Stage Senior 2012 – Livello Basic

Stampato integrale delle lezioni

Autori vari

Indice

SENIOR 2012 – Basic – P

Titolo nota 02/09/2012

INDUZIONE

p proposizione che parla di n

" - - - - - n - - "

Volete dimostrare che $\forall n \in \mathbb{N}$ $p(n)$ è vera

$$I \begin{cases} (1)\ p(0) \text{ è vera} \\ (2)\ p(n) \Rightarrow p(n+1) \quad \forall n \in \mathbb{N} \end{cases}$$

Se p soddisfa le ipotesi I allora $\forall n \in \mathbb{N}$ $p(n)$ è vera

Teorema 0 Nelle ipotesi I, $p(0)$ è vera

Dim. La tesi è l'ip. (1)

Teorema 1 nelle ip I $p(1)$ è vera

$p(0)$ vera per T_0

$p(0) \Rightarrow p(1)$ per (2) con $n=0$

$p(1)$ è vera

Teorema 2 Nelle ip I $p(2)$ è vera

$p(1)$ vera per T_1

$p(1) \Rightarrow p(2)$ per (2) con $n=1$

$p(2)$ vera

Non riusciamo a dimostrare "$\forall n \in \mathbb{N}$ $p(n)$ è vera"

Esempio 1

$p(n) =$ " $n+1 \leq 2^n$ "

(1) PASSO BASE $\quad n=0 \quad p(0)$ è vera

$0+1 \leq 2^0 = 1$

(2) PASSO INDUTTIVO

Abbiamo dimostrare che $p(n+1)$ è vera sapendo che $p(n)$ è vera

$p(n+1) =$ " $(n+1)+1 \leq 2^{n+1}$ "

$(n+1) + 1 \leq 2^n + 2^n$ $\quad n+1 \leq 2^n$ perché $p(n)$ è vera

$1 \leq 2^n \quad \forall n \in \mathbb{N}$

Quindi $p(n) \Rightarrow p(n+1)$

Per induzione $\quad \forall n \in \mathbb{N} \quad n+1 \leq 2^n$

Esempio 2

$$0+1+2+\ldots+n = \sum_{i=0}^{n} i = \frac{n(n+1)}{2} \qquad \forall n \in \mathbb{N}$$

P.B. $\quad n=0 \qquad 0 = \dfrac{0(1)}{2}$

P.I. $\quad \boxed{0+\ldots+n} + n+1 = \dfrac{(n+1)(n+2)}{2}$

Sappiamo che $0+\ldots+n = \dfrac{n(n+1)}{2}$

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

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

Esempio 3

$$\sum_{i=0}^{n} \frac{i}{4^i} < \frac{1}{2} \qquad \forall n \in \mathbb{N}$$

Usiamo l'induzione

P.B. $\displaystyle\sum_{i=0}^{0} \frac{i}{4^i} = \frac{0}{4^0} < \frac{1}{2}$

P.I. $$\sum_{i=0}^{n+1} \frac{i}{4^i} = \left(\sum_{i=0}^{n} \frac{i}{4^i}\right) + \frac{n+1}{4^{n+1}} < \frac{1}{2} + \frac{n+1}{4^{n+1}}$$

Bisogna cambiare la disuguaglianza

Proviamo con $\displaystyle\sum_{i=0}^{n} \frac{i}{4^i} \leq \frac{1}{2} - \frac{1}{2^{n+1}} \left(< \frac{1}{2}\right)$

P.B. $\displaystyle\frac{0}{4^0} \leq \frac{1}{2} - \frac{1}{2} = 0$

P.I. $$\sum_{i=0}^{n+1} \frac{i}{4^i} \leq \frac{1}{2} - \frac{1}{2^{n+2}}$$

$$\sum_{i=0}^{n} \frac{i}{4^i} + \frac{n+1}{4^{n+1}} \leq \frac{1}{2} - \frac{1}{2^{n+1}} + \frac{1}{2^{n+1}} - \frac{1}{2^{n+2}}$$

$$\sum_{i=0}^{n} \frac{i}{4^i} \leq \frac{1}{2} - \frac{1}{2^{n+1}} \quad \text{per ip. induttiva}$$

$$\frac{n+1}{4^{n+1}} \overset{?}{\leq} \frac{1}{2^{n+1}} - \frac{1}{2^{n+2}} = \frac{1}{2^{n+2}}$$

$$n+1 \leq \frac{4^{n+1}}{2^{n+2}} = 2^{2(n+1)-(n+2)} = 2^n$$

Es. 4 $p(n) =$ "$n > 500$"

② è verificata: se $n > 500$ anche $n+1 > 500$

① non è verificata $0 \not> 500$

INDUZIONE FORTE

Sia q una proposizione che parla di un numero naturale n

$$J \begin{cases} ① \ q(0) \text{ è vera} \\ ②' \ \forall n \in \mathbb{N} \ \left(\text{Se } \forall k \leq n \ \ q(k) \text{ è vera, allora } q(n+1) \text{ è vera} \right) \end{cases}$$

Nelle ipotesi J, $q(n)$ è vera $\forall n \in \mathbb{N}$

Dim. Sia $p(n)$ la proposizione

$p(n) =$ "$\forall k \leq n$, $q(k)$ è vera"

p soddisfa ① perché q soddisfa ①

P.B. $p(0) =$ " $\forall k \leq 0$, $q(k)$ è vera"

P.I. $p(n) \overset{?}{\Longrightarrow} p(n+1)$

$p(n) \Rightarrow q(n+1)$ per ②'

Sappiamo allora che $\forall k \leq n$, $q(k)$ è vera, e in più $q(n+1)$ è vera

Dunque $p(n+1)$ è vera

Per induzione semplice $p(n)$ è vera $\forall n$

$p(n)$ dice che $\forall k \leq n$, e in particolare per $k = n$
$q(k)$ è vera

$p(n) \Rightarrow q(n)$ $\forall n \in \mathbb{N}$

Esempio 5

Sia $(a_n)_{n \in \mathbb{N}}$ una successione di naturali

$a_0, a_1, a_2, \ldots$

Sappiamo che $a_0 = 1$ e che $\forall n \in \mathbb{N}$ $a_n < a_{n+1} \leq 2a_n$

Allora ogni naturale M si può scrivere come somma di alcuni a_k tutti distinti.

$a_n = n+1$ verifica le ipotesi

$a_n = 2^n$ //

$a_n \doteq F_n$

Dim. per induzione forte

P.B. $M = 0$ $\quad 0$ è la somma senza addendi

P.I. Supponiamo la tesi per $0, \dots, M$ e la dimostriamo per $M+1$

1° oss. $M+1 \geq 1 = a_0$

$\exists\, k$ t.c. $a_k \leq M+1$

Per k abbastanza grande $a_k > M+1$

Sia $\bar{k}$ il massimo naturale k t.c. $a_k \leq M+1$

$a_{\bar{k}} \geq 1$ perché tutti gli el. della succ. lo sono (dimostratelo per induzione)

$0 \leq M+1 - a_{\bar{k}} < M+1$

Posso usare l'ipotesi induttiva sul naturale $M+1 - a_{\bar{k}}$

$M+1 - a_{\bar{k}} = a_{i_1} + a_{i_2} + \dots + a_{i_h}$ con i_j tutti distinti (ip. induttiva)

$M+1 = a_{i_1} + \dots + a_{i_h} + a_{\bar{k}}$

Resta da verificare che $i_j \neq \bar{k}$

$M+1 < a_{\bar{k}+1} \leq 2a_{\bar{k}}$ $\qquad M+1 - a_{\bar{k}} < a_{\bar{k}}$

Se $a_{i_j} = a_{\bar{k}}$ allora $M+1 - a_{\bar{k}} = a_{i_1} + \dots + a_{i_h} \geq a_{i_j} = a_{\bar{k}}$ assurdo

PIGEONHOLE Sia $n \geq 1$ un naturale
Abbiamo $n+1$ scarpe e le riponiamo in n cassetti. Allora esiste almeno un cassetto contenente almeno 2 scarpe.

PIGEONHOLE 2 $n, k \geq 1$ naturali
Se ho $nk+1$ scarpe e le colloco in n cassetti, almeno un cassetto contiene almeno $k+1$ scarpe.

Es. 6 A una festa partecipano n persone, alcune coppie delle quali si conoscono.
Esistono 2 persone con lo stesso numero di conoscenze.

Quante persone può conoscere una persona?
$0, 1, \dots, n-1$

Consideriamo i seguenti cassetti
C_0 contiene le persone che non conoscono nessuno o conoscono tutti

C_i (con $1 \leq i \leq n-2$) contiene le persone che hanno i conoscenze

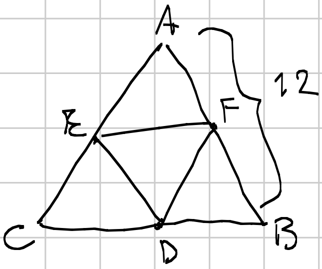
Allora C_0 contiene 2 persone oppure un altro C_i contiene 2 persone
Se C_i contiene 2 persone, queste conoscono i persone ognuna

Se C_0 contiene 2 persone, non possono essere di tipo diverso

Esempio 7

T_ℓ un triangolo equilatero di lato ℓ.

Qual è il minimo a per cui si può ricoprire un T_{12} con 5 T_a?



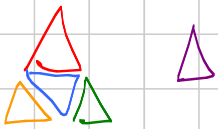
Abbiamo segnato 6 punti, dunque per ogni ricoprimento con 5 T_a c'è un T_a che copre 2 dei 6 punti.

$\forall x, y \in \{A, B, C, D, E, F\} \quad \overline{XY} \geq 6$

Se x, y sono ricoperti da un T_a, $\overline{XY} \leq a$

$a \geq 6$ usando una coppia di punti x, y come sappiamo esistere.

$a = 6$ basta (basterebbero anche 4 triangoli)

 è un ricoprimento

Esempio 8 Trovare il più piccolo naturale n con questa proprietà

"Comunque si prendano n numeri naturali ≥ 1 le cui scomposizioni in fattori primi contengano solo primi < 30, ce ne sono 2 il cui prodotto è un $\square$"

I primi < 30 sono 10

Sia $K = 2^{a_2} \cdot 3^{a_3} \cdot \ldots \cdot 29^{a_{29}}$ con $a_p \geq 0$

$h = 2^{b_2} \cdot \ldots \cdot 29^{b_{29}}$ $\quad b_p \geq 0$

$$K h = 2^{a_2+b_2} \cdot \ldots \cdot 29^{a_{29}+b_{29}}$$

Quando Kh è un $\square$? Quando $a_p + b_p$ è pari per $p = 2, 3, \ldots, 29$

$n = 2^{10}+1$ funziona

Associo al numero K la seguente 10-upla

$$\left([a_2]_{\bmod 2}, [a_3]_{\bmod 2}, \ldots, [a_{29}]_{\bmod 2}\right)$$

Le possibili 10-uple sono 2^{10}

Se $n = 2^{10}+1$ esistono K, h con la stessa sequenza

Se $n \leq 2^{10}$ considero

l'insieme S dei naturali della forma

$$2^{c_2} \cdot 3^{c_3} \cdot \ldots \cdot 29^{c_{29}} \quad \text{con } c_p = 0 \text{ oppure } 1$$

$|S| = 2^{10}$ e quindi posso prendere un sottoinsieme di n elementi di S, se $n \leq 2^{10}$

Esempio 9 (USAMO 1990/1)

Uno stato deve produrre targhe per automobili. Le targhe sono composte da 6 cifre decimali. La legge vuole che due targhe differiscano in almeno 2 posizioni. Quante targhe è possibile emettere?

Supponiamo di avere targhe con 2 cifre decimali

Allora posso avere al più 10 targhe.
Se ne avessi 11, per PIGEONHOLE 2 di esse coinciderebbero nella prima cifra, dunque avrebbero al più una cifra diversa (la seconda)

Se le targhe hanno 3 cifre

Se ho 101 targhe, $101 = 10 \cdot 10 + 1$
dunque ci sono 11 targhe con la prima cifra uguale, e fra queste ce ne sono 2 con anche la seconda cifra uguale. Dunque non si possono emettere 101 targhe.

In generale dimostriamo, per induzione su $n \geq 2$ che se le targhe hanno n cifre non possono essere più di 10^{n-1}.

P.B. $n=2$ già visto

P.I. Se ho più di 10^n targhe con $n+1$ cifre, dunque almeno $10^n + 1$, ce ne sono almeno $10^{n-1} + 1$ che coincidono sulla prima cifra.
Per ipotesi induttiva fra queste ce ne sono 2 che coincidono ovunque tranne che sull'ultima cifra

---

Dunque se le targhe hanno n cifre, se ne possono produrre non più 10^{n-1}.

Esibiamo 10^{n-1} targhe che rispettano la legge

Prendiamo tutte le targhe $(a_1, \dots, a_n)$ tali che $a_1 + \dots + a_n$ sia divisibile per 10.

$$a_1 + \dots + a_n \equiv 0 \pmod{10}$$

1) Queste targhe sono 10^{n-1}. Infatti per costruire una targa scelgo a piacere le prime $n-1$ cifre, a quel punto l'ultima è determinata.

2) Due di queste targhe non coincidono in almeno due posizioni

$$(a_1, \dots, a_n) \qquad (b_1, \dots, b_n)$$

Per assurdo le due targhe in esattamente una posizione j

$$a_i = b_i \quad \forall i \neq j$$
$$a_j \neq b_j$$

$$\sum_{i=1}^{n} a_i - \sum_{i=1}^{n} b_i \text{ è un multiplo di } 10$$

$$\parallel$$

$$a_j - b_j \text{ non è un multiplo di } 10$$

$$a_j - b_j \neq 0 \qquad -9 \leq a_j - b_j \leq 9$$

$$\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod{10}$$

$$a_j \equiv b_j \pmod{10}$$

Dunque le 10^{n-1} targhe scelte rispettano la legge.

A1 BASIC Numeri complessi e polinomi – Maria –

Titolo nota 04/09/2012

Numeri complessi

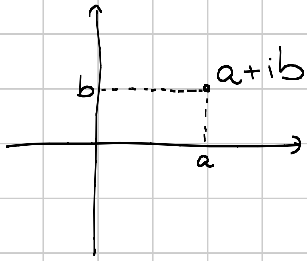
$\mathbb{C} = \{a+ib : a, b \in \mathbb{R}\}$

i è un segnaposto

Dato $z \in \mathbb{C}$, $z = a+ib$, diciamo $a = \operatorname{Re} z$ $b = \operatorname{Im} z$.

Piano di Gauss

Associamo ad $a+ib$ il punto (a,b).



$z \in \mathbb{R} \iff \operatorname{Im} z = 0 \iff z$ sta sull'asse x.

Operazioni

Somma: $a+ib + c+id = (a+c) + i(b+d)$

Prodotto: $\boxed{i^2 = -1}$.

$$(a+ib)(c+id) = ac + ibc + iad + i^2bd$$
$$= ac - bd + i(bc+ad).$$

Divisione: $\dfrac{a+ib}{c+id} = \dfrac{a+ib}{c+id} \cdot \dfrac{c-id}{c-id} = \dfrac{(ac+bd)+i(bc-ad)}{c^2-(id)^2}$

$$= \frac{ac+bd+i(bc-ad)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + i\,\frac{bc-ad}{c^2+d^2}$$

È ben definito $c+id \neq 0$ (0 è $0+i\cdot 0$)

Coniugio $\overline{a+ib} = a-ib$

Modulo $|a+ib| = \sqrt{a^2+b^2}$

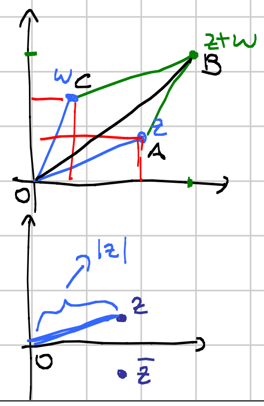
Operazioni nel piano di Gauss

Somma: regola del parallelogramma

Prodotto e divisione: dopo

Coniugio: simmetria rispetto all'asse x

Modulo: distanza dall'origine.



Oss: $|z+w| \le |z|+|w|$

$|z+w| = \overline{OB} \le \overline{OA} + \overline{AB} = \overline{OA} + \overline{OC} = |z|+|w|$.

disuguaglianza triangolare

Proprietà: ① $z\bar{z} = |z|^2$

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

② $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$

③ $\overline{z+w} = \bar{z} + \bar{w}$ $\qquad \overline{z\cdot w} = \bar{z}\cdot\bar{w}$ $\qquad \overline{\left(\frac{z}{w}\right)} = \frac{\bar{z}}{\bar{w}}$.

④ $|z\cdot w| = |z|\cdot|w|$

$z = a+ib \qquad w = c+id$

$(a+ib)(c+id) = (ac-bd) + i(bc+ad)$

$|z\cdot w|^2 = |z|^2 |w|^2$

$(ac-bd)^2 + (bc-ad)^2 \underset{(ex)}{=} (a^2+b^2)\cdot(c^2+d^2)$.

Oss: possiamo generare terne pitagoriche

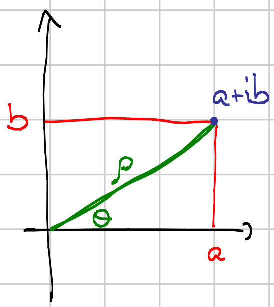
$a^2+b^2 = c^2 \qquad d^2+e^2 = f^2$

$(a^2+b^2)(d^2+e^2) = c^2f^2$

$(ac-bd)^2 + (bc-ad)^2$

L'insieme dei numeri della forma a^2+b^2 $\quad a,b \in \mathbb{N}$ è chiuso rispetto al prodotto.

Forma trigonometrica



Individuo z mediante

- ρ = distanza dall'origine
- θ = angolo col semiasse positivo delle ascisse.

Forma trigonometrica $\longleftrightarrow$ cartesiana

$$\begin{cases} a = \rho\cos\theta \\ b = \rho\sin\theta \end{cases} \qquad \begin{cases} \rho = \sqrt{a^2+b^2} \\ \theta \approx \operatorname{arctg}\frac{b}{a} \end{cases}$$

$$\boxed{z = \rho(\cos\theta + i\sin\theta)}$$

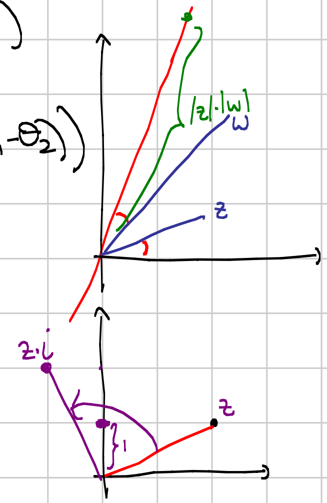
Forma trigonometrica e prodotto

$z = \rho_1 (\cos\theta_1 + i \sin\theta_1)$

$\omega = \rho_2 (\cos\theta_2 + i \sin\theta_2)$

$z \cdot \omega = \rho_1 \rho_2 (\cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2 + i \sin\theta_1 \cos\theta_2 + i \sin\theta_2 \cos\theta_1)$

$= \rho_1 \rho_2 (\cos(\theta_1+\theta_2) + i \sin(\theta_1+\theta_2))$



Analogamente $\frac{z}{\omega} = \frac{\rho_1}{\rho_2} (\cos(\theta_1-\theta_2) + i \sin(\theta_1-\theta_2))$

Es: cosa significa moltiplicare per i?
Ruotare di $90°$

Notazione: $\cos\theta + i\sin\theta = e^{i\theta}$

$e^{i\theta} \cdot e^{i\varphi} = e^{i(\theta+\varphi)}$.

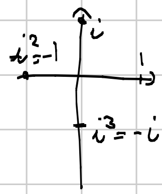
$(e^{i\theta})^{-1} = e^{-i\theta}$

Esempio: $-1 = e^{i\pi}$.

Es: $[\rho(\cos\theta + i\sin\theta)]^2 = \rho^2 [\cos 2\theta + i \sin 2\theta]$

In generale

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



Es: $\cos 4\theta = \mathrm{Re}\, [\cos 4\theta + i \sin 4\theta]$

$= \mathrm{Re}\, [(\cos\theta + i\sin\theta)^4]$

$= \mathrm{Re}\, [\cos^4\theta + 4 i \sin\theta \cos^3\theta + 6 i^2 \sin^2\theta \cos^2\theta + 4 i^3 \sin^3\theta \cos\theta + i^4 \sin^4\theta]$

$= \cos^4\theta - 6 \sin^2\theta \cos^2\theta + \sin^4\theta$

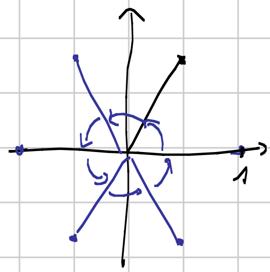
Es: $z = \frac{1}{2} + i \frac{\sqrt{3}}{2}$. Allora $z^6 = 1$

1° modo: svolgo la moltiplicazione.

2° modo: $|z| = 1$ $\quad \theta = \frac{\pi}{3}$

$z^6 = (\cos \frac{\pi}{3} + i \sin \frac{\pi}{3})^6 = \cos 2\pi + i \sin 2\pi = 1$

3° modo: graficamente



Es: $z = 1 + \sqrt{3}i$. $\quad z^{2012} = ?$

$z^{2012} = 2^{2012} (\cos \frac{\pi}{3} + i \sin \frac{\pi}{3})^{2012}$

$$= 2^{2012}\left(\cos\tfrac{\pi}{3} + i\sin\tfrac{\pi}{3}\right)^{6\cdot 335+2}$$
$$= 2^{2012}\left[\left(\cos\tfrac{\pi}{3} + i\sin\tfrac{\pi}{3}\right)^{6}\right]^{335}\cdot\left(\cos\tfrac{\pi}{3} + i\sin\tfrac{\pi}{3}\right)^{2}$$
$$= 2^{2012}\left(\cos\tfrac{2\pi}{3} + i\sin\tfrac{2\pi}{3}\right)$$
$$= 2^{2012}\left(-\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}\right)$$
$$= -2^{2011} + i\sqrt{3}\,2^{2011}$$

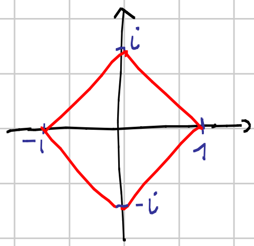
Radici di un numero complesso

Dato $a \in \mathbb{C}$, trovare $z \in \mathbb{C}$ $z^n = a$.

Es: se $a = 0 \Rightarrow z = 0$

Es: $z^4 = 1$ $\quad 1, -1, i, -i$ sono radici

$\quad i^4 \quad i^2 \quad i \quad i^3$



$$z^4 - 1 = (z-1)(z+1)(z-i)(z+i)$$

Verifica: $(z-1)(z+1)(z-i)(z+i) = (z^2-1)(z^2+1) = z^4 - 1$.

Teorema se $a \neq 0$. Allora esistono n numeri complessi t.c. $z^n = a$ e nel piano di Gauss sono i vertici di un poligono regolare con n lati centrato nell'origine.

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

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

Devono avere lo stesso modulo $\begin{cases}\rho = r^n \\ \theta = n\varphi + 2k\pi \quad k \in \mathbb{Z}.\end{cases}$

" " " " angolo

a meno di 2π

$$\begin{cases} r = \sqrt[n]{\rho} & (\sqrt{\ } \text{ dei numeri reali}) \\ \varphi = \dfrac{\theta - 2k\pi}{n} & k \in \mathbb{Z}? \text{ basta prendere } k = 0, \ldots, n-1 \end{cases}$$

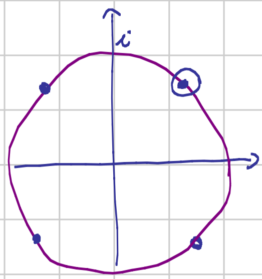
Esempio: $z^4 = -1$

$n = 4 \quad \rho = 1 \quad \theta = \pi$

$\pm\frac{1}{\sqrt{2}} \pm i\frac{1}{\sqrt{2}} = \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right)$, $\quad \cos -\frac{\pi}{4} + i\sin -\frac{\pi}{4} = \cos\frac{7}{4}\pi + i\sin\frac{7}{4}\pi$

$\cos\left(-\frac{3}{4}\pi\right) + i\sin\left(-\frac{3}{4}\pi\right) = \cos\frac{5}{4}\pi + i\sin\frac{5}{4}\pi$

$\cos\left(-\frac{5}{4}\pi\right) + i\sin\left(-\frac{5}{4}\pi\right) = \cos\frac{3}{4}\pi + i\sin\frac{3}{4}\pi$



2° modo: $\frac{1+i}{\sqrt{2}}$ funziona.

Polinomi

$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$

$a_0, \dots, a_n \in \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono detti coefficienti.

$n = \deg(p(x))$ è il grado.

Diciamo che p è monico se $a_n = 1$.

Possiamo sommare, moltiplicarli, fare la divisione col resto: dati $p(x), q(x)$ polinomi, esistono unici $a(x)$ e $r(x)$ t.c.

$$p(x) = a(x) \cdot q(x) + r(x) \qquad \text{con } \deg r(x) < \deg q(x)$$

Si dimostra per induzione su $\deg p$.

Esempio:

$$\begin{array}{rrrrr|l} x^4 & -x^3 & +3x^2 & -2x & +1 & x^2+x+1 \\ \hline -x^4 & -x^3 & -x^2 & & & x^2-2x+4 \\ \hline & -2x^3 & +2x^2 & -2x & +1 & \\ & +2x^3 & +2x^2 & +2x & & \\ \hline & & 4x^2 & +0 & +1 & \\ & & -4x^2 & -4x & -4 & \\ \hline & & & -4x & -3 & \end{array}$$

$$x^4 - x^3 + 3x^2 - 2x + 1 = (x^2+x+1)(x^2-2x+4) - 4x - 3$$

Possiamo fare la divisione con $q(x) = x - a$

$$p(x) = q(x)(x-a) + r\cancel{(x)} \qquad \underset{\substack{\shortparallel \\ 0}}{\deg r(x)} < 1 \;\Rightarrow\; r(x) \text{ è costante}$$

Chi è r? Valuto il polinomio in $x = a$

$$p(a) = r.$$

Abbiamo ottenuto il

Teorema di Ruffini: $p(x) = q(x)(x-a) + p(a)$.

Corollario: se a è una radice di $p(x)$ (ovvero $p(a) = 0$) allora $p(x) = q(x)(x-a)$.

Corollario: un polinomio di grado n ha al più n radici $x_1, \dots, x_n$.

Supponiamo per assurdo che ne abbia $n+1$: $x_1, \dots, x_{n+1}$

$p(x) = (x - x_1)\, q(x)$.

Valuto x_i $\quad 0=p(x_i)=(x_i-x_1)\,q(x_i) \Rightarrow q(x_i)=0$

$\Rightarrow q(x)=(x-x_2)\,r(x)\dots$

$p(x)=(x-x_1)\,q(x)=(x-x_1)(x-x_2)\,r(x)$ ___

$\qquad = (x-x_1)\dots(x-x_{n+1})\,s(x)$.

Ma allora il RHS ha grado $\geq n+1$ oppure è $\equiv 0$, assurdo.

Possiamo pensare a un polinomio come $x \to p(x)$. Chiamiamo funzione polinomiale.

È chiaro che se $p=q$ come polinomi, allora

$$p(x)=q(x) \quad \forall x$$

(cioè sono $=$ come funzioni polinomiali).

Principio di identità dei polinomi

Se esistono $n+1$ ($\geq \deg p,q$) valori su cui $p(x)$ e $q(x)$ coincidono, allora $p=q$ come polinomi (ovvero hanno gli stessi coefficienti).

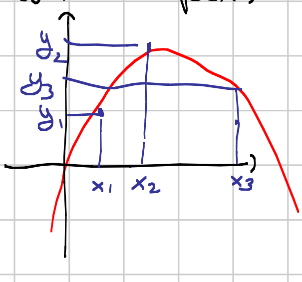
Siano $x_1, \dots, x_{n+1}$ t.c. $p(x_i)=q(x_i)$.

Considero $p(x)-q(x)$. Ha $n+1$ radici (gli x_i).

$\Rightarrow$ per il corollario $p(x)-q(x)$ è il polinomio $\equiv 0$.

Costruire un polinomio di grado n assegnati $n+1$ valori

Date $n+1$ coppie (x_i, y_i), esiste un unico polinomio $p(x)$ di grado $\leq n$ t.c. $p(x_i)=y_i$ $\forall i=1,\dots,n+1$.



Dim:

Unicità: segue dal principio di identità.

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

$$\begin{cases} a_n x_1^n + \dots + a_0 = y_1 \\ a_n x_2^n + \dots + a_0 = y_2 \\ \vdots \end{cases}$$

$$\begin{pmatrix} x_1^n & x_1^{n-1} & \dots & x_1 & 1 \\ x_2^n & x_2^{n-1} & \dots & x_2 & 1 \\ \vdots & & & & \end{pmatrix}$$

È un sistema di $n+1$ equazioni lineari in $n+1$ incognite.

In questo caso il sistema ha sempre un'unica soluzione (ma non è banale vederlo).

Nuova strategia:

- $y_1 = \dots = y_{n+1} = 0 \longrightarrow p(x) \equiv 0$
- $y_1 = \dots = y_n = 0 \quad y_{n+1} = 1$

  $p(x)$ ha n radici $x_1, \to x_n$

  $$p(x) = (x-x_1)(x-x_2)\dots(x-x_n)\cdot r$$

  è un numero perchè vogliamo $\deg p \leq n$

  Scegliamo r per verificare $p(x_{n+1}) = 1$:

  $$(x_{n+1}-x_1)(x_{n+1}-x_2)\dots(x_{n+1}-x_n)\cdot r = 1$$

  Scegliamo $r = \dfrac{1}{(x_{n+1}-x_1)\dots(x_{n+1}-x_n)}$.

  Chiamiamo $p_i(x) = \dfrac{\prod_{j\neq i}(x-x_j)}{\prod_{j\neq i}(x_i-x_j)}$. $p_i(x)$ vale 1 in x_i e 0 negli altri x_j, $j \neq i$.

- caso generale:

  $$p(x) = \sum_{i=1}^{n+1} y_i\, p_i(x)$$

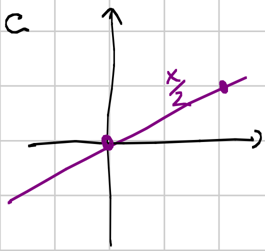
  Funziona:

  $$p(x_k) = y_1 p_1(x_k) + y_2 p_2(x_k) \dots + y_{n+1} p_{n+1}(x_k)$$
  $$= y_k\, p_k(x_k) = y_k.$$

Oss: la possibilità di assegnare $n+1$ valori vale in $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, ma non in $\mathbb{Z}$.

Es: non esiste un poli di grado ≤ 1 con coeff in $\mathbb{Z}$ t.c

$p(0) = 0 \qquad p(2) = 1$



Polinomi a coeff complessi

Teorema (difficile): $p(x)$ a coeff complessi, $\deg p(x) \geq 1$
$\Rightarrow$ $p(x)$ ha (almeno!) una radice in $\mathbb{C}$.

Corollario (teorema fondamentale dell'algebra)
$p(x)$ polinomio a coeff complessi
Allora esistono $\lambda_1, \dots, \lambda_n$ t.c.

$$p(x) = a_n (x-\lambda_1) \dots (x-\lambda_n).$$

Dim:
Per induzione su $n = \deg p$.
Se p ha grado 1 ovvio.
$n \to n+1$. Per il teo precedente $p(x)$ (con $\deg p(x) = n+1$) ha una radice $\lambda_{n+1} \Rightarrow$

$$p(x) = (x-\lambda_{n+1})\, q(x). \quad (*)$$

$\Rightarrow$ q ha grado n e per hp induttiva

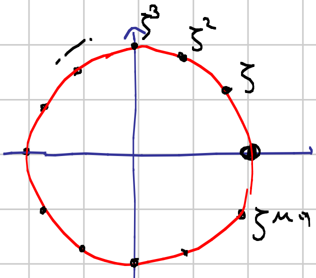
$$q(x) = a_n (x-\lambda_1) \dots (x-\lambda_n)$$

Sostituendo in $(*)$, ottengo

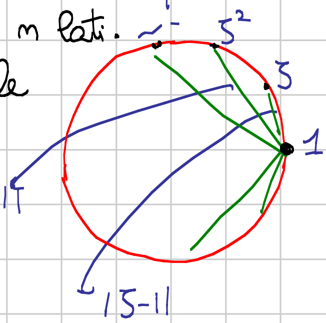
$$p(x) = a_n (x-\lambda_1) \dots (x-\lambda_n)(x-\lambda_{n+1}).$$

Es: $x^n - 1 = 1 \cdot (x-\zeta)(x-\zeta^2) \dots (x-\zeta^{n-1})(x-1)$

non c'è coeff perché il polinomio è monico



Esercizio: consideriamo un poligono regolare di n lati.
Vogliamo calcolare il prodotto dei lati e delle diagonali uscenti da un vertice fissato.



Vogliamo $\prod_{k=1}^{n-1} |\zeta^k - 1|$

$$= \left| \prod_{k=1}^{n-1} (\zeta^k - 1) \right| = |p(1)| = n.$$

Consideriamo $p(x) = \prod_{k=1}^{n-1}(x-\zeta^k) \overset{\text{esempio precedente}}{=} \dfrac{x^n - 1}{x-1} = x^{n-1} + x^{n-2} + \dots + x + 1$

$|p(1)| = n$.

Polinomi a coefficienti reali

Un polinomio a coeff reali si scrive sempre come prodotto

- fattori di grado 1
- fattori di grado 2 con $\Delta < 0$.

Dim:

Nella fattorizzazione in $\mathbb{C}$ ci sono alcune radici reali e radici "veramente" complesse.

Oss: $\lambda \in \mathbb{C}$ è radice, ovvero $p(\lambda) = 0 \Rightarrow \bar{\lambda}$ è radice.

$$a_n \lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_0 = 0$$

$$\overline{a_n}\,\bar{\lambda}^n + \overline{a_{n-1}}\,\bar{\lambda}^{n-1} + \ldots + \overline{a_0} = 0$$

$$a_n \bar{\lambda}^n + a_{n-1}\bar{\lambda}^{n-1} + \ldots + a_0 = 0 \iff p(\bar{\lambda}) = 0.$$

Nella fattorizzazione in $\mathbb{C}$ c'è $(x-\lambda)(x-\bar{\lambda})$

È un poli di grado 2 a coeff reali

$$x^2 - \underbrace{(\lambda+\bar{\lambda})}_{\in\mathbb{R}} x + \underbrace{\lambda\bar{\lambda}}_{=|\lambda|^2 \in \mathbb{R}}$$

Oppure $\lambda = a + ib$

$$(x-a-ib)(x-a+ib) = (x-a)^2 + b^2$$

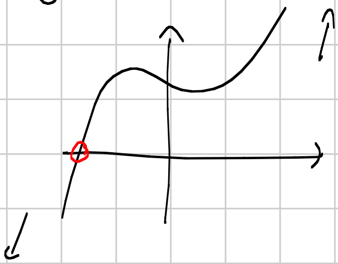
Oss: Un polinomio a coeff reali di grado dispari ha sempre una radice reale.

Idea: le radici complesse "vanno a coppie".

Oss: un polinomio ha lo stesso comportamento a $\pm\infty$ del suo termine di grado massimo

Es $x^{100} - 257x^{20} + x - 1$

Es $x^3 - 2x + 7$



Esercizio: Trovare tutti i poli a coeff reali $p(x)$ di grado dispari t.c.

$$p(x^2+1) = p(x)^2 + 1 \quad \forall x \in \mathbb{R}.$$

$p(x) = x$ funziona: $x^2+1 = x^2+1$

$p(x) = c$? $\quad c = c^2+1 \iff c^2-c+1=0$ non ha sol reali.

Sappiamo che un poli di grado dispari si annulla sempre.

Supponiamo che esista $a \in \mathbb{R}$ t.c $p(a) = a$.

(esiste, perché $p(x)-x$ ha grado dispari $\Rightarrow$ ha una radice).

Sostituendo $x = a$ $\quad p(a^2+1) = a^2+1$

Sostituendo a^2+1 $\quad p((a^2+1)^2+1) = (a^2+1)^2+1$. ....

$a < a^2+1 < (a^2+1)^2+1 < \dots$ risolvono

$$p(x) = x, \text{ ovvero } p(x)-x=0$$

Ma allora, visto che $p(x)-x$ ha un numero finito di radici oppure è nullo, $p(x)-x \equiv 0$.

<u>Polinomi a coefficienti interi</u>

<u>Teorema delle radici razionali</u>

$p(x)$ a coeff interi $p(x) = a_n x^n + \dots + a_0$.

Allora se q/r è una radice, $q \mid a_0$ e $r \mid a_n$

$\hookrightarrow$ ridotta ai min termini.

Sostituiamo

$$r^n \left(a_n \frac{q^n}{r^n} + a_{n-1} \frac{q^{n-1}}{r^{n-1}} + \dots + a_0 \right) = 0$$

$$a_n q^n + a_{n-1} q^{n-1} r + \dots + a_1 q r^{n-1} + a_0 r^n = 0$$

q divide tutti i primi n addendi $\Rightarrow q \mid a_0 r^n$.

Ma $(q, r) = 1$.

Lo stesso per r.

<u>Es</u>: x^3+x+1 è riducibile come poli a coeff in $\mathbb{Z}$?

No!

Se fosse riducibile, avrebbe un fattore di grado 1, cioè una radice.

Ma per il teo precedente le radici razionali possono essere solo ± 1. Verificando, non funzionano.

Esercizio: $p(x)$ a coeff interi. $p(1)=1$ e $p(7)=7$

Mostrare che $p(4) \equiv 4 \ (9)$.

1° modo: Ruffini

$$p(x) = (x-1)\, q(x) + 1 \qquad (\bullet)$$

$$7 = p(7) = 6\, q(7) + 1 \Rightarrow q(7) = 1$$

$$\Rightarrow q(x) = (x-7)\, r(x) + 1$$

Quindi da $(\bullet)$ $p(x) = (x-1)\left[(x-7)\, r(x) + 1\right] + 1$

$= (x-1)(x-7)\, r(x) + x$

Valuto in $x=4$ $p(4) = 3 \cdot (-3)\, r(4) + 4$

$= -9\, r(x) + 4$

2° modo: consideriamo $q(x) = p(x) - x$

$q(x)$ si annulla in 1 e 7 $\Rightarrow q(x) = (x-1)(x-7)\, r(x)$

...

Esercizio esiste $p(x)$ a coeff interi t.c. $p(8)=8$ $p(15)=15$

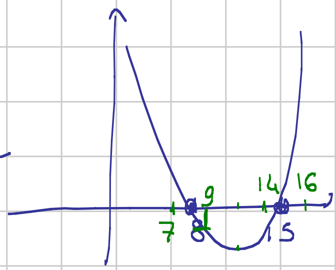
Trovare il min $a>0$ t.c. $p(x)=x+a$ ha una sol intera

$$p(x) - x = (x-8)(x-15)\, r(x) = a$$

vogliamo che esista una sol intera.

Mi conviene prendere $r(x) = \pm 1$

Vogliamo il pto a coordinate intere con ordinata + piccola che sta sulla parabola.



$$(7-8)(7-15)(\pm 1) = 8 = a$$

$$(9-8)(9-15)(\pm 1) = \boxed{6 = a}$$

$$(14-8)(14-15)(\pm 1) = 6 = a$$

$$(16-8)(16-15)(\pm 1) = 8 = a$$

Oss: $a-b \mid a^n-b^n$ $(*)$ $a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\_\_ +ab^{n-2}+b^{n-1})$

$a+b \mid a^n+b^n$ se n è dispari.

Metto $-b$ nella precedente

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

↑ uso n dispari

Lemma: $p(x)$ a coeff interi.

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

[$(*)$ si ottiene con $p(x)=x^n$]

Dim 1:

Per Ruffini: $p(x)=(x-a)\,q(x)+p(a)$.

Valuto in b: $p(b)=(b-a)\,q(b)+p(a)$.

Dim 2:

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

$p(b)-p(a)=a_n(b^n-a^n)+a_{n-1}(b^{n-1}-a^{n-1})+\_\_+a_1(b-a)$

$a-b$ divide ogni addendo per l'oss.

Lemma [IMO 2006]

$p(x)$ a coeff interi. $p^{(k)}(x)=\underbrace{p(p\dots p(x)\dots))}_{k\text{ volte}}$

Supponiamo che $p^{(k)}(a)=a$ per un certo $a\in\mathbb{Z}$.

Allora $p^{(2)}(a)=a$.

Usiamo il lemma con $b=p(a)$

$p(a)-a \mid p(p(a))-p(a) \mid p^{(3)}(a)-p^{(2)}(a) \mid \dots$

$\mid \dots \mid p^{(k)}(a)-p^{(k-1)}(a) \mid p^{(k+1)}(a)-p^{(k)}(a)=p(a)-a$

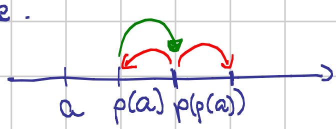
Sono tutti $=$ a meno del segno.

$\cancel{p(a)}-a=-p(p(a))+\cancel{p(a)} \Rightarrow$ tesi.

$p(a)-a=p(p(a))-p(a)$

Vediamo che il 2° caso è impossibile.

Ci sono 2 casi:



$p^{(3)}(a)-\cancel{p^{(2)}(a)}=-\cancel{p^{(2)}(a)}+p(a)$ oppure

$p^{(3)}(a)-p^{(2)}(a)=p^{(2)}(a)-p(a)=p(a)-a$

Sappiamo che $p^{(n)}(a) = a$.
Per tornare ad a, la successione $p^{(i)}(a)$ deve andare su $p(a)$. Ma da $p(a)$ si va a $p(p(a))$, non ad a! Assurdo.

Relazioni radici-coefficienti

$p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$.
Siano $\lambda_1, \dots, \lambda_n$ le radici $\in \mathbb{C}$ (eventualmente ripetute).
Allora:

$$-a_{n-1} = \lambda_1 + \dots + \lambda_n = \sum_{1 \leq i \leq n} \lambda_i$$

$$a_{n-2} = \sum_{1 \leq i < j \leq n} \lambda_i \lambda_j$$

$$-a_{n-3} = \sum_{1 \leq i < j < k \leq n} \lambda_i \lambda_j \lambda_k$$

$$\vdots$$

$$(-1)^n a_0 = \lambda_1 \cdots \lambda_n.$$

$$p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 = (x-\lambda_1)(x-\lambda_2)\dots(x-\lambda_n)$$

$$= x^n - x^{n-1}(\lambda_1 + \dots + \lambda_n) + x^{n-2}\left(\sum \lambda_i \lambda_j\right) + \dots + (-1)^n \lambda_1 \dots \lambda_n$$

Esempio: $2x^3 + 6x + 6$.
Non è monico. Considero $x^3 + 3x + 3$

$\lambda_1 + \lambda_2 + \lambda_3 = 0$
$\lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3 = 3$
$\lambda_1\lambda_2\lambda_3 = -3$

$$\lambda_1^2+\lambda_2^2+\lambda_3^2 = (\lambda_1+\lambda_2+\lambda_3)^2 - 2(\lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_2\lambda_3)$$
$$= -6$$

$\Rightarrow$ il polinomio ha 2 radici complesse

Oss: $p(\lambda)=0 \Rightarrow \frac{1}{\lambda}$ è radice di $a_0x^n+a_1x^{n-1}+\dots+a_n=0$

$$a_n\lambda^n + a_{n-1}\lambda^{n-1}+\dots+a_0=0$$

Divido per λ^n $\quad a_n + a_{n-1}\frac{1}{\lambda}+\dots+a_0\frac{1}{\lambda^n}=0$

Oss: $\frac{1}{\lambda_1}+\frac{1}{\lambda_2}+\dots+\frac{1}{\lambda_n} = -\frac{a_1}{a_0}$

1° modo: $\dfrac{\lambda_2\lambda_3\dots\lambda_n+\lambda_1\lambda_3\dots\lambda_n+\dots}{\lambda_1\dots\lambda_n}$

$$= \frac{(-1)^{n-1}a_1}{(-1)^n a_0} = -\frac{a_1}{a_0}$$

2° modo: $\frac{1}{\lambda_i}$ sono radici $\dfrac{a_0x^n+\dots+a_n}{a_0}=0$

$\Rightarrow$ la somma delle radici è $-\frac{a_1}{a_0}$.

