Stage Senior 2010 – Livello Basic

Stampato integrale delle lezioni

Autori vari

Indice

A1 basic polinomi / complessi F. MORANDIN

Titolo nota 07/09/2010

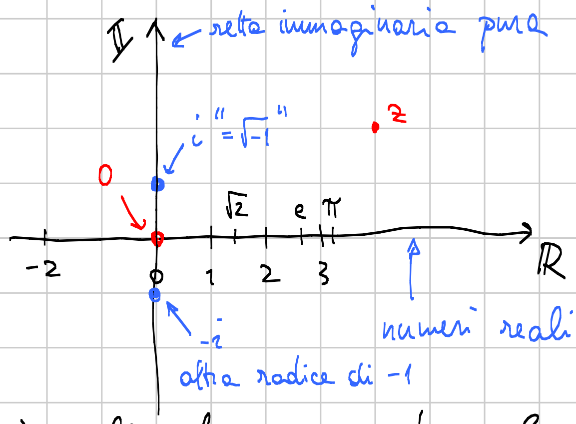
- Numeri complessi

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

$(\mathbb{C}, +, \cdot)$

$\sqrt{2}$ $x^2 = 2$

$-\sqrt{2}$



$\mathbb{C} \ni z = x + iy$ con x, y numeri reali che rappresentano le coordinate di z sul piano

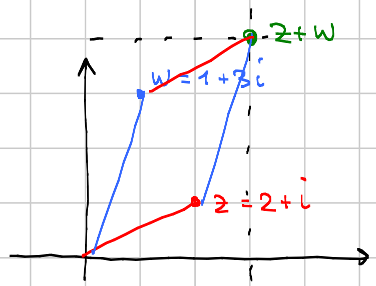
$\mathbb{R}^2 \longleftrightarrow \mathbb{C}$

$(x, y) \longleftrightarrow x + iy$

$\boxed{i^2 = -1}$

- Operazioni :

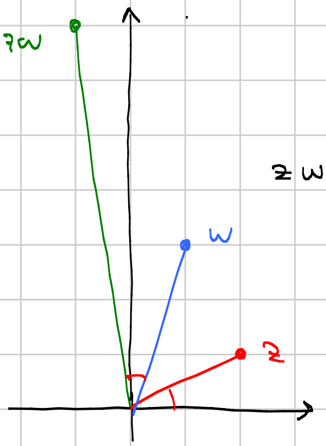
- somma componente per componente = come i vettori = regola del parallelogramma



$z + w = 2 + i + 1 + 3i = 3 + 4i$

- prodotto si esegue formalmente sulle espressioni $x + iy$ equivale a moltiplicare le lunghezze e sommare gli angoli

$z \cdot w = (2+i)(1+3i) = 2 + i + 6i + 3i^2 = 2 + i + 6i - 3 = -1 + 7i$



$|z| = \sqrt{5}$ $\qquad |w| = \sqrt{10}$ $\qquad |zw| = \sqrt{50}$

$$zw = (x+iy)(s+it) = xs - yt + i(ys + xt)$$

$$|zw| = \sqrt{(xs-yt)^2 + (ys+xt)^2}$$

$$= \sqrt{x^2s^2 + y^2t^2 \cancel{- 2xsyt} + y^2s^2 + x^2t^2 \cancel{+ 2ysxt}}$$

$$= \sqrt{x^2s^2 + y^2t^2 + y^2s^2 + x^2t^2} = \sqrt{(x^2+y^2)(s^2+t^2)} = \sqrt{x^2+y^2}\sqrt{s^2+t^2} = |z||w|$$

$\operatorname{Arg}(z)$ angolo che il "vettore" z forma con il semiasse reale positivo

$z = x+iy$

$$\operatorname{tg} \operatorname{Arg}(z) = y/x \qquad \operatorname{sen} \operatorname{Arg}(z) = \frac{y}{\sqrt{x^2+y^2}} \qquad \cos \operatorname{Arg}(z) = \frac{x}{\sqrt{x^2+y^2}}$$

$$\cos \operatorname{Arg}(z \cdot w) = \frac{xs - yt}{\sqrt{x^2+y^2}\sqrt{s^2+t^2}} = \underbrace{\frac{x}{\sqrt{x^2+y^2}}}_{\cos \operatorname{Arg}(z)} \cdot \underbrace{\frac{s}{\sqrt{s^2+t^2}}}_{\cos \operatorname{Arg}(w)} - \underbrace{\frac{y}{\sqrt{x^2+y^2}}}_{\operatorname{sen} \operatorname{Arg}(z)} \underbrace{\frac{t}{\sqrt{s^2+t^2}}}_{\operatorname{sen} \operatorname{Arg}(w)}$$

$$= \cos \operatorname{Arg} z \cos \operatorname{Arg} w - \operatorname{sen} \operatorname{Arg} z \operatorname{sen} \operatorname{Arg} w = \cos(\operatorname{Arg} z + \operatorname{Arg} w)$$

$$\operatorname{sen} \operatorname{Arg}(z \cdot w) = \ldots = \operatorname{sen}(\operatorname{Arg} z + \operatorname{Arg} w)$$

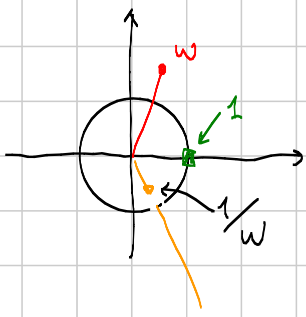
$$\Rightarrow \boxed{\operatorname{Arg}(zw) = \operatorname{Arg}(z) + \operatorname{Arg}(w)}$$

★ Bonus: $(n^2+m^2)(a^2+b^2)$ è sempre somma di due quadrati

- Divisione, reciproco

$\qquad w \neq 0$

$z/w = z \cdot \frac{1}{w}$ $\qquad$ chi è $\frac{1}{w}$?



