} = 1$

$p, q > 0$

Sugg $f(x) = \log_b x$ è CONCAVA

$b > 1$

$\left(f''(x) = -\frac{1}{x^2} < 0 \right)$



$\log\left(ta + (1-t)b\right) \ge t\log a + (1-t)\log b$ ($a^{1/p}$, $b^{1/q}$, $t = \frac{1}{p}$)

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

$a = A^p$, $b = B^q$

$\log\left(\frac{1}{p}A^p + \frac{1}{q}B^q\right) \ge \frac{1}{p}p\log A + \frac{1}{q}q\log B = \log AB$

abbiamo detto

f STRETTAMENTE convessa su I se vale

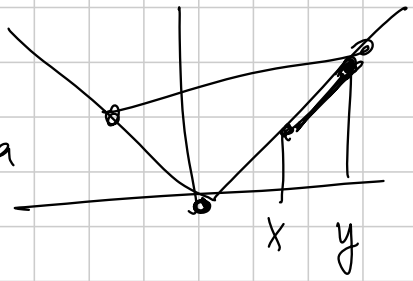
$$f(tx+(1-t)y) < tf(x)+(1-t)f(y)$$

$t \in [0,1]$ $\quad x, y \in I$

$t \in (0,1)$

Es f convessa non strettam. convessa

$f(x) = |x|$



EX Dimostrare che:

$x_1, \dots, x_n \geq 0$

$\sum_i x_i = 1$

$$\Rightarrow \sum_{i=1}^{n} \frac{x_i}{\sqrt{1-x_i}} \geq \sqrt{\frac{n}{n-1}}$$

$$f(x) = \frac{x}{\sqrt{1-x}}$$

$$\frac{1}{n} f(x_1) + \dots + \frac{1}{n} f(x_n) \geq f\left(\frac{x_1+\dots+x_n}{n}\right) = f\left(\frac{1}{n}\right)$$

A3 Basic - Successioni e funzioni

Titolo nota 09/09/2011

$\sum_{i=1}^{n} i^k = P_{k+1}(n)$ $\quad i^k = P_{k+1}(i) - P_{k+1}(i-1) =$

$= \left(i^{k+1} + \dots\right) - \left((i-1)^{k+1} + \dots\right)$

Equazioni alle differenze finite

$P_5(x) = 3x^5 - 2x^3 + x^2 + x - 3$

Progressione aritmetica : $x_n = x_0 + nr$

$\begin{cases} x_n = x_{n-1} + r \\ x_0 \text{ dato} \end{cases}$ $\quad x_n - x_{n-1} = r$

$\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} (x_0 + ir) =$

$= \sum_{i=1}^{n} x_0 + \sum_{i=1}^{n} ir = nx_0 + r \cdot \frac{n(n+1)}{2}$

Progressione geometrica: $x_n = x_0 \cdot r^n$

$\begin{cases} x_n = r\, x_{n-1} \\ x_0 \text{ dato} \end{cases}$ $\quad \log x_n = \log x_{n-1} + \log r$

$\log x_n = \log x_0 + n \log r$

$x_n = x_0 \cdot r^n$

$x_n = a\, x_{n-1} + b$ $\quad y_n = x_n - x_{n-1}$

$x_{n-1} = a\, x_{n-2} + b$

$x_n - x_{n-1} = a(x_{n-1} - x_{n-2})$ $\qquad y_n = a y_{n-1}$

$y_n = y_0 \cdot a^n$ $\qquad x_n - x_{n-1} = y_0 \cdot a^n$

$+ \qquad +$

$x_{n-1} - x_{n-2} = y_0 \cdot a^{n-1}$

$x_n - x_{n-2} = y_0(a^n + a^{n-1})$

$x_n - x_0 = y_0(a^n + a^{n-1} + \dots + a^1)$

$1 + a + a^2 + a^3 + \dots + a^n = \frac{a^{n+1} - 1}{a - 1}$ $\qquad a \neq 1$ $\qquad a(1 + a + \dots + a^{n-1})$

$x_n = x_0 + a y_0 \cdot \frac{a^n - 1}{a - 1}$

b_0, b_1 dati

$b_{n+1} = (n+1) b_n - n b_{n-1}$

Allora $\forall m$ naturale da un certo $\bar{k}$ in poi $b_n \equiv k \pmod m$ $\quad n \geq \bar{k}$

$b_{n+1} - b_n = n(b_n - b_{n-1})$

$c_{n+1} = b_{n+1} - b_n \qquad c_{n+1} = n c_n \qquad c_n = a \cdot (n-1)!$

$c_1 = b_1 - b_0 = a$

$b_{n+1} = b_n + c_{n+1} = b_n + a\, n!$ Se $n \geq m$,

$m \mid n!$

$b_{n+1} = a_1 b_n + a_2 b_{n-1} + \gamma$

$b_n \longmapsto c_n = b_n - s \qquad b_n = c_n + s$

$c_{n+1} + s = a_1 c_n + a_1 s + a_2 c_{n-1} + a_2 s + \gamma$

$s = (a_1 + a_2) s + \gamma \qquad s = \dfrac{\gamma}{1 - a_1 - a_2}$

✳ $\boxed{b_{n+1} = a_1 b_n + a_2 b_{n-1}}$ Ricorrenza a due termini

1) E' lineare : B_n e β_n sono soluzioni, anche λB_n e $B_n + \beta_n$ sono soluzioni.

$B_{n+1} = a_1 B_n + a_2 B_{n-1}$

$\beta_{n+1} = a_1 \beta_n + a_2 \beta_{n-1}$

$(B_{n+1} + \beta_{n+1}) = a_1 (B_n + \beta_n) + a_2 (B_{n-1} + \beta_{n-1})$

✳ ha soluzioni che sono progressioni geometriche?

$F_0 = 0 \quad F_1 = 1 \qquad F_{n+1} = F_n + F_{n-1}$

0 1 1 2 3 5 8 13 21 34 55 89

Se $x_0 r^n$ soddisfa $(*)$

$x_0 r^{n+1} = a_1 x_0 r^n + a_2 x_0 r^{n-1}$ $\quad x_0 = 0$ oppure $r = 0$ oppure $r, x_0 \neq 0$

$r^2 - a_1 r - a_2 = 0$

Trovo r_1 e r_2 soluzioni di

$x_0 r_1^n$ e $x_0 r_2^n$ sono soluzioni

qualunque sia x_0, quindi

$\alpha r_1^n + \beta r_2^n$ è soluzione $\forall \alpha, \beta \in \mathbb{R}$.

Si può dimostrare che sono tutte così,

purché $r_1 \neq r_2$.

Se $r_1 = r_2$ anche $n r_1^n$ è soluzione:

$x^2 - 2r_1 x + r_1^2 = 0$ $\qquad b_{n+1} = 2r_1 b_n - r_1^2 b_{n-1}$

$(n+1) r_1^{n+1} = 2r_1 \cdot n r_1^n - r_1^2 \cdot (n-1) r_1^{n-1}$

$n+1 = 2n - (n-1)$.

Le soluzioni (tutte) sono allora del tipo

$\alpha r_1^n + \beta n r_1^n$

$x^2 - x - 1 = 0$ $\quad F_{n+1} = F_n + F_{n-1}$

$r_1 = \frac{1+\sqrt{5}}{2}$ $\quad r_2 = \frac{1-\sqrt{5}}{2}$ $\quad r_1 + r_2 = 1$

$r_1^2 + r_2^2 \qquad \frac{1+2\sqrt{5}+5}{4} + \frac{1-2\sqrt{5}+5}{4}$

$\alpha r_1^n + \beta r_2^n = F_n$

$\begin{cases} \alpha + \beta = 0 \\ \alpha r_1 + \beta r_2 = 1 \end{cases} \qquad \alpha = -\beta \qquad \alpha = \frac{1}{r_1 - r_2}$

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

$$F_3 = \frac{1}{\sqrt{5}} \left(\frac{1+3\sqrt{5}+15+5\sqrt{5}}{8} - \frac{1-3\sqrt{5}+15-5\sqrt{5}}{8} \right) = 2$$

$a_0 > 0$

$a_{n+1} = 3a_n - 2a_{n-1}; \; a_1 - a_0 > 1$ $\quad$ Allora $a_{100} > 2^{99}$

$x^2 - 3x + 2 = 0 \qquad 2, 1$

$a_n = \alpha \cdot 2^n + \beta \qquad (2\alpha + \beta) - (\alpha + \beta) > 1$

$\alpha > 1$

$a_{100} = \alpha \cdot 2^{100} + \beta$

$\alpha \cdot 2^{99} + \alpha \cdot 2^{99} + \beta \qquad \alpha \cdot 2^{99} + \beta > \alpha + \beta > 0$

$a_{n+1} - a_n = 2(a_n - a_{n-1})$ $\quad a_{100} - a_{99} = 2^{99}(a_1 - a_0)$

$a_{99} > 0$ perché se $a_0 \geq 0$ e $a_1 - a_0 \geq 1$

$0 < a_0 < a_1 < a_2 < \dots < a_{99}$

$b_1 \; b_2 \; b_3 \; \dots \; b_n$

In quanti modi possono disporsi in modo che distino al più 1 passo dalla posizione iniziale?

$N_k \quad N_1 = 1 \quad N_2 = 2 \quad N_3 = 3$

1 2 3
2 1 3
1 3 2

$N_4 = 5$

1 2 3 4
1 3 2 4
1 2 4 3
2 1 3 4
2 1 4 3

$M_k = \{\text{modi per } k \text{ bambini}\}$

$M_k = A_k \cup B_k \quad A_k = \{b_1 \text{ resta fermo}\}$

$B_k = \{b_1 \text{ e } b_2 \text{ si scambiano}\}$

$|A_k| = |M_{k-1}| = N_{k-1} \quad |B_k| = |M_{k-2}| = N_{k-2}$

$N_k = N_{k-1} + N_{k-2} \quad N_1 = 1 \quad N_2 = 2$

$$\begin{cases} b_{n+1} = b_n + b_{n-1} \\ b_0 = 3 \\ b_1 = 2 \end{cases}$$

3 2 5 7 12 19 31

$$r_1 = \frac{1+\sqrt{5}}{2} \qquad r_2 = \frac{1-\sqrt{5}}{2}$$

$$|r_2| < 1$$

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n \pm \varepsilon$$

$[\alpha^n]$ $\lambda\bar{\alpha}^n + \mu\alpha^n$

$p \mid 2^n + 3^n + 6^n - 1^n$ n grande, p primo

b_n

$(x+1)(x+2)(x-3)(x-6)$

b_n è soluzione $b_{n+4} = c_1 b_n + c_2 b_{n-1} + c_3 b_{n-2} + c_4 b_{n-3}$

$b_0\ b_1\ b_2\ b_3$ mod p ci sono p^4 possibilità

$b_0 b_1 b_2 b_3\ b_4 b_5 b_6 \ldots$

La quaterna $b_0 b_1 b_2 b_3$ prima o poi si ripete mod p

$n = -1$ $\quad 2^{-1} + 3^{-1} + 6^{-1} - 1^{(-1)}$ $\quad p \neq 2,3$

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

$18+12+6=36$

$b_{-1} = 0 \mod p$

Allora se il periodo è lungo N,

$b_{N-1} \equiv 0 \mod p$.

Equazioni funzionali

L'incognita è una funzione $f: A \to B$

$\mathbb{N}$ $\mathbb{Z}$ $\mathbb{Q}$ $\mathbb{R}$ $(0, +\infty)$

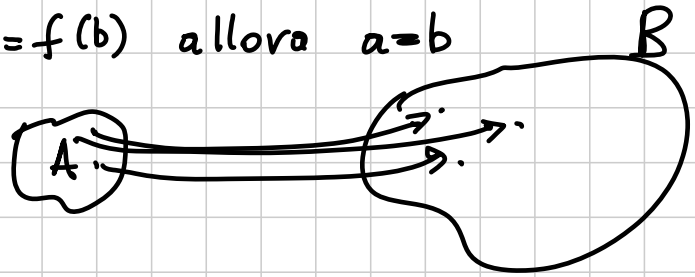
funzione $\neq$ formula

$f(n) = \{$numero delle persone con n capelli$\}$

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

$f: A \to B$ iniettiva $\doteq$

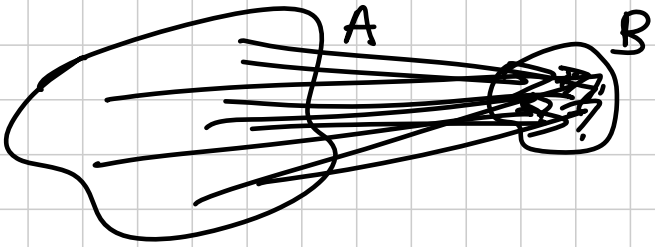
Se $f(a) = f(b)$ allora $a = b$



$f: A \to B$ è surgettiva $\doteq$

$\forall b \in B \ \exists a \in A$ t.c. $f(a) = b$

(anche più di uno)



Se $|A|$ e $|B|$ sono finiti,

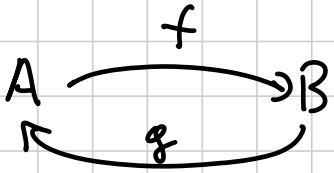
f iniettiva $\Rightarrow |A| \leq |B|$

f surgettiva $\Rightarrow |A| \geq |B|$

f iniettiva e surgettiva $\Rightarrow$ biiettiva
biunivoca

In questo caso $\exists\, g : B \to A$ t.c.

se $f(a) = b \Rightarrow g(b) = a$



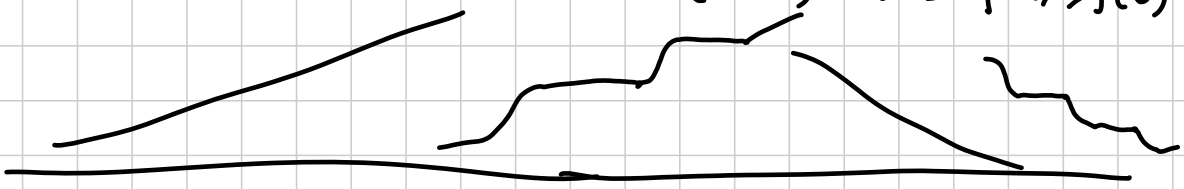
f monotòna

monotona strett. crescente $a<b$ $f(a)<f(b)$

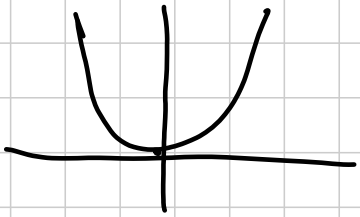
" crescente (debolmente) $a<b$ $f(a)\leq f(b)$

monotona strett. decrescente $a<b$ $f(a)>f(b)$

" decrescente (deb.) $a<b$ $f(a)\geq f(b)$



x^2 su $\mathbb{R}$



Su $\mathbb{R}^+$ è crescente (strett.)
su $\mathbb{R}^-$ decrescente (strett.)

- divido in casi
- mi serve solo uno dei due

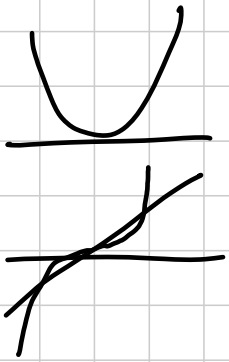
f periodica $\exists k$ t.c. $f(x+k)=f(x)$ $\forall x$

Il più piccolo k che soddisfa la condizione è detto periodo (minimo) di f

(0 f costante)

f pari $f(x)=f(-x)$

f dispari $f(x)=-f(-x)$

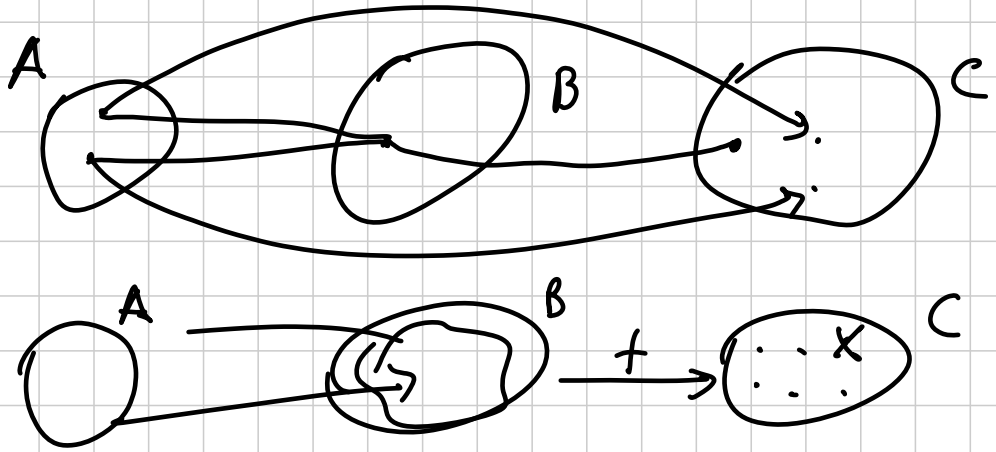


$f \circ g$ $A \xrightarrow{g} B \xrightarrow{f} C$

$f \circ g : A \longrightarrow C$
$x \longmapsto f(g(x))$

$f \circ g$ iniettiva $\Rightarrow$ g iniettiva

$f \circ g$ surgettiva $\Rightarrow$ f surgettiva



$f(f(x)) = x$ su $\mathbb{R}$

f è iniettiva e surgettiva

$x = f(z)$ $\qquad f(f(f(f(z)))) = f(z)$

$f(f(f(z))) = f(z)$

$f(f(z)) = z$

$f(x) = x$
$f(x) = -x$

x	$f(x)$
a	b

$f(a) = b$ $\qquad f(f(a)) = a$
$f(b) = a$ $\qquad f(f(b)) = b$

$\mathbb{R} = \bigcup_i \{a_1^i\ a_2^i\}$ $\qquad f(a_1^i) = a_2^i$ $\quad f(a_2^i) = a_1^i$.

Eq. di Cauchy :

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

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

1) $f(0)$ $\quad$ $f(0+0) = f(0) + f(0)$ $\quad$ $f(0) = 0$.

2) $f(0+1) = f(0) + f(1)$

$f(1+1) = f(1) + f(1) = 2f(1)$

$f(3) = f(2+1) = 2f(1) + f(1) = 3f(1)$,

$f(n) = f(n-1) + f(1) = (n-1)f(1) + f(1) = nf(1)$.

↑ Induzione

$f(-1)$ $\quad$ $f(-1+1) = f(-1) + f(1)$

$f(-1) = -f(1)$

$f(-n) = -f(n)$ $\quad$ $f(x) + f(-x) = f(x-x) = 0$

$f(x) = -f(-x)$

f è dispari

$n \in \mathbb{Z}$ $\quad$ $f(n) = nf(1)$

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

$f\left(\frac{1}{2}\right) = \frac{1}{2}f(1)$

$f\left(\frac{m}{n}\right) = \frac{m}{n} f(1)$ [Induzione]

2) $f(1) = a$ $\quad f(x) = ax$ $\quad a \in \mathbb{Q}$ $\quad a \in \mathbb{R}$

$a(x+y) = ax + ay$

Su $\mathbb{Q}$ è finita

Su $\mathbb{R}$ che si fa con $\sqrt{2}$? con π?

$f(1) = a = 2$

$f(\sqrt{2}) = \pi$ $\quad f(m\sqrt{2}) = m\pi$ $\quad f\left(\frac{m}{n}\sqrt{2}\right) = \frac{m}{n}\pi$

$\sqrt{3}$ $\quad \pi\sqrt{e}$ $\quad \log\left(\frac{e+\pi}{\sqrt{2}}\right)$ ....

Su $\mathbb{R}$ ∄ tantissime soluzioni

a meno che...

- f monotòna crescente o decrescente
- f continua
- f localmente limitata: ∃ intervallino $[a,b]$ su cui $|f| \leq K$.

$\Longrightarrow f(x) = ax \quad \forall x \in \mathbb{R}$.

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

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

(1) $f(f(0)) = f(0)$ $\qquad f(0) = 0$? NO

$f(f(y)) = f(0) + y$

$f(0) + y$ è bigettiva, quindi anche f lo è (grazie al suo doppio ruolo in $f(f(y))$). Quindi $f(0) = 0$ per (1)

$f(f(y)) = y$

$x = f(z)$

$f(f(z) + f(y)) = f(f(z)) + y = z + y$

$y = f(z)$

$f(x + f(f(z))) = f(x) + f(z)$

$f(x + z)$ (1)

$\Rightarrow f(x) = ax$

$a(x + ay) = ax + y \qquad ax + a^2 y = ax + y \quad \forall x, y$

$a^2 = 1 \qquad a = \pm 1$

1) $f(x) = x$
2) $f(x) = -x$

1) $x + y = x + y$ ✓
2) $-(x - y) = -x + y$ ✓

IMO 2008 - 4

Trovare tutte le $f:(0,+\infty)\to(0,+\infty)$

t.c. $\dfrac{[f(w)]^2+[f(x)]^2}{f(y^2)+f(z^2)} = \dfrac{w^2+x^2}{y^2+z^2}$ $\forall x,y,z,w \in (0,+\infty)$ t.c. $xw=yz$

$x=y=z=w=1$

$\dfrac{2f(1)^2}{2f(1)} = 1$ $\qquad f(1)^2 = f(1)$ $\qquad f(1)=1$

$x=1$
$y=w$
$w=w$
$z=1$

$\dfrac{f(w)^2+1}{f(w^2)+1} = \dfrac{w^2+1}{w^2+1} = 1$

$f(w)^2 = f(w^2)$

$x^2:(0,+\infty)\circlearrowleft$ è biiettiva

$\dfrac{f(w^2)+f(x^2)}{f(y^2)+f(z^2)} = \dfrac{w^2+x^2}{y^2+z^2}$

$(*)$ $\dfrac{f(w)+f(x)}{f(y)+f(z)} = \dfrac{w+x}{y+z}$ $\qquad \forall x,y,z,w \in (0,+\infty)$ $xw=yz$

$x=w$
$y=w^2$
$z=1$
$w=w$

$\dfrac{2f(w)}{f(w^2)+1} = \dfrac{2w}{w^2+1}$ $\qquad f(w^2)=f(w)^2$

$2(w^2+1)f(w) = 2w + 2w f(w)^2$

$f(w)^2 - 2\dfrac{w^2+1}{2w} f(w) + 1 = 0$ $\qquad f(w) = \begin{cases} w \\ \dfrac{1}{w} \end{cases}$

2 soluz.?

$$\frac{f(w)+f(x)}{f(y)+f(z)} = \frac{w+x}{y+z} \qquad f(x)=x \ \checkmark \qquad f(x)=\frac{1}{x}$$

$$\frac{\frac{1}{w}+\frac{1}{x}}{\frac{1}{y}+\frac{1}{z}} = \frac{\frac{w+x}{wx}}{\frac{y+z}{yz}}$$

E' possibile che $f(a)=\frac{1}{a}$ $f(b)=b$ $a,b \neq 1$?

$w=a$ $x=b$ $y=ab$ $z=1$ $\qquad \frac{\frac{1}{a}+b}{f(ab)+1} = \frac{a+b}{ab+1}$

$$f(ab)=\begin{cases} ab & 1) \\ \frac{1}{ab} & 2) \end{cases}$$

1) $\frac{\frac{1}{a}+b}{ab+1} = \frac{a+b}{ab+1}$ $\quad \frac{1}{a}=a$ $\quad a^2=1$ $\quad a=1$ ans.

2) $\frac{\frac{1}{a}+b}{\frac{1}{ab}+1} = \frac{a+b}{ab+1}$

$\frac{\frac{1+ab}{a}}{\frac{ab+1}{ab}} = b = \frac{a+b}{ab+1}$ $\quad ab^2+b = a+b$ $\quad b^2=1$ $\quad b=1$ ans.

Non esistono 2 punti con soluzioni diverse

quindi
- $f(x)=x \quad \forall x$
- $f(x)=\frac{1}{x} \quad \forall x$

(e loro soddisfano).

TST 2002 : Trovare tutte le $f:(0,+\infty)\to(0,+\infty)$ t.c.

1) $f(x+yf(x))=f(x)f(y)$
2) assumono il valore 1 al più un numero finito di volte.

$f(t)=1 \quad f(2t)$

$x=t, y\neq t \quad f(t+tf(t))=f(t)f(t)=1$

$f(2t)$

$f(t+2tf(t))=f(2t)f(t)=1$

$f(3t)$ Induzione: allora $\exists$ infiniti t_i t.c. $f(t_i)=1$ [i.t.] ass.

$y=x$; $x=y$

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

$f(a)=f(b) \quad a\neq b \quad a<b \qquad x=a \quad y=\frac{b-a}{f(a)}$

$f\left(a+\frac{b-a}{f(a)}\cdot f(a)\right)=f(a)\cdot f\left(\frac{b-a}{f(a)}\right) \qquad f\left(\frac{b-a}{f(a)}\right)=1$ ass.

$f(b)$ "

Allora f è iniettiva e

$x+yf(x)=y+xf(y) \qquad y(f(x)-1)=x(f(y)-1)$

$\frac{f(x)-1}{x}=\frac{f(y)-1}{y}=a \;\forall x,y. \qquad \frac{f(x)-1}{x}=a \;\forall x$

$f(x)=ax+1. \qquad a>0$

$a\left(x+y\cdot(ax+1)\right)+1=(ax+1)(ay+1)$

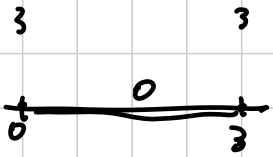
$ax+a^2xy+ay+1=a^2xy+ax+ay+1$ □.

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

$f(x+3f(y))=f(x)+ay$

i) per $a=0$ $\mathbb{R}$ esiste una sol. non costante.

periodo 3



1) $x=3k$, $y=3k$

2) $x=3k$, y no

3) x no, $y=3k$

4) x,y no

1) $f(3k+3\cdot 3)=f(3k)$ $\quad$ 2) $f(3k+3\cdot 0)=f(3k)$

3) $f(x+3\cdot 3)=f(x)$ $\quad$ 4) $f(x+3\cdot 0)=f(x)$

$x=0$ $\quad f(3f(y))=f(0)+ay$ $\quad$ f biiettiva

$x=y=0$ $\quad f(3f(0))=f(0) \Rightarrow 3f(0)=0 \quad f(0)=0$

$$f(3f(y))=ay$$

$f(x+9f(y))$?

$x=x+3f(y)$ $\quad f(x+3f(y)+3f(y))=f(x+3f(y))+ay$

$=f(x)+ay+ay$

$x+6f(y)$

$$f(x+9f(y))=f(x)+3ay$$

$y=3f(z)$

$f(x+3f(3f(z)))=f(x)+3af(z)$

$x=0$

$f(3az)=3af(z)$

$f(x+3az)$ x $\quad$ $y=f(z)$

$$f(x+9f(f(z)))=f(x)+3af(z)$$

$\cancel{x} + 9f(f(z)) = \cancel{x} + 3f(3f(z))$ $\quad 3f(f(z)) = f(3f(z))$

$\cancel{x} + 3az \qquad\qquad \| \; az$

$f(f(z)) = \frac{a}{3}z$

$f(3f(y)) = ay \qquad f\left(3f\left(\frac{z}{3}\right)\right) = \frac{a}{3}z$

$f(z) = 3f\left(\frac{z}{3}\right)$

$f(3az) = \cancel{3}af(z)$

$\cancel{3}f(az)$

$f(x + 3f(y)) = f(x) + ay \qquad f(3y) = z$

$f(x + f(3y))$

$f(f(z)) = \frac{a}{3}z$

$f(x+z) = f(x) + \frac{a}{3}3y =$ $\quad z = 3y$

$= f(x) + \frac{\cancel{a}}{\cancel{3}} f(f(3y)) =$

$= f(x) + f(z).$

E' un'equazione di Cauchy!

su $\mathbb{Q}$ $\quad f(x) = \lambda x$

$\lambda(x + 3\cdot\lambda y) = \lambda x + ay \qquad \forall x, y \in \mathbb{R}$

$\lambda x + 3\lambda^2 y \qquad 3\lambda^2 = a$

$\mathbb{Q} \quad a = 57^{57} \quad 3^{57}\cdot 19^{57}$ no

$a = 75^{75} \quad 3^{75}\cdot 5^{150}$ sì $\qquad$ (E).

$\mathbb{R} \quad a \geq 0$ ✓

COMBINATORIA 1

Titolo nota 06/09/2011

Principi sciocchi.

1) Principio di equivalenza
se e'è corrisp. Biunivoca tra A e B
$|A| = |B|$

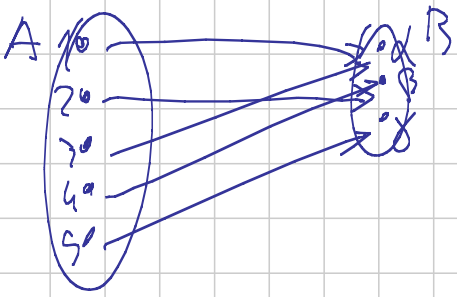
2) Principio della somma
se $A \cap B = \emptyset$ $|A \cup B| = |A| + |B|$

3) Principio del prodotto
$|A \times B| = |A| \times |B|$

Esempio $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$

$(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \dots \cdot (\alpha_k + 1)$

Ultimo come semi-sciocco
Ci sono 3 modi (almeno)
di provare una formula
1) modo con freccette



2) modo con parole

Esempio: α β α β γ

rappresenta funzione di prima

3) occupazione di B da parte di A

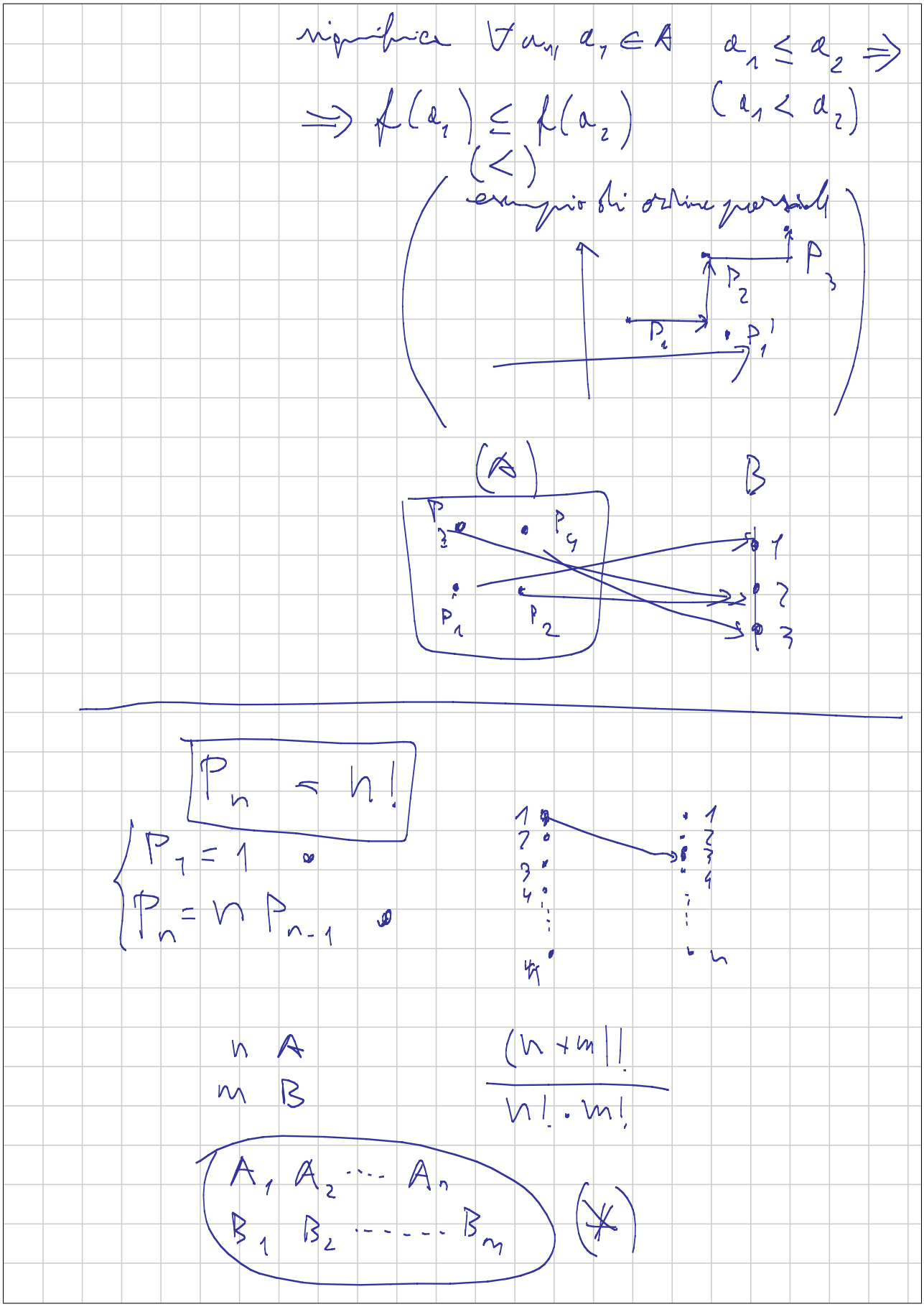
1, 3	2, 4	5
α	β	γ

Nomenclatura : $f: A \to B$

1) **iniettiva** $\forall a_1, a_2 \in A \quad a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$

2) **suriettiva** $\forall b \in B \ \exists a \in A$ t.c. $f(a) = b$

3) Se A e B sono insiemi totalmente ordinati, f crescente (debolmente) (strettamente)


significa $\forall a_1, a_2 \in A \quad a_1 \leq a_2 \Rightarrow$
$\Rightarrow f(a_1) \leq f(a_2)$
$(a_1 < a_2)$
$(<)$
esempio di ordine parziale
P_3
P_2
P_1
P_1'
(A)
B
P_3
P_4
P_1
P_2
1
2
3
$P_n = n!$
$P_1 = 1$
$P_n = n P_{n-1}$
1
2
3
4
n
n A
m B
$\frac{(n+m)!}{n! \cdot m!}$
$A_1, A_2 \cdots A_n$
$B_1, B_2 \cdots B_m$
(*)

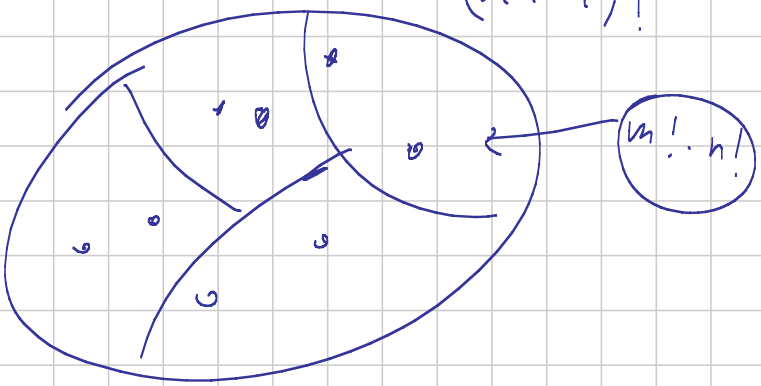
$(n+m)!$

Se P_1 P_2 non vanno fatte contatti i vicini (*)

$P_1 \approx P_2 \iff$ cancellando gli inizi sono uguali.