Torniamo a coeff in $\mathbb{Z}$.

Criteri di irriducibilità

Criterio di Eisenstein

$f(x)$ a coeff interi. p primo

$$p\nmid a_n \qquad p\mid a_0,\dots,a_{n-1} \qquad p^2\nmid a_0.$$

Allora $p(x)$ è irriducibile tra i poli a coeff interi.

Supponiamo per assurdo

$$a_nx^n+\dots+a_0 = (b_kx^k+b_{k-1}x^{k-1}+\dots+b_0)(c_\ell x^\ell+\dots+c_0)$$

$p\mid a_0=b_0c_0$.

Esattamente uno tra b_0 e c_0 è divisibile per p.

Wlog, $p\mid b_0$ $\quad p\nmid c_0$.

$p \mid a_1 = b_0 c_1 + b_1 c_0 \Rightarrow p \mid b_1.$

$p \mid a_2 = b_2 c_0 + b_1 c_1 + b_0 c_2 \Rightarrow p \mid b_2$

$\vdots \qquad \vdots$

$p \mid b_k$

$p \nmid a_m = b_k c_\ell$ ma questo è divisibile per p.

Esercizio: $x^{p-1} + x^{p-2} + \ldots + x + 1$ è irriducibile in $\mathbb{Z}$.

È $\frac{x^p - 1}{x-1} = P(x)$. $p(x)$ è irriducibile $\Leftrightarrow p(x+1)$ è irriducibile

Vediamo che $P(x+1)$ è irriducibile.

$$P(x+1) = \frac{(x+1)^p - 1}{x+\cancel{1}-\cancel{1}} = \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \ldots + px + \cancel{1} - \cancel{1}}{x}$$

$$= x^{p-1} + \binom{p}{1}x^{p-2} + \ldots + p$$

Siamo nelle hp di Eisenstein: $p \mid \binom{p}{i}$ $\forall i \neq 0, p$.

$\boxed{4 \nmid \binom{4}{2} = 6}$

A2 - BASIC : disuguaglianze

Titolo nota 06/09/2012

§1 Medie

§2 Cauchy-Schwartz

§3 Riarrangiamento

§4 Convessità

§1 Medie

$A((x_i)) \quad (x_i) = (x_1, \dots, x_n)$

× rapidità

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

media aritmetica

$$G(x_1, \dots, x_n) = \sqrt[n]{x_1 \cdot \dots \cdot x_n} \qquad x_i \geq 0$$

media geometrica

$$Q(x_1 \dots x_n) = \sqrt{\frac{\sum_{i=1}^{n} x_i^2}{n}} \qquad \text{media quadratica}$$

$$M_p(x_1 \dots x_n) = \sqrt[p]{\frac{\sum_{i=1}^{n} x_i^p}{n}} \qquad \text{media } p\text{-ma}$$

$x_i \geq 0$

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

media armonica

Disuguaglianze fondamentali tra medie:

$$M_{-1} = H((x_i)) \leq G((x_i)) \leq \overset{M_1}{\overset{\shortparallel}{A}}((x_i)) \leq Q((x_i))$$

(CS)

(≤) ovvie "$M_0(x_i)$" (R)

$\min_i(x_i)$ $\quad M_{-\infty}(x_i)$

L $\quad$ $p \geq 1$ $\quad$ $\leq$ $M_p((x_i)) \leq M_q((x_i))$ $\quad p<q$

(C)

$M_p \leq M_q$ $\quad p \leq q$

(≥) ovvie

$\max_i(x_i)$ $\quad M_{+\infty}(x_i)$

Vale l'= in ~~una~~ qualsiasi di queste $\iff$ $x_1 = x_2 = \dots = x_n$

$(x_i \geq 0)$

1) ottimalità, caratterizzazione di =

2) universalità ($\to$ omogeneità)

ex $\quad G, A, M_p$ sono tutte omogenee

$$G(\lambda x_1,\dots,\lambda x_n) = \lambda G(x_1,\dots,x_n) \quad \text{di grado 1}$$

idem per A, Q, M_p $\longrightarrow$ omogenee di grado 1

Si cerca $\underbrace{f((x_i))}_{\substack{\text{omog.} \\ \text{di grado } d}} \leq \underbrace{g((x_i))}_{\substack{\text{omog.} \\ \text{di grado } d'}}$

universale $\Rightarrow d = d'$

ex $\quad ab + bc + ca \leq a^3 + b^3 + c^3$

è una dis. $\forall a, b, c$

omog. di grado 2 $\qquad$ di grado 3

se fosse vera $\forall a, b, c$ e a_0, b_0, c_0 è sol.

$\longrightarrow \lambda a_0, \lambda b_0, \lambda c_0$ è sol $\forall \lambda$

$$\lambda^2(a_0b_0 + b_0c_0 + a_0c_0) \leq \lambda^3(a_0^3 + b_0^3 + c_0^3) \quad \forall \lambda$$

$$\lambda \geq \frac{a_0b_0 + b_0c_0 + a_0c_0}{a_0^3 + b_0^3 + c_0^3} \qquad (a_0, b_0, c_0) \text{ fissato}$$

$\lambda \to 0$ $\quad$ assurdo

3) disuguaglianze con parametro

$$A((x)) \leq M_p((x_i))$$

Come si comporta variando p ?

EX 1.1: Far vedere che, fissati $x, y > 0$:

(i) $\sqrt[p]{\frac{x^p+y^p}{2}} = M_p(x,y) \xrightarrow[\text{p molto grande}]{} \max\{x,y\}$

$\parallel$

$$\lim_{p\to\infty} \sqrt[p]{\frac{x^p+y^p}{2}} = \max\{x,y\}$$

Cosa significa? posso rendere $\sqrt[p]{\frac{x^p+y^p}{2}}$ vicino quanto mi pare al $\max\{x,y\}$ pur di scegliere p molto grande

Come si fa? z fissato >0

$$\begin{cases} z^p \xrightarrow[\text{p molto grande}]{} \begin{cases} +\infty & \text{se } z>1 \\ 0 & 0<z<1 \end{cases} \\ \sqrt[p]{z} \xrightarrow[\text{p molto grande}]{} 1 \quad \forall z>0 \end{cases}$$

Sia ora $0 < x \le y$ $\quad y = \max\{x,y\}$ fissati.

$$\sqrt[p]{\frac{x^p+y^p}{2}} = \underset{\text{fissato}}{y} \; \underbrace{\sqrt[p]{\underbrace{\frac{\left(\frac{x}{y}\right)^p + 1}{2}}_{\sim \frac{1}{2}}}}_{\xrightarrow[\text{p molto grande}]{} 1} \longrightarrow y, \qquad \left(\frac{x}{y}\right)^p \to 0$$

(ii) $x_1, \dots, x_n \geq 0 \Rightarrow M_p(x_1, \dots, x_n) \xrightarrow[p \to -\infty]{} \min_i \{x_i\}$

(iii) [solo per chi conosce le derivate e l'Hopital]

$$\underbrace{G(x_1, \dots, x_n)}_{\text{"} M_0(x_1 \dots x_n) \text{"}} = \lim_{p \to 0} M_p(x_1, \dots, x_n)$$

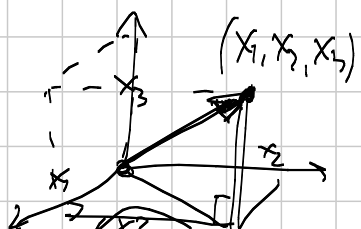
§2 Disuguaglianza di Cauchy-Schwarz

dati $(x_1, \dots, x_n)$ e $(y_1, \dots, y_n)$

$$|x_1 y_1 + \dots + x_n y_n| \leq \sqrt{\sum_{i=1}^n x_i^2} \cdot \sqrt{\sum_{i=1}^n y_i^2}$$

$$\left(\sum_i x_i y_i\right)^2 \leq \left(\sum x_i^2\right)\left(\sum y_i^2\right)$$

$\vec{X} = (x_1, \dots, x_n)$ $\qquad n = 2, 3$



$|\vec{X}| = \sqrt{\sum_{i=1}^n x_i^2}$ norma o lunghezza del vettore $\vec{X}$

$\vec{X} = (x_1, \dots, x_n)$, $\vec{Y} = (y_1, \dots, y_n)$

$\vec{X} \cdot \vec{Y} = x_1 y_1 + x_2 y_2 + \dots x_n y_n$

prodotto scalare

Nota $|\vec{X}| = \sqrt{\underbrace{\vec{X}}_{(x_1,\dots,x_n)} \cdot \underbrace{\vec{X}}_{(x_1,\dots,x_n)}}$

Riformulazione di Cauchy-Schwarz con queste notazioni

$|\vec{X} \cdot \vec{Y}| \leq |\vec{X}|\,|\vec{Y}|$

Vale l'$=$ $\Longleftrightarrow$ $\vec{X} = \lambda \vec{Y}$ $\exists \lambda$

cioè $\exists \lambda$ $x_i = \lambda y_i$ $\forall i$

(o viceversa)

Significato geometrico di Cauchy-Schwarz.

ex 2.1 dati $\vec{X}, \vec{Y}$ vettori in $\mathbb{R}^2, \mathbb{R}^3$

θ l'angolo tra i due

$0 \le \theta \le \pi$

$$\cos\theta = \frac{\vec{X}\cdot\vec{Y}}{|\vec{X}|\,|\vec{Y}|} \qquad (\vec{X},\vec{Y} \neq 0)$$

C.S. $$|\underbrace{\vec{X}\cdot\vec{Y}}_{\text{numero}}| \le \underbrace{\|\vec{X}\|}_{\text{norma}}\|\vec{Y}\|$$

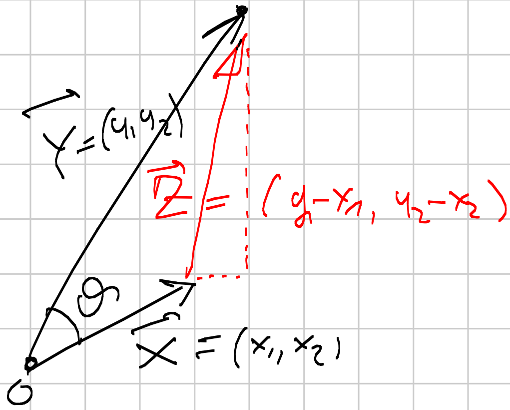
$$|\cos\theta| = \frac{|\vec{X}\cdot\vec{Y}|}{\|\vec{X}\|\,\|\vec{Y}\|} \le 1$$ banalità geometrica

quand'è che vale $=1$?

quando $|\cos\theta| = 1 \to \theta = 0, \pi$

i.e. $\exists\, \alpha : \vec{X} = \alpha\vec{Y}$

Suggerimento per l'ex 2.1



Teor. del coseno: $\underbrace{|\vec{z}|^2}_{\text{(calcolo)}} = \cancel{|\vec{x}|^2} + \cancel{|\vec{y}|^2} - \cancel{2}\cos\theta\, |\vec{x}||\vec{y}|$

$$(\vec{z})^2 = \vec{z}\cdot\vec{z} = \cancel{|\vec{x}|^2} + \cancel{|\vec{y}|^2} - \cancel{2}\,\vec{x}\cdot\vec{y} \quad \Downarrow$$

$$\cos\theta = \dots$$

$\square$

questa dà una dimostrazione geometrica di C-S per $n = 2, 3$

per n qualsiasi?

dim C-S per n qualsiasi:

$$\left(\sum_i^n x_i y_i\right)^2 \overset{?}{\leq} \cancel{\left(\sqrt{\sum_i x_i^2}\right)\left(\sqrt{\sum_i y_i^2}\right)}$$

$$\underbrace{\left(\sum_{i=1}^n x_i^2\right)\left(\sum_{j=1}^n y_j^2\right)}_{\sum_{i,j=1}^n x_i^2 y_j^2} - \underbrace{\left(\sum_{i=1}^n x_i y_i\right)^2}_{\underbrace{\left(\sum_{i=1}^n x_i y_i\right)\left(\sum_{j=1}^n x_j y_j\right)}_{\sum_{i,j=1}^n x_i y_i x_j y_j}} \overset{?}{\geq} 0$$

$$\cancel{\sum_{i=j=1}^n x_i^2 y_i^2} + \underbrace{\sum_{i\neq j} x_i^2 y_j^2} - \cancel{\sum_{i=j=1}^n x_i^2 y_i^2} - \underbrace{\sum_{i\neq j} x_i x_j y_i y_j} \overset{?}{\geq} 0$$

$$x_1^2 y_2^2 + x_2^2 y_1^2$$

$$\sum_{i<j}\left(x_i^2 y_j^2 + x_j^2 y_i^2\right) - \sum_{i<j} 2 x_i y_i x_j y_j$$

$$\sum_{i<j} (x_i y_j - y_i x_j)^2 \geq 0 \quad \text{ok!}$$

quando $= 0$?

$$\boxed{x_i y_j = y_i x_j} \quad \forall i,j \Rightarrow \frac{x_i}{y_i} = \frac{x_j}{y_j} = \exists \lambda$$

$\forall i,j$

oppure ($y_i = \lambda x_i$)

$$\boxed{\exists \lambda \quad \forall i \quad x_i = \lambda y_i}$$

Esempi di applicazione di C-S :

ex 2.2 $A(x_1 \dots x_n) \le Q(x_1 \dots x_n)$

$$\frac{1}{n} \underbrace{\sum_i x_i \cdot 1}_{\vec{X} \cdot \underbrace{(1,1,\dots,1)}_{\mathbb{1}}} \overset{?}{\le} \sqrt{\frac{1}{n} \sum_i x_i^2} = \sqrt{\frac{1}{n}} \underbrace{\sqrt{\sum x_i^2}}_{|\vec{X}|}$$

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

$$\frac{\vec{X} \cdot \mathbb{1}}{n} \le \frac{\sqrt{\sum x_i^2} \cdot \cancel{\sqrt{n}}}{\cancel{n}\ \sqrt{n}}$$

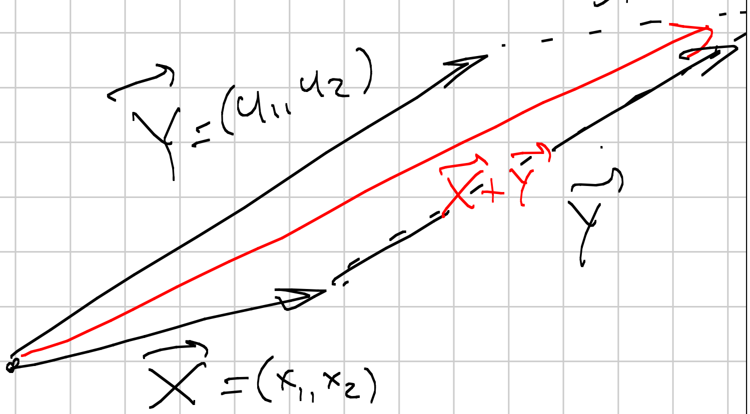
Ok! vale $=$ $\exists \lambda$ tes $x_i = \lambda\ \forall i$

ex 2.3 Dis di Minkowsky o Triangolare $(p=2)$

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

e vale $=$ sse $\exists\, \lambda \geq 0$ t.c. $x_i = \lambda y_i \ \forall i$

interpretazione per $n=2,3$



$$\vec{X}+\vec{Y} = (x_1+y_1,\ x_2+y_2)$$

Mink in termini di vettori:

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

(dis. triangolare)

Uguaglianza

Dim. $\underbrace{|\vec{X}+\vec{Y}|^2}_{(\vec{X}+\vec{Y})\cdot(\vec{X}+\vec{Y})} \overset{?}{\le} \underbrace{(|\vec{X}|+|\vec{Y}|)^2}_{\cancel{|\vec{X}|^2}+\cancel{|\vec{Y}|^2}+2|\vec{X}||\vec{Y}|}$

$$(\vec{X}+\vec{Y})\cdot(\vec{X}+\vec{Y}) = \cancel{|\vec{X}|^2} + \cancel{|\vec{Y}|^2} + 2\,\vec{X}\cdot\vec{Y}$$

vale = sse vale $\boxed{\vec{X}\cdot\vec{Y} = |\vec{X}|\,|\vec{Y}|}$

$\Downarrow$

è più difficile $\underbrace{|\vec{X}\cdot\vec{Y}| = |\vec{X}|\,|\vec{Y}|}$

$\vec{X} = \lambda\vec{Y}$

dal fatto che $\vec{X}\cdot\vec{Y} > 0 \to \underline{\underline{\lambda > 0}}$.

§3 Riarrangiamento

Siano $a_1 \leq a_2 \leq \dots \leq a_n$ crescente
$b_1 \leq b_2 \leq \dots \leq b_n$ crescente

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

$$\sigma : \begin{pmatrix} 1 \to \sigma(1) \\ 2 \to \sigma(2) \\ \vdots \\ n \to \sigma(n) \end{pmatrix}$$

$=$ vale se e solo se ho accoppiato in modo $\nearrow$

$=$ se e solo se ho accoppiato in modo $\searrow$

x dim. Supp. che σ sia una permutazione che mi dà il massimo.

Guardiamo le coppie di indici (i,j) tali che $a_i < a_j$ ma $b_{\sigma(i)} > b_{\sigma(j)}$

$\underbrace{}$
"Coppie invertite da σ"

Th σ dà il max $\Rightarrow \nexists$ coppie (i,j) invertite da σ

Supp. che $\exists (i,j)$ invertite da σ : $M = \cancel{a_1 b_{\sigma(1)}} + \dots + a_i b_{\sigma(i)} + \dots + a_j b_{\sigma(j)} + \dots \cancel{a_n b_{\sigma(n)}}$

$\geq$

corrisponde a una permutaz. σ' $\longrightarrow \cancel{a_1 b_{\sigma(1)}} + \dots + a_i b_{\sigma(j)} + \dots + a_j b_{\sigma(i)} + \dots + \cancel{a_n b_{\sigma(n)}}$

$$\Rightarrow a_i\left(b_{\sigma(i)} - b_{\sigma(j)}\right) + a_j\left(b_{\sigma(j)} - b_{\sigma(i)}\right) \geq 0$$

$$i<j \qquad \underbrace{\underbrace{(a_i - a_j)}_{\leq 0}\underbrace{\left(b_{\sigma(i)} - b_{\sigma(j)}\right)}_{\geq 0}} \geq 0$$

può essere solo = se $a_i = a_j$ oppure $b_{\sigma(i)} = b_{\sigma(j)}$

cioè (i,j) non è invertita da σ $\square$

es. 1 2 3 3 4 5 $= (a_i)$

6 7 7 8 9 10 $= (b_i)$

$$\sum_i a_i b_{\sigma(i)} \leq 6 + 14 + 21 + 24 + 36 + 50 \qquad \sigma = id$$

ex. 3.1 a, b, c qualsiasi:

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

$(a_i) = b \; a \; c$

$(b_i) = b \; a \; c$

ex 3.2 $a, b, c > 0$

$$a^b \cdot b^c \cdot c^a \leq a^a \cdot b^b \cdot c^c$$

$$\overset{?}{\Longleftrightarrow} \operatorname{Log}(a^b \cdot b^c \cdot c^a) \leq \operatorname{Log}(a^a \cdot b^b \cdot c^c)$$

$\log_{10}$ (equivalente perché Log è crescente)

$$b \operatorname{Log} a + c \operatorname{Log} b + a \operatorname{Log} c \overset{?}{\leq} a \operatorname{Log} a + b \operatorname{Log} b + c \operatorname{Log} c$$

se $a \leq b \leq c$ allora $\operatorname{Log} a \leq \operatorname{Log} b \leq \operatorname{Log} c$ $\square$

$\xrightarrow{(R)}$ fine

ex 3.3 (Test)

Trovare il minimo k t.c. :

$$\frac{a^2}{b}+\frac{b^2}{c}+\frac{c^2}{a} \le k \sqrt{\frac{a^2}{b^4}+\frac{b^2}{c^4}+\frac{c^2}{a^4}}$$

$\forall \begin{cases} a,b,c \ge 0 \\ a^4+b^4+c^4 = 4 \end{cases}$

$u \cdot v = ?$

$v = (ab, bc, ca)$

$$\underbrace{\left|\left(\frac{a}{b^2}, \frac{b}{c^2}, \frac{c}{a^2}\right)\right|}_{u}$$

CS: $\frac{a^2}{b}+\frac{b^2}{c}+\frac{c^2}{a} = u \cdot v \le |u||v|$

$$\le \sqrt{\frac{a^2}{b^4}+\frac{b^2}{c^4}+\frac{c^2}{a^4}} \cdot \underbrace{\sqrt{a^2b^2+b^2c^2+a^2c^2}}_{\wedge\ k}$$

$a^4+b^4+c^4 = 4$ $\quad \sqrt{a^4+b^4+c^4} = 2$

$=$ sse $a=b=c$

Risp il k max è 2.

Ma $\exists\, a,b,c$ t.c. ho l'$=$ (con $k=2$)?

Si prendo $a=b=c$ + $\Rightarrow$ $=$. Ok $a=\sqrt[4]{4/3}=b=c$.

ex 3.4 Siano $a_1, a_2, \dots, a_n > 0$

Mostrare che $a_1/a_2 + a_2/a_3 + \dots + a_n/a_1 \geq n$

Cioè $\forall$ ordinamento $\sigma : \begin{pmatrix} 1 \\ \vdots \\ n \end{pmatrix} \to \begin{pmatrix} \sigma(1) \\ \vdots \\ \sigma(n) \end{pmatrix}$

vale $\boxed{a_{\sigma(1)}/a_{\sigma(2)} + \dots + a_{\sigma(n)}/a_{\sigma(1)} \geq n}$

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

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

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

$$a_1/a_2 + \dots + a_n/a_1 \geq \sum_i \underbrace{a_{\sigma(i)} \cdot \frac{1}{a_{\sigma(i)}}}_{1} = n$$

$=$ sse $a_1 = a_2 = \dots = a_n$

Ex 35 Dis aritmetico-geometrica

$$G((x_i)) \leq A((x_i))$$

$$x_1, \dots, x_n \geq 0$$

Dim

$$y_1 = G/x_1$$
$$y_2 = G^2/x_1x_2$$
$$\vdots$$
$$y_n = G^n/x_1 \cdots x_n$$

$$\Rightarrow \begin{cases} y_i/y_{i+1} = \dfrac{\cancel{G^i}}{\cancel{x_1 \cdots x_i}} \cdot \dfrac{\cancel{x_1 \cdots} x_{i+1}}{G^{\cancel{i+1}}} = x_{i+1}/G \\ y_n/y_1 = \dfrac{\cancel{G^n}}{\cancel{x_1 \cdots x_n}} \cdot \dfrac{x_1}{G} \end{cases}$$

$$y_1/y_2 + y_2/y_3 + \dots + y_n/y_1 \geq n$$

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

$$\frac{x_1 + \dots + x_n}{n} \geq G$$

Vale l'$=$ $\iff$ vale l'$=$ sse $y_i = y_j = G$ $\forall i, j$

sse $x_i = G$ $\forall i$ $= x_j$

A-G è utile quando debbo calcolare

|| il minimo di $\sum x_i$

|| conoscendo il $\prod x_i$

oppure quando debbo calcolare

|| il max di $\prod x_i$

|| conoscendo la $\sum x_i$

$$\sqrt[n]{x_1 \cdot \ldots \cdot x_n} \le \frac{1}{n}\underbrace{(x_1 + \cdots + x_n)}$$

ex. 3.6 Calcolare $\min\left\{x+2y+3z \;\middle|\; \begin{array}{l} x,y,z \ge 0 \\ \underbrace{x^3y^2z} = 1 \end{array}\right\}$

$$\prod x_i = x^3y^2z$$

val = def

$\frac{x}{3} = y = 3z$

$\frac{x^3}{3^3} y^2 3z = \frac{1}{9}$ $\quad (3y)^3 y \left(\frac{y}{3}\right) = 1$

$$(x_i) = \left(\frac{x}{3}, \frac{x}{3}, \frac{x}{3}, y, y, 3z\right)$$

$$G(x_i) = \sqrt[6]{\prod_i x_i} = \sqrt[6]{\frac{1}{9}x^3y^2z} = \sqrt[6]{\frac{1}{9}}$$

$$6A(x_i) = x + 2y + 3z$$

$$x + 2y + 3z \underset{A \ge G}{\ge} 6\,G(x_i) \ge 6 \cdot \sqrt[6]{1/9} = \underline{\underline{\min}}$$

Es. 3.7 Trovare $\max \left\{ \underbrace{x^2 y z^3}_{\prod x_i} \;\middle|\; \begin{array}{l} x,y,z \geq 0 \\ x+y+z=1 \end{array} \right\}$

$$(x_i) = \left(\frac{x}{2}, \frac{x}{2}, y, \frac{z}{3}, \frac{z}{3}, \frac{z}{3} \right)$$

$$G(x_i) = \frac{1}{\sqrt[6]{4\cdot 27}} \sqrt[6]{x^2 y z^3}$$

$$\leq$$

$$A(x_i) = \frac{x+y+z}{6} = 1/6$$

$$x^2 y z^3 \leq \frac{4\cdot 27}{6^6} = \max ?$$

vale l' $=$: $\frac{x}{2} = y = z/3$ con $x+y+z=1$

troviamo x, y, z.

Es. 3.8 Calcolare $\min \{ x^2 + y^4 + z^6 \mid xyz = k \}$

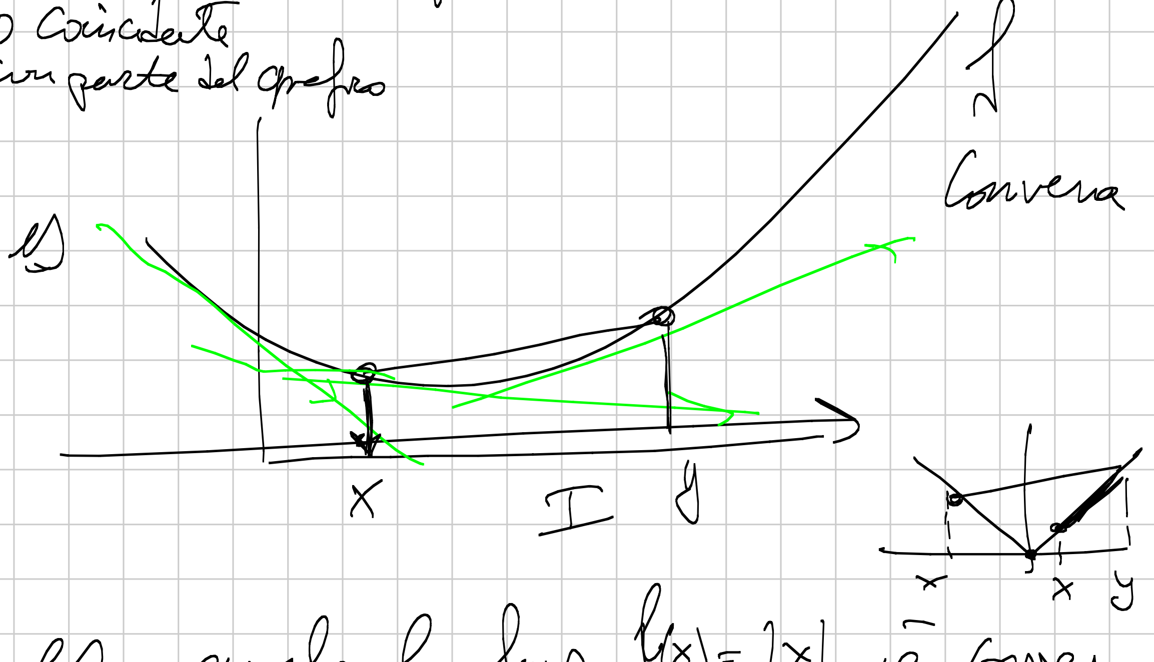
$x, y, z > 0$

$$\underbrace{\frac{x^2}{6} \cdot \frac{x^2}{6} \cdots \frac{x^2}{6}}_{6} \cdot \underbrace{\frac{y^4}{3} \cdot \frac{y^4}{3} \cdot \frac{y^4}{3}}_{3} \cdot \underbrace{\frac{z^6}{2} \cdot \frac{z^6}{2}}_{2} = x^{12} y^{12} z^{12} = k^{12}$$

§4 Dis. di convessità

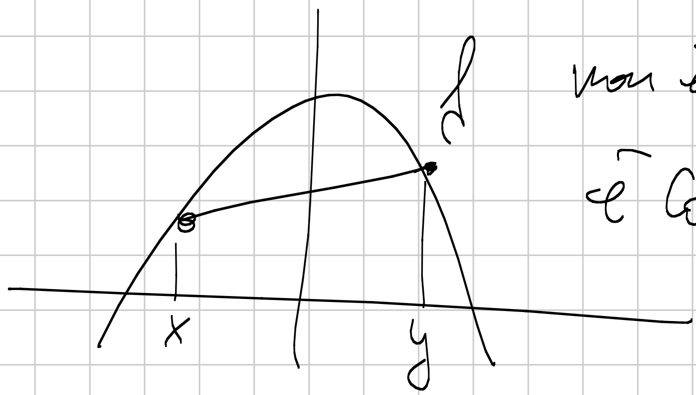
<u>definizione</u> una funzione f (definita su un intervallo I) si dice <u>convessa</u> (<u>CONCAVA</u>) se il segmento che congiunge due qualsiasi punti del suo grafico in I sta <u>AL DI SOPRA</u> (<u>AL DI SOTTO</u>) del grafico stesso :

o coincidente con parte del grafico



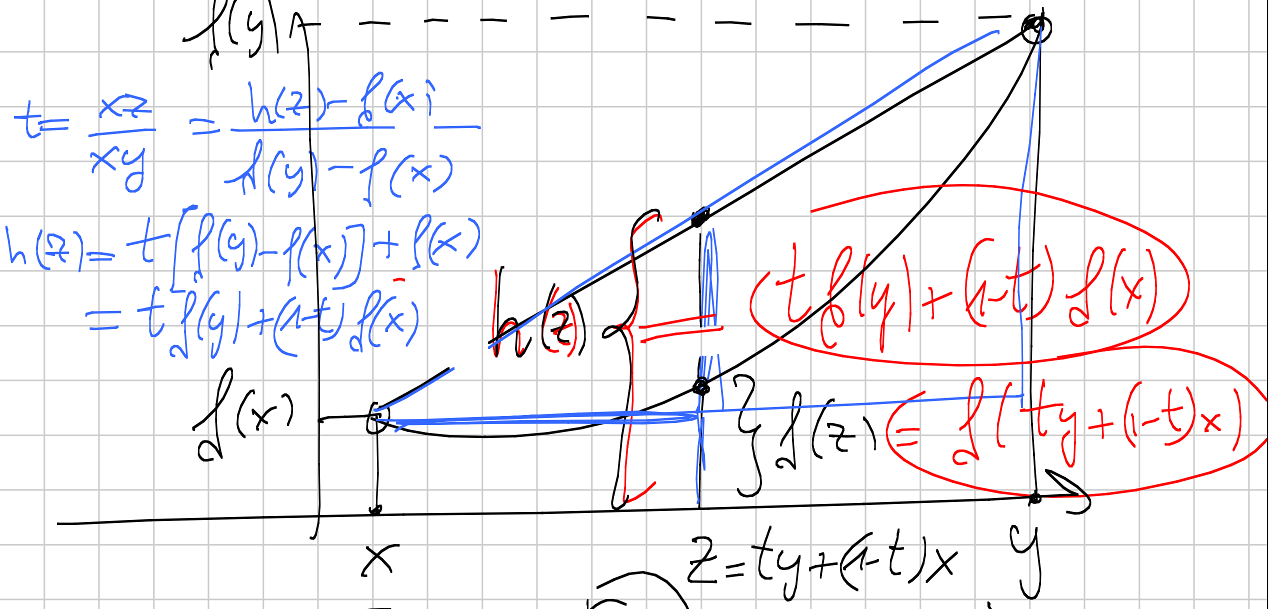
<u>es.</u> anche la funz $f(x) = |x|$ è convessa

es.



f non è convessa! è concava.

Come si scrive questa condizione di convessità con una formula?



Convessità $\iff$ $h(z) \geq f(z)$ $\cancel{\forall z \in [x,y]}$ $\forall t \in [0,1]$

SCRIVIAMOLA MEGLIO

OSS

Un punto $z \in [x,y]$ si può sempre scrivere come

$$z = x + t(y-x) \qquad 0 \le t \le 1$$
$$= ty + (1-t)x$$

PROP Sia f una funz. definita su I. Sono condizioni equivalenti:

(i) f è convessa (concava) su I

(ii) $f(tx+(1-t)y) \le (\ge)\ tf(x)+(1-t)f(y) \quad \forall x,y \in I \quad \forall t \in [0,1]$

(iii) $f(t_1x_1+\dots+t_nx_n) \le (\ge)\ t_1f(x_1)+\dots+t_nf(x_n)$

$\forall x_1,\dots,x_n \in I, \ \forall t_1,\dots,t_n \in [0,1]$, $\sum_i t_i = 1$

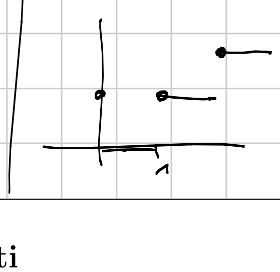
(iv) $f\left(\frac{x+y}{2}\right) \le (\ge)\ \frac{1}{2}[f(x)+f(y)] \quad \forall x,y \in I$

└ (equivalente se f è continua)

(v) $f''(x) \ge 0$ ($\le$) $\quad \forall x \in I$

└ (equivalente se f ammette derivata seconda)

ex. $f(x) = [x]$ non è conv.

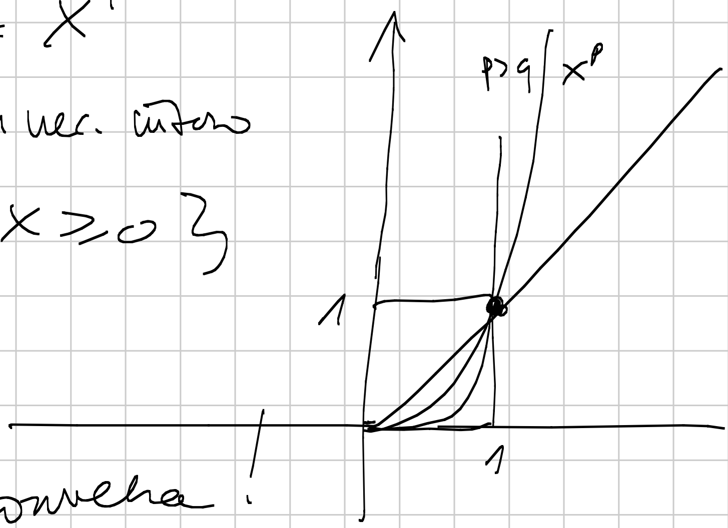


ex $f(x) = x^p$

p non nec. intero

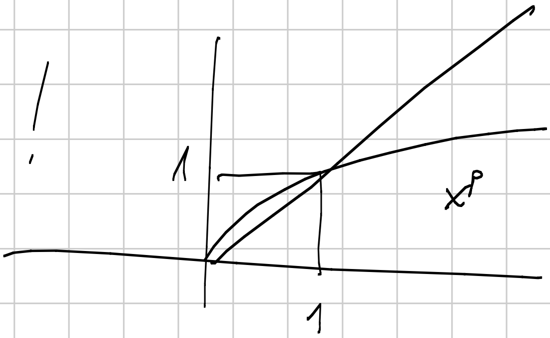
$I = \{x \geq 0\}$

$p > 1$



è convessa!

$0 < p < 1$ è concava!

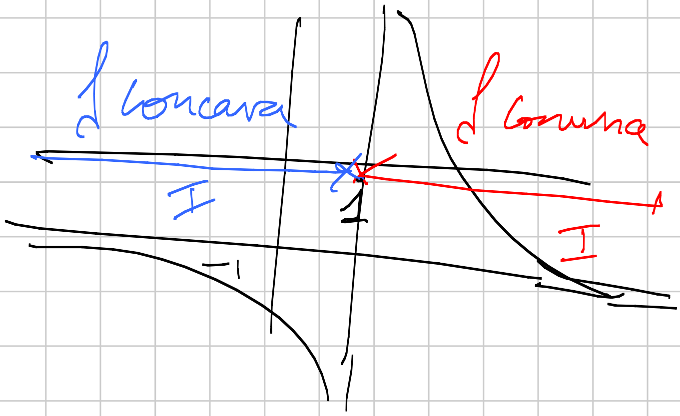


$f(x) = x^p$

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

$f''(x) = \underbrace{p}_{>0}(p-1)\underbrace{x^{p-2}}_{>0} > 0 \iff p > 1$

ex $f(x) = \dfrac{x}{1-x}$



ex $f(x) = \log_a x$

$= \log_a x \Big]$ convessa

$0<a<1$

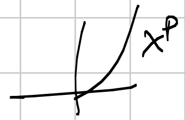
$f'(x) = \frac{1}{x} / \ln a$ >0 $a>1$

$f''(x) = -\frac{1}{x^2} / \ln a$ <0 $0<a<1$

Ogni funzione convessa / concava dà luogo a disuguaglianze interessanti ex. 4.1 Mostrare che $A(x_1,x_2) \le M_p(x_1,x_2)$ $\qquad p \ge 1.$

Th $\dfrac{x_1+x_2}{2} \le \sqrt[p]{\dfrac{x_1^p+x_2^p}{2}}$

$x_1, x_2 \ge 0$



$\downarrow$ viene dal fatto che $f(x) = x^p$ è convessa $\quad p \ge 1$

Cond (iv) $\Rightarrow$ $f\left(\dfrac{x_1+x_2}{2}\right) \le \dfrac{f(x_1)+f(x_2)}{2}$

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

$$\frac{x_1+x_2}{2} \le \sqrt[p]{\frac{x_1^p+x_2^p}{2}}$$

Se voglio mostrare $A(x_1,\dots,x_n) \underset{p\ge 1}{\le} M_p(x_1\dots x_n)$

uso la (iii)

$$f\left(\frac{1}{n}x_1 + \frac{1}{n}x_2 + \dots + \frac{1}{n}x_n\right) \le \frac{f(x_1)+\dots+f(x_n)}{n}$$

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

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

$\longrightarrow$ ok.

ex 4.2 Mostrare $M_p(x_1,x_2) \leq M_q(x_1,x_2)$

$p \leq q$

Th $\sqrt[p]{\frac{x_1^p + x_2^p}{2}} \leq \sqrt[q]{\frac{x_1^q + x_2^q}{2}}$

Th $\left(\frac{x_1^p + x_2^p}{2}\right) \leq \frac{x_1^q + x_2^q}{2} = \sqrt[q/p]{\frac{(x_1^p)^{q/p} + (x_2^p)^{q/p}}{2}}$

ok $\square$

oppure:

$f(x) = x^{q/p}$ convessa

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

$\left(\frac{x_1^p + x_2^p}{2}\right)^{\cancel{q}/p} \leq \sqrt[q]{\frac{x_1^q + x_2^q}{2}}$

ex $AB \leq \frac{1}{p}A^p + \frac{1}{q}B^q$ $p,q>0$

(Young) $\underbrace{\frac{1}{p}}_{t}$ $\underbrace{\frac{1}{q}}_{1-t}$ $\frac{1}{p}+\frac{1}{q}=1$

$AB>0$

$\frac{1}{2}(A^2+B^2) \geq AB$ $A^2+B^2 \geq 2AB$

$Q \geq A \geq G$ $A^2+B^2-2AB \geq 0$

$= (A-B)^2$

$f(x) = \log x$ Concava

$\log\left(\underbrace{\frac{1}{p}}_{t}A^p + \underbrace{\frac{1}{q}}_{1-t}B^q\right) \geq \underbrace{\frac{1}{p}\log(A^p) + \frac{1}{q}\log(B^q)}_{\log(AB)}$

$\log_{10}$ crescente $\Downarrow$

$\frac{1}{p}A^p + \frac{1}{q}B^q \geq AB$.

ex Dimostrare che se $x_1, \dots, x_n \geq 0$
$\sum_i x_i = 1$

allora $\frac{1}{n} \sum_{i=1}^{n} \frac{x_i}{\sqrt{1-x_i}} \geq \underbrace{\sqrt{\frac{n}{n-1}} \cdot \frac{1}{n}}_{\sqrt{\frac{1}{n(n-1)}}}$

t_i $\quad$ $\frac{1}{\dots}$ $\quad$ y_i

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

$\sum_{i=1}^{n} \underbrace{x_i}_{t_i} f(x_i) \overset{?}{\geq} f\left(\sum_i x_i \cdot x_i\right)$

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

$\frac{1}{n} \frac{x_1}{\sqrt{1-x_1}} + \dots + \frac{1}{n} \frac{x_n}{\sqrt{1-x_n}} \geq f\left(\frac{\sum_i x_i}{n}\right)$

$\geq f(1/n)$

$\geq \sqrt{\frac{1}{n(n-1)}}$

Verifica: si deriva e $f'' \geq 0$

facile! sostituire

$f'' \sim \frac{4-x}{(1-x)^{7/2}} > 0 \quad x \in (0,1)$

ALGEBRA 3 - BASIC

Titolo nota 07/09/2012

→ 1) Somme tipo $\underbrace{\sum_{k=1}^{n} p(k) a^k}$ con K polinomio

2) Succ. definite per ricorrenze lineari.