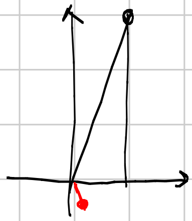
$\frac{1}{w}$ è un complesso tale che $w \cdot \frac{1}{w} = 1$

$\operatorname{Arg} \frac{1}{w} = -\operatorname{Arg} w \qquad \left|\frac{1}{w}\right| = \frac{1}{|w|}$

$w = s + it \qquad \frac{1}{w} = s' + it'$

$s' = \cos \operatorname{Arg} \frac{1}{w} \cdot \left|\frac{1}{w}\right| = \frac{\cos(-\operatorname{Arg} w)}{\sqrt{s^2+t^2}} = \frac{\cos \operatorname{Arg} w}{\sqrt{s^2+t^2}} = \frac{s}{s^2+t^2}$

$t' = -\frac{\operatorname{sen} \operatorname{Arg} w}{\sqrt{s^2+t^2}} = -\frac{t}{s^2+t^2}$



$w = 1+3i \qquad |w| = \sqrt{10} \qquad \cos \operatorname{Arg} w = \frac{1}{\sqrt{10}} \qquad \operatorname{sen} \operatorname{Arg} w = \frac{3}{\sqrt{10}}$

$s' = \frac{1}{\sqrt{10}} \cdot \frac{1}{\sqrt{10}} = \frac{1}{10} \qquad t' = -\frac{3}{\sqrt{10}} \cdot \frac{1}{\sqrt{10}} = -\frac{3}{10}$

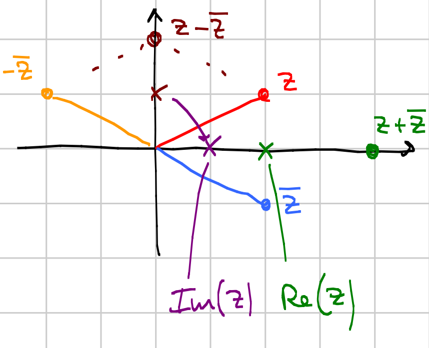
- Coniugio

$z = x + iy \qquad \bar{z} := x - iy \qquad z\bar{z}$ è sempre reale ≥ 0

$z\bar{z} = x^2 - i^2y^2 = x^2 + y^2 = |z|^2 \qquad \boxed{|z| = \sqrt{z\bar{z}}}$

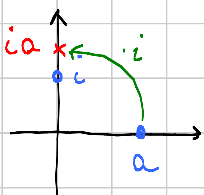
$z + \bar{z} = 2x \qquad \boxed{x =: \operatorname{Re}(z) := \frac{z+\bar{z}}{2}}$ parte reale

$z - \bar{z} = 2iy \qquad \boxed{y =: \operatorname{Im}(z) := \frac{z-\bar{z}}{2i}}$ parte immaginaria



$x \quad u \in \mathbb{R} \quad \operatorname{Arg}(u) = 0$

- $a \in \mathbb{R} \qquad ai$



- moltiplicare per un reale = omotetia di centro 0
- moltiplicare per i = rotazione di $90°$

POLINOMI

grado = deg p — coefficienti di solito numeri $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (o polinomi)

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

← termine noto

↑ coeff. direttore (se $=1$ il pol. è MONICO)

x non è un numero, ma un simbolo; può essere sostituito con qualunque oggetto di cui si sappiano fare somme e prodotti

I polinomi hanno una struttura algebrica $(\mathbb{R}[x], +, \cdot)$

pol. a coeff. reali

- Prodotti notevoli

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

$$\boxed{1 + x + x^2 + \ldots + x^k = \frac{x^{k+1} - 1}{x - 1}}$$ serie geometrica

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

- identità di Sophie Germain

$$x^4 + 4y^4 = (x^2 + 2y^2 + 2xy)(x^2 + 2y^2 - 2xy)$$

- $x^3 + y^3 + z^3 - 3xyz = (x+y+z)(x^2+y^2+z^2 - xy - yz - zx)$
- $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \ldots + xy^{n-2} + y^{n-1})$

$(\mathbb{Z}[x])[y]$ $\quad (x-1)y^2 - (x^2+2)y + (x+2) = xy^2 - x^2y - y^2 - 2y + x + 2$

- Divisione (con resto)

$4x^3 - 3x + 7 = p(x) \qquad a(x) = 2x+1$

$(2x+1)\cdot 2x^2 = 4x^3 + 2x^2 \qquad p(x) - a(x)\cdot 2x^2 = -2x^2 - 3x + 7$

$(2x+1)(-x) = -2x^2 - x \qquad p(x) - a(x)(2x^2 - x) = -2x + 7$

$(2x+1)(-1) = -2x - 1 \qquad p(x) - a(x)\underbrace{(2x^2 - x - 1)}_{q(x)} = 8 = r(x)$

$q(x) = 2x^2 - x - 1 \qquad a(x) = 2x+1$

$a(x)q(x) = 4x^3 - 3x - 1 = p(x) - r(x)$

$\boxed{p(x) = a(x)q(x) + r(x)}$

$\deg r < \deg a$

$\exists!\ q(x),\ r(x) \quad \deg r < \deg a \quad : \quad p(x) = a(x)q(x) + r(x)$

$p(x) = 4x^3 - 3x^2 + 7 \qquad a(x) = 2x+1$

$\mathbb{Z}[x] \subseteq \mathbb{Q}[x] \qquad \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$

4	-3	0	7	2	1		
4	2			2	$-5/2$	$5/4$	
	-5	0	7				
	-5	$-5/2$					
		$5/2$	7				
		$5/2$	$5/4$				
			$23/4$				

$\in \mathbb{Q}[x]$

$q(x) = 2x^2 - \frac{5}{2}x + \frac{5}{4} \notin \mathbb{Z}[x]$

$r(x) = 23/4$

- Algoritmo euclideo per MCD

$(96, 60) = 12$

96	60
60	36
36	24
24	12
12	0

$x^3 + 3x^2 + 3x + 1 = p(x) \qquad q(x) = 2x^2 + 3x + 1$

1	3	3	1	2	3	1
1	$3/2$	$1/2$		$\frac{1}{2}$	$\frac{3}{4}$	
	$3/2$	$5/2$	1			
	$3/2$	$9/4$	$3/4$			
		$1/4$	$1/4$			