A_1 B_1 A_2 B_2 A_3

$(n+m)!$



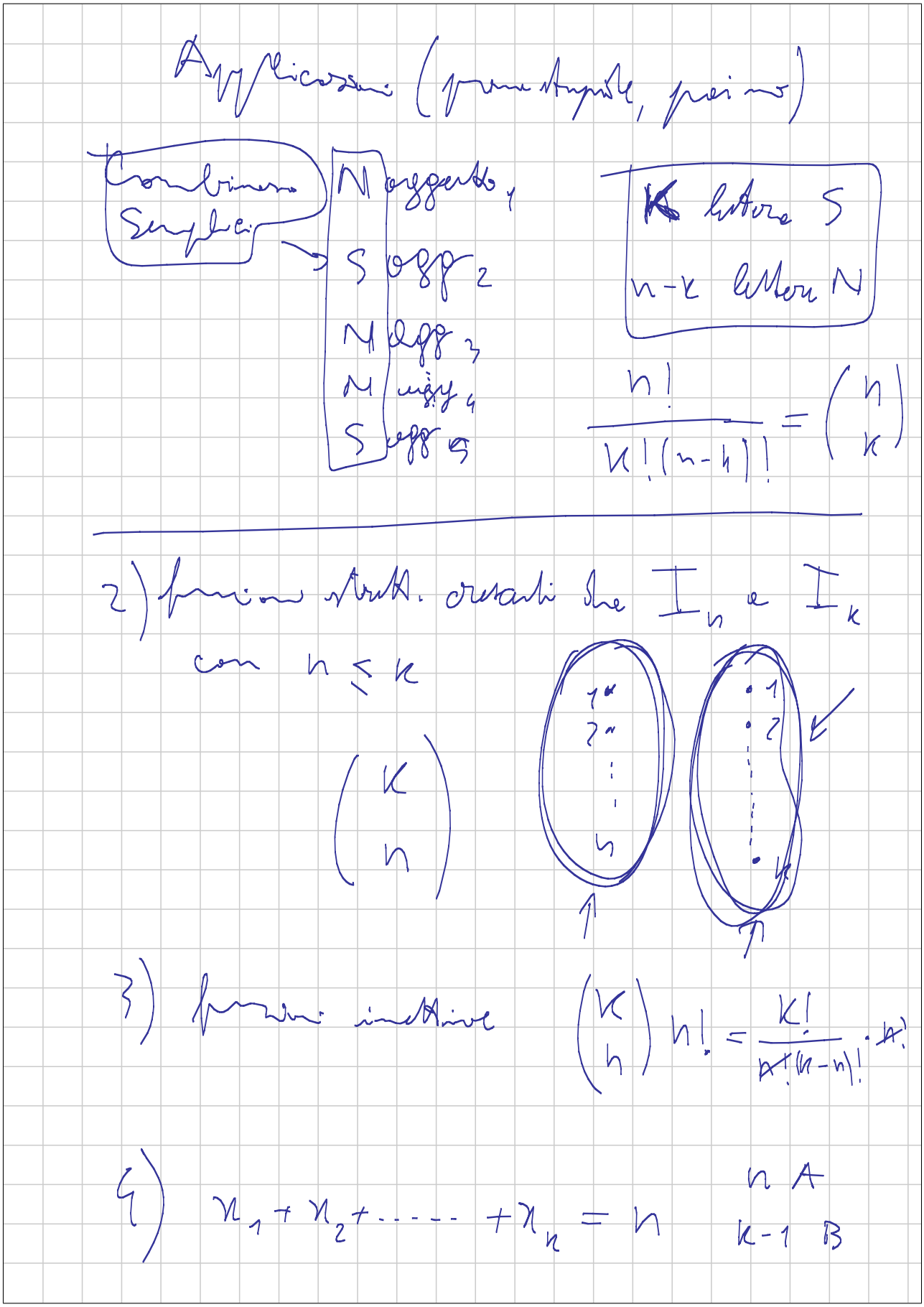
$$\frac{(n+m)!}{n! \cdot m!}$$

n_1 X_1

n_2 X_2

n_k X_k

$$\frac{(n_1+n_2+\cdots+n_k)!}{n_1! \cdot n_2! \cdots n_k!}$$


Applicazioni (prima stampata, poi no)
Combinazioni Semplici
N oggetti
S oggetti 2
N oggetti 3
N oggetti 4
S oggetti 5
K lettere S
n-k lettere N
n!/(k!(n-k)!) = (n k)
2) funzioni strett. crescenti fra I_n e I_k
con n ≤ k
(k n)
3) funzioni iniettive
(k n) n! = k!/(k-n)!
4) n_1 + n_2 + ... + n_k = n
n A
k-1 B

$x_1 + x_2 + x_3 = 5$

(2, 2, 1) : 5 A

→ (0, 5, 0) : 2 B

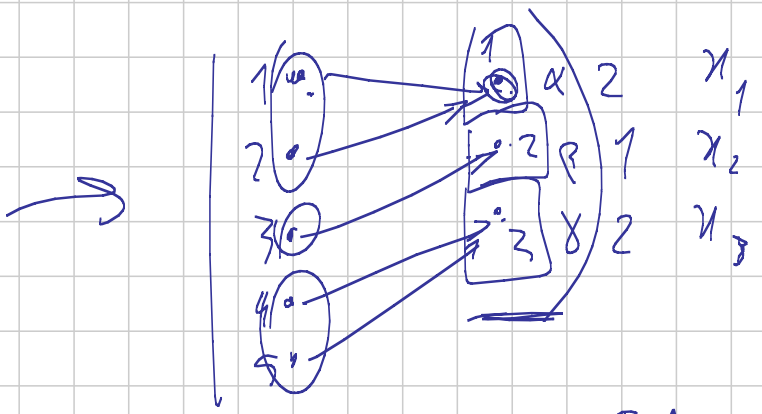
→ (5, 0, 0) :

A A B A A B A

n A , $n-1$ B

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

5) $f : I_n \to I_m$ crescenti



$x_1 + x_2 + x_3 = 5$

5 A
2 B

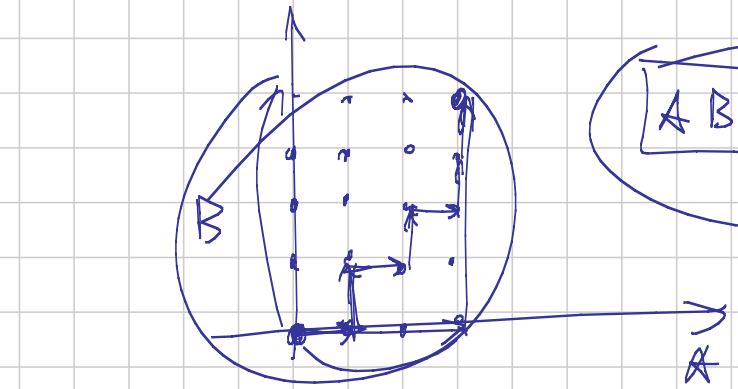
$$\frac{7!}{5!\cdot 2!} =$$

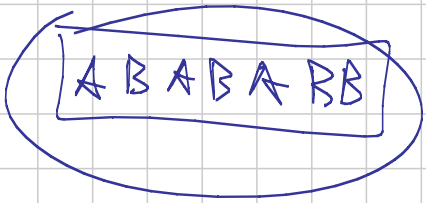
$$= \frac{7 \cdot 6}{2} = 21$$

$f : I_n \to I_m$ crescente

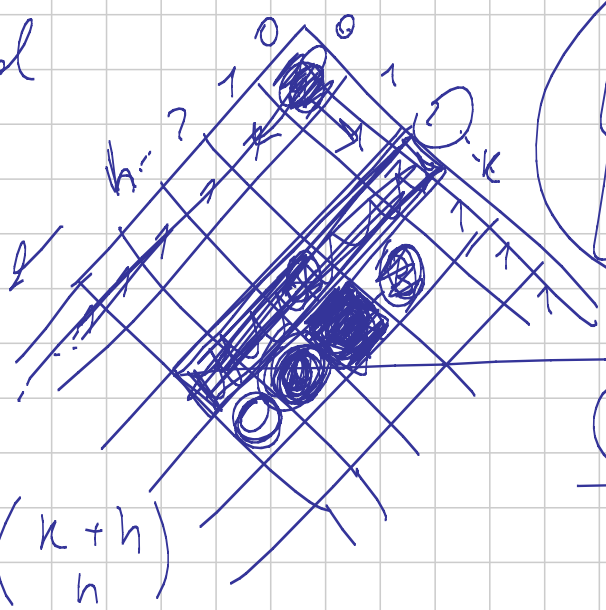
$$n_1 + n_2 + \cdots + n_m = n$$

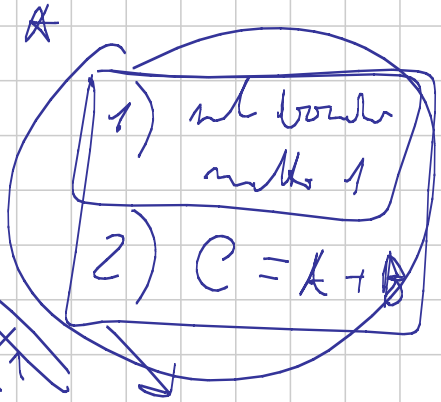
$$\binom{n+m-1}{m-1}$$





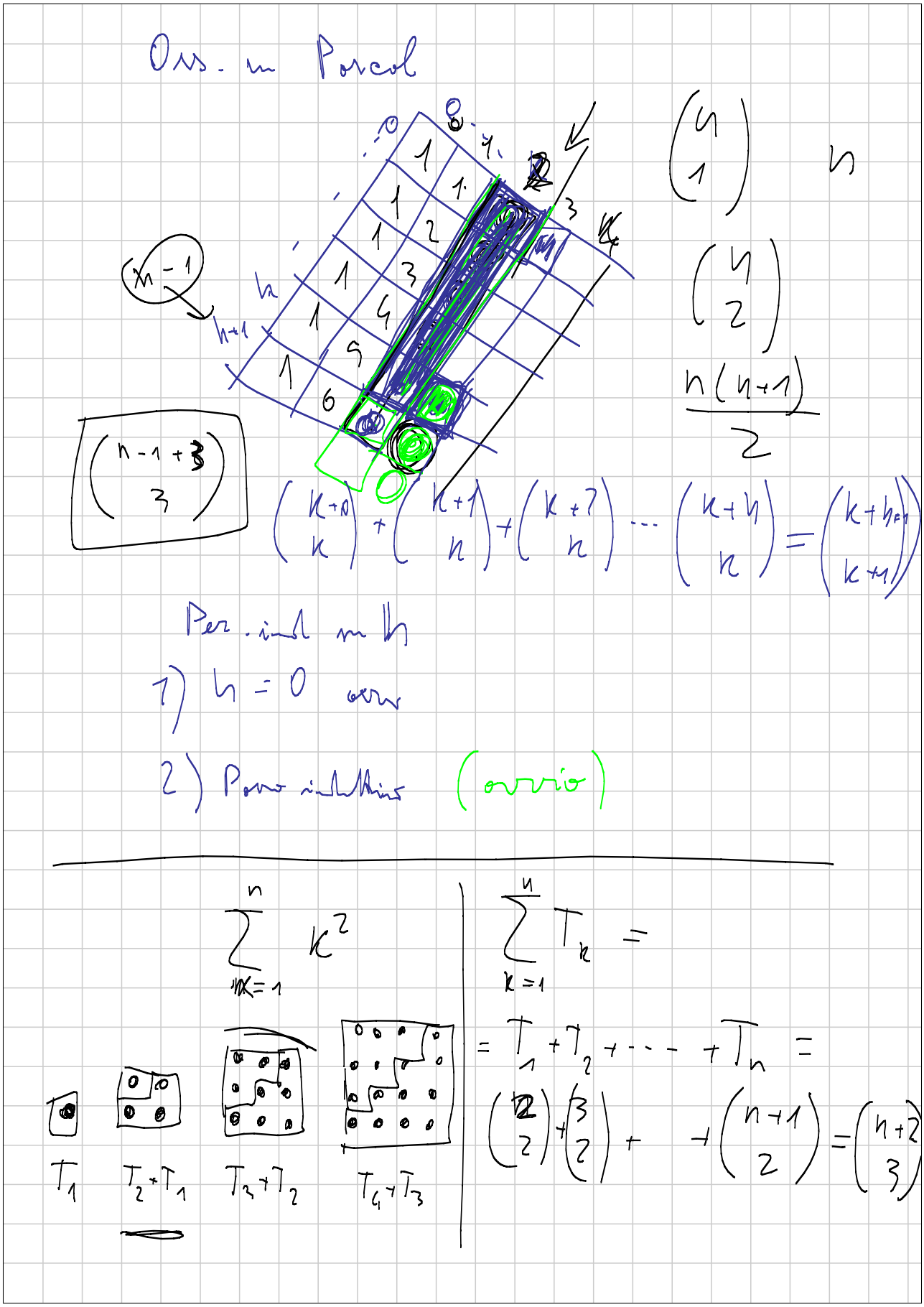
8) Pascal





$$= \binom{k+h}{h}$$

$$\frac{(k+h)!}{k! \cdot h!} =$$


Oss. in Parcel
Per. ind su h
1) h = 0 ovvio
2) Passo induttivo (ovvio)

$$1^2 + 2^2 + 3^2 + \dots + n^2$$

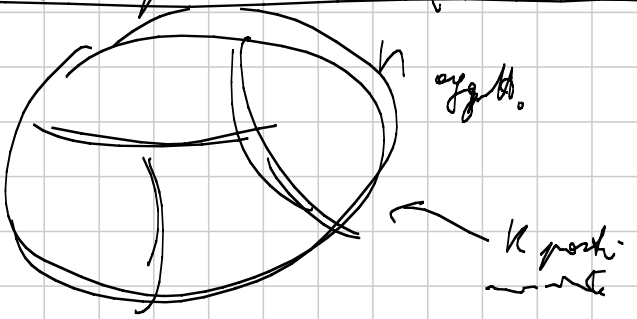
$$= \left(T_1 + T_2 + T_3 + \dots + T_n\right) + \left(T_1 + T_2 + \dots + T_{n-1}\right) =$$

$$= \binom{n+2}{3} + \binom{n+1}{3} = \frac{(n+2)(n+1)n}{3 \cdot 2} + \frac{(n+1)n(n-1)}{3 \cdot 2}$$

$$= \boxed{\frac{(n+1)n(2n+1)}{6}}$$

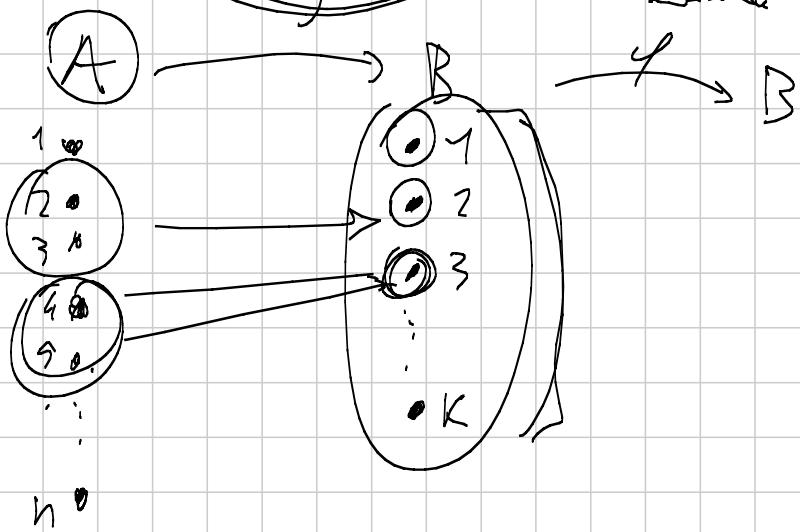
INIZIO II° parte

9) $S_{n,k}$



$\forall b \in B$

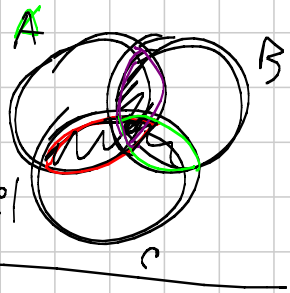
$f^{-1}(b)$



$$S_{n,k} = \frac{1}{k!} \cdot (\text{num. di funzioni iniettive da } A \to B)$$

Principio di inclusione esclusione

$$|A \cup B| = |A| + |B| - |A \cap B|$$



$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

$A_1, A_2, \ldots, A_n$

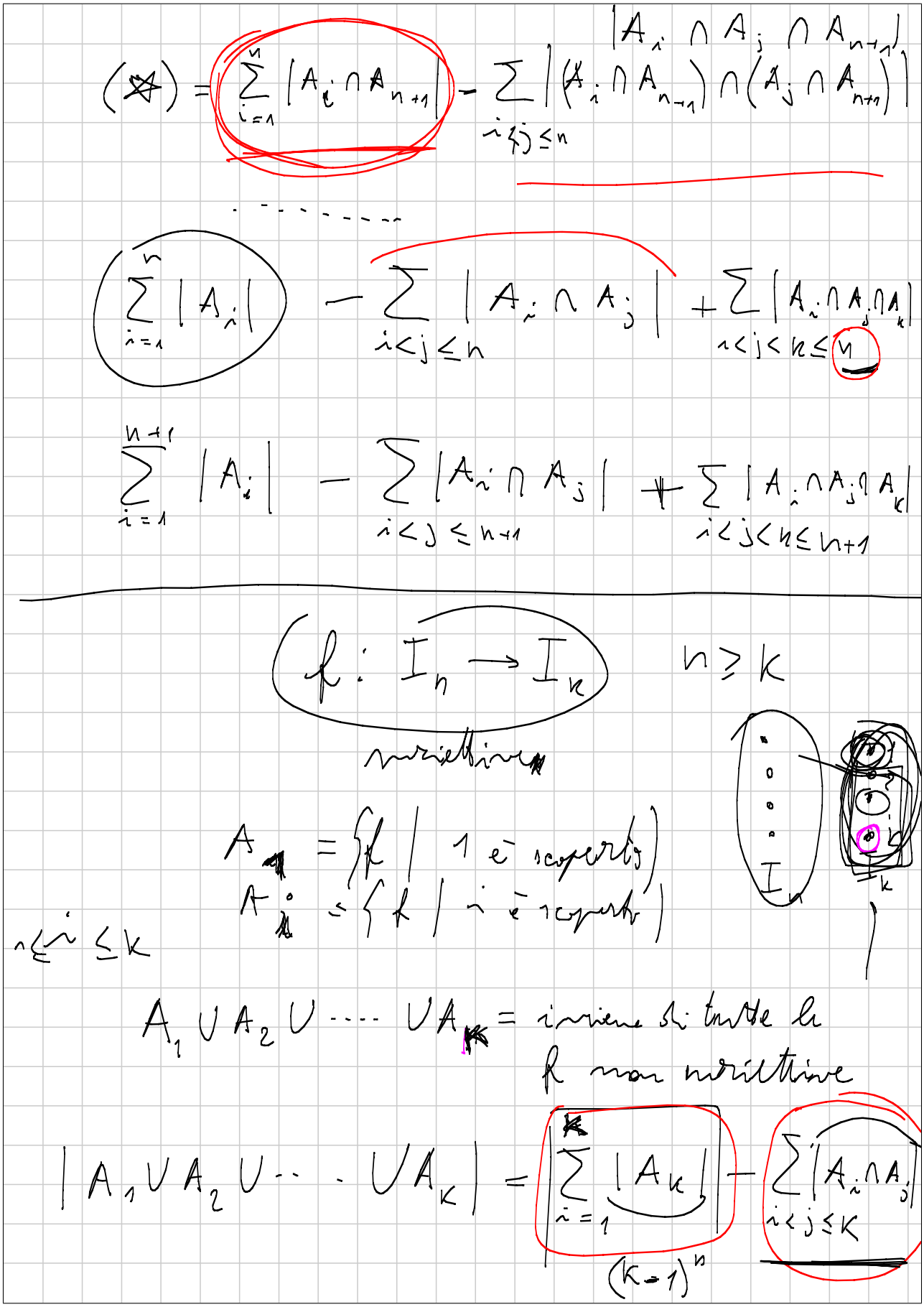
$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{i<j\le n} |A_i \cap A_j| + \sum_{i<j<k\le n} |A_i \cap A_j \cap A_k| \mp \cdots + (-1)^{k+1} \sum_{i_1<i_2<\cdots<i_k\le n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|$$

$$|(A_1 \cup A_2 \cup \cdots A_n) \cup A_{n+1}| =$$

$$= |A_1 \cup A_2 \cup \cdots \cup A_n| + |A_{n+1}| - |(A_1 \cup A_2 \cup \cdots \cup A_n) \cap A_{n+1}|$$

$$= (*) + |A_{n+1}| - |(A_1 \cap A_{n+1}) \cup (A_2 \cap A_{n+1}) \cup \cdots \cup (A_n \cap A_{n+1})|$$

$(\star)$


$(\star) = \sum_{i=1}^{n} |A_i \cap A_{n+1}| - \sum_{i<j\le n} |(A_i \cap A_{n+1}) \cap (A_j \cap A_{n+1})|$
$|A_i \cap A_j \cap A_{n+1}|$
$\sum_{i=1}^{n} |A_i| - \sum_{i<j\le n} |A_i \cap A_j| + \sum_{i<j<k\le n} |A_i \cap A_j \cap A_k|$
$\sum_{i=1}^{n+1} |A_i| - \sum_{i<j\le n+1} |A_i \cap A_j| + \sum_{i<j<k\le n+1} |A_i \cap A_j \cap A_k|$
$f : I_n \to I_k$
$n \ge k$
suriettiva
$A_k = \{f \mid k \text{ è scoperto}\}$
$A_i = \{f \mid i \text{ è scoperto}\}$
$1 \le i \le k$
$A_1 \cup A_2 \cup \dots \cup A_k$ = insieme di tutte le f non suriettive
$|A_1 \cup A_2 \cup \dots \cup A_k| = \left|\sum_{i=1}^{k} |A_k|\right| - \sum_{i<j\le k} |A_i \cap A_j|$
$(k-1)^n$
I_n
I_k

$$+ \sum_{i<j<l\le k} |A_i \cap A_j \cap A_l| - \dots$$

$$= \binom{k}{1}(k-1)^n - \binom{k}{2}(k-2)^n + \binom{k}{3}(k-3)^n - \binom{k}{4}(k-4)^n$$

$$= \sum_{i=1}^{k} (-1)^{i+1} \binom{k}{i} (k-i)^n$$

$$= \sum_{i=1}^{k} (-1)^{i+1} \binom{k}{i} (k-i)^n$$

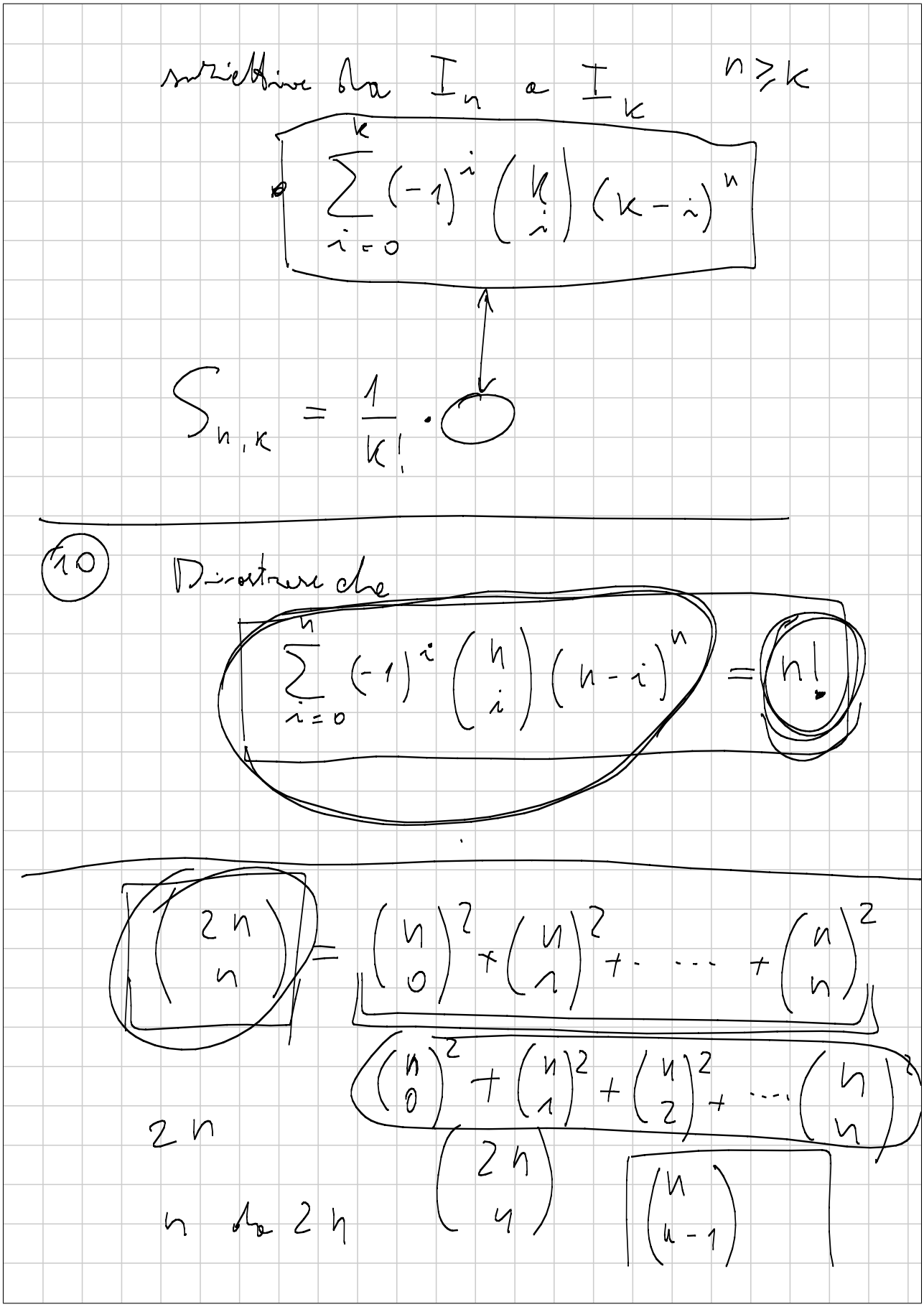
k^n

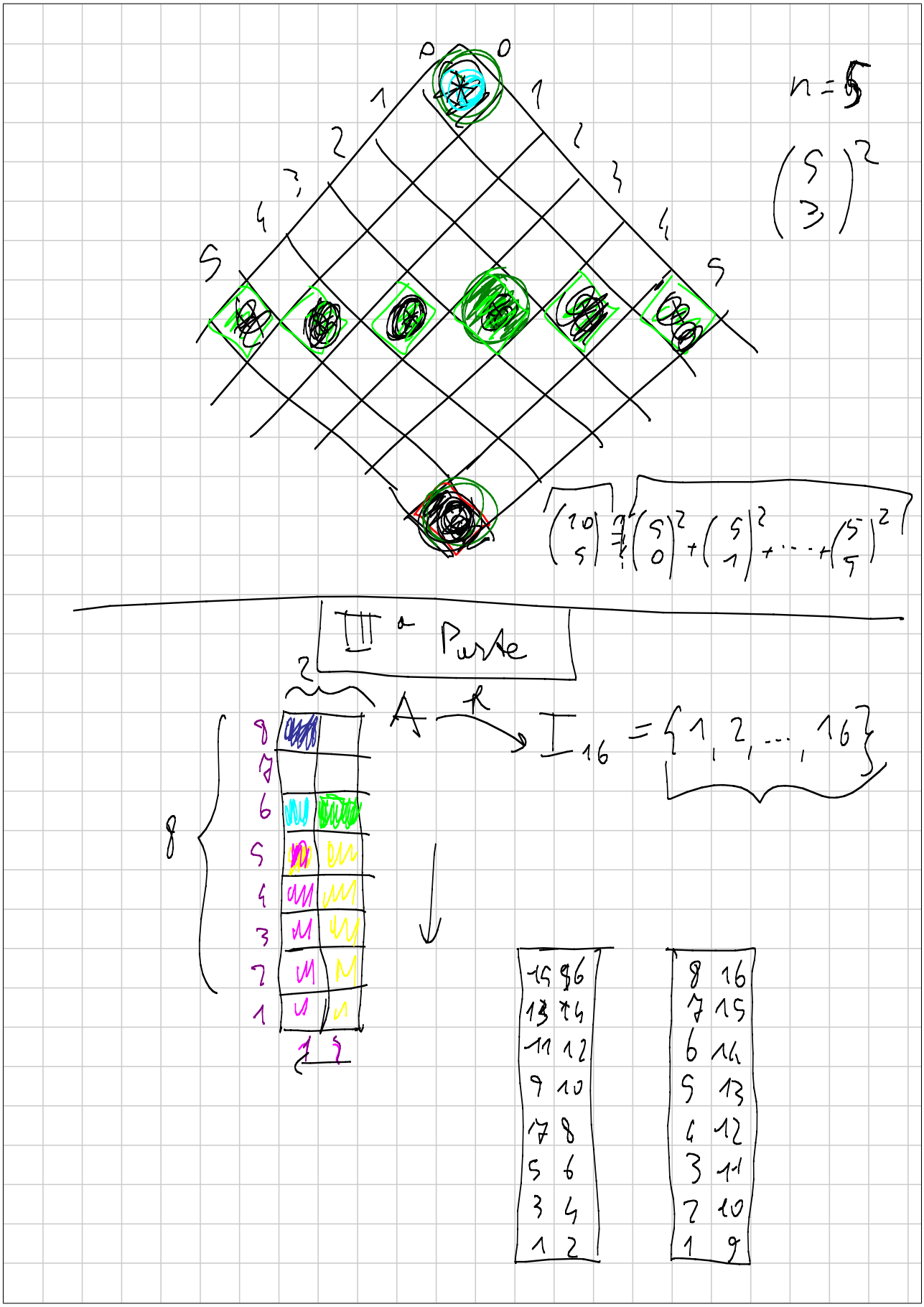
buone = totale − cattive =

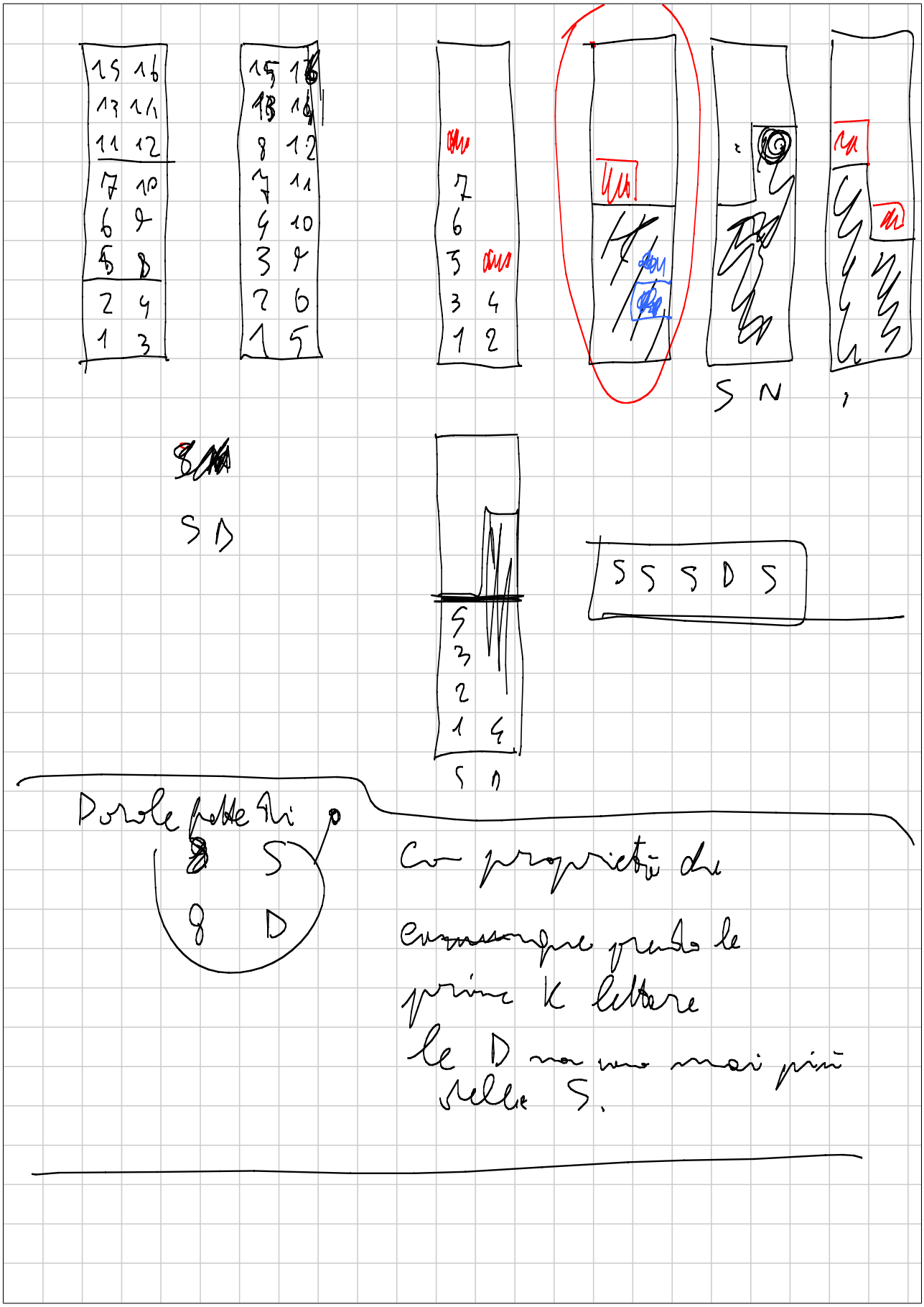
$$= \binom{k}{0}(k-0)^n + \sum_{i=1}^{k} (-1)^{i+1} \binom{k}{i} (k-i)^n$$

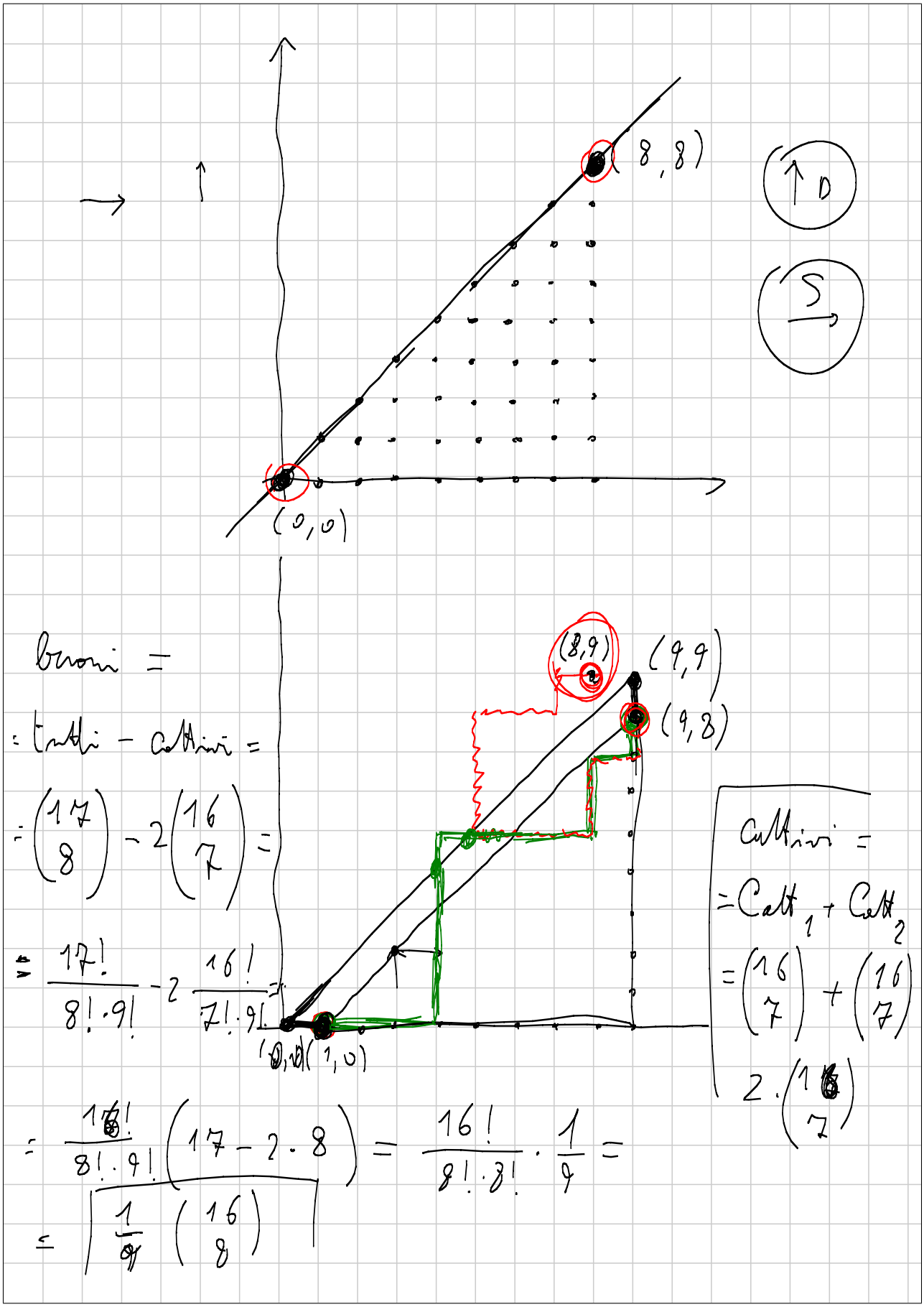
$(i+2)$

$$= \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n$$


suriettive da I_n a I_k
$n \geq k$
$\sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n$
$S_{n,k} = \frac{1}{k!} \cdot$
10
Dimostrare che
$\sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^n = n!$
$\binom{2n}{n} = \binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2$
$\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots \binom{n}{n}^2$
$2n$
n da $2n$
$\binom{2n}{n}$
$\binom{n}{n-1}$


n = 5
III a Parte
A
f
$I_{16} = \{1, 2, \dots, 16\}$


S N
S D
S S S D S
Parole fatte di
S
D
Con proprietà che
cominciano prendo le
prime k lettere
le D non sono mai più
delle S.


(8,8)
(0,0)
(8,9)
(9,9)
(9,8)
(0,0)
(1,0)
Buoni =
= Tutti − Cattivi =
= $\binom{17}{8} - 2\binom{16}{7}$ =
= $\frac{17!}{8!\cdot 9!} - 2\frac{16!}{7!\cdot 9!}$ =
= $\frac{16!}{8!\cdot 9!}(17 - 2\cdot 8) = \frac{16!}{8!\cdot 8!}\cdot\frac{1}{9}$ =
= $\frac{1}{9}\binom{16}{8}$
Cattivi =
= $Catt_1 + Catt_2$
= $\binom{16}{7} + \binom{16}{7}$
$2\cdot\binom{16}{7}$

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

IMO 4 (omissis questo)

$$S_n = (2n-1)\,S_{n-1}$$

$$S_1 = 1$$

$$S_n = (2n-1)(2n-3)\cdots 3\cdot 1$$

COMBINATORIA 2 BASIC

Titolo nota 09/09/2011

$\{1, 2, \dots n\} \xrightarrow{\sigma} \{1, 2, \dots n\}$

Biiettiva

	1	2	3	4	5	6	7	8	9
σ:	2	6	3	5	7	4	1	9	8

Tutte le permutazioni su n elementi

n!

σ:	1	2	3	4	5
	5	2	1	4	3

τ:	1	2	3	4	5
	2	1	3	5	4

$\sigma \circ \tau$:	1	2	3	4	5
	5	2	1	3	4

$\tau \circ \sigma$	1	2	3	4	5
	4	1	2	5	3

$(1\ 5\ 3)$

1	2	3	4	5
1	3	2	4	5

$\in \{1, \dots n\}$

$\sigma = (a_1\ a_2\ \dots\ a_k)$

$\sigma(a_1) = a_2$

$\sigma(a_2) = a_3$

$\dots$

$\sigma(a_{k-1}) = a_k$

$\sigma(a_k) = a_1$

TUTTI GLI ALTRI FISSI

$(1\ 2\ 3)\quad (4\ 5)$

1	2	3	4	5
2	3	1	5	4

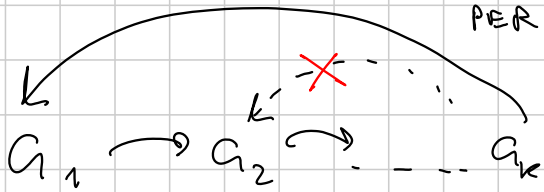
$a_1 \to a_2 \xrightarrow{\sigma} a_3 \to \dots$

$a_k = a_h \quad h < k \quad \exists$ cassetti

$\exists$ k più piccolo con questa proprietà
minimo

$a_k = a_1$ $\quad h = 1$ $\qquad a_k = a_h$ $\quad k > h > 1$ $\qquad a_k = \sigma(a_{k-1})$ $\quad a_h = \sigma(a_{h-1})$

PER ASSURDO $\qquad a_{k-1} = a_{h-1}$



$\sigma = (a_1\ a_2\ \dots\ a_{k-1})\sigma'$

1	2	3	4	5	6	7	8	9
2	6	3	5	7	4	1	9	8

$(1\ 2\ 6\ 4\ 5\ 7)(8\ 9)$

segno

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

$\sigma : \{1 \dots n\} \to \{1 \dots n\}$

$\operatorname{Sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$

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

$$\prod_{1\le i<j\le n} \frac{\sigma\circ\tau(i)-\sigma\circ\tau(j)}{\tau(i)-\tau(j)} \cdot \frac{\tau(i)-\tau(j)}{i-j}$$

$\operatorname{sgn}\sigma$ $\operatorname{sgn}\tau$

$\tau(i)=k \quad k>l$

$\tau(j)=l$

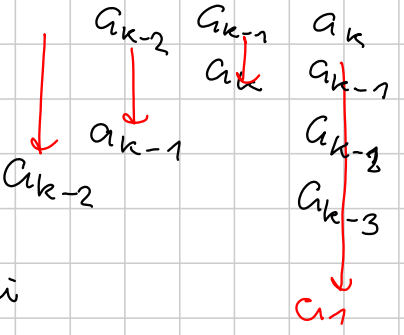
$k<l \qquad \frac{\sigma(k)-\sigma(l)}{k-l} = \frac{\sigma(l)-\sigma(k)}{l-k}$

Il segno di σ conta la parità del numero di coppie (i,j) con $1\le i<j\le n$ tali che $i<j$ ma $\sigma(i)>\sigma(j)$

$(a_1\ a_2\ \dots\ a_k) = (a_1\ a_2)(a_2\ a_3)\cdots(a_{k-1}\ a_k)$

$a_1\ a_2\ \dots\ a_{k-1}\ a_k$

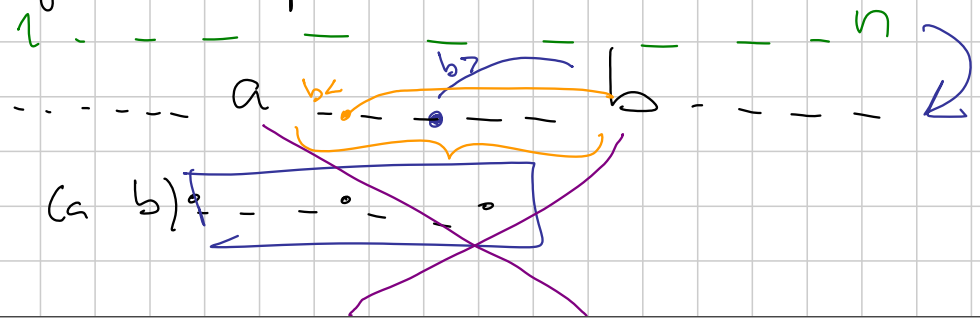
$a_2\ a_3\ \dots\ a_k\ a_1$

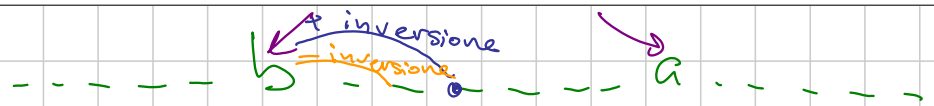


pari Sgn +1 : prodotto di pari trasposizioni

dispari Sgn −1 : prodotto di dispari trasposizioni

Segno parità del numero di inversioni



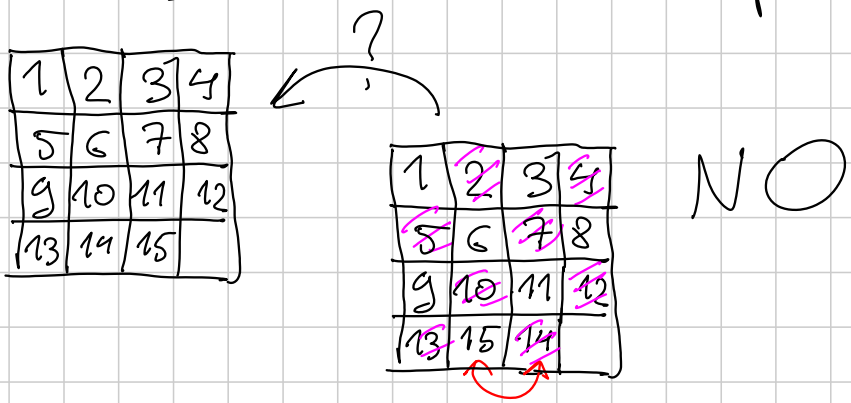


parità del numero di inversioni
= parità del numero di trasposizioni

$(a_1\ a_2\ \dots\ a_k) = (a_1\ a_2)(a_2\ a_3) \dots (a_{k-1}\ a_k)$

Un ciclo di lunghezza pari è una permutazione dispari

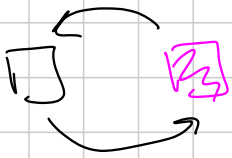
dispari è pari.