3) equazioni funzionali

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

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

$$\boxed{(n+1)^3 - n^3 = 3n^2 + 3n + 1}$$

$$(n+1)^3 - \cancel{n^3} = 3n^2 + 3n + 1$$

$$\cancel{n^3} - \cancel{(n-1)^3} = 3(n-1)^2 + 3(n-1) + 1$$

$$\cancel{(n-1)^3} - \cancel{(n-2)^3} = 3(n-2)^2 + 3(n-2) + 1$$

$$\vdots$$

$$\cancel{2^3} - 1^3 = 3 \cdot 1^2 + 3 \cdot 1 + 1$$

$$S_n = \sum_{k=1}^{n} k^2$$

$$\boxed{(n+1)^3 - 1 = 3 S_n + 3\frac{n(n+1)}{2} + n}$$

$$S_n = \frac{1}{3}\Big(n^3 + 3n^2 + \underbrace{3n - n}_{2n} - \frac{3}{2}n(n+1)\Big) =$$

$$= \frac{2n^3 + 6n^2 + 4n - 3n(n+1)}{6} =$$

$$2n^2+6n+4$$
$$2(n^2+3n+2)$$
$$2(n+2)(n+1)$$

$$= \frac{n\left(2n^2 + 6n + 4 - 3(n+1)\right)}{6} =$$

$$= \frac{n\left(2(n+2)(n+1) - 3(n+1)\right)}{6} =$$

$$= \frac{n(n+1)(2n+4-3)}{6} =$$

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

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

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

$$(n+1)^4 - \cancel{n^4} = 4n^3 + 6n^2 + 4n + 1 \qquad S_n = \sum_1^n k^3$$

$$\cancel{n^4} - \cancel{(n-1)^4} = 4(n-1)^3 + 6(n-1)^2 + 4(n-1) + 1$$

$$\vdots$$

$$\vdots$$

$$\cancel{2^4} - 1^4 = 4\cdot 1^3 + 6\cdot 1^2 + 4\cdot 1 + 1$$

$$(n+1)^4 - 1 = 4\, S_n + 6\cdot \frac{n(n+1)(n+\frac{1}{2})}{3} + 4\,\frac{n(n+1)}{2} + n$$

$$\vdots$$

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

$$\sum_{k=1}^{n} k^4 = \frac{n(n+1)\left(n+\frac{1}{2}\right)\left(n^2+n-\frac{1}{3}\right)}{5}$$

$$\sum_{k=1}^{n} k^5 = \cdots\cdots$$

$$\sum_{k=1}^{n} k^p = \quad n\,,\ p$$

$$\sum_{k=1}^{n} P(k) \qquad\qquad \sum k^p$$

$$\underbrace{\sum_{k=1}^{n} \left(3k^2 + 5k + 11\right)} = 3\sum_{k=1}^{n} k^2 + 5\sum_{k=1}^{n} k + 11\sum_{k=1}^{n} 1$$

Algebra 3 (Basic) – Emanuele Callegari

$$\sum_{k=0}^{50} (k+4)(k+3)(k+2)(k+1) =$$

$$= \sum_{k=0}^{50} 4! \boxed{\frac{(k+4)(k+3)(k+2)(k+1)}{4!}} =$$

$$= 4! \sum_{k=0}^{50} \binom{k+4}{4} = 24 \binom{55}{5}$$

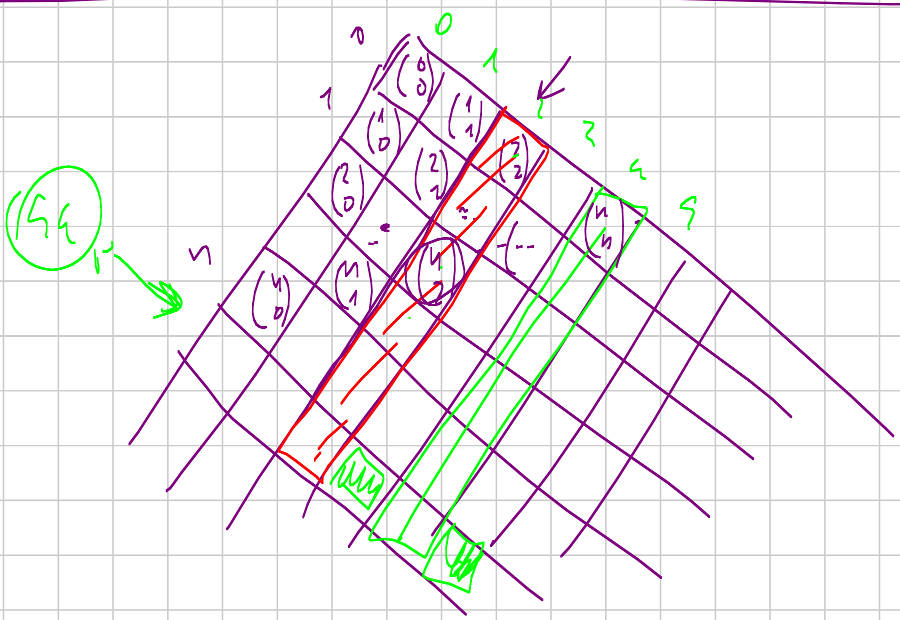
$$= \dots$$

$$\binom{4}{4} + \binom{5}{4} + \binom{6}{4} + \dots + \binom{54}{4} =$$

$$= \binom{55}{5}$$

$$= \sum_{k=1}^{n} k^p =$$

$$\sum_{k=0}^{n} \binom{k+p}{p} = \boxed{\binom{n+p+1}{p+1}}$$



$$\sum_{k=0}^{100} \underbrace{k^2 + 7k + 5} =$$

$$\binom{k+2}{2} \leftarrow$$

$$\binom{k+1}{1} \leftarrow$$

$$\binom{k}{0} \leftarrow$$

$$k^2+7k+5 = \underbrace{k^2+3k+2}_{(k+2)(k+1)} + 4k+3 =$$

$$= 2\underbrace{\frac{(k+2)(k+1)}{2}} + 4\frac{(k+1)}{1} - 1 =$$

$$= \underbrace{2\binom{k+2}{2} + 4\binom{k+1}{1} - \binom{k}{0}}$$

$$\sum_{k=0}^{100} k^2+7k+5 = \sum_{k=0}^{100} 2\binom{k+2}{2} + 4\binom{k+1}{1} - \binom{k}{0} =$$

$$= 2\binom{103}{3} + 4\binom{102}{2} - \binom{101}{1} = \dots$$

$$\sum_{k=0}^{100} \underbrace{(k+1)^2(k+3)^3}$$

$$\boxed{6} \qquad \underbrace{\alpha_1\binom{k+5}{5} + \alpha_2\binom{k+4}{4} + \dots + \alpha_6\binom{k}{0}}$$

$$\sum_{k=0}^{n} p(k)\, a^k \qquad \sum_{k=0}^{n} a^k = \frac{a^{n+1}-1}{a-1} \qquad a \neq 1$$

$$\boxed{\sum_{k=1}^{100} k\,2^k} = 1\cdot 2^1 + 2\cdot 2^2 + 3\cdot 2^3 + 4\cdot 2^4 + \dots + 100\cdot 2^{100}$$

$$S_n = \sum_{k=1}^{n} k 2^k$$

$$\boxed{S_n - S_{n-1} = n 2^n}$$

$$S_1 = 2$$

$$\boxed{\begin{cases} S_n - S_{n-1} = n 2^n \\ S_1 = 2 \end{cases}}$$

$$S_n = \quad n$$

$$\sum_{k=1}^{n} k^5 2^k = S_n$$

$$\begin{cases} S_n - S_{n-1} = \boxed{n^5 2^n} \\ S_1 = 2 \end{cases}$$

$$2^{n^2}$$

EQ. DIFF. FINITE LINEARI

(OMOGENEE)

non omogenee

$$\boxed{F_n - \alpha_1 F_{n-1} \quad \alpha_2 F_{n-2} + \cdots + \alpha_k F_{n-k} = 0} + \cancel{f(n)}$$

$$\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{R}$$

k ordine

Es. Fibonacci $\boxed{F_n = F_{n-1} + F_{n-2}}$

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

Polinomio caratteristico

$$\lambda^k - \alpha_1 \lambda^{k-1} - \alpha_2 \lambda^{k-2} - \cdots - \alpha_{k-1} \lambda - \alpha_k = 0$$

$\boxed{\text{Teorema}}$

Data $\boxed{F_{n+2} + aF_{n+1} + bF_n = 0}$

tale che le radici del pol. caratteristico

$\lambda^2 + a\lambda + b$ siano λ_1 e λ_2 reali e

distinte, allora tutte e sole le

sue soluzioni sono quelle della forma

$$\longrightarrow F_n = \alpha\lambda_1^n + \beta\lambda_2^n \quad \text{per ogni } \alpha, \beta \in \mathbb{R}$$

$\boxed{\text{Esempio}}$

$$\longrightarrow F_{n+2} = 5F_{n+1} - 6F_n$$

$$\cancel{F_1 = 2 \quad F_2 = 4}$$

$$\lambda^2 - 5\lambda + 6 =$$

$\lambda = 2$

$\lambda = 3$

$$\boxed{F_n = 2^n} \qquad \boxed{F = 3^n}$$

$$2^{n+2} \overset{?}{=} 5 \cdot 2^{n+1} - 6 \cdot 2^n$$

$$4 \cdot 2^n \overset{?}{=} \underbrace{10 \cdot 2^n - 6 \cdot 2^n}_{4 \cdot 2^n}$$

$$\underbrace{3^{n+2}}_{9\cdot 3^n} \neq \underbrace{5\cdot 3^{n+1} - 6\cdot 3^n}_{\underbrace{15\cdot 3^n - 6\cdot 3^n}}$$

$$\begin{cases} F_{n+2} = F_{n+1} + F_n \\ F_1 = 1 \\ F_0 = 0 \end{cases} \longleftarrow F_{n+2} - F_{n+1} - F_n = 0$$

$$\underbrace{\lambda^2 - \lambda - 1 = 0}$$

$$\lambda^2 - \lambda - 1 = 0$$

$$\lambda = \frac{1 \pm \sqrt{5}}{2} \begin{matrix} \nearrow \frac{1+\sqrt{5}}{2} \\ \searrow \frac{1-\sqrt{5}}{2} \end{matrix}$$

$$\boxed{F_n = \underset{\uparrow\, \frac{1}{\sqrt{5}}}{\alpha} \left(\frac{1+\sqrt{5}}{2}\right)^n + \underset{\uparrow\, -\frac{1}{\sqrt{5}}}{\beta} \left(\frac{1-\sqrt{5}}{2}\right)^n}$$

$F_1 = 1$ ⟷
$F_0 = 0$ ⟷

$$\begin{cases} \alpha + \beta = 0 \\ \underbrace{\alpha \frac{1+\sqrt{5}}{\cancel{2}} + \beta \frac{1-\sqrt{5}}{\cancel{2}}} = \cancel{1}\,2 \end{cases}$$

$$\alpha + \alpha\sqrt{5} + \beta - \beta\sqrt{5} = 2$$

$$\begin{cases} \alpha+\beta=0 \iff \alpha=-\beta \\ \underbrace{\alpha\sqrt{5}-\beta\sqrt{5}=2} \end{cases}$$

$$\cancel{2}\alpha\sqrt{5}=\cancel{2}$$

$$\alpha=\frac{1}{\sqrt{5}}$$

$$\beta=-\frac{1}{\sqrt{5}}$$

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

I^a parte: tutte le succ. del tipo

$$\alpha\cdot\lambda_1^n+\beta\cdot\lambda_2^n \quad \text{vanno bene}$$

1) Se A_n e B_n sono succ. che vanno bene anche $\alpha A_n+\beta B_n$ va bene.

$$\longrightarrow \quad A_{n+2}+aA_{n+1}+bA_n=0$$

$$\longrightarrow \quad B_{n+2}+aB_{n+1}+bB_n=0$$

$\forall\alpha,\beta\in\mathbb{R}$

$$\underbrace{\left(\alpha A_{n+2}+\beta B_{n+2}\right)}+a\left(\underbrace{\alpha A_{n+1}+\beta B_{n+1}}\right)+b\left(\underbrace{\alpha A_n+\beta B_n}\right)=0$$

2) Se λ_1 è una radice del pol. caratteristico allora λ_1^n è una succ. buona.

$$(1, \lambda_1, \lambda_1^2, \lambda_1^3, \lambda_1^4, \ldots)$$

? $F_{n+2}+aF_{n+1}+bF_n=0$

? $\lambda_1^{n+2}+a\lambda_1^{n+1}+b\lambda_1^n \stackrel{?}{=} 0$

$$\underbrace{\lambda_1^2+a\lambda_1+b=0}$$

(1) + (2) $\Longrightarrow$ Vanno bene tutte queste:

$$(*)\quad \boxed{\alpha\lambda_1^n+\beta\lambda_2^n} \longleftarrow$$

---

(3) (*) sono tutte

$$F_{n+2}=-aF_{n+1}-bF_n$$

$\forall$ ... F_0 , F_1

$$\begin{cases} \alpha + \beta = F_0 \\ \alpha\lambda_1 + \beta\lambda_2 = F_1 \end{cases}$$

$$\begin{cases} \alpha\lambda_1 + \beta\lambda_1 = \lambda_1 F_0 \\ \alpha\lambda_1 + \beta\lambda_2 = F_1 \end{cases}$$

$$(\lambda_1 - \lambda_2)\beta = \lambda_1 F_0 - F_1$$

$$\boxed{\beta = \frac{\lambda_1 F_0 - F_1}{\lambda_1 - \lambda_2}}$$

$\boxed{\text{OSS.}}$ Se c'era una sola radice reale con molt. 2.

$$(x - \lambda_0)^2$$

$$\boxed{\lambda_0^n} \qquad \boxed{n\lambda_0^n} \qquad \boxed{(\alpha + \beta n)\lambda_0^n}$$

$$\varsigma$$

$$\begin{array}{ccccc} 1 & \varsigma & \varsigma^2 & \varsigma^3 & \dots \\ 0 & 1\cdot\varsigma & 2\cdot\varsigma^2 & 3\cdot\varsigma^3 & \dots \end{array}$$

$$\boxed{F_{n+2} + aF_{n+1} + bF_n = 0}$$

$$\boxed{F_{n+2} + aF_{n+1} + bF_n = f(n)}$$

$$\boxed{ax + by = c} \qquad (x_1, y_1)$$

$$\boxed{ax + by = 0}$$

A_n e B_n risolvono non omogenea

$$A_{n+2} + aA_{n+1} + bA_n = \boxed{f(n)}$$

$$B_{n+2} + aB_{n+1} + bB_n = f(n)$$

$$(A_{n+2} - B_{n+2}) + a(A_{n+1} - B_{n+1}) + b(A_n - B_n) = 0$$

$$\boxed{\underbrace{F_{n+2} + aF_{n+1} + bF_n} = \underbrace{f(n)}_{\boxed{p(n)\cdot a^n}}}$$

$$q(n)\,a^n$$

$$\begin{cases} S_n - S_{n-1} = n2^n \\ S_1 = 2 \end{cases}$$

$$\boxed{S_n = \sum_{k=1}^{n} k2^k}$$

$S_n - S_{n-1} = 0$

$$\boxed{H_n = (an+b)2^n}$$

$2 \qquad -2$

$$(an+b)2^n - (a(n-1)+b)2^{n-1} \overset{?}{=} n2^n$$

$$2(an+b) - a(n-1) - b \overset{?}{=} 2n$$

$$2an + 2b - an + a - b = 2n$$

$$an + b + a = 2n$$

$a = 2 \qquad b = -2$

$$\boxed{S_n = (2n-2)2^n + c}$$

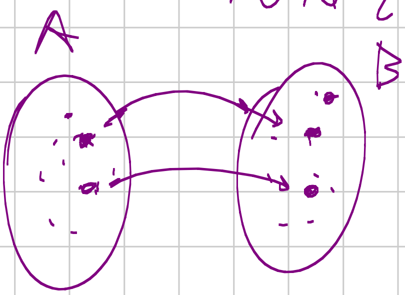
$S_1 = 2$

$$\boxed{S_n = (2n-2)2^n + 2}$$

$S_n - S_{n-1} = 0$

$S_n = S_{n-1}$

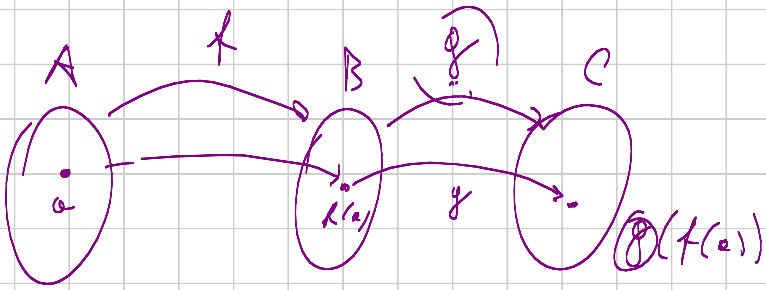
EQUAZIONI FUNZIONALI



iniettiva

suriettiva

biiettiva



$\cancel{g \circ f} : a \longrightarrow \boxed{g(f(a))}$

$g(f(a))$ è iniettiva $\Rightarrow$ f è iniettiva

$g(f(a))$ è suriettiva $\Rightarrow$ g è suriettiva

CAUCHY

$\boxed{f : \mathbb{Q} \to \mathbb{Q}}$ $\boxed{f(x+y) = f(x) + f(y)}$ $\boxed{\forall x, y \in \mathbb{Q}}$

$\mathbb{R}$

$\longrightarrow \boxed{f(x) = ax}$

1) f continua
2) f monotona
3) $\exists\, (a,b)$ e $\exists K$ t.c. $|f(x)| \le K$ $\forall x \in (a,b)$

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

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

$f(0) = 2f(0)$

$\Downarrow$

$\boxed{f(0) = 0}$

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

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

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

$f((x_1 + x_2 + \dots) + x_{n+1}) =$

$= f(x_1 + x_2 + \dots + x_n) + f(x_{n+1}) =$

$= f(x_1) + f(x_2) + \dots + f(x_n) + f(x_{n+1})$

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

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

3) $\boxed{f(n) = n f(1)}$?

$f(\underbrace{1+1+\dots+1}_{n}) = \underbrace{f(1) + f(1) + \dots + f(1)}_{n} = n f(1)$

4) $f\left(\frac{1}{n}\right) = \frac{1}{n} f(1)$??

$\boxed{f(1)} = f(\underbrace{\tfrac{1}{n} + \tfrac{1}{n} + \dots + \tfrac{1}{n}}_{n}) = \overbrace{f\left(\tfrac{1}{n}\right) + f\left(\tfrac{1}{n}\right) + \dots + f\left(\tfrac{1}{n}\right)}^{n}$

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

5) $\boxed{f\left(\frac{m}{n}\right) = \frac{m}{n} f(1)} \longleftarrow \boxed{\forall x \in \mathbb{Q} \quad f(x) = x f(1)}$

$f\left(\frac{m}{n}\right) = f(\overbrace{\tfrac{1}{n} + \tfrac{1}{n} + \dots + \tfrac{1}{n}}^{m}) =$

$$= \underbrace{f\left(\frac{1}{n}\right) + f\left(\frac{1}{n}\right) + \cdots + f\left(\frac{1}{n}\right)}_{m} =$$

$$= m\, f\left(\frac{1}{n}\right) = m \cdot \frac{1}{n} f(1) =$$

$$= \frac{m}{n} f(1)$$

$$\boxed{f(1) = a} \qquad \boxed{\forall x \in \mathbb{Q}} \quad f(x) = x \cdot f(1) = \boxed{a x}$$

$$\underline{f(x+y) = f(x) + f(y)}$$

$$\underline{f(x_1 + x_2 + \cdots + x_n) = f(x_1) + f(x_2) + \cdots + f(x_n)}$$

$$f\left((x_1 + x_2 + \cdots + x_n) + x_{n+1}\right) = \underline{f(x_1 + \cdots + x_n)} + f(x_{n+1})$$

$$= f(x_1) + f(x_2) + \cdots + f(x_n) + f(x_{n+1})$$

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

$$f(x + f(y)) = f(x) + f(y) \qquad \underline{\text{iniettive}}$$

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

$\forall x, y \in \mathbb{R}$ $\quad f(x + f(y)) = f(y + f(x))$

$\Downarrow \leftarrow$ in.

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

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

$f(x) - x =$ costante

$\boxed{f(x) = \text{costante} + x}$ $\quad f(x) = c + x$

$f(x) = 2011 + x$

$f(x) = \lfloor x \rfloor$ $\quad f(x + f(y))$ $\quad f(x) + f(y)$

$\lfloor x + \lfloor y \rfloor \rfloor = \lfloor y \rfloor + \lfloor x \rfloor$

$f(x+f$

$\boxed{f(x) = x + \lfloor x \rfloor}$

$f(x) \equiv 0$

$f(y) = a \neq 0$

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

$$f(x+a) = f(x) + a \qquad \forall x$$

$$f(x+2a) = f((x+a)+a) = f(x+a) + a = f(x)+2a$$

$$f(x+3a) = \dots = f(x) + 3a$$

$$\vdots$$

$$f(x+na) = f(x) + na$$

C 1 - BASIC Luigi

Titolo nota 04/09/2012

COMBINATORIA =

= "CONTARE"

Es 1: ~~Fattori~~ divisori di un n.

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

div. di n: $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$

$$\underbrace{(\alpha_1+1)\cdot(\alpha_2+1)\cdot\ldots\cdot(\alpha_k+1)}$$

$$|A| = n, \quad |B| = m$$

$$|A \times B| = n \cdot m$$

$$f(a) = b \land f(a) = c \Rightarrow b = c$$

$$A = \{1, 2, 3, 4, \ldots, 10\}$$

$$B = \{a, b, c, d\}$$

$$\underbrace{4 \cdot 4 \cdot \ldots \cdot 4}_{10} = 4^{10} = |B|^{|A|}$$

Es. QUANTE SONO LE FUNZ "INIETTIVE"

da A a B?

$(a, a, b, c \ldots)$

$|A| > |B|$ NESSUNA!

$|A| \leq |B|$

$|A| = \{1, 2, 3\}$ 1 < 4 sc.

$|B| = \{a, b, c, d\}$ 2 < 3 sc.

3 < 2 sc.

$|A| = n$

$|B| = m$ $\underline{\underline{n \leq m}}$

$m \cdot (m-1) \cdot (m-2) \cdot \ldots \cdot (m-n+1)$

FATTORIALE!

$n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$

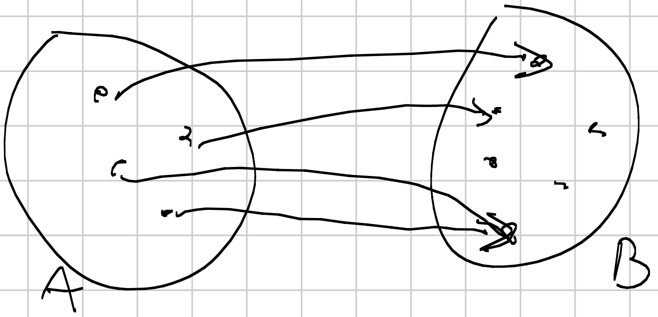
$2! = 2$ $4! = 24$

$3! = 6$ $5! = 120$

$$m \cdot (m-1) \cdot \ldots \cdot (m-n+1) =$$

$$= \frac{m \cdot (m-1) \cdot \ldots \cdot (m-n+1) \cdot (m-n) \cdot \ldots \cdot 1}{(m-n) \cdot \ldots \cdot 1} =$$

$$= \frac{m!}{(m-n)!}$$



Una funz. da A a B può essere

<u>BIIETTIVA</u> SE E SOLO SE $|A| = |B|$

Se $|A| = |B| = n$, le funz. biiett. da A a B sono $n!$

<u>N.B.: $0! = 1$</u>

Es. In una classe di 30 persone devo scegliere 3 stud. da mandare in gita. In quanti modi posso farlo?

$$\binom{30}{3} = \frac{30 \cdot 29 \cdot 28}{3 \cdot 2 \cdot 1} = \frac{30!}{3! \cdot 27!}$$

Def. COEFFICIENTE BINOMIALE

$\binom{n}{k}$ = "i modi di scegliere k oggetti da un insieme di n el."

$$= \frac{n!}{k!(n-k)!} \qquad \underline{0 \leq k \leq n}$$

- $\binom{n}{k}$ è SEMPRE INTERO
- RICORRENZA:

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

- SIMMETRIA:

$$\binom{n}{k} = \binom{n}{n-k}$$

• BINOMIO DI NEWTON

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

"DIM"

$$\underbrace{(a+b)\cdot(a+b)\cdot \ldots \cdot(a+b)}_{n}$$ SCELGO k "a" ...

$\square$

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

$$\sum_{k=0}^{n} \binom{n}{k} \cancel{\cdot 1^k \cdot 1^{n-k}}$$

ES. QUANTI SONO I SOTTOINSIEMI DI UN INSIEME A con $|A| = n$?

$$\binom{n}{0} = 1$$

$$\binom{n}{1} = n \quad \ldots \quad \binom{n}{n} = 1$$

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

$$|P(A)| = 2^{|A|}$$

IL TRIANGOLO DI TARTAGLIA (PASCAL)

$$
\begin{array}{ccccccccccccl}
 & & & & & 1 & & & & & & & \leftarrow n=0 \\
 & & & & 1 & & 1 & & & & & & \leftarrow n=1 \\
 & & & 1 & & 2 & & 1 & & & & & \leftarrow n=2 \\
 & & 1 & & 3 & & 3 & & 1 & & & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & & & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 & & \leftarrow n=5 \\
 & & & & & & & & & & -- & &
\end{array}
$$

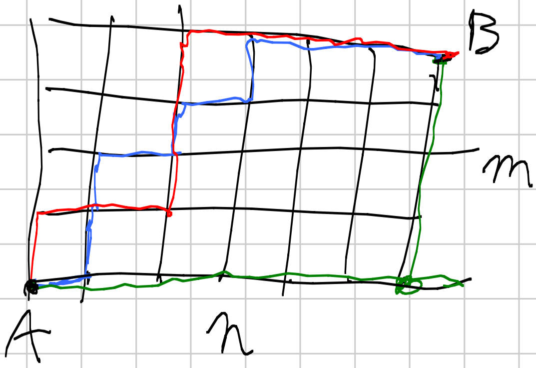
$\nearrow$ $k=0$ $\quad$ $k=1$ $\quad$ ....

$$\sum_{n=k}^{k+t} \binom{n}{k} = \binom{k+t+1}{k+1}$$

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

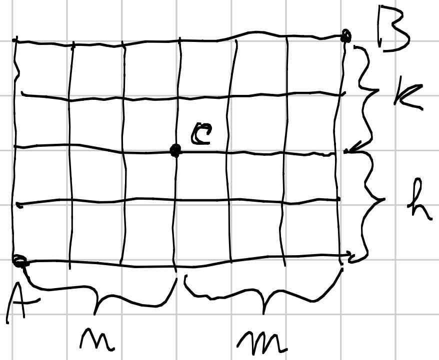
$$(-1+1)^n = 0^n = 0$$

Percorsi su un reticolo



Quanti perc. da A a B?

$$\binom{n+m}{n} = \binom{n+m}{m}$$



Quanti sono i perc. da A a B per C?

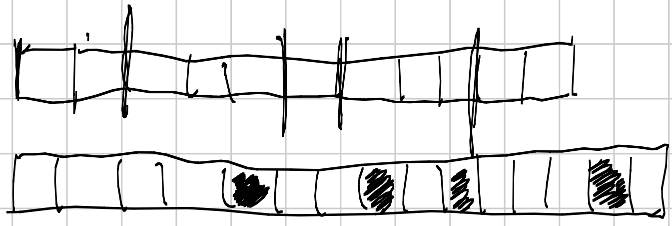
$$\binom{n+h}{n} \cdot \binom{m+k}{m}$$

Partizioni di un intero

$n \in \mathbb{N}$

In quanti modi posso trovare $(a_1, \dots, a_k)$ t.c.

$a_1 + a_2 + \dots + a_k = n$ $a_1, \dots, a_k \geq 0$



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

Pb. Se volessi $a_i \geq 1$

$$\binom{n + \cancel{k} - 1 - \cancel{k}}{k-1} = \binom{n-1}{k-1}$$

Se invece $a_i \geq 2$

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

ANAGRAMMI

- Q.S. GLI ANAGR. DI "CIAO"?

  FACILE! $4!$

- Q.S. GLI ANAGR. DI "ABRACADABRA"?

  COEFF. MULTINOMIALE

$$\frac{11!}{5! \cdot 2! \cdot 2!} = \binom{11}{5\ 2\ 2}$$

$$\binom{a}{b} = \binom{a}{b \quad a-b}$$

$$\binom{n}{k_1, \dots, k_m} = \# \text{ Partiz. di } n \text{ in } k_i\text{-insiemi}$$

$$\sum_i k_i = n$$

---

11 GIOCATORI

1P, ~~2~~4 D, 4C, 2A ?

$$\binom{11}{1} \cdot \binom{10}{\cancel{4}\,4} \cdot \binom{6}{4} \cdot \binom{2}{2} = \binom{11}{1 \quad 4 \quad 4 \quad 2}$$

ES. Un gioc. non può andare in porta.

Quante formazioni?

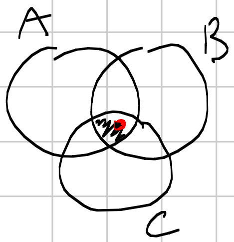
C 2 Basic

Titolo nota 07/09/2012

Principio di Inclusione Esclusione

$$\#\{A \cup B\} = \#A + \#B - \#A \cap B$$

$$\#\{A \cup B \cup C\} = \#A + \#B + \#C - \#A \cap B - \#A \cap C - \#B \cap C$$
$$+ \# A \cap B \cap C$$



$$\# \bigcup_{i=1}^{n} A_i = \sum_{i=1}^{n} \# A_i - \sum_{\substack{i,j \\ i<j}} \# A_i \cap A_j + \dots$$

$$= \sum_{k=1}^{n} (-1)^{k+1} \# \bigcap_{k \text{ insiemi}}$$

Funzioni Suriettive

Permutazioni Su $\{1 \dots n\}$ sono $n!$

Si indicano con σ, τ

$$\sigma = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 1 & 2 \end{matrix} \qquad \tau = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 4 & 1 & 5 \end{matrix} \qquad \sigma \circ \tau = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 5 & 6 & 3 & 1 \end{matrix}$$

$$\sigma \circ \tau \neq \tau \circ \sigma$$

- trasposizioni $\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 5 & 6 \end{matrix}$

- cicli $\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{matrix}$ $\quad (1\,2\,3\,4\,5\,6) \quad (1\,2\,3)\ (5\,6)$ $\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{matrix}$

Prop: Ogni permutazione può essere scritta come prodotto di cicli disgiunti in modo unico a meno dell'ordine.

$a_1 \curvearrowright a_2 \curvearrowright a_3$ $\qquad a_k = a_h \qquad h < k$

"prima o poi si ripete"

Per il principio del minimo intero $\exists$ il più piccolo k per cui vale.

$\boxed{h = 1}$ Abbiamo detto che sono iniettive.
Supponiamo p. ass. $k > h > 1$

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

σ iniettiva $\Rightarrow a_{k-1} = a_{h-1}$
ma questo andrebbe contro la minimalità di k ⚡

Per dimostrarlo procediamo per induzione

$$\sigma = (a_1 \ldots a_{k-1})\,\tilde{\sigma}$$

Vale anche l'unicità.

Esempio

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 3 & 11 & 5 & 8 & 1 & 9 & 10 & 7 & 4 & 2 & 12 \end{matrix}$$

$$(1\,6)\,(2\,3\,11)\,(4\,5\,8\,10)\,(7\,9)\,(12)$$

Prop? Possiamo scrivere ogni permutazione come prodotto di trasposizioni? SI

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

σ permut. su $\{1 \dots n\}$

- $\operatorname{sgn}(\sigma) \in \{-1, +1\}$
- il segno conta la parità del numero di inversioni cioè $i < j$ e $\sigma(i) > \sigma(j)$

Lemma $\quad \operatorname{sgn}(\sigma \circ \tilde{\sigma}) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tilde{\sigma})$

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

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

■

Come dimostriamo la proposizione?

BdC ogni ciclo è prodotto di trasposizioni e segno.

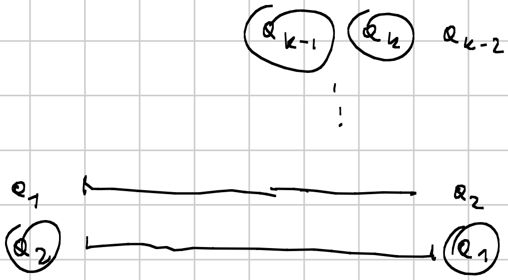
Caso $k = 3 \qquad (a_1\, a_2\, a_3) = (a_1 a_2) \circ (a_2\, a_3)$

$$\begin{array}{lccc} & a_1 & a_2 & a_3 \\ (a_2 a_3) & a_1 & a_3 & a_2 \\ (a_1 a_2) & a_2 & a_3 & a_1 \end{array} \quad (a_1\, a_2\, a_3)$$

In generale $\quad (a_1 \dots a_k) = (a_1 a_2)(a_2 a_3) \dots (a_{k-2} a_{k-1})(a_{k-1} a_k)$

$a_1 \; a_2 \; \dots \; a_{k-2} \; a_{k-1} \; a_k$

$a_k \; a_{k-1}$

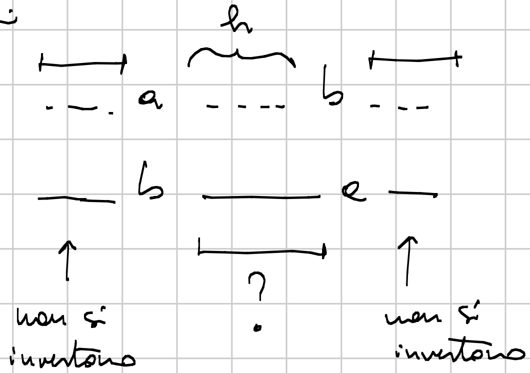


E il segno? Dipende solo dal numero di trasposizioni

Se abbiamo $2h$ trasp. $\longrightarrow$ sgn $= +1$

" " $2h+1$ " $\longrightarrow$ sgn $= -1$

Ogni trasposizione contribuisce un n.ro dispari di inversioni



Quante inversioni ci sono in mezzo? $h \geq 0$

Se tra a e b ci sono h el.ti le inversioni sono h con a e h con b, quindi $2h$ e a ci aggiungiamo lo scambio a con b, per un totale di $2h+1$ inversioni

<u>Allora</u> $$\underset{\text{ciclo di lungh. } k}{(a_1 \dots a_k)} = \underbrace{(a_1 a_2)(a_2 a_3) \dots (a_{k-1} a_k)}_{k-1 \text{ trasp}}$$

Un ciclo di lunghezza pari è DISPARI

" " " " dispari è PARI

Permutazioni senza punti fissi

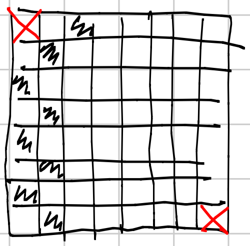
Quelle con almeno un p.to fisso sono $\binom{n}{1}(n-1)!$
ma abbiamo tolto 2 volte quelle con esattamente
2 p.ti fissi.
Dobbiamo andare a contare quelle con almeno 2 p.ti
fissi che sono $\binom{n}{2}(n-2)!$

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

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

$$n! \Big(\underbrace{\cancel{1} - \cancel{1} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} + \dots + (-1)^n \frac{1}{n!}}_{\sim \frac{1}{e}} \Big) \simeq \frac{n!}{e}$$

Colorazioni e Invarianti



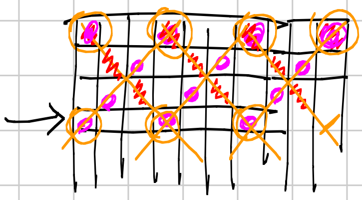
si può ricoprire? NO

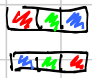
62 caselle 32 B 30 N

ma o

2. Scacchiera 10 × 10 33

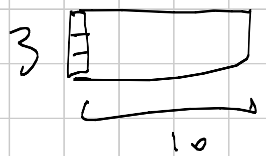
Dove può essere il quadratino scoperto?

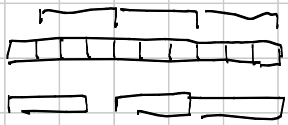




34 R

33 B 33 V



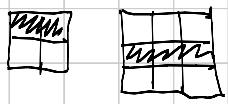


3. Scacchiera 101 × 101 con tasselli 2 × 2 o 3 × 3

$$101^2 = 4x + 9y$$

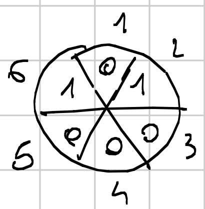
Coloriamo a strisce orizzontali bianche e nere

Ci sono 101 bianche in più



Se mettiamo una 3 × 3 copriamo 3 bianche in +
ma 101 non è multiplo di 3.

→ Invarianti caselle in $\{0, 1, \ldots\}$



· aumento 2 adiacenti di 1

· diminuisco 2 adiacenti di 1

$\sum$ Posti dispari − $\sum$ posti pari è invariante

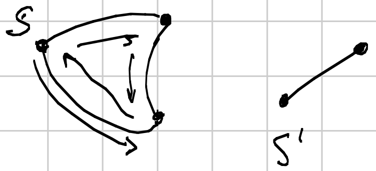
Non è possibile.

- Ci sono 12 amici che hanno magliette R e N. Cambiano secondo maggioranza

  Invariante coppie di colori diversi.

GRAFI

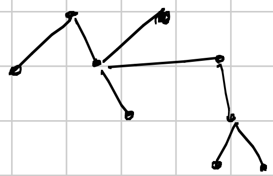
vertici e archi



* grafo connesso

* ciclo

– Albero grafo connesso SENZA cicli.



se tolgo un arco sconnetto

se aggiungo un arco ciclo

- Ogni albero ha almeno una foglia (i.e. vertice con un solo arco)

P. ass. ci sarebbe un ciclo

Formula: $V = E + 1$

Dim: per induzione Base • : $1 = 0 + 1$ ✓

passo induttivo:

passo con aggiungere NO

Togliamo un vertice, in particolare una foglia
entra in gioco l'ipotesi induttiva ✓

Esempio: Un labirinto 2012 × 2012 porte tra stanze adiacenti.

Quante possono essere al più le porte chiuse per poter arrivare da ogni stanza ad ogni altra stanza?

$2012 \times 2011 \times 2$: totale porte

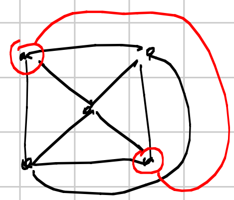
Quante devono essere aperte? stanze $- 1$

Le stanze sono 2012×2012

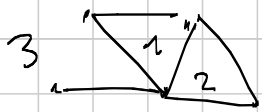
Quindi $2012 \times (2011 \times 2 - 2012) + 1$

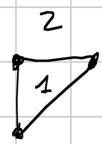
Grafi planari (connessi)

non ci sono archi che si intersecano



$$V + F = S + 2$$





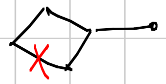
Per induzione sul numero di archi o spigoli S
non $\emptyset$!

Base: • : $1 + 1 = 0 + 2$ ✓

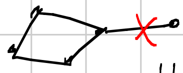
$n \geq 0$

Passo: supponiamo sia vero per tutti $S \leq n$
vogliamo che valga per $S = n+1$

Togliamo un arco: → non sconnettiamo
→ sconnettiamo



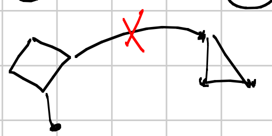
non sconnetto



sconnetto

- non sc. abbiamo un arco in meno e una faccia in meno ✓

- sconnetto ① ②



$$V_1 + F_1 = S_1 + 2 \qquad V_2 + F_2 = S_2 + 2$$

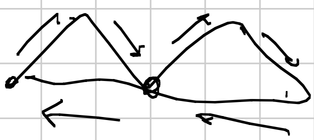
sommiamo

$$(V_1+V_2) + (F_1+F_2) = (S_1+S_2) + 4$$

$$V_1+V_2 = V, \quad F_1+F_2 = F+1, \quad S_1+S_2 = S-1$$

$$V + F = S + 2 \qquad \blacksquare$$

- Cammini chiusi su grafi planari connessi Euleriani



Un grafo planare connesso ammette un cammino chiuso sse # archi in uscita è pari per ogni vertice

[⇒] ogni volta che entro in un vertice devo uscire ✓

[$\Leftarrow$] partiamo con il nostro cammino prima o poi torniamo in un vertice già visto

* se è quello iniziale ✓
* se è intermedio devo uscirne per parità ma il numero di archi è finito

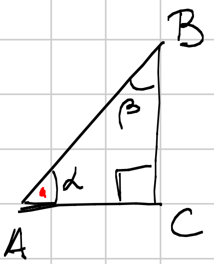
quindi prima o poi torno all'origine.

TRIGONOMETRIA (G1 basic)

Titolo nota 03/09/2012

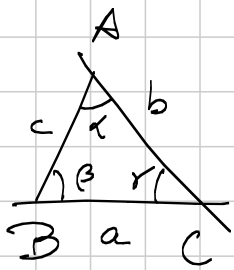
Sam

G1 – Trigo
G2 – metodi analitici
G3 – sintetica



$\gamma = 90^\circ$

$\alpha + \beta = 90^\circ$



$$\cos\alpha = \frac{AC}{AB} = \frac{b}{c} = \frac{\text{CATETO ADIACENTE}}{\text{IPOTENUSA}}$$

$$\sin\alpha = \frac{BC}{AB} = \frac{a}{c} = \frac{\text{CATETO OPPOSTO}}{\text{IPOTENUSA}}$$

$$\cos\beta = \frac{\text{CAT. AD}}{\text{IP.}} = \frac{BC}{AB} \qquad \sin\beta = \frac{\text{CAT. OP}}{\text{IP}} = \frac{AC}{AB}$$

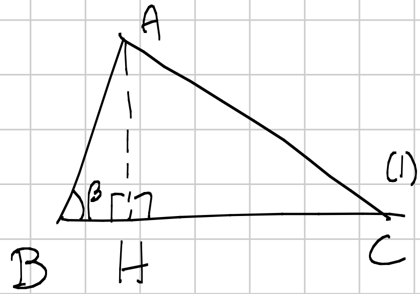
$$\boxed{\cos(90^\circ - \theta) = \sin\theta \qquad \sin(90^\circ - \theta) = \cos\theta}$$

$$Tg\,\alpha = \frac{\text{CAT. OP}}{\text{CAT. AD}} = \frac{BC}{AC} = \frac{\sin\alpha}{\cos\alpha} \qquad \text{TANGENTE}$$

$$Tg\,\beta = \frac{AC}{BC} = \frac{\sin\beta}{\cos\beta} = \frac{\cos\alpha}{\sin\alpha} = \frac{1}{Tg\,\alpha} := \cot\alpha$$

COTANGENTE

$$Tg(90^\circ - \alpha) = \cot\alpha$$



$AH = ?$

(I) Tri. rett. $\overset{\triangle}{BHA}$ $\quad B\hat{H}A = 90°$

$A\hat{B}H = \beta$

$B\hat{A}H = 90° - \beta$

$\frac{AH}{BA} = \sin\beta \implies AH = c \cdot \sin\beta$

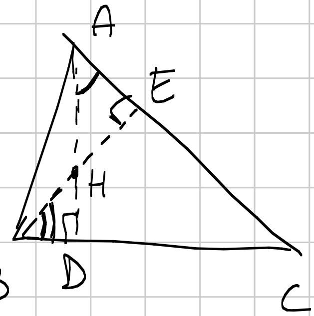
(II) Tri. rett. $\overset{\triangle}{AHC}$

$AH = b \cdot \sin\gamma$

$BH = c \cdot \cos\beta$

$CH = b \cdot \cos\gamma$

•)



AD, BE altezze, H ortocentro

$AH = ?$

in $\overset{\triangle}{AHE}$, $\quad A\hat{E}H = 90°$

$H\hat{A}E = D\hat{A}C = 90° - A\hat{C}D = 90° - \gamma$

$$\underbrace{\cos(H\hat{A}E)}_{\substack{\| \\ \cos(90°-\gamma) \\ \| \\ \sin\gamma}} = \frac{AE}{AH} = \frac{c \cdot \cos\alpha}{AH}$$

$$AH = c \cdot \frac{\cos\alpha}{\sin\gamma}$$

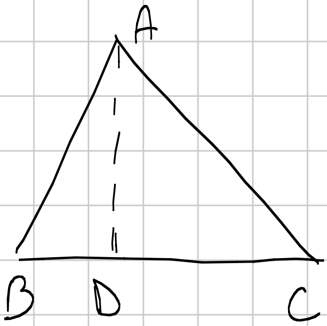
$$\boxed{HD = AD - AH = b \cdot \sin\gamma - c \cdot \frac{\cos\alpha}{\sin\gamma}}$$

in $\overset{\triangle}{BDH}$ $\quad B\hat{D}H = 90°$

$\frac{HD}{BD} = \operatorname{Tg} H\hat{B}C = \operatorname{Tg}(90° - \gamma) = \cot\gamma$

$BD = c \cdot \cos\beta$

$HD = \cot\gamma \cdot c \cdot \cos\beta$

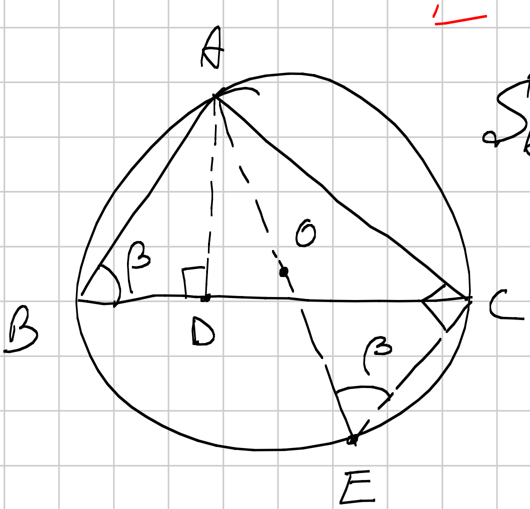


$$S_{ABC} = \frac{1}{2} BC \cdot AD = \boxed{\frac{1}{2} ac \cdot \sin\beta}$$

$$= \boxed{\frac{1}{2} ab \cdot \sin\gamma}$$

$$= \frac{1}{2} bc \cdot \sin\alpha$$

$$S_{ABC} = \frac{abc}{4R}$$



$$S_{ABC} = \frac{1}{2} BC \cdot AD$$

$A\hat{C}E = 90°$

$A\hat{E}C = \beta$

$\overset{\triangle}{ABD} \simeq \overset{\triangle}{AEC}$ simili

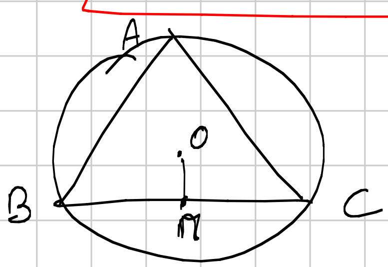
$$\frac{AD}{AC} = \frac{AB}{AE} \qquad AD = \frac{AB \cdot AC}{AE} = \frac{c \cdot b}{2R}$$

$$S = \frac{1}{2} \, \frac{a \cdot c \cdot b}{2R} = \frac{abc}{4R}$$

Teo dei Seni : $S_{ABC} = \frac{1}{\cancel{2}} \cancel{ab} \sin\gamma = \frac{\cancel{ab}c}{\cancel{4}R}$ 2

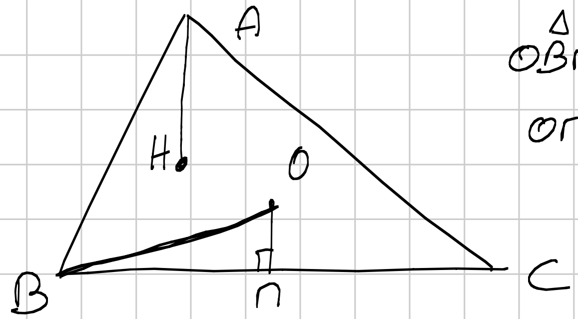
$$\Rightarrow \boxed{\sin\gamma = \frac{c}{2R}}$$

o)



M = pt. medio di BC

OM = ?