$p(x)$	$q(x)$
$q(x)$	$r(x)$
$r(x)$	0

MCD non è unico

$\frac{1}{4}x + \frac{1}{4}$ è un $MCD(p, q)$

$x + 1$ è un $MCD(p, q)$

è unico a meno di fattori di deg 0.

$$\begin{array}{ccc|cc} 2 & 3 & 1 & \frac{1}{4} & \frac{1}{4} \\ \hline 2 & 2 & & 8 & 4 \\ & 1 & 1 & & \\ & 1 & 1 & & \\ & & 0 & & \end{array}$$

$p(x) = 2$ $\quad \deg p = 0$

$q(x) = 0$ $\quad \deg q = -\infty$

- **Fattorizzazione**

scrivere $p(x)$ come prodotto di polinomi più piccoli "minimi" (= irriducibili)

$18 = 9 \cdot 2 = 2 \cdot 3 \cdot 3 \qquad 18 = 3 \cdot 6 = 2 \cdot 3 \cdot 3$

la fattorizzazione unica vale per tutti gli insiemi di polinomi che voi troverete $\mathbb{Z}[x], \dots, \mathbb{C}[x], \dots \mathbb{R}[x][y], \dots$

$$x^7 - 2x^4 - 2x^3 + 4 = (x^3 - \overset{y^3}{2})(x^4 - 2) \qquad \mathbb{Z}[x] \text{ o } \mathbb{Q}[x]$$

$$= (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}\,x + \sqrt[3]{4})(x^2 - \sqrt{2})(x^2 + \sqrt{2})$$

$$= (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}\,x + \sqrt[3]{4})(x^2 + \sqrt{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}) \qquad \mathbb{R}[x]$$

$$= (x - \sqrt[3]{2})(x - \sqrt[3]{2}\,\xi)(x - \sqrt[3]{2}\,\bar{\xi})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2})$$

dove $\mathbb{C} \ni \xi = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$

- Alla fine su $\mathbb{C}$ si riesce sempre ad arrivare a $\deg p$ fattori di grado 1 $\in \mathbb{C}[x]$ (thm fond algebra)

- Su $\mathbb{R}$ non devono restare fattori di grado > 2 (nell'ipotesi che $p \in \mathbb{R}[x]$) (esercizio)

- Su $\mathbb{Q}$ e su $\mathbb{Z}$ si arriva alla stessa fattorizzazione (a meno di costanti) (nell'ipotesi che $p \in \mathbb{Z}[x]$) (lemma di Gauss)

- Vediamo nei dettagli

- Thm di Ruffini

$\mathbb{C} \ni \alpha$ radice di $p \iff p(\alpha)=0$ ovvero $a_n\alpha^n+a_{n-1}\alpha^{n-1}+\dots+a_1\alpha+a_0=0$

Se α è radice di p, $(x-\alpha)$ divide p

$a(x)=(x-\alpha)$ $\qquad p(x)=a(x)q(x)+r(x)$

$$0=p(\alpha)=\underbrace{a(\alpha)}_{0}q(\alpha)+r(\alpha) \Rightarrow r(\alpha)=0$$

$\deg r<\deg a=1$

$\left.\begin{array}{l}\Rightarrow r(x)=c\\ r(\alpha)=0\end{array}\right\} r(x)=0$

★ <u>Thm fond algebra</u> : $p\in\mathbb{C}[x]$ $\quad \exists\,\alpha\in\mathbb{C} : p(\alpha)=0$

+ induz + Ruffini

$\Rightarrow$ p si fattorizza in $\deg p$ polinomi di grado 1

- Su $\mathbb{R}$

$z,w\in\mathbb{C}$ $\qquad \boxed{\overline{z+w}=\bar z+\bar w}$ $\qquad \boxed{\overline{zw}=\bar z\,\bar w}$ $\qquad$ (verifica per casa)

$p\in\mathbb{R}[x]$ $\qquad$ thm.f.alg. $\exists\,\alpha\in\mathbb{C}$ $p(\alpha)=0$

$$0=\bar 0=\overline{p(\alpha)}=\overline{a_n\alpha^n+a_{n-1}\alpha^{n-1}+\dots+a_1\alpha+a_0}=\overline{a_n\alpha^n}+\dots+\overline{a_1\alpha}+\overline{a_0}$$
$$=\bar a_n\bar\alpha^n+\dots+\bar a_1\bar\alpha+\bar a_0=a_n\bar\alpha^n+\dots+a_1\bar\alpha+a_0=p(\bar\alpha)$$

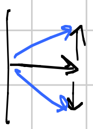
Ho scoperto che se α è una radice, anche $\bar\alpha$ lo è

- $\alpha\in\mathbb{R}$ non dice niente però $(x-\alpha)\,|\,p$ per Ruffini
- $\alpha\in\mathbb{C}\setminus\mathbb{R}$ $\bar\alpha$ è radice $(x-\alpha)$ e $(x-\bar\alpha)\,|\,p$ " "

$$(x-\alpha)(x-\bar\alpha)=x^2-\underbrace{(\alpha+\bar\alpha)}_{\mathbb{R}}x+\underbrace{\alpha\bar\alpha}_{\mathbb{R}}=x^2-\underset{2\mathrm{Re}(\alpha)}{\underset{\|}{a}}x+\underset{|\alpha|^2}{\underset{\|}{b}}\in\mathbb{R}[x]$$

I fattori di grado 2 irriducibili di $\mathbb{R}[x]$ sono sempre fatti così

$$x^2+ax+b \qquad x_{1,2}=\frac{-a\pm\sqrt{\Delta}}{2}$$



~ Conseguenza : $p \in \mathbb{R}[x]$ $\deg p$ dispari
$\Rightarrow$ p ha almeno una radice reale

- Lemma di Gauss

$p, q \in \mathbb{Z}[x]$ r numero primo

Se r divide tutti i coefficienti di $p(x)q(x)$
allora r divide tutti i coefficienti di p o tutti quelli di q

Dim $p(x) = p_0(x) + p_1(x)$ tutti i coeff di $p_0(x)$ sono
$q(x) = q_0(x) + q_1(x)$ multipli di r e nessun coeff
di $p_1(x)$ è multiplo di r

$$p(x)q(x) = \underbrace{p_0(x)q_0(x) + p_0(x)q_1(x) + q_0(x)p_1(x)}_{\text{tutti i coeff multipli di } r} + p_1(x)q_1(x)$$

almeno il termine direttivo non è $\equiv 0 \pmod r$

trovo che il coeff corrispondente di $p(x)q(x)$ non è multiplo di r $\rightarrow$ assurdo a meno che uno tra p_1 e q_1 sia nullo ovvero uno tra p e q abbia tutti i coeff divisibili per r.