MOSSA = TRASPOSIZIONE

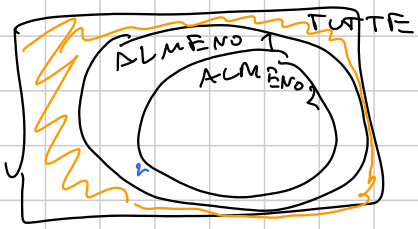
VOGLIAMO OTTENERE UNA PERMUTAZIONE DISPARI

NUMERO DISPARI DI MOSSE



PERMUTAZIONI SENZA PUNTI FISSI

$$n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \dots + \binom{n}{1}(n-1)!$$

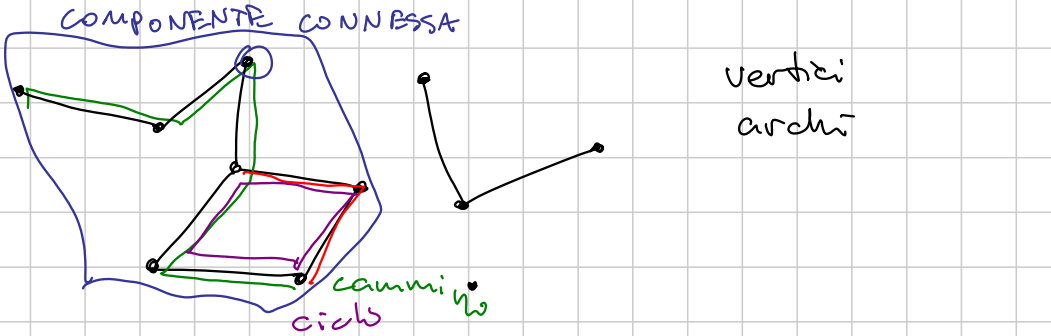


$$n! - \frac{n}{1}(n-1)! + \frac{n(n-1)}{2!}(n-2)! - \frac{n(n-1)(n-2)}{3!}(n-3)! + \dots + (-1)^n \frac{n!}{n!} 0!$$

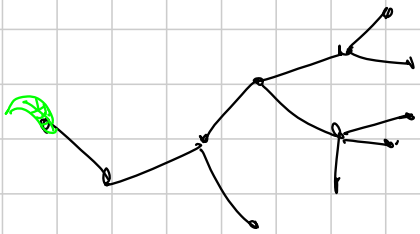
$$n!\left(1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \dots + (-1)^n \frac{1}{n!}\right)$$

L'intero più vicino a $\frac{n!}{e}$ è $\sim \frac{1}{e}$

$e = 2{,}71828\ldots$



vertici
archi



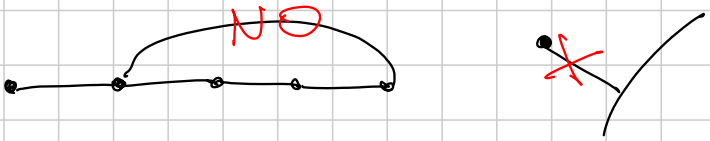
ALBERO

togliendo un arco: non più connesso

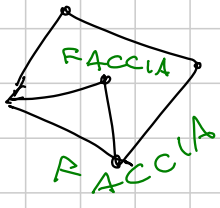
aggiungendo un arco: ottengo un ciclo

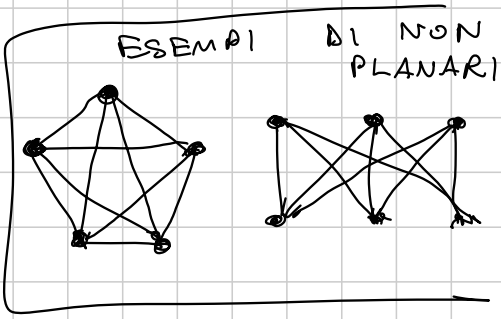
$V = e + 1$

"edges" ~ archi



- $1 = 0 + 1$

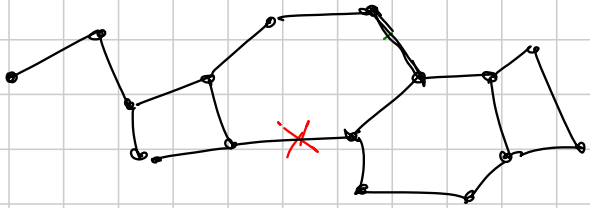




GRAFI PLANARI CONNESSI (NON VUOTI)

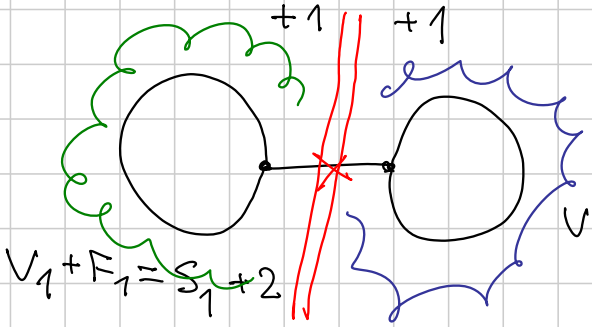
$V+F=S+2$

- $1+1=0+2$



$V+F=S+2$

$+1 \quad +1$



$V_1+F_1=S_1+2$

$V_2+F_2=S_2+2$

$(V_1+V_2)+F = (S_1+S_2+1)+2$

SPERIAMO

$(V_1+V_2)+(F_1+F_2-1)=(S_1+S_2+1)+2+1$

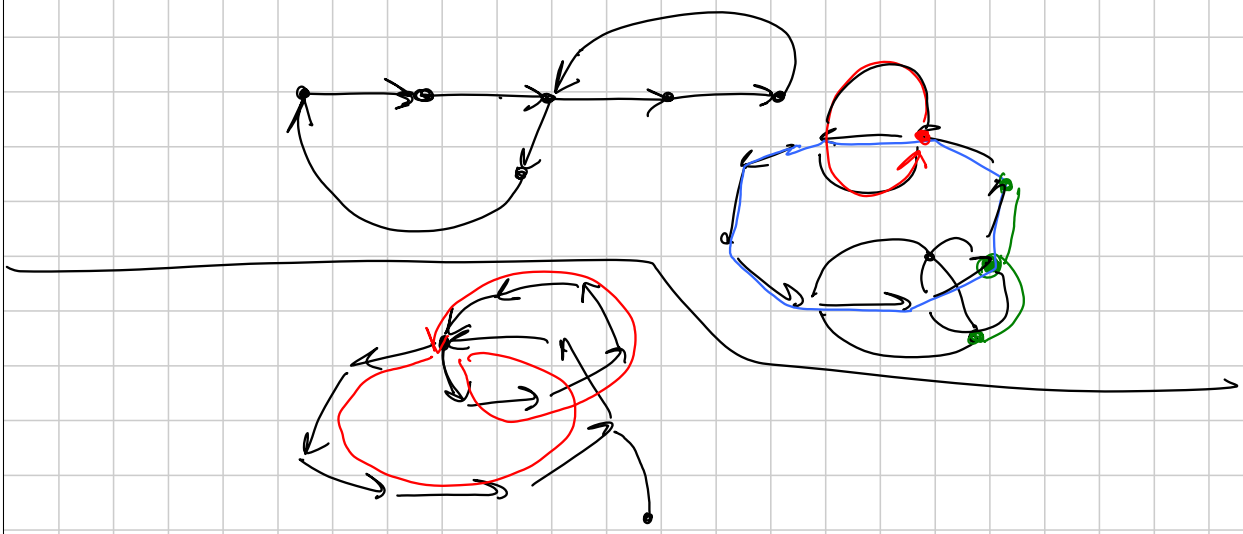
IP (ND) $\begin{cases} V_1+F_1=S_1+2 \\ V_2+F_2=S_2+2 \end{cases}$

$(V_1+V_2)+(F_1+F_2)=(S_1+S_2)+4$

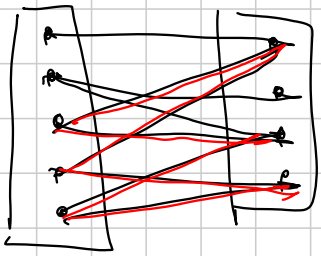
CICLO EULERIANO ESISTE SSE OGNI VERTICE HA ORDINE PARI

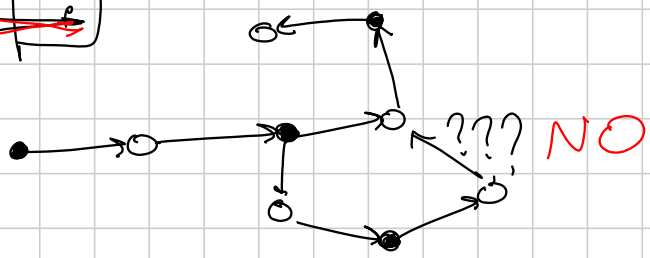
CICLO DI EULERO ⟹ CARATTERIZZAZIONE

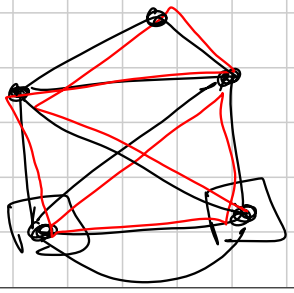
CICLO : ESCE ED ENTRA IN OGNI VERTICE



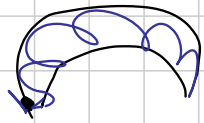
IL CICLO PIÙ GRANDE COMPRENDE TUTTI GLI ARCHI

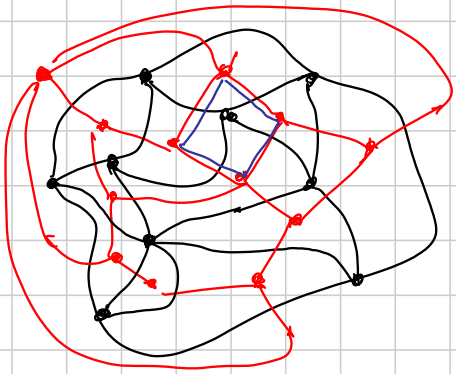






$$\sum_{\text{Vertici}} \underbrace{\deg(v)}_{\substack{\text{NUMERO} \\ \text{DI ARCHI} \\ \text{DAL VERTICE}}} = 2e$$

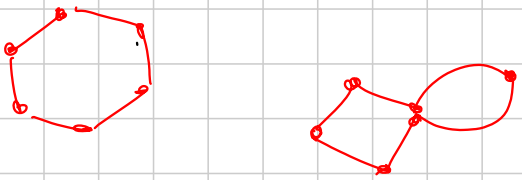


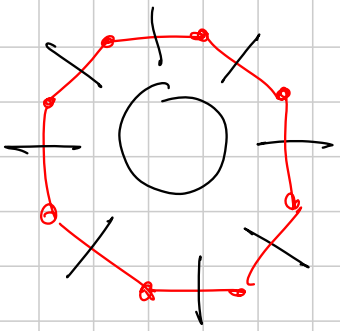


- CARTINA CON 2 COLORI
- FERROVIA LUNGO I CONFINI

GRAFO DEI CONFINI = CICLO DI EULERO

GRAFO DEGLI STATI BIPARTITO





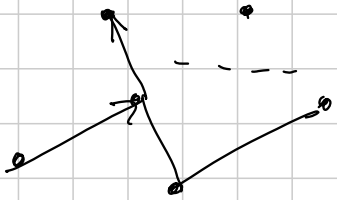
$\sum_{\text{vertici grafo confini DENTRO IL CICLO}} o(v) = \text{PARI} =$

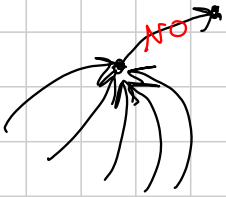
$= 2 \cdot$ archi interni $+$

$1 \cdot$ archi corrispondenti agli archi del ciclo

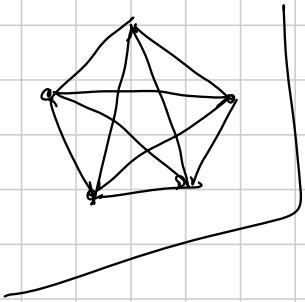
SONO PARI

GRAFI ORIENTATI





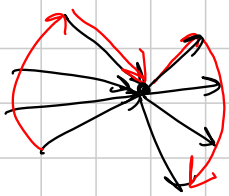
IP : PER OGNI COPPIA (a,b), POSSIAMO ANDARE da a a b o VICEVERSA



GRAFO COMPLETO

OGNI ARCO È ORIENTATO

OGNI VERTICE UNA E UNA SOLA VOLTA



INVARIANTI

$a_1\ a_2\ a_3\ \dots\ a_{n-1}\ a_n \in \mathbb{R}$

$a_1,\ \frac{a_2+a_3+a_{n-1}}{3},\ \frac{a_2+a_3+a_{n-1}}{3},\ \dots\ \frac{a_2+a_3+a_{n-1}}{3},\ a_n$

SOMMA È UN INVARIANTE

SOMMA DEI QUADRATI CALA

GNOMI CONFORMISTI

Gennaio, Febbraio, ... Dicembre

Azzurro Rosa

Alcune coppie: Amici

Si ridipinge da conformisti

Processo è finito

Felicità (gnomo) = amici con casa stesso colore − amici con casa dell'altro colore

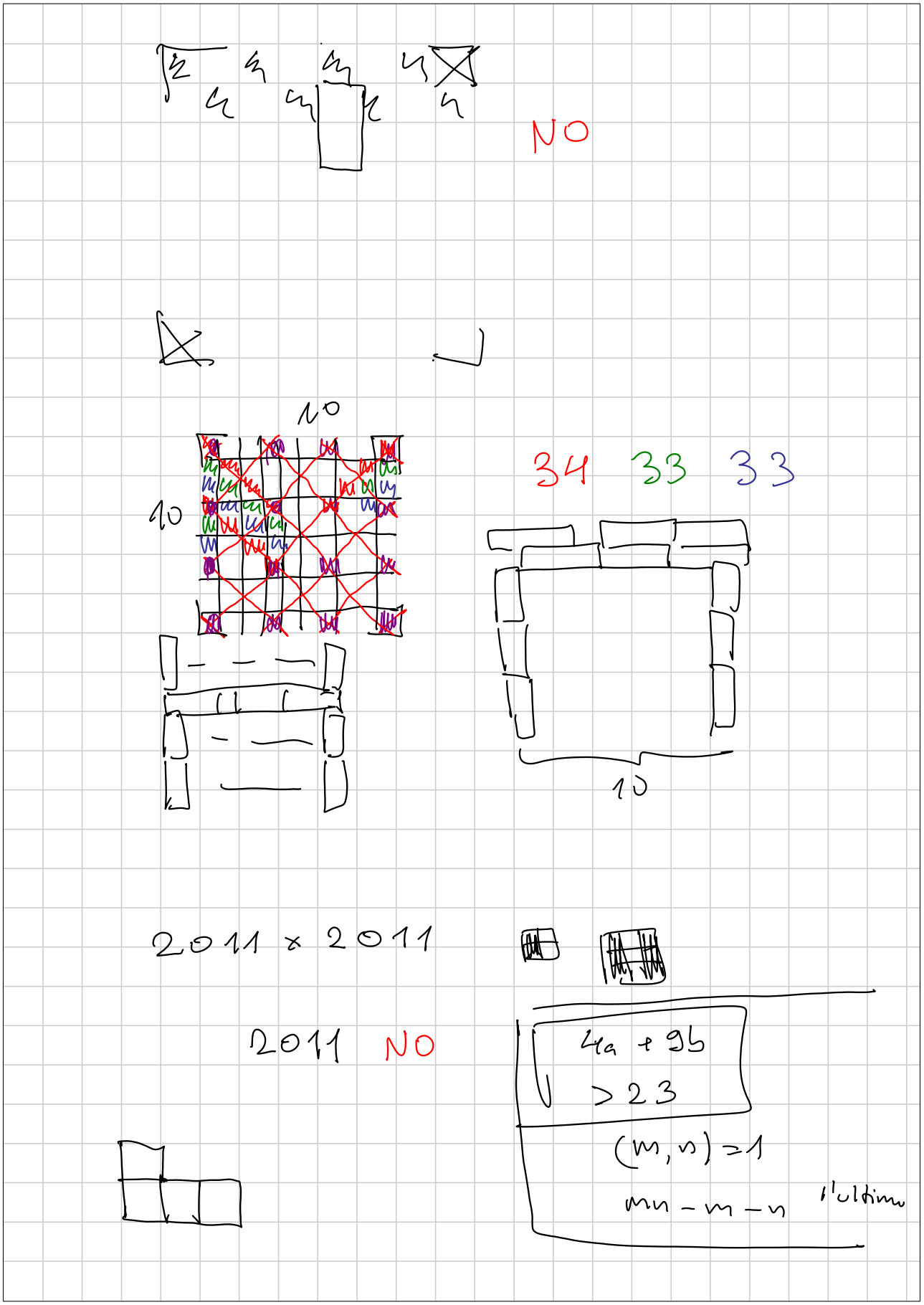
$F = \sum_{\text{gnomi}} F(\text{gnomo})$ → +

$m > n$

$+2m - 2n = 2(m-n) > 0$

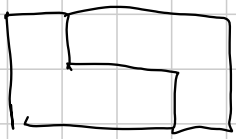
$F \le \sum_{\text{gnomi}} \text{N}^\circ \text{ amici (gnomo)}$

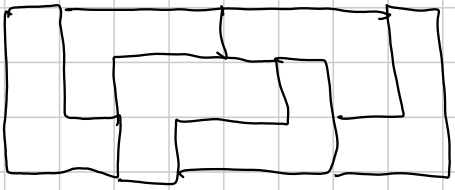
Prima o poi non si ridipinge più

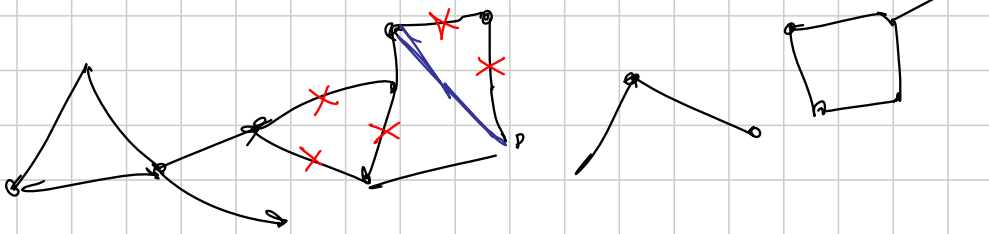

NO
NO
10
34 33 33
10
2011 × 2011
2011 NO
4a + 9b
> 23
(m, n) = 1
mn - m - n
l'ultimo

un lato pari → striscia perpendicolare a esso

stesso numero bianche e nere caselle (pari)



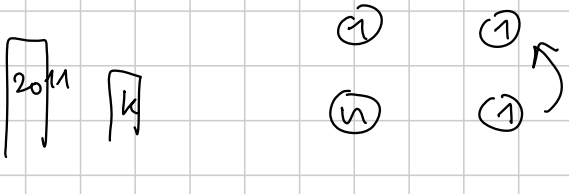




Alla fine sappiamo quanti vertici con arco uscente

Quanti archi

Sappiamo mosse fatte parità



$m \neq n$ $m > n$

n n

perdente: qualunque mossa risulta in una config vincente per l'avversario

vincente: ∃ mossa che risulta in una config perdente per l'avversario

SENIOR 2011 – G1 (Basic)

Titolo nota 05/09/2011

① GEOMETRIA SINTETICA G3

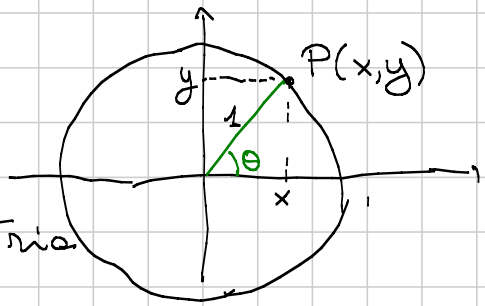
② ALGEBRIZZAZIONI (vettori, numeri complessi, geometria analitica) G2

③ CALCOLO TUTTO (trigonometria).

GONIOMETRIA

$$\begin{cases} x = \cos\theta \\ y = \sin\theta \end{cases}$$

$x^2+y^2=1$



$\Rightarrow$ Formula fond. della goniometria.

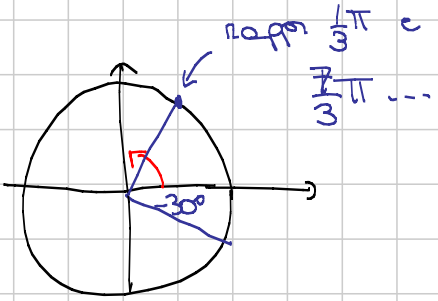
$\cos^2\theta + \sin^2\theta = 1$.

Gradi vs radianti: θ != lunghezza dell'arco.

$$\frac{\theta^\circ}{360^\circ} = \frac{\theta^{rad}}{2\pi}$$

Angoli con segno

$\frac{1}{3}\pi + 2\pi = \frac{1}{3}\pi$



Periodicità e simmetrie.

$\sin\theta + 2\pi = \sin\theta$

θ, $\pi-\theta$, $\pi+\theta$, $\frac{\pi}{2} \pm \theta$

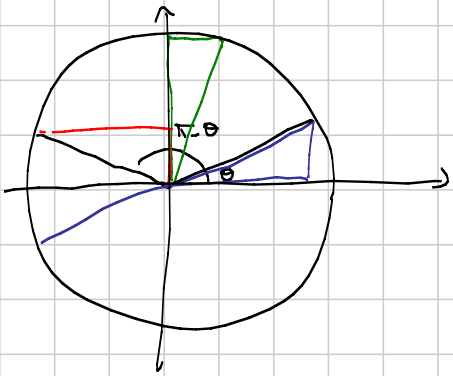
$\cos\pi-\theta = -\cos\theta$

$\sin\pi-\theta = \sin\theta$

$\cos\pi+\theta = -\cos\theta$

$\sin\pi+\theta = -\sin\theta$

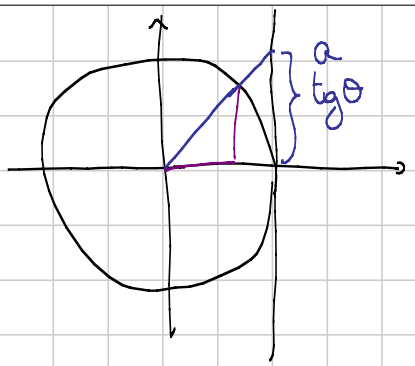
$\begin{cases} \cos\frac{\pi}{2}-\theta = \sin\theta \\ \sin\frac{\pi}{2}-\theta = \cos\theta \end{cases}$



Altre funzioni trigonometriche

$\tan\theta = \operatorname{tg}\theta := \frac{\sin\theta}{\cos\theta}$

$\operatorname{cotg}\theta := \frac{\cos\theta}{\sin\theta}$



$\frac{a}{1} = \frac{\sin\theta}{\cos\theta}$

Periodo di $\operatorname{tg}\theta$?

sin e cos hanno periodo 2π.
$\Rightarrow$ tg ha periodo $\mid 2\pi$

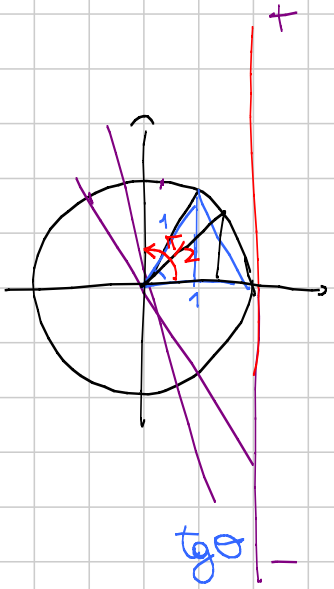
$$\operatorname{tg}(\theta+\pi) = \frac{\sin\theta+\pi}{\cos\theta+\pi} = \frac{-\sin\theta}{-\cos\theta} = \operatorname{tg}\theta$$

Ex: tg ha periodo ESATTAM π. (Rimti segni).

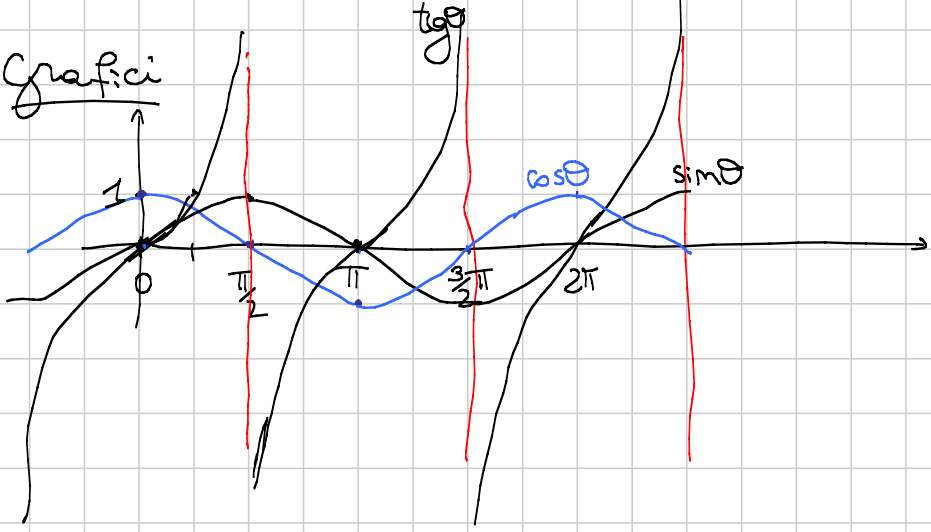
Valori notevoli

$0, \pi, \frac{\pi}{2}, \frac{\pi}{3}$ e $\frac{\pi}{6}$, $\frac{\pi}{4}$

	cos	sin	tg	
$\frac{\pi}{2}$	0	1	....	
$\frac{\pi}{3}$	$\frac{1}{2}$	$\frac{\sqrt{3}}{2}$	$\sqrt{3}$	$(\frac{\pi}{6})$
$\frac{\pi}{4}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{2}}{2}$	1	



Grafici



Funzioni inverse:

$\operatorname{tg}\theta : \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \longrightarrow (-\infty, +\infty) = \mathbb{R}$

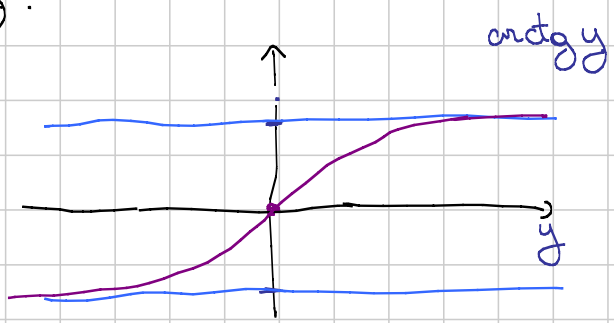
è biunivoca.

$\operatorname{arctg} y :=$ l'angolo θ tra $-\frac{\pi}{2}$ e $\frac{\pi}{2}$ t.c

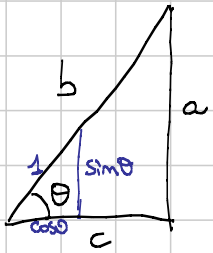
$\operatorname{tg}\theta = y$.

Grafico $\operatorname{arctg} y$?

$y \longrightarrow +\infty$



Trigonom del triangolo rettangolo



a in funzione di b e θ?

$a = b \cdot \sin\theta$

$c = b \cos\theta$

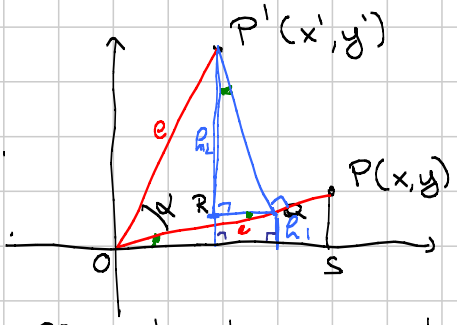
$b^2 = a^2 + c^2 \quad (\Rightarrow \quad 1 = \cos^2\theta + \sin^2\theta$

FORMULE

Rotazione nel piano

$(x',y') = (x,y)$ ruotato di α.

Scriviamo in funzione di x, y, α.



Oss 1: $x'^2 + y'^2 = x^2 + y^2 = e^2$ È sufficiente trovare y'.

$\overline{OQ} = e\cos\alpha$

$h_1 = y\cos\alpha$

$\frac{R_1}{\overline{OQ}} = \frac{y}{e}$ $\overline{OQ} =$

$P'\hat{Q}R$ e $O\hat{P}S$ sono simili.

$\frac{h_2}{P'Q} = \frac{OS}{OP} = \frac{x}{e}$

$P'Q = e\sin\alpha$

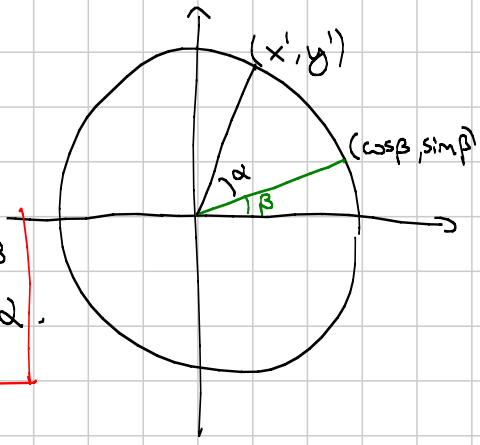
$h_2 = x\sin\alpha$.

$$\begin{cases} x' = x\cos\alpha - y\sin\alpha \\ y' = x\sin\alpha + y\cos\alpha \end{cases}$$ (ex: ricavare con oss 1).

Formula di addizione

$\cos(\alpha+\beta) = ?$

$\sin(\alpha+\beta) = ?$



rotazione

$x' = \cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$

$y' = \sin(\alpha+\beta) = \sin\alpha\cos\beta + \sin\beta\cos\alpha$.

$$\begin{aligned} \cos(\alpha-\beta) &= \cos(\alpha+(-\beta)) \\ &= \cos\alpha\cos(-\beta) - \sin\alpha\sin(-\beta) \\ &= \cos\alpha\cos\beta + \sin\alpha\sin\beta \end{aligned}$$

$\sin(\alpha-\beta) = \sin\alpha\cos\beta - \sin\beta\cos\alpha$.

Formule di duplicazione

$\cos 2\alpha = \cos^2\alpha - \sin^2\alpha \overset{\text{formula fond.}}{=} 1-2\sin^2\alpha = 2\cos^2\alpha - 1 \quad (*)$

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

Formule di bisezione

$\cos\frac{\beta}{2} = ?$ $\qquad \frac{\beta}{2} = \alpha$

Sostituisco $\alpha = \beta/2$ in $(*)$

$\cos\beta = 2\cos^2\frac{\beta}{2} - 1$

$\cos\frac{\beta}{2} = \pm\sqrt{\frac{\cos\beta+1}{2}}$ $\qquad \cos\beta \geq -1 \Rightarrow$ ok radice.

$\sin\frac{\beta}{2} = \pm\sqrt{\frac{1-\cos\beta}{2}}$

$\sin^2\frac{\beta}{2} + \cos^2\frac{\beta}{2} = 1 \Rightarrow$ ricavo $\sin\frac{\beta}{2}$

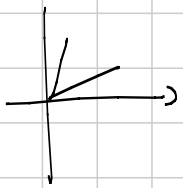
$$\operatorname{tg}(\alpha+\beta) = \frac{\sin(\alpha+\beta)}{\cos(\alpha+\beta)} = \frac{\sin\alpha\cos\beta + \sin\beta\cos\alpha}{\cos\alpha\cos\beta - \sin\alpha\sin\beta}$$

$$= \frac{\frac{\sin\alpha}{\cos\alpha} + \frac{\sin\beta}{\cos\beta}}{1 - \frac{\sin\alpha}{\cos\alpha}\frac{\sin\beta}{\cos\beta}} = \frac{\operatorname{tg}\alpha + \operatorname{tg}\beta}{1 - \operatorname{tg}\alpha\operatorname{tg}\beta}$$

Fatto: $\alpha, \beta, \gamma \in (0, \pi)$. Allora

$\alpha+\beta+\gamma = \pi$ se e solo se

$\operatorname{tg}\frac{\alpha}{2}\operatorname{tg}\frac{\beta}{2} + \operatorname{tg}\frac{\beta}{2}\operatorname{tg}\frac{\gamma}{2} + \operatorname{tg}\frac{\gamma}{2}\operatorname{tg}\frac{\alpha}{2} = 1$



Dim:

$\Rightarrow)$ $\operatorname{tg}\frac{\gamma}{2} = \operatorname{tg}\frac{\pi-\alpha-\beta}{2} = \operatorname{tg}\left(\frac{\pi}{2} - \frac{\alpha+\beta}{2}\right)$

$\operatorname{tg}\left(\frac{\pi}{2} - \theta\right) = \frac{1}{\operatorname{tg}\theta}$

$\frac{\sin\left(\frac{\pi}{2}-\theta\right)}{\cos\left(\frac{\pi}{2}-\theta\right)} = \frac{\cos\theta}{\sin\theta}$

$$= \frac{1}{\tg \frac{\alpha+\beta}{2}}$$

$$= \frac{1 - \tg\frac{\alpha}{2}\tg\frac{\beta}{2}}{\tg\frac{\alpha}{2} + \tg\frac{\beta}{2}} \quad \text{ok.}$$

($\Leftarrow$) $\alpha, \beta, \pi - \alpha - \beta = \theta$ verificano la relazione
Per hp α, β, γ verificano.

$$\tg\frac{\gamma}{2} = \tg\frac{\pi - \alpha - \beta}{2}$$

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

Ex: concludere questa uguaglianza

Ex (difficile): $a, b, c \in (0,1)$ t.c $ab + bc + ca = 1$
Allora

$$\sum_{a,b,c} \frac{a}{1-a^2} \geq \frac{3}{4} \sum_{a,b,c} \frac{1-a^2}{a}.$$

Idea:

(1) $a = \tg\frac{\alpha}{2}$ con $\alpha \in [0, \frac{\pi}{2})$
b, c

(2) $ab + bc + ca = 1 \iff \alpha + \beta + \gamma = \pi$

(3) Riscriviamo la disug

$$\frac{a}{1-a^2} = \frac{\tg\frac{\alpha}{2}}{1 - \tg^2\frac{\alpha}{2}} = \dots = \frac{\tg\alpha}{2}$$

(4) In generale, se $\alpha + \beta + \gamma = \pi$ allora

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

Formula di bisezione per $\operatorname{tg}\theta$

$$\operatorname{tg}\frac{\theta}{2} = \frac{\sin\frac{\theta}{2}}{\cos\frac{\theta}{2}} = \sqrt{\frac{1-\cos\theta}{1+\cos\theta}} = \sqrt{\frac{1-\cos^2\theta}{(1+\cos\theta)^2}}$$

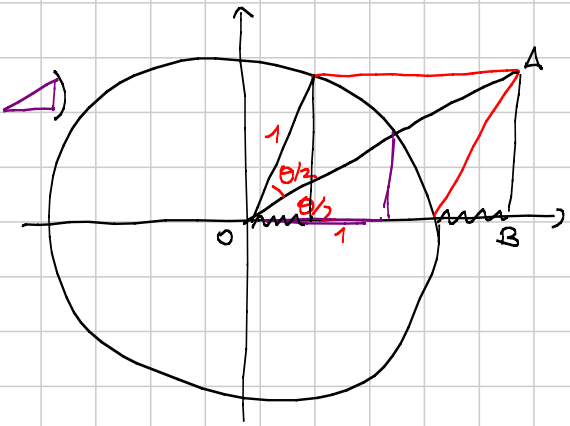
$$= \sqrt{\frac{\sin^2\theta}{(1+\cos\theta)^2}} = \frac{\sin\theta}{1+\cos\theta}.$$

Altro modo.

$\operatorname{tg}\frac{\theta}{2} = \frac{AB}{OB}$ (similitudine con $\triangle$)

$AB = \sin\theta$

$OB = 1 + \cos\theta$



Formule parametriche

$t = \operatorname{tg}\frac{\theta}{2}$. Allora vale

$$\sin\theta = \frac{2t}{1+t^2} \quad (1) \qquad \cos\theta = \frac{1-t^2}{1+t^2} \quad (2)$$

Esempio: $5\cos\theta + 2\sin\theta = 1$

Sostituendo, diventa $5\cdot\frac{2t}{1+t^2} + 2\,\frac{1-t^2}{1+t^2} = 1$, eq di 2° grado

---

Verifichiamo (1).

$$\frac{2t}{1+t^2} = \frac{2\operatorname{tg}\frac{\theta}{2}}{1+\operatorname{tg}^2\frac{\theta}{2}} = \frac{2\,\frac{\sin\theta}{1+\cos\theta}}{1+\frac{\sin^2\theta}{(1+\cos\theta)^2}} = \frac{2\sin\theta(1+\cos\theta)}{(1+\cos\theta)^2+\sin^2\theta}$$

$$= \frac{2\sin\theta(1+\cos\theta)}{2+2\cos\theta}$$

Verifichiamo (2).

$$\cos\theta = \sqrt{1-\sin^2\theta} = \sqrt{1-\left(\frac{2t}{1+t^2}\right)^2} = \sqrt{\frac{1+t^4+2t^2-4t^2}{(1+t^2)^2}} = \sqrt{\frac{(1-t^2)^2}{(1+t^2)^2}}.$$

↑ occhio ai segni... ora assumo $\cos\theta > 0$

Oss: esistono ∞ pt: a coordinate razionali sulla circonferenza unitaria.

Dim1

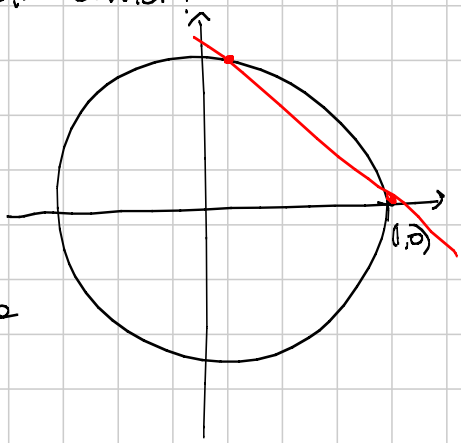
Prendo t numero razionale. $\sin\theta$ e $\cos\theta$ corrisp sono numeri razionali.

Ex: a t diversi corrispondono pt: diversi?

Dim2

$y = k(x-1) \qquad k \in \mathbb{Q}$

$\begin{cases} y = k(x-1) & (1) \\ x^2+y^2=1 & (2) \end{cases}$ altra intersezione retta circonferenza



x e y sono razionali?

Da (1), basta verif che x sia razionale.

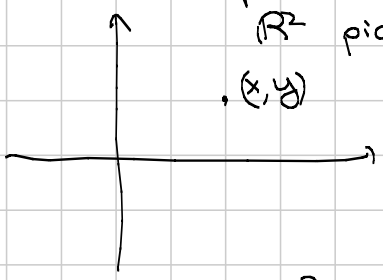
(2) diventa

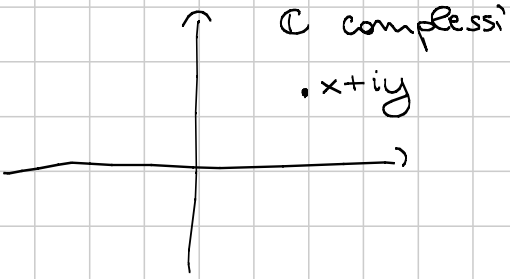
$$x^2 + k^2(x-1)^2 = 1$$

$x=1$ è soluzione, è razionale $\Rightarrow$

anche l'altra sol dell'eq di 2° grado è razionale.

Numeri complessi.





Moltiplicazione?

In $\mathbb{R}$, prodotto scalare

$(x_1, y_1) \cdot (x_2, y_2) := x_1x_2 + y_1y_2$

vett · vett = numero reale

Ok per perpendicolarità

Ex: vettori ortogonali $\Leftrightarrow$ prod scal = 0

In $\mathbb{C}$, moltiplicazione

$(x+iy)(u+iv) := xu - yv + i(xv + yu)$

compl · compl = complesso.