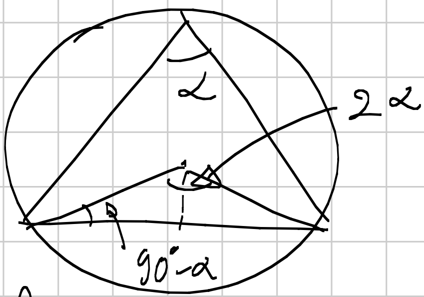
$\overset{\triangle}{OBM}$

$OM = OB \cdot \sin O\hat{B}M =$

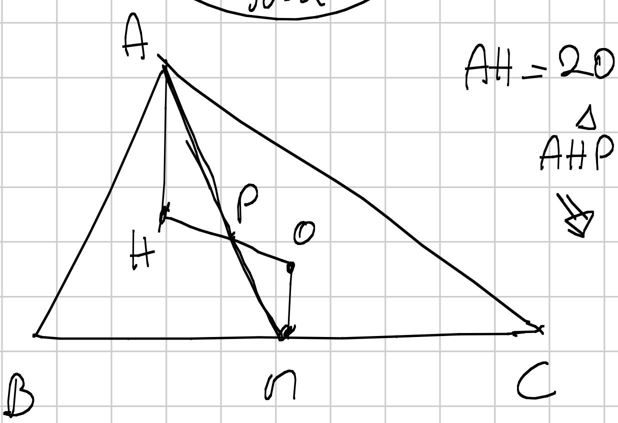
$= R \cdot \sin(90 - \alpha) = R \cos\alpha$

$AH = c \cdot \dfrac{\cos\alpha}{\sin\gamma} = 2R\cos\alpha$

$\underbrace{\dfrac{c}{\sin\gamma}}_{2R}$ Teo del seno



$AH = 2OM$



$AH = 2OM$

$\overset{\triangle}{AHP} \simeq \overset{\triangle}{POM}$

$\Rightarrow AP = 2PM$

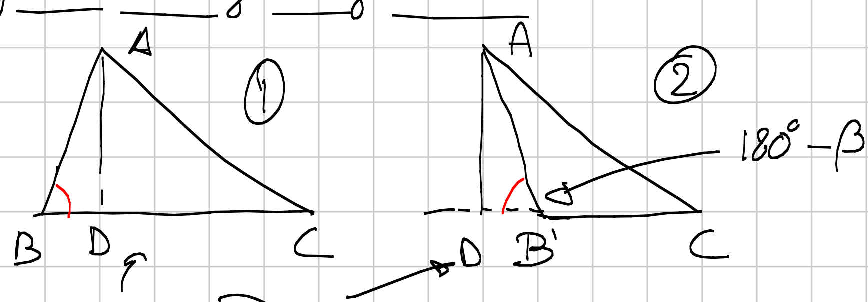
$\Rightarrow$

$P = G$ baricentro

$\Rightarrow H, G, O$ allineati in quest'ordine

con $HG = 2 \cdot GO$

<u>Digressione sugli angoli ottusi</u>



$BD = B'D$

$AD = AD$

$DC = DC$

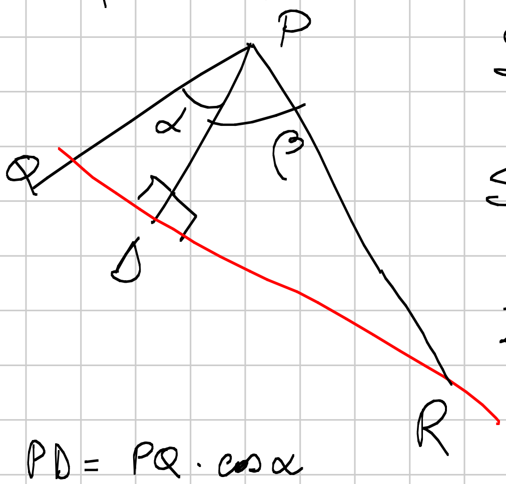
① $BD + DC = BC$

② $DC - B'D = B'C$

$$\sin(180^\circ-\beta)=\sin\beta \qquad ① \quad c\cdot\cos\beta+b\cdot\cos\gamma=a$$

$$\cos(180^\circ-\beta)=-\cos\beta$$

•) $\alpha,\beta \quad \alpha+\beta<180^\circ$



$$S_{PQR}=\frac{1}{2}PQ\cdot PR\cdot\sin(\alpha+\beta)$$

$$\parallel$$

$$S_{PQD}+S_{PDR}=\frac{1}{2}PR\cdot PD\cdot\sin\beta$$

$$S_{PQD}=\frac{1}{2}PQ\cdot PD\cdot\sin\alpha=\frac{1}{2}PQ\cdot PR\cdot\cos\beta\cdot\sin\alpha$$

$$\frac{1}{2}PR\cdot PD\cdot\sin\beta=\frac{1}{2}PR\cdot PQ\cdot\cos\alpha\sin\beta$$

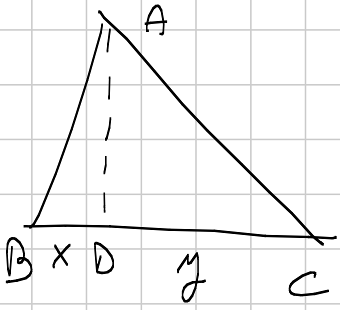
$$PD=PQ\cdot\cos\alpha$$
$$PD=PR\cdot\cos\beta$$

$$\cancel{\frac{1}{2}PQ\,PR}\cdot\sin(\alpha+\beta)=\cancel{\frac{1}{2}PQ\cdot PR}\cos\alpha\sin\beta+\cancel{\frac{1}{2}PQ\,PR}\sin\alpha\cos\beta$$

$$\boxed{\sin(\alpha+\beta)=\sin\alpha\cos\beta+\cos\alpha\sin\beta}$$

$$\boxed{\sin(\alpha-\beta)=\sin\alpha\cos\beta-\cos\alpha\sin\beta}$$

•)



$$AD^2=AB^2-BD^2$$
$$AD^2=AC^2-DC^2$$

$$\begin{cases}c^2-b^2=x^2-y^2\\ x+y=a\end{cases}\qquad\begin{cases}c^2-b^2=a(x-y)\\ a=x+y\end{cases}$$

$$\begin{cases}x+y=a\\ x-y=\dfrac{c^2-b^2}{a}\end{cases}\qquad\begin{cases}x=\dfrac{1}{2}\left(a+\dfrac{c^2-b^2}{a}\right)\\ y=\dfrac{1}{2}\left(a-\dfrac{c^2-b^2}{a}\right)\end{cases}$$

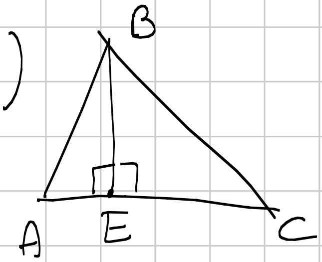
$$\begin{cases} x = \dfrac{a^2+c^2-b^2}{2a} \\ y = \dfrac{a^2-c^2+b^2}{2a} \end{cases} \qquad \begin{aligned} x &= c\cdot\cos\beta \\ y &= b\cdot\cos\gamma \end{aligned}$$

$$c\cdot\cos\beta = \frac{a^2+c^2-b^2}{2a}$$

Teo del Coseno: (di Carnot) $\boxed{\cos\beta = \dfrac{a^2+c^2-b^2}{2ac}}$

$$b^2 = a^2+c^2-2ac\cdot\cos\beta$$ Pitagora generalizzato.

a)



$$AB^2+BC^2 = AE^2+EB^2+EB^2+EC^2 =$$
$$= AE^2+EC^2+2EB^2 = AC^2-2AE\cdot EC+2EB^2 =$$
$$= AC^2-2AB\cdot\cos\alpha\cdot BC\cos\gamma+2AB\cdot BC\cdot\sin\alpha\cdot\sin\gamma$$
$$= AC^2-2AB\cdot BC\,(\cos\alpha\cos\gamma-\sin\alpha\sin\gamma)$$

$$EB = AB\cdot\sin\alpha$$
$$EB = BC\cdot\sin\gamma$$

$$c^2+a^2+2ac\,(\cos\alpha\cos\gamma-\sin\alpha\sin\gamma) = b^2$$

$$c^2+a^2-2ac\cos\beta = b^2$$

$$-\cos\beta = \cos\alpha\cos\gamma-\sin\alpha\sin\gamma$$

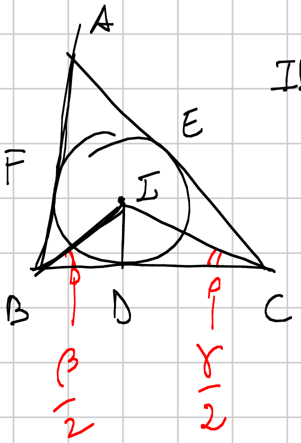
$$\|$$

$$-\cos(180°-(\alpha+\gamma))$$

$$\|$$

$$\cos(\alpha+\gamma)$$

$$\boxed{\cos(\alpha+\gamma) = \cos\alpha\cos\gamma-\sin\alpha\sin\gamma}$$
$$\boxed{\cos(\alpha-\gamma) = \cos\alpha\cos\gamma+\sin\alpha\sin\gamma}$$



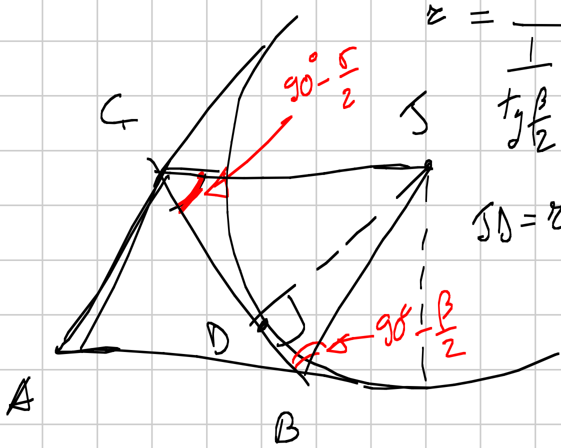
$$ID = r = ?$$

$$\operatorname{Tg}\frac{\beta}{2} = \frac{ID}{BD} \qquad \operatorname{Tg}\frac{\gamma}{2} = \frac{ID}{DC}$$

$$BD = \frac{ID}{\operatorname{Tg}\frac{\beta}{2}} \qquad DC = \frac{ID}{\operatorname{Tg}\frac{\gamma}{2}}$$

$$a = \frac{r}{\operatorname{Tg}\frac{\beta}{2}} + \frac{r}{\operatorname{Tg}\frac{\gamma}{2}}$$

$$r = \frac{a}{\frac{1}{\operatorname{tg}\frac{\beta}{2}} + \frac{1}{\operatorname{tg}\frac{\gamma}{2}}} = \frac{a}{\cot\frac{\beta}{2} + \cot\frac{\gamma}{2}}$$



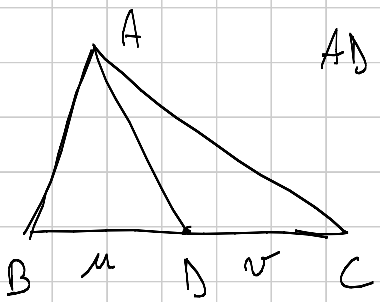
$$JD = r_a$$

$$a = \frac{r_a}{\operatorname{Tg}(90^\circ - \frac{\gamma}{2})} + \frac{r_a}{\operatorname{Tg}(90^\circ - \frac{\beta}{2})} =$$

$$= \frac{r_a}{\cot\frac{\gamma}{2}} + \frac{r_a}{\cot\frac{\beta}{2}}$$

$$r_a = \frac{a}{\frac{1}{\cot\frac{\gamma}{2}} + \frac{1}{\cot\frac{\beta}{2}}} = \frac{a}{\operatorname{tg}\frac{\beta}{2} + \operatorname{tg}\frac{\gamma}{2}}$$

•)



AD = ~~retta~~ a CASO ceviana

$BD = u$

$DC = v$

$AD = ?$

$u + v = a$

in $\overset{\triangle}{ABD}$, $\widehat{ABD} = \beta$, $AB = c$, $BD = u$

$$AD^2 = c^2 + u^2 - 2c\cdot u\cdot \cos\beta \qquad \text{(Teo di Carnot)}$$

In $\overset{\Delta}{ABC}$ $\qquad \cos\beta = \dfrac{c^2+a^2-b^2}{2ac} \qquad$ (Teo di Carnot)

$$AD^2 = c^2+u^2-\cancel{2}\cancel{c}\,u\left(\frac{c^2+a^2-b^2}{\cancel{2}a\cancel{c}}\right) = \qquad a = u+v$$

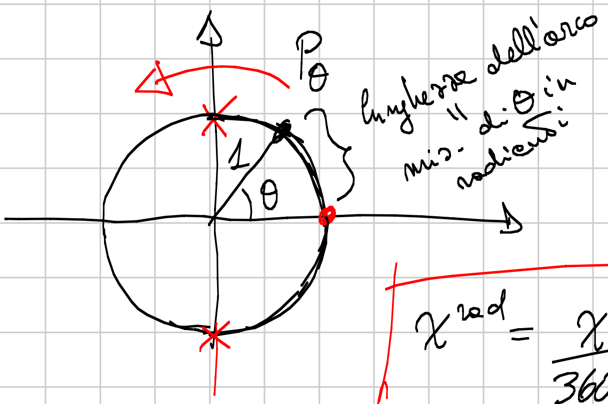
$$= c^2+u^2-u\left(\frac{c^2+u^2+v^2+2uv-b^2}{u+v}\right) =$$

$$= \frac{\cancel{uc^2}+vc^2+\cancel{u^3}+\cancel{u^2v}-\cancel{uc^2}-\cancel{u^3}-uv^2-\cancel{2}u^2v+ub^2}{u+v} =$$

$$AD^2 = \boxed{\frac{ub^2+vc^2-uv(u+v)}{u+v}} = \boxed{\frac{ub^2+vc^2}{u+v}-uv}$$

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

Teo di STEWART



$360°$	2π
$0°$	0

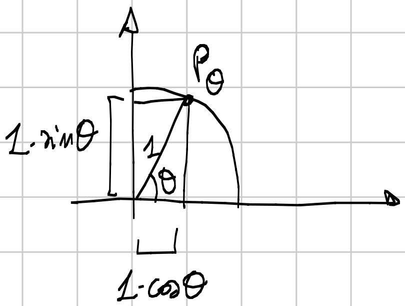
$$\frac{x°}{360°} = \frac{x^{rad}}{2\pi}$$

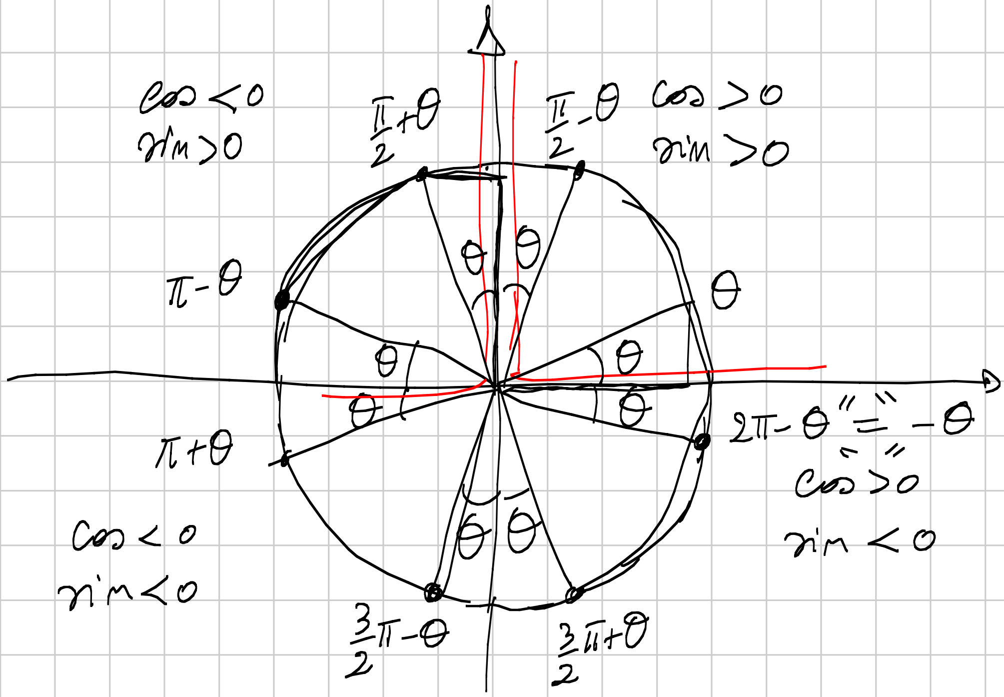
$$\boxed{x^{rad} = \frac{x°}{360°}\cdot 2\pi}$$

Es:

rad	deg
0	0°
$\pi/6$	30°
$\pi/4$	45°
$\pi/3$	60°
$\pi/2$	90°

$P_\theta = (\cos\theta, \sin\theta)$





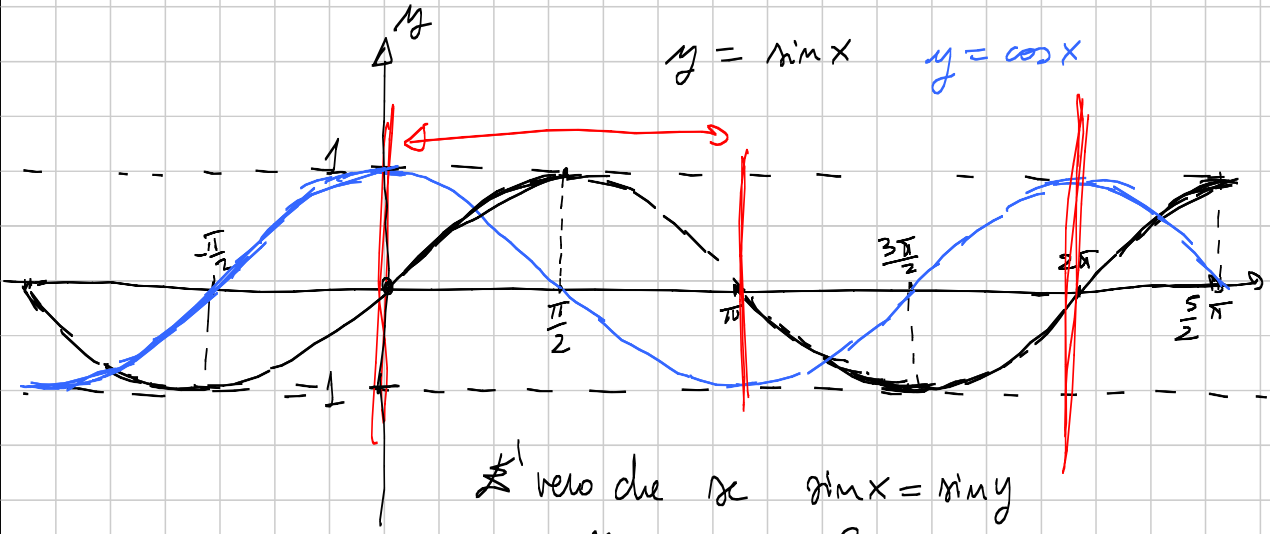
$$\sin\left(\frac{\pi}{2}+\theta\right) = \cos\theta$$

$$\cos\left(\frac{3}{2}\pi-\theta\right) = -\cos\left(\frac{3}{2}\pi+\theta\right)$$

$$\boxed{\sin(x) = \sin(x+2\pi) \quad \forall x \in \mathbb{R}}$$

$$\cos(x) = \cos(x+2\pi) \quad \forall x \in \mathbb{R}$$

SENO e COSENO hanno periodo 2π



È vero che se $\sin x = \sin y$ allora $x = y$?

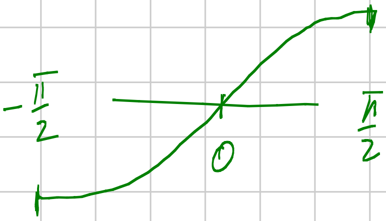
no, nemmeno come angolo

E se $0 \le x,y \le \pi$? Nemmeno.

Se $0 \le x,y \le \frac{\pi}{2}$ e $\sin x = \sin y \implies x = y$

Se $-\frac{\pi}{2} \le x,y \le \frac{\pi}{2}$ e $\sin x = \sin y \implies x = y$

$\left(\frac{\pi}{2} \le x,y \le \frac{3}{2}\pi\right)$

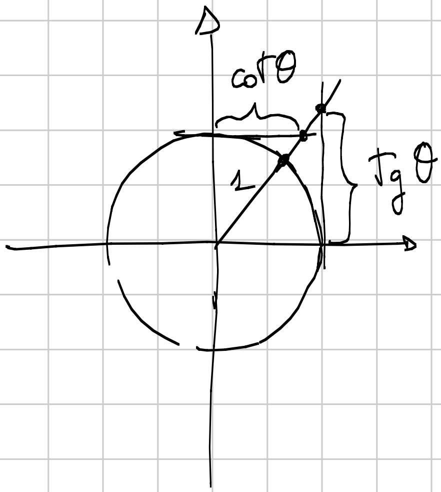


Su $\left[-\frac{\pi}{2} + 2k\pi, \frac{\pi}{2} + 2k\pi\right]$ $\sin(x)$ è monotona crescente

$\implies$ iniettiva

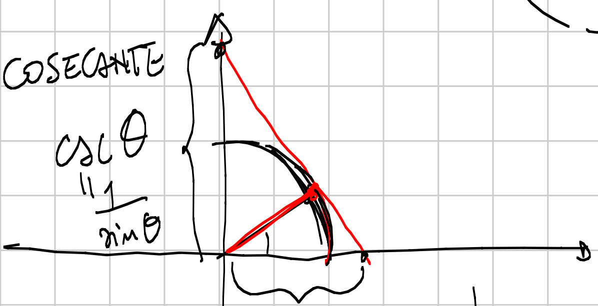
Su $\left[\frac{\pi}{2}+2k\pi, \frac{3}{2}\pi+2k\pi\right]$ $\sin(x)$ è monotona decrescente $\rightarrow$ iniettiva.

$$\mathrm{Tg}\,\theta = \frac{\sin\theta}{\cos\theta}$$



COSECANTE

$\csc\theta = \frac{1}{\sin\theta}$



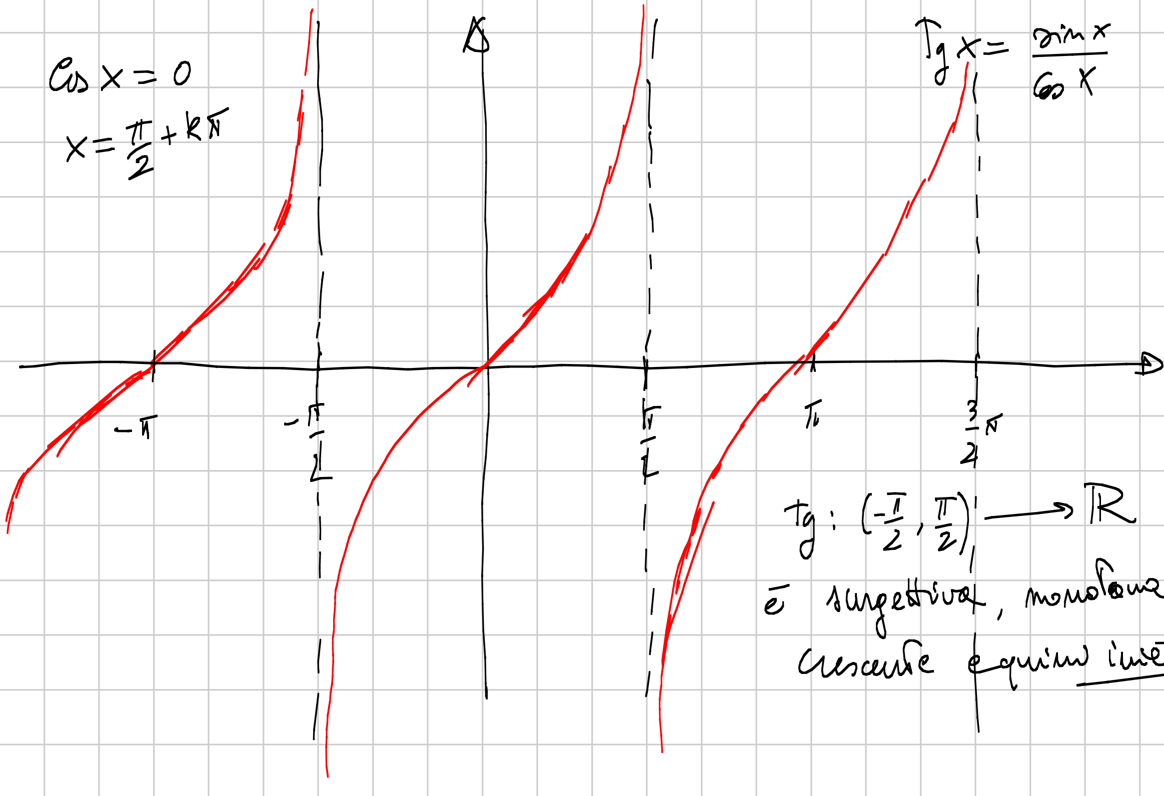
$\sec\theta = \frac{1}{\cos\theta}$

SECANTE

$\cos x = 0$

$x = \frac{\pi}{2} + k\pi$

$\mathrm{Tg}\,x = \frac{\sin x}{\cos x}$



$\mathrm{Tg}: \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \longrightarrow \mathbb{R}$

è surgettiva, monotona crescente e quindi iniettiva

" Tg é iniettiva su $\left[0, \frac{\pi}{2}\right) \cup \left(\frac{\pi}{2}, \pi\right]$

Formule di ADDIZIONE e SOTTRAZIONE

$$\cos(x+y) = \cos x \cos y - \sin x \sin y$$
$$\cos(x-y) = \cos x \cos y + \sin x \sin y$$
$$\sin(x+y) = \sin x \cos y + \cos x \sin y$$
$$\sin(x-y) = \sin x \cos y - \cos x \sin y$$

$$Tg(x+y) = \frac{\sin(x+y)}{\cos(x+y)} = \frac{\sin x \cos y + \cos x \sin y}{\cos x \cos y - \sin x \sin y} =$$

$$= \frac{\frac{\sin x}{\cos x} + \frac{\sin y}{\cos y}}{1 - \frac{\sin x \sin y}{\cos x \cos y}} = \frac{Tg\, x + Tg\, y}{1 - Tg\, x\, Tg\, y}$$

$$Tg(x) = -Tg(-x)$$

$$Tg(x-y) = \frac{Tg\, x - Tg\, y}{1 + Tg\, x\, Tg\, y}$$

Formule di DUPLICAZIONE $(x=y)$

$$\boxed{\cos 2x = \cos^2 x - \sin^2 x}$$
$$\boxed{\sin 2x = 2 \sin x \cos x}$$
$$\boxed{Tg\, 2x = \frac{2\, Tg\, x}{1 - Tg^2 x}}$$

$$\boxed{1 = \cos 0 = \cos^2 x + \sin^2 x}$$

$$\to \cos^2 x = 1 - \sin^2 x$$

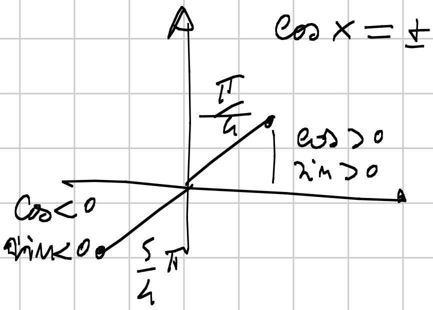
$$\boxed{\begin{aligned} \cos 2x &= 1 - 2\sin^2 x \\ \cos 2x &= 2\cos^2 x - 1 \end{aligned}}$$

$$\Downarrow \quad \sin x = \pm\sqrt{\frac{1-\cos 2x}{2}} \qquad 2\theta = \frac{\pi}{2} + 2k\pi$$

$$\cos x = \pm\sqrt{\frac{\cos 2x + 1}{2}} \qquad k \in \mathbb{Z}$$

$$\theta = \frac{\pi}{4} + k\pi$$

$$\theta = \frac{\pi}{4}\,, \quad \theta = \frac{5}{4}\pi$$



$$\bullet) \quad \cos 3x = \cos(2x + x) = \cos 2x \cos x - \sin 2x \sin x =$$

$$= (\cos^2 x - \sin^2 x)\cos x - 2\sin x \cos x \sin x =$$

$$= \cos^3 x - \cos x \sin^2 x - 2\sin^2 x \cos x =$$

$$= \cos^3 x - 3\underbrace{\sin^2 x}_{(1-\cos^2 x)} \cos x = 4\cos^3 x - 3\cos x$$

$$\operatorname{tg} 2x = \frac{2\operatorname{tg} x}{1 - \operatorname{tg}^2 x} \qquad \operatorname{tg} x = \pm\sqrt{\frac{1-\cos 2x}{1+\cos 2x}}$$

$$\operatorname{tg}^2 x + 1 = \frac{\sin^2 x}{\cos^2 x} + 1 = \frac{\sin^2 x + \cos^2 x}{\cos^2 x} = \frac{1}{\cos^2 x}$$

$$\cos^2 x = \frac{1}{\operatorname{tg}^2 x + 1} \qquad \cos 2x = 2\cos^2 x - 1 =$$

$$= \frac{2}{\operatorname{tg}^2 x + 1} - 1 =$$

$$= \frac{1 - \operatorname{tg}^2 x}{1 + \operatorname{tg}^2 x}$$

$$\sin 2x = \operatorname{tg} 2x \cdot \cos 2x = \frac{2\operatorname{tg} x}{1-\operatorname{tg}^2 x} \cdot \frac{1-\operatorname{tg}^2 x}{1+\operatorname{tg}^2 x} = \frac{2\operatorname{tg} x}{1+\operatorname{tg}^2 x}$$

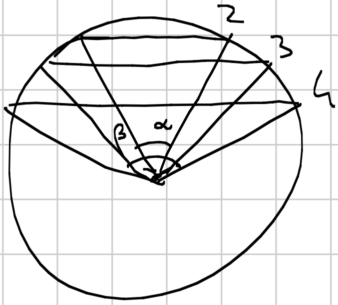
$$t = \operatorname{tg}\frac{x}{2}$$

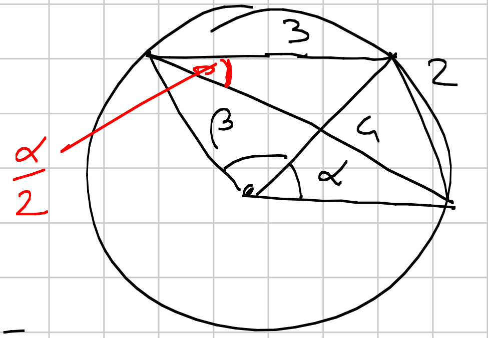
$$\cos x = \frac{1-t^2}{1+t^2}$$

$$\sin x = \frac{2t}{1+t^2}$$

$$\operatorname{tg} x = \frac{2t}{1-t^2}$$

Ex: In uno cfr. ci sono tre corde lunghe 2, 3, 4 che insistono su archi ampi α, β, $\alpha+\beta$. Quanto vale $\cos\alpha$?

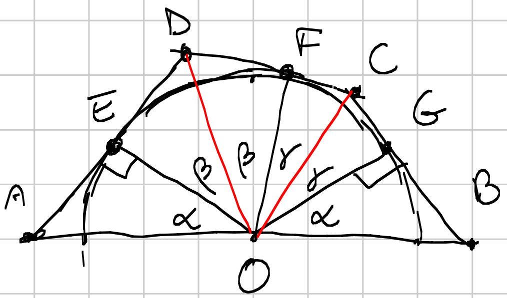




$$\cos\frac{\alpha}{2} = \frac{3^2+4^2-2^2}{2\cdot 3\cdot 4} = \frac{9+16-4}{24} = \cancel{\frac{21}{24}}\ \frac{7}{8}$$

$$\cos\alpha = 2\cos^2\frac{\alpha}{2} - 1 = 2\,\frac{7^2}{8^2} - 1 = \frac{2\cdot 7^2 - 8^2}{8^2} = \frac{2\cdot 49 - 64}{64} = \frac{98-64}{64} =$$

$$= \frac{34}{64} = \frac{17}{32}$$



$AO = OB$

$\Rightarrow AB^2 = 4 BC \cdot AD$

Dim: $O\overset{\triangle}{A}E \cong O\overset{\triangle}{B}G \Rightarrow O\widehat{A}E = O\widehat{B}G$

$R =$ raggio

$$2\alpha + 2\beta + 2\gamma = \pi$$

$$\alpha + \beta + \gamma = \frac{\pi}{2}$$

$$BC = BG + GC =$$
$$= R\,Tg\,\alpha + R\,Tg\,\gamma$$

$$AB = 2 \cdot AO = 2 \frac{R}{\cos\alpha}$$

$$AD = R\,Tg\,\alpha + R\,Tg\,\beta$$

$\boxed{R = 1}$

$$AB^2 = \frac{\cancel{4}}{\cos^2\alpha} \overset{?}{=} 4\,BC \cdot AD = \cancel{4}(Tg\,\alpha + Tg\,\gamma)(Tg\,\alpha + Tg\,\beta)$$

$$\frac{1}{\cos^2\alpha} = \cancel{Tg^2\alpha} + Tg\,\alpha\,Tg\,\gamma + Tg\,\alpha\,Tg\,\beta + Tg\,\gamma\,Tg\,\beta$$

$$\| \quad \cancel{Tg^2\alpha} + 1$$

$$\gamma = \frac{\pi}{2} - (\alpha + \beta)$$

$$Tg\,\gamma = Tg\left(\frac{\pi}{2} - (\alpha+\beta)\right) = \frac{1}{Tg(\alpha+\beta)} = \frac{1 - Tg\,\alpha\,Tg\,\beta}{Tg\,\alpha + Tg\,\beta}$$

$$1 \overset{?}{=} (Tg\,\alpha + Tg\,\beta)\,Tg\,\gamma + Tg\,\alpha\,Tg\,\beta =$$

$$\cancel{(Tg\,\alpha + Tg\,\beta)} \frac{(1 - Tg\,\alpha\,Tg\,\beta)}{\cancel{Tg\,\alpha + Tg\,\beta}} + Tg\,\alpha\,Tg\,\beta = 1 \quad \boxed{OK}$$

•) $5\cos x + 2\sin x = 1.$ $\qquad t = Tg\,\frac{x}{2}$

$$5\,\frac{1-t^2}{1+t^2} + 2\,\frac{2t}{1+t^2} = 1 \qquad 5 - 5t^2 + 4t = 1 + t^2$$

$$6t^2 - 4t - 4 = 0$$

$$t = \frac{2 \pm \sqrt{4+24}}{6} = \frac{2 \pm \sqrt{28}}{6} = \frac{1 \pm \sqrt{7}}{3}$$

$$\operatorname{tg}\frac{x}{2} = \frac{1+\sqrt{7}}{3} \qquad \operatorname{tg}\frac{x}{2} = \frac{1-\sqrt{7}}{3}$$

$$\frac{x}{2} = \theta_1 + k\pi \qquad \frac{x}{2} = \theta_2 + k\pi$$

$$x = 2\theta_1 + 2k\pi \qquad x = 2\theta_2 + 2k\pi$$

——— • ———

Ex: $0 < \alpha, \beta, \gamma < \pi$

$$\alpha + \beta + \gamma = \pi$$
$$\Updownarrow$$
$$\operatorname{tg}\frac{\alpha}{2}\operatorname{tg}\frac{\beta}{2} + \operatorname{tg}\frac{\beta}{2}\operatorname{tg}\frac{\gamma}{2} + \operatorname{tg}\frac{\gamma}{2}\operatorname{tg}\frac{\alpha}{2} = 1$$

Sappiamo che vale $\boxed{\Longrightarrow}$

Facciamo $\boxed{\Longleftarrow}$: Sappiamo che

1) per ipotesi $\operatorname{tg}\frac{\alpha}{2}\operatorname{tg}\frac{\beta}{2} + \operatorname{tg}\frac{\beta}{2}\operatorname{tg}\frac{\gamma}{2} + \operatorname{tg}\frac{\gamma}{2}\operatorname{tg}\frac{\alpha}{2} = 1$

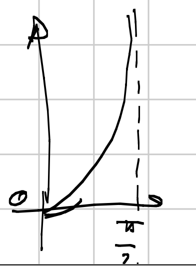
2) per conti $\operatorname{tg}\frac{\alpha}{2}\operatorname{tg}\frac{\beta}{2} + \operatorname{tg}\frac{\beta}{2}\operatorname{tg}\left(\frac{\pi}{2}-\frac{\alpha}{2}-\frac{\beta}{2}\right) + \operatorname{tg}\left(\frac{\pi}{2}-\frac{\alpha}{2}-\frac{\beta}{2}\right)\operatorname{tg}\frac{\alpha}{2} = 1.$

$$\operatorname{tg}\frac{\gamma}{2} = \frac{1 - \operatorname{tg}\frac{\alpha}{2}\operatorname{tg}\frac{\beta}{2}}{\operatorname{tg}\frac{\alpha}{2} + \operatorname{tg}\frac{\beta}{2}} \qquad \operatorname{tg}\left(\frac{\pi}{2}-\frac{\alpha}{2}-\frac{\beta}{2}\right) = \frac{1 - \operatorname{tg}\frac{\alpha}{2}\operatorname{tg}\frac{\beta}{2}}{\operatorname{tg}\frac{\alpha}{2} + \operatorname{tg}\frac{\beta}{2}}$$

$$\Downarrow$$

$$\operatorname{tg}\frac{\gamma}{2} = \operatorname{tg}\left(\frac{\pi}{2}-\frac{\alpha}{2}-\frac{\beta}{2}\right) \qquad 0 < \gamma < \pi \qquad 0 < \frac{\gamma}{2} < \frac{\pi}{2}$$

tg è iniettiva tra 0 e $\frac{\pi}{2}$



$$\Rightarrow \frac{\gamma}{2} = \frac{\pi}{2} - \frac{\alpha}{2} - \frac{\beta}{2}$$

Es x voi: $\alpha+\beta+\gamma = \pi$

$\Downarrow$

- $\tan\alpha + \tan\beta + \tan\gamma = \tan\alpha \tan\beta \tan\gamma$
- $\sin\alpha + \sin\beta + \sin\gamma = 4 \cos\frac{\alpha}{2} \cos\frac{\beta}{2} \cos\frac{\gamma}{2}$

- $\dfrac{\cos 2\alpha - \cos 4\alpha}{\sin 2\alpha + \sin 4\alpha} = \tan\alpha$

Formule brutte (Somma/Prodotto)

$$\cos(x+y) = \cos x \cos y - \sin x \sin y$$
$$\cos(x-y) = \cos x \cos y + \sin x \sin y$$

$$\cos x \cos y = \frac{\cos(x+y) + \cos(x-y)}{2}$$

$$\alpha = \frac{x+y}{2} \qquad \beta = \frac{x-y}{2}$$

$$\sin x \sin y = \frac{\cos(x-y) - \cos(x+y)}{2}$$

$$2\cos(\alpha+\beta)\cos(\alpha-\beta) = \cos\alpha + \cos\beta$$

$$\sin x \cos y = \frac{\sin(x+y) + \sin(x-y)}{2}$$

$$\sin y \cos x = \frac{\sin(x+y) - \sin(x-y)}{2}$$

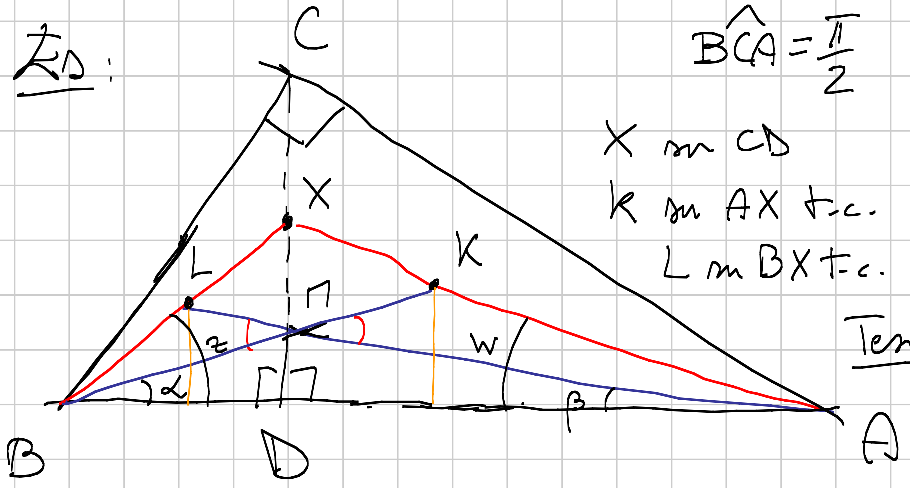
Es: $\cos x + \cos\left(x + \frac{\pi}{3}\right) = 0$

$$2\cos\left(2x + \frac{\pi}{3}\right)\cos\left(-\frac{\pi}{3}\right) = 0 \Rightarrow \cos\left(2x+\frac{\pi}{3}\right) = 0$$

$$2x + \frac{\pi}{3} = \frac{\pi}{2} + k\pi$$

$$x = \left(\frac{\pi}{6} + k\pi\right)\frac{1}{2} = \frac{\pi}{12} + k\frac{\pi}{2}$$