★ $p \in \mathbb{Z}[x]$ $p(x) = a(x)b(x)$ $a, b \in \mathbb{Q}[x]$
tesi: allora $\exists$ fattorizzazione $p(x) = \tilde{a}(x)\tilde{b}(x)$ $\tilde{a}, \tilde{b} \in \mathbb{Z}[x]$

Dim Sia m il mcm di tutti i denominatori dei coeff di a
Sia n il mcm di tutti i denominatori dei coeff di b

$a(x) = \frac{1}{m} a'(x)$ $b(x) = \frac{1}{n} b'(x)$ con $a', b' \in \mathbb{Z}[x]$

$p(x) = \frac{a'(x)b'(x)}{mn} \in \mathbb{Z}[x]$ ciascuno dei coeff di $a'(x)b'(x)$ deve essere divisibile per mn

r primo $r \mid mn$ + Lemma di Gauss $\Rightarrow$ a' o b' ha coeff divisibili per r. Ad esempio è a'

$$p(x) = \frac{\frac{a'(x)}{r} \cdot b'(x)}{mn/r} \in \mathbb{Z}[x] \qquad \text{prendo } r' \text{ primo } r' \mid \frac{mn}{r} \quad + \text{ L.G. } \dots$$

per induzione sul numero di fattori primi di mn

$$p(x) = \underbrace{\frac{a'(x)}{\prod r_i}}_{\mathbb{Z}[x]} \cdot \underbrace{\frac{b'(x)}{\prod r_i'}}_{\mathbb{Z}[x]} = \tilde{a}(x) \cdot \tilde{b}(x)$$

✱ Se $p \in \mathbb{Z}[x]$ ha una radice razionale $\alpha = \frac{a}{b}$, $(a,b)=1$ allora $a \mid$ il termine noto e $b \mid$ il termine direttivo

$p(\alpha) = 0 \qquad (x-\alpha) = \left(x - \frac{a}{b}\right) = \frac{1}{b}(bx - a) \qquad bx - a \mid p$ su $\mathbb{Z}[x]$

$$p(x) = (bx-a)(c_n x^n + \dots + c_1 x + c_0) = b c_n x^{n+1} + \dots - a c_0$$

- Identità polinomi

$p, q \in \mathbb{C}[x] \qquad p(x_i) = q(x_i) \qquad i = 1, 2, \dots, n+1$

$\mathbb{C} \ni x_i$ distinti $\qquad n = \max(\deg p, \deg q)$

Allora $p = q$

$r(x) = p(x) - q(x) \qquad r(x_i) = 0 \qquad i = 1, 2, \dots, n+1$

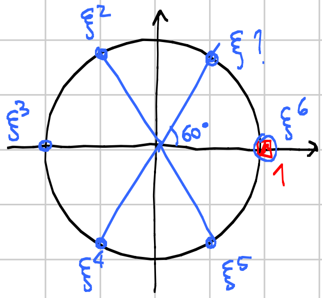
$\deg r \leq n \qquad$ ma r ha $n+1$ radici distinte,

quindi $\underbrace{(x-x_1)(x-x_2)\dots(x-x_{n+1})}_{\deg\, n+1} \mid \underbrace{r(x)}_{\deg\, \leq n}$

$\Rightarrow r(x) = 0 \Rightarrow p = q$.

- RADICI UNITÀ

$x^n = 1 \qquad \cancel{x=1} \qquad x^n - 1 = 0 \to n$ radici complesse distinte



$n=6 \qquad x \in \mathbb{C} \quad : \quad x \cdot x \cdot x \cdot x \cdot x \cdot x = 1$

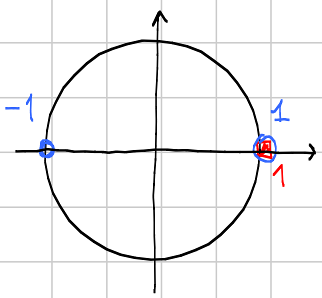
$1 = |1| = |x^n| = |x|^n \implies |x| = 1$

$\xi = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ è soluzione di $x^6 - 1 = 0$

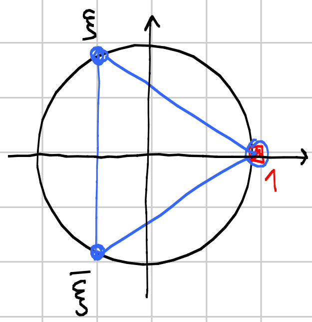
$\xi^2 = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \qquad (\xi^2)^6 = \xi^{12} = (\xi^6)^2 = 1^2 = 1$

$(\xi^m)^6 = (\xi^6)^m = 1^m = 1$

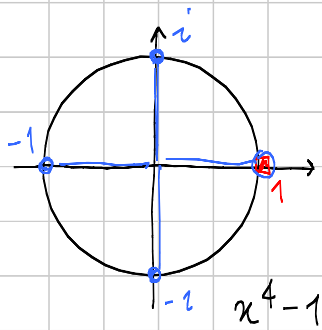
★ In generale le radici di $x^n - 1$ sono numeri complessi che stanno sui vertici di un n-agono regolare di raggio 1 e che ha un vertice in 1



$x^2 - 1$



$x^3 - 1$



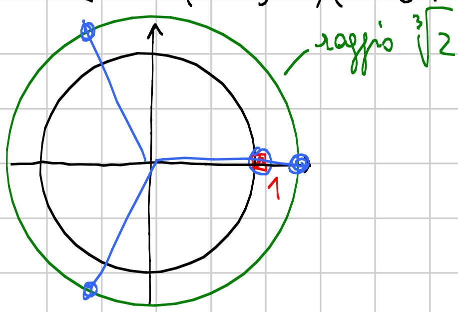
$x^4 - 1 = (x^2-1)(x^2+1)$

$1, -1, i, -i$

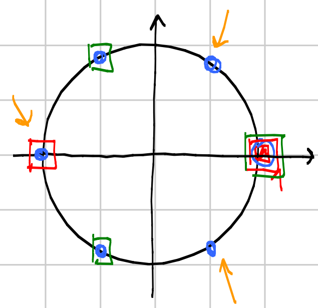
$1, \xi, \bar{\xi} \qquad \xi = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$