$i^2 = -1$

$$(\cos\alpha + i\sin\alpha)(x+iy) = x\cos\alpha - y\sin\alpha + i(x\sin\alpha + y\cos\alpha)$$

Moltiplicare per $\cos\alpha + i\sin\alpha$ equivale a ruotare di α!

$$x+iy = \cos\beta + i\sin\beta$$

$$(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) = \cos\alpha+\beta + i\sin\alpha+\beta. \quad (*)$$

Definizione: $e^{i\alpha} := \cos\alpha + i\sin\alpha$.

Abbiamo mostrato (*)

$$e^{i(\alpha+\beta)} = e^{i\alpha} \cdot e^{i\beta}$$

Ex: $\cos 3\alpha = \cos(2\alpha+\alpha) = \ldots$

$\cos 6\alpha = \ldots$

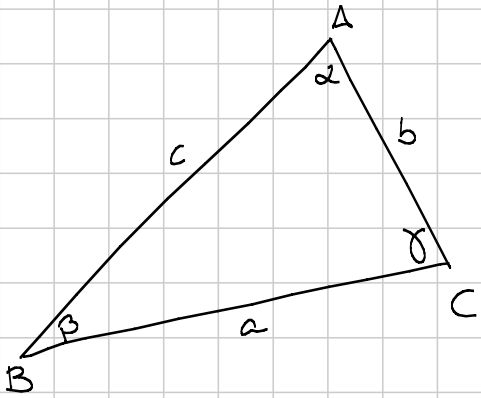
$$\cos 6\alpha = \mathrm{Re}\left(e^{i6\alpha}\right)$$
$$= \mathrm{Re}\left(\underbrace{e^{i\alpha} \cdot e^{i\alpha} \cdot \ldots \cdot e^{i\alpha}}_{6 \text{ volte}}\right)$$
$$= \mathrm{Re}\left((e^{i\alpha})^6\right)$$
$$= \mathrm{Re}\left((\cos\alpha + i\sin\alpha)^6\right)$$

$$= (\cos\alpha)^6 + \binom{6}{2} \cos^2\alpha \sin^4\alpha - \binom{6}{4} \cos^4\alpha \sin^2\alpha - \sin^6\alpha$$

TRIGONOMETRIA

- 3 lati
- 2 lati e un angolo
- 1 lato e 2 angoli

Un triangolo ha 3 gradi di libertà.



Teorema dei seni

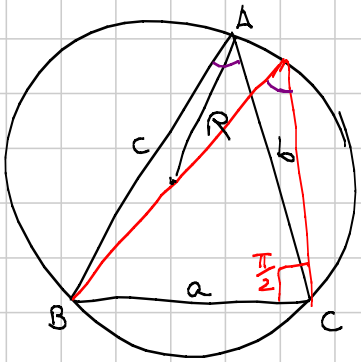
$$\frac{a}{\sin\alpha} = \frac{b}{\sin\beta} = \frac{c}{\sin\gamma} = 2R$$

Dim:

$a = 2R\sin\alpha$ (guardando $\triangle_R$)

$2R = \frac{a}{\sin\alpha}$

Stessa cosa sugli altri lati:...

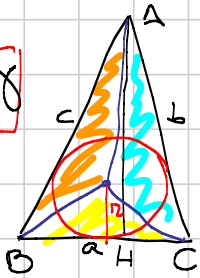


Formule per l'area

$$[ABC] = \frac{\overline{BC}\cdot\overline{AH}}{2} = \frac{a\cdot b\sin\gamma}{2} = \frac{1}{2}ab\sin\gamma$$

$$= \frac{abc}{4R}$$

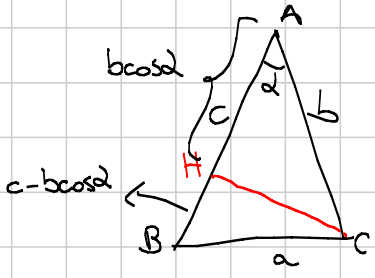
$$[ABC] = \frac{a+b+c}{2}r$$



Teorema di Carnot

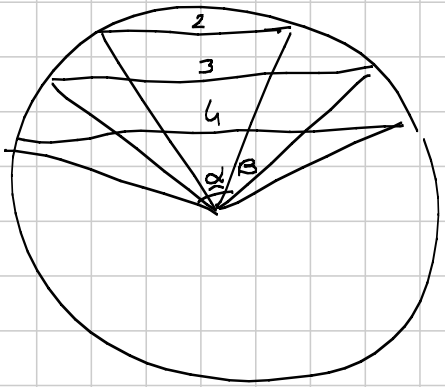
Noti b, c, α, quanto vale a?

$$a^2 = b^2 + c^2 - 2bc\cos\alpha$$

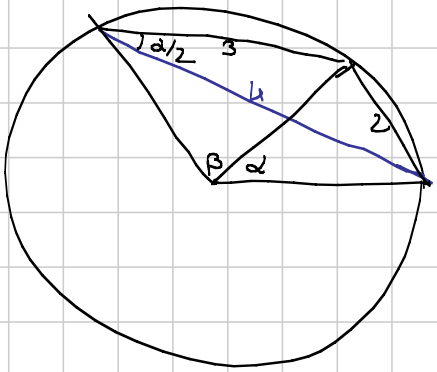


$$a^2 = \overline{BH}^2 + \overline{HC}^2 = (c - b\cos\alpha)^2 + b^2\sin^2\alpha$$
$$= c^2 - 2bc\cos\alpha + b^2\cos^2\alpha + b^2\sin^2\alpha$$
$$= b^2 + c^2 - 2bc\cos\alpha \,. \qquad (b^2)$$

Ex libretto
Corde lunghe 2, 3, 4 insistono su $\alpha, \beta, \alpha+\beta$.
$\cos\alpha$?



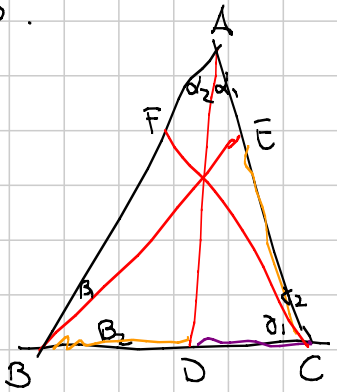
Per il teo di Carnot
$$2^2 = 3^2 + 4^2 - 2\cdot 3\cdot 4\cdot \cos\frac{\alpha}{2}$$
$$4 = 25 - 24\cdot\cos\frac{\alpha}{2}$$
$$24\cos\frac{\alpha}{2} = 21$$
$$\cos\frac{\alpha}{2} = \frac{7}{8}$$
$$\cos^2\frac{\alpha}{2} = \frac{1+\cos\alpha}{2}$$
$$\left(\frac{7}{8}\right)^2 = \frac{1+\cos\alpha}{2}$$
Risolvendo $\cos\alpha = \frac{17}{32}$ (forse).



Ex: teorema di Ceva trigonometrico.

Si fa che

$$\frac{\sin\alpha_1}{\sin\alpha_2} \cdot \frac{\sin\beta_1}{\sin\beta_2} \cdot \frac{\sin\gamma_1}{\sin\gamma_2} = 1.$$



Teorema d. Ceva:

$$\frac{BD}{DC} \cdot \frac{CE}{EA} \cdot \frac{AF}{FB} = 1 \qquad (*)$$

Dim: ved. G3.

Dim di Ceva trigo dato Ceva:

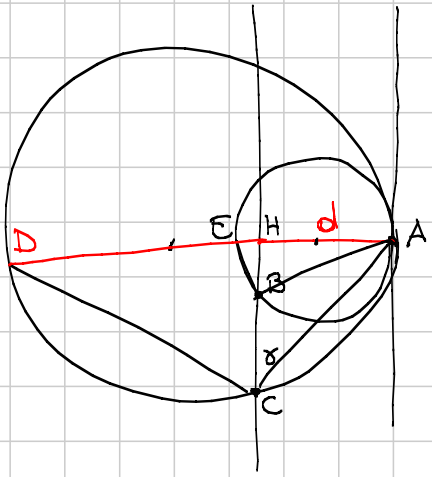
Dal teorema dei seni su ABD

$$\frac{BD}{\sin\alpha_2} = \frac{AD}{\sin\beta} \Rightarrow BD = \frac{\sin\alpha_2}{\sin\beta} \cdot AD$$

Ripetiamo sui 6 triangolini e sostituiamo in (*)

Ex: vederlo.

Ex 10 test iniziale.
Calcolare il raggio della circo circoscritta ad ABC (viene indipendente da d).



$\hat{ABE}$, teorema di Euclide

$AB^2 = AH \cdot AE$

$AB = \sqrt{2dr}$

$AC^2 = AH \cdot AD$

$AC = \sqrt{2dR}$

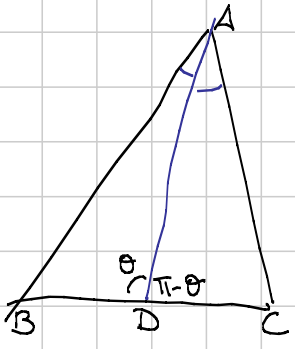
raggio cercato $= \frac{AB}{2\sin\gamma}$ (per il teo dei seni)

$\sin\gamma = \frac{d}{AC}$ (vedi triangolo $\hat{ACH}$)

raggio $= \frac{\sqrt{2dr}\,\sqrt{2dR}}{2d} = \sqrt{rR}$.

Ex: teorema della bisettrice

$$\frac{BD}{DC} = \frac{AB}{AC}$$



Dim:

Teorema dei seni su $\hat{ABD}$ dice

$$\frac{AB}{\sin\theta} = \frac{BD}{\sin\frac{\alpha}{2}}$$

$$\Rightarrow \boxed{\frac{BD}{AB}} = \frac{\sin\frac{\alpha}{2}}{\sin\theta} = \circledast$$

Teorema dei seni su $\hat{ADC}$

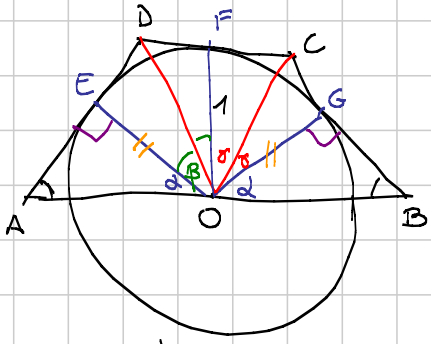
$$\frac{AC}{\sin\theta} = \frac{DC}{\sin\alpha/2}$$

$$\boxed{\frac{DC}{AC}} = \frac{\sin\alpha/2}{\sin\theta} = (*)$$

Es 9 libretto.

AD, DC, BC tangenti al cerchio centrato nel pto medio di AB.

Tesi: $AB^2 = 4\, BC \cdot AD$



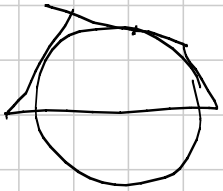
Oss: $\hat{A} = \hat{B}$.

I triangoli $A\hat{E}O$ e $G\hat{O}B$ sono congruenti.

(volendo $AE = GB$ poiché A e B hanno la stessa potenza)

$\alpha + 2\beta + 2\gamma + \alpha = \pi$ ovvero

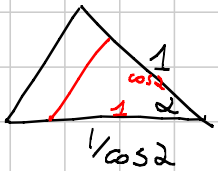
$\alpha + \beta + \gamma = \pi/2$.



$$AB = 2\,AO = \frac{2}{\cos\alpha}$$

$$BC = BG + GC = \tg\alpha + \tg\gamma$$

$$AD = AE + ED = \tg\alpha + \tg\beta$$



Dobbiamo dimostrare

$$\frac{1}{\cos^2\alpha} = \underbrace{(\tg\alpha + \tg\gamma)(\tg\alpha + \tg\beta)}_{RHS}$$

1° modo $\gamma = \frac{\pi}{2} - \alpha - \beta$, sviluppare $\tg\gamma = \ldots$

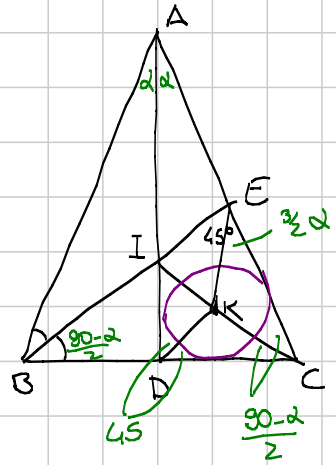
2° modo

$$RHS = \tg^2\alpha + \tg\alpha\,\tg\gamma + \tg\beta\,\tg\alpha + \tg\beta\,\tg\gamma$$
$$= \tg^2\alpha + 1$$

↑ fatto visto prima con α al posto di $\frac{\alpha}{2}$
(ie vincolo diventa, $\alpha+\beta+\gamma=\frac{\pi}{2}$)

Resta da dim
$\frac{1}{\cos^2\alpha} = (\tg^2\alpha+1)\cos^2\alpha = \sin^2\alpha+\cos^2\alpha$

$$\boxed{\frac{1}{\cos^2\alpha} = \tg^2\alpha + 1}$$



Ex IMO 09 - 4
$\hat B = \hat C$
BE bisettrice di $\hat B$
K centro della "incirconf" di ADC

Trovare $B\hat AC$.

Oss: IKC allineati (sulla bisettr di $\hat C$)

$K\hat EC = 180 - \frac{90-\alpha}{2} - (90-\alpha) - 45 = \frac{3}{2}\alpha$

$E\hat IK = 180 - \frac{3}{2}\alpha - 45 - \frac{90-\alpha}{2} = 90-\alpha$

Idea: calcolo $\frac{IK}{KC}$ in 2 modi diversi.

Dal teo dei seni su $\hat{EIK}$ $\quad \frac{IK}{\sin 45} = \frac{EK}{\cos\alpha}$

" " " " " $E\hat KC$ $\quad \frac{KC}{\sin\frac{3}{2}\alpha} = \frac{EK}{\sin\frac{90-\alpha}{2}}$

Quindi:
$$\frac{IK}{KC} = \frac{\sin 45 \ \sin\frac{90-\alpha}{2}}{\cos\alpha \ \sin\frac{3}{2}\alpha}$$

D'altra parte
$$\frac{IK}{KC} = \frac{ID}{DC} = \tg\frac{90-\alpha}{2}$$

α deve soddisfare
$$\tg\frac{90-\alpha}{2} = \frac{\sin 45 \ \sin\frac{90-\alpha}{2}}{\cos\alpha \ \sin\frac{3}{2}\alpha}$$

$$\frac{\sin\frac{90-\alpha}{2}}{\cos\frac{90-\alpha}{2}}$$

ovvero

$$\cos\alpha \sin\tfrac{3}{2}\alpha = \sin 45 \cos\frac{90-\alpha}{2}.$$

Fatto generale:

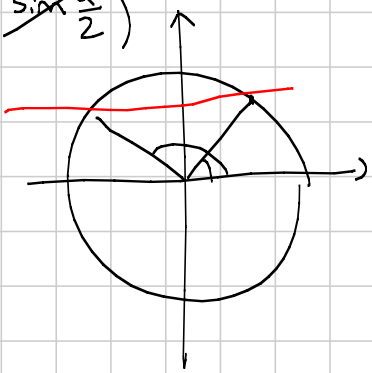
$$\sin(x+y) = \sin x\cos y + \sin y\cos x$$

$$\sin(x-y) = \sin x\cos y - \sin y\cos x$$

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

$$\frac{1}{2}\left(\sin\tfrac{5}{2}\alpha + \sin\tfrac{\alpha}{2}\right) = \frac{1}{2}\left(\sin\frac{90-\alpha}{2} + \sin\tfrac{\alpha}{2}\right)$$

$$\sin\tfrac{5}{2}\alpha = \sin\frac{90-\alpha}{2}$$



Ci sono 2 casi:

$$\begin{cases} \frac{5}{2}\alpha = 90 - \frac{\alpha}{2} + 2\cdot k\cdot 180 \\ \text{oppure} \\ \frac{5}{2}\alpha = 180 - (90 - \frac{\alpha}{2}) + 2k\,180 \end{cases}$$

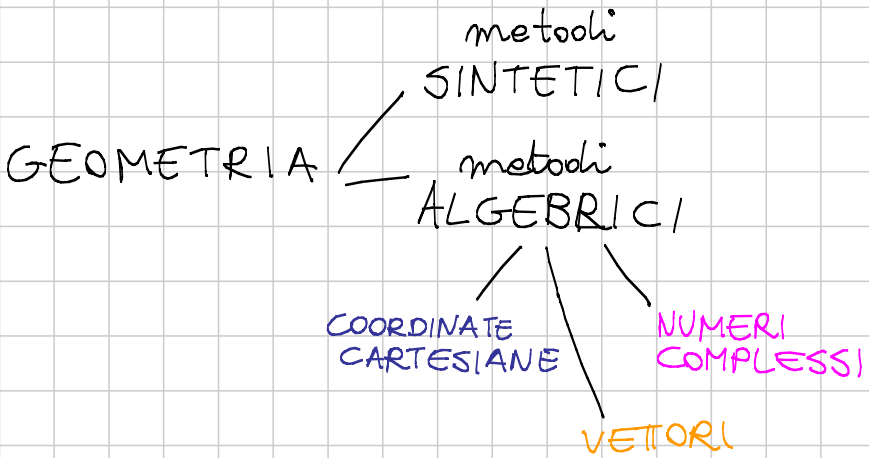
$\alpha \in (0, 90)$

$\alpha = 30$ (dalla 1ª con $k=0$)

$\alpha = 45$.

G2 - METODI ALGEBRICI

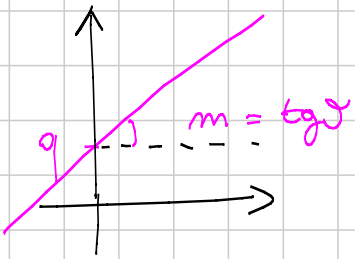
Titolo nota 07/09/2011



COORDINATE

- RETTA $y = mx + q$

m = coeff. angolare



mancano le parallele all'asse y!

$ax + by + c = 0$

- rette $\parallel$ hanno = coeff angolare
- rette $\perp$ hanno coeff ang. m_1, m_2 | $m_1 m_2 = -1$

- CIRCONFERENZA

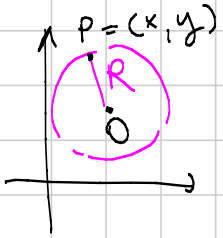
$x^2 + 3y^2 + x + 5 = 0$ NO

$2x^2 + 2y^2 = 8$ OK

$x^2 + y^2 + ax + by + c = 0$

ACHTUNG! non è sempre una circ. (reale)

e.g. $x^2 + y^2 + 1 = 0$



$O: (x_0, y_0)$

$(x - x_0)^2 + (y - y_0)^2 = R^2$

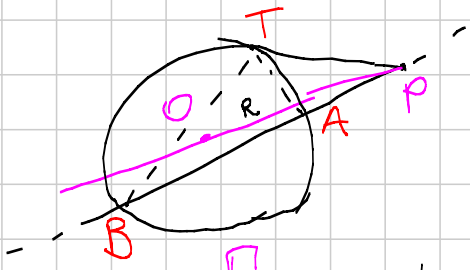
$\left(x + \frac{a}{2}\right)^2 - \frac{a^2}{4} + \left(y + \frac{b}{2}\right)^2 - \frac{b^2}{4} + c = 0$

CONDIZIONE: $\frac{a^2}{4} + \frac{b^2}{4} \geq c$

CENTRO: $\left(-\frac{a}{2}, -\frac{b}{2}\right)$

RAGGIO: $R^2 = \frac{a^2}{4} + \frac{b^2}{4} - c$

- POTENZA di pto rispetto a circ.



$\text{pow}_\Gamma(P) = PA \cdot PB$

dimostro $PT^2 = PA \cdot PB$

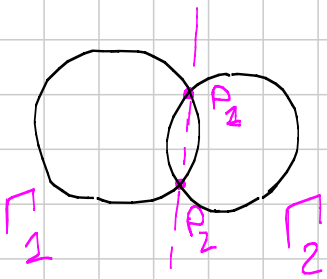
$OP = d$

$\text{pow}_\Gamma(P) = (d - R)(d + R) = d^2 - R^2$

$\Gamma \quad (x - x_0)^2 + (y - y_0)^2 = R^2 \qquad P \quad (a, b)$

$\text{pow}_\Gamma(P) = (a - x_0)^2 + (b - y_0)^2 - R^2$

- ASSE RADICALE



luogo dei punti P tali che

$$pow_{\Gamma_1}(P) = pow_{\Gamma_2}(P)$$

Γ_1 $x^2+y^2+a_1x+b_1y+c_1=0$

Γ_2 $x^2+y^2+a_2x+b_2y+c_2=0$

(x,y) |

$$x^2+y^2+a_1x+b_1y+c_1 = x^2+y^2+a_2x+b_2y+c_2$$

$$(a_1-a_2)x+(b_1-b_2)y+c_1-c_2=0$$

è l'equazione di una retta!

- LA RETTA per 2 PUNTI

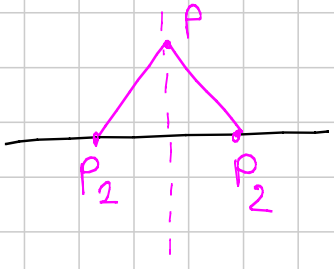
$P_1: (a_1, b_1)$
$P_2: (a_2, b_2)$

$\alpha x+\beta y+\gamma=0$

$$\frac{x-a_1}{a_2-a_1} = \frac{y-b_1}{b_2-b_1}$$

← primo grado (in x, y), si annulla in P_1, P_2 → è la retta per P_1, P_2

- L'ASSE di un SEGMENTO

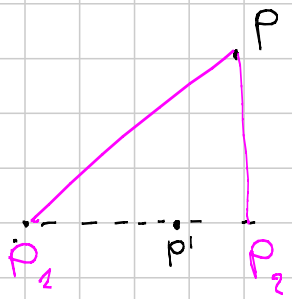


$P_1\,(a_1,b_1)$ $P_2\,(a_2,b_2)$

$P\,(x,y)$ |

$$(x-a_1)^2+(y-b_1)^2 = (x-a_2)^2+(y-b_2)^2$$

- CIRCONFERENZA di APOLLONIO



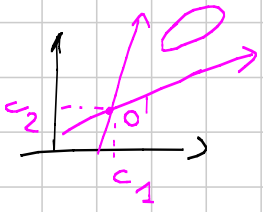
$PP_1 = \lambda PP_2$

$\lambda > 0$

(esattamente come prima: pol. di 2° grado in x e y, coeff x^2 = coeff y^2, non ci sono termini misti (in xy))

PROBLEMI "INVARIANTI PER AFFINITÁ"

$(x, y) \longmapsto (a_1x + b_1y + c_1,\ a_2x + b_2y + c_2)$



AFFINITÁ

mandano RETTE in RETTE

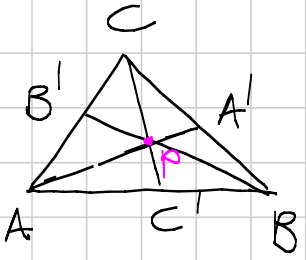
CIRCONFERENZE in ? ELLISSI →

conservano
- parallelismo
- rapporti fra aree
- rapporti di segmenti su stessa retta

NON conservano
- angoli
- lunghezze

∃! affinità

3 punti non allineati → 3 punti non allineati



CESE 6 . 2004

$x = \frac{AP}{PA'}$

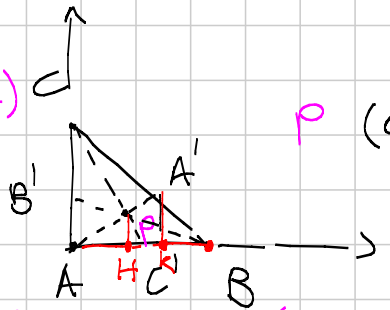
$y = \frac{BP}{PB'}$

$z = \frac{CP}{CP'}$

$xyz = x+y+z+2$

è invariante per affinità!

equilatero (mah...)



AB $y = 0$

AC $x = 0$

BC $y = -x + 1$

$x = \frac{a}{b}y$ $\quad y = -\frac{a}{b}x + \frac{a}{b}$

$x = \frac{a}{a+b}$ $\quad y = \frac{b}{a+b}$

$\left(\frac{a}{a+b}, \frac{b}{a+b}\right)$ A'

AA' $\frac{x}{a} = \frac{y}{b}$

$\left(0, \frac{b}{1-a}\right)$ B' $\quad y = \frac{b}{1-a}$ $\quad x = 0$

BB' $\frac{x-1}{a-1} = \frac{y}{b}$

$\left(\frac{a}{1-b}, 0\right)$ C'

CC' $\frac{x}{a} = \frac{y-1}{b-1}$

$\frac{AP}{PA'} = \frac{a}{a\left(1+\frac{1}{a+b}\right)} = \frac{a+b}{1+a-b}$

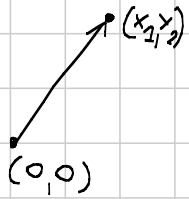
$\frac{BP}{PB'} = \frac{1-a}{a}$

$\frac{CP}{CC'} = \frac{1-b}{b}$

VETTORI

coordinate

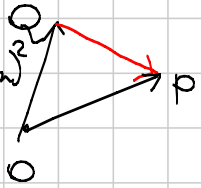
$(x_1, x_2, \dots, x_n) \in \mathbb{R}^n$



norma $\|(x_1, x_2, \dots, x_n)\|^2 = x_1^2 + x_2^2 + \dots + x_n^2$

$\|\vec{P} - \vec{Q}\|^2 = (x_1-y_1)^2 + (x_2-y_2)^2 + \dots + (x_n-y_n)^2$

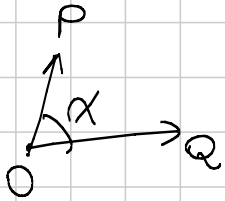
$(x_1, \dots, x_n)$ $(y_1, \dots, y_n)$



prodotto scalare

$\vec{P} \cdot \vec{Q} = x_1y_1 + x_2y_2 + \dots + x_ny_n$

$\vec{P} \cdot \vec{Q} = \|\vec{P}\| \, \|\vec{Q}\| \cos\alpha$

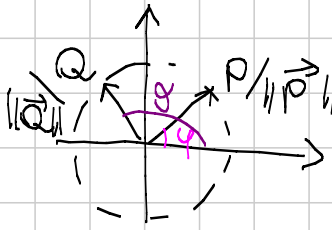


dimostrazione nel piano

$\vec{P} \cdot \lambda\vec{Q} = \lambda \, \vec{P} \cdot \vec{Q}$

$\vec{P} \cdot \vec{Q} = \|\vec{P}\| \|\vec{Q}\| \left(\frac{\vec{P}}{\|\vec{P}\|} \cdot \frac{\vec{Q}}{\|\vec{Q}\|} \right)$

?



$\frac{\vec{P}}{\|\vec{P}\|} = (\cos\varphi, \operatorname{sen}\varphi)$

$\frac{\vec{Q}}{\|\vec{Q}\|} = (\cos\vartheta, \operatorname{sen}\vartheta)$

$? = \cos\varphi\cos\vartheta + \operatorname{sen}\vartheta\operatorname{sen}\varphi =$

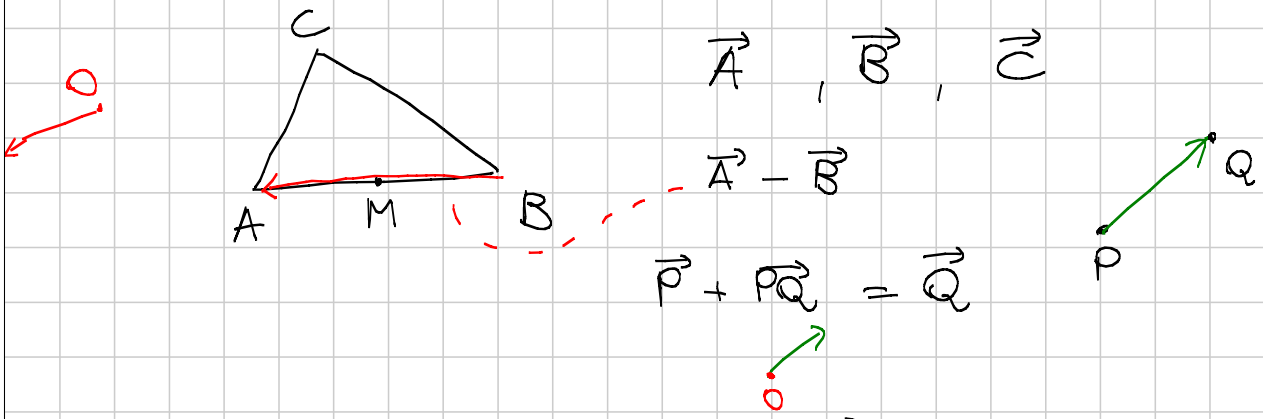
$= \cos(\vartheta - \varphi) = \cos\alpha$

$\|\vec{P}\|^2 = \vec{P}\cdot\vec{P}$

$\vec{P}\cdot\vec{Q} = 0$

$\vec{P} \perp \vec{Q}$

$\|\vec{P}+\vec{Q}\|^2 = \|\vec{P}\|^2 + \|\vec{Q}\|^2 + 2(\vec{P}\cdot\vec{Q})$



$\vec{A}$, $\vec{B}$, $\vec{C}$

$\vec{A}-\vec{B}$

$\vec{P}+\vec{PQ} = \vec{Q}$

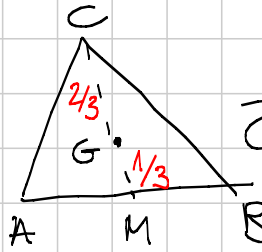
punto medio di AB $\quad \frac{\vec{A}+\vec{B}}{2}$

retta AB $\quad \vec{A}+\lambda(\vec{B}-\vec{A}) \quad \lambda \in \mathbb{R}$

segmento AB $\quad \lambda \in [0,1]$

punto medio $\quad \lambda = \frac{AM}{AB} = \frac{1}{2}$

BARICENTRO



$\vec{G}$

$\vec{C}+\lambda(\vec{M}-\vec{C}) =$ ← retta CM da (partendo da C)

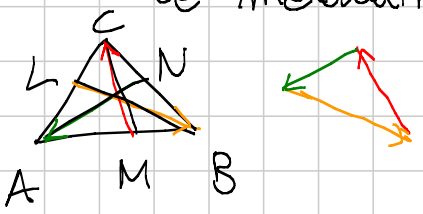
$= \vec{C} + \lambda\left(\frac{\vec{A}+\vec{B}}{2} - \vec{C}\right)$

$\lambda = \frac{CG}{CM} = \frac{2}{3}$

$\vec{G} = \vec{C} + \frac{1}{3}(\vec{A}+\vec{B}) - \frac{2}{3}\vec{C} = \boxed{\frac{1}{3}(\vec{A}+\vec{B}+\vec{C})}$

ESERCIZIO

le mediane "formano un triangolo"



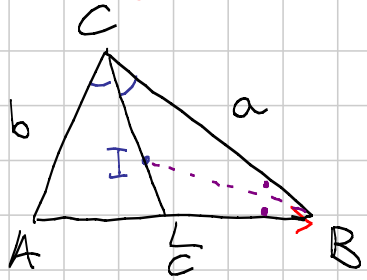
$(\vec{C}-\vec{M})+(\vec{A}-\vec{N})+(\vec{B}-\vec{L})=0$

TESI

$\vec{A}+\vec{B}+\vec{C}-\frac{1}{2}\vec{A}-\frac{1}{2}\vec{A}-\dots=0$ ($-\vec{A}$)

$\vec{C}-\frac{\vec{A}}{2}-\frac{\vec{B}}{2}+-\vec{A}-\frac{\vec{B}}{2}-\frac{\vec{C}}{2}+\vec{B}-\frac{\vec{C}}{2}-\frac{\vec{A}}{2}$

INCENTRO



$b:a+b=AL:BL+AL$

$b:a=AL:BL$

$\vec{L}=\vec{A}+\lambda(\vec{B}-\vec{A})$

$\frac{AL}{AB}=\frac{b}{a+b}$

ó

$\vec{L}=\frac{b}{a+b}\vec{B}+\frac{a}{a+b}\vec{A}$

$1-\lambda$, $\lambda=\frac{b}{a+b}$

retta CL

$\vec{C}+\mu(\vec{L}-\vec{C})$

$\vec{I}=\vec{C}+\mu(\vec{L}-\vec{C})$ con $\mu=\frac{CI}{CL}$

Teo della bisettrice su BCL mi dà

$a:BL=CI:IL$

$a:BL+a=CI:IL+CI$

$$\mu = \frac{a}{BL+a} = \frac{a}{a\left(\frac{c}{a+b}+1\right)} = \frac{a+b}{a+b+c}$$

$$\overrightarrow{LB} = \vec{B} - \vec{L} = -\vec{A}\frac{a}{a+b} + \vec{B}\frac{a}{a+b} =$$

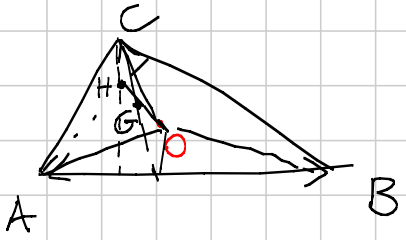
$$= \frac{a}{a+b}(\vec{B}-\vec{A})$$

$$\|\overrightarrow{LB}\| = \frac{a}{a+b}c$$

$$\vec{I} = \vec{C} + \frac{a+b}{a+b+c}\left(\frac{a}{a+b}\vec{A} + \frac{b}{a+b}\vec{B} - \vec{C}\right)$$

$$= \frac{1}{a+b+c}\left(a\vec{A} + b\vec{B} + c\vec{C}\right)$$

CIRCOCENTRO



$$\|\vec{A}\| = \|\vec{B}\| = \|\vec{C}\| = R$$

SE origine la metto nel circocentro

ORTOCENTRO

$\vec{O}$ è l'origine $\rightarrow$

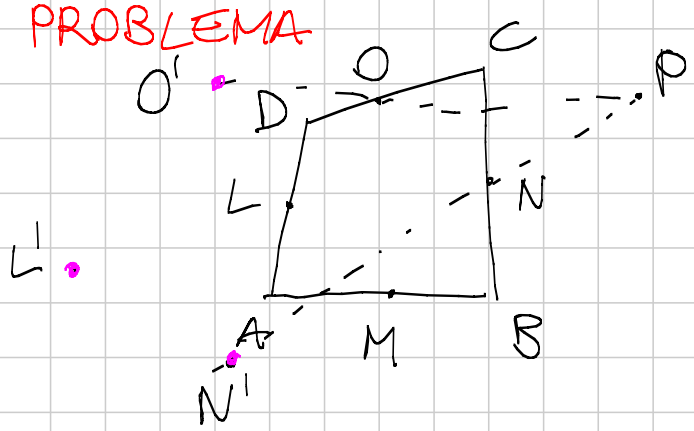
retta OH $\quad \lambda\left(\frac{\vec{A}+\vec{B}+\vec{C}}{3}\right)$

punto H è su OH con $\lambda = \frac{OH}{OG} = 3$

$\vec{H} = \vec{A} + \vec{B} + \vec{C}$

SE $\vec{O}$ è l'origine

PROBLEMA



tesi

$N'M'L'O'$

è un parallelogrammo!

$N \quad \frac{\vec{B}+\vec{C}}{2} \quad N' \quad \vec{B}+\vec{C}$

se origine in P

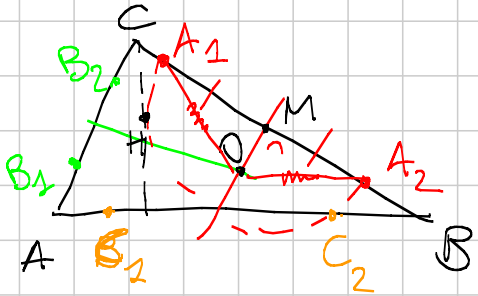
$M' \quad \vec{A}+\vec{B}$

$O' \quad \vec{D}+\vec{C}$

$L' \quad \vec{A}+\vec{D}$

$$\vec{N'O'} = \vec{O'} - \vec{N'} = \vec{D} - \vec{B}$$
$$\vec{M'L'} = \vec{L'} - \vec{M'} = \vec{D} - \vec{B}$$

IMO 2008. 1



$A_1A_2C_2C_1B_1B_2$ è ciclico

origine in O !

$$\|\vec{A}_1\|^2 = \|\vec{B}_2\|^2$$

$$OM^2 + MA_1^2$$

$$\left\|\frac{\vec{B}+\vec{C}}{2}\right\|^2 + \left\|\vec{A}+\frac{\vec{B}+\vec{C}}{2}\right\|^2$$

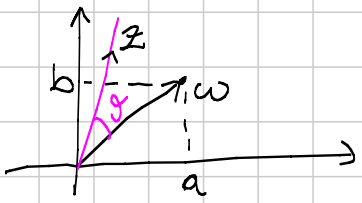
$$\left\|\frac{\vec{B}+\vec{C}}{2}\right\|^2 + \left\|\vec{A}+\frac{\vec{B}+\vec{C}}{2}\right\|^2$$

$$\|B_1\|^2 = \left\|\frac{\vec{A}+\vec{C}}{2}\right\|^2 + \left\|\vec{B}+\frac{\vec{A}+\vec{C}}{2}\right\|^2$$

$$\|\vec{A}\|^2 = \|\vec{B}\|^2 = \|\vec{C}\|^2$$

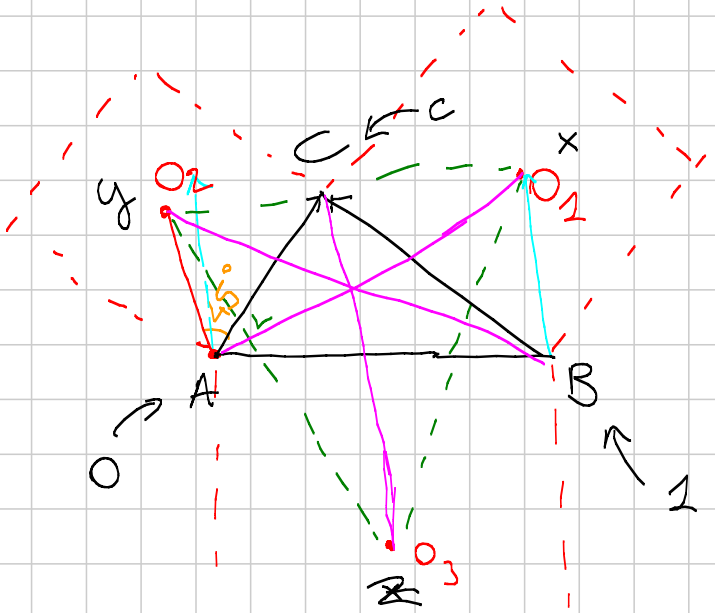
□

NUMERI COMPLESSI



$w = a + ib$

$z = w \cdot e^{i\vartheta}$



AO_1, BO_2, CO_3 concorrono.