Sd:



$\widehat{BCA} = \frac{\pi}{2}$

X su CD

K su AX t.c. BK = BC

L su BX t.c. AL = AC

Tesi: ML = MK

$\frac{MK}{ML}$ MK in $\overset{\triangle}{AMK}$ ML in $\overset{\triangle}{BML}$

$$\frac{MK}{\sin KAM} = \frac{AK}{\sin KMA} \qquad \frac{ML}{\sin LBM} = \frac{BL}{\sin LMB}$$

$$\frac{MK}{ML} = \frac{AK \cdot \sin KAM}{BL \sin LBM}$$

•) AK in AKB

$$\frac{AK}{\sin ABK} = \frac{AB}{\sin AKB}$$

•) BL in ALB

$$\frac{BL}{\sin BAL} = \frac{AB}{\sin ALB}$$

$$\frac{AK}{BL} = \frac{\sin ABK \cdot \sin ALB}{\sin BAL \cdot \sin AKB}$$

$$\frac{MK}{ML} = \frac{\sin ABK \cdot \sin ALB \cdot \sin KAM}{\sin BAL \cdot \sin AKB \cdot \sin LBM} = \frac{\sin\alpha \cdot \sin(z+\beta)\sin(w-\beta)}{\sin\beta \cdot \sin(w+\alpha)\sin(z-\alpha)}$$

$$\sin\alpha\left[\sin z\cos\beta + \cos z\sin\beta\right]\left[\sin w\cos\beta - \sin\beta\cos w\right] =$$

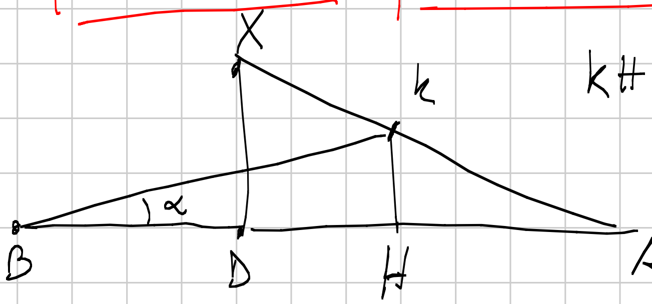
$$= \left[\cos z\cos w\right]^2 \sin\alpha \left[\operatorname{tg} z \frac{\cos\beta}{\cos w} + \frac{\sin\beta}{\cos w}\right]\left[\operatorname{tg} w \cdot \frac{\cos\beta}{\cos z} - \frac{\sin\beta}{\cos z}\right] =$$

$$= \left[\cos z\cos w\right]^{\cancel{2}} \sin\alpha \left[\operatorname{tg} z \operatorname{tg} w \frac{\cos^2\beta}{\cancel{\cos z\cos w}} - \operatorname{tg} z \frac{\cos\beta\sin\beta}{\cancel{\cos w\cos z}} + \operatorname{tg} w \frac{\cos\beta\sin\beta}{\cancel{\cos w\cos z}} - \right.$$

$$- \frac{\sin^2\beta}{\cancel{\cos w}\cos z}\Big] = \cos z \cos w \sin\alpha \Big[\operatorname{tg} z \operatorname{tg} w \cos^2\beta +$$

$$+ (\operatorname{tg} w - \operatorname{tg} z)\left(\frac{\sin 2\beta}{2}\right) - \sin^2\beta \Big]$$

$$\boxed{\operatorname{tg} z = \frac{c\cdot XD}{a^2}} \qquad \boxed{\operatorname{tg} w = \frac{c\cdot XD}{b^2}}$$



$$KH = BK\cdot\sin\alpha =$$
$$= BC\sin\alpha = a\cdot\sin\alpha$$

$$AH = c - a\cdot\cos\alpha$$

$$\frac{a\sin\alpha}{c - a\cos\alpha} = \frac{KH}{AH} = \frac{XD}{DA} = \frac{XD\cdot c}{b^2}$$

$$\frac{b\sin\beta}{c - b\cos\beta} = \frac{XD\cdot c}{a^2} \to \boxed{\sin\beta = \frac{c^2 XD}{a^2 b} - \frac{cXD}{a^2}\cos\beta}$$

$$\Big[\operatorname{tg} z \operatorname{tg} w \cos^2\beta - (\operatorname{tg} z - \operatorname{tg} w)\cos\beta\sin\beta - \sin^2\beta\Big] =$$

$$= \Big[\frac{XD^2 c}{b^2 a^4}\cos\beta - \frac{c^5 XD^2}{b^3 a^4}\Big] = \frac{c^3 XD}{b^2 a^2}\Big[-\sin\beta\Big]$$

$$-\frac{c^3 XD}{b^2 a^2}\cos z\cos w\sin\alpha\sin\beta.$$

$ML = MK.$ (IMO'12 / 5)

Senior 2012

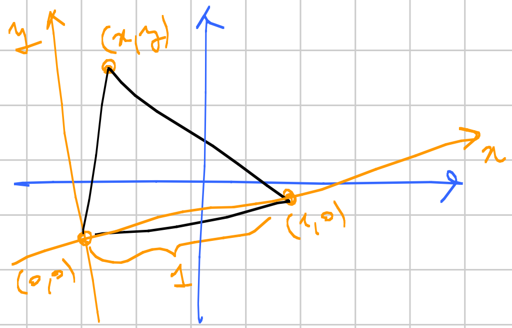
GEOMETRIA 2 BASIC

F. Morandin

Titolo nota 05/09/2012

Metodi algebrici : coordinate cartesiane
vettori
complessi

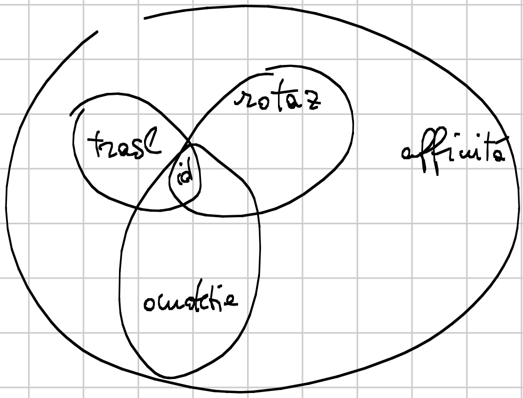
CARTESIANE

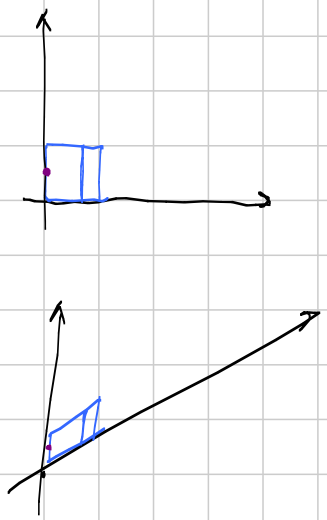


problemi invarianti per rotazioni e traslazioni
↳ scelgo O e la direzione di $\vec{x}$ in modo comodo

se non è fissata una scala, fisso anche quella
(inv. per omotetie)

AFFINITÀ e INVARIANZA





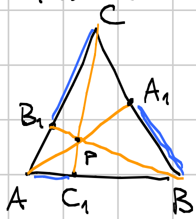
$$\begin{cases} x' = ax + by + c \\ y' = dx + ey + f \end{cases}$$

a, b, c, d, e, f determinano l'affinità

$$P' = MP + Q \qquad M = \begin{pmatrix} a & b \\ d & e \end{pmatrix} \qquad Q = \begin{pmatrix} c \\ f \end{pmatrix}$$

Conservano: parallelismo tra rette (manda rette in rette)
rapporti tra aree
rapporti tra segmenti paralleli

Es 1. Thm di Ceva

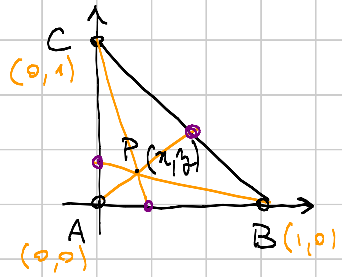


$AC_1 \cdot BA_1 \cdot CB_1 = C_1B \cdot A_1C \cdot B_1A$

$$\frac{AC_1}{C_1B} \cdot \frac{BA_1}{A_1C} \cdot \frac{CB_1}{B_1A} = 1$$

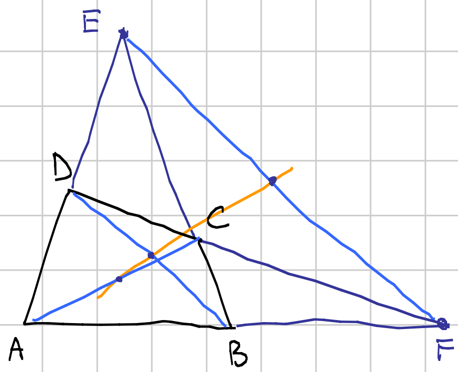
↑ rapporto tra segmenti paralleli

enunciato invariante per affinità

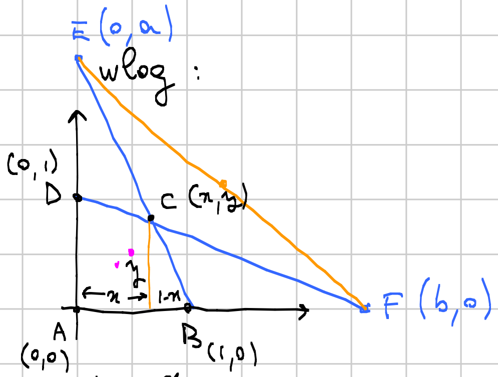


posso mandare 3 punti qualsiasi in 3 punti qualsiasi (a meno che non siano allineati)

Es 2. Quadrilatero A,B,C,D $E = AD \cap BC$ $F = AB \cap CD$
Tesi: i pti medi di EF, AC, BD sono allineati



enunciato invariante per affinità



$a : y = 1 : 1-x$ $\quad a = \dfrac{y}{1-x}$ $\quad b = \dfrac{x}{1-y}$

pto medio di EF : $\left(\frac{b}{2}, \frac{a}{2}\right) = \left(\frac{x/2}{1-y}, \frac{y/2}{1-x}\right)$

pto medio di AC : $\left(\frac{x}{2}, \frac{y}{2}\right)$ Q

pto medio di BD : $\left(\frac{1}{2}, \frac{1}{2}\right)$ P

Per vedere se tre punti P, Q, R sono allineati, verifico se esiste $\lambda \in \mathbb{R}$ t.c. $\lambda P + (1-\lambda)Q = R$

$$\begin{cases} \lambda x_P + (1-\lambda)x_Q = x_R \\ \lambda y_P + (1-\lambda)y_Q = y_R \end{cases}$$

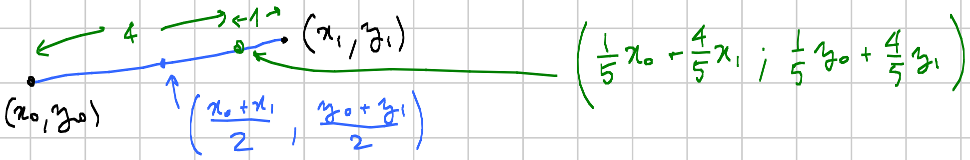
$$\begin{cases} \lambda + (1-\lambda)x = \frac{x}{1-y} \\ \lambda + (1-\lambda)y = \frac{y}{1-x} \end{cases} \qquad \begin{cases} \lambda(1-x) + x = \frac{x}{1-y} \\ \lambda(1-y) + y = \frac{y}{1-x} \end{cases}$$

$$\begin{cases} \lambda = \left(\frac{x}{1-y} - x\right)\frac{1}{1-x} = \frac{xy}{(1-x)(1-y)} \\ \lambda = \qquad = \frac{xy}{(1-x)(1-y)} \end{cases}$$

Un po' di teoria

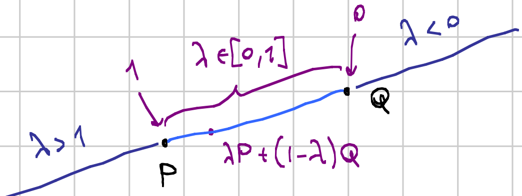
$y = mx + q$ retta non verticale

$ax + by + c = 0$ retta qualunque



Punti del segmento : combinazioni lineari convesse degli estremi

$$(\underset{\lambda}{a}\, x_0 + \underset{(1-\lambda)}{b}\, x_1 ; \underset{\lambda}{a}\, y_0 + \underset{(1-\lambda)}{b}\, y_1) \qquad 0 \le a, b \le 1,\ a+b=1$$



$$\begin{cases} \lambda x_P + (1-\lambda) x_Q = x \\ \lambda y_P + (1-\lambda) y_Q = y \end{cases}$$ retta per PQ

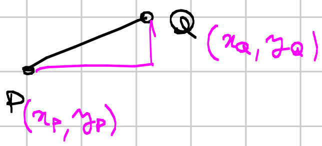
$$\begin{cases} x = \lambda (x_P - x_Q) + x_Q \\ y = \lambda (y_P - y_Q) + y_Q \end{cases}$$ eq. parametrica

$$\lambda = \frac{x - x_Q}{x_P - x_Q} \qquad y = \frac{y_P - y_Q}{x_P - x_Q}(x - x_Q) + y_Q$$ eq. implicita

---

DISTANZA e CIRCONFERENZA

$$d(P,Q) = \overline{PQ} = \sqrt{(x_P - x_Q)^2 + (y_P - y_Q)^2}$$ distanza Euclidea



$$\Gamma = \{ (x,y) : d((x,y),(x_0,y_0)) = r \}$$

$$(x - x_0)^2 + (y - y_0)^2 = r^2$$

$$x^2 + y^2 - 2x_0 x - 2y_0 y + \underbrace{x_0^2 + y_0^2 - r^2}_{c} = 0$$

$$\boxed{x^2 + y^2 + ax + by + c = 0}$$ non sempre questa è una circonf.

$$x_0 = -\frac{a}{2} \qquad y_0 = -\frac{b}{2} \qquad \frac{a^2}{4} + \frac{b^2}{4} - c \overset{?}{\lessgtr} 0$$

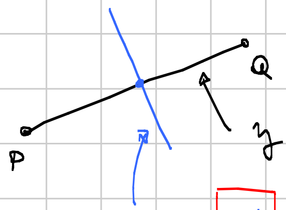
- Asse di un segmento

$$r = \{ (x,y) : d((x,y),(x_P,y_P)) = d((x,y),(x_Q,y_Q)) \}$$

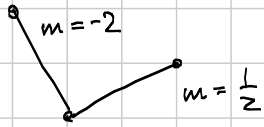
$$(x - x_Q)^2 + (y - y_Q)^2 = (x - x_P)^2 + (y - y_P)^2$$

$$2x(x_P - x_Q) + 2y(y_P - y_Q) + x_Q^2 + y_Q^2 - x_P^2 - y_P^2 = 0$$

$$ax + by + c = 0$$



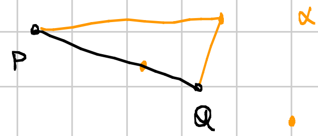
$y = \boxed{m}x + q$



$y = \boxed{-\frac{1}{m}}x + \text{mostro}$ equazione retta ortogonale

- Circonferenza di Apollonio

$$r = \{(x,y) : d((x,y),(x_P,y_P)) = \alpha \cdot d((x,y),(x_Q,y_Q))\} \qquad \alpha \neq 1, \ \alpha > 0$$



$$(x - x_Q)^2 + (y - y_Q)^2 = \alpha^2 (x - x_P)^2 + \alpha^2 (y - y_P)^2$$

$$(1-\alpha^2)x^2 + (1-\alpha^2)y^2 + \ldots = 0$$ circonferenza

- Bisettrici, potenza, asse radicale .. alla fine, se riesco

VETTORI

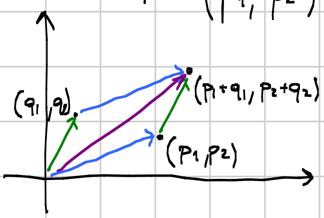
$\vec{X} = (x_1, x_2, x_3, \ldots, x_n)$ $\quad n = 2, 3$ o più. $\quad x_i \in \mathbb{R} \quad i = 1, 2, \ldots, n$

$\vec{X}, X, x \qquad \vec{Y} = (y_1, y_2, \ldots, y_n)$

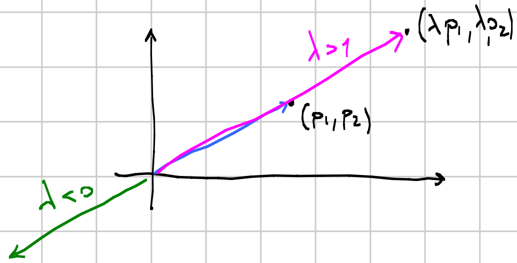
$\vec{X} + \vec{Y} = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$ somma

$\lambda \in \mathbb{R} \qquad \lambda\vec{X} = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n)$ prod per scalare

$n=2$ $\vec{P}=(p_1,p_2)$ $\vec{Q}=(q_1,q_2)$ $\vec{P}+\vec{Q}=(p_1+q_1,p_2+q_2)$



$\vec{P}$ è il punto o la freccia a seconda di cosa ci fa comodo



- Prodotto scalare

simmetrico

$$\mathbb{R}\ni\vec{X}\cdot\vec{Y}=\langle\vec{X},\vec{Y}\rangle=(\vec{X},\vec{Y})=x_1y_1+x_2y_2+\dots+x_ny_n=\sum_{i=1}^n x_iy_i$$

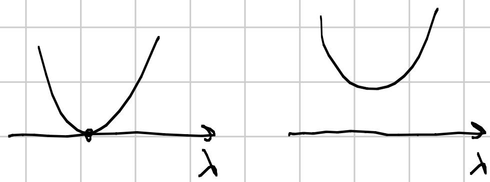
$$0\leq\vec{X}\cdot\vec{X}=\sum_{i=1}^n x_i^2=:\|\vec{X}\|^2$$ norma (o lunghezza) del vettore al quadrato

$$(\lambda\vec{X})\cdot\vec{Y}=(\lambda x_1,\dots)\cdot(y_1,\dots)=\lambda x_1y_1+\lambda x_2y_2+\dots=\lambda(\vec{X}\cdot\vec{Y})=\vec{X}\cdot\lambda\vec{Y}$$

$$(\vec{X}+\vec{Y})\cdot\vec{Z}=\dots=\vec{X}\cdot\vec{Z}+\vec{Y}\cdot\vec{Z}$$ distributiva

$$0\leq\|\vec{X}+\lambda\vec{Y}\|^2=(\vec{X}+\lambda\vec{Y})\cdot(\vec{X}+\lambda\vec{Y})=\vec{X}\cdot(\vec{X}+\lambda\vec{Y})+\lambda\vec{Y}\cdot(\vec{X}+\lambda\vec{Y})$$

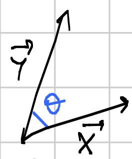
$$=\vec{X}\cdot\vec{X}+\lambda\vec{X}\cdot\vec{Y}+\lambda\vec{Y}\cdot\vec{X}+\lambda^2\vec{Y}\cdot\vec{Y}=\|\vec{X}\|^2+2(\vec{X}\cdot\vec{Y})\lambda+\|\vec{Y}\|^2\lambda^2$$



$$\frac{\Delta}{4}=(\vec{X}\cdot\vec{Y})^2-\|\vec{X}\|^2\|\vec{Y}\|^2\leq 0$$

$$|\vec{X}\cdot\vec{Y}|\leq\|\vec{X}\|\|\vec{Y}\|\qquad C\text{-}S$$

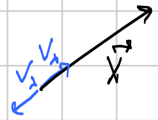
$n=2$ $\quad\vec{X}\cdot\vec{Y}:=x_1y_1+x_2y_2\overset{\text{thm}}{=}\|\vec{X}\|\|\vec{Y}\|\cos\theta$



in C-S vale $=$ se e solo se $\vec{X}\parallel\vec{Y}$ $\quad\vec{X}=\nu\vec{Y}$ $\quad\nu\in\mathbb{R}$

$$\frac{\vec X\cdot\vec Y}{\|\vec X\|\|\vec Y\|} = \cos\theta$$

lo dimostro



$$\frac{\vec X\cdot\vec Y}{\|\vec X\|\|\vec Y\|} = \frac{\vec X}{\|\vec X\|}\cdot\frac{\vec Y}{\|\vec Y\|} = (\cos\alpha, \operatorname{sen}\alpha)\cdot(\cos\beta, \operatorname{sen}\beta) = \cos\alpha\cos\beta + \operatorname{sen}\alpha\operatorname{sen}\beta$$

$$= \cos(\alpha-\beta) = \cos(\beta-\alpha) = \cos\theta$$

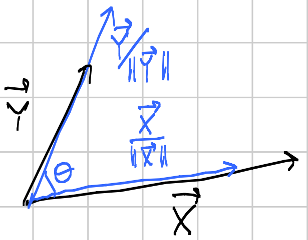
$\vec V_\lambda := \lambda\vec X \quad \parallel \vec X$

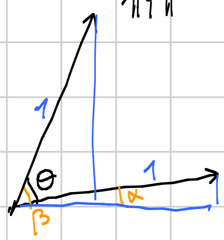
$$\|\vec V_\lambda\| = \|\lambda\vec X\| = \sqrt{\|\lambda\vec X\|^2} = \sqrt{\lambda\vec X\cdot\lambda\vec X} = |\lambda|\sqrt{\vec X\cdot\vec X} = |\lambda|\|\vec X\|$$

$\|\lambda\vec X\| = |\lambda|\,\|\vec X\|$

$1 = \|\vec V_\lambda\| = |\lambda|\|\vec X\| \qquad \lambda = \pm\|\vec X\|^{-1}$

$\vec Y/\|\vec Y\| = (\cos\beta, \operatorname{sen}\beta)$



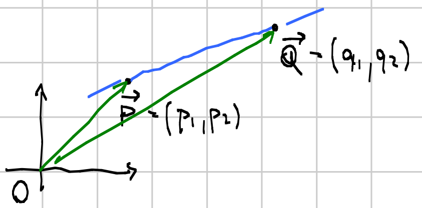


$\frac{\vec X}{\|\vec X\|} = (\cos\alpha, \operatorname{sen}\alpha)$

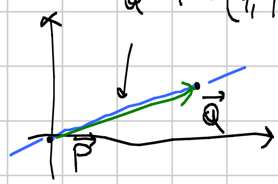
$\theta = \beta - \alpha$

- Retta per due punti

$\vec Q - \vec P = (q_1-p_1, q_2-p_2)$



traslo $\vec P$ nell'origine (sottraggo $\vec P$)



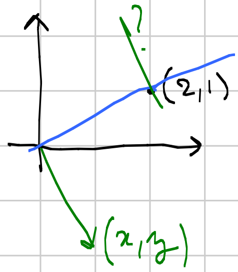
$\lambda \in \mathbb{R}$ $\quad \lambda(\vec Q - \vec P)$ sono i punti della retta

somma $\vec P$

$$\lambda(\vec Q - \vec P) + \vec P$$
$$\parallel$$
$$\lambda\vec Q + (1-\lambda)\vec P$$

di nuovo combinazione convessa di $\vec P$ e $\vec Q$

- Retta ortogonale



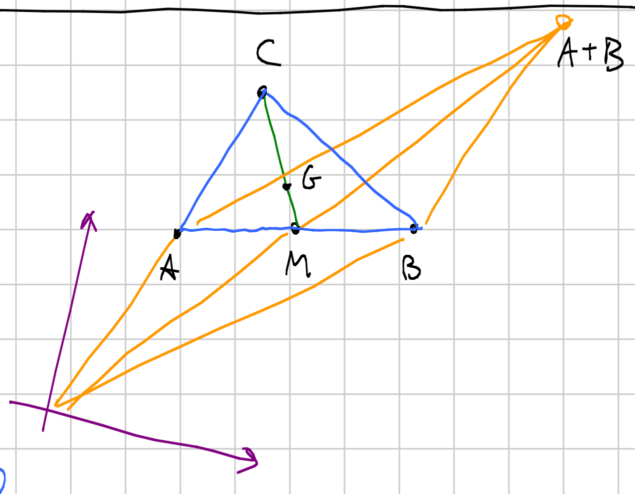
la direzione verde deve essere ortogonale a quella blu

$$0 = (2,1)\cdot(x,y) = 2x + y \qquad \text{ad es } x=1,\ y=-2$$

$(1,-2)$ è ortogonale a $(2,1)$

retta cercata: $(2,1) + \lambda(1,-2) = (2+\lambda, 1-2\lambda)$

▫ Punti dei triangoli



- Baricentro

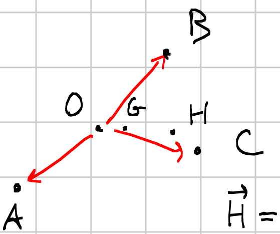
$$\vec{M} = \frac{\vec{A}+\vec{B}}{2}$$

comb. lin. conv.
⇒ non dipende da O

$$\vec{G} = \frac{2}{3}\vec{M} + \frac{1}{3}\vec{C} = \frac{2}{3}\left(\frac{\vec{A}+\vec{B}}{2}\right) + \frac{1}{3}\vec{C} = \frac{\vec{A}+\vec{B}+\vec{C}}{3}$$ baricentro della fisica

$$\boxed{\vec{G} = \frac{\vec{A}+\vec{B}+\vec{C}}{3}}$$

- Circocentro / ortocentro
  spesso ci si mette l'origine



$\vec{H} = 3\vec{G}$

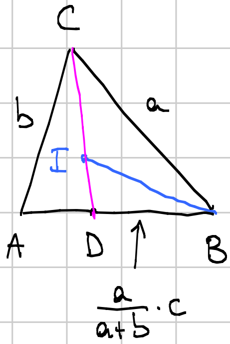
- $\|\vec{A}\| = \|\vec{B}\| = \|\vec{C}\|$
- $\boxed{\vec{H} = \vec{A}+\vec{B}+\vec{C}}$ solo se O è l'origine

Più in generale

$$\boxed{\vec{H} = \vec{A}+\vec{B}+\vec{C}-2\vec{O}}$$

$$\vec{H} = \vec{O} + \underbrace{(\vec{H}-\vec{O})}_{\overrightarrow{OH}} = \vec{O} + 3(\vec{G}-\vec{O}) = \vec{O} + \vec{A}+\vec{B}+\vec{C}-3\vec{O}$$

- Incentro $\boxed{\vec{I} = \dfrac{a\vec{A} + b\vec{B} + c\vec{C}}{a+b+c}}$ non dipende da O



$$\vec{D} = \lambda\vec{A} + (1-\lambda)\vec{B}$$

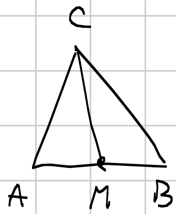
$$AD : DB = AC : CB = b : a$$

$$\vec{D} = \frac{a}{a+b}\vec{A} + \frac{b}{a+b}\vec{B}$$

$$\vec{I} = \frac{\frac{ac}{a+b}}{\frac{ac}{a+b}+a}\vec{C} + \frac{a}{\frac{ac}{a+b}+a}\vec{D}$$

$$\vec{I} = \frac{\cancel{a}c}{\cancel{a}c + a^2 + \cancel{a}b}\vec{C} + \frac{\cancel{a+b}}{a+b+c}\cdot\frac{1}{\cancel{a+b}}\left(a\vec{A} + b\vec{B}\right) = \frac{a\vec{A} + b\vec{B} + c\vec{C}}{a+b+c}$$

- Lunghezza mediana



$$\overline{CM} = \frac{1}{2}\sqrt{2a^2 + 2b^2 - c^2}$$

$$\vec{M} = \frac{\vec{A} + \vec{B}}{2} \qquad \overline{CM} = \|\vec{C} - \vec{M}\| = \left\|\frac{2\vec{C} - \vec{A} - \vec{B}}{2}\right\|$$

$$\overline{CM}^2 = \frac{1}{4}\left(2\vec{C} - \vec{A} - \vec{B}\right)\cdot\left(2\vec{C} - \vec{A} - \vec{B}\right)$$

$$= \frac{1}{4}\left(4\|\vec{C}\|^2 + \|\vec{A}\|^2 + \|\vec{B}\|^2 + 2\vec{A}\cdot\vec{B} - 4\vec{A}\cdot\vec{C} - 4\vec{B}\cdot\vec{C}\right)$$

$$a^2 = \overline{BC}^2 = \|\vec{B} - \vec{C}\|^2 = \|\vec{B}\|^2 + \|\vec{C}\|^2 - 2\vec{B}\cdot\vec{C}$$

$$b^2 \qquad = \|\vec{A}\|^2 + \|\vec{C}\|^2 - 2\vec{A}\cdot\vec{C}$$

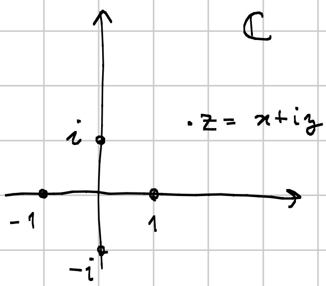
$$c^2 \qquad = \|\vec{A}\|^2 + \|\vec{B}\|^2 - 2\vec{A}\cdot\vec{B}$$

$$2a^2 + 2b^2 - c^2 = \|\vec{A}\|^2 + \|\vec{B}\|^2 + 4\|\vec{C}\|^2 + 2\vec{A}\cdot\vec{B} - 4\vec{B}\cdot\vec{C} - 4\vec{A}\cdot\vec{C}$$

$$\overline{CM}^2 = \frac{1}{4}\left(2a^2 + 2b^2 - c^2\right)$$

- altri esempi ... alla fine se riesco

COMPLESSI



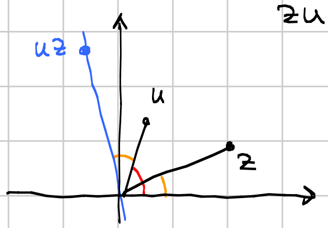
come i vettori, ma in più:

- coniugio (simmetrie vs rette)
- prodotto (rotazioni)

regola del parallelogramma vale sempre

$z = x+iy \qquad u = r+it \qquad \in \mathbb{C}$

$zu \in \mathbb{C} \qquad zu = (x+iy)(r+it) = xr - yt + i(yr + xt)$



$|z| = x^2+y^2 = z\bar{z}$

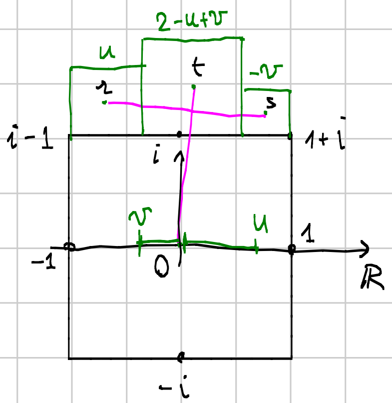
$|zu| = |z||u|$

$\arg(zu) = \arg z + \arg u$

se $|u| = 1$ moltiplicare per u esegue una rotazione

moltiplicare per i ↺ di $90°$

Es 1



$u, v \in \mathbb{R} \qquad u \in (0,1) \qquad v \in (-1, 0)$

$r = i - 1 + \frac{u}{2} + i\frac{u}{2} = -1 + \frac{u}{2} + i\left(1 + \frac{u}{2}\right)$

$s = 1 + i + \frac{v}{2} - i\frac{v}{2} = 1 + \frac{v}{2} + i\left(1 - \frac{v}{2}\right)$

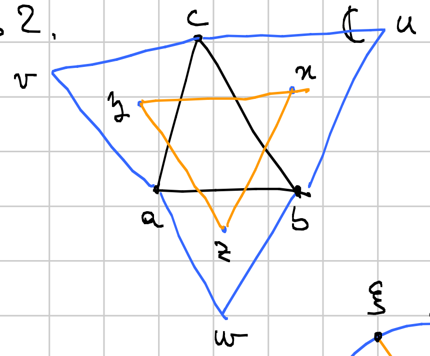
$t = i - \cancel{1} + u + \cancel{1} - \frac{u}{2} + \frac{v}{2} + i\left(1 - \frac{u}{2} + \frac{v}{2}\right)$

$= \frac{u+v}{2} + i\left(2 - \frac{u}{2} + \frac{v}{2}\right)$

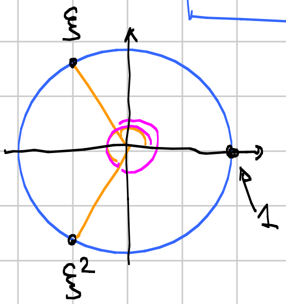
$s - r = 2 + \frac{v}{2} - \frac{u}{2} - i\left(\frac{u+v}{2}\right)$

$i(s-r) = t \qquad$ finito

Es 2.



Lemma: u, v, w formano un triangolo equilatero se
$$u + \xi v + \xi^2 w = 0$$
dove ξ è una delle radici terze dell'unità ($\xi \neq 1$)

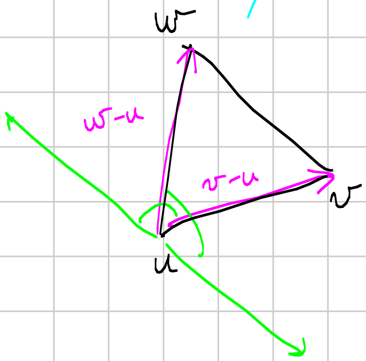


$$x^n - 1 = 0$$
$$\xi = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

$$(1+\xi+\xi^2)(1-\xi) = 0 \qquad 1 + \xi + \xi^2 = 0$$

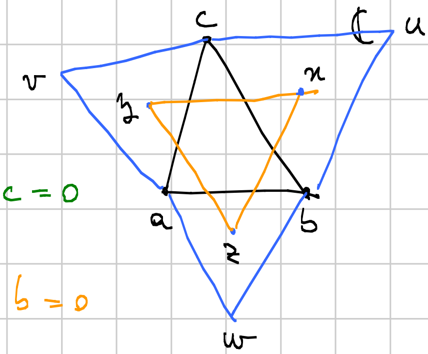
$$\cancel{u} + \xi v + \xi^2 w - \cancel{u} - \xi u - \xi^2 u = \xi(v-u) + \xi^2(w-u) = 0$$

sse equil.



Occhio: se ξ è quello che ho scelto, u, v, w vanno presi in senso antiorario

torno all'esercizio



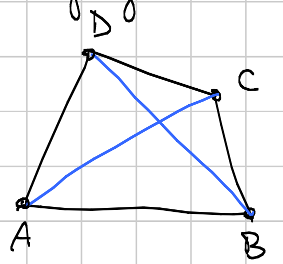
$$b + \xi u + \xi^2 c = 0 \quad \cdot \xi^2 \quad \xi^2 b + u + \xi c = 0$$
$$c + \xi v + \xi^2 a = 0$$
$$a + \xi w + \xi^2 b = 0 \quad \cdot \xi \quad \xi a + \xi^2 w + b = 0$$

$$x = \frac{b+u+c}{3} \quad \text{e analoghi}$$

$$3(x + \xi y + \xi^2 z) = b + u + c + \xi(c + v + a) + \xi^2(a + w + b) = 0$$

- Disuguaglianza di Tolomeo

$\mathbb{C}$



$AB \cdot CD + BC \cdot DA \geq AC \cdot BD$

uguaglianze

$\overline{AB} = |a-b|$ e analoghi

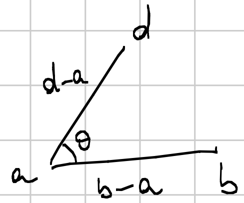
$|a-b||c-d| + |b-c||d-a| - |a-c||b-d| \overset{?}{\geq} 0$

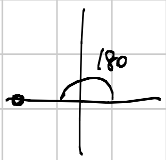
$|ac - ad - bc + bd| + |bd - ba - cd + ac| - |ab - ad - bc + cd| \geq$

$\geq |\cancel{ac} - ad - bc + \cancel{bd} - \cancel{bd} + ba + cd - \cancel{ac}| - |ab - ad - bc + cd| = 0$

vale = solo se

$\dfrac{(a-b)(c-d)}{(b-c)(a-d)} > 0$ reale e positivo

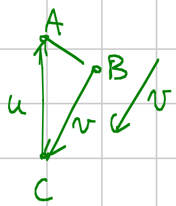




$\underbrace{\dfrac{b-a}{d-a} \cdot \dfrac{d-c}{b-c}}_{\arg = 180} < 0$

$\Leftrightarrow \alpha + \gamma = 180$

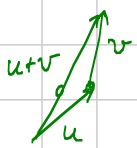
quindi ciclico o allineati



disuguaglianza triangolare

a, b, c

$\underbrace{|a-b|}_{u+v} \leq |\underbrace{a-c}_{u}| + |\underbrace{c-b}_{v}|$



$\forall u, v \in \mathbb{C}$

$|u+v| \leq |u| + |v|$

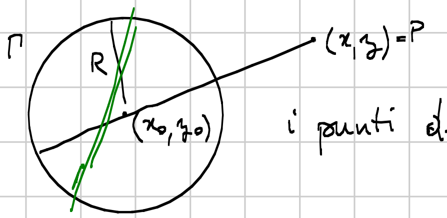
$\forall \vec{X}, \vec{Y}$

$\|\vec{X} + \vec{Y}\| \leq \|\vec{X}\| + \|\vec{Y}\|$

☆ vale = se $u = \lambda v$ $\lambda > 0$

Torno alle cartesiane

- (Bisettrici), potenza, asse radicale … alla fine, se riesco



$Pow_\Gamma(P) = d^2 - R^2 = (x-x_0)^2 + (y-y_0)^2 - R^2$

i punti della circonferenza sono quelli con $Pow_\Gamma(P) = 0$

Γ_1, Γ_2 due circonferenze $\quad \{P : Pow_{\Gamma_1}(P) = Pow_{\Gamma_2}(P)\} \quad P = (x, y)$

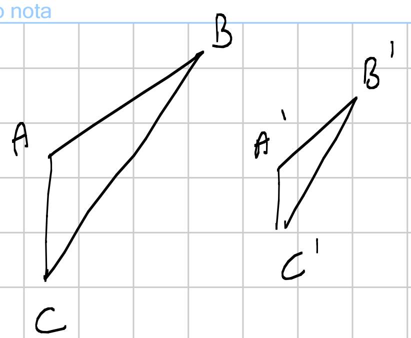
$$(x-x_1)^2 + (y-y_1)^2 - R_1^2 = (x-x_2)^2 + (y-y_2)^2 - R_2^2$$

viene lineare :

$$\underbrace{2(x_2-x_1)}_{a}x + \underbrace{2(y_2-y_1)}_{b}y + \underbrace{x_1^2 + y_1^2 - x_2^2 - y_2^2 - R_1^2 + R_2^2}_{c} = 0$$

SENIOR 2012 - G3 BASIC

Titolo nota 06/09/2012

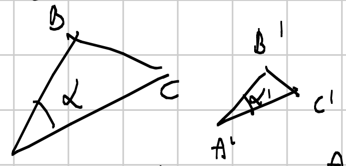


$\alpha = \alpha'$
$\beta = \beta'$
$\gamma = \gamma'$

$$\frac{AB}{A'B'} = \frac{AC}{A'C'} = \frac{BC}{B'C'}$$

$\boxed{\text{I}}$ Due triangoli con 2 angoli congruenti sono simili.

$\boxed{\text{II}}$ Due triangoli con 1 angolo congruente e i lati che lo comprendono in proporzione sono simili.

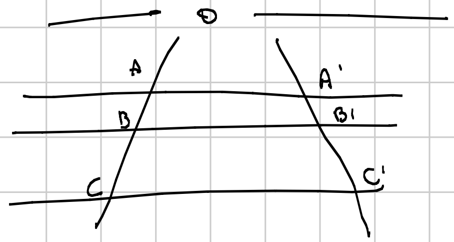


$\alpha = \alpha'$ $\quad \frac{AB}{A'B'} = \frac{AC}{A'C'}$

$\boxed{\text{III}}$ 3 coppie di lati in proporzione

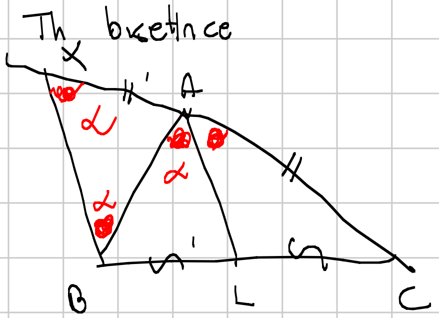
$$\frac{AB}{A'B'} = \frac{AC}{A'C'} = \frac{BC}{B'C'}$$

TALETE

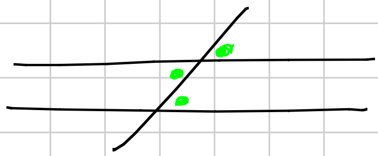


$$\frac{AB}{BC} = \frac{A'B'}{B'C'}$$

Esempio Th. bisettrice



$$\frac{BL}{LC} = \frac{AB}{AC}$$

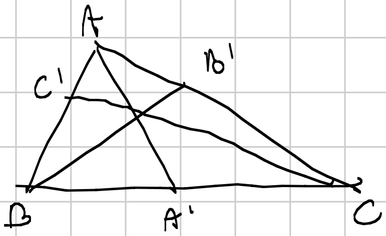


$X = AC \cap$ (parallela ad AL per B)

Per conto di angoli $\overset{\triangle}{ABX}$ isoscele $\longrightarrow AX = AB$

Per talete $\frac{LC}{AC} = \frac{BL}{AX} \Rightarrow \frac{LC}{AC} = \frac{BL}{AB} \Rightarrow \frac{BL}{LC} = \frac{AB}{AC}$ ■

Teo. Ceva



AA', BB', CC' allineati

$\Longleftrightarrow$

$$\frac{AB'}{B'C} \cdot \frac{CA'}{A'B} \cdot \frac{BC'}{C'A} = 1$$

e.g. bisettrici concorrono

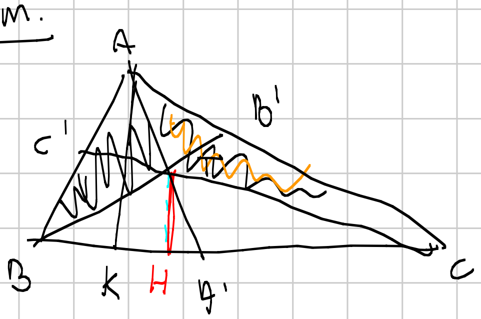
$$\frac{\cancel{c}}{\cancel{a}} \cdot \frac{\cancel{b}}{\cancel{c}} \cdot \frac{\cancel{a}}{\cancel{b}} = 1$$

mediane concorrono

$$1 \cdot 1 \cdot 1 = 1$$

Dim.