$x^3 - 1 = (x-1)\underbrace{(x^2+x+1)}$

$x^3 - 2 = (x - \sqrt[3]{2})(x - \xi\sqrt[3]{2})(x - \bar{\xi}\sqrt[3]{2})$



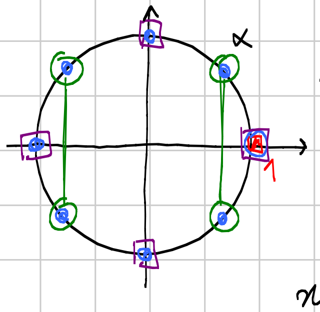
$x^3 + 1 = 0$



$x^6 - 1 = (x^3-1)(\qquad\qquad) = (x-1)(x^2+x+1)(\qquad$

$= (x^2-1)(\qquad\qquad) = (x-1)(x+1)(\qquad\qquad)$

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



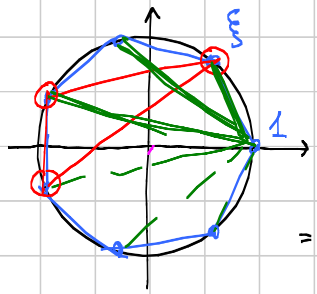
$$x^8-1=(x^4-1)(x^4+1)=(x-1)(x+1)(x^2+1)(x^4+1)$$

$$(x-\alpha)(x-\bar{\alpha})=x^2-2\,\mathrm{Re}\,x+|\alpha|^2=x^2-\sqrt{2}x+1$$

$$x^4+1=(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)$$

quindi non si fattorizza su $\mathbb{Z}[x]$

Esercizio



Q: prodotto dei lati del triangolo

$$\text{prod}=\sqrt{\prod 6 \text{ corde verdi}}$$

$$=\sqrt{|\xi-1|\,|\xi^2-1|\,|\xi^3-1|\,|\xi^4-1|\,|\xi^5-1|\,|\xi^6-1|}$$

$$(\xi-1)(\xi^6-1)=(\xi-1)(\overline{\xi-1})=|\xi-1|^2=|\xi-1|\,|\xi^6-1|$$

$$\text{prod}=\sqrt{(\xi-1)(\xi^2-1)(\xi^3-1)(\xi^4-1)(\xi^5-1)(\xi^6-1)}=\sqrt{p(1)}=\sqrt{7}$$

dove $p(x)=\dfrac{x^7-1}{x-1}=x^6+x^5+\ldots+x+1 \qquad p(1)=7$

$$x^7-1=(x-\xi)(x-\xi^2)\cdot\ldots\cdot(x-\xi^6)(x-1)$$

Relazioni radici coefficienti

$p\in\mathbb{C}[x] \qquad p(x)=a_nx^n+\ldots \qquad q(x)=\dfrac{p(x)}{a_n}$ è monico e ha le stesse radici

$$q(x)=x^n+b_{n-1}x^{n-1}+\ldots+b_1x+b_0$$
$$=(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$$

$\alpha_1\ldots\alpha_n\in\mathbb{C}$ sono le radici

$$=x^n-(\alpha_1+\alpha_2+\ldots+\alpha_n)x^{n-1}+(\alpha_1\alpha_2+\alpha_1\alpha_3+\ldots+\alpha_1\alpha_n+\alpha_2\alpha_3+\ldots\alpha_2\alpha_n+\ldots+\alpha_{n-1}\alpha_n)x^{n-2}$$
$$-\sum_{i<j<k}\alpha_i\alpha_j\alpha_k\,x^{n-3}+\ldots\pm\alpha_1\alpha_2\ldots\alpha_n$$

★ I coefficienti di q sono delle particolari funzioni simmetriche delle radici

— Ogni polinomio simmetrico di $\alpha_1 \dots \alpha_n$ si può scrivere in funzione di questi coefficienti

$$x^4 + x^3 - 2x^2 + 3x - 7$$

$$\frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \frac{1}{\alpha_3} + \frac{1}{\alpha_4} = \frac{\alpha_2\alpha_3\alpha_4 + \dots + \alpha_1\alpha_2\alpha_3}{\alpha_1\alpha_2\alpha_3\alpha_4} = -\frac{b_1}{b_0} = \frac{3}{7}$$

$$b_3 = -(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)$$
$$b_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4$$
$$b_1 = -(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4)$$
$$b_0 = \alpha_1\alpha_2\alpha_3\alpha_4$$

x, y $\qquad x + y = 7 \qquad xy = 5 \qquad x, y = ?$

$T^2 - (x+y)T + xy$ ha per radici x, y

$$T^2 - 7T + 5$$

$$x, y = \frac{7 \pm \sqrt{29}}{2}$$

A2 - base Disuguaglianze

Titolo nota 09/09/2010

no $\mathbb{C}$: $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ no $\mathbb{Z}/n\mathbb{Z}$

$x^2 \geq 0$ $\quad \frac{a^2+b^2}{2} \geq ab$ $\quad (a-b)^2 \geq 0$

x^2+x+1, x^2-x+1 sempre positivi

$x^2+\lambda x+1 \geq 0$ quando è sempre ≥ 0?