$AO_1 = O_2O_3$

$$y = c\, e^{i\frac{\pi}{4}} \frac{\sqrt{2}}{2} = c\frac{\sqrt{2}}{2}\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = \frac{1}{2}c(1+i)$$

$$z = 1\, e^{-i\frac{\pi}{4}} \frac{\sqrt{2}}{2} = \frac{1}{2}(1-i)$$

$$x = (c-1)\, e^{-i\frac{\pi}{4}} \frac{\sqrt{2}}{2} + 1 = \frac{1}{2}(c-1)(1-i) + 1 = \frac{1}{2}(c-1+2) + i\left(\frac{1-c}{2}\right)$$

$$= \frac{1}{2}(c+1)$$

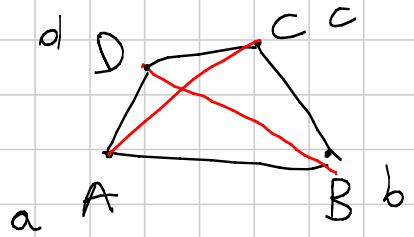
$$y - z = \frac{1}{2}c(i+1) - \frac{1}{2}(1-i) = \frac{c-1}{2} + i\left(\frac{c+1}{2}\right)$$

ruoto x di 90°

ottengo $ix = -\frac{(1-c)}{2} + i\frac{1+c}{2} =$

$= \frac{c-1}{2} + i\left(\frac{c+1}{2}\right) = y - z$

DISUGUAGLIANZA di TOLOMEO



$AB \cdot DC + BC \cdot AD \geq AC \cdot BD$

= vale SSE ABCD è ciclico

$|b-a||d-c| + |c-b||d-a| =$ (disug. triangolare)

$= |(b-a)(d-c)| + |(c-b)(d-a)| \geq$

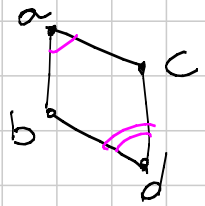
$|(b-a)(d-c) + (c-b)(d-a)| =$

$= |bd - ad + ac - bc + cd - bd - ca + ba|$

$= |c(d-b) - a(d-b)| = |(c-a)(d-b)|$

Caso di =

$$\frac{(b-a)(d-c)}{(c-b)(d-a)} \in \mathbb{R}$$

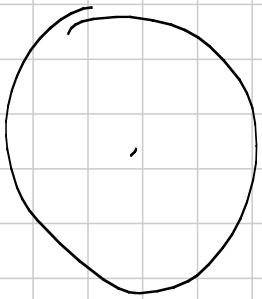


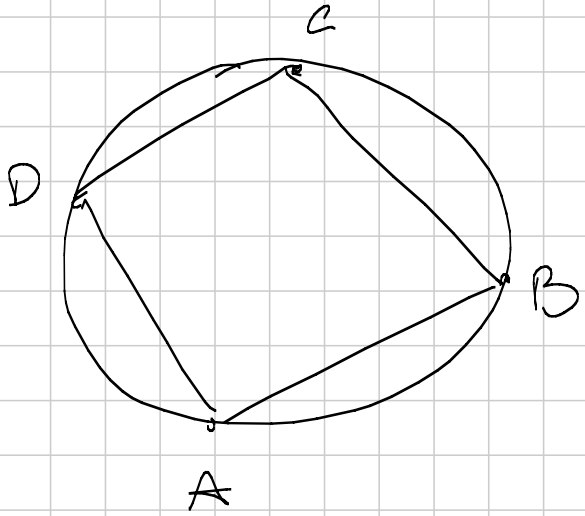
G3 - BASIC

53 the best (Julian)

Titolo nota 08/09/2011

Circonferenza = Luogo dei punti P equidistanti da un punto dato

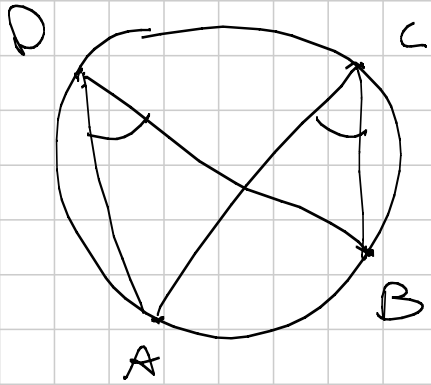




ABCD ciclico
$\Leftrightarrow$ i 4 punti stanno su una circ.

$\Updownarrow$

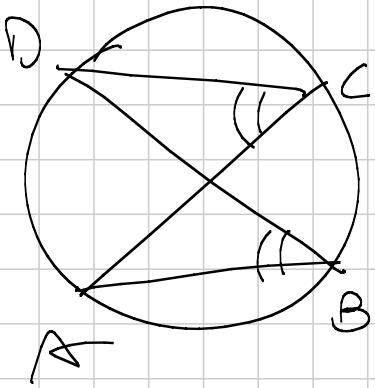
$D\hat{A}B = \pi - D\hat{C}B$



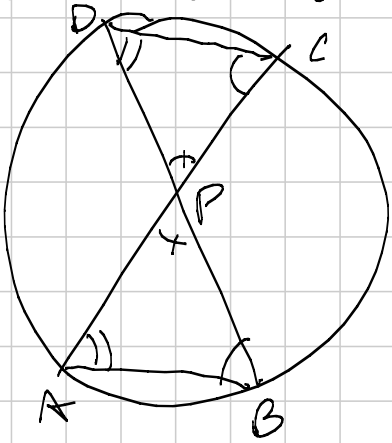
$A\hat{D}B \cong A\hat{C}B$

$\Updownarrow$

ABCD ciclico



Teorema delle corde



$ABCD$ ciclico

$PA \cdot PC$ $P \in AC \cap BD$

$=$

$PB \cdot PD$

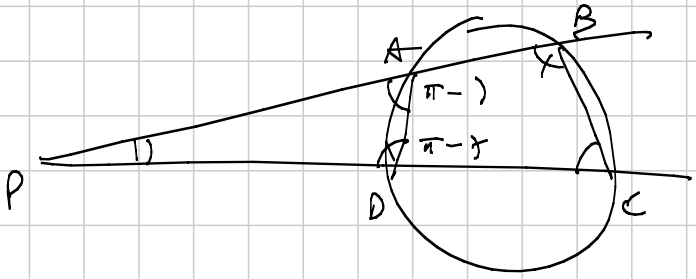
$P\hat{A}B \sim P\hat{D}C$

per il secondo criterio

$\Downarrow$

$$\frac{PA}{PB} = \frac{PD}{PC} \Rightarrow PA \cdot PC = PB \cdot PD$$

Teorema delle secanti



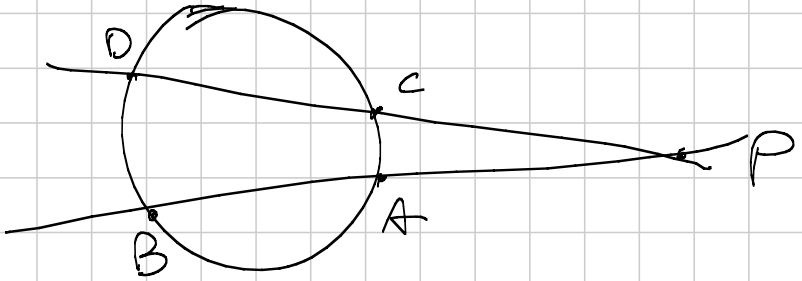
$PA \cdot PB$

$=$

$PD \cdot PC$

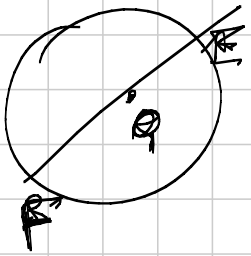
$\hat{PAD} \sim \hat{PCB} \Rightarrow \frac{PD}{PA} = \frac{PB}{PC} \Rightarrow$ Th

Potenza

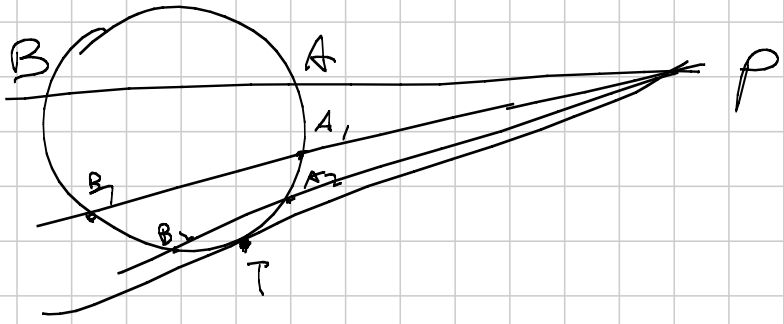


$Pow_\Gamma(P) = PA \cdot PB$

$PC \cdot PD = PA \cdot PB$



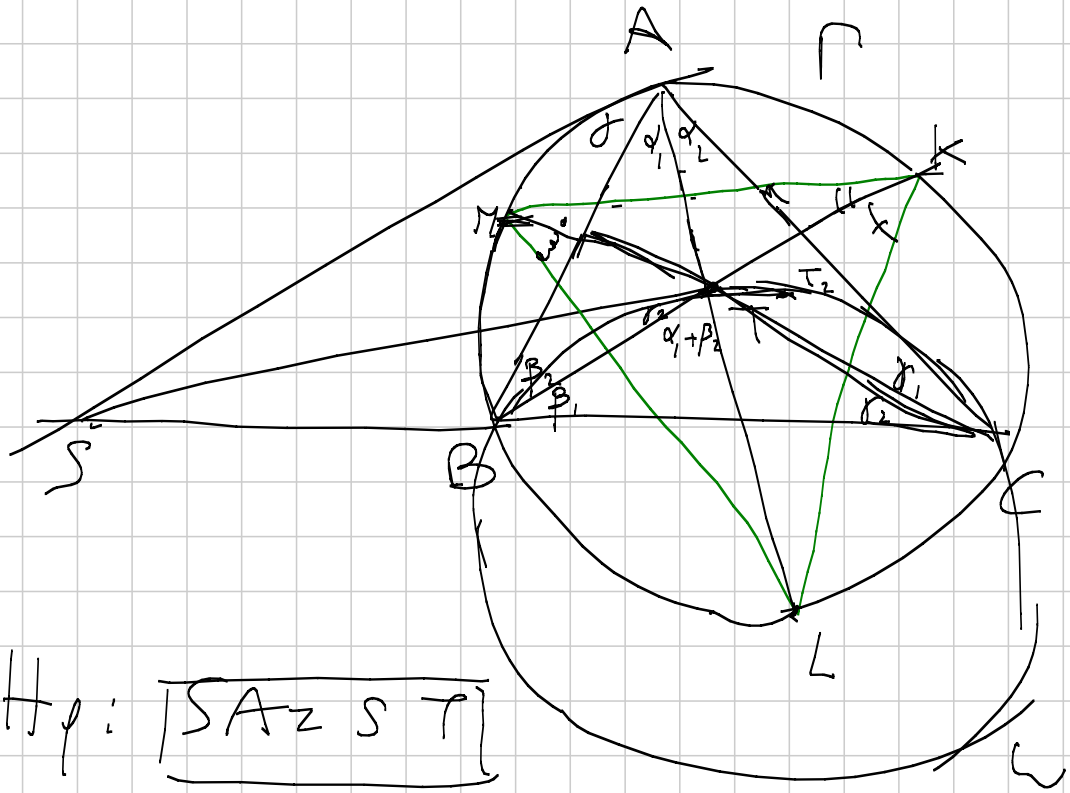
$Pow_\Gamma(Q) = QE \cdot QF$



$PA \cdot PB = PA_1 \cdot PB_1 = PA_2 \cdot PB_2 \rightarrow PT^2$

$Pow_\Gamma(P) = PT^2$

IMO 2010 – 4



Hp: $\boxed{SA \text{ tg } S\Gamma}$

Th: $ML = KL$

$SA^2 = SB \cdot SC = Pow_\Gamma(S)$

$\parallel$

ST^2

$ST^2 = SB \cdot SC$

Prendiamo la circ. ω che passa per B, C, T. Vogliamo dimostrare che ω tange ST. Perché se ci fosse $T \neq T_2 = \omega \cap ST$

$\Rightarrow ST \cdot ST_2 = SB \cdot SC = Pow_\Gamma(S)$
$\quad\quad\quad\quad\quad\quad\quad\quad \shortparallel$
$\quad\quad\quad\quad\quad\quad\quad\quad ST^2$

$\Downarrow$

$ST = ST_2 \Rightarrow$ assurdo

$S\hat{T}B = T\hat{C}B$ (insistono sullo stesso arco di ω)

$T\hat{C}B = \gamma_2 \Rightarrow S\hat{T}B = \gamma_2$

$B\hat{T}L = \alpha_1 + \beta_2$ (teo. dell'ang. esterno)

$S\hat{A}T = S\hat{A}L = \alpha_1 + S\hat{A}B = \alpha_1 + \gamma_1 + \gamma_2$
$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \shortparallel$
$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \gamma_1 + \gamma_2$
(insistono sullo stesso arco)

$S\hat{T}A \overset{Hp}{=} S\hat{A}T = \alpha_1 + \gamma_1 + \gamma_2$

$$S\hat{T}A + S\hat{T}B + B\hat{T}L = \pi$$

$$\| \qquad \| \qquad \|$$

$$(\alpha_1 + \gamma_1 + \gamma_2) + (\gamma_2) + (\alpha_1 + \beta_2) = \pi$$

$$\boxed{2\alpha_1 + \beta_2 + \gamma_1 + 2\gamma_2 = \pi}$$

Lavoro sulla tesi

$$Th \iff M\hat{K}L = K\hat{M}L \iff \gamma_2 + \alpha_1 = \beta_1 + \alpha_2$$

$$\| \qquad \|$$

$$\gamma_2 + \alpha_1 \qquad \beta_1 + \alpha_2$$

Hoc: $2\alpha_1 + \beta_2 + \gamma_1 + 2\gamma_2 = \pi \Rightarrow \gamma_2 + \alpha_1 = \beta_1 + \alpha_2$

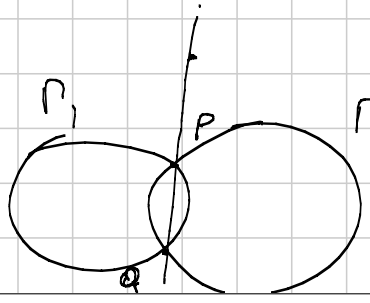
$$2\alpha_1 + \beta_2 + \gamma_1 + 2\gamma_2 = \pi$$

$$2\alpha_1 - \alpha_1 + \beta_2 + \gamma_1 + 2\gamma_2 = \pi - \alpha_1 = \alpha_1 + \alpha_2 + \beta_1 + \beta_2 + \gamma_1 + \gamma_2$$

$$\| \qquad \| \qquad \|$$

$$\alpha_1 + \gamma_2 = \beta_1 + \alpha_2 \Rightarrow \text{Win}$$

Asse radicale

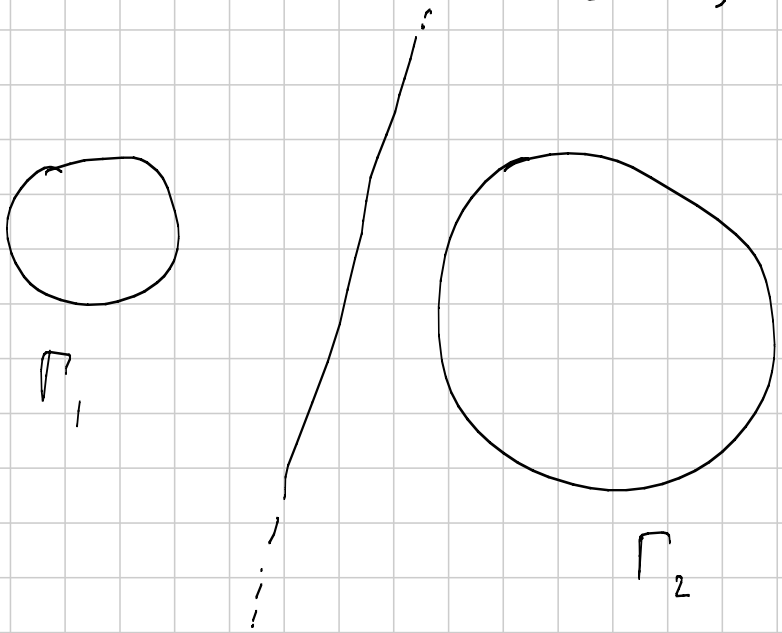


L'asse radicale r di Γ_1 e Γ_2 := la retta PQ

$A \in r \iff Pow_{\Gamma_1}(A) = Pow_{\Gamma_2}(A)$

$PA \cdot QA = PA \cdot QA$

(scelgo PQ come secante) (scelgo PQ come secante)



Def: generale = Luogo dei punti P t.c

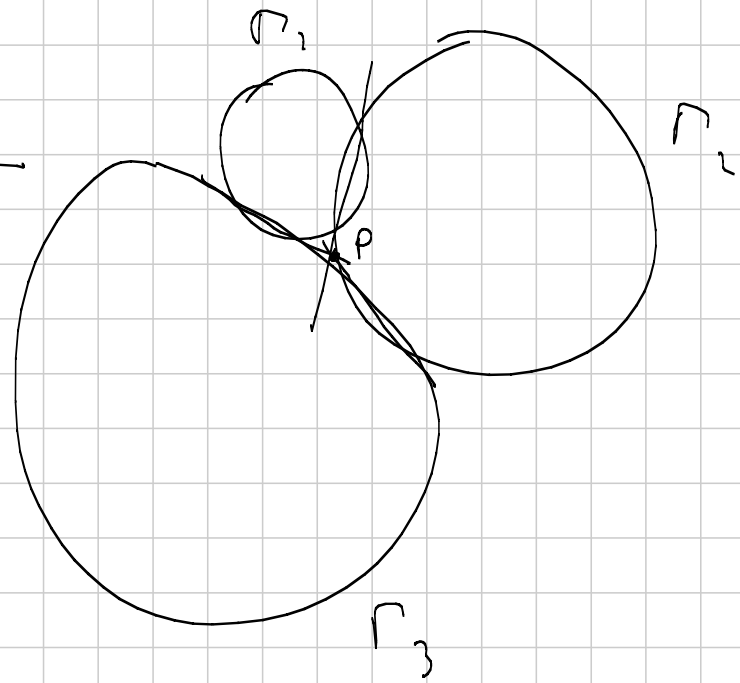
$Pow_{\Gamma_1}(P) = Pow_{\Gamma_2}(P)$

Fatto 1 Asse $\perp O_1 O_2$

dove O_1 = centro di Γ_1

e O_2 = centro di Γ_2

Fatto 2



Asse (Γ_1, Γ_2), Asse (Γ_2, Γ_3), Asse (Γ_3, Γ_1) concorrono.

$P' = \text{Asse}(\Gamma_1, \Gamma_2) \cap \text{Asse}(\Gamma_2, \Gamma_3)$

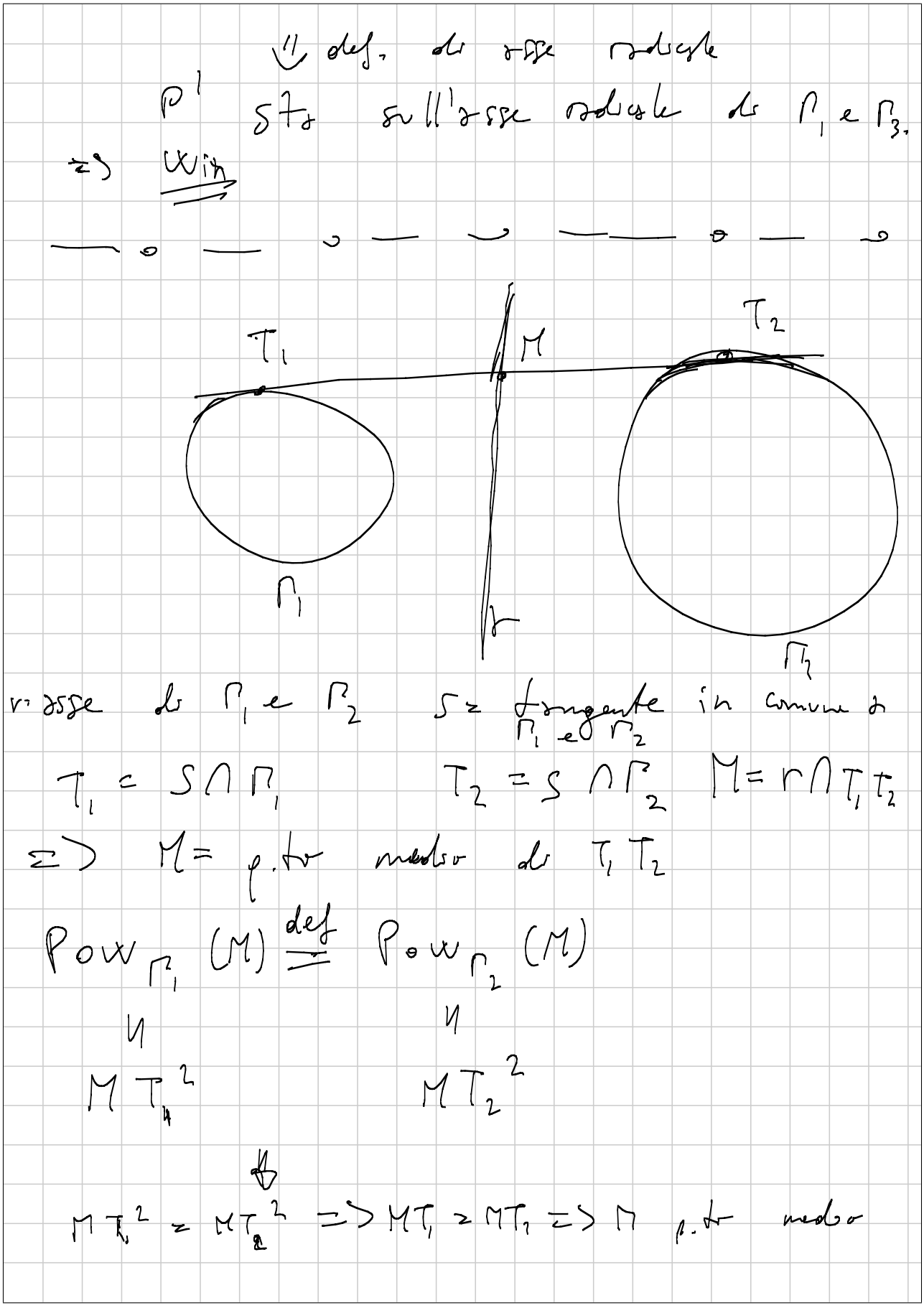
$\text{Pow}_{\Gamma_1}(P') = \text{Pow}_{\Gamma_2}(P')$

ma P' sta anche sul secondo asse

$\Rightarrow$ $\text{Pow}_{\Gamma_2}(P') = \text{Pow}_{\Gamma_3}(P')$

Asse $\Rightarrow$ $\text{Pow}_{\Gamma_1}(P') = \text{Pow}_{\Gamma_2}(P') = \text{Pow}_{\Gamma_3}(P')$

$\Rightarrow$ $\text{Pow}_{\Gamma_1}(P') = \text{Pow}_{\Gamma_3}(P')$



r asse di Γ_1 e Γ_2 S è tangente in comune a Γ_1 e Γ_2

$T_1 = S \cap \Gamma_1$ $\quad T_2 = S \cap \Gamma_2$ $\quad M = r \cap T_1 T_2$

$\Rightarrow$ M = p.to medio di $T_1 T_2$

$$Pow_{\Gamma_1}(M) \overset{def}{=} Pow_{\Gamma_2}(M)$$

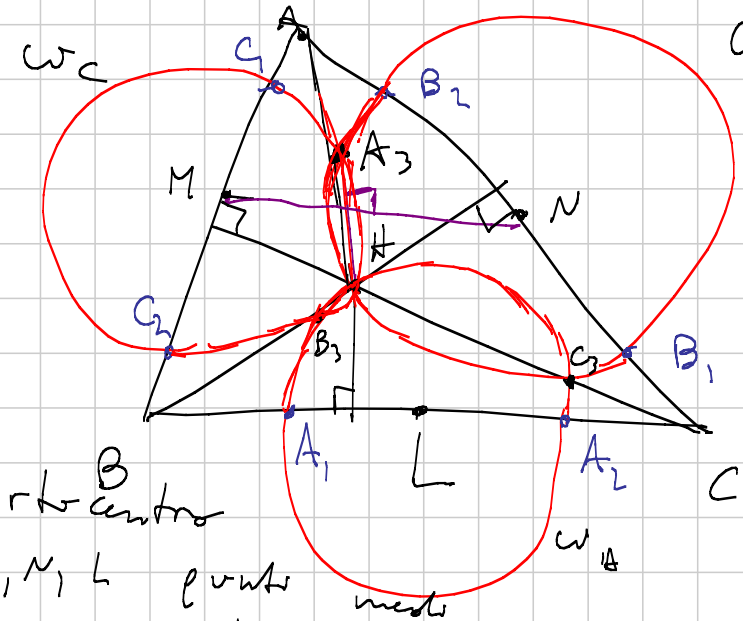
$$\| \qquad\qquad \|$$

$$MT_1^2 \qquad MT_2^2$$

$$\Downarrow$$

$MT_1^2 = MT_2^2 \Rightarrow MT_1 = MT_2 \Rightarrow M$ p.to medio

Mo 1 - 2008



Ortocentro

M, N, L punti medi

ω_A centro in L passante per H

ω_B " " N " " "

ω_C " " Γ " " "

Th: $A_1, A_2, B_1, B_2, C_1, C_2$ stanno su una circ.

$\omega_B \cap \omega_C = A_3$ e $\neq C$

Vogliamo dimostrare che $A_3 \in AH$

Fatto 1. $A_3 H$ = asse radicale di ω_B e ω_C

$\Rightarrow$ [redacted]

Fatto 2 $MN \parallel BC$

Fatto 1 + Fatto 2 = Fatto 3

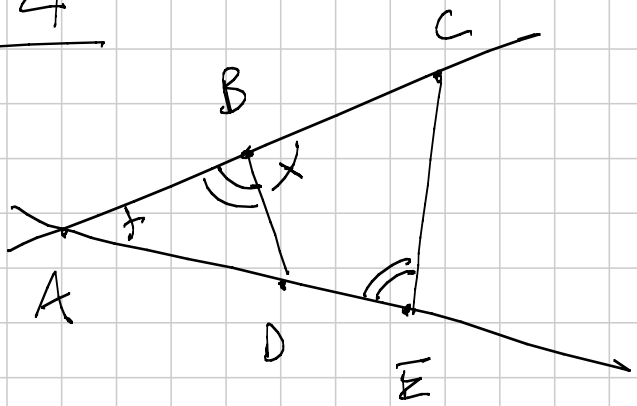
$A_3H \perp MN \parallel BC \Rightarrow A_3H \perp BC$

$\Rightarrow A_3H \equiv AH$ (retta perp. per A è unica)

$\Rightarrow A_3 \in AH \Rightarrow AH$ è asse radicale di ω_B e $\omega_C \Rightarrow Pow_{\omega_B}(A) = Pow_{\omega_C}(A)$

$\Rightarrow AB_1 \cdot AB_2 = AC_1 \cdot AC_2$

Fatto 4



Hp: $AB \cdot AC = AD \cdot AE$

Th: $DECB$ ciclico

Dim: $AB \cdot AC = AD \cdot AE \Rightarrow \frac{AB}{AD} = \frac{AE}{AC}$

$\Rightarrow$ $A\hat{B}D$ e $A\hat{E}C$ sono simili per il 1° criterio ($\hat{A}$ in comune) e $\frac{AB}{AD} = \frac{AE}{AC}$

$\Rightarrow$ $A\hat{B}D = D\hat{E}C \Rightarrow \pi - A\hat{B}D = \pi - D\hat{E}C$

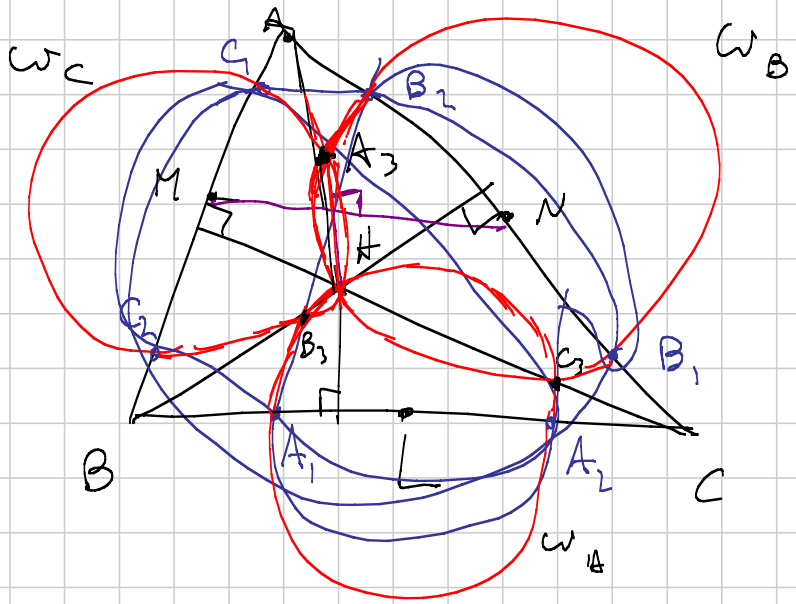
$\pi - A\hat{B}D = D\hat{B}C$

$\Rightarrow D\hat{B}C + D\hat{E}C = \pi \Rightarrow$ Th

Torno al problema

$AB_1 \cdot AB_2 = AC_1 \cdot AC_2 \Rightarrow$ $B_1 B_2 C_1 C_2$ ciclico

Ragionando in modo uguale su B_1 su C dimostro che $A_1 A_2 B_1 B_2$ e $A_1 A_2 C_1 C_2$ sono ciclici ma queste 3 potrebbero essere distinte



Asse $(A_1A_2, B_1B_2, A_1A_2, C_1C_2) = A_1A_2$

Asse $(B_1B_2, C_1C_2, A_1A_2, C_1C_2) = C_1C_2$

Asse $(A_1A_2, B_1B_2, B_1B_2, C_1C_2) = B_1B_2$

Se le 3 circ. fossero distinte

A_1A_2, B_1B_2 e C_1C_2 concorrerebbero

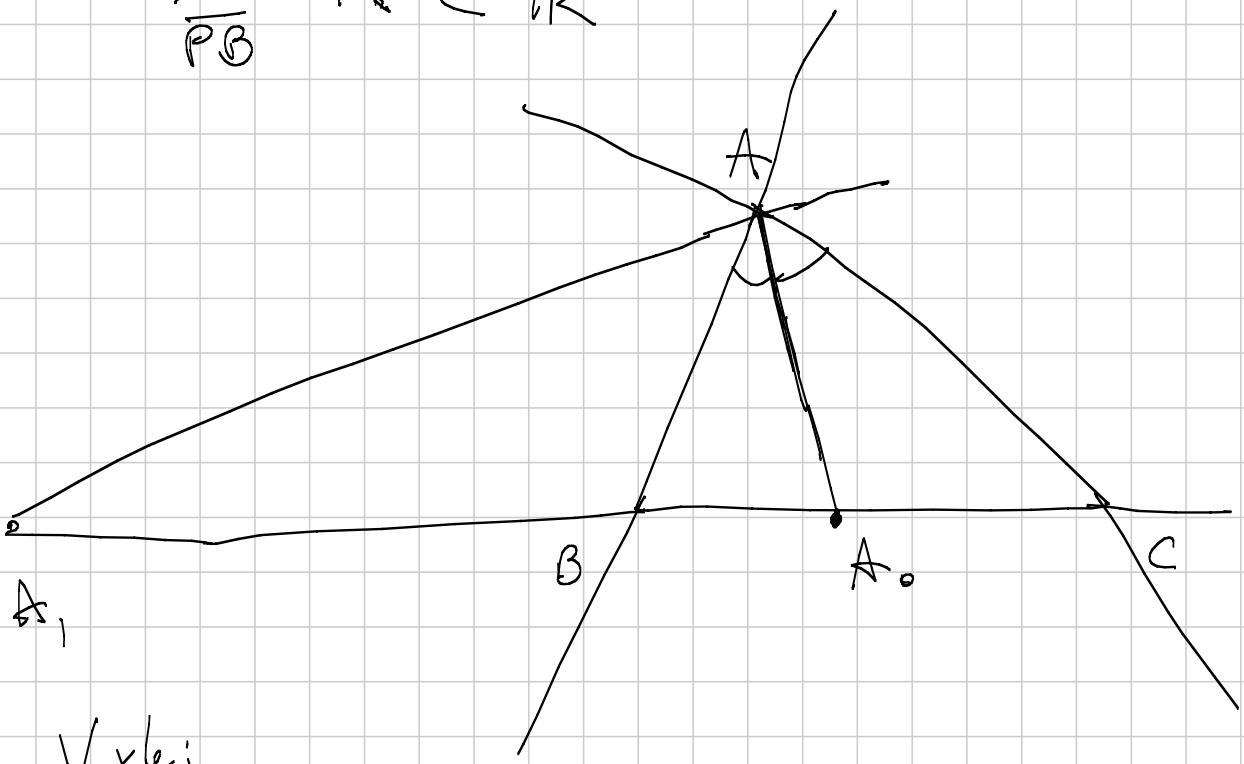
nei lati del triangolo $\Rightarrow$ assurdo

$\Rightarrow$ $A_1A_2B_1B_2C_1C_2$ ciclico

Circonferenze di Apollonio

Def Luogo dei punti P t.c.

$$\frac{\overline{PA}}{\overline{PB}} = k \in \mathbb{R}^+$$



Vale:

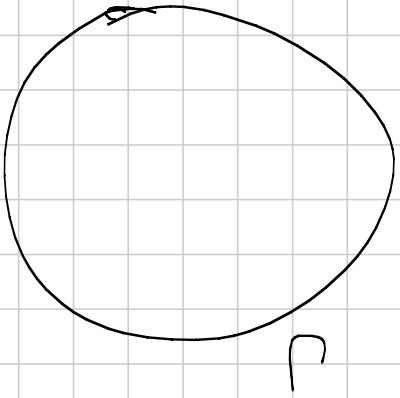
$$\frac{A_0B}{A_0C} = \frac{AB}{AC} \qquad \frac{A_1B}{A_1C} = \frac{AB}{AC}$$

(esercizio per casa, dimostrarlo)

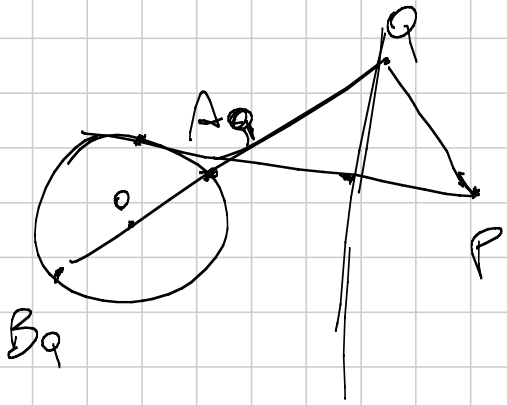
$\Rightarrow$ A_0, A, A_1 stanno su una

circonferenza di Apollonio. Circonferenza di Apollonio del triangolo (ce ne sono una per vertice).

Teorema degli assi radicali

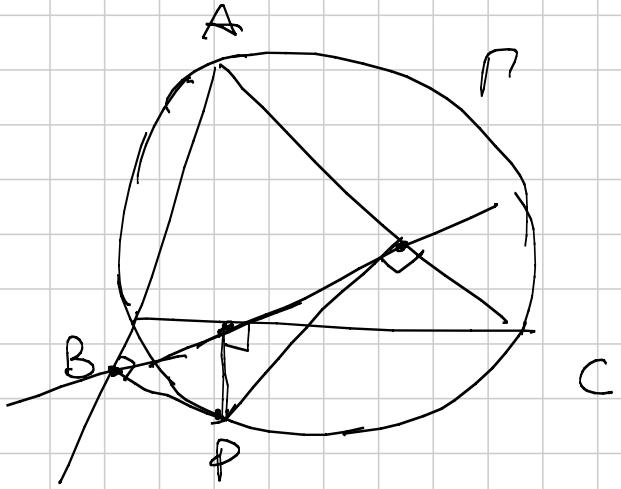


∃ l'asse radicale di Γ e P (perché P la potete vedere come una circ. di r=0)



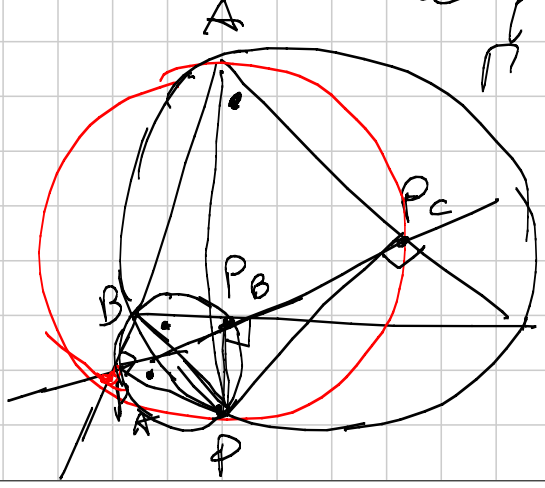
$\mathrm{Pow}_P(Q) = QP^2$

Retta di Simson



P sta su $\Gamma \iff$ le proiezioni di P sui lati sono allineate

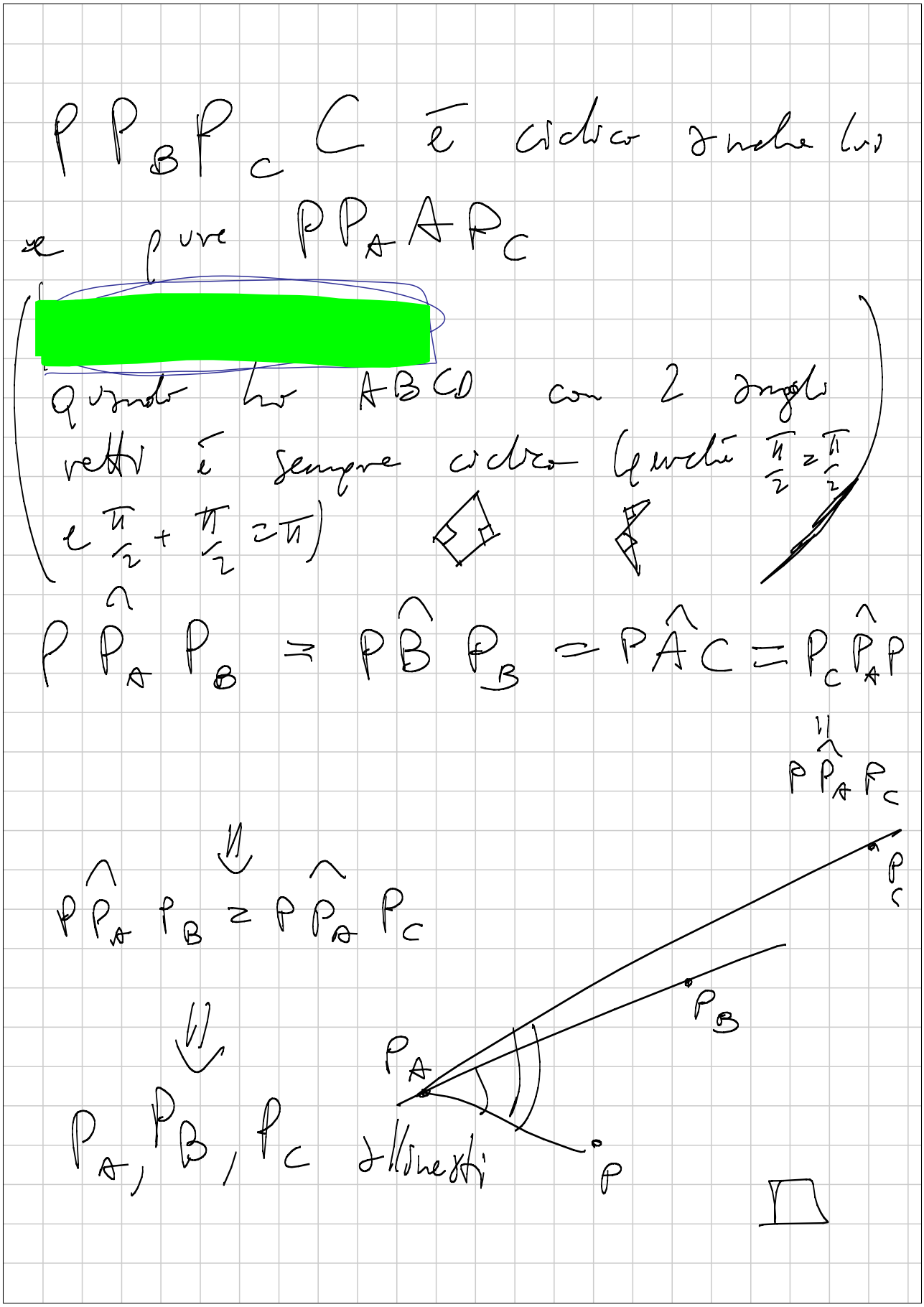
Dim Chiamiamo le proiezioni P_A, P_B, P_C