$[A] = \text{Area}$



$$\frac{BA'}{A'C} = \frac{[BA'T]}{[CA'T]} = \frac{[BAT]}{[CAT]}$$

$$\frac{BA'}{A'C} = \frac{[BA'A]}{[CA'A]}$$

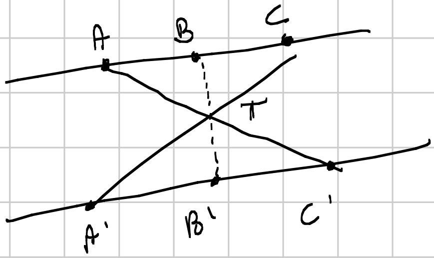
$$\frac{[BA'A]}{[CA'A]} = \frac{[BA'T]}{[CA'T]} \Rightarrow \frac{[BA'A]}{[BA'T]} = \frac{[CA'A]}{[CA'T]} \Rightarrow \frac{[BA'A]-[BA'T]}{[BA'T]} = \frac{[CA'A]-[CA'T]}{[CA'T]}$$

$$\longrightarrow \frac{[BAT]}{[BA'T]} = \frac{[CAT]}{[CA'T]} \Rightarrow \frac{[BAT]}{[CAT]} = \frac{[BA'T]}{[CA'T]}$$

Analogamente $\frac{CB'}{B'A} = \frac{[CBT]}{[BAT]}$ e $\frac{AC'}{C'B} = \frac{[CAT]}{[CBT]}$

Quindi moltiplicando si ha la tesi

Dim. 2

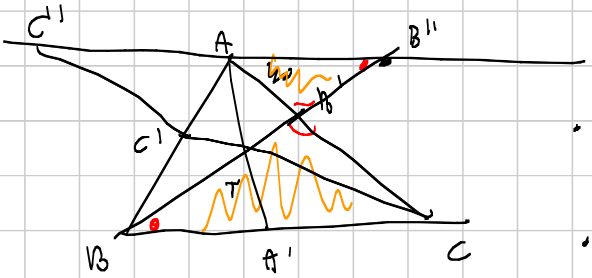


$$\frac{A'B'}{B'C'} = \frac{BC}{AB}$$

$$\Updownarrow$$

$B, B', AC \cap A'C'$ sono allineati

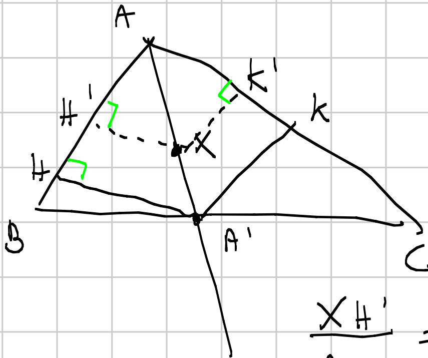
Provate a mostrarlo!



- $\dfrac{BA'}{A'C} = \dfrac{B''A}{AC''}$
- $\dfrac{CB'}{B'A} = \dfrac{BC}{B''A}$
- $\dfrac{AC'}{C'B} = \dfrac{AC''}{BC}$

REMIND: $\dfrac{a}{\sin\alpha} = 2R$

CEVA $\boxed{V2}$



$$\frac{XH'}{XK'} = ?$$

$$\frac{XH'}{AX} = \frac{A'H}{AA'} \Rightarrow XH' = \frac{A'H}{AA'} \cdot AX$$

$$\frac{XK'}{AX} = \frac{A'K}{AA'} \Rightarrow XK' = \frac{A'K}{AA'} \cdot AX$$

Se faccio il rapporto $\dfrac{XH'}{XK'} = \dfrac{A'H}{A'K} = \dfrac{A'B \sin\beta}{A'C \sin\gamma} = \dfrac{A'B}{A'C} \cdot \dfrac{b}{c}$

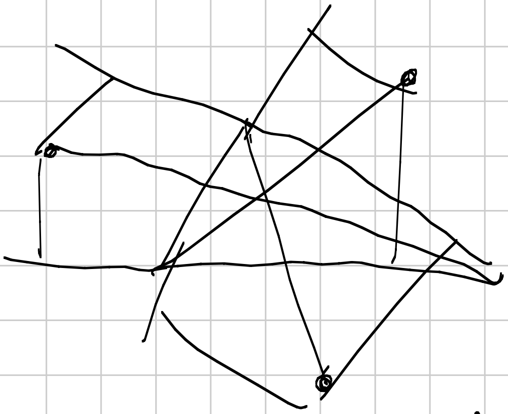
$$V(AA') \overset{x \in AA'}{=} \frac{d(X, AB)}{d(X, AC)} = \frac{A'B}{A'C} \cdot \frac{b}{c}$$

$$v(BB') = \frac{B'C}{B'A} \cdot \frac{c}{a}$$

$$v(CC') = \frac{C'A}{C'B} \cdot \frac{a}{b}$$

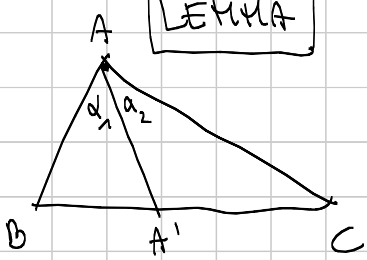
$$v(AA') \cdot v(BB') \cdot v(CC') = \frac{A'B}{A'C} \cdot \frac{B'C}{B'A} \cdot \frac{C'A}{C'B} = 1 \iff$$

$$v(AA') \cdot v(BB') \cdot v(CC') = 1$$



CEVA $\boxed{V3}$ (trigonometrico)

$\boxed{\text{LEMMA}}$



Th sen $A\hat{B}A'$:

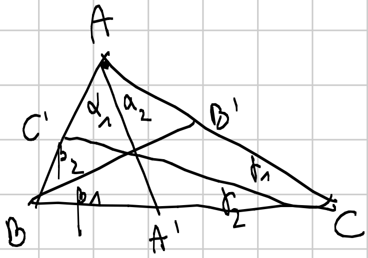
$$\frac{BA'}{AA'} = \frac{\sin\alpha_1}{\sin\beta} \qquad \frac{A'C}{AA'} = \frac{\sin\alpha_2}{\sin\gamma}$$

$$\Downarrow \qquad\qquad \Downarrow$$

$$BA' = \frac{AA' \sin\alpha_1}{\sin\beta} \qquad A'C = \frac{AA' \sin\alpha_2}{\sin\gamma}$$

$$\Downarrow$$

$$\frac{BA'}{A'C} = \frac{\sin\alpha_1}{\sin\alpha_2} \cdot \frac{\sin\gamma}{\sin\beta} = \frac{\sin\alpha_1}{\sin\alpha_2} \cdot \frac{c}{b}$$



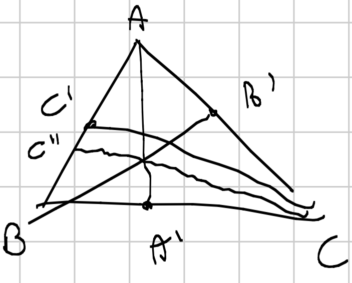
$$\frac{CB'}{B'A} = \frac{\sin\beta_1}{\sin\beta_2} \cdot \frac{a}{c}$$

$$\frac{AC'}{C'B} = \frac{\sin\gamma_1}{\sin\gamma_2} \cdot \frac{b}{a}$$

$$\frac{BA'}{A'C}\cdot\frac{CB'}{B'A}\cdot\frac{AC'}{C'B}=\frac{\sin\alpha_1}{\sin\alpha_2}\cdot\frac{\sin\beta_1}{\sin\beta_2}\,\frac{\sin\gamma_1}{\sin\gamma_2}$$

Le tre ceviane concorrono sse $\dfrac{\sin\alpha_1}{\sin\alpha_2}\cdot\dfrac{\sin\beta_1}{\sin\beta_2}\,\dfrac{\sin\gamma_1}{\sin\gamma_2}=1$

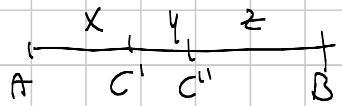
Idea dell'altra freccia



$$\frac{BA'}{A'C}\cdot\frac{CB'}{B'A}\cdot\frac{AC'}{C'B}=1$$

$$\frac{BA'}{A'C}\cdot\frac{CB'}{B'A}\cdot\frac{AC''}{C''B}=1$$

Ma allora $\dfrac{AC'}{C'B}=\dfrac{AC''}{C''B}$



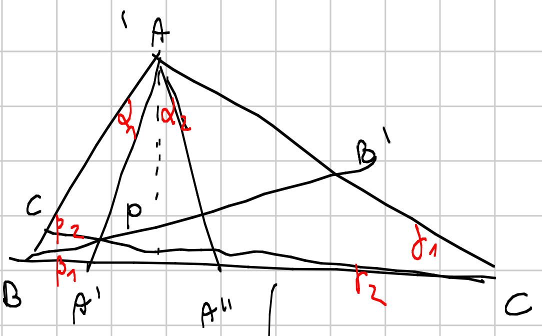
$$\frac{x}{y+z}=\frac{x+y}{z}$$

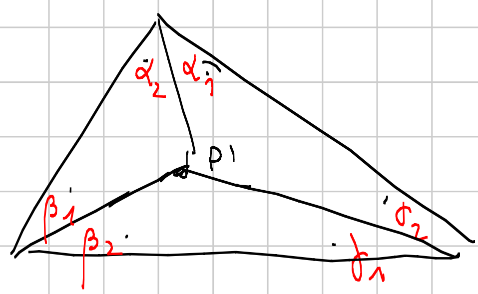
$$\Updownarrow$$

$$\cancel{xz}=xy+\cancel{xz}+y^2+yz$$

$$y(x+y+z)=0 \qquad \text{ASSURDO}$$

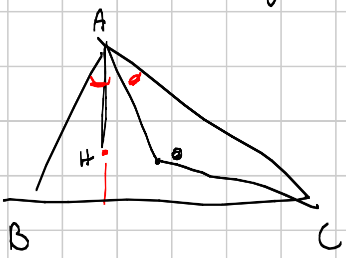
Esercizi





$$\frac{\sin\alpha_1\cdot\sin\beta_1\cdot\sin\gamma_1}{\sin\alpha_2\cdot\sin\beta_2\cdot\sin\gamma_2}=1 \longrightarrow$$ le tre ceviane simmetriche risp. alle bisettrici concorrono

P e P' sono coniugati isogonali



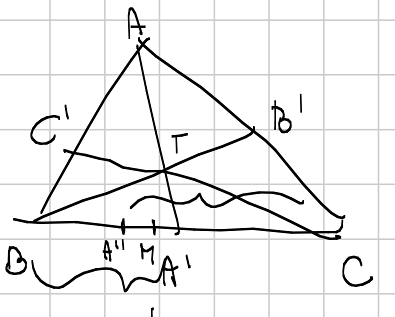
O, H coniugati isogonali

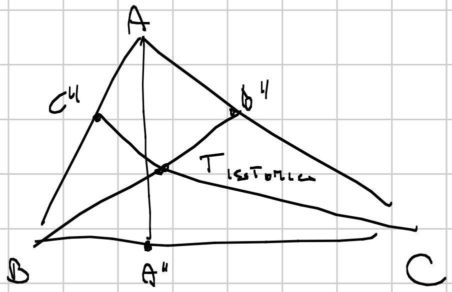
Lemoine

(G e K sono coniugati isogonali)

$\widehat{HAB} \simeq 90-\beta$

$\widehat{OAC} \simeq \frac{180-2\beta}{2} = 90-\beta$





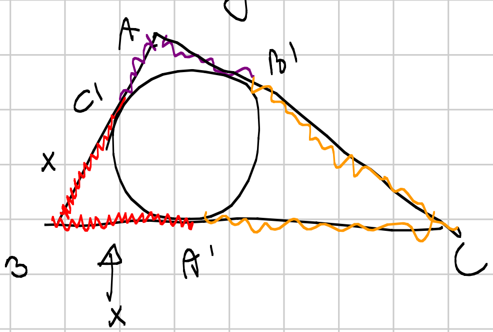
$BA' = BM + MA'$

$CA'' = CM + MA''$

$$\frac{BA'}{A'C}\cdot\frac{CB'}{B'A}\cdot\frac{AC'}{C'B}=1 \Rightarrow \frac{CA''}{A''B}\cdot\frac{AB''}{B''C}\cdot\frac{BC''}{C''A}=1$$

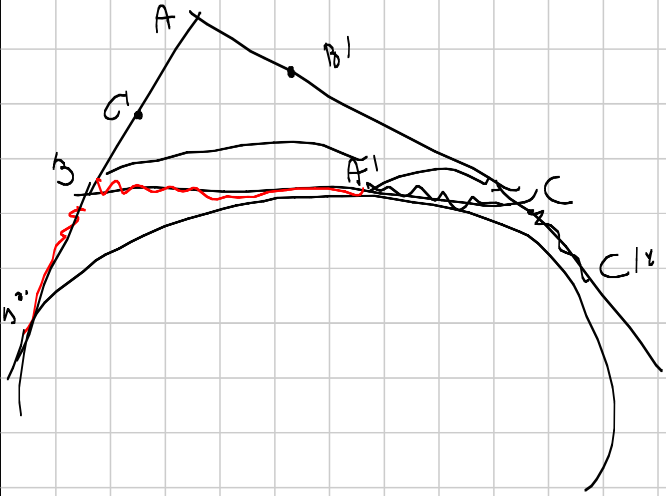
AA'', BB'', CC'' concorrono per Ceva inverso (nel coniugato isotomico di T)

P.to di Gergonne



$$\frac{BA'}{A'C}\cdot\frac{CB'}{B'A}\cdot\frac{AC'}{C'B}=1$$

AA', BB', CC' concorrono in un punto che si chiama p.to di Gergonne.



$BA' = BB' = AB' - AB$

$AB'' = AC''$

$AB'' + AC'' = AB + BB'' + AC + CC'' =$

$= AB + BA' + AC + CA'$

$= AB + AC + BC = 2p$

$AB' = AC' = p$

$BA' = p - c, \quad A'C = p - b$

$CB' = p - a, \quad B'A = p - c$

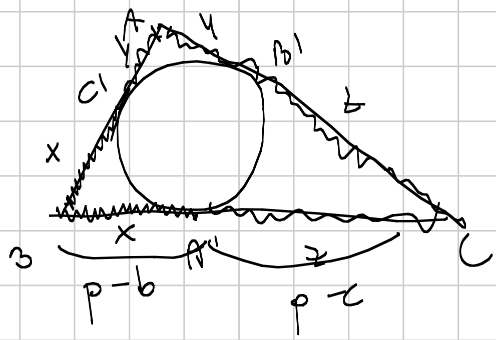
$AC' = p - b, \quad C'B = p - a$

$$\frac{BA'}{A'C} \cdot \frac{CB'}{B'A} \cdot \frac{AC'}{C'B} = \frac{\cancel{p-c}}{\cancel{p-b}} \cdot \frac{\cancel{p-a}}{\cancel{p-c}} \cdot \frac{\cancel{p-b}}{\cancel{p-a}} = 1$$

$\Downarrow$

AA', BB', CC' concorrono in Nagel.

Ger



$$\begin{cases} x + z = a \\ y + z = b \\ x + z = c \end{cases} \rightarrow x + y + z = p$$

$\Downarrow$

$x = p - b$

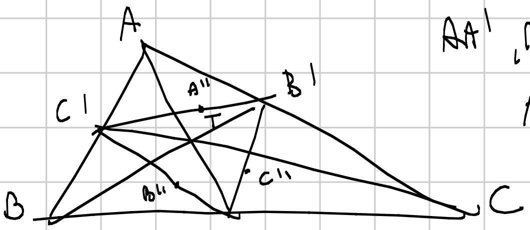
$y = p - a$

$z = p - c$

$\hookrightarrow$ Nagel e Gergonne isotomici

o

Esercizio



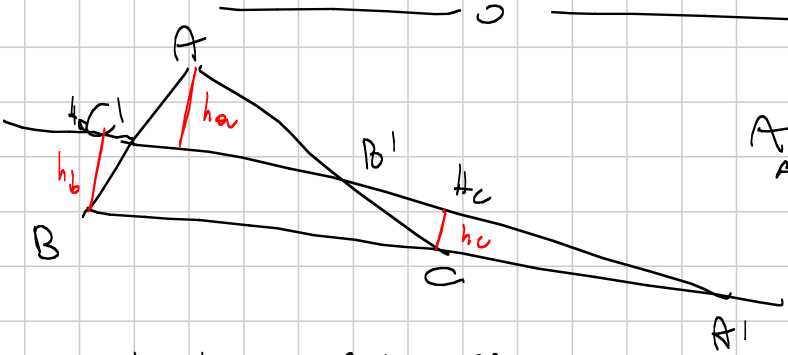
AA', BB', CC' concorrono

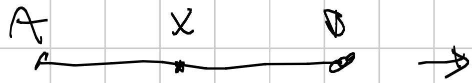
$A'' \in B'C'$ e [illegible]

A'

AA'', BB'', CC'' concorrono $\Longleftrightarrow$ A'A'', B'B'' e C'C'' concorrono.

FATELO!





AX positivo
XA negativo

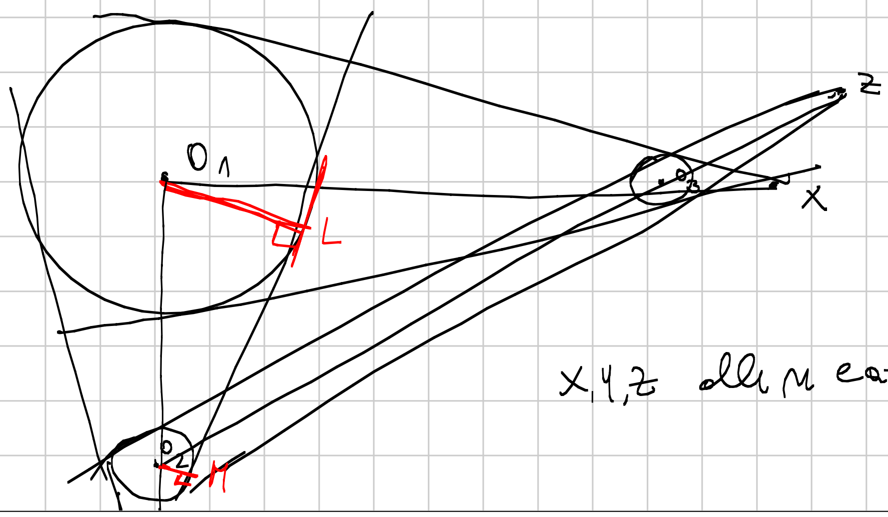
A', B', C' sui lati allineati sse $\frac{BA'}{A'C} \cdot \frac{CB'}{B'A} \cdot \frac{AC'}{C'B} = -1$

$$\frac{BA'}{A'C} = -\frac{h_b}{h_c}$$

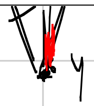
$$\frac{CB'}{B'A} = \frac{h_c}{h_a} \longrightarrow \prod \frac{BA'}{A'C} = -1$$

$$\frac{AC'}{C'B} = \frac{h_a}{h_b}$$

Esercizio



X, Y, Z allineati

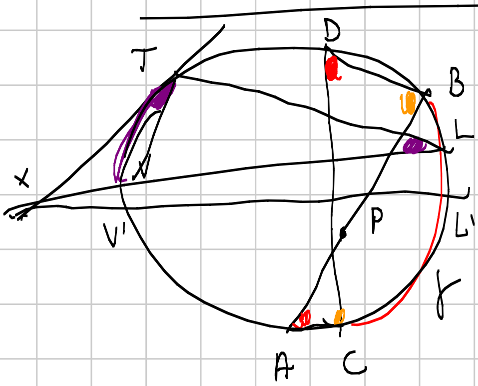


$$\frac{O_1Y}{YO_2} = \frac{O_1L}{O_2M} = \frac{-r_1}{r_2}$$

$$\frac{O_2Z}{ZO_3} = \frac{r_2}{r_3}$$

$$\frac{O_3X}{XO_1} = \frac{-r_3}{r_1}$$

$$\frac{O_1Y}{YO_2} \cdot \frac{O_2Z}{ZO_3} \cdot \frac{O_3X}{XO_1} = -\cancel{\frac{r_1 r_2 r_3}{r_1 r_2 r_3}} = -1$$



$PA \cdot PB = PC \cdot PD$

$XT^2 = XV \cdot XL = XV' \cdot XL'$

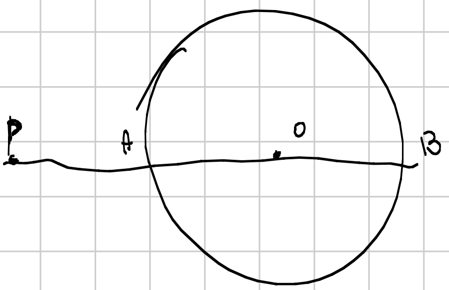
Valgono anche gli inversi

$Pow_\gamma P = -PA \cdot PB$ (Negativa)

$Pow_\gamma X = XT^2 = XV \cdot XL$ (Positiva)

P esterno

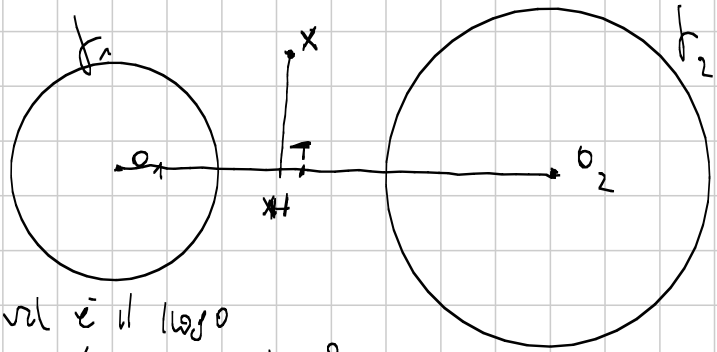
$PA \cdot PB = ?$



$(PO - OA)(PO + OB) =$

$= (d - R)(d + R) = d^2 - R^2$

$Pow_\gamma P = OP^2 - r_\gamma^2$



Qual è il luogo

$\mathrm{Pow}_{\gamma_1} X = \mathrm{pow}_{\gamma_2} X$?

$$\Downarrow$$

$$O_1X^2 - r_1^2 = O_2X^2 - r_2^2 \longrightarrow O_2X^2 - O_1X^2 = r_2^2 - r_1^2$$

$$\begin{cases} O_1T + TO_2 = O_1O_2 \\ O_2T^2 - O_1T^2 = r_2^2 - r_1^2 \end{cases} \longrightarrow \begin{cases} O_1T + TO_2 = O_1O_2 \\ O_2T - O_1T = \dfrac{r_2^2 - r_1^2}{O_1O_2} \end{cases} \longrightarrow \text{1 sola sol.}$$

$O_1O_2 \geq r_2 - r_1 \longrightarrow T$ si trova su O_1O_2

$O_1O_2 < r_2 - r_1 \longrightarrow T$ si trova fuori O_1O_2

Suppongo $\exists X \in$ luogo.

$$\mathrm{Pow}_{\gamma_1} X = \mathrm{Pow}_{\gamma_2} X \to O_2X^2 - O_1X^2 = r_2^2 - r_1^2 \longrightarrow$$

$$\longrightarrow O_2H^2 + HX^2 - (O_1H^2 + HX^2) = r_2^2 - r_1^2 \longrightarrow$$

$$\longrightarrow O_2H^2 - O_1H^2 = r_2^2 - r_1^2$$

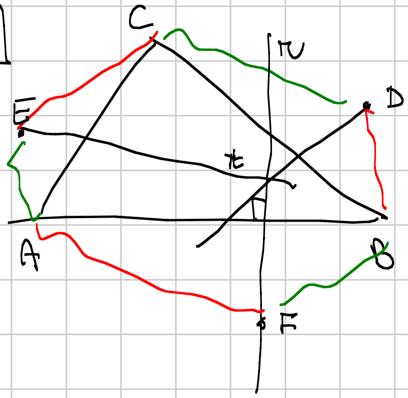
H è il punto su O_1O_2 che soddisfa la relazione. Ma allora

$H \equiv T$. $\quad XT \perp O_1O_2$

Il luogo è la perpendicolare per T ad O_1O_2

LEMMA Dati A e B due punti, il luogo dei p.ti tali che $AX^2 - BX^2 = k$ è una retta $\perp$ AB

Teorema



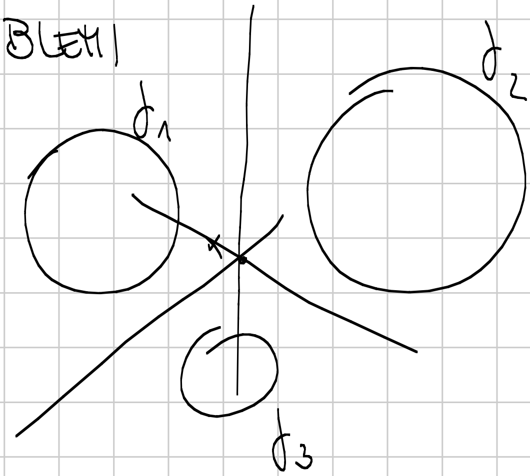
$r = \perp$ da F ad AB
$s = \perp$ da D a BC
$t = \perp$ da E a AC

r, s, t concorrono $\Leftrightarrow$

$\Leftrightarrow EA^2 + FB^2 + CD^2 = AF^2 + BD^2 + CE^2$

PROBLEMI

(1)



X ∈ asse radicale (γ_1, γ_2)

$Pow_{\gamma_1} X = Pow_{\gamma_2} X$

X ∈ asse radicale (γ_1, γ_3)

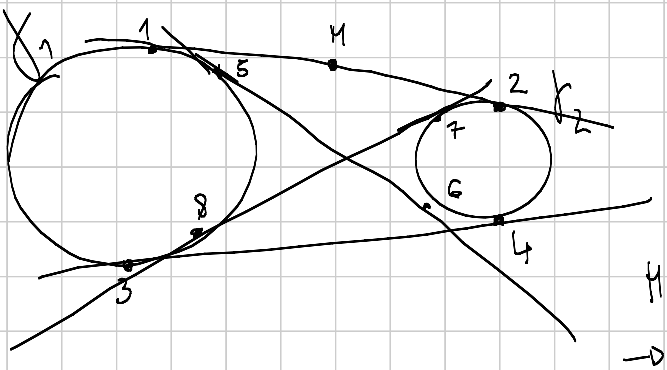
$Pow_{\gamma_1} X = Pow_{\gamma_3} X$

$\Downarrow$

$Pow_{\gamma_2} X = Pow_{\gamma_3} X \rightarrow$

$\rightarrow$ X ∈ asse radicale (γ_2, γ_3)

(2)



I punti medi di 12, 34, 56, 78?

Appartengono all'asse radicale

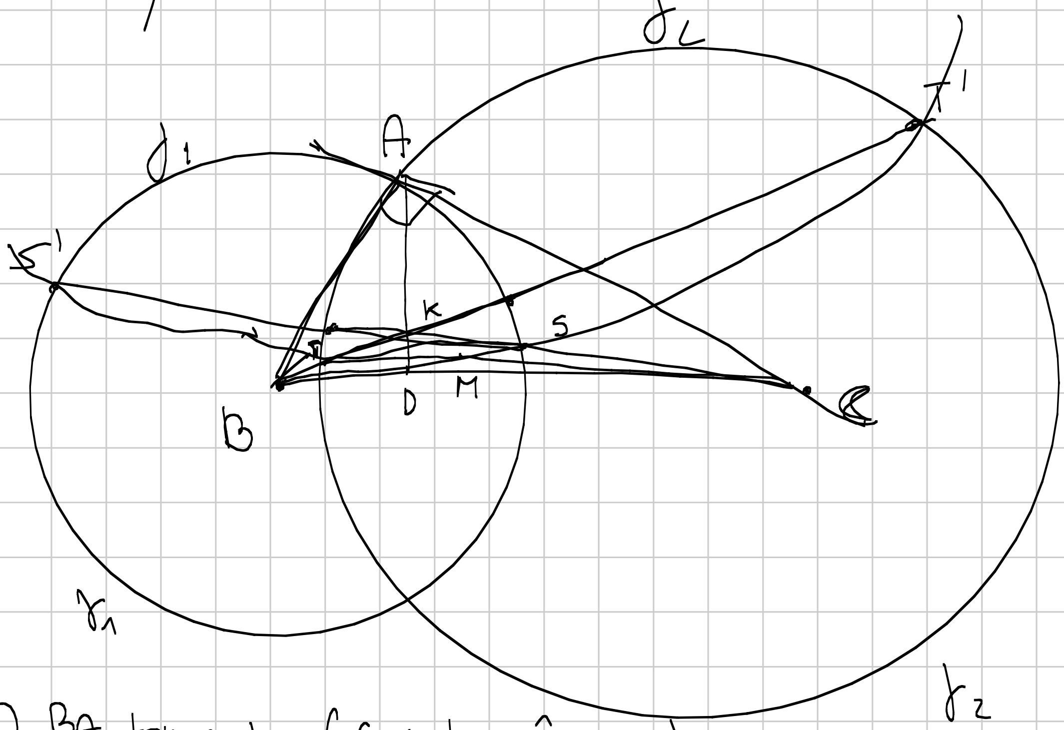
$M1 = M2 \rightarrow M1^2 = M2^2 \rightarrow$

$\rightarrow Pow_{\gamma_1} M = Pow_{\gamma_2} M$

Quindi M ∈ asse radicale

Quindi tutti i punti medi delle tangenti comuni sono allineati sull'asse radicale.

IMO 5/2012



① BA tange γ_2 (C centro, $B\hat{A}C = 90°$)

CA tange γ_1 (B centro, $B\hat{A}C = 90°$)

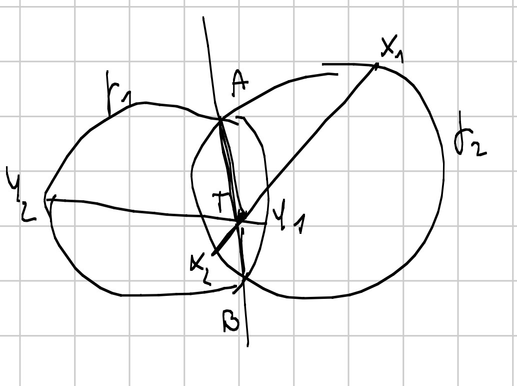
② AD è asse radicale di γ_1 e γ_2 perché $pow_{\gamma_1} A = pow_{\gamma_2} A$ e $AD \perp BC$

Fatto da casa

$T \in$ asse radicale di γ_1, γ_2. Tar $\cap\, \gamma_1 = \{Y_2, Y_1\}$

$T \cap \gamma_2 = \{X_2, X_1\}$

$X_1 X_2 Y_1 Y_2$ ciclico



$$Pow_{\gamma_1} T = TY_1 \cdot TY_2 = TA \cdot TB$$
$$Pow_{\gamma_2} T = TX_1 \cdot TX_2 = TA \cdot TB$$

$TX_1 \cdot TX_2 = TY_1 \cdot TY_2 \iff X_1Y_1X_2Y_2$ ciclico

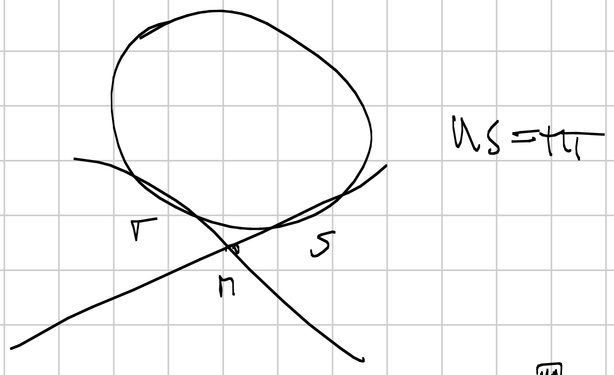
(3) S, T, S', T' sono conciclici

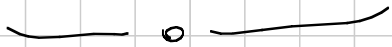
La nostra speranza è che BS, CT tangono la nuova circonferenza

BS tange $\iff BS^2 \underset{\uparrow \text{speranza}}{=} \overbrace{BT \cdot BT'} = BA^2$

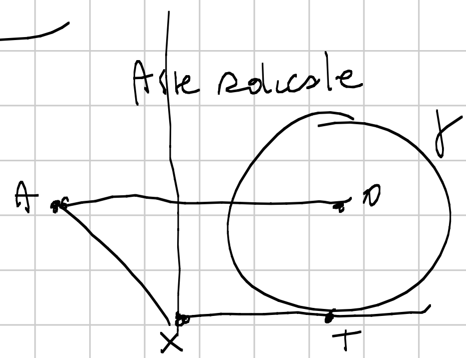
$\uparrow$ BA tange γ_2

Ma $BA = BS$ quindi la speranza è vera! BS tange, CT tange





Asse radicale = Asse



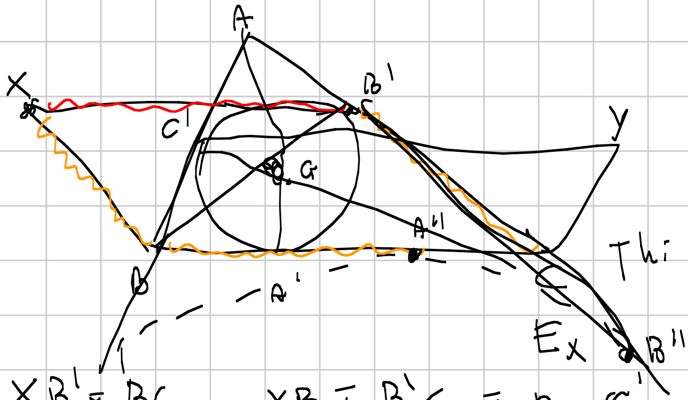
$Pow_{O}\, X = OX^2 - r^2$

$Pow_A\, X = AX^2$

$Pow_\gamma\, X = OX^2 - r^2$

$OX^2 - r^2 = AX^2 \to OX^2 - AX^2 = r^2$

BST 2010/5



$BCB'X$, $CBC'Y$ paral.

Th: $GX = GY$

$XB' = BC$, $XB = B'C = p - c$

$BA'' = p - c = BX$

X come circonferenza degenere $BX = BA'' \to$

$\to BX^2 = BA''^2 \to$

$\to Pow_X B = Pow_{E_X} B$

$B'B'' = AB'' - AB' = a = BC = XB'$

$ p - (p - a)$

$B'B'' = XB' \to$

$\to B'B''^2 = XB'^2 \to$

$\to Pow_{E_X} B' = Pow_X B'$

$\to BB'$ è asse radicale di X e E_X

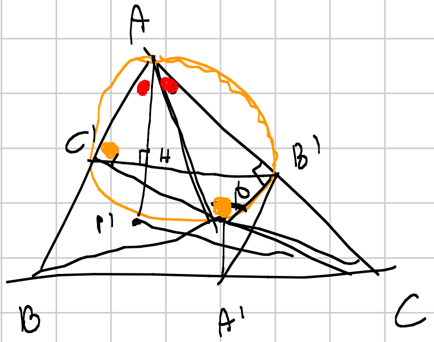
CC' è asse radicale fra Y e E_X

(X, Y, E_X)

$BB' \cap CC' = G$ ed è il punto per cui passa l'asse radicale fra X e Y

Ma l'asse radicale fra X e Y è l'asse, quindi $G \in$ asse XY, $GX = GY$

TRIANGOLI PEDALI

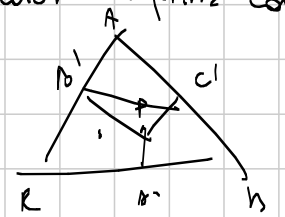


$AC'PB'$ ciclico

Se traccio la perpendicolare da A a $B'C'$, $C'\hat{A}H = P\hat{A}B'$ per conto di angoli

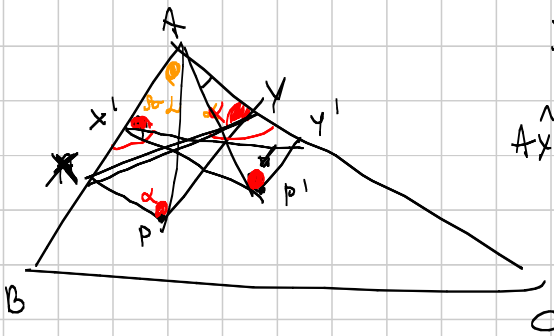
① Le perpendicolari condotte da A a $B'C'$, da C a $A'B'$, da B a $A'C'$ sono le simmetriche di AP, CP, BP rispetto alle bisettrici giuste. Ciò vuol dire che siccome AP, BP, CP concorrono le perpendicolari di prima concorrono in P'

1) Proprietà



$AP' \perp B'C'$ et simila.

Cosa posso dire su $XX'YY'$?



$A\hat{X'}Y' = A\hat{P'}Y' = 90 - P'\hat{A}Y'$

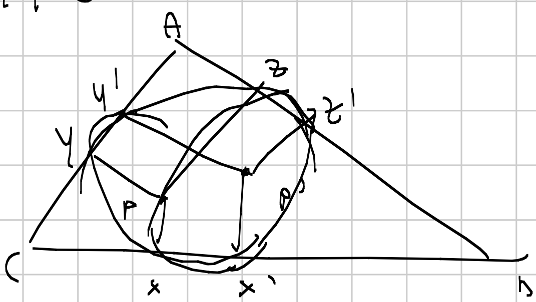
$= 90 - \alpha$

$\Downarrow$

$AP'Y' = \alpha = A\hat{X'}Y'$

Per uguaglianze di angoli

$XX'YY'$ è ciclico



$YY'ZZ'$ (γ_1), $XX'YY'$ (γ_2), $XX'ZZ'$ (γ_3) ciclici

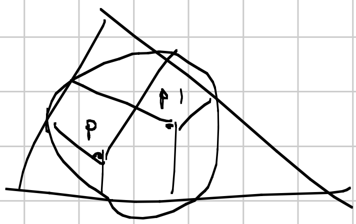
YY' è asse radicale fra γ_1 e γ_2

XX' " " γ_2 e γ_3

ZZ' è " γ_1 e γ_3

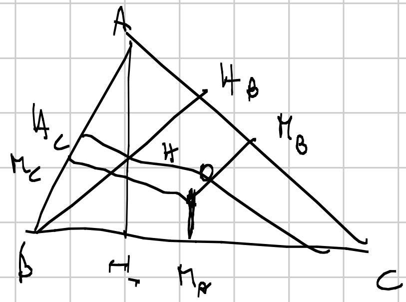
Ma questi dovrebbero concorrere. Però non lo fanno! Assurdo! Quindi non è vero che stanno su tre circonferenze ovvero ma su una sola

2)



I triangoli pedali di P e P' sono conciclici

Es. $P \equiv O$, $P' \equiv H$



$H_A, H_B, H_C, M_A, M_B, M_C$ stanno sulla stessa circonferenza (Cfr. di Feuerbach)

(e coll.)

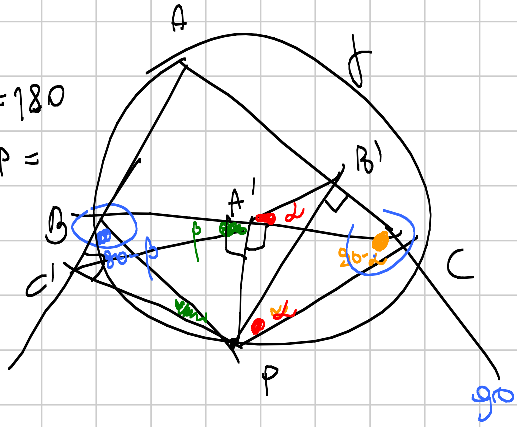
Tutti i punti sulla circ circoscritta fanno degenerare il triangolo pedale

Se $P \in \gamma$ A', B', C' allineati

$A\hat{B}P + A\hat{C}P = 180$

$A\hat{C}P = 180 - A\hat{B}P =$

$= P\hat{B}C'$

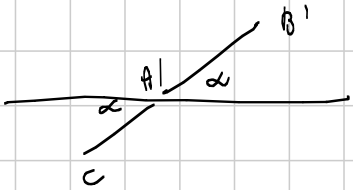


$B'CPA'$ ciclico $\rightarrow$

$\rightarrow B'\hat{C}P = 90-\alpha$

$BC'A'P$ ciclico

$90-\alpha = 90-\beta$

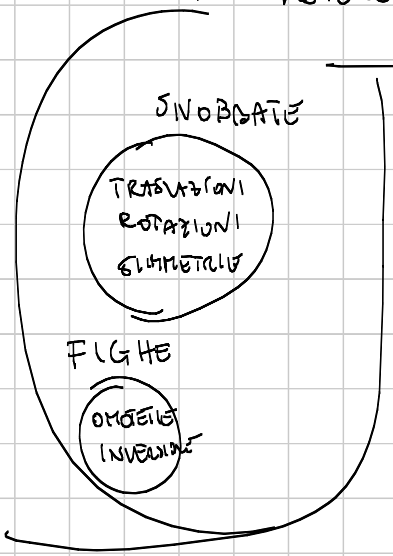


$\alpha = \beta$

B', A', C' allineati

La retta $A'B'C'$ si chiama retta di Simson di P

Proprietà interessante (difficile). Il punto medio di PH dove H è l'ortocentro, sta sulla retta di Simson di P



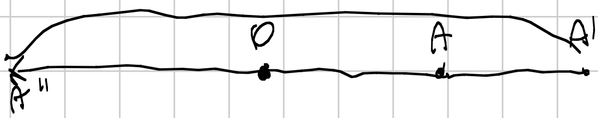
OMOTETIA (O, k) $k \in \mathbb{R}$

O $\quad$ A

$A \to A'$ $\qquad$ O, A, A' allineati

$$\frac{OA'}{OA} = k$$

- Se $k > 0$, A, A' stanno dalla stessa parte rispetto ad O
- Se $k < 0$ A, A' stanno da parti opposte rispetto ad O

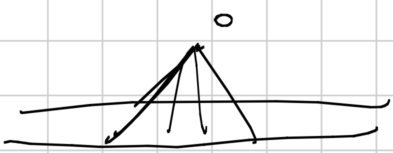


Centro O rapporto 2 (A')

" " " -2 (A'')

Cosa mantengono le omotetie:

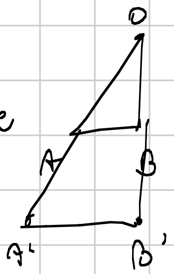
1) Retta $\to$ Retta parallela



2) Rapporti fra distanze sono mantenuti e fanno k

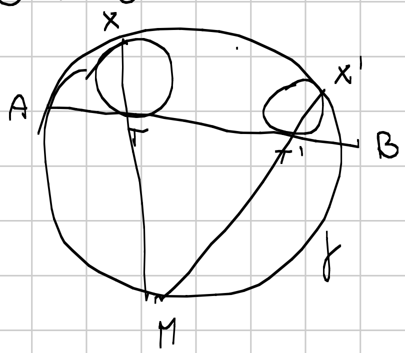
b) Mantiene gli angoli

c) Circonferenze $\to$ Circonferenze

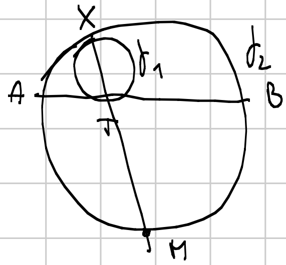


$$\frac{OA}{OA'} = \frac{AB}{A'B'}$$

USIAMOLE!

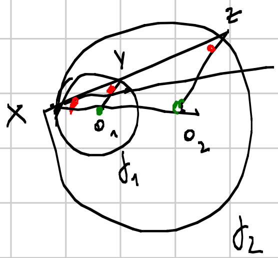


Th XT, $X'T'$ concorrono su γ.