$x^2+1 \geq |\lambda x|$ per $|\lambda| \leq 2$

$\frac{x^2+1}{2} \geq x$

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

$(a+b-c)^2 = a^2+b^2+c^2-2ac-2bc+2ab$

$\frac{a^2+b^2}{2} \geq ab$

$\frac{b^2+c^2}{2} \geq bc$

$\frac{a^2+c^2}{2} \geq ca$

$a^2+b^2+c^2+$ $\quad (a+b+c)^2 \geq 0$

$a^2+b^2+c^2+2ab+2bc+2ca \geq 0$

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

$x > 0$

$$x + \frac{1}{x} \geq 2 \qquad \frac{x^2+1}{2} \geq \cancel{2}x$$

Riarrangiamento

$$a_1, a_2, \dots, a_n \xrightarrow{\sigma} a_{\sigma(1)}, a_{\sigma(2)}, \dots, a_{\sigma(n)}$$

$$\sigma: \begin{array}{c|c} 1 & \sigma(1) \\ 2 & \sigma(2) \\ 3 & \vdots \\ \vdots & \vdots \\ n & \sigma(n) \end{array} \qquad \text{bigettiva}$$

Supponiamo di avere $a_1 \geq a_2 \geq \dots \geq a_n$

e $b_1 \geq b_2 \geq \dots \geq b_n$ e una permutazione σ

$$\sum_{i=1}^{n} a_i b_{n+1-i} \underset{2}{\leq} \sum_{i=1}^{n} a_i \cdot b_{\sigma(i)} \underset{1}{\leq} \sum_{i=1}^{n} a_i b_i \qquad \begin{array}{c|c} i & \mathrm{id} \\ 1 & 1 \\ 2 & 2 \\ 3 & 3 \\ \vdots & \\ n & n \end{array}$$

<u>Dim.</u> 1: Supponiamo che $\sigma \neq \mathrm{id}$

dia somma maggiore di tutte

$$\sum_{i=1}^{n} a_i b_{\sigma(i)} > \sum_{h=1}^{n} a_i b_i$$

Allora esisterà una coppia j_1, j_2

tale che $\sigma(j_1) > \sigma(j_2)$ $j_1 < j_2$

$$\begin{array}{c|c} & \sigma \\ j_1 & \sigma(j_1) \\ \wedge & \vee \\ j_2 & \sigma(j_2) \end{array}$$

$$a_1 b_{\sigma(1)} + \cdots + a_{j_1} b_{\sigma(j_1)} + \cdots + a_{j_2} b_{\sigma(j_2)} + \cdots$$

$$a_1 b_{\sigma(1)} + \cdots + a_{j_1} b_{\sigma(j_2)} + \cdots + a_{j_2} b_{\sigma(j_1)} + \cdots$$

$$a_{j_1}\underbrace{\left(b_{\sigma(j_1)} - b_{\sigma(j_2)}\right)}_{\leq 0} + a_{j_2}\underbrace{\left(b_{\sigma(j_2)} - b_{\sigma(j_1)}\right)}_{\geq 0}$$

$$\sigma(j_1) > \sigma(j_2) \Rightarrow b_{\sigma(j_1)} \leq b_{\sigma(j_2)}$$

$$\underbrace{(a_{j_2} - a_{j_1})}_{\geq 0}\underbrace{\left(b_{\sigma(j_2)} - b_{\sigma(j_1)}\right)}_{\geq 0} \leq 0$$

Ma se era il massimo, < 0 è assurdo

$= 0 \Rightarrow$ $a_{j_1} = a_{j_2}$ e anche quelli tra j_1 e j_2

$b_{\sigma(j_2)} = b_{\sigma(j_1)}$ $\sigma(j_2)$ e $\sigma(j_1)$

Quindi

- o σ scambia solo elementi uguali
- o σ non è massimo

Se σ scambia solo elementi uguali allora

$$\sum_{i=1}^{n} a_i b_{\sigma(i)} = \sum_{i=1}^{n} a_i b_i .$$

2 Il caso del minimo è analogo.

$a, b, c > 0$ reali

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

$$b \log a + c \log b + a \log c \leq a \log a + b \log b + c \log c$$

a, b e c hanno lo stesso ordine di $\log a$, $\log b$ e $\log c$

Quindi $a \log a + b \log b + c \log c \geqslant$ tutte le somme con le altre permutazioni, quindi anche $\geqslant b \log a + c \log b + a \log c$

$$\frac{a^2}{b} + \frac{b^2}{c} + \frac{c^2}{a} \geqslant a+b+c$$

a^2 b^2 e c^2 sono in ordine inverso rispetto a $\frac{1}{a}$ $\frac{1}{b}$ $\frac{1}{c}$.

Allora $a^2 \cdot \frac{1}{a} + b^2 \cdot \frac{1}{b} + c^2 \cdot \frac{1}{c} \leq$ tutte le somme

tra cui .

$a_1, \ldots, a_n > 0$ reali

$$\frac{a_1}{a_2} + \frac{a_2}{a_3} + \cdots + \frac{a_{n-1}}{a_n} + \frac{a_n}{a_1} \geqslant n$$

$a_1 \ldots a_n$ e $\frac{1}{a_1} \ldots \frac{1}{a_n}$ inversamente ordinati

tutte le somme $\geqslant a_1 \cdot \frac{1}{a_1} + a_2 \cdot \frac{1}{a_2} + \cdots = 1+1+\cdots 1$
$= n$

Disuguaglianza di Chebychev

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

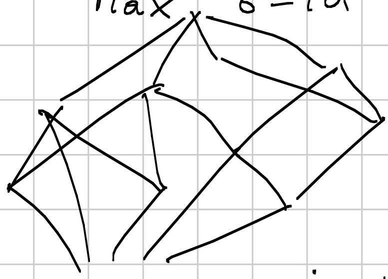
$$\frac{\sum a_i b_{n+1-i}}{n} \leq \frac{\sum_{i=1}^n a_i}{n} \cdot \frac{\sum_{i=1}^n b_i}{n} \leq \frac{\sum_{i=1}^n a_i b_i}{n}$$

Dim

$$
\begin{array}{llll}
0 & a_1 b_1 + a_2 b_2 + \dots & + a_n b_n & \leq a_1 b_1 + a_2 b_2 + \dots + a_n b_n \\
+1 & a_1 b_2 + a_2 b_3 + \dots & + a_n b_1 & \leq a_1 b_1 + a_2 b_2 + \dots + a_n b_n \\
+2 & a_1 b_3 + a_2 b_4 + \dots & + a_n b_2 & \leq \quad \dots \\
\vdots & & & \\
+n-1 & a_1 b_n + a_2 b_1 + & + a_n b_{n-1} & \leq \quad \dots \\
\hline
\end{array}
$$

$$\frac{n \sum_{i=1}^n a_i b_{n+1-i}}{n^2} \leq \frac{\left(\sum_{i=1}^n a_i\right)}{n} \frac{\left(\sum_{i=1}^n b_i\right)}{n} \leq \frac{n \sum_{i=1}^n a_i b_i}{n^2}$$

Max $\sigma = id$



Min $\sigma = i \mapsto n+1-i$

$$\sigma \quad \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{array} \qquad \tau \quad \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{array}$$

σ cambia l'ordine di 3 e 4 $\quad \tau$ lo conserva

per il resto sono uguali

$$\sum_{i=1}^{5} a_i b_{\sigma(i)} \le \sum_{i=1}^{5} a_i b_{\tau(i)}$$

variabili solo positive ?

quando vale = ?