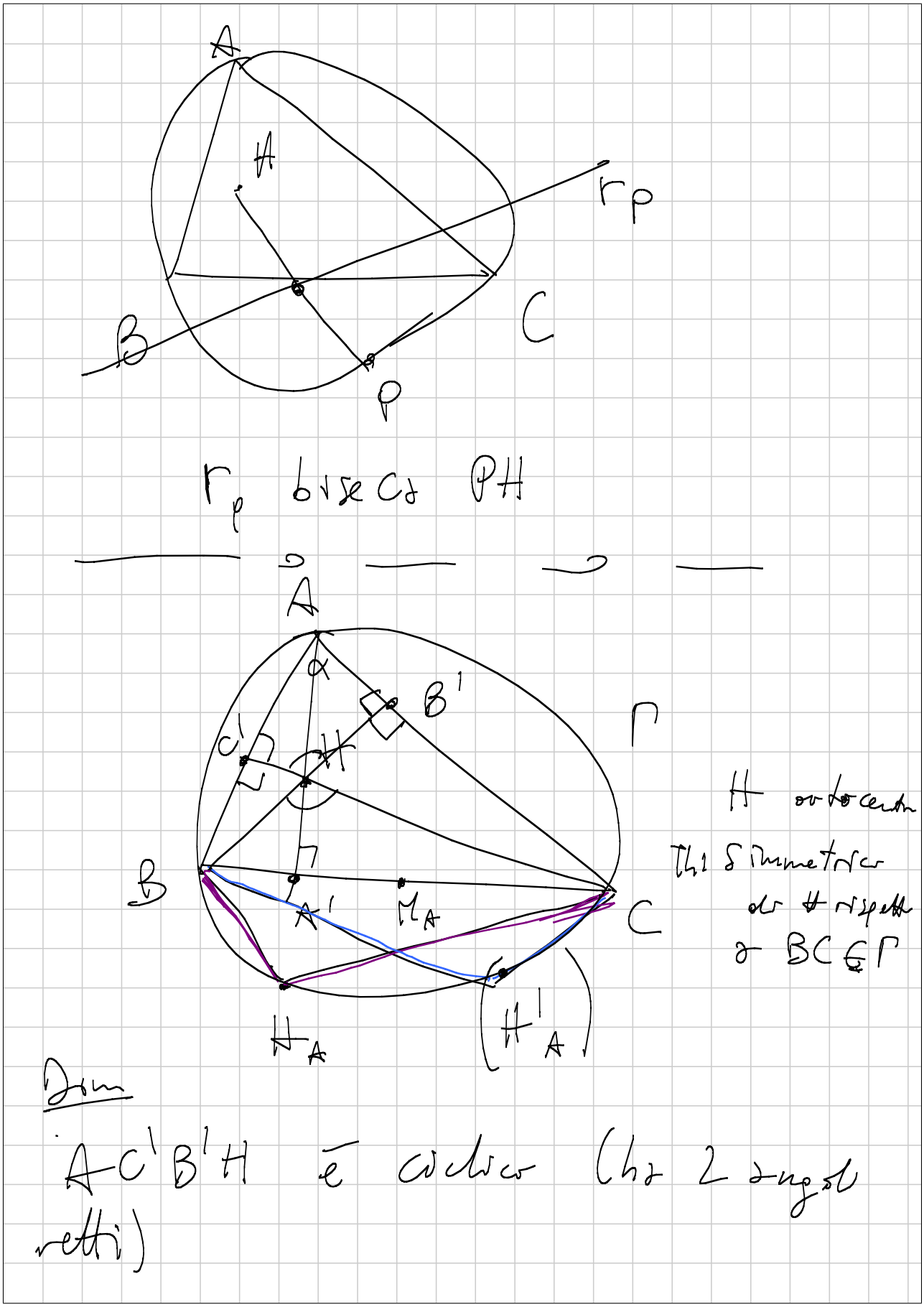


PP_AP_BB è ciclico

$(PP_AB = \pi - PP_BB)$

$\frac{\pi}{2}$ $\quad \pi - \frac{\pi}{2}$

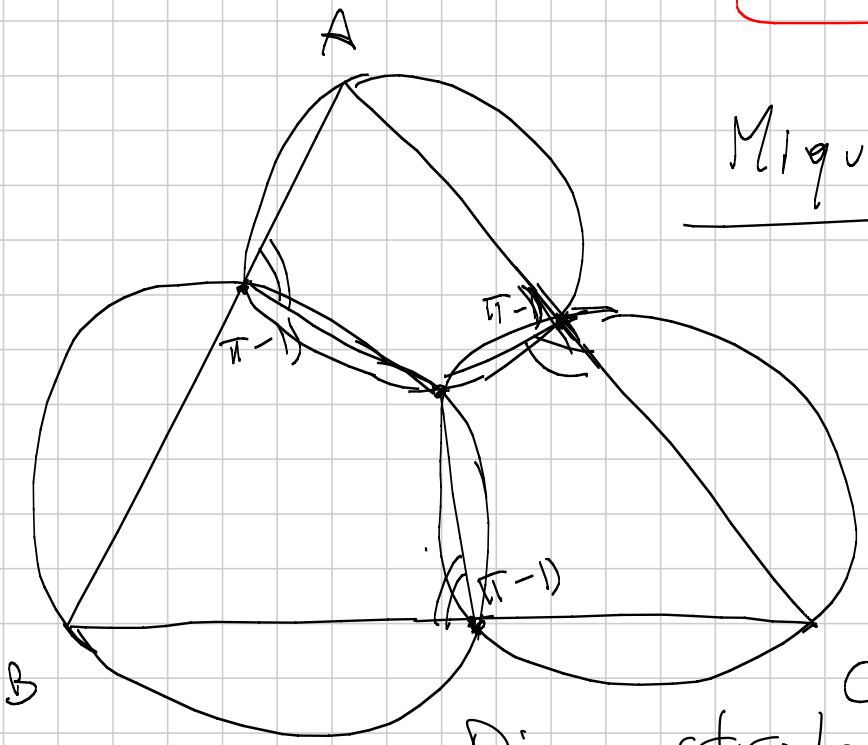

PP_BP_C C è ciclico anche lui
se pure PP_AAP_C
(quando ho $ABCD$ con 2 angoli
retti è sempre ciclico (perché $\frac{\pi}{2}=\frac{\pi}{2}$
e $\frac{\pi}{2}+\frac{\pi}{2}=\pi$)
$P\hat{P}_AP_B = P\hat{B}P_B = P\hat{A}C = P_C\hat{P}_AP$
$P\hat{P}_AP_C$
$P\hat{P}_AP_B = P\hat{P}_BP_C$
P_A, P_B, P_C allineati
P_A
P_B
P_C
P


A
H
r_P
B
C
P
r_P bisec di PH
A
B'
C'
H
Γ
B
A'
M_A
C
H_A
H'_A
H ortocentro
Th: Simmetrico di H rispetto a BC ∈ Γ
Dim
$AC'B'H$ è ciclico (ha 2 angoli retti)

$B\hat{H}C = B'\hat{H}C' = \pi - \alpha$

$B\hat{H}_A C = B\hat{H}C = \pi - \alpha = \pi - B\hat{A}C$

$\Rightarrow BACH_A$ ciclico $\Rightarrow H_A$ ortocentro



Miquel

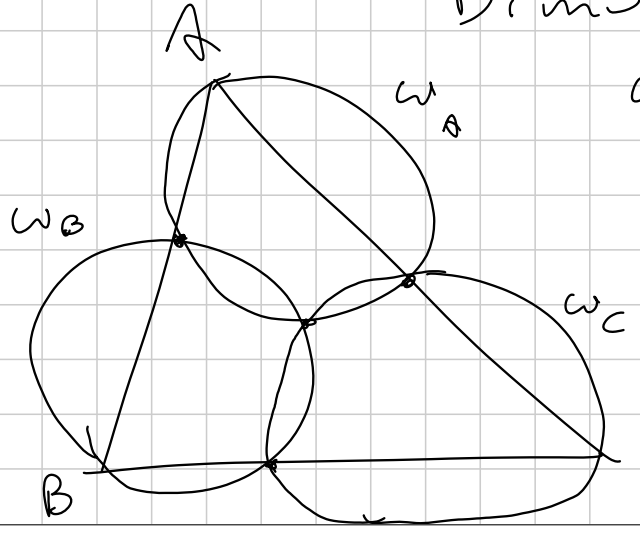
Dimostrate il caso

$\omega_A \cap \omega_B \in AB$

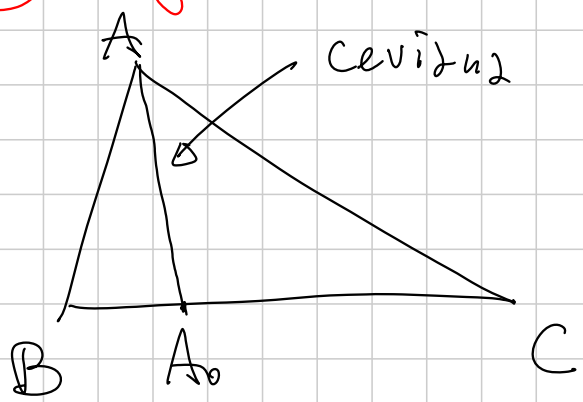
e ciclo

$\Downarrow$

$\omega_A, \omega_B, \omega_C$ concorrono

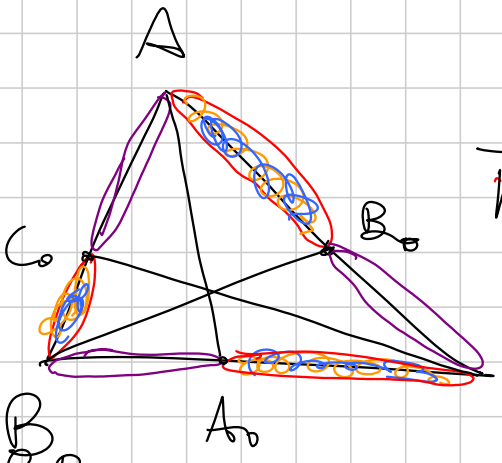


Ceva



AA_0 cevviana (qualsiasi retta passante x un vertice)

Teo



$$\frac{\text{viola}}{\text{mix}} = 1$$

Ae: AA_0, BB_0, CC_0 cevviane

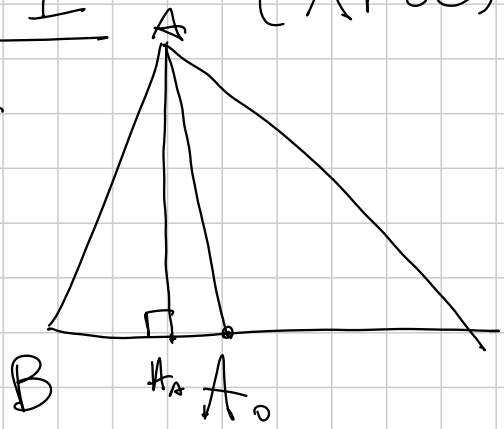
Th: AA_0, BB_0, CC_0 concorrono

$$\Updownarrow$$

$$\frac{BA_0}{A_0C} \cdot \frac{CB_0}{B_0A} \cdot \frac{AC_0}{C_0B} = 1$$

Dim 1 (Aree)

Lemma



$[ABC]$

$$\frac{[ABA_0]}{[AA_0C]} = \frac{BA_0}{A_0C}$$

Dim

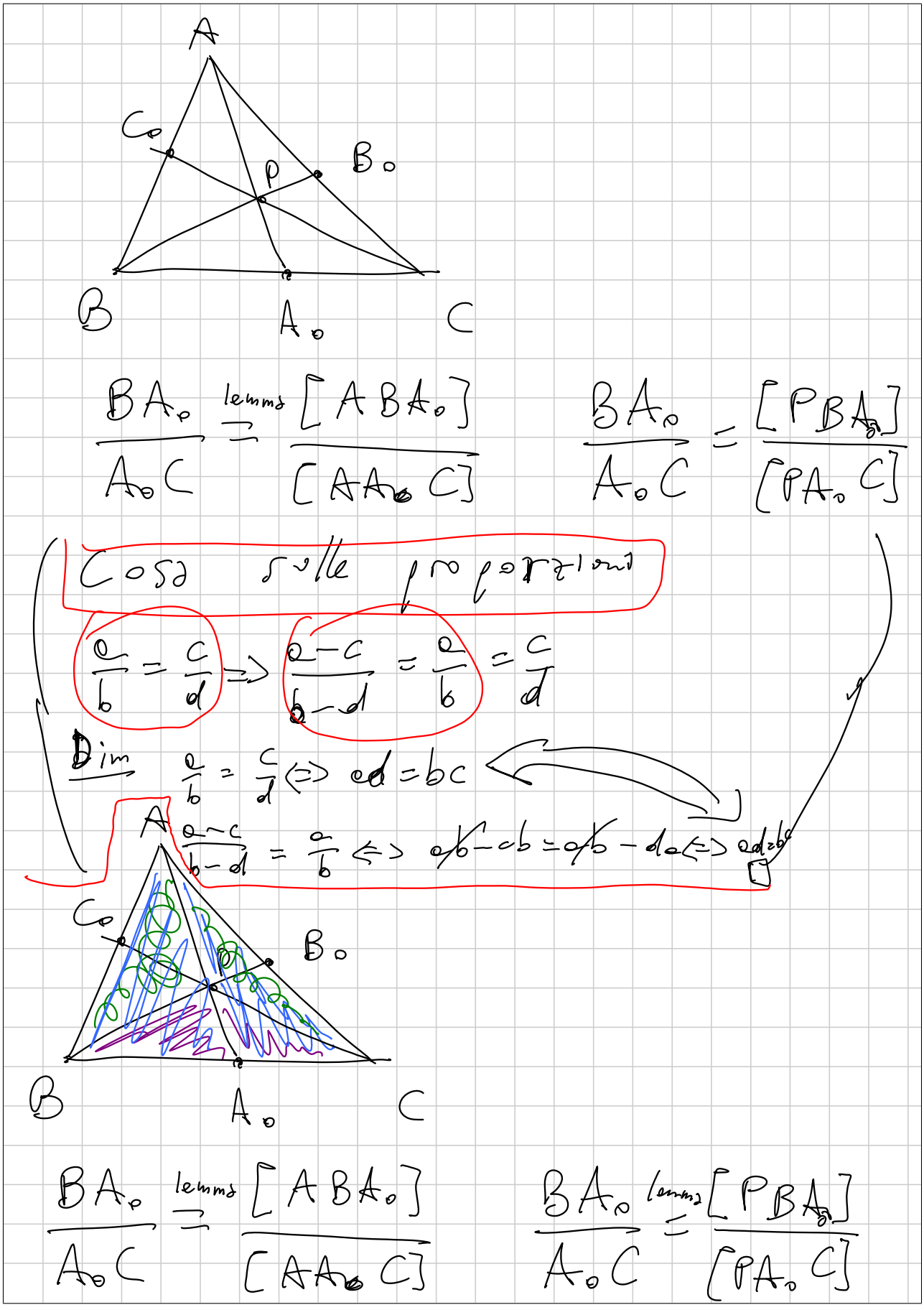
Sia AH_A l'altezza di A

$$\Rightarrow [ABA_0] = \frac{1}{2} A_0B \cdot AH_A$$

$$[AA_0C] = \frac{1}{2} A_0C \cdot AH_A$$

$$\Rightarrow \frac{[ABA_0]}{[AA_0C]} = \frac{\frac{1}{2} A_0B \cdot AH_A}{\frac{1}{2} A_0C \cdot AH_A} = \frac{A_0B}{A_0C}$$

□


A
C₀
B₀
P
B
A₀
C
BA₀ / A₀C =lemma [ABA₀] / [AA₀C]
BA₀ / A₀C = [PBA₀] / [PA₀C]
Cosa sulle proporzioni
a/b = c/d ⇒ (a−c)/(b−d) = a/b = c/d
Dim a/b = c/d ⇔ ad = bc
(a−c)/(b−d) = a/b ⇔ ab − cb = ab − da ⇔ ad = bc
A
C₀
B₀
B
A₀
C
BA₀ / A₀C =lemma [ABA₀] / [AA₀C]
BA₀ / A₀C =lemma [PBA₀] / [PA₀C]

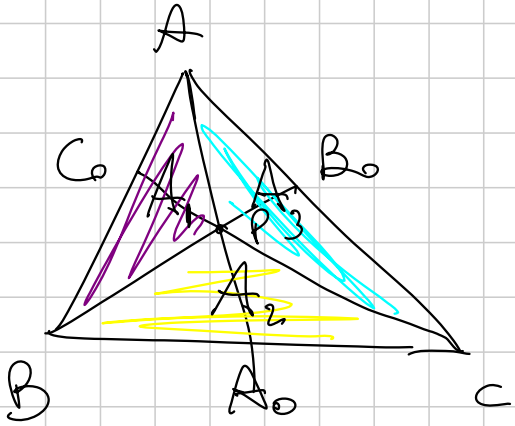
$$\frac{BA_0}{A_0C} = \frac{[ABA_0]}{[AA_0C]} = \frac{[PBA_0]}{[PA_0C]}$$

(V)

$$\frac{BA_0}{A_0C} = \frac{[ABA_0]-[PBA_0]}{[AA_0C]-[PA_0C]} = \frac{[PAB]}{[PAC]}$$

Analogamente:

$$\frac{CB_0}{B_0A} = \frac{[PBC]}{[PBA]} \quad e \quad \frac{AC_0}{C_0B} = \frac{[PCA]}{[PCB]}$$



$[PAB] = A_1$

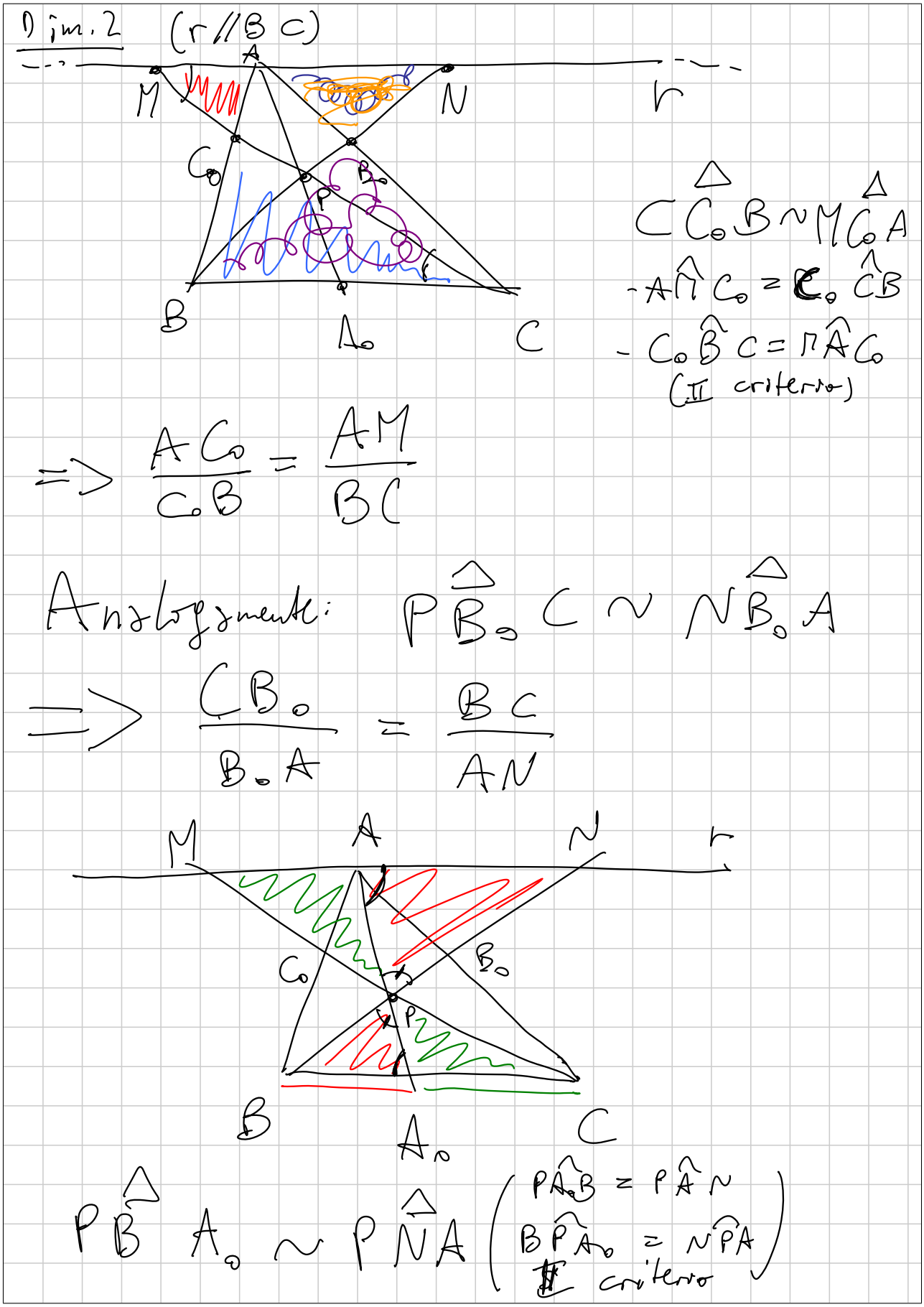
$[PAC] = A_3$

$[PBC] = A_2$

$$\frac{BA_0}{A_0C} \cdot \frac{CB_0}{B_0A} \cdot \frac{AC_0}{C_0B} = \frac{A_1}{A_3} \cdot \frac{A_2}{A_1} \cdot \frac{A_3}{A_2}$$

$= 1.$

□


Dim. 2 (r // BC)
A
M
N
r
C₀
B₀
P
B
A₀
C
△CC₀B ~ △MC₀A
- AMC₀ = BC₀C
- C₀BC = MAC₀
(II criterio)
⇒ AC₀/C₀B = AM/BC
Analogamente: △PB₀C ~ △NB₀A
⇒ CB₀/B₀A = BC/AN
M
A
N
r
C₀
B₀
P
B
A₀
C
△PBA₀ ~ △PNA
(PA₀B = PÂN
BPA₀ = NPA
# criterio)

$\Rightarrow \frac{BA_0}{AN} = \frac{PA_0}{PA}$ (x similitudine)

Analogamente: $\frac{A_0C}{AM} = \frac{PA_0}{PA}$

$\Rightarrow \boxed{\frac{BA_0}{AN} = \frac{A_0C}{AM}} \Rightarrow \frac{BA_0}{A_0C} = \frac{AN}{AM}$

$\frac{BA_0}{A_0C} \cdot \frac{CB_0}{B_0A} \cdot \frac{AC_0}{C_0B} = \frac{AN}{AM} \cdot \frac{BC}{AN} \cdot \frac{AM}{BC}$

$= 1$

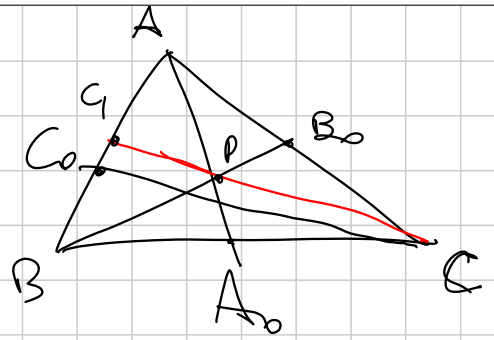
$\square$

AA_0, BB_0, CC_0 concorrono

$\Updownarrow$

$\frac{BA_0}{A_0C} \cdot \frac{CB_0}{B_0A} \cdot \frac{AC_0}{C_0B} = 1$

Freccia blu:



Supponiamo per assurdo $\frac{AB_0}{B_0C} \cdot \frac{CA_0}{A_0B} \cdot \frac{BC_0}{C_0A} = 1$

ma AA_0, BB_0, CC_0 non concorrono

Sia $P = AA_0 \cap BB_0$

e $C_1 = CP \cap AB$

$$\Rightarrow \frac{AB_0}{B_0C} \cdot \frac{CA_0}{A_0B} \cdot \frac{BC_1}{C_1A} = 1$$

$$\Rightarrow \frac{BC_1}{C_1A} = \frac{BC_0}{C_0A} \Rightarrow \frac{BC_1}{C_1A} + 1 = \frac{BC_0}{C_0A} + 1$$

$$\Rightarrow \frac{BC_1 + C_1A}{C_1A} = \frac{BC_0 + C_0A}{C_0A} \Rightarrow \frac{BA}{C_1A} = \frac{BA}{C_0A}$$

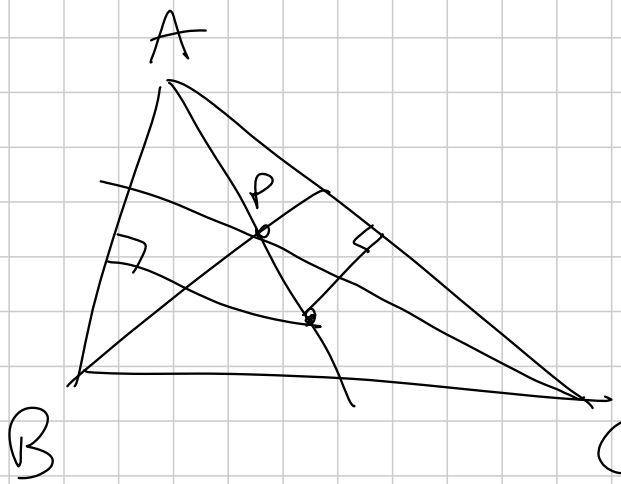
$\Rightarrow C_1A = C_0A \Rightarrow$ assurdo.

Cos'è un segmento orientato?

$\overline{AB} > 0$ se B viene dopo A

e $\overline{AB} < 0$ se A viene dopo B

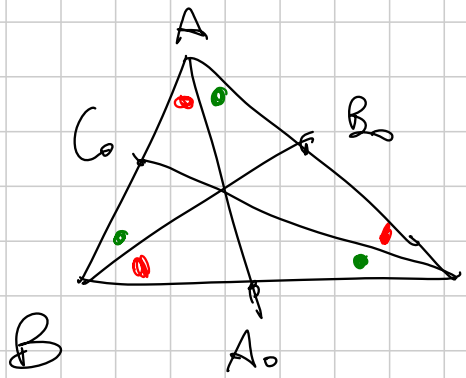
$\overline{AB} = -\overline{BA}$



Esercizio per casa: ricordiamo Stewart

Ceva

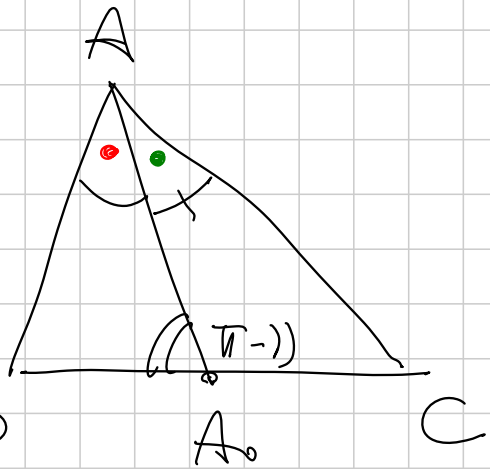
Ceva trigonometrica



$\frac{\prod \sin \text{rossi}}{\prod \sin \text{verdi}} = 1$

$\frac{\sin B\hat{A}A_0}{\sin A_0\hat{A}C} \cdot \frac{\sin A\hat{C}C_0}{\sin C_0\hat{C}B} \cdot \frac{\sin C\hat{B}B_0}{\sin B_0\hat{B}A} = 1$

Lemma



$$\frac{BA_0}{A_0C} = \frac{AB}{AC} \cdot \frac{\sin\beta}{\sin\gamma}$$

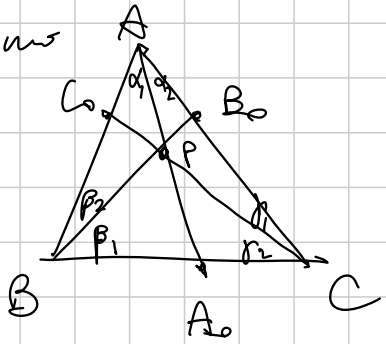
Dim

$$\frac{BA_0}{BA} = \frac{\sin\beta}{\sin\gamma}$$

$$\frac{A_0C}{CA} = \frac{\sin\gamma}{\sin(\pi-\beta)} = \frac{\sin\gamma}{\sin\beta}$$

$$\Rightarrow \frac{\frac{BA_0}{BA}}{\frac{A_0C}{CA}} = \frac{\frac{\sin\beta}{\sin\gamma}}{\frac{\sin\gamma}{\sin\beta}} \Rightarrow \frac{BA_0}{A_0C} = \frac{BA}{CA} \cdot \frac{\sin\beta}{\sin\gamma}$$

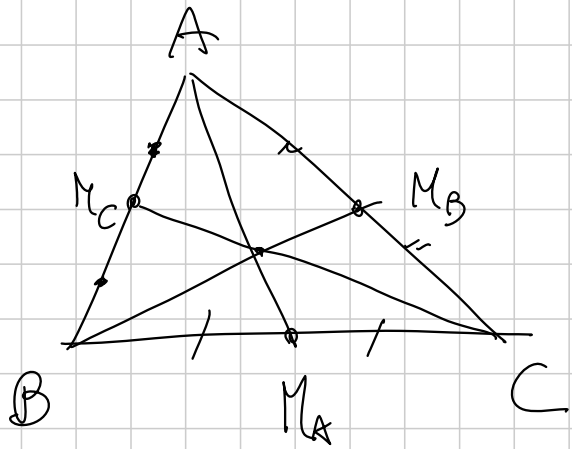
Teorema di Ceva trig.



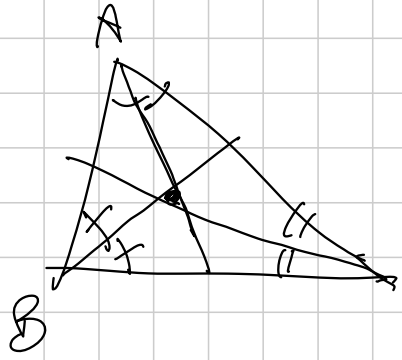
AA_0, BB_0, CC_0 concorrono $\iff \frac{BA_0}{A_0C} \cdot \frac{CB_0}{B_0A} \cdot \frac{AC_0}{C_0B} = 1$

$\iff \left(\frac{AB}{AC} \cdot \frac{\sin\alpha_1}{\sin\alpha_2}\right)\left(\frac{AC}{BC} \cdot \frac{\sin\beta_1}{\sin\beta_2}\right)\left(\frac{BC}{AB} \cdot \frac{\sin\gamma_1}{\sin\gamma_2}\right) = 1$

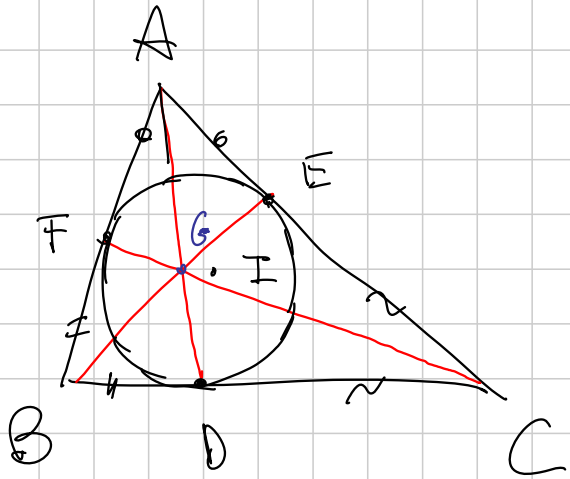
$\iff$ Vin $\square$



$\frac{BM_A}{M_AC} \cdot \frac{CM_B}{M_BA} \cdot \frac{AM_C}{M_CB} = 1$



$\frac{\sin\alpha_1}{\sin\alpha_2} \cdot \frac{\sin\beta_1}{\sin\beta_2} \cdot \frac{\sin\gamma_1}{\sin\gamma_2} = 1$

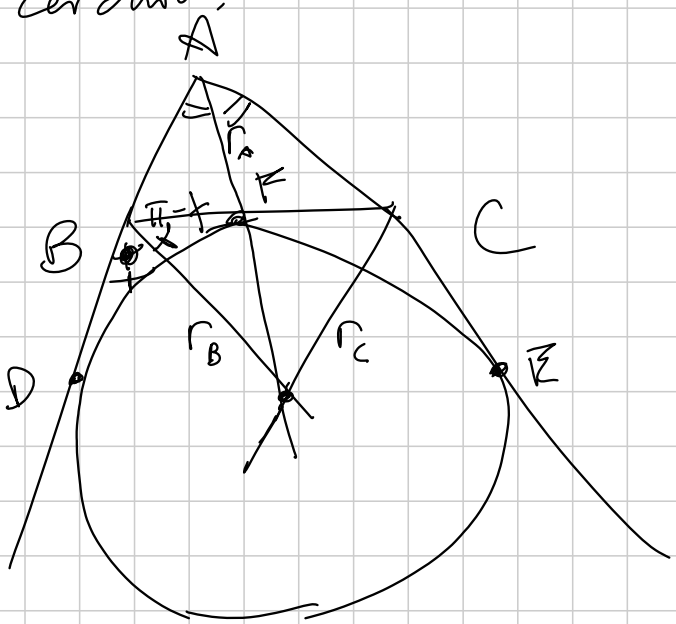


Th: AD, BE, CF } concorrono

$$\frac{BD}{DC}\cdot\frac{CE}{EA}\cdot\frac{AF}{FB}=1$$

G = Gergonne (deve concorrere)

Ex-cerchio:

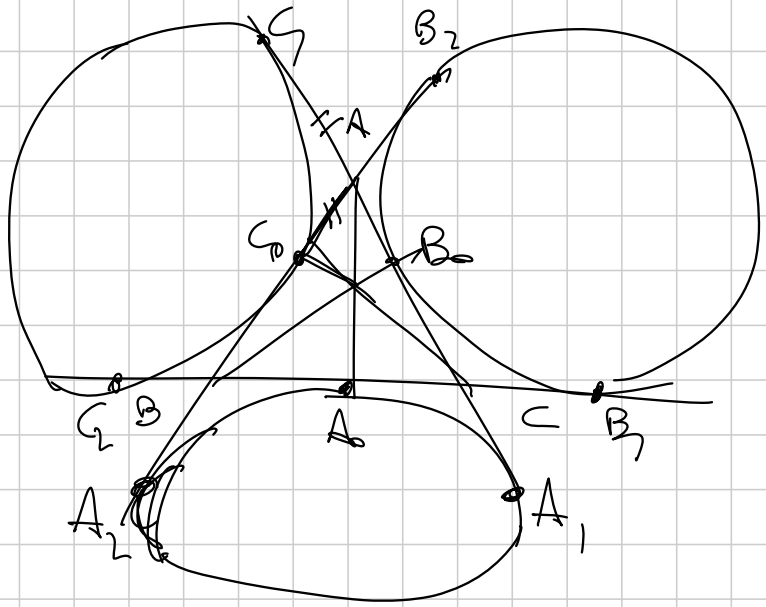


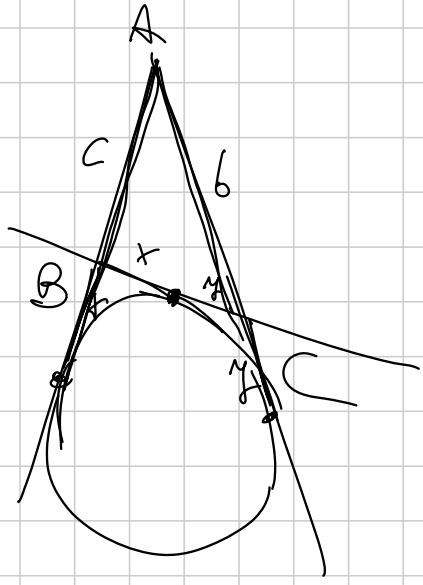
$r_A \cap r_B = I_A$ $\quad d(I_A, AB) = d(I_A, BC)$

$d(I_A, AB) \overset{r_A}{=} d(I_A, AC)$

$\Downarrow$

$d(I_A, AC) = d(I_A, BC) \Rightarrow$ sfera r_c □





$c + x = b + y$ (tangenti da A)