Lemma noto

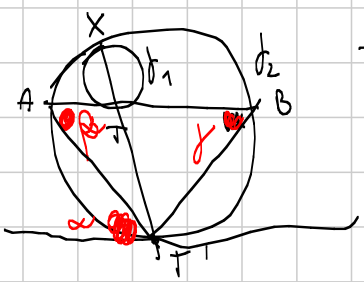
X, T, M punto medio di AB sono allineati



$$\frac{XZ}{XY} = \text{costante} = \frac{XO_2}{XO_1} = \frac{r_2}{r_1}$$

XYO_1 è isoscele

XZO_2 è isoscele



Dopo l'omotetia

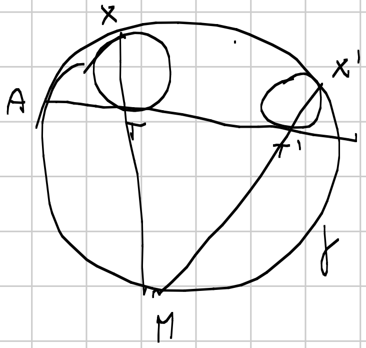
$T \to T'$

$AB \to$ tangente in T'

$\alpha = \beta$ perché alterni interni

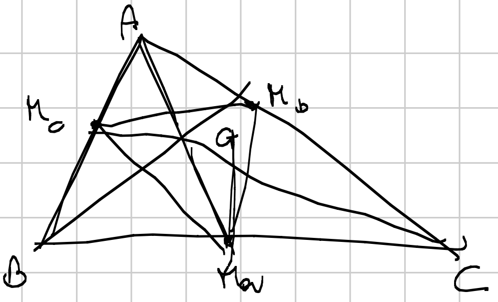
$\alpha = \gamma$ perché angoli alla circonferenza $\to$

$\to \beta = \gamma \to T'$ punto medio dell'arco AB



Per questo mostrato XT e $X'T'$ concorrono in M medio di AB. ∎

②



$$\frac{AG}{GM_a} = 2 = \frac{BG}{GM_b} = \frac{CG}{GM_c}$$

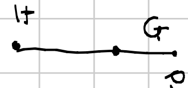
Esiste un'omotetia di centro G e rapporto $k = -\frac{1}{2}$ che manda $A \to M_a$, $B \to M_b$, $C \to M_c$

$$H_{ABC} \to H_{M_aM_bM_c}$$

$$M_a H_{M_aM_bM_c} \perp M_bM_c \parallel BC \to M_a H_{M_aM_bM_c} \perp BC$$

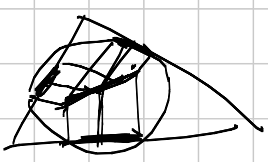
$\to M_a H_{M_aM_bM_c}$ è l'asse $\to H_{M_aM_bM_c} = O$

$$H \to O$$

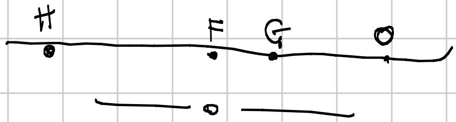


H, G, O sono allineati (retta di Eulero) $\frac{OG}{GH} = \frac{1}{2}$

Da prima il centro della cfc circoscritta il pedale di P e P' è a metà fra questi due

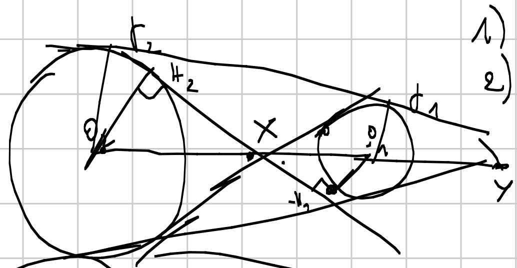


Da prima: F centro della circonferenza di Feuerbach è il punto medio di OH



$$\frac{OG}{GF} = 2$$

Date Γ_1, Γ_2 quali omotetie esistono che mandano una nell'altra?



1) il centro sta su O_1O_2
2) il rapporto è obbligato ed è $\frac{r_2}{r_1}$

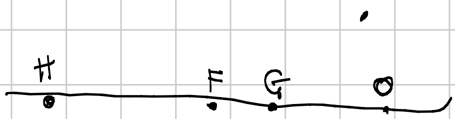
I punti sono le intersezioni delle tangenti comuni esterne e interne

$$\frac{O_2X}{XO_1} = \frac{O_2H_2}{O_1H_1} = \frac{r_2}{r_1}$$

$$\frac{O_2Y}{YO_1} = \frac{r_2}{r_1}$$

Quali sono i centri di omotetia di Feuerbach e circoscritta?

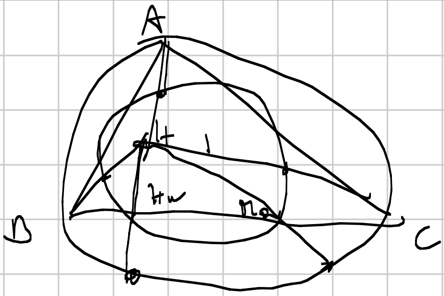
G è uno dei centri di omotetia fra Feuerbach e ⊙ABC



$$\frac{r_{\text{circoscritta}}}{r_{\text{Feuerbach}}} = 2$$

$$\frac{OY}{YF} = 2$$

Quindi H è l'altro centro di omotetia fra Feuerbach e ⊙ABC.



L'omotetia di centro H e fattore 2/

$H_a \to$ simmetrico di H rispetto a BC

$M_a \to$ simmetrico di H rispetto a M_a

$\boxed{\text{LEMMA}}$ I simmetrici di H rispetto ai lati e i simmetrici di H rispetto ai punti medi dei lati stanno sulla circoscritta.

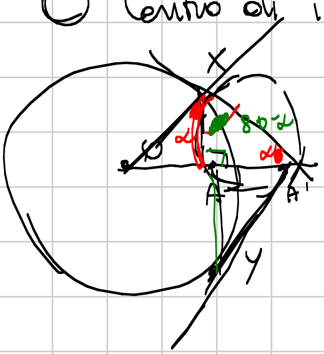
$\boxed{\text{FATTO 2}}$ Anche i punti medi di AH, BH e CH sono su Feuerbach

Esercizio (difficile) Nagel, Incentro, Baricentro sono allineati

e $\dfrac{GN}{NI} = 2$

INVERSIONE CIRCOLARE

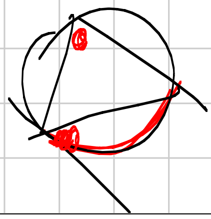
O centro di inversione   circonferenza centrata in O di raggio r.



$f(A) = A'$

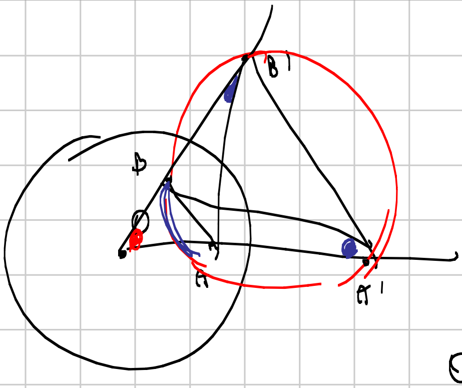
O, A, A' sono allineati, A, A' stanno dalla stessa parte rispetto ad O e $\underline{OA \cdot OA' = r^2}$

1) X, A, Y sono allineat. $OX^2 = r^2 = OA \cdot OA' \to$
$\to X\hat{A}A' = 90°$



Analogamente $A'\hat{A}Y = 90° \to X, A, Y$ allineati

Le distanze?



$OA \cdot OA' = OB \cdot OB' = r^2$

$\Downarrow$

$ABA'B'$ è ciclico

$\overset{\triangle}{OBA'} \sim \overset{\triangle}{OB'A}$

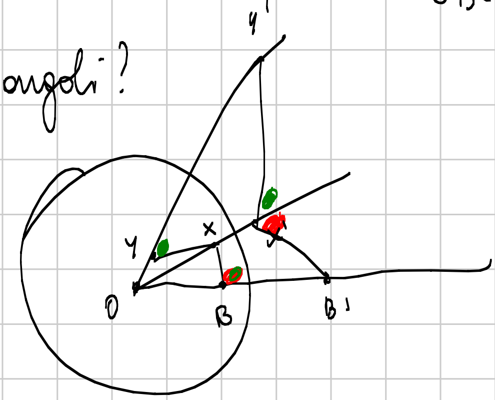
$\Downarrow$

$$\frac{AB}{A'B'} = \frac{OB \cdot OA}{r^2} \Leftarrow \frac{AB}{A'B'} = \frac{OA \cdot OB}{OB' \cdot OB}$$

$$\hookrightarrow A'B' = AB \cdot \frac{r^2}{OB \cdot OA}$$

2) E gli angoli?

$\widehat{BXY}$ e $\widehat{B'X'Y'}$?



$\widehat{B'X'Y'} = \bullet + \bullet =$

$= 180 - \widehat{OBX} + 180 - \widehat{OYX} =$

$= 360 - \widehat{OBX} - \widehat{OYX} =$

$= \widehat{BXY} + \widehat{YOB}$

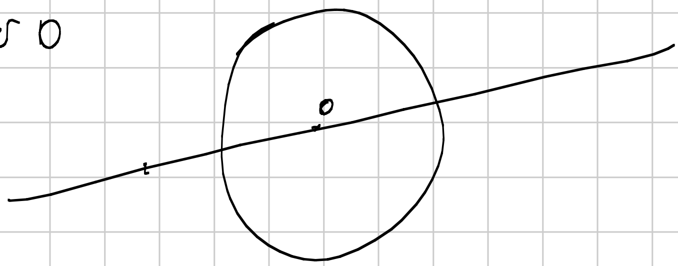
Lemma $\widehat{B'X'Y'} = \widehat{BXY} + \widehat{BOY}$

3) Dove vanno le cose?

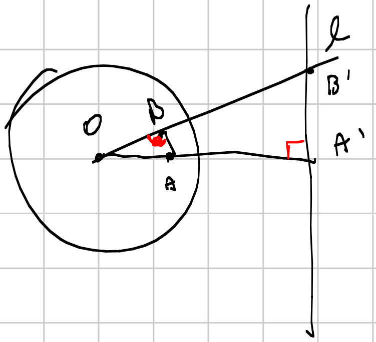
a) Una retta per O

$\Downarrow$

Se stessa



b) Una retta qualsiasi $\longrightarrow$? Circonferenza di diametro OX, dove X è l'inverso dell'intersezione fra ℓ e la perpendicolare passante per O

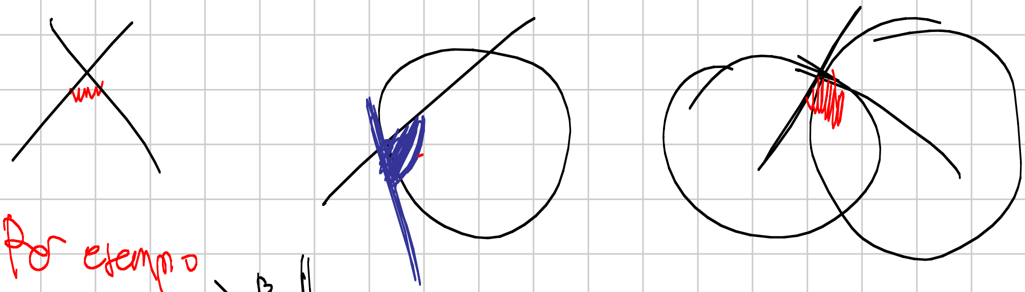


c) Una cfr passante per O $\longrightarrow$ retta

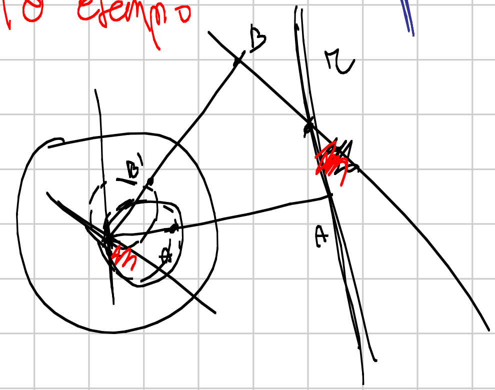
d) Una cfr generica dove va? $\longrightarrow$ Cfr generica

Idea: Con le relazioni sugli angoli dimostrare che A, B, C, D ciclici $\longrightarrow$ A', B', C', D' ciclici

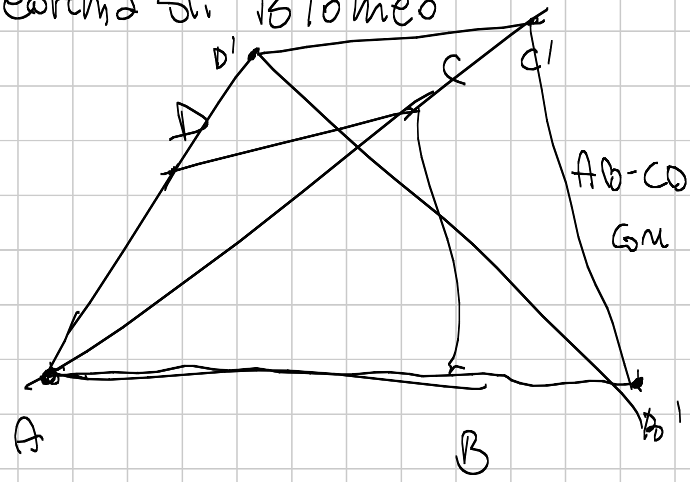
4) Gli angoli si mantengono



Per esempio



Teorema di Tolomeo



$AB \cdot CD + BC \cdot AD \geq AC \cdot BD$
con uguaglianza se $\odot ABCD$

$$D'C' = DC \cdot \frac{r^2}{AD \cdot AC} \qquad D'B' = DB \cdot \frac{r^2}{AD \cdot AB}$$

$$B'C' = BC \cdot \frac{r^2}{AB \cdot AC}$$

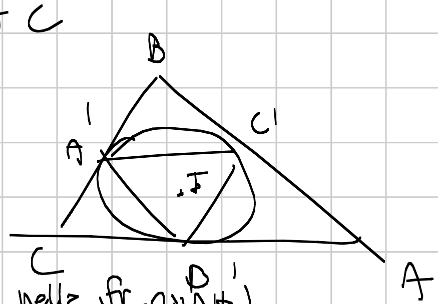
$$D'C' + C'B' \geq D'B' =$$

$$\frac{DC}{AD \cdot AC} + \frac{BC}{AB \cdot AC} \geq \frac{DB}{AD \cdot AB}$$

$$AB \cdot DC + BC \cdot AD \geq DB \cdot AC$$

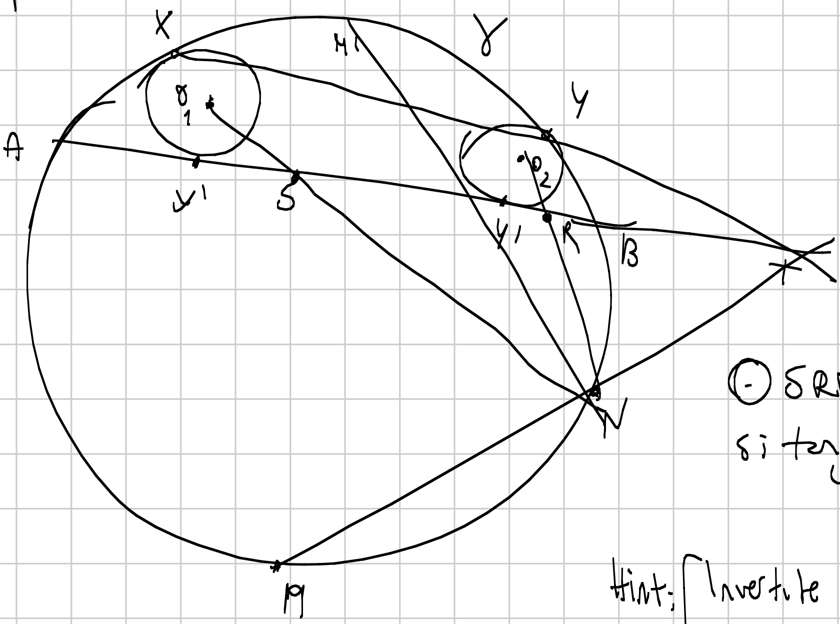
Se fosse ciclico, degenera e vale l'uguaglianza

1) Dimostrare che OI è la retta di Eulero di $A'B'C'$



(Hint: inverti nella circonferenza inscritta)
Ricorda che $\odot[E] \to \odot[F]$ allora E, F sono allineati col centro d'inversione

c) X esperti



⊙ SRN, γ si tangono in N

Hint: [Invertire in N + simmetria rispetto a NM' dove M' è pto medio dell'altro arco AB]

FINE

StheW

Teoria dei Numeri 1 (BASIC)

Titolo nota 03/09/2012

1ª parte
- divisibilità (mcd)
- fattorizzazione, (valutazioni p-adiche)
- scrittura in base b
- $ax+by=c$

(appl.)

---

a divide b vuol dire che b è multiplo di a o equivalentemente che esiste un intero k tale che $\boxed{k \cdot a = b}$

$a \mid b \iff a \cdot k = b$ (per qualche intero k)

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

$a \mid b \qquad a \mid c \qquad a \mid b+c \qquad a \mid b-c$

$a \mid kb + jc + ha$

fatti notevoli:

- $a-b \mid a^n - b^n \qquad \frac{a^n-b^n}{a-b} = a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots + b^{n-1}$
- $a+b \mid a^n + b^n$ (solo se n è dispari)

$$a^3+b^3$$
$$a^2+b^2 \mid a^6+b^6$$
$$(a^2)^3+(b^2)^3$$

$$a^2+b^2 \mid a^6+b^6$$

$c=a^2 \quad d=b^2$

$$c+d \mid c^3+d^3$$

p si dice primo se $(p>1)$

- $p \mid ab \Rightarrow p \mid a$ o $p \mid b$

  se p divide un prodotto allora divide uno dei fattori

- $p = ab \Rightarrow a=\pm 1$ o $b=\pm 1$ (irriducibili)

(primi di Mersenne)

Es. 2^n-1 è primo $\Rightarrow$ n è primo

[se n è primo $\Rightarrow 2^n-1 \equiv 1 \ (n)$]

Supponiamo $p \mid n$ $\quad 1<p<n$ (Hp1)

$$\underbrace{(2^p)-(1^p)}_{a-b} \mid a^{\frac{n}{p}} - b^{\frac{n}{p}} = 2^n - 1^n$$

$$2^p-1 \mid 2^n-1$$

Abbiamo trovato un fattore che divide 2^n-1

$$(2^p-1)\cdot k = 2^n-1$$

ma (Hp1) $\Rightarrow 1 < 2^p-1 < 2^n-1$

(primi di fermat) ($2^{64}+1$ non è primo)

Es. 2 2^n+1 è primo $\Rightarrow$ n è una potenza di 2

Proviamo a dimostrarlo per assurdo, quindi prendo $n = 2^k \cdot d$ con d dispari, $d > 1$, ora vorrei far vedere che 2^n+1 non è primo

$$2^{2^k} + 1^{2^k} \mid 2^{2^k \cdot d} + 1^{2^k \cdot d} \quad (?)$$

$$2^{2^k} + 1^{2^k} \mid \left(2^{2^k}\right)^d + \left(1^{2^k}\right)^d$$

Massimo Comun Divisore (MCD)

MCD (a, b) $\left\{ (a,b) \text{ è il MCD tra } a \text{ e } b \right\}$

<u>Fattorizzazione</u>: Ogni numero naturale è esprimibile in modo <u>UNICO</u> come prodotto di primi

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$$

$12 = 2^2 \cdot 3$ $\qquad$ $128 = 2^7$

$33 = 3 \cdot 11$ $\qquad$ $2012 = 2^2 \cdot 503$

$2013 = 3 \cdot 11 \cdot 61$

$$2^2 \cdot 503 = 2012 = a^2 - b^2 = (a+b)(a-b)$$

$$\cancel{\begin{cases} a+b = 503 \\ a-b = 2^2 \end{cases}} \qquad \begin{cases} a+b = 503\cdot 2 \\ a-b = 2 \end{cases} \qquad \cancel{\begin{cases} a+b = 503\cdot 2^2 \\ a-b = 1 \end{cases}}$$

$$2a = 507$$

$a = 504$
$b = 502$

$S + D =$ pari

$$2012 = 504^2 - 502^2$$

se $2 \mid n$ ma $4 \nmid n$ $\Rightarrow$ no sol. a $n = a^2 - b^2$

MCD fatto con la fattorizzazione

$a = p_1^{\alpha_1} \, p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ $\qquad 2^2 \cdot 3 \qquad 3 \cdot 11 \cdot 13$

$b = p_1^{\beta_1} \, p_2^{\beta_2} \cdots p_k^{\beta_k}$ $\qquad 2 \cdot 3^2 \qquad 3^2 \cdot 67$

$$\boxed{(a, b) = p_1^{\min(\alpha_1,\beta_1)} \, p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}} \qquad 2\cdot 3 \qquad 3$$

d è il massimo comun divisore tra a e b se per ogni c t.c. $c \mid a$ e $c \mid b$, allora $c \mid d$ e $d \mid a$ e $d \mid b$

$$a = p_1^{\alpha_1}\, p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$
$$b = p_1^{\beta_1}\, p_2^{\beta_2} \cdots p_k^{\beta_k}$$
$$c = p_1^{\gamma_1}\, p_2^{\gamma_2} \cdots p_k^{\gamma_k}$$

$$\begin{cases} c \mid a \iff \gamma_i \le \alpha_i \quad \forall i \\ c \mid b \iff \gamma_i \le \beta_i \quad \forall i \end{cases}$$

$$c \mid (a,b) \iff \gamma_i \le \min(\alpha_i, \beta_i)$$

$v_{p_i}(a) = \alpha_i$ valutazione p-adica di a = "l'esponente di p nella fattorizzazione di a"

$$v_2(a \cdot b) = v_2(a) + v_2(b)$$

$$v_2(a+b) \ge \min(v_2(a), v_2(b))$$

$$\to \quad a+b = p^\alpha \cdot k + p^\beta \cdot J = \begin{cases} p^\beta (p^{\alpha-\beta} \cdot k + J) & \alpha > \beta \\ p^\alpha (k + J \cdot p^{\beta-\alpha}) & \alpha < \beta \end{cases}$$

$v_2(10) = 1$ $\qquad v_2(10+15) = 0 \ge \min(1,0)$

$v_2(15) = 0$

$$\min\left(v_p(a), v_p(b)\right) = k \qquad a = p^k \cdot a_1$$
$$b = p^k \cdot b_1$$

$$v_p((a+b)) = v_p\left(p^k(a_1+b_1)\right) \geq k.$$

Oss. Se $v_p(a) \neq v_p(b) \Rightarrow v_p(a+b) = \min(v_p(a), v_p(b))$

Se $v_p(a) = v_p(b) \Rightarrow$ boh? $v_p(a+b)$ può essere qualunque numero $\geq$ di $\min(v_p(a), v_p(b))$

$$p = 2 \qquad v_2(a) = v_2(b) \Rightarrow v_2(a+b) \geq \min(v_2(a), v_2(b)) + 1$$

$$2^{k_1} \cdot d_1 + 2^{k_1} \cdot d_2 = 2^{k_1}(d_1 + d_2)$$

$$\underset{(2)}{v_2(1+3)} = \underset{(0)}{v_2(1)} + 2$$

$$v_p(a+b) \leq ? \qquad a = p^k - 1 \qquad v_p(a) = v_p(b) = 0$$
$$b = 1 \qquad v_p(a+b) \geq k$$

Es. Trovare il massimo valore di

$$(n^2 + 2012, (n+1)^2 + 2012)$$

$d_n = (n^2 + 2012, (n+1)^2 + 2012)$

$d_n \mid n^2 + 2012$

$d_n \mid (n+1)^2 + 2012$

$d_n \mid 2n+1$

bisogna "togliere" n

$d_n \mid 2\cdot(n^2 + 2012)$

$\boxed{d_n \mid n(2n+1)}$ $-$

$d_n \mid 2n+1$

$d_n \mid 2\cdot(4024 - n)$

$d_n \mid 2n+1$ $+$

$d_n \mid 8049$

$3 \cdot 2683$

noi vorremo un n per cui $d_n = 8049$

$d_n \mid 2n+1$ $\qquad 8049 \mid 2n+1$

$8049 = 2n+1$? $\qquad 4024$

$8049 \mid (4024)^2 + 2012$

$$(n^2+2012, (n+1)^2+2012) =$$

$$= (n^2+2012, 2n+1)$$

$$= (2n^2+4024, 2n+1)$$

$$= (4024-n, 2n+1)$$

$$= (8049, 2n+1)$$

$$d_n = (8049, 2n+1)$$

$$d_n = (n^3+56, (n+1)^3+56)$$

quando è massimo?

$$d_n = (407+6n, 7n+2-68\cdot 407)$$

Teorema di Bezout

fissiamo a,b,c, vogliamo trovare x,y tali che

$$\boxed{ax+by=c}$$

$$2x+3y=4 \quad (1)$$

$(x,y)=(2,0)$
$(x,y)=(-1,2)$
$(x,y)=(5,-2)$
$(x,y)=(-4,4)$

Cerco di risolvere $2x+3y=0$ (2) $(x,y)=(3k,-2k)$
"omogeneo"

$$2x=-3y \xrightarrow{x=3k} -2k=y$$

se (x_0, y_0) è sol. di (1) e (x_1, y_1) è sol. di (2) allora

$$2x_0 + 3y_0 = 4$$
$$2x_1 + 3y_1 = 0$$

$$2(x_0+x_1) + 3(y_0+y_1) = 4$$

(x_0+x_1, y_0+y_1) è sol. di (1)

$(2+3k, -2k)$ sono sol. di (1) (al variare di k)

$$2x + 4y = 3$$

NON CI SONO SOLUZIONI PERCHÉ IL PRIMO MEMBRO È PARI MENTRE IL SECONDO " È DISPARI ASSURDO!

$$ax + by = c$$

oss. se $d \mid a$ e $d \mid b \Rightarrow d \mid c$

$\rightsquigarrow$ $\boxed{(a,b) \mid c}$ ⟵ CONDIZIONE NECESSARIA AFFINCHÉ CI SIANO SOLUZIONI

Th. (Bezout) (La condizione è anche sufficiente)

Dati $a, b \in \mathbb{Z}$, esistono due interi x, y, tali che

$$a x + b y = (a, b)$$

Se volessi risolvere

$$ax + by = c$$

con $(a,b) \mid c \Rightarrow c = k \cdot (a,b)$

$$(x, y) = (k \cdot x_B,\ k \cdot y_B)$$

$$\boxed{ax + by = c}$$

$$= a k x_B + b k y_B = k\,(a x_B + b y_B) =$$

$$= k\,(a,b) = c$$

$(401, 355)$	$401 = 1 \cdot 355 + 46$	$61 \cdot 355 - 54 \cdot 401 = 1$
$= (355, 46)$	$355 = 7 \cdot 46 + 33$	$7 \cdot 355 - 54 \cdot 46 = 1$
$= (46, 33)$	$46 = 1 \cdot 33 + 13$	$7 \cdot 33 - 5 \cdot 46 = 1$
$= (33, 13)$	$33 = 2 \cdot 13 + 7$	$2 \cdot 33 - 5 \cdot 13 = 1$
$= (13, 7)$	$13 = 1 \cdot 7 + 6$	$2 \cdot 7 - 1 \cdot 13 = 1$
$= (7, 6)$	$7 = 1 \cdot 6 + 1$	$\leftarrow \; 7 - 1 \cdot 6 = 1$

$\overset{\shortparallel}{(6,1)}$ $\quad 6 = 6 \cdot 1$

[Curiosità: le coppie più "lente" sono (F_n, F_{n+1})]

Scrittura in base

$$n = b_0 + b_1 \cdot b + b_2 \cdot b^2 + b_3 \cdot b^3 + \dots + b_k \cdot b^k =$$

$$= \underline{b_k b_{k-1} b_{k-2} \dots b_0}_{\,b}$$

$$\underline{10}_2 = 2 = \underline{2}_3 = \underline{2}_4 = \underline{2}_{2012}$$

$$\underline{1001}_3 = 28 = \underline{11100}_2$$

$$7 \cdot 4 = \underline{111}_2 \cdot \underline{100}_2 = \underline{11100}_2$$

Es. 15 test iniziale $(a > b,\ c > d;\ b > d)$

$$\frac{2^a - 2^b}{2^c - 2^d} = \frac{2^b(2^{a-b} - 1)}{2^d(2^{c-d} - 1)} =$$

$$= 2^{b-d} \cdot \frac{2^\alpha - 1}{2^\beta - 1}$$

Quando $2^\beta - 1 \mid 2^\alpha - 1$? CLAIM: $\beta \mid \alpha$

1^a parte se $\beta \mid \alpha \Rightarrow 2^\beta - 1 \mid 2^\alpha - 1$

$$2^\beta - 1 \mid (2^\beta)^{\frac{\alpha}{\beta}} - (1)^{\frac{\alpha}{\beta}} = 2^\alpha - 1$$

2^a parte $2^\beta - 1 \mid 2^\alpha - 1 \Leftrightarrow$

$$2^\beta - 1 \mid 2^\beta (2^{\alpha-\beta} - 1) \Leftrightarrow$$

$$2^\beta - 1 \mid 2^{\alpha-\beta} - 1$$

$$\boxed{a \mid bc \,, \; (a,b) = 1 \Leftrightarrow a \mid c}$$

1^o caso $\alpha - \beta < \beta$

Fatto se $a \mid b$ (e $b \neq 0$)

allora $|a| \leq |b|$

$$a \cdot k = b$$

$$|a| \leq |a| \, |k| = |b|$$

Se $0 < |b| < |a| \Rightarrow a \nmid b$

$$|2^{\alpha-\beta} - 1| < |2^\beta - 1|$$

NON contraddice la tesi

solo quando $\alpha > \beta$

ma $\alpha = \beta \Rightarrow \beta \mid \alpha$ che contraddice l'ipotesi

se itero il procedimento di prima arrivo a

$$2^\beta - 1 \mid 2^r - 1 \qquad 0 \le r < \beta$$

$r = 0 \Rightarrow \beta \mid \alpha$

$r \neq 0 \Rightarrow$ assurdo

$$\boxed{2^\beta - 1 \mid 2^\alpha - 1 \Leftrightarrow \beta \mid \alpha}$$

Es. $\left(3^\alpha - 1, 3^\beta - 1\right) = 3^{(\alpha,\beta)} - 1$

$\left[\,(a, b) = (a, b-a)\,\right] \leftarrow$ parte questa

$= (b, b-a)$

numeri della forma $2^r \cdot \dfrac{2^\alpha - 1}{2^\beta - 1}$. Dal

Fatto precedente $\alpha = k\beta$

$$2^\gamma \frac{2^{k\beta} - 1}{2^\beta - 1} = 2^\gamma \left(2^{(k-1)\beta} + 2^{(k-2)\beta} + \dots + 2^\beta + 1\right) =$$

$$
N = \left(\begin{array}{r} 1 + \\ 1\overbrace{0000}^{\beta} + \\ 1\overbrace{00000000}^{2\beta} + \\ 1\overbrace{-- \; 0000 \; 0}^{2\beta} + \\ \vdots \\ 1\overbrace{-----\;0}^{(k-1)\beta} = \end{array} \right)
$$

$$
1\underbrace{0000}_{\beta-1}1\underbrace{000}_{\beta-1}1\underbrace{000}_{\beta-1}1\underbrace{000}_{\beta-1}1\,00000
$$

$$
\overbrace{1\underbrace{0000}_{a}1\underbrace{00\cdots}_{a}1\underbrace{0\cdots}_{a}1 \cdots}^{n^\circ \text{ uni } b} 1\underbrace{000}_{c}\,{}_2 =
$$

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

$$9 = 101_2 \qquad 11010000000_2$$

$$13 = 1101_2$$

$$\boxed{1101}\,0000000000000_2$$

$$\boxed{c = 2 \quad d = 1 \quad b = 1}$$

$$\frac{2^a - 2^b}{2^c - 2^d} = 2^{a-1} - 1 \qquad a = p.$$

ARITMETICA MODULARE (O DELL'OROLOGIO)

Sono le 8. Tra 5 ore che ore sono? l'una

"$8+5=1$" "$5+12\cdot 8=5$"

"$8+24=8$" "$5+11\cdot 8=9$"

"$8+77=1$"

Le ore sono uguali a meno di multipli di 12. Considero gli interi "a meno" di multipli di 12.

$$(a+12k)(b+12J) =$$

$$= ab + 12kb + 12Ja + 144Jk$$
$$= ab + 12h$$

$$(3k\pm 1)^2 = 1 \pm 6k + 9k^2 = 1 + 3J$$

"un numero non multiplo di 3, elevato al quadrato, dà resto 1 diviso per 3"

"è congruo a 1 modulo 3"

$$(2k+1)^2 = 1 + 4k + 4k^2 = 1 + 4(k(k+1))$$
$$= 1 + 8J$$

generico $2|n$ ma $4 \nmid n$

$4k+2$

$2d = 2(2k+1) = 4k+2$

"un q. di un n° disp. è $\equiv 1 \mod 8$"

$a \equiv b \quad (n) \qquad a = b + kn$

$c \equiv d \quad (n) \qquad c = d + Jn$

$a + c \equiv b + d \quad (n) \qquad a + c = b + d + n h_1$

$a \cdot c \equiv b \cdot d \quad (n) \qquad ac = bd + n \cdot h_2$

Come funziona la divisione?

Cosa vuol dire dividere per 2?

Vuol dire moltiplicare per $\frac{1}{2}$. Chi è $\frac{1}{2}$?

$\frac{1}{2}$ è l'inverso moltiplicativo (detto reciproco) di 2, cioè quel numero che, moltiplicato per 2, dà come prodotto 1.

Se siamo in $\mathbb{N}$, esiste l'inverso di 1? sì

" " " 2? No

Se siamo in $\mathbb{Z}/n\mathbb{Z}$, esiste l'in. di 1? sì

esiste " " 2? non si sa

$\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}/3\mathbb{Z}$

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

2 ha un inverso e questo è 2 stesso

$$2^{-1} \equiv 2 \quad (3)$$

Quando esiste l'inverso di a modulo n? Voglio trovare x tale che

$$ax \equiv 1 \quad (n)$$

$$ax = 1 + k \cdot n$$

$$ax - k \cdot n = 1 \qquad (*)$$

Ho riformulato in questo modo: devo trovare x, k tali che $(*)$ sia verificata, ossia esistono sse $(a,n) \mid 1 \iff (a,n) = 1$.

Per trovare nei fatti x, mi basta applicare l'algoritmo di Bezout.

$$a \equiv b \quad (n)$$

$$c \equiv d \quad (n) \qquad (n, c) = 1$$

$$[(n, c) = (n, c + kn)]$$

$$a \cdot c^{-1} \equiv b \cdot d^{-1} \quad (n)$$

$$a \equiv b \quad (n)$$

(i) $2 | a \quad 2 | b \quad 2 \nmid n$

$$a \cdot 2^{-1} \equiv b \cdot 2^{-1} \quad (n)$$

$$\left(\frac{a}{2}\right) \qquad \left(\frac{b}{2}\right)$$

$$2 \equiv 16 \quad (7)$$

$$1 \equiv 8 \quad (7) \qquad 8 \equiv 64 \quad (7)$$

$$2 \cdot 1 \equiv 2 \cdot 8$$

$$\boxed{2^{-1} \cdot 2} \cdot 1 \equiv \boxed{2^{-1} \cdot 2} \cdot 8 \quad (7)$$

$$1 \cdot 1 \equiv 1 \cdot 8$$

(ii) $2 | a \quad 2 | b \quad 2 | n$

$$a \equiv b \quad (n)$$

$$a = b + kn$$

$$\cancel{2}a' = \cancel{2}b' + k\cancel{2} \cdot n'$$

$$a' = b' + kn'$$

$$a' \equiv b' \quad (n')$$

$$\left(\frac{a}{2}\right) \equiv \left(\frac{b}{2}\right) \quad \left(\frac{n}{2}\right)$$

$a_1, a_2, a_3, \ldots, a_k$ sono numeri naturali distinti $\leq n$

Hp: $n \mid a_1(a_2-1)$

$n \mid a_2(a_3-1)$

$\vdots$

$n \mid a_{k-1}(a_k-1)$

Th: $n \nmid a_k(a_1-1)$

$n \mid a_1(a_2-1) \Rightarrow n \cdot k = a_1(a_2-1)$

$\Rightarrow a_1(a_2-1) \equiv 0 \quad (n)$

$a_1a_2 - a_1 \equiv 0 \quad (n)$

$a_1 \equiv a_1a_2 \quad (n)$

Attenzione, non possiamo dividere per a_1, o meglio non è detto.

$a_1 \equiv a_1a_2 \quad (n)$

$a_2 \equiv a_2a_3 \quad (n)$

$a_3 \equiv a_3a_4 \quad (n)$

$\vdots$

$a_{k-1} \equiv a_ka_{k-1} \quad (n)$

$a_1 \equiv a_1a_2a_3a_4a_5 \cdots a_k \quad (n)$

$a_2 \equiv a_1a_2a_3 \quad a_k$.

se avessimo $a_k \equiv a_ka_1$ otterrei $a_1 \equiv a_2 \equiv a_3 \cdots \equiv a_k \equiv a_1 \cdots a_k$

quindi tutti i numeri sono congrui tra di loro ho contraddetto l'ipotesi? sì, usando il fatto che sono tutti $0 \leq \quad < n$

$$a, b \quad a \neq b \quad e \quad a \equiv b \quad (n)$$

$$n \mid a-b \quad \Rightarrow \quad n \leq |a-b| \quad \underline{\text{no!!}}.$$

IMO - 2009 / 1.

Struttura moltiplicativa

$(2, 31) = 1$

		(31)	(11)	(5)	(3)
		5	10	4	2
2^0	$\equiv$	1	1	1	1
2^1	$\equiv$	2	2	2	2
2^2	$\equiv$	4	4	-1	1
2^3	$\equiv$	8	-3	-2	2
2^4	$\equiv$	16	5	1	1
2^5	$\equiv$	1	-1	2	2
			-2		1
			-4		2
			3		1
			-5		2
2^{10}			1		

$(a,n)=1$ è vero che esiste $J>0$ t.c.

$$a^J \equiv 1 \quad (n) \ ?$$

Posso dire (principio dei cassetti) che esistono due esp. k_1, k_2 t.c. $(k_2>k_1)$

$$a^{k_1} \equiv a^{k_2} \quad (n)$$

$$a^{k_1} \equiv a^{k_1} \cdot a^{k_2-k_1} \quad (n)$$

Ora divido per a k_1 volte e ottengo

$$1 \equiv a^{k_2-k_1} \quad (n)$$

il periodo di a^k modulo n si indica con $\mathrm{ord}_n(a)$. È il minimo $J>0$ per cui $a^J \equiv 1 \ (n)$.

- Se $a^k \equiv 1 \ (n)$ allora $\mathrm{ord}_n(a) \mid k$.

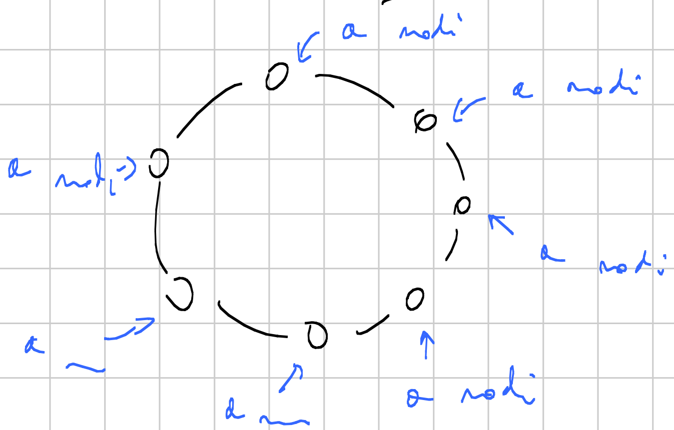
Piccolo Teorema di Fermat (LFT)

Sia p un numero primo e a un qualunque intero; allora vale

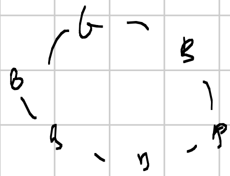
$$a^p \equiv a \quad (p)$$

Modo combinatorio (calato dal nulla)

Voglio costruire delle collane di perline, con p perline e ho a disposizione perline di a colori diversi. Quante sono le collane <u>NON</u> monocromatiche?



Scelgo in a^p modi le perline, tolgo le monocromatiche: $a^p - a$. Poiché se prendo una collana non monocromatica e la giro p volte ottengo p conf. diverse, allora



il numero di collane non monoc. è $\frac{a^p - a}{p}$

$\rightsquigarrow \quad p \mid a^p - a \quad$ cioè $\quad a^p \equiv a \ (p)$

II modo

$$\{1, 2, 3, 4, \dots, p-1\}$$

poi prendo $(a,p)=1$ $p \nmid a$

$$\{a, 2a, 3a, 4a, \dots, (p-1)a\}$$

nessuno di essi e' zero. Può essere che ci siano 2 numeri uguali modulo p?

$$i\cancel{a} \equiv j\cancel{a} \quad (p)$$

$$i \equiv j \quad (p)$$

$$1 \cdot 2 \cdot 3 \cdots (p-1) = a \cdot (2a) \cdot (3a) \cdots ((p-1) \cdot a) \quad (p)$$

$$\cancel{(p-1)!} \equiv a^{p-1} \cancel{(p-1)!} \quad (p)$$

$$1 \equiv a^{p-1} \quad (p)$$

$$a \equiv a^p \quad (p)$$

modo III, per induzione $\quad \binom{p}{i} \equiv 0 \quad (p)$ se $i \neq 0$, $i \neq p$

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \dots + \binom{p}{p-1} a + 1$$

$$\equiv a^p + 1$$

Dim. per induz. (su a) che $a^p \equiv a \quad (p)$

base induttiva: $a=0 \qquad 0^p \equiv 0 \quad (p)$

passo induttivo: Supp. che $a^p \equiv a \quad (p)$

ma allora $(a+1)^p \equiv a^p + 1 \equiv a+1 \quad (p)$.

$\square$.

$$(a,p)=1 \implies a^{p-1} \equiv 1 \quad (p)$$

$$\mathrm{ord}_p(a) \mid p-1$$

$$x^3 + y^5 = 7^k$$

lavorate
modulo primi
t.c. $3 \mid p-1$ o
$5 \mid p-1$ o
$15 \mid p-1$

N 2 – BASIC

SENIOR 2012

Titolo nota 05/09/2012

23 $m = 30$

$23 \equiv 23 \pmod{30}$ $30 = 5 \cdot 6$

$23 \equiv 3 \pmod 5$

$23 \equiv 5 \pmod 6$

Possiamo fare viceversa

$x \equiv 3 \pmod 5$

$x \equiv 5 \pmod 6$

$5 \cdot 6$

SI!

Teorema Cinese del Resto

Moduli $m_1, m_2, \dots m_k$ a due a due primi tra loro

$MCD(m_i, m_j) = 1$

Resti $r_1, r_2, \dots r_k$

Esiste un'unica classe di resto x modulo $m_1 \cdot m_2 \cdot m_3 \cdot \dots \cdot m_k$ tale che

$$x \equiv r_1 \pmod{m_1}$$
$$x \equiv r_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv r_k \pmod{m_k}$$

Esiste un unico intero che fa questo tra 1 e $m_1 m_2 \dots m_k$ (estremi inclusi)

α_i

$$\begin{aligned} \alpha_i &\equiv 0 \pmod{m_1} \\ \alpha_i &\equiv 0 \pmod{m_2} \\ &\vdots \\ \alpha_i &\equiv 1 \pmod{m_i} \\ &\vdots \\ \alpha_i &\equiv 0 \pmod{m_k} \end{aligned}$$

$$\alpha_i = \underbrace{m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k}\, \beta_i$$

$\exists\, \beta_i$ t.c. $(m_1 \cdots m_{i-1} m_{i+1} \cdots m_k) \cdot \beta_i \equiv 1 \pmod{m_i}$

$$r_1 \overset{1}{\alpha_1} + r_2 \alpha_2 + \cdots + r_k \alpha_k = x$$

modulo m_1 $\quad r_1$

modulo m_2 $\quad r_2$

$\vdots$

$$1 \le x < y \le m_1 \cdots m_k$$

$$\begin{aligned} y - x &\equiv r_1 - r_1 \equiv 0 \pmod{m_1} \\ &\equiv r_2 - r_2 \equiv 0 \pmod{m_2} \\ &\vdots \\ &\equiv r_k - r_k \equiv 0 \pmod{m_k} \end{aligned}$$

$\Rightarrow m_1 \cdots m_k \mid y - x$ NO!