è omogenea?

$$\frac{a^2+b^2}{2} \geq ab \qquad a \to \lambda a \quad b \to \lambda b$$

$$\frac{\cancel{\lambda^2} a^2 + \cancel{\lambda^2} b^2}{2} \geq \cancel{\lambda^2} ab$$ omogenea di grado 2

Riarrang. → omog. grado 2

Dis. non omogenea vale con difficoltà su tutto $\mathbb{R}^+$

$x^2 \geq x^3 \quad 0 \le x \le 1$

$x^2 \le x^3 \quad x \geq 1$

Chebychev omog. grado 2

Quando = ? Se esiste $b_i \neq b_j$ prima o poi li scambio con uno "shift" della dim. di Chebychev ⇒ tutti i b_i devono essere = perché valga l'= a destra. Ma anche a sinistra è la stessa cosa.

Media

$$\{a_1, \dots, a_n\} \longrightarrow m$$

$$\min\{a_i\} \le m \le \max\{a_i\}$$

$$a_i \longmapsto \lambda a_i \qquad m \longmapsto \lambda m$$

$$a_i \longmapsto a_i + k \qquad m \longmapsto m + k$$

AM $\quad \dfrac{a_1 + a_2 + \dots + a_n}{n}$

GM $\quad \sqrt[n]{a_1 \cdot a_2 \cdot \dots \cdot a_n} \qquad a_i \geq 0$

Disuguaglianza AM–GM

$$\sqrt[n]{a_1 \dots a_n} \le \frac{a_1 + a_2 + \dots a_n}{n} \qquad \mathbb{R}^+ \qquad = \iff a_i \text{ tutti uguali}$$

omog. grado 1

$$\frac{a_1 + a_2}{2} \geq \sqrt{a_1 a_2} \qquad x_1 = \sqrt{a_1} \quad x_2 = \sqrt{a_2}$$

$$\frac{x_1^2 + x_2^2}{2} \geq x_1 x_2 \qquad \frac{a_1^2 + 2a_1a_2 + a_2^2}{4} \geq a_1 a_2$$

$$(a_1 - a_2)^2 \geq 0$$

$$\frac{a_1^2 + a_2^2}{\cancel{2}\, 4} \geq \frac{a_1 a_2}{2}$$

$$G = \sqrt[n]{a_1 \dots a_n} \qquad x_1 = \left(\frac{a_1}{G}\right)^{-1} \quad x_2 = \left(\frac{a_2 a_2}{G^2}\right)^{-1} \dots x_n = \left(\frac{a_1 a_2 \cdots a_n}{G^n}\right)^{-1}$$

$$\frac{x_1}{x_2}+\frac{x_2}{x_3}+\cdots\geq n \qquad \frac{x_1}{x_2}=\cancel{\frac{\frac{a_1}{G}}{\frac{a_1a_2}{G^2}}}=\frac{G}{a_2}\ \frac{a_2}{G}$$

$$\frac{x_2}{x_3}=\cancel{\frac{\frac{a_1a_2}{G^2}}{\frac{a_1a_2a_3}{G^3}}}=\frac{G}{a_3}\ \cdots\ \frac{a_3}{G}$$

Anzi voglio $\frac{x_1}{x_2}=\frac{a_2}{G}$ $\frac{x_2}{x_3}=\frac{a_3}{G}\cdots$

$$\frac{x_1}{x_2}+\frac{x_2}{x_3}+\cdots=\frac{a_2}{G}+\frac{a_3}{G}+\cdots+\frac{a_1}{G}\geq n$$

$$\Rightarrow\ \frac{a_1+a_2+\cdots+a_n}{n}\geq G$$

Trovare il minimo di $x+2y+3z$ se $x^3y^2z=1$

$x>0\ y>0\ z>0$

$$\frac{x+2y+3z}{3}\geq\sqrt[3]{x\cdot 2y\cdot 3z}=\sqrt[3]{6xyz}$$

$$\frac{\frac{x}{3}+\frac{x}{3}+\frac{x}{3}+y+y+3z}{6}\geq\sqrt[6]{\frac{x^3}{\cancel{27}_{9}}\cdot y^2\cdot\cancel{3}z}=\sqrt[6]{\frac{1}{9}}\sqrt[6]{\underset{\substack{\shortparallel\\1}}{x^3y^2z}}$$

$$x+2y+3z\geq 6\cdot\sqrt[3]{\frac{1}{3}} \qquad \overset{?}{=} \qquad \frac{x}{3}=y=3z$$

$$x=9z \qquad y=3z \qquad 9^3 3^2 z^6=1 \qquad z^6=\frac{1}{9^3 3^2}$$

$$z=\frac{1}{3}\frac{1}{\sqrt[3]{3}}$$

$$(a+3b)(b+4c)(c+2a)\geq 60\,abc$$

$$\underset{2\sqrt{3ab}}{\rotatebox{90}{$\leq$}}\quad \underset{2\sqrt{4bc}}{\rotatebox{90}{$\leq$}}\quad \underset{2\sqrt{2ac}}{\rotatebox{90}{$\leq$}}\quad =8\sqrt{24abc}$$

$$a+b+b+b \qquad b+c+c+c+c \qquad c+a+a$$

$$4\sqrt[4]{ab^3} \qquad 5\sqrt[5]{bc^4} \qquad 3\sqrt[3]{ca^2} \qquad \frac{1}{4}+\frac{2}{3} \qquad \frac{4}{5}+\frac{1}{3}$$