$(c + x) + (b + y) = 2p$

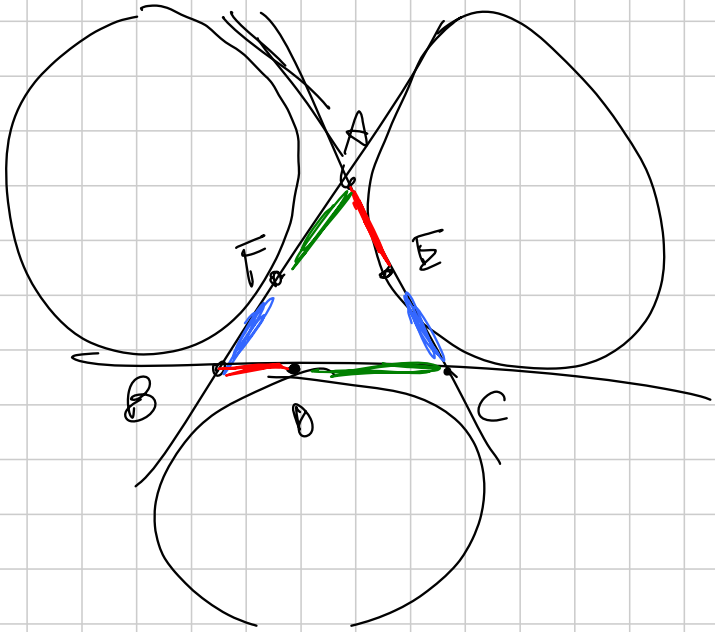
$\Downarrow$

$2(c + x) = 2p$

$x = p - c$

$x = p - c \quad y = p - b$

Torniamo a prima



$AE = p - c$

$BD = p - c$

$AF = p - b$

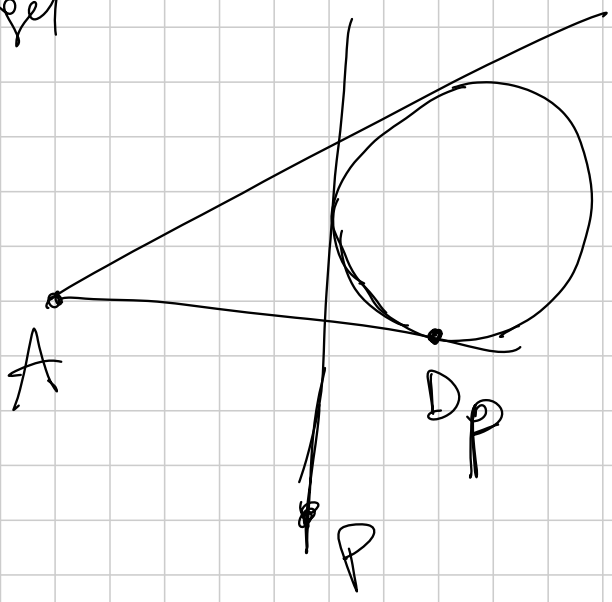
$\overline{DC}$

$EC = p - a$

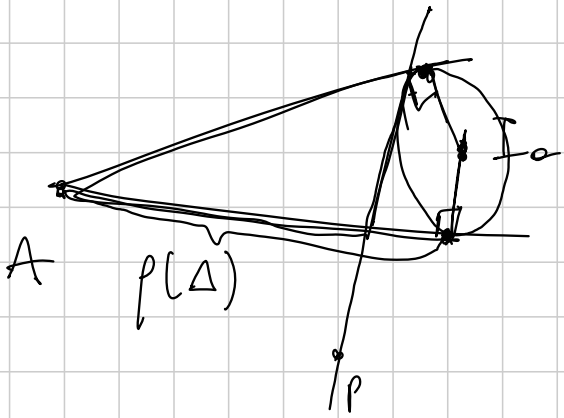
$\overline{BF}$

$\Rightarrow \frac{BD}{DC} \cdot \frac{EC}{AE} \cdot \frac{AF}{FB} = 1$

Il punto in cui concorrono si chiama Nagel



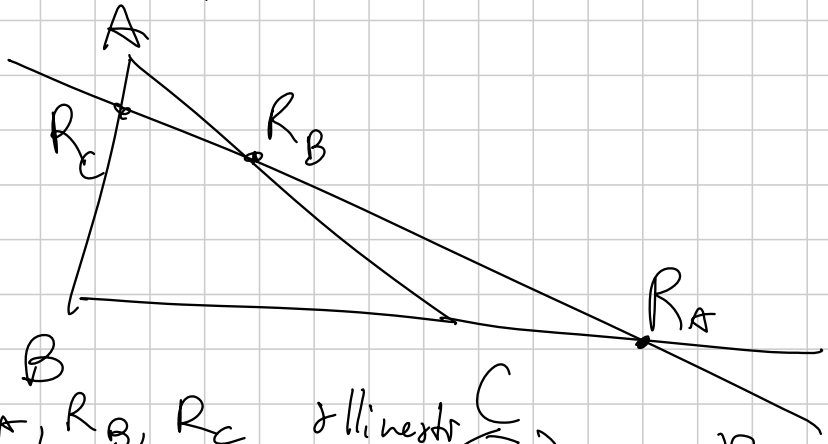
$AD_p = p(\Delta)$



p(Δ) è l'ho gris

□

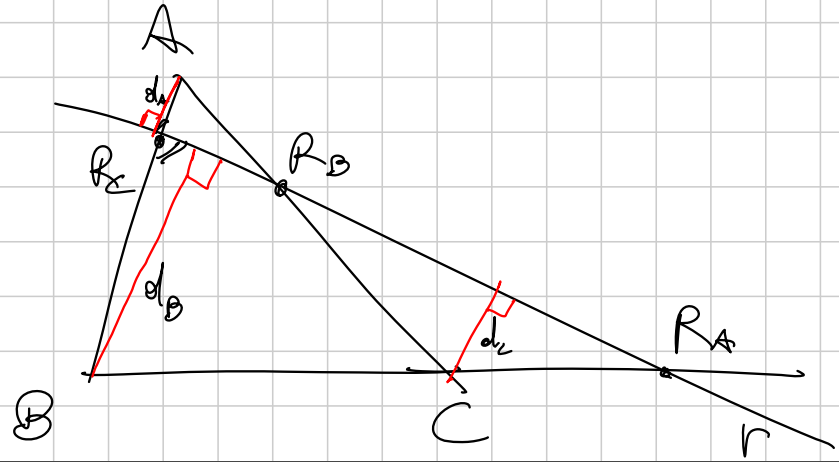
Menelao



R_A, R_B, R_C allineati $\Leftrightarrow$

$$\frac{AR_B}{R_BC} \cdot \frac{BR_C}{R_CA} \cdot \frac{CR_A}{R_AB} = -1$$

Dim

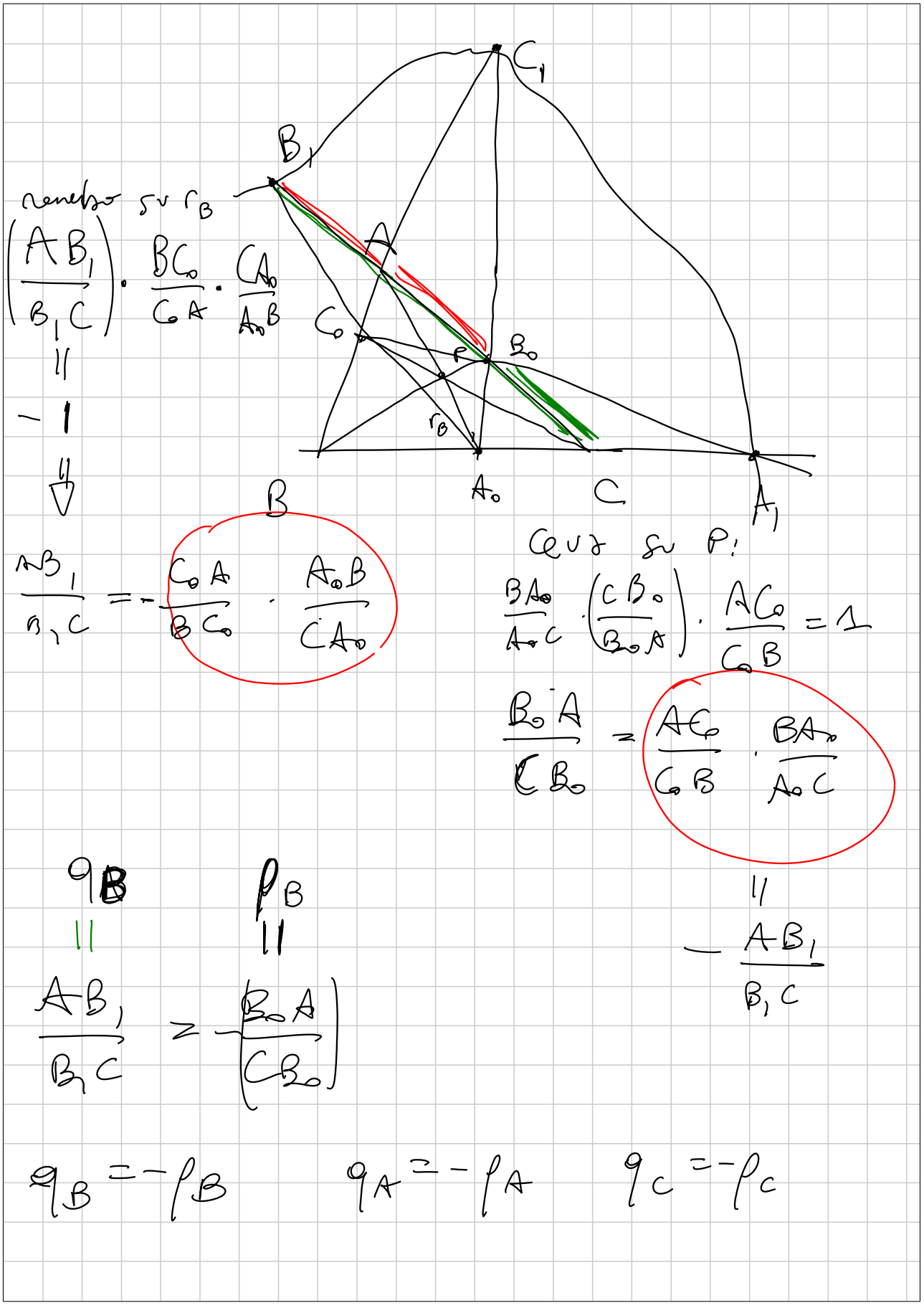


$$\frac{A R_C}{R_C B} = \frac{d_A}{d_B} \qquad \frac{C R_B}{R_B A} = \frac{d_C}{d_A}$$

$$\frac{B R_A}{R_A C} = \frac{d_B}{d_C}$$

$$\frac{A R_C}{R_C B} \cdot \frac{C R_B}{R_B A} \cdot \frac{B R_A}{R_A C} = \frac{d_A}{d_B} \cdot \frac{d_C}{d_A} \cdot \frac{d_B}{d_C} = 1$$

L'altra freccia la dimostro come ho fatto con Ceva



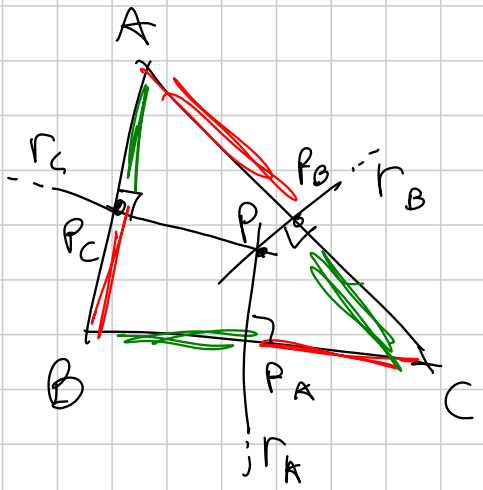
Geometria 3 (Basic) – Julian Demeio

$\Rightarrow q_A q_B q_C = (-1)^3 \underbrace{\ell_A \ell_B \ell_C}_{\text{!}} = -1$

$\Rightarrow$ Win

□

Carnot



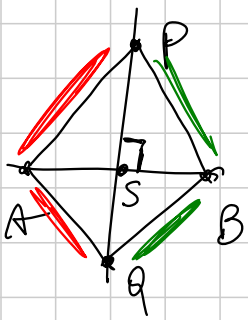
r_A, r_B, r_C Concorrono

$\Leftrightarrow$

$PB^2 - PC^2 + CP_B^2 - P_B A^2 + AP_C^2 - P_C B^2 = 0$

$\sum \text{rossi}^2 = \sum \text{verdi}^2$

Lemma



$AP^2 - PB^2$ $\quad$ $AP^2 + QB^2$

$\Updownarrow$ $\quad$ $\Updownarrow$

$AQ^2 - QB^2$ $\quad$ $PB^2 + QA^2$

$\Updownarrow$

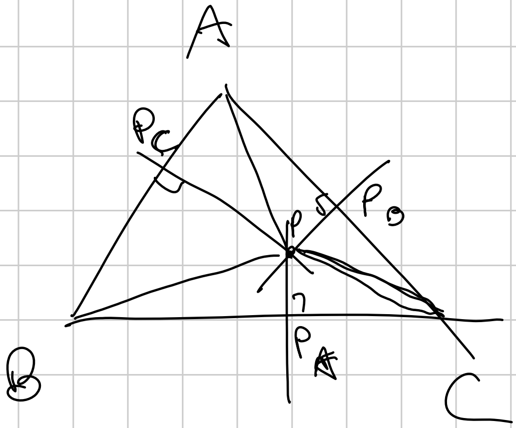
$PQ \perp AB$

$$AP^2 = AS^2 + PS^2 \qquad PB^2 = BS^2 + PS^2$$

$$AQ^2 = AS^2 + QS^2 \qquad QB^2 = BS^2 + QS^2$$

$$AP^2 - PB^2 = AS^2 + \cancel{PS^2} - BS^2 \cancel{- PS^2}$$

$$= AS^2 + QS^2 - BS^2 - QS^2 = AQ^2 - QB^2$$



$$+\begin{cases} BP_A^2 - P_AC^2 = \cancel{BP^2} - \cancel{PC^2} \\ CP_B^2 - P_BA^2 = \cancel{PC^2} - \cancel{PA^2} \\ AP_C^2 - P_CB^2 = \cancel{AP^2} - \cancel{PB^2} \end{cases}$$

$$\begin{array}{ccc} \| & & \| \\ \text{LHS} & & 0 = \text{RHS} \end{array}$$

<u>Win</u>

Trasformazioni geometriche (del piano)

ISOMETRIE (conservano tutto)

↳ SIMILITUDINI (conservano tutto - le lunghezze)
(OMOTETIE)

↳ AFFINITÁ

(PROIETTIVITÁ che conservano allineamenti
concorrenze e rapporti (ABCD)
$= \frac{CA}{CB} : \frac{DA}{DB}$)

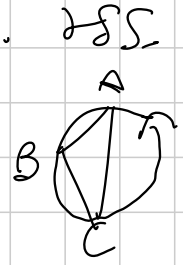
ISOMETRIE

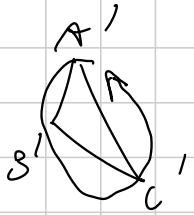
Def Un'isometria è una trasformazione che conserva le distanze

Isometria = Rotazione + simm. assiale / trasl.

= 3 simm. ass.

Segno dell'isometria:

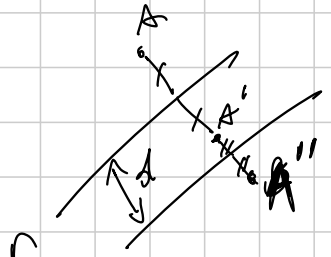




Se ABC e $A'B'C'$ girano nello stesso verso il segno è positivo, altrimenti è negativo.

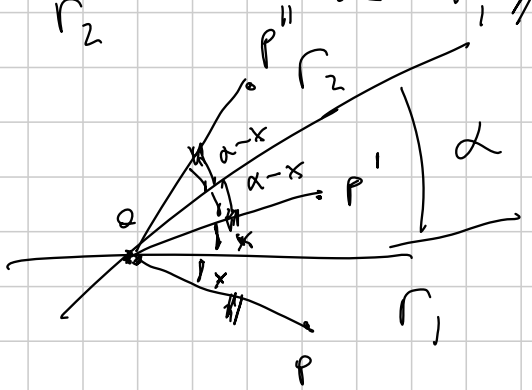
Fatti interessanti:

Simmetria assiale + simm. assiale = rotazione/traslazione



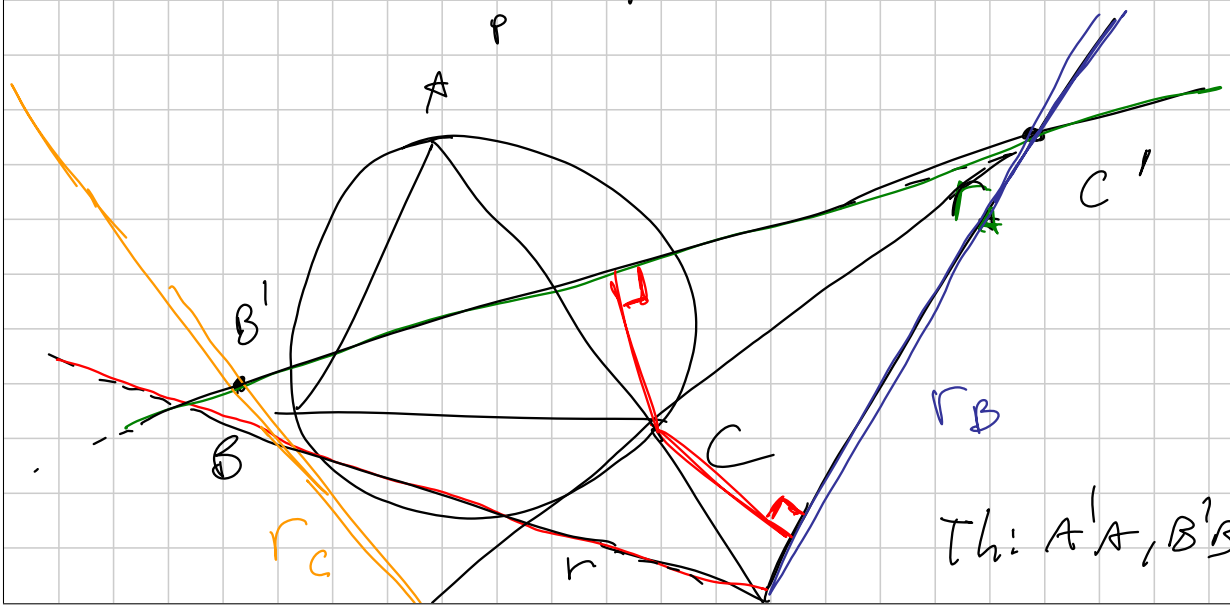
$|AA''| = 2d$

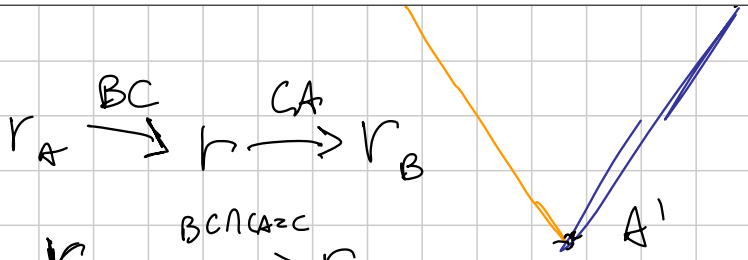
se $r_1 \parallel r_2$ simm + simm. = trasl



$\hat{PQP''}$

$2x + 2\alpha - 2x = 2\alpha$





$C'C$ concorrono

$r_A \xrightarrow{BC} r \xrightarrow{CA} r_B$

$r_A \xrightarrow{BC \cap CA = C} r_B$

$\Downarrow$

$d(C, r_A) = d(C, r_B) \Rightarrow C'C$ è bisettrice

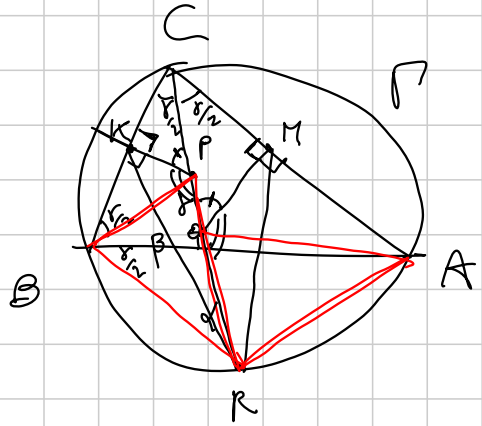
$\Rightarrow A'A, B'B, C'C$ concorrono nell'incentro di $A'B'C'$. $\square$

Similitudini

Def Una sim. mantiene i rapporti tra lunghezze $\Rightarrow$ Mantiene tutte tranne le lunghezze

—— $\circ$ —— $\circ$ ——

IMO 4 – 2007



$R\hat{B}A = \gamma$

$P\hat{B}R = \beta$

$[RQM] = \frac{1}{2} QR \cdot QM \cdot \sin \hat{Q}$

$[RPK] = \frac{1}{2} RP \cdot PK \cdot \sin \hat{P}$

$\sin \hat{Q} = \sin \hat{P}$

Th $\Leftrightarrow$ $QR \cdot QM = RP \cdot PK$

$PK = PC \sin \frac{\gamma}{2}$

$QM = QC \sin \frac{\gamma}{2}$

$QR \cdot QC \cdot \sin \frac{\gamma}{2} = RP \cdot PC \cdot \sin \frac{\gamma}{2}$

$QR = x$ $\quad$ $CP = y$

$x \quad (CR - x) \qquad y (CR - y)$

$x = y$

$P\hat{B}R \sim C\hat{B}A$ simili

$Q\hat{R}A \sim C\hat{B}A$

$P\hat{B}R \sim Q\hat{R}A \Rightarrow \frac{PR}{PB} = \frac{AQ}{QR}$ $(= QC)$

(PC)

$\Rightarrow \frac{PR}{PC} = \frac{QC}{QR}$ $\quad PC = y$ $\quad QR = x$

$$\frac{CR - M_2}{\vec{y}} = \frac{CR - X}{\vec{x}}$$

$\vec{n}$

$$\frac{CR}{y} = 1 = \frac{CR}{x} = 1 \quad \Rightarrow \quad y = x$$

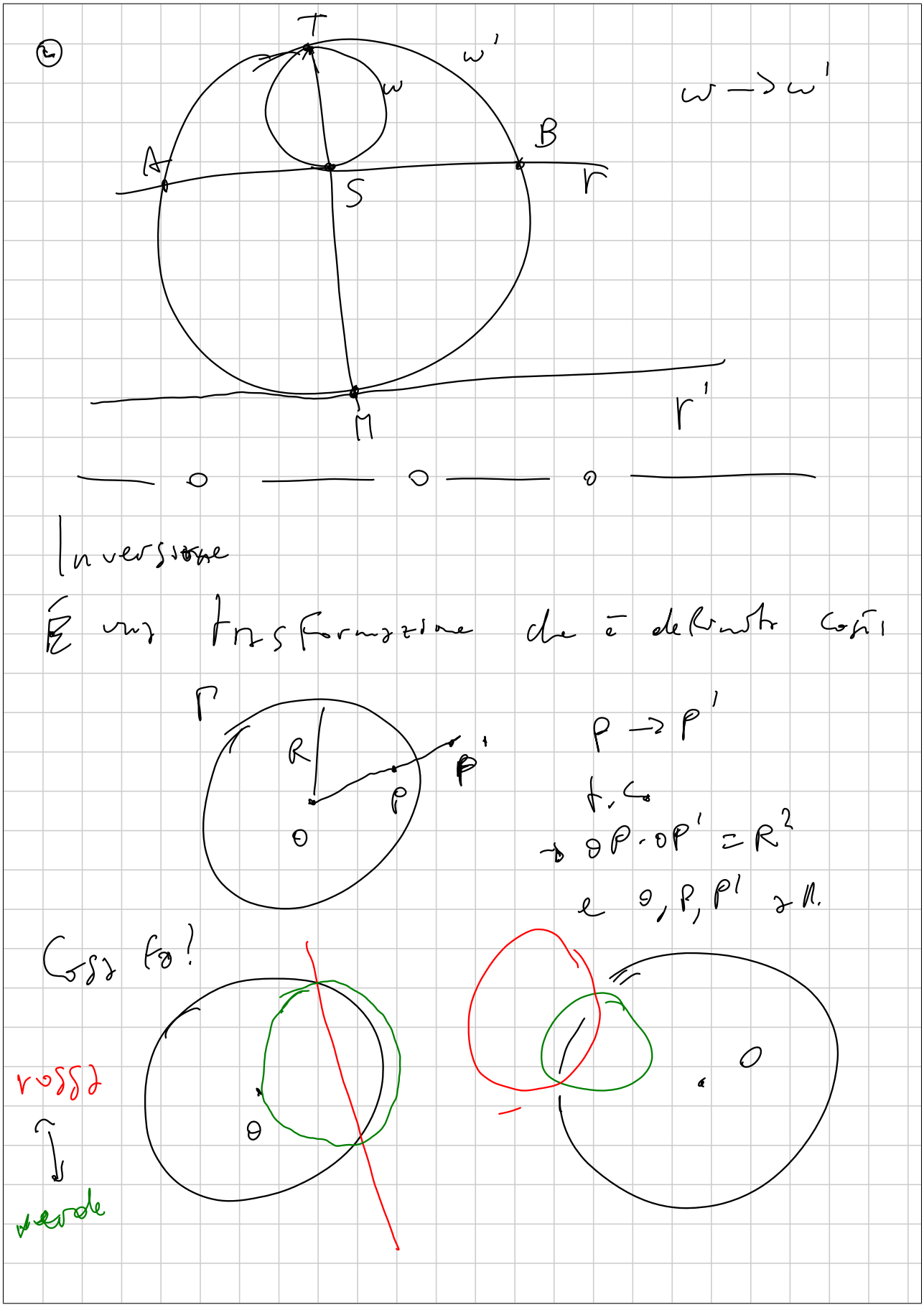
Omotetia

Dato un punto O si chiama omotetia di fattore k e centro O quella trasformazione che manda P in P' t.c.

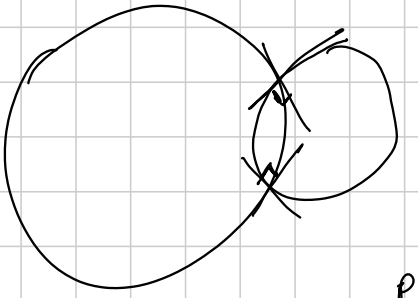
$$\overrightarrow{OP'} = k\,\overrightarrow{OP}$$

2 fatti utili:

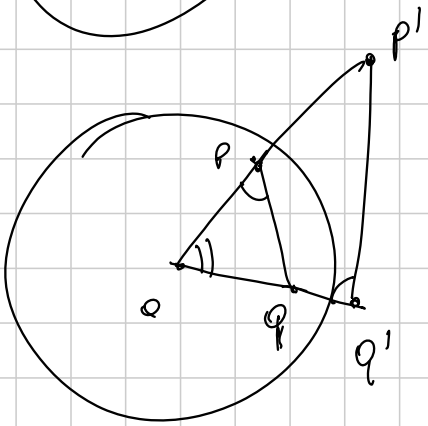
(1) omotetia $\circ$ omotetia = omotetia di fattore = prodotto dei fattori e centro allineato con gli altri 2 centri di omotetia


T
ω'
ω
ω → ω'
A
B
S
r
M
r'
Inversione
È una trasformazione che è definita così:
Γ
R
P'
P
O
P → P'
t.c.
→ OP · OP' = R²
e O, P, P' ≠ A.
Cosa fa?
rossa
verde
O

Mantiene fisse le circ. ortogonali a Γ



Teorema



Fatto 1

$PQP'Q'$ ciclico

$\overrightarrow{OP}\cdot\overrightarrow{OP'} = \overrightarrow{OQ}\cdot\overrightarrow{OQ'} = R^2$

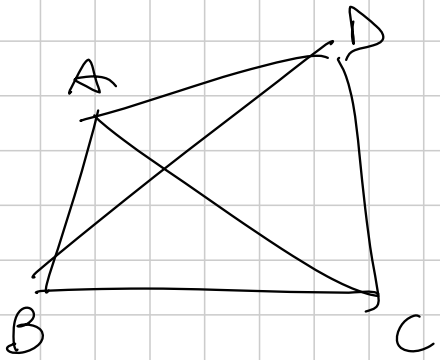
$\Rightarrow O\hat{P}Q = \pi - Q\hat{P}'P' = Q\hat{Q}'P'$

$\Rightarrow \triangle OPQ \sim \triangle OQ'P'$

$$\Rightarrow \frac{P'Q'}{PQ} = \frac{OQ'}{OP} = \frac{\frac{R^2}{OQ}}{OP} = \frac{R^2}{OP\cdot OQ}$$

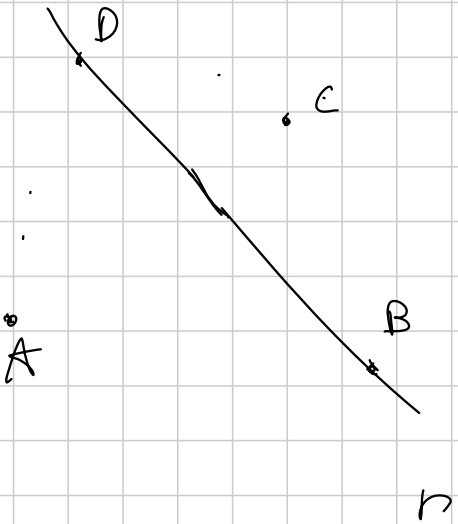
$$\Rightarrow P'Q' = \frac{PQ\cdot R^2}{OP\cdot OQ}$$

Teorema



$$BD \cdot AC \leq AB \cdot DC + AD \cdot BC$$

Dim



$DC \to D'C'$

$CB \to C'B'$

$DB \to D'B'$

$$D'C' + C'B' \geq D'B'$$

$$\frac{DC \cdot R^2}{AD \cdot AC} + \frac{CB \cdot R^2}{AC \cdot AB} \geq \frac{DB \cdot R^2}{AD \cdot AB}$$

$$DC \cdot AB + CB \cdot AD \geq DB \cdot AC \Rightarrow \text{Win}$$

SENIOR 2011 – Teoria dei Numeri 1 (Basic)

Titolo nota 05/09/2011

Esempio 1 $\quad \frac{1}{a} + \frac{4}{b} = 1$

$$\frac{b+4a}{ab} = 1 \qquad b+4a = ab \qquad b(1-a) = -4a$$

$$b = -\frac{4a}{1-a} = \frac{4a}{a-1}$$

(Ho usato che è di 1° grado rispetto alla variabile b)

$$= \frac{4a-4+4}{a-1} = \frac{4(a-1)+4}{a-1} = 4 + \frac{4}{a-1}$$

Quindi $a-1$ deve essere un divisore di 4, quindi $\pm 1, \pm 2, \pm 4$.

Esempio 2 Parallelepipedo $a \times b \times c$ (interi)

Parallelepipedo interno $(a-2)(b-2)(c-2)$

voglio che abbia volume metà del precedente

$$2(a-2)(b-2)(c-2) = abc$$

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

Idea: → parte di divisibilità, congruenze, fattorizzazioni
↳ disuguaglianze

Domanda: possono a, b, c essere TUTTI enormi?
Possono essere tutti ≥ 10? Sarebbe

$$\left(1-\frac{2}{a}\right)\left(1-\frac{2}{b}\right)\left(1-\frac{2}{c}\right) \geq \frac{64}{125} > \frac{1}{2}$$

quindi è impossibile. Pertanto almeno una delle 3 è ≤ 9.
Quindi WLOG $c = 3, 4, 5, 6, 7, 8, 9$
Non resta che fare 7 comodi casi, che sono equivalenti all'esempio 1.

Esempio 3 Risolvere $a^2 - b^2 = 998$

Impossibile perché $998 \equiv 2 \pmod 4$

Fatti generali: ① I $\square$ mod 4 possono essere solo 0, 1
② a^2+b^2 mod 4 non può essere 3
③ a^2-b^2 " " " " 2

Dim: ② e ③ seguono da ①.
* a pari $\Rightarrow a = 2k \Rightarrow a^2 = 4k^2 \equiv 0 \pmod 4$
* a dispari $\Rightarrow a = 2k+1 \Rightarrow a^2 = 4k^2+4k+1 = 4(k^2+k)+1 \equiv 1 \pmod 4$

Risolvere $a^2 - b^2 = 1.000$

$(a+b)(a-b) = 1.000$

Quindi $a+b$ e $a-b$ devono essere divisori di 1000.
Però $a+b$ e $a-b$ hanno la stessa parità, quindi devo scegliere coppie di divisori con la stessa parità, quindi in questo caso pari.

$1.000 = 2^3 \cdot 5^3$ $\qquad a+b = 2^k \cdot 5^h$ $\qquad k = 1, 2$

$h = 0, 1, 2, 3$

Quindi ho 8 possibilità positive e 8 negative per $a+b$, e idem per $a-b$.

Oss. Mi riduco al sistema $\quad a+b = S$

$a-b = D$

$2a = S+D \qquad a = \frac{S+D}{2}$

$2b = S-D \qquad b = \frac{S-D}{2}$

} Se S e D hanno la stessa parità, il sistema ha sempre soluzione.

Quindi in totale abbiamo 16 coppie (a,b) che risolvono.

Back to 998 $\qquad (a+b)(a-b) = 998$

avendo la stessa parità, il LHS è
* o dispari
* o multiplo di 4.

Esempio 4 ---- $b = \dfrac{a^2+3}{a+1}$

$$b = \frac{a^2+3+a-a}{a+1} = a + \frac{3-a}{a+1} = a + \frac{3+1-1-a}{a+1} = \boxed{a-1} + \frac{4}{a+1}$$

$$\begin{array}{r|l} a^2 + 3 & a+1 \\ \hline -a^2 - a & \boxed{a-1} \\ \hline -a+3 & \\ +a+1 & \\ \hline 4 & \end{array}$$

$$a^2+3 = (a+1)(a-1) + 4$$

$$\frac{a^2+3}{a+1} = a - 1 + \frac{4}{a+1}$$

— o —

$$b = \frac{a^2+3}{2a+1} = \frac{1}{2}\,\frac{2a^2+6}{2a+1} = \frac{1}{2}\,\frac{2a^2+a-a+6}{2a+1}$$

$$= \frac{1}{2}\left\{a + \frac{-a+6}{2a+1}\right\}$$

$$= \frac{a}{2} + \frac{1}{4}\,\frac{-2a+12-1+1}{2a+1}$$

$$= \frac{a}{2} + \frac{1}{4}\left\{-1 + \frac{13}{2a+1}\right\}$$

$$= \frac{a}{2} - \frac{1}{4} + \boxed{\frac{13}{2a+1}}\cdot\frac{1}{4} = \frac{1}{4}\left\{2a - 1 + \frac{13}{2a+1}\right\}$$

deve essere intero

Di siamo $2a+1$ deve dividere 13 e resta un numero finito di casi da provare.

— o — o —

Divisione Euclidea Dati 2 interi positivi a e b, esistono q ed r (unici) tali che

$$\boxed{a = q\cdot b + r \qquad 0 \le r < b}$$

Teorema di Bezout Siano a e b due interi (diciamo positivi). Allora esistono due interi m ed n tali che

$$\boxed{a\,m + b\,n = \text{massimo comun divisore di } a \text{ e } b}$$

Fatto generale Dati a e b interi. Quali sono tutti gli interi che si scrivono come

$$ax + by \qquad x \in \mathbb{Z},\ y \in \mathbb{Z}$$

Sono tutti e soli i multipli di $MCD(a,b)$

Come calcolare m ed n dati a e b?

Intanto suppongo WLOG che $MCD(a,b) = 1$.

Divisioni euclidee iterate

$a = 70 \quad b = 13$

$$\begin{aligned} 70 &= 13 \cdot 5 + 5 \\ 13 &= 5 \cdot 2 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \end{aligned}$$

Iterando l'algoritmo prima o poi si trova resto $= 1$.

Adesso procedo al contrario

Mi prendo 1 dall'ultima

Mi prendo 2 dalla penultima

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ &= 3 - (5 - 3 \cdot 1) \cdot 1 \\ &= 3 \cdot 2 - 5 \qquad \text{Mi prendo 3} \\ &= (13 - 5 \cdot 2) \cdot 2 - 5 \\ &= 13 \cdot 2 - 5 \cdot 5 \qquad \text{Mi prendo 5} \\ &= 13 \cdot 2 - (70 - 13 \cdot 5) \cdot 5 \\ &= 13 \cdot 27 - 70 \cdot 5 \end{aligned}$$

Quindi ho ottenuto che $13 \cdot 27 - 70 \cdot 5 = 1$

Dati a e b con $MCD(a,b) = 1$, sono unici m ed n t.c. $am + bn = 1$?

Ovviamente NO! Nell'esempio $13 \cdot (27 + 70) - 70 \cdot (5 + 13) = 1$

Come sono fatte TUTTE le soluzioni?

Sia (m, n) una soluzione: $am + bn = 1$
Sia (m_1, n_1) un'altra soluzione: $am_1 + bn_1 = 1$

Differenza: $a(m - m_1) + b(n - n_1) = 0$
$a(m - m_1) = b(n_1 - n)$

Poiché $MCD(a,b) = 1$, si ha che $a \mid (n_1 - n)$ (a divide), quindi
$n_1 - n = ka$, e di conseguenza $m - m_1 = kb$, cioè

$m_1 = m - kb$ $\qquad$ $n_1 = n + ka$

Basta sostituire per vedere che (m_1, n_1) va bene per ogni $k \in \mathbb{Z}$.

— o — o —

Scrittura di un intero positivo in base b

$$n = \underbrace{a_k a_{k-1} \dots a_1 a_0}_{\text{cifre in base } b,\ \text{quindi } 0 \le a_i \le b-1}$$
$$= a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0$$

Esempio Scrivere 70 in base 2

$$70 = 1 \cdot 64 + 0 \cdot 32 + 0 \cdot 16 + 0 \cdot 8 + 1 \cdot 4 + 1 \cdot 2 + 0 \cdot 1$$
$$= (1000110)_2$$

Esempio $f : \mathbb{N} \to \mathbb{N}$ $\qquad$ $f(0) = f(1) = 0$
$f(2n) = 2f(n) + 1$ $\qquad$ $f(2n+1) = 2f(n)$

In binario

$f(0) = 0$
$f(1) = 0$
$f(2) = 1$
$f(3) = 0$
$f(4) = 3$
$f(5) = 2$
$f(6) = 1$
$f(70) =$

$f(0) = 0$
$f(1) = 0$
$f(10) = 1$
$f(11) = 0$
$f(100) = 11$
$f(101) = 10$
$f(110) = 1$
$f(1000110) = 111001$

[Si tratta di dim. formalmente per induzione che f "inverte" le cifre in base 2]

$n = [1\,1\,0\ldots\ldots]$ $\qquad 2n+1 = [\qquad\quad]\,1$ ← invertito.

$f(n) = [$ invertito $]$ $\qquad f(2n+1) = 2f(n)$

$= [$ invertito $]\,0$

— o — o —

Esercizio $\qquad d_n = MCD\,(100+n^2,\ 100+(n+1)^2)$

Quanto può valere al massimo d_n ?

$d_n \mid 100+n^2$

$d_n \mid 100+(n+1)^2 = n^2+2n+101$

$\Rightarrow d_n \mid n^2+2n+101-(100+n^2) = 2n+1$

Ora so che $\quad d_n \mid n^2+100 \Rightarrow d_n \mid 4n^2+400$

$d_n \mid 2n+1$

$4n^2+400 \;\big|\; 2n+1$

$-4n^2-2n \;\big|\; 2n-1$

$-2n+400$

$+2n+1$

401

$4n^2+400 = (2n+1)(2n-1)+401$

$d_n \uparrow \qquad d_n \uparrow$

$\Rightarrow d_n \mid 401$

$\Rightarrow d_n$ può essere solo 1 oppure 401

Devo trovare un esempio in cui effettivamente $d_n = 401$

Dalla condizione $d_n \mid 2n+1$ una possibilità è provare $n = 200$

Devo controllare $\quad 401 \mid 200^2+100 = 4\cdot 100\cdot 100+100 = 401\cdot 100$

$401 \mid 201^2+100$

Per la 2ª o si fa il conto scrivendo $201^2 = (200+1)^2$,

oppure si osserva che

$200 \equiv -201 \pmod{401}$

$200^2 \equiv 201^2 \pmod{401}$

— o — o —

CONGRUENZE

$a \equiv b \pmod n$ $\quad n$ intero ≥ 2

$\iff$ a e b hanno stesso resto quando divisi per n

$\iff$ $a-b$ è multiplo di n.

Fatto generale: ogni intero è congruo (mod n) ad un intero in $\{0, 1, \dots, n-1\}$

Si comportano bene rispetto a somma e prodotto

$$\begin{aligned} a_1 &\equiv b_1 \\ a_2 &\equiv b_2 \end{aligned} \implies a_1 \pm a_2 \equiv b_1 \pm b_2 \qquad a_1 \cdot a_2 \equiv b_1 \cdot b_2$$

Divisione $\quad 5x \equiv 2 \pmod{13} \quad x \equiv "\frac{2}{5}" \pmod{13}$

Inverso di 5 mod 13 è 8 : infatti $5 \cdot 8 = 40 \equiv 1 \pmod{13}$

$$\begin{aligned} 5x &\equiv 2 \pmod{13} \\ 40x &\equiv 16 \pmod{13} \end{aligned}$$ Moltiplico per 8 !

$$x \equiv 3 \pmod{13}$$

Come si trova l'inverso ? Trovare l'inverso di 5 (mod 13) vuol dire trovare un numero m t.c. $5m \equiv 1 \pmod{13}$ cioè $5m = 1 + 13w$, cioè $5m - 13w = 1$, quindi è come in BEZOUT.

L'inverso esiste se e solo se ciò che voglio invertire ed il modulo hanno MCD = 1.

Inverso di 7 mod 13 : 2 $\quad (7 \cdot 2 \equiv 1 \pmod{13})$

di 7 mod 16 : 7 $\quad (7 \cdot 7 \equiv 1 \pmod{16})$

di 7 mod 12 : 7 $\quad (7 \cdot 7 \equiv 1 \pmod{12})$

Inverso di 7 mod 36:

$7 \cdot 5 = 35 \equiv -1 \pmod{36}$

$7 \cdot (-5) = -35 \equiv 1 \pmod{36}$

$7 \cdot 31 \equiv 1 \pmod{36}$

Fatto generale: voglio risolvere $ax \equiv b \pmod{n}$

OK se $MCD(a,n) = 1$.

Se a ed n non sono primi tra loro, può esistere o non esistere x.

$3x \equiv 5 \pmod{12}$

Impossibile perché $3x = 5 + 12k$ (3 | NO 3 | 3)

$6x \equiv 8 \pmod{12} \iff 2x \equiv 3 \pmod{4}$

$6x = 8 + 12k \iff 2x = 3 + 4k \iff 2x \equiv 3 \pmod{4}$

Occhio a semplificare nelle congruenze.

— o — o —

Criteri di congruenza

Un numero è congruo modulo 2 alla sua cifra delle unità

" " " 3 alla somma delle sue cifre

" " " 4 al numero costituito dalle ultime 2 cifre

" " modulo 8 alla somma delle cifre

" " modulo 11 alla somma delle cifre a segno alterno, in modo che la cifra delle unità abbia segno +.

$$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0 \overset{\text{mod } 3 \text{ o } 9}{\equiv} a_k + a_{k-1} + \dots + a_1 + a_0 \overset{\text{mod } 11}{\equiv} a_0 - a_1 + a_2 - a_3 + \dots$$

Esercizio 182 $18 - 2\cdot 2 = 14$ divisibile per 7, allora divisibile per 7 all'inizio

2008 $\rightsquigarrow 200 - 8\cdot 2 = 182 \rightsquigarrow 14 \rightsquigarrow$ ok

2072 $\rightsquigarrow 207 - 2\cdot 2 = 203 \rightsquigarrow 20 - 3\cdot 2 = 14 \rightsquigarrow$ ok

Questo è un criterio di DIVISIBILITÀ, ma non di congruenza.

Perché funziona?

Enunciato: $10A + B \equiv 0 \pmod 7 \iff A - 2B \equiv 0 \pmod 7$

Dim. Prendo $10A + B$ e moltiplico per 5 (inverso di 10)

$50A + 5B \equiv A - 2B \pmod 7$

Viceversa: se $A - 2B \equiv 0 \pmod 7$ moltiplico per 10 e ottengo

$10A - 20B \equiv 0 \pmod 7$

$10A + B \equiv 0$ ~.

C'è lo stesso modulo 13? $10A + B \equiv 0 \pmod{13}$

$\Updownarrow$

$A + kB \equiv 0 \pmod{13}$

Sol: $k = 4$. Basta prendere la 1ª e moltiplicare per 4 (inverso di 10 modulo 13).

Residui quadratici Risolvere $x^2 \equiv a \pmod m$

Si dice che a è residuo quadratico mod m se riesco a risolvere.

Appena $m \geq 3$ esistono valori di a per cui non si risolve.

Esercizio I residui quadratici mod 401 sono 201.

Calcolo $0^2, 1^2, 2^2, \dots, 400^2$. Tranne 0^2, tutti gli altri $(\pm k)^2 = k^2$. Ci possono essere più sovrapposizioni?

$x^2 \equiv y^2 \pmod{401}$ vuol dire per forza che $x \equiv \pm y \ (401)$?

$(x+y)(x-y) = 401k$. Essendo 401 primo abbiamo che

o $401 \mid x-y$ (quindi $x \equiv y$) o $401 \mid x+y$ (quindi $x \equiv -y$).