---

m, d, k interi positivi

Successione aritmetica di
- lunghezza m - ragione d
- ogni termine sia divisibile per una

potenza k-esima perfetta

$$\begin{aligned} n &\equiv 0 \pmod{p_1^k} \\ n+d &\equiv 0 \pmod{p_2^k} \\ n+2d & \\ &\vdots \\ n+(m-1)d &\equiv 0 \pmod{p_m^k} \end{aligned}$$

$p_1, \dots, p_m$ primi distinti

$$\begin{aligned} n &\equiv 0 \pmod{p_1^k} \\ n &\equiv -d \pmod{p_2^k} \\ &\vdots \\ n &\equiv -(m-1)d \pmod{p_m^k} \end{aligned}$$

TCR: Tale n esiste

$$\begin{cases} n \equiv 3 \pmod 6 \\ n \equiv 2 \pmod 4 \end{cases} \qquad \begin{cases} m \equiv 5 \pmod 6 \\ m \equiv 3 \pmod 4 \end{cases}$$

$n \equiv 0 \pmod 3$

NO $n \equiv 1 \pmod 2$

$n \equiv 2 \pmod 4$

$m \equiv 2 \pmod 3$

$\begin{cases} m \equiv 1 \pmod 2 \\ m \equiv 3 \pmod 4 \end{cases}$

$\to m \equiv 3 \pmod 4$

$m \equiv 11 \pmod{12}$

mcm$(6,4)$

---

m, d

Successione aritmetica di

- lunghezza m – ragione d
- nessun termine è una potenza

perfetta

$$n \equiv p_1 \pmod{p_1^2}$$
$$n+d \equiv p_2 \pmod{p_2^2}$$
$$\vdots$$
$$n+(m-1)d \equiv p_m \pmod{p_m^2}$$

$p_1 \dots p_m$ primi distinti

$$a^h = (q_1^{\alpha_1} \dots q_s^{\alpha_s})^h$$

ϕ φ

GIUSTO

$\varphi(n)$ = numero degli interi tra 1 e n estremi inclusi coprimi con n

$\varphi(1) = 1$ $\varphi(2) = 1$ $\varphi(3) = 2$

$\varphi(p) = p-1$ p primo

$\varphi(6) = 2$ $\varphi(4) = 2$

[$MCD(m,n) = 1$

$$\varphi(mn) = \varphi(m)\varphi(n)$$

SE NO, È FALSO

MOLTIPLICATIVA

φ è moltiplicativa MA NON COMPLET. MOLTIPLICATIVA

$F(mn) = F(m)F(n)$ per ogni m,n intero positivo
F è completamente moltiplicativa

$\mathrm{MCD}(m,n)=1$

Chi sono gli interi coprimi con mn?

a coprimo con mn $\Rightarrow$ a coprimo con m
$\Rightarrow$ a coprimo con n

Scelgo $1 \leq r_1 \leq m$ coprimo con m
$1 \leq r_2 \leq n$ coprimo con n

Esiste unico $1 \leq r \leq mn$
tale che $r \equiv r_1 \pmod{m}$
$r \equiv r_2 \pmod{n}$

Viceversa $1 \leq s \leq mn$ coprimo con mn
$s \equiv s_1 \pmod{m}$
$s \equiv s_2 \pmod{n}$

Interi tra 1 e mn coprimi con mn

Coppie di interi (c,d)
$1 \leq c \leq m$ c coprimo con m
$1 \leq d \leq n$ d coprimo con n

$$\varphi(mn) = \varphi(m)\varphi(n)$$

$$\varphi(p)=p-1$$

$$\varphi(p^k) = p^k - \frac{p^k}{p} = p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right)$$

$$\varphi(p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \cdots \varphi(p_\ell^{k_\ell})$$

$$= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_\ell^{k_\ell} - p_\ell^{k_\ell-1}) =$$

$$= p_1^{k_1} \cdots p_\ell^{k_\ell}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_\ell}\right)$$

Numero di divisori (positivi)

Moltiplicativa ma NON completamente moltiplicativa

$$p_1^{\alpha_1} \cdots p_r^{\alpha_r} \times q_1^{\beta_1} \cdots q_s^{\beta_s}$$

$$(\alpha_1+1)\cdots(\alpha_r+1) \times (\beta_1+1)\cdots(\beta_s+1)$$

Somma dei divisori (positivi)

Moltiplicativa ma NON completamente moltiplicativa

$MCD(m,n) = 1$

$c \mid m \quad d \mid n \qquad MCD(c,d) = 1$

$cd \mid mn$

$h \mid mn \qquad MCD(h,m) \mid m$

$MCD(h,n) \mid n$

$MCD(h,m) \cdot MCD(h,n) = h$

$$\underbrace{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}_{m} \underbrace{q_1^{\beta_1} \cdots q_s^{\beta_s}}_{n}$$

Divisori di mn — Coppie (divisore di m, divisore di n)

$$\sigma(mn) = \sigma(m)\sigma(n)$$

---

n intero positivo

$$\sum_{d \mid n} \varphi(d) = n$$

$n = p^k \qquad 1, p, p^2, \ldots, p^{k-1}, p^k$

$$\varphi:\ 1 + (p-1) + (p^2-p) + (p^3-p^2) + \ldots + (p^{k-1}-p^{k-2}) + (p^k - p^{k-1}) =$$
$$= p^k$$

$$\underbrace{p_1^{k_1} \cdots p_h^{k_h}}_{d} \quad p_{h+1}^{k_{h+1}}$$

$d \cdot 1 \longrightarrow \sum \varphi = p_1^{k_1} \cdots p_h^{k_h} \cdot 1$

$d \cdot p_{h+1} \longrightarrow \sum \varphi(d \cdot p_{h+1}) =$

$d \cdot p_{h+1}^2$ * $\qquad = \sum \varphi(d)\varphi(p_{h+1}) =$

$\qquad = \sum (p_{h+1}-1)\varphi(d) =$

$d \cdot p_{h+1}^{k_{h+1}} \qquad = (p_{h+1}-1)\, p_1^{k_1} \cdots p_h^{k_h}$

$$* \quad \sum \varphi(d\, p_{h+1}^2) = \sum \varphi(d)\, \varphi(p_{h+1}^2) =$$
$$= (p_{h+1}^2 - p_{h+1}) \sum \varphi(d) = (p_{h+1}^2 - p_{h+1})\, p_1^{k_1} \cdots p_h^{k_h}$$

$$p_1^{k_1} \cdots p_k^{k_h} \left(\cancel{1} + (\cancel{p_{h+1}} - \cancel{1}) + (p_{h+1}^2 - \cancel{p_{h+1}}) + \ldots \right.$$
$$\left. \ldots + (p_{h+1}^{k_{h+1}} - p_{h+1}^{k_{h+1}-1}) \right) =$$

$$= p_1^{k_1} \cdots p_k^{k_h} \, p_{k+1}^{k_{h+1}}$$

$n \geq 2$ intero

$a, a^2, a^3, a^4, \ldots$ a intero

modulo n

$a^k \_ a^{k+1} \ldots$ $a^h \equiv a^k \pmod{n}$

$a^{h+1} \equiv a^h \cdot a \equiv a^k \cdot a \equiv a^{k+1} \pmod{n}$

$a^{h+2} \equiv a^{k+2} \pmod{n}$

La successione è periodica modulo n da un certo punto in poi

$MCD(a,n) = 1$ allora

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

$\mathrm{ord}_n(a) =$ il più piccolo intero positivo r tale che $a^r \equiv 1 \pmod{n}$

$\mathrm{ord}_n(a) \leq \varphi(n)$ $\quad \mathrm{ord}_n(a) \mid \varphi(n)$

$$\varphi(n) = d \cdot \mathrm{ord}_n(a) + b \quad 0 \leq b < \mathrm{ord}_n(a)$$

$$a^{\mathrm{ord}_n(a)} \equiv 1 \pmod{n}$$

$$\left(a^{\mathrm{ord}_n(a)}\right)^d \equiv 1 \pmod{n}$$

$$a^{\underbrace{\mathrm{ord}_n(a) \cdot d + b}_{\varphi(n)}} \equiv 1 \pmod{n}$$

$$\underbrace{a^{\mathrm{ord}_n(a)}}_{1} a^b \equiv 1 \pmod n$$
$$a^b \equiv 1 \pmod n$$

$$\mathrm{ord}_n(a) \mid \varphi(n)$$

Può essere $\mathrm{ord}_n(a) = \varphi(n)$?

dipende da n

$n=2$ sì

$n=4$ sì

$n=2^k$ $k \geq 3$ NO

p primo dispari tale a esiste

p^k, $2 \cdot p^k$ sì $k \geq 1$

TUTTI GLI ALTRI: NO

$$n = p_1^{\alpha_1} \cdots p_h^{\alpha_h} \cdot 2^{k \geq 2}$$

$\mathrm{MCD}(a,n) = 1$

$$a^{\varphi(p_1^{\alpha_1})} \equiv 1 \pmod{p_1^{\alpha_1}}$$

$$a^{\overbrace{2^{k-1}}^{\varphi(2^k)}} \equiv 1 \pmod{2^k}$$

$\vdots$

$$a^{\varphi(p_h^{\alpha_h})} \equiv 1 \pmod{p_h^{\alpha_h}}$$

$$a^{\underbrace{\mathrm{mcm}(\varphi(p_1^{\alpha_1}), \dots, \varphi(p_h^{\alpha_h}), 2^{k-1})}_{< \varphi(n)}} \equiv 1 \pmod n$$

$$\varphi(p_1^{\alpha_1}) = p_1^{\alpha_1} - p_1^{\alpha_1 - 1}$$

$$\varphi(2^k) = 2^{k-1}$$

Prendo n t.c. esiste a coprimo con n t.c. $\mathrm{ord}_n(a) = \varphi(n)$

Un tale a è detto generatore modulo n.

Sia g un generatore modulo n

$$g, g^2, g^3, g^4, \dots \underbrace{g^{\varphi(n)}}_{1} \pmod n$$

SONO DIVERSI MODULO N

$$g^k \equiv g^h \pmod n \qquad 1 \le k < h \le \varphi(n)$$

Esiste $(g^k)^{-1} \pmod n$

$$\equiv (g^{-1})^k \qquad g^k \underbrace{g^{-1} g^{-1} \dots g^{-1}}_{k \text{ volte}} \equiv 1$$

$$1 \equiv g^k (g^k)^{-1} \equiv g^h \underbrace{(g^{-1})^k}_{g^{-k}} \equiv g^{h-k} \qquad h-k < \varphi(n)$$

ASSURDO

Quindi

$g, g^2, g^3, \dots g^{\varphi(n)}$ sono <u>tutte</u> le classi di resto modulo n coprime con n

n che ha un generatore

a t.c. $\mathrm{MCD}(a,n) = 1$ a è un generatore

$$\varphi(n) = q_1^{\beta_1} \dots q_s^{\beta_s}$$

$$\underbrace{\frac{\varphi(n)}{q_1} \quad \cdots \quad \frac{\varphi(n)}{q_s}}_{*}$$

qualunque divisore di $\varphi(n)$ divide uno di questi

Se a non è un generatore, $\text{ord}_n(a)$ divide uno tra $*$

$$a^{\text{ord}_n(a)} \equiv 1 \pmod n$$

$$a^{k\cdot \text{ord}_n(a)} = (\underbrace{a^{\text{ord}_n(a)}}_{1})^k \equiv 1$$

Se a non è generatore, uno tra

$$a^{\frac{\varphi(n)}{q_1}}, a^{\frac{\varphi(n)}{q_2}}, \dots a^{\frac{\varphi(n)}{q_s}}$$ è $\equiv 1 \pmod n$

È SE E SOLO SE UN

Quindi se tutti questi sono $\not\equiv 1 \pmod n$, a è un generatore

$$a^m \equiv 1 \pmod n \iff \text{ord}_n(a) \mid m$$

Dimostrazione: $m = d \cdot \text{ord}_n(a) + r$

$0 \le r < \text{ord}$

Se $r \neq 0$ $a^r \equiv 1$, ASSURDO

---

n tale che esiste generatore modulo n

$$g, g^2, g^3, \dots\dots g^{\varphi(n)} \equiv 1 \pmod n$$

Quanti sono gli elementi con un determinato ordine (in particolare, quanti sono i generatori?)

$1 \le k \le \varphi(n)$ g^k. che ordine ha g^k?

$$\frac{\varphi(n)}{MCD(\varphi(n),k)}$$

$$g^{k \cdot \boxed{ord_n(g^k)}} \equiv 1 \pmod n$$

$$\varphi(n) \mid k \cdot ord_n(g^k)$$

$$g^{mcm(k,\varphi(n))} \equiv 1 \pmod n$$

$$mcm(k,\varphi(n)) = \frac{k\,\varphi(n)}{MCD(\varphi(n),k)}$$

Perché g^k sia un generatore, il suo ordine deve essere $\varphi(n)$, quindi

$$\frac{\varphi(n)}{MCD(\varphi(n),k)} = \varphi(n) \qquad MCD(\varphi(n),k) = 1$$

Ci sono $\varphi(\varphi(n))$ esponenti per g con questa proprietà, e quindi $\varphi(\varphi(n))$ generatori

Fissiamo $d \mid \varphi(n)$. Quanti sono le classi di resto modulo n coprime con n e con ordine d?

Avendo g generatore g^k ha ordine $\dfrac{\varphi(n)}{MCD(\varphi(n),k)}$

$$\frac{\varphi(n)}{MCD(\varphi(n),k)} = d \qquad MCD(\varphi(n),k) = \frac{\varphi(n)}{d}$$

$$k = \frac{\varphi(n)}{d},\ 2\frac{\varphi(n)}{d},\ \dots\dots\ (d-1)\frac{\varphi(n)}{d},\ \varphi(n)$$

$$k = h\frac{\varphi(n)}{d} \qquad MCD(h,d) = 1$$

$$k = h_1 \cdot \underbrace{MCD(h,d)}_{>1} \frac{\varphi(n)}{d} = h_1 \frac{\varphi(n)}{d/MCD(h,d)}$$

$$\frac{\varphi(n)}{d/MCD(h,d)} \mid k \qquad \frac{\varphi(n)}{d/MCD(h,d)} \mid \varphi(n)$$

$$\frac{\varphi(n)}{d/MCD(h,d)} \mid MCD(\varphi(n),k) \qquad \frac{\varphi(n)}{d/MCD(h,d)} > \frac{\varphi(n)}{d}$$

se $MCD(h,d) > 1$

Se invece $MCD(h,d) = 1$

Allora $MCD\left(h\frac{\varphi(n)}{d}, \varphi(n)\right) = \frac{\varphi(n)}{d}$

Se h è coprimo anche con $\varphi(n)$ siamo a posto

Se no, tutti i fattori primi di $\varphi(n)$ in h ci sono già in $\frac{\varphi(n)}{d}$

Conclusione! Gli elementi di ordine d sono $\varphi(d)$ perche mi vanno bene tutti gli h coprimi con d

n che ha un generatore g modulo n

$$g, g^2, \dots\, g^{\varphi(n)}$$

Quanti sono i residui delle potenze k-esime coprimi con n

Sono $\dfrac{\varphi(n)}{MCD(\varphi(n),k)}$

$$g^k, g^{2k}, g^{3k}, \dots\, g^{\varphi(n)\cdot k}$$

Questi esponenti modulo $\varphi(n)$ sono

$\boxed{MCD(\varphi(n),k)}$, $2\cdot MCD(\varphi(n),k)$, $\dots\ \dfrac{\varphi(n)}{MCD(\varphi(n),k)} \cdot MCD(\varphi(n),k)$

$$MCD(\varphi(n),k) = b\varphi(n) + ck \quad \text{Bezout}$$

$$(g^c)^k = g^{ck}\cdot 1 = g^{ck} g^{b\cdot\varphi(n)} =$$
$$= g^{b\varphi(n)+ck} = g^{MCD(\varphi(n),k)}$$

$\alpha \mid \beta$ $\quad \alpha, 2\alpha, 3\alpha, \dots\, \frac{\beta}{\alpha}\alpha$

$\alpha \to MCD(k,\varphi(n))$, $\beta \to \varphi(n)$

I possibili esponenti sono i multipli di k modulo $\varphi(n)$

$$1 \leq \ell k - t\varphi(n) \leq \varphi(n)$$

$MCD(k,\varphi(n)) \mid \ell k$

$MCD(k,\varphi(n)) \mid t\varphi(n)$

I residui k-esimi sono "i multipli" di $MCD(k,\varphi(n))$ modulo $\varphi(n)$ e sono

$$\frac{\varphi(n)}{MCD(k,\varphi(n))}$$

---

p primo dispari

-1 è un residuo quadratico modulo p?

Lo è se e solo se $p \equiv 1 \pmod 4$

$p = 4h+1$

$g, g^2, \ldots, \underset{-1}{g^{2h}} \to (g^h)^2, \ldots\ldots, g^{4h} \equiv 1$

$(g^{2h})^2 \equiv 1 \pmod p$ $\qquad g^{2h} \not\equiv 1 \pmod p$

$x^2 \equiv 1 \pmod p$ $\qquad x^2-1 \equiv (x+1)(x-1) \equiv 0 \pmod p$

$x \equiv -1 \qquad x \equiv 1$

$p = 4h+3$

$g,\ g^2,\ g^3, \dots, g^{2h+1}, \dots\ g^{4h+2} \equiv 1$

$\uparrow$
-1

$MCD(2, 4h+2) \cdot \ell$

$2 \cdot \ell$

$g^2, g^4, g^6 \dots\ g^{4h+2}$ sono residui quadratici

$p \equiv 3 \pmod 4$

$p \mid x^2+y^2 \implies \begin{matrix} p \mid x \\ p \mid y \end{matrix}$

$p \nmid x \underset{\substack{\uparrow \\ p \text{ primo}}}{\implies} MCD(p,x) = 1$ esiste $x^{-1} \bmod p$

$(x^{-1})^2 \equiv (x^2)^{-1} \equiv$
$\equiv x^{-2}$

$p \mid x^2+y^2$ prendo z t.c. $z \equiv x^{-1}$

$p \mid z^2(x^2+y^2)$

$(x^2)^{-1}x^2 + (x^2)^{-1}y^2 \equiv 0 \pmod p$

$1 + y^2x^{-2} \equiv 0 \pmod p$

$y \cdot x^{-1}$ sarebbe tale che

$(y \cdot x^{-1})^2 \equiv -1 \pmod p$

"square - free"

$p \mid a$ $\quad \underset{0}{\overset{\equiv}{a}}, \underset{0}{\overset{\equiv}{a^2}}, \underset{0}{\overset{\equiv}{a^3}},$ (mod p) $\qquad p \nmid a \quad a, a^2, \dots \underbrace{a^{\mathrm{ord}_p(a)}}_{1}, a, a^2$

$p_1 p_2 \dots p_s$ $\quad a$ intero

La successione $a, a^2, a^3, \dots$ è periodica modulo ciascun p_i, quindi modulo il loro ~~prodotto~~ prodotto per TCR

periodo modulo p_1 --

1 se $p_1 \mid a$

$\mathrm{ord}_{p_1}(a)$ se $p_1 \nmid a$

periodo modulo p_2 - —

Il periodo modulo il prodotto è il mcm dei periodi modulo i fattori

$p^{\alpha > 1} \cdot K$

$a = p \qquad p, p^2, \dots p^{\alpha-1}, 0 \dots$

n intero positivo

$2 \nmid n \quad 5 \nmid n$ Allora esiste m tale che

$\underbrace{1111\ldots111}_{m \text{ "uni"}}$ è divisibile per n

$\underbrace{9999\ldots\ldots999}_{m \text{ "nove"}} = 10^m - 1$

$10^m \equiv 1 \pmod{n}$ $\pmod{9n}$

$MCD(10, n) = 1$

$m = ord_{n}(10)$
$(9n)$

Dato p primo, esistono infiniti n tali che

$p \mid 2^n - n$

$2^n \equiv n \pmod{p}$

$2^{p-1} \equiv 1 \pmod{p}$

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

$\boxed{a^p \equiv a \pmod{p} \text{ per qualunque } a}$

$$\boxed{a^{\varphi(m)+1} \equiv a \pmod{m} \text{ se } m \text{ è square-free per qualunque } a}$$

$$2^{(p-1)^2} - (p-1)^2 =$$

$$= \cancel{1} - p^2 + 2p - \cancel{1} \equiv 0 \pmod{p}$$

$(p-1)^2$

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

$$\equiv 1 - (\text{Mutipli di } p + 1)$$

2^n è periodica modulo p di periodo divisore di $p-1$

$-n$ è periodica modulo p con periodo p

$2^n - n$ è periodica modulo p di periodo mcm dei periodi sicuramente $p(p-1)$

---

a intero positivo, m intero positivo

$$a,\ a^a,\ \underbrace{a^{a^a}}_{a^{(a^a)}},\ a^{a^{a^a}},\ \ldots$$

$$a^{(a^{(a^a)})}$$

Definitivamente (Da un certo in poi)

costante modulo m

$$a^{\boxed{a^{a^{\cdot^{\cdot^{\cdot^{a}}}}}}} \pmod m$$

mi basta l'esponente modulo $\varphi(m)$

$$a = \underbrace{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}_{\text{stanno in } m} \underbrace{q_1^{\beta_1} \cdots q_s^{\beta_s}}_{\text{non ci stanno}}$$

$$m = p_1^{\gamma_1} \cdots p_r^{\gamma_r} K$$

$$a^{a^{\cdot^{\cdot^{\cdot^{a}}}}} \equiv 0 \mod p_1^{\gamma_1} \cdots p_r^{\gamma_r}$$

$$a^{\boxed{a^{a^{\cdot^{\cdot^{\cdot^{a}}}}}}}$$

modulo $\varphi(\varphi(m))$

$\varphi(n) < n$ tranne per $n=1$

$\varphi(n)$ $\varphi(\varphi(n))$, $\varphi(\varphi(\varphi(n)))$ ...

$$a^{\boxed{a^{\cdot^{\cdot^{\cdot^{a}}}}}} \to \text{costante modulo } 2$$

$$a^{a^{a^{\cdot^{\cdot}}}}$$

$\to$ definitivamente costante modulo $\varphi(\varphi \ldots \varphi(n) \ldots)$

$$n \mid 2^n + 1$$

Allora $3 \mid n$

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

$$2^{2n} \equiv 1 \pmod{n}$$

$$\mathrm{ord}_n(2) \mid 2n \qquad \mathrm{ord}_n(2) \mid \varphi(n)$$

PPP sia p il ppp che divide n
(primo piccolo)

$$p \mid 2^n + 1$$

$$2^{2n} \equiv 1 \pmod{p}$$

$$\mathrm{ord}_p(2) \mid 2n \qquad \mathrm{ord}_p(2) \mid p-1$$

$$\mathrm{ord}_p(2) \mid \mathrm{MCD}(2n, p-1) \to 1, \to 2$$

$$\mathrm{ord}_p(2) = 1, 2$$

$$2^1 \equiv 1 \pmod{p} \qquad 2^2 \equiv 1 \pmod{p}$$

$$p = 3 \qquad 2^3 + 1 = 3^2$$

$$2^9+1=513$$

$$3^h \mid 2^{3^h}+1 \qquad 2^{3^h}=k3^h-1$$

$$2^{3^{h+1}}=\underbrace{k^3 3^{3h}-3k^2 3^{2h}+k3\cdot 3^h}_{\text{Qui c'è } 3^{h+1}}-1$$

$$3q \mid 2^{3q}+1 \qquad q>3$$

$$2^{3q}\equiv -1 \pmod q$$

$$2^{6q}\equiv 1 \pmod q$$

$$\mathrm{ord}_q(2) \mid 6q \qquad \mathrm{ord}_q(2) \mid q-1$$

$$\mathrm{ord}_q(2)=1,2,3,6 \rightarrow 2^6\equiv 1 \pmod q$$

$$2^3\equiv 1 \pmod q$$

$$q=7$$

$$21 \mid 2^{21}+1 \ ?$$

NO, MODULO 7

2, 4, 1 sono le potenze di 2 modulo 7

$$3^2\cdot 19=171$$

Quali sono

Qual è il modulo comodo per i residui cubici?

7, 9 $\qquad -1, 0, 1$

I residui k-esimi modulo n: Le classi g^h con g generatore modulo n, h residui dei multipli di $MCD(k, \varphi(n))$ modulo $\varphi(n)$

$\varphi(7) = \varphi(9) = 6$

g_7 generatore modulo 7, allora $g_7^3 \leftarrow -1$ e $g_7^6 \leftarrow 1$ sono i residui modulo 7 coprimi con 7. Poi c'è lo 0

g_9 generatore modulo 9
$g_9^3 \equiv -1$, $g_9^6 \equiv 1$ sono i residui cubici modulo 9 coprimi con 9. Ricordatevi lo 0

Massimo ordine possibile modulo 2^k con $k \geq 3$ è 2^{k-2}

Provate, dando per noto p, a mostrare per induzione che modulo p^k esiste il generatore

Titolo nota 04/09/2012

PROBLEMA 1

- C'è un campo rettangolare suddiviso da 4 tagli verticali e 4 tagli orizz. nel seguente modo.

	b	e	g	h
f		20	14	
a	12			* ?
c	8		15	
d		25		21

$ah = ?$

$dh = 21 \qquad d = \dfrac{21}{h}$

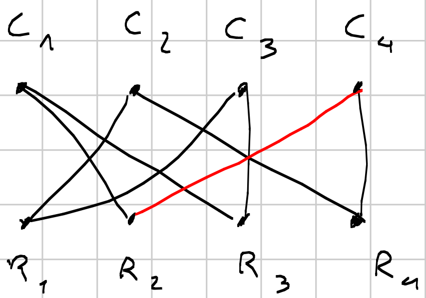
$e = \dfrac{25}{21} h$

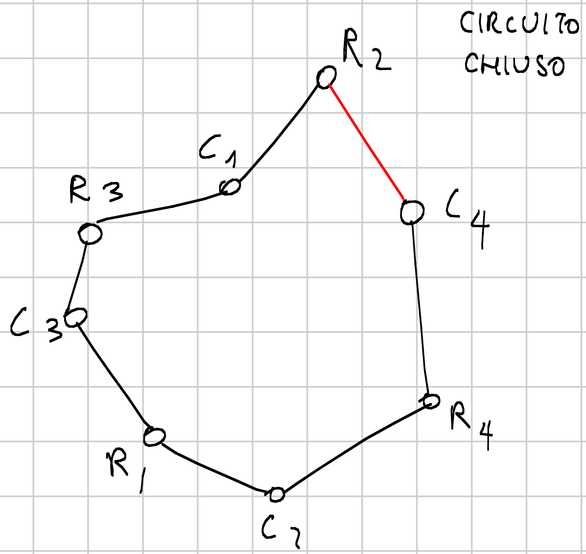
$f = \dfrac{20 \cdot 21}{25 h} \qquad g = \dfrac{14 \cdot 25}{20 \cdot 21} h$

$c = \dfrac{15 \cdot 20 \cdot 21}{14 \cdot 25 \cdot h} \qquad b = \dfrac{8 \cdot 14 \cdot 25 h}{15 \cdot 20 \cdot 21}$

$\boxed{ah} = \dfrac{12 \cdot 15 \cdot 20 \cdot 21}{8 \cdot 14 \cdot 25} = 27$

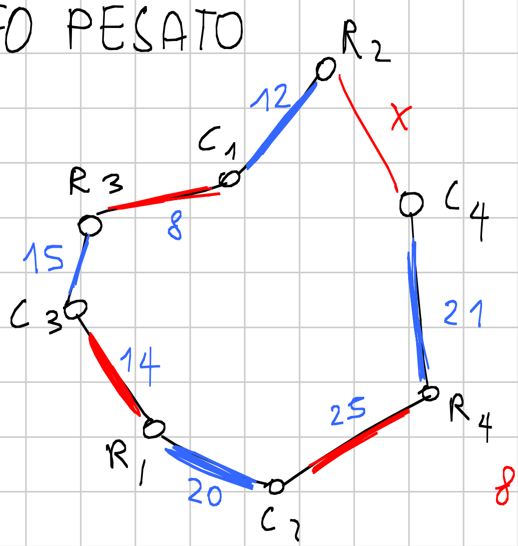
GRAFO





Se ad ogni vertice viene assegnato un valore si ha un GRAFO PESATO

GRAFO PESATO



$ah = x = R_2 \cdot C_4$

- Come posso calcolare il prodotto 12?

$R_2 \cdot C_1$

$8 \cdot 14 \cdot 25 \cdot x = 12 \cdot 15 \cdot 20 \cdot 21$

PROBLEMA 2

(1) $5x - 7y \geq 24$

(2) $2x + y \geq 21$

- trovare il minimo di $20x - 9y$

$2 \cdot (1) \qquad 10x - 14y \geq 48$

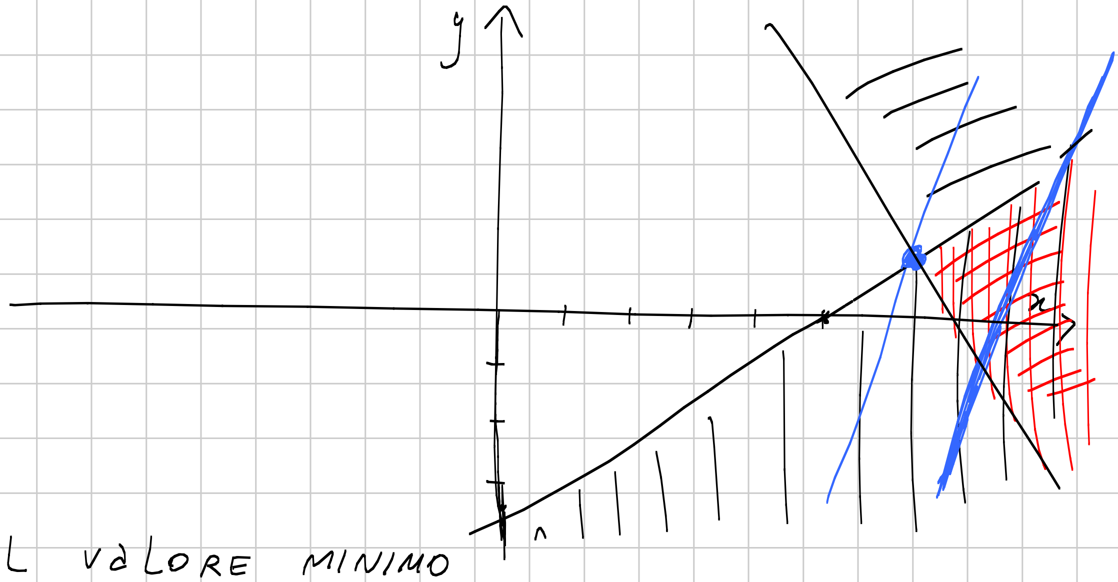
$5 \cdot (2) \qquad 10x + 5y \geq 105$

$(1) + (2) \qquad 20x - 9y \geq 153$

——— ∘ ——— ∘ ———

SPIEGAZIONE ANALITICA

$14y \leq 10x - 48 \qquad y \leq \frac{5}{7}x - \frac{24}{7}$



IL VALORE MINIMO

$\downarrow$

$\frac{5}{7}x - \frac{24}{7} = 21 - 2x$ $\qquad$ $\frac{5+14}{7}\,x = \frac{21\cdot 7+24}{7}$

$19x = 147+24$ $\qquad$ $x = \frac{171}{19} = 9$

$x = 9 \Rightarrow y = 3$

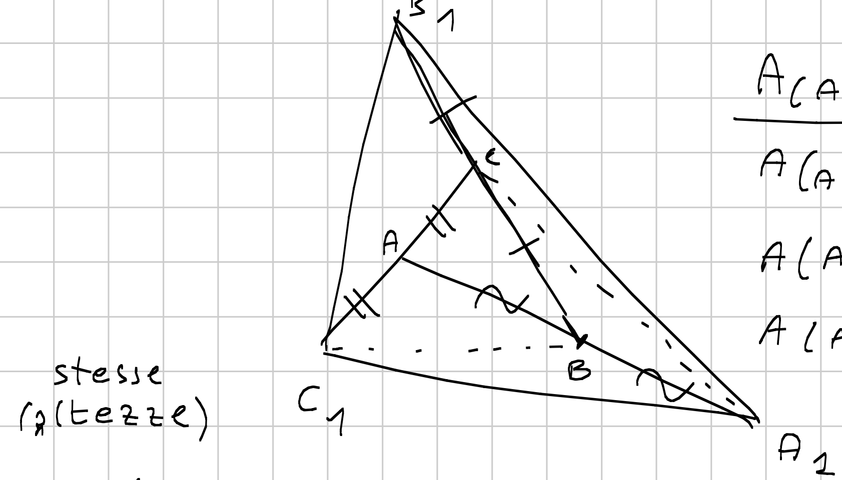
$\lambda > 0 \quad , \quad \mu > 0$

$\lambda\cdot(1) + \mu\,(2) \Rightarrow 20x - 9y$

$$\begin{cases} 5\lambda + 2\mu = 20 \\ -7\lambda + \mu = -9 \end{cases}$$

PROBLEMA 3

Abbiamo un generico triangolo $\overset{\triangle}{ABC}$



$$\frac{A(ABC)}{A(A_1B_1C_1)} = ?$$

$A(ABC) = A(ABC_7)$

$A(ABC_7) = A(A_7BC_7)$

$A(CC_1B) = 2A(ABC) = A(B_7CC_1)$

$A(ABC) = A(BA_7C) = A(CB_7A_7)$

$$\frac{A(ABC)}{A(A_1B_1C_1)} = \frac{1}{7}$$

PROBLEMA 4

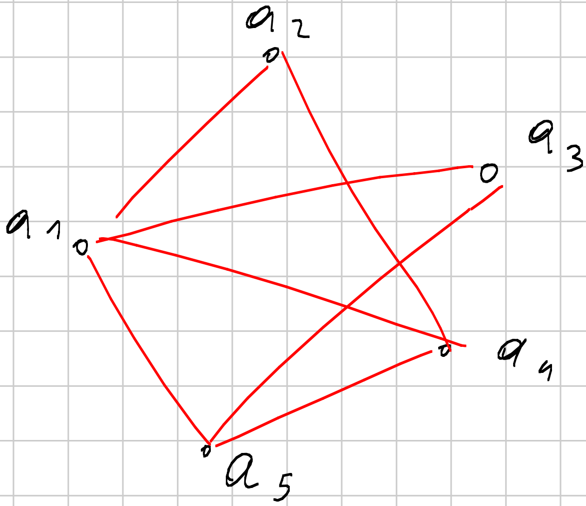
$a_1, a_2, a_3, a_4, a_5 \in \mathbb{N}$

Si sa che ci sono $\binom{5}{2} = 10$ coppie di numeri.

- Ci sono almeno 7 coppie di numeri, che sommati danno un multipo di 3.
- Dimostrare che ogni numero è multiplo di 3

→ Se, per esempio avessimo $a_1 \equiv a_2 \equiv 1 \ (3)$ e $a_3 \equiv a_4 \equiv a_5 \equiv 2 \ (3)$ al massimo riusciremmo ad avere 6 multipli di 3. Non 7

Disegnamo un grafo per rappresentare la situazione



① colleghiamo due nodi se la somma dei due numeri è un multiplo di 3

La somma dei gradi è 14

1) Per PIGEON HOLE ci sono almeno 2 numeri che compaiono in due coppie

$$3 \mid a_1 + a_2 \quad e \quad 3 \mid a_1 + a_3 \Rightarrow a_2 \equiv a_3 \ (3)$$

SENIOR 2012 – Basic – Miscellanea (Janos)

Titolo nota 07/09/2012

ESERCIZIO 1

$a_1, a_2, a_3, a_4, a_5 \in \mathbb{Z}$

Le somme di forma $a_i + a_j : 3 \mid a_i + a_j$ sono almeno 7

Tesi: Dimostrare che $3 \mid a_i$

Dim: Per Pigeonhole, almeno un a_i compare in 3 coppie

$3 \mid a_1 + a_2$
$3 \mid a_1 + a_3$ $\Rightarrow a_2 \equiv a_3 \equiv a_4 \ (3)$
$3 \mid a_1 + a_4$

a_5 deve comparire perché $\binom{4}{2} = 6$ e $6 < 7$

$a_5 + a_1 \vee a_5 + a_2 (a_3, a_4)$

$\Rightarrow a_1 \equiv a_5$ e $a_2 \equiv a_3 \equiv a_4 \vee$
$(a_2 \equiv a_3 \equiv a_4 \equiv a_5)$

in questo caso sono dunque tutti $\equiv$ perché se no ci sarebbero solo 4 coppie, ma potrei prenderne per esempio due $\equiv 1$ e tre $\equiv 2$ (3). Ma ciò mi genera solo 6 coppie accettabili, quindi dovrebbero essere tutti $\equiv$ tra loro e quindi $\equiv 0$ (3).

c.v.d.

se le coppie in considerazione fossero $8, 9, 10$ la tesi iniziale

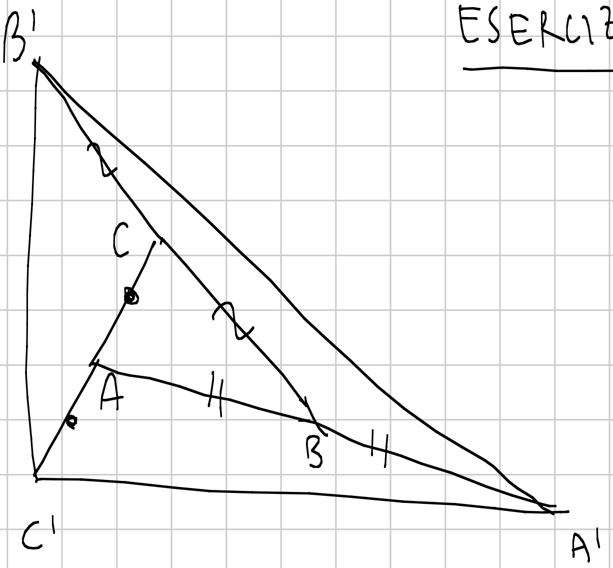
$\equiv 0 \ (3)$

sarebbe comunque vera.

questo problema si può risolvere anche con un grafo, infatti basta considerare i vertici come gli a_i e gli spigoli come gli accoppiamenti tra a_i e a_j.

ESERCIZIO 2

dati i punti A', B', C' determinare il triangolo ABC t.c.



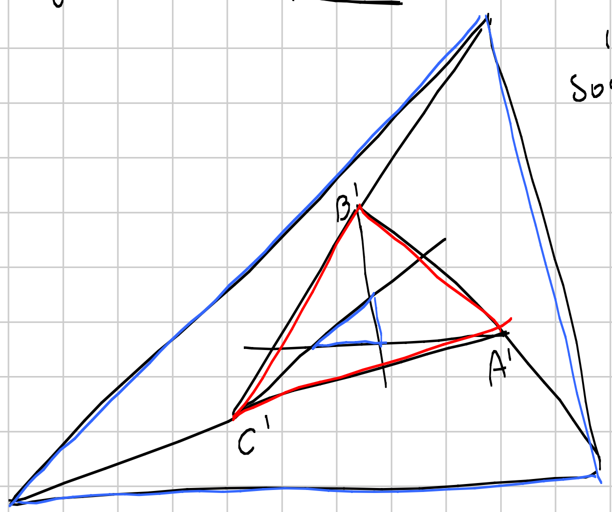
$\overline{AB} = \overline{BA'}$

$\overline{AC} = \overline{AC'}$

$\overline{CB} = \overline{CB'}$

Congettura di Lisa (Lentati)

i due triangoli blu sono OMOTETICI perché hanno lati paralleli per costruzione

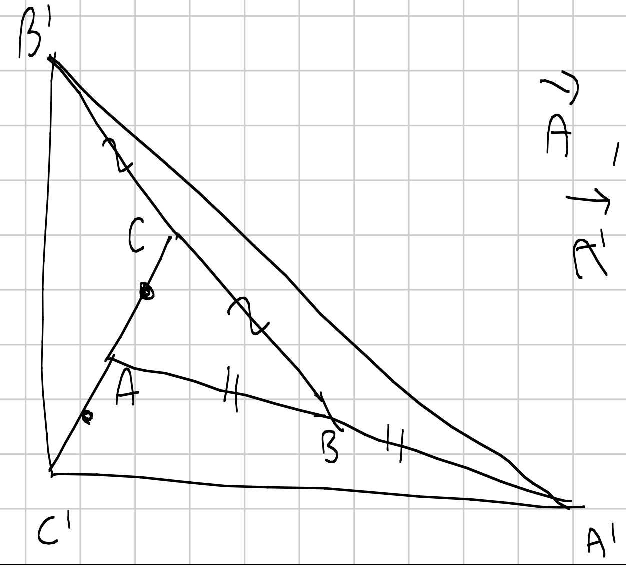


A triangolo Blu grande $= 7\,A$ triangolo rosso

A triangolo rosso $= 7\,A$ triangolo blu piccolo

$\Rightarrow A$ tr Blu grande $= 49$ tr Blu piccolo

Dimostrazione DEL PROF. (con i vettori)



$\vec{A}$, $\vec{B}$, $\vec{C}$

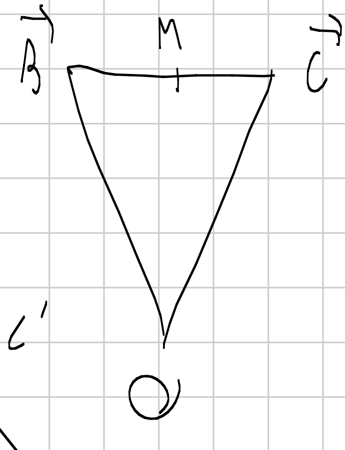
$$\vec{A'} = \vec{A} + 2(\vec{B} - \vec{A}) = 2\vec{B} - \vec{A}$$

$$\begin{cases} \vec{A}' = 2\vec{B} - \vec{A} \\ \vec{B}' = 2\vec{C} - \vec{B} \\ \vec{C}' = 2\vec{A} - \vec{C} \end{cases} \qquad \begin{cases} 2y - x = a \\ 2z - y = b \\ 2x - z = c \end{cases} \qquad \begin{cases} x = 2y - a \\ y = 2z - b \\ z = 2x - c \end{cases}$$

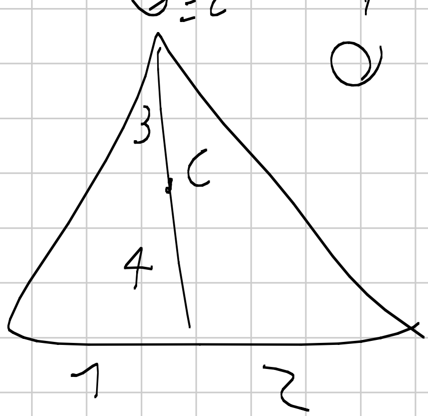
$$\ldots \begin{cases} \vec{A} = \dfrac{4\vec{C}' + 2\vec{B}' + \vec{A}'}{7} \\ \text{e ciclici} \end{cases}$$

$\Rightarrow$ se metto l'origine in C', $4\vec{C}' = 0$

$$\Rightarrow \quad \vec{A} = \frac{2\vec{B}' + \vec{A}'}{7}$$

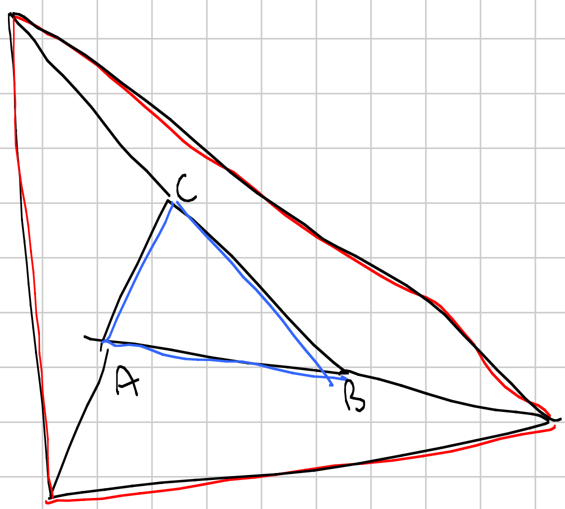


$$\vec{M} = \frac{\vec{B} + \vec{C}}{2}$$



abbiamo che C si trova in proporzione 3 a 4

SOLUZIONE 3



SOLUZIONE CON LA FANTASIA