STRUTTURA MOLTIPLICATIVA — p PRIMO

Come si comportano $a^0, a^1, a^2, a^3, \ldots \pmod p$
nel caso $MCD(a,p) = 1$.
Le potenze sono periodiche!!

Esempio $p = 7$

$2^0 \equiv 1$ $\quad 2^3 \equiv 1$
$2^1 \equiv 2$ $\quad 2^4 \equiv 2^3 \cdot 2 \equiv 2 \pmod 7$
$2^2 \equiv 4$ $\quad 2^5 \equiv 4$

Le potenze di 2 si ripetono con periodo 3.

$3^0 \equiv 1$
$3^1 \equiv 3$
$3^2 \equiv 2$
$3^3 \equiv 6 \equiv (-1)$
$3^4 \equiv 4 \equiv (-3)$
$3^5 \equiv 5$
$3^6 \equiv 1$

Le potenze di 3 si ripetono con periodo 6

Le potenze di 6, cioè le potenze di -1, si ripetono con periodo 2.

Definizione Si chiama ordine moltiplicativo di $a \bmod p$ il periodo (più piccolo) delle potenze di $a \bmod p$.
Si indica con

$$\boxed{\mathrm{ord}_p(a)}$$

Esempi $\mathrm{ord}_7(2) = 3$ $\quad \mathrm{ord}_7(3) = 6$ $\quad \mathrm{ord}_7(6) = 2$
$\mathrm{ord}_7(1) = 1$

Dim. della periodicità. Considero $a^0, a^1, a^2, \ldots, a^p, \ldots$
Sono infiniti oggetti che possono essere solo $1, 2, \ldots, p-1$.
Quindi prima o poi c'è una ripetizione, cioè esistono
$m < n$ t.c. $a^m \equiv a^n \pmod p$, cioè
$a^n - a^m = kp$, cioè $a^m(a^{n-m} - 1) = kp$. Essendo
$MCD(a,p) = 1$, devo avere $p \mid (a^{n-m} - 1)$, cioè
$a^{n-m} \equiv 1 \ (p)$, quindi c'è una potenza con esp $\neq 0$ che fa 1.

Corollario Fino a quando non si ripete la classe 1, nessuna classe si ripete.

Quindi $a^0 = 1$, poi tutti diversi fino a quando per un certo k si ha che $a^k \equiv 1$, da lì in poi si ripete. Chi è k? $k = \mathrm{ord}_p(a)$.

Applicazione 1 Supponiamo che $a^n \equiv 1 \pmod p$.
Allora $\mathrm{ord}_p(a) \mid n$

Applicazione 2 Supponiamo che $a^n \equiv a^m \pmod p$
Allora $\mathrm{ord}_p(a) \mid m-n$

PICCOLO TEOREMA DI FERMAT

Versione 1 : $a^{p-1} \equiv 1 \pmod p$ se $\mathrm{MCD}(a,p) = 1$
Versione 2 : $a^p \equiv a \pmod p$ per ogni a

Corollario $\mathrm{ord}_p(a)$ è sempre un divisore di $p-1$.

— o — o —

DIM FLT 1 $a^p \equiv a \pmod p$
Per induzione su a : banale per $a=0$ o per $a=1$
P.I. Hp : $a^p \equiv a \pmod p$ Tesi : $(a+1)^p \equiv a+1 \pmod p$

$$(a+1)^p = a^p + \underbrace{\binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \dots + \binom{p}{p-1}a}_{\text{multipla di } p} + 1 = (\star)$$

dove $\binom{p}{k} = \dfrac{p!}{k!(p-k)!}$ ← Tutti multipli di p, tranne per $k=0$ e $k=p$

uso Hp induttiva.

$$(\star) \equiv a^p + 1 \equiv a + 1$$

DIM FLT 2 $a^{p-1} \equiv 1 \pmod p$

$\{1, 2, \dots, p-1\}$ = tutte classi non nulle mod p

$\{a, 2a, \dots, (p-1)a\}$ = nuovamente tutte le classi mod p

Perché? Sono $(p-1)$ oggetti e sono tutti distinti perché se fosse $ma = na \pmod p$

vorrebbe dire che $a(m-n)$ è multiplo di p

a: no multiplo di p per ipotesi; $(m-n)$: troppo piccolo per essere multiplo di p

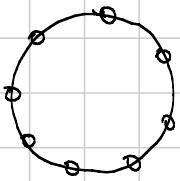
Allora

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \equiv a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a$$

$$(p-1)! \equiv (p-1)!\, a^{p-1} \pmod p$$

cioè $(p-1)!\,[a^{p-1}-1] = kp$ $\Rightarrow$ p sta per forza in $(a^{p-1}-1)$

DIM FLT 3



Collana con p palline che voglio colorare con a colori. Considero equivalenti 2 collane che si ottengono l'una dall'altra mediante rotazioni.

Quante sono le possibili collane NON monocromatiche?

TUTTE: a^p — MONOCROMATICHE: a

Devo dividere per tener conto della rotazione.

Una certa colorazione, quante altre diverse ne genera RUOTANDO?

Se ne genera p ho che $\frac{a^p - a}{p}$ è intero e ho finito.

Se una collana ruotando di k torna in sé vuol dire che la 0 è colorata come la k, la 2k, la 3k, …, $(p-1)k$, ma queste sono tutte distinte, quindi sarebbe monocromatica.

— o — o —

IMO 2009 – 1 $a_1, \dots, a_k$ interi in $\{1, \dots, n\}$ distinti

$n \mid a_i (a_{i+1} - 1) \quad i = 1, \dots, k-1$

Tesi: $n \nmid a_k (a_1 - 1)$

Ipotesi: $n \mid a_1 (a_2 - 1)$
$n \mid a_2 (a_3 - 1)$
$n \mid a_3 (a_4 - 1)$
$\vdots$
$n \mid a_{k-1} (a_k - 1)$

Tesi: $n \nmid a_k (a_1 - 1)$

Dim Supponiamo che oltre all'ipotesi valga anche $n \mid a_k (a_1 - 1)$ e cerchiamo un assurdo.

$n \mid a_1 (a_2 - 1) \iff a_1 (a_2 - 1) \equiv 0 \pmod n \iff a_1 \equiv a_1 a_2 \pmod n$

$a_1 \equiv a_1 a_2 \pmod n$
$a_2 \equiv a_2 a_3 \pmod n$ } $a_1 \equiv a_1 a_2 a_3$
$a_3 \equiv a_3 a_4 \pmod n$ } $a_1 \equiv a_1 a_2 a_3 a_4$
$\vdots$

Per induzione ottengo che $a_1 \equiv a_1 \cdots a_k \pmod n$

Oss.: Fin qui ho usato l'ipotesi, ma non la tesi negata.

Nel momento in cui assumo che la tesi sia falsa, l'ipotesi diventa ciclica, quindi posso partire da un qualunque a_i

Ottengo $a_i \equiv$ prodotto di tutti per ogni $i = 1, \dots, k$.

Quindi tutti gli a_i hanno la stessa classe $\pmod n$ ed essendo in $\{1, \dots, n\}$ dovrebbero coincidere. Assurdo.

—o—o—

IMO 2006 – 4 $\quad 1 + 2^x + 2^{2x+1} = y^2 \qquad x, y$ interi

Bisognerebbe trattare il caso di $x \le 0$, che è facile ma richiede qualche considerazione (e vengono soluzioni)
D'ora in poi $x > 0$, quindi LHS dispari, quindi y dispari
$y = 2n+1$

$$1 + 2^x + 2^{2x+1} = 4n^2 + 4n + 1$$

$$2^x (1 + 2^{x+1}) = 4n(n+1) \qquad \text{quindi } x \ge 2$$

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

Ora il 2^{x-2} deve andare tutto nello stesso fattore del RHS

- Caso 1: $n = k \cdot 2^{x-2}$: $2^{x-2}(1 + 2^{x+1}) = k \cdot 2^{x-2}(k \cdot 2^{x-2} + 1)$

$$1 + 2^{x+1} = k^2 2^{x-2} + k$$

Per ragioni di disuguaglianze k può essere solo 1 oppure 2

Se $k \ge 3$, allora $k^2 2^{x-2} + k \ge 9 \cdot 2^{x-2} + 3$
$> 8 \cdot 2^{x-2} + 3$
$> 2^{x+1} + 1$

Sostituito $k=1$ o $k=2$, c'è una sola incognita...

- Caso 2: $n+1 = k \cdot 2^{x-2}$: $2^{x-2}(1 + 2^{x+1}) = k 2^{x-2}(k 2^{x-2} - 1)$

$$1 + 2^{x+1} = k^2 2^{x-2} - k$$

Ancora una volta k non può essere troppo grande, ma va detto bene

$k^2 \ge k + 8$ vera per ogni $k \ge 4$, quindi se $k \ge 4$ ho che

$$k^2 2^{x-2} - k \ge (k+8) 2^{x-2} - k = k 2^{x-2} + 2^{x+1} - k \overset{?}{\ge} 2^{x+1} + 1$$
$$= k(2^{x-2} - 1) \overset{?}{\ge} 1$$

vera appena $x \ge 3$ (controllare $x = 2$ a mano).

— o — o —

IMO 2005-4 Per ogni primo p esiste un intero positivo n t.c.
$p \mid 2^n + 3^n + 6^n - 1$

$p=2$ $\quad 2 \mid 2^n+3^n+6^n-1 \iff 2 \mid 3^n-1$ basta $n=1$
$p=3$ $\quad 3 \mid$ " $\iff 3 \mid 2^n-1$ " $n=2$

Oss. "border line": $n=-1$ in un certo senso va bene
$\frac{1}{2}+\frac{1}{3}+\frac{1}{6}-1=0$

Oss. "più seria": se $p \neq 2,3$, allora

(inverso di 2) + (inverso di 3) + (inverso di 6) $\equiv 1 \pmod p$

a = inv. di 2
b = inv. di 3
c = inv. di 6

$6(a+b+c) \equiv 6a+6b+6c$
$\equiv 3\cdot 2a + 2\cdot 3b + 6c$
$\equiv 3+2+1$
$\equiv 6 \pmod p$

Essendo $p \neq 2,3$ posso "semplificare il 6"

FLT $\Rightarrow$ elevare alla $p-1$ è come elevare alla 0, quindi
" " $p-2$ " " " " -1, cioè come fare l'inverso.

Quindi basta prendere $n=p-2$.

Per $p \neq 2,3$ considero $n=p-2$

$$6\left(2^{p-2}+3^{p-2}+6^{p-2}\right) = 3\cdot 2^{p-1} + 2\cdot 3^{p-1} + 6^{p-1} \overset{(FLT)}{\equiv}$$
$$\equiv 3+2+1$$
$$\equiv 6 \pmod p$$

Essendo $p \neq 2,3$ ho che $2^{p-2}+3^{p-2}+6^{p-2} \equiv 1 \pmod p$.

— o — o —

SENIOR 2011 – TEORIA DEI NUMERI 2 (Basic)

Titolo nota 07/09/2011

TEOREMA CINESE DEL RESTO (CRT)

Sistema di congruenze: cerco x intero t.c.

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

Si intende che $a_1, \dots, a_n$ sono dati e anche i moduli $m_1, \dots, m_n$ sono dati

Teorema Se i moduli sono a 2 a 2 coprimi, cioè $\overbrace{(m_i, m_j)}^{MCD} = 1$ per ogni $1 \le i < j \le n$, allora il sistema ammette soluzione unica modulo $m_1 \cdot \dots \cdot m_n$.

Dim. **Unicità** Siano x e y 2 sol. Allora $x - y \equiv 0 \pmod{m_i}$ per ogni $i = 1, \dots, n$, quindi $x - y = k\, m_1 \cdot \dots \cdot m_n$.

Esistenza 1 Induzione su n. Per $n = 1$ non è difficile...
Supponiamo di saper risolvere un sistema di n congruenze, e aggiungiamo $x \equiv a_{n+1} \pmod{m_{n+1}}$.
La soluzione del sistema di n congruenze sarà

$$y + k\, m_1 \cdot \dots \cdot m_n$$

Ora cerco k in modo tale che

$$y + k\, m_1 \cdot \dots \cdot m_n \equiv a_{n+1} \pmod{m_{n+1}}$$

cioè

$$k\, m_1 \cdot \dots \cdot m_n \equiv a_{n+1} - y \pmod{m_{n+1}}$$

Poiché m_{n+1} è coprimo con i moduli precedenti, esiste di sicuro l'inverso di $m_1 \cdot \dots \cdot m_n \pmod{m_{n+1}}$
Basta moltiplicare per quello!

Esistenza 2 Divide et impera! Risolvo nel caso $a_1 = 1$ e $a_2 = \dots = a_n = 0$. La sol. sarà del tipo

$$x = k\, m_2 \cdot \dots \cdot m_n$$

Cerco k in modo che $x \equiv 1 \pmod{m_1}$.

Basta prendere k = inverso di $m_2 \cdot \dots \cdot m_n \pmod{m_1}$.

Per ogni $i = 1, \dots, n$ sia x_i la soluzione con $a_i = 1$ e tutti gli altri 0. Allora

$$x = a_1 x_1 + a_2 x_2 + \dots + a_n x_n$$

A cosa è congruo x modulo m_i?

$$x \equiv a_i x_i \equiv a_i \pmod{m_i}$$

— o — o —

Esempio

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 7 \\ x \equiv 1 \pmod{10} \end{cases}$$

$x = 2 + 3a$. Sistemo la 2ª: $2 + 3a \equiv 3 \pmod 7$

$3a \equiv 1 \pmod 7$ $\quad a \equiv 5 \pmod 7$, quindi

$$x = 2 + 3a = 2 + 3(5 + 7b) = 17 + 21b$$

Sistemo la 3ª: $17 + 21b \equiv 1 \pmod{10}$ $\quad 21b \equiv -16 \pmod{10}$

$b \equiv 4 \pmod{10} \Rightarrow x = 17 + 21(4 + 10c) = 101 + 210c.$

— o — o —

Oss. Se i moduli non sono primi tra di loro, allora il sistema può avere o non avere soluzioni.

Basta spezzare le varie congruenze rispetto ai fattori primi degli m_i e vedere se le condizioni sono compatibili

Esempio

$$\begin{cases} x \equiv 3 \pmod{10} \\ x \equiv 12 \pmod{15} \end{cases} \iff \begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 3 \pmod 2 \\ x \equiv 12 \pmod 5 \\ x \equiv 12 \pmod 3 \end{cases}$$

$x \equiv 3 \pmod{10}$

$x \equiv 12 \pmod{15}$

INCOMPATIBILI

(quindi nessuna soluzione

$$\begin{cases} x \equiv 7 \pmod{10} \\ x \equiv 12 \pmod{15} \end{cases} \qquad \begin{cases} x \equiv 7 \pmod 5 \\ x \equiv 7 \pmod 2 \\ x \equiv 12 \pmod 5 \\ x \equiv 12 \pmod 3 \end{cases} \quad \text{Ok} \qquad \begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 2 \\ x \equiv 0 \pmod 3 \end{cases}$$

La soluzione è $x \equiv 27 \pmod{30}$.

— o — o —

Fatto generale Sia $n = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$. Allora conosco x modulo n se e solo se conosco x modulo $p_i^{k_i}$ per ogni $i = 1, \ldots, r$.

— o — o —

Φ di Eulero Sia n un intero positivo. Si definisce

$$\Phi(n) = \#\{ m : 1 \le m \le n \text{ e } (m,n) = 1 \}$$

= numero degli interi tra 1 ed n che sono relativamente primi con n.

Casi facili: $\Phi(p) = p-1$ per ogni primo p.

$$\Phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

(p^k: tutti; p^{k-1}: quelli multipli di p) per ogni potenza di un primo p

Fatto fondamentale: Φ è una funzione moltiplicativa, cioè

$$\Phi(a \cdot b) = \Phi(a) \cdot \Phi(b) \quad \text{per ogni } a \text{ e } b \text{ coprimi}$$

Corollario Se $n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$, allora

$$\Phi(n) = \Phi(p_1^{k_1}) \cdot \ldots \cdot \Phi(p_r^{k_r}) = p_1^{k_1-1}(p_1-1) \cdot \ldots \cdot p_r^{k_r-1}(p_r-1)$$

$$= n\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right)$$

Dim. fatto fondamentale. Conosco m modulo ab se e solo se conosco m modulo a e modulo b.
Inoltre $(m, ab) = 1$ se e solo se $(m, a) = 1$ e $(m, b) = 1$.
Tutto ciò segue dal CRT.
Quindi

$$\{\text{Classi coprime con } ab\} = \{\text{Classi coprime con } a\} \cdot \{\text{Classi coprime con } b\}$$

ha $\phi(ab)$ elem. $\phi(a)$ elem. $\phi(b)$ elem.

— o — o —

Esempi

$$\phi(10) = \phi(2)\cdot\phi(5) = 1\cdot 4 = 4$$
$$\phi(25) = 25 - 5 = 20$$
$$\phi(100) = \phi(4)\cdot\phi(25) = 2\cdot 20 = 40$$
$$\phi(2000) = \phi(16)\cdot\phi(125) = (16-8)(125-25) = 8\cdot 100 = 800$$
$$\phi(360) = \phi(8\cdot 5\cdot 9) = \phi(8)\cdot\phi(5)\cdot\phi(9) = 4\cdot 4\cdot 6 = 96$$

— o — o —

Le classi coprime con m sono le classi invertibili modulo m, e sono le classi dove fare la struttura moltiplicativa

— o — o —

Esempio 1 Dim. che per ogni intero positivo n esisto n interi consecutivi divisibili per un quadrato perfetto non banale.

Siano $x+1, x+2, \dots, x+n$ gli interi cercati. Scelgo n primi distinti $p_1, p_2, \dots, p_n$ e impongo

$$x+1 \equiv 0 \pmod{p_1^2} \qquad x \equiv -1 \pmod{p_1^2}$$
$$x+2 \equiv 0 \pmod{p_2^2} \qquad x \equiv -2 \pmod{p_2^2}$$
$$\vdots \qquad\qquad \vdots$$
$$x+n \equiv 0 \pmod{p_n^2} \qquad x \equiv -n \pmod{p_n^2}$$

Esempio 2 Per ogni n esistono n interi consecutivi ciascuno dei quali NON è una potenza perfetta.

Dim. 1 (CRT) Come prima impongo $x+i \equiv p_i \pmod{p_i^2}$ per $i = 1, \dots, n$. Così p_i compare con esponente uno nella fattorizzazione di $x+i$.

Dim. 2 (conteggio) In $1, 2, \dots, n$, quante sono circa le potenze perfette?

Saranno al max $\sqrt{n} + \sqrt[3]{n} + \sqrt[4]{n} + \dots + \sqrt[k]{n}$ dove $k = \log_2 n$

Quindi

Numero potenze perfette minori od uguali di n $\leq$ $\sqrt{n} \cdot \log_2 n$

↓ Questo numero è molto minore di n, cioè $\lim_{n\to+\infty} \frac{\sqrt{n}\cdot \log_2 n}{n} = 0$

Quindi tra le potenze perfette ci devono essere dei buchi enormi.

Conclusione stile pigeonhole: scelgo n grande tale che $\sqrt{n} \log_2 n \leq \frac{n}{11}$. Ora divido $1, \dots, n$ in

$\frac{n}{10}$ blocchi di 10 interi consecutivi. Almeno 1 blocco non contiene una potenza perfetta.

— o — o —

IMO 1989 – 5 Per ogni n esistono n interi consecutivi nessuno dei quali è primo o potenza di un primo.

Prendo $p_1, \dots, p_n, q_1, \dots, q_n$ $2n$ primi distinti e impongo

$x + i \equiv 0 \pmod{p_i q_i}$.

— o — o —

STRUTTURA MOLTIPLICATIVA MODULO m

Si riduce facilmente alla struttura modulo p^k.

Prendo $(a,m)=1$ e considero $a^0, a^1, a^2, a^3, \dots$
Sono tutte classi coprime con m.
Prima poi una classe si ripete (pigeonhole).
Se $a^k \equiv a^R \pmod m$, con WLOG $R<k$, allora

$$a^k - a^R = bm, \text{ cioè } a^R(a^{k-R}-1) = bm$$

Poiché $(a,m)=1$ dovrà essere $a^{k-R}-1 \equiv 0 \pmod m$,
quindi la classe 1 è la prima a ripetersi.

Pongo $\operatorname{ord}_m(a)$ il più piccolo k positivo t.c. $a^k \equiv 1 \pmod m$.

Fatto generale. Se $(a,m)=1$, allora $\operatorname{ord}_m(a) \mid \phi(m)$

Dim Siano $\{x_1, x_2, \dots, x_{\phi(m)}\}$ tutte le classi coprime con m
Allora $\{ax_1, ax_2, \dots, ax_{\phi(m)}\}$ sono le stesse classi, eventualmente permutate (se fosse $ax_i \equiv ax_j$ sarebbe $a(x_i - x_j) = bm$, ma ciò non può essere perché $(a,m)=1$ e $x_i - x_j$ è troppo piccolo per essere divisibile per m)
Quindi

$$x_1 \cdot \dots \cdot x_{\phi(m)} = ax_1 \cdot \dots \cdot ax_{\phi(m)} = a^{\phi(m)} \cdot x_1 \cdot \dots \cdot x_{\phi(m)}$$

Se semplifico $x_1 \cdot \dots \cdot x_{\phi(m)}$ (che è coprimo con m) ottengo

$$\boxed{a^{\phi(m)} \equiv 1 \pmod m}$$ estensione del FLT.

Per la periodicità gli esponenti k t.c. $a^k \equiv 1 \pmod m$ sono tutti e soli i multipli dell'ordine, quindi $\phi(m)$ è multiplo di $\operatorname{ord}_m(a)$.

— o — o —

Teorema di Wilson Se p è primo, allora $(p-1)! \equiv -1 \ (p)$

Dim. $(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2)(p-1)$. Se accoppio ogni termine con il suo inverso il prodotto viene 1. Questo vale per tutti i termini che non sono inversi di se stessi.
Qui è inverso di se stesso? Deve essere $x^2 \equiv 1 \ (p)$, cioè $x^2 - 1 = kp$, cioè $(x+1)(x-1) = kp$, cioè $x = \pm 1 \ (p)$.

—o— o —

Achtung! Modulo m non è vero in generale che $x^2 \equiv 1 \ (m)$ ha come soluzioni solo $x \equiv \pm 1 \ (m)$

Esempio Risolvere $x^2 \equiv 1 \pmod{40}$

Per il CRT è equivalente a risolvere $\begin{cases} x^2 \equiv 1 \pmod 8 \\ x^2 \equiv 1 \pmod 5 \end{cases}$

$\begin{cases} x \equiv 1, 3, 5, 7 \pmod 8 \\ x \equiv \pm 1 \pmod 5 \end{cases}$ Quindi in totale ho 8 soluzioni.

—o— o —

GENERATORI Se $(a, m) = 1$ e $\text{ord}_m(a) = \varphi(m)$ si dice che a è un generatore modulo m.

Questo vuol dire che facendo le potenze di a con esponente che va da 1 a $\varphi(m)$ (oppure da 0 a $\varphi(m)-1$) ottengo TUTTE le classi coprime con m.

Teorema Esiste un generatore se e solo se $m = 2, 4, p^k, 2p^k$ (con p primo dispari e $k \geq 1$).

—o— o —

Esempi -1 è generatore mod 4, 2 è gen. mod 3, 2 è gen. mod 5, 2 NON è generatore mod 7 in quanto $\text{ord}_7 2 = 3$, ma 3 è gen. mod. 7.

—o— o —

Esercizio Determinare se 2 è un generatore mod 37.

Considero $\mathrm{ord}_{37}\, 2$. Di sicuro è un divisore di 36. Se non fosse 36, allora dividerebbe o 18 o 12.

Fatto generale Se $d \mid n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ e $d \neq n$, allora $d \mid \frac{n}{p_i}$ per un qualche i.

Quindi se divide 36 e non è 36, allora divide $\frac{36}{2}$ o $\frac{36}{3}$.
Quindi mi basta dimostrare che
$2^{12} \not\equiv 1 \pmod{37}$ e $2^{18} \not\equiv 1 \pmod{37}$
Ora $2^6 = 64 \equiv -10 \pmod{37}$, quindi $2^{12} \equiv 100 \equiv -11 \pmod{37}$
$2^{18} \equiv -1000 \equiv -1 \pmod{37}$

Conseguenza: La congruenza $2^x \equiv a \pmod{37}$ ha soluzione per ogni $(a, 37) = 1$.

— o — o —

Perché non esiste un generatore mod 77? Dovrebbe avere ordine $\phi(77) = \phi(7) \cdot \phi(11) = 60$.
La classe mod 77 dipende da quella mod 7 e mod 11.
Le potenze di un certo a ciclano con periodo 6 mod 7 e periodo 10 mod 11,
quindi di sicuro $a^{30} \equiv 1 \pmod{77}$ per ogni $(a, 77) = 1$.
Quindi per ogni $(a, 77) = 1$ si ha che $\mathrm{ord}_{77}(a) \mid 30$.

Oss. 1 Esiste sempre un elemento di ordine 30 mod 77.
Basta che sia congruo ad un gen. mod 7 e un gen. mod. 11.

Oss. 2 Lo stesso ragionamento dice che il massimo ordine modulo un certo n è il m.c.m. delle ϕ delle potenze dei primi che compongono n.

Fatto generale Se g è un generatore mod p, allora g oppure $g+p$ è un generatore mod p^2.

Dim. Devo dimostrare che $\mathrm{ord}_{p^2}(g) = \phi(p^2) = p(p-1)$.
Ora se $g^k \equiv 1 \pmod{p^2}$, allora $g^k \equiv 1 \pmod{p}$, quindi k è multiplo di $\mathrm{ord}_p(g) = p-1$ (perché g è gen. mod p).
Quindi ho 2 possibilità:
$\mathrm{ord}_{p^2}(g) = p-1$ oppure $\mathrm{ord}_{p^2}(g) = p(p-1)$.
Se sono nel primo caso provo con $g+p$. Lo stesso ragionamento di prima mi porta a dire che
$\mathrm{ord}_{p^2}(g+p) = p-1$ oppure $\mathrm{ord}_{p^2}(g+p) = p(p-1)$
Se fossi nel primo caso vorrebbe dire che

$$(g+p)^{p-1} \equiv 1 \pmod{p^2}$$

$$= g^{p-1} + (p-1)g^{p-2} \cdot p + \text{roba con } p^2$$

↕ perché sono nel 1° caso

$$\equiv 1 - g^{p-2} \pmod{p^2}$$

Questo vorrebbe dire che $g^{p-2} \equiv 0 \pmod{p^2}$, che è assurdo.

—o—o—

Fatto generale Se g è generatore mod p e mod p^2, allora g è generatore mod p^k per ogni $k \geq 1$.

Esempio: 2 è gen. modulo 3^{50}.

—o—o—

Quante sono i generatori modulo p? Sono $\phi(\phi(p))$.

Sia g un generatore. Ogni altro elemento si scrive come $a = g^k$
Se $(k, p-1) = d > 1$, allora a non è generatore. Infatti

$$a^{\frac{p-1}{d}} = g^{k\frac{p-1}{d}} = g^{\boxed{\frac{k}{d}}(p-1)} = \left[g^{p-1}\right]^{\frac{k}{d}} \equiv 1 \pmod p$$

(intero)

quindi $\operatorname{ord}_p(a) \mid \frac{p-1}{d}$ e quindi è $< p-1$.

Viceversa, se $(k, p-1) = 1$, allora $a = g^k$ è generatore.

Supponiamo che $a^\alpha \equiv 1 \pmod p$. Allora $g^{k\alpha} \equiv 1 \ (p)$.

Allora $k\alpha = b(p-1)$, ma essendo $(k, p-1) = 1$ dovrà essere $p-1 \mid \alpha$, quindi $\alpha \geq p-1$.

— o — o —

<u>Esempio</u> Sia $p = 37$, sia g un generatore mod 37

$$\underset{\downarrow}{g^0}, \underset{\downarrow}{g^1}, \underset{\downarrow}{g^2}, \underset{\downarrow}{g^3}, \underset{\downarrow}{g^4}, \underset{\downarrow}{g^5}, \underset{\downarrow}{g^6}, \underset{\downarrow}{g^7}, \underset{\downarrow}{g^8}, \underset{\downarrow}{g^9}, \underset{\downarrow}{g^{10}}, \ldots$$

$$1 \quad 36 \quad 18 \quad 12 \quad 9 \quad 36 \quad 6 \quad 36 \quad 9 \quad 4 \quad 18 \quad \text{ordini}$$

— o — o —

<u>Esercizio</u> $x^9 \equiv a \pmod{37}$ ha soluzione se e solo se $\operatorname{ord}_{37}(a) \mid 4 \iff a^4 \equiv 1 \ (37)$

In particolare $x^9 \equiv 6 \pmod{37}$ ha sol. perché $6^4 = 36^2 \equiv 1 \ (37)$

— o — o —

<u>Fatto generale</u> Si ha che -1 è residuo quadratico mod p $\iff p \equiv 1 \ (4)$ oppure $p = 2$.

<u>Dim.</u> $x^2 \equiv -1 \ (p) \quad x^4 \equiv 1 \ (p)$

$\Rightarrow \operatorname{ord}_p(x) \mid 4$ e $\operatorname{ord}_p(x)$ non è 1 o 2 se $p \neq 2$

$\Rightarrow \operatorname{ord}_p(x) = 4$

$\Rightarrow 4 \mid p-1$, cioè $p \equiv 1 \ (4)$ (perché ord $\mid \phi$)

Fatto generale Si ha che $x^4 \equiv -1 \pmod p$ ha soluzione $\iff$ $p \equiv 1 \pmod 8$ oppure $p = 2$.

Achtung! Vale solo con i fattori 2.

Fatto generale Come sono fatti i primi che dividono a^2+b^2?
" " " a^4+b^4?
" " " a^8+b^8?

O sono primi che dividono a e b, oppure sono $\equiv 1 \bmod 4$ nel 1° caso, $\bmod 8$ o $\bmod 16$ nel 2° e 3° caso.

Dim. Sia $p \mid a^2+b^2$, e supponiamo $p \nmid a$ e $p \nmid b$.
Questo dice che

$$a^2 \equiv -b^2 \pmod p$$

Quindi esiste c ($=$ a. inverso di b) tale che

$$c^2 \equiv -1 \pmod p$$

$\Rightarrow -1$ è residuo quadratico $\Rightarrow$ $p \equiv 1 \pmod 4$.

— o — o —

Esistono ∞ primi $\equiv 3 \pmod 4$ Se fossero solo $p_1, \dots, p_n$, prendo

$$4 p_1 \cdot \dots \cdot p_n - 1 \qquad (\equiv 3 \bmod 4 \text{ e ha nuovo primo})$$

Esistono ∞ primi $\equiv 1 \pmod 4$. Non basta considerare

$4 p_1 \cdot \dots \cdot p_n + 1$, perché questo ha fattori nuovi che potrebbero essere $\equiv 3 \bmod 4$. Basta però considerare

$$(2 p_1 \cdot \dots \cdot p_n)^2 + 1$$

Essendo $\square + 1$, tutti i suoi fattori primi sono $\equiv 1 \pmod 4$.

— o — o —

BMO 2009 – 1 $3^x - 5^y = z^2$ x, y, z interi positivi

z è pari. Facendo mod 4: $(-1)^x - 1 \equiv 0 \pmod 4$

$\Rightarrow x$ è pari $\Rightarrow x = 2a$

$3^{2a} - z^2 = 5^y \Rightarrow (3^a + z)(3^a - z) = 5^y$

$$\Rightarrow \begin{cases} 3^a + z = 5^{y_1} \\ 3^a - z = 5^{y_2} \end{cases} \Rightarrow 2 \cdot 3^a = 5^{y_1} + 5^{y_2} \Rightarrow$$ il più piccolo esponente $y_2 = 0$

$\Rightarrow 2 \cdot 3^a = 5^y + 1$ ($a = y = 1$ è una soluzione)

Prendo mod 9 perché le cose cambiano quando $a \geq 2$.

$5^y \equiv -1 \pmod 9 \Rightarrow y \equiv 3 \pmod 6$

Quando modulo 7 perché $\phi(7) = \phi(9)$

Essendo $y \equiv 3 \pmod 6$ ho che $5^y \equiv -1 \pmod 7$, quindi RHS è $\equiv 0$ mod 7, mentre LHS $= 2 \cdot 3^a$ non lo è. Quindi no altre soluzioni

Altra soluzione: $5^y \equiv -1 \pmod{3^a}$

$5^{2y} \equiv 1 \pmod{3^a}$

$\Rightarrow \operatorname{ord}_{3^a}(5) \mid 2y$

Ora $\operatorname{ord}_{3^a}(5) = \phi(3^a) = 2 \cdot 3^{a-1}$ (questo perché 5, essendo generatore mod 9, lo è pure mod 3^a per ogni a)

$\Rightarrow 2 \cdot 3^{a-1} \mid 2y \Rightarrow 3^{a-1} \mid y$

Quindi $5^y + 1 \geq 5^{3^{a-1}} + 1$ e questo è ben presto molto più grande di $2 \cdot 3^a$

(le disuguaglianze vanno scritte e dimostrate).

— o — o —

Esercizio FONDAMENTALE (PPP)

$$D = \{n \in \mathbb{N} : \ n \mid 2^n + 1\}$$

① Trovare tutti i primi $p \in D$.

$p \in D \iff 2^p + 1 \equiv 0 \pmod p \overset{\text{FLT}}{\iff} 2 + 1 \equiv 0 \pmod p \iff p = 3.$

② Trovare tutti i $p^k \in D$.

$p^k \in D \iff 2^{p^k} + 1 \equiv 0 \pmod{p^k} \implies 2^{p^k} + 1 \equiv 0 \pmod p \implies 2 + 1 \equiv 0 \pmod p$
$\implies p = 3$

Devo vedere per quali k ho che $3^k \mid 2^{3^k} + 1$

$k = 1 \quad 3 \mid 2^3 + 1$ Ok

$k = 2 \quad 9 \mid 2^9 + 1 = 513$ Ok $\qquad 513 = 9 \cdot 57 = 3^3 \cdot 19$

Fatto generale: $3^{k+1} \parallel 2^{3^k} + 1$ per ogni $k \geq 0$.
↓ divide esattamente

Induzione: $n = 1$ Ok

$n \implies n+1$

$$2^{3^{k+1}} + 1 = \left[2^{3^k}\right]^3 + 1 \qquad a^3 + 1 = (a^2 - a + 1)(a + 1)$$

$$= \underbrace{\left(2^{3^k} + 1\right)}_{3^{k+1} \parallel} \cdot \underbrace{\left(2^{2 \cdot 3^k} - 2^{3^k} + 1\right)}_{\text{devo dim. che } 3 \mid \text{il termine}}$$

Essendo $a \equiv -1 \pmod 3$ sarà $a = 3b - 1$, quindi

$$a^2 - a + 1 = (3b-1)^2 - (3b-1) + 1 = 9b^2 - 6b + 1 - 3b + 1 + 1$$
$$= 9b^2 - 9b + 3 \equiv 3 \pmod 9$$

Quindi $3^k \in D$ per ogni k.

Fatto ancora più generale Qual è la max potenza di 3 che divide 2^n+1 ?

Se n è pari, non è nemmeno divisibile per 3.
Se n è dispari lo scrivo come $n = 3^k \cdot d$, con $3 \nmid d$.
Allora la massima potenza è 3^{k+1}, cioè d è come se non ci fosse. Per dim. si usa la scomposizione $a^d+1 = (a+1)\cdot(\dots)$.

③ Dimostrare che tutti gli elementi di D sono multipli di 3.

Dim. Sia $n \in D$ e sia p il + piccolo primo che divide n.

$$n \in D \Leftrightarrow 2^n+1 \equiv 0 \ (n) \Rightarrow 2^n \equiv -1 \ (n)$$
$$\Rightarrow 2^n \equiv -1 \ (p)$$
$$\Rightarrow 2^{2n} \equiv 1 \ (p)$$

$\text{ord}_p(2) \mid 2n$
$\text{ord}_p(2) \mid (p-1)$

Supponiamo per assurdo che $(\text{ord}_p(2), n) = d > 1$.
Allora d dovrebbe dividere sia n, sia $(p-1)$, ma questo non è possibile perché p è il PPP.
Quindi $\text{ord}_p(2) = 1$ oppure $\text{ord}_p(2) = 2$

$2 \equiv 1 \ (p)$ $\quad$ $2^2 \equiv 1 \ (p)$
$\nexists$ $\quad$ $p = 3$.

④ Determinare tutti gli $n = pq \in D$, con p e q primi distinti

Dim: WLOG $p = 3$, quindi considero $2^{39} \equiv -1 \ (39)$

$2^{39} \equiv -1 \ (3)$ Banale perché 39 è dispari
$2^{39} \equiv -1 \ (q)$ FLT: $2^{39} \equiv 2^3 \equiv -1 \ (q) \Rightarrow q = 3 = p$.

⑤ Determinare tutti gli $n = p^2 q \in D$, con p e q primi dist.

DIM: devo considerare $3p^2$ e $9q$

$2^{3p^2} \equiv -1 \ (3p^2) \Rightarrow 2^{3p^2} \equiv -1 \ (p) \Rightarrow 2^3 \equiv -1 \ (p) \Rightarrow p = 3.$

$2^{9q} \equiv -1 \ (9q) \Rightarrow 2^{9q} \equiv -1 \ (9)$

$2^{9q} \equiv -1 \ (q) \overset{FLT}{\Rightarrow} 2^9 \equiv -1 \ (q)$

$513 \equiv 0 \ (q)$

$\Rightarrow q = 19$. Si tratta di verificare che 19 risolve anche la 1ª congruenza, ma questo si fa.

—o— o —

IMO 1990 – 3 Trovare tutti gli $n \in \mathbb{N}$ t.c. $n^2 \mid 2^n + 1$

Sol. $2^n + 1 \equiv 0 \ (n^2) \Rightarrow 2^n + 1 \equiv 0 \ (n) \Rightarrow n \in D$ di prima
$\Rightarrow n$ è dispari e multiplo di 3, quindi
$n = 3^k \cdot d$, con $3 \nmid d$.
Se n è soluzione del problema, sarebbe

$(3^k \cdot d)^2 \mid 2^{3^k d} + 1 \Rightarrow 3^{2k} \mid \underbrace{2^{3^k d} + 1}_{\text{la max potenza di 3 è } 3^{k+1}, \text{ quindi per } k \geq 2 \text{ è assurdo.}}$

—o —o —

IMO 2000 – 5 Dimostrare che l'insieme D di prima contiene elementi n divisibili per 2000 fattori primi

Dim. che esiste un elemento con 3 fattori primi. Con 2 fattori primi abbiamo $9 \cdot 19 = 3^2 \cdot 19$

$2^{3^3 \cdot 19} + 1 = \left[2^{3^2 \cdot 19}\right]^3 + 1 = \underbrace{\left(2^{3^2 \cdot 19} + 1\right)(\ldots)}_{\text{div. per } 3^4 \cdot 19}$

Lemma di guadagno di un primo

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

Tutti i primi che dividono $(a+1)$ dividono anche (a^3+1).
Però (a^3+1) ha un fattore primo in +, tranne nel caso

$$2^3+1 = (2+1)(4-2+1)$$

— o — o —

IMO 2008-3 Esistono infiniti n per cui n^2+1 ha un fattore primo $\geq 2n+\sqrt{2n}$.

Dim. Sia p il fattore. Allora -1 è residuo quadratico mod p.
Quindi $p \equiv 1 \pmod 4$.

Prendo un qualunque $p \equiv 1 \pmod 4$. So che $n^2 \equiv -1 \ (p)$ ha soluzione, anzi ha 2 soluzioni, di cui una è $n \leq \frac{p-1}{2}$.
Questo da solo dice che $p \geq 2n+1$.
In generale sarà $n = \frac{p-k}{2}$ per un opportuno k.

$$n^2+1 \equiv 0 \ (p) \iff \frac{p^2-2pk+k^2}{4} + 1 \equiv 0 \ (p)$$

$$\iff \frac{p^2-2pk+k^2+4}{4} \equiv 0 \ (p)$$

$$\iff k^2+4 \equiv 0 \ (p)$$
$$\implies k^2+4 \geq p$$

$$n = \frac{p-k}{2} \implies p = 2n+k$$
$$k^2+4 \geq p = 2n+k \implies k^2+4-k \geq 2n$$

Tolti i casi $k = 1, 2, 3, 4$ abbiamo che
$k^2 \geq k^2+4-k \geq 2n$, quindi $k \geq \sqrt{2n}$ e $p = 2n+k$
$\geq 2n+\sqrt{2n}$.

— o — o —