$b \quad \frac{4}{3}c \quad \frac{4}{3}c \cdot \frac{4}{3}c \qquad c \quad \frac{2}{3}a \quad \frac{2}{3}a \quad \frac{2}{3}a$

$$4\sqrt[4]{ab^3} \qquad 4\sqrt[4]{\frac{64}{27}bc^3} \qquad 4\sqrt[4]{\frac{8}{27}ca^3}$$

$$64\sqrt[4]{a^4b^4c^4\,\frac{512}{729}}$$

$a=b=c \qquad\qquad a+3b = x_1+x_2+\dots+x_n$

$$\overbrace{\frac{a}{15}\quad\dots}^{15} + \overbrace{\frac{b}{15}\quad\dots}^{45} \qquad a+3b$$

$$\overbrace{\frac{b}{12}\quad\dots}^{12} \quad \overbrace{\frac{c}{12}\quad\dots}^{48} \qquad b+4c$$

$$\overbrace{\frac{a}{20}\quad\dots}^{40} \quad \overbrace{\frac{c}{20}\quad\dots}^{20} \qquad c+2a$$

$$\min\ \{x^2+y^4+z^6 \quad \text{su} \quad xyz=n\} = A_n$$

$$\overbrace{\frac{x^2}{6}}^{6} \quad \overbrace{\frac{y^4}{3}}^{3} \quad \overbrace{\frac{z^6}{2}}^{2}$$

$$\frac{x^2+y^4+z^6}{11} \geq \sqrt[11]{(xyz)^{12}\cdot\frac{1}{6^6\cdot 3^3\cdot 2^2}} = \sqrt[11]{\frac{1}{6^6 3^3 2^2}}\, n^{12/11}$$

$$\frac{z^6}{2}=t \qquad \frac{y^4}{3}=t \qquad \frac{x^2}{6}=t$$

Media quadratica: $\sqrt[2]{\dfrac{a_1^2+a_2^2+\dots+a_n^2}{n}} = QM$

Media armonica: $\dfrac{1}{\dfrac{\frac{1}{a_1}+\frac{1}{a_2}+\frac{1}{a_3}\dots+\frac{1}{a_n}}{n}} = HM$

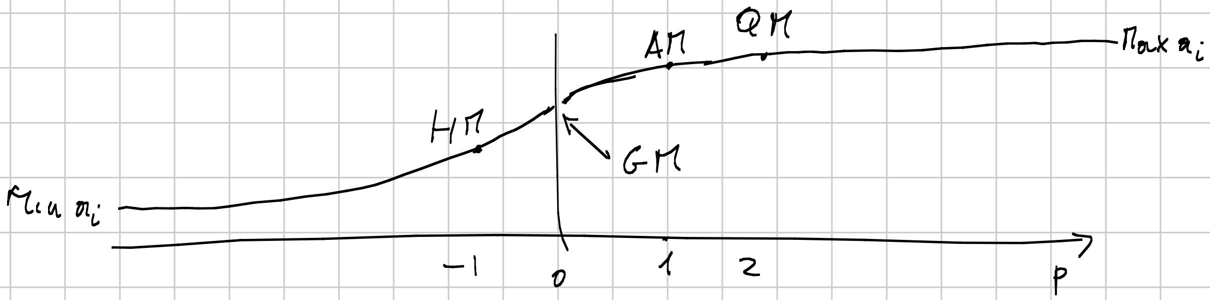
$$M_p = \left(\frac{a_1^p+a_2^p+\dots+a_n^p}{n}\right)^{1/p} \qquad \begin{array}{ll} p=2 & QM \\ p=1 & AM \\ p=-1 & HM \end{array}$$

$p = 0$?   se $p \le q$ $M_p \le M_q$

se $p < q$ e $M_p = M_q$ $\iff$ a_i tutti uguali

se faccio un grafico

al variare di p $a_1 \cdots a_n$ fissati



HM–GM ? $$\frac{n}{\frac{1}{a_1}+\dots+\frac{1}{a_n}} \le \sqrt[n]{a_1 \cdots a_n}$$

$b_i = \frac{1}{a_i}$ $$\frac{n}{b_1+\dots+b_n} \le \sqrt[n]{\frac{1}{b_1 \cdots b_n}}$$

$$\sqrt[n]{b_1 \cdots b_n} \le \frac{b_1+\dots+b_n}{n}$$

<u>Dim</u>   sia $b_i = \frac{1}{a_i}$ per AM–GM

$$\sqrt[n]{b_1 \cdots b_n} \le \frac{b_1+\dots b_n}{n}$$ Allora

$$\frac{n}{b_1+\dots+b_n} \le \sqrt[n]{\frac{1}{b_1 \cdots b_n}}$$ quindi sost.

$$\frac{n}{\frac{1}{a_1}+\dots+\frac{1}{a_n}} \le \sqrt[n]{a_1 \cdots a_n}$$ cioè la tesi.

Disuguaglianza di Cauchy-Schwarz

$$a_1 \dots a_n \qquad b_1 \dots b_n \qquad \in \mathbb{R}$$

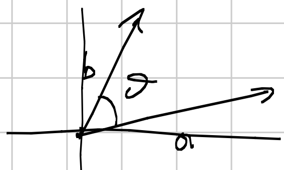
$$\sqrt{\sum_{i=1}^{n} a_i^2} \cdot \sqrt{\sum_{i=1}^{n} b_i^2} \geq \left| \sum_{i=1}^{n} a_i \cdot b_i \right|$$

$$v = (a_1, a_2, \dots a_n) \qquad w = (b_1, \dots, b_n)$$

$$\|v\| = \sqrt{a_1^2 + a_2^2 + \dots a_n^2}$$

prodotto scalare tra v e w

$$\|v\| \cdot \|w\| \geq \left| \sum_{i=1}^{n} a_i b_i \right|$$



$$a \cdot b = ab \cos \vartheta$$

$$\|v\| \geq 0$$

$$\|v + \lambda w\| \geq 0 \qquad \forall \lambda$$

$$(a_1 + \lambda b_1)^2 + (a_2 + \lambda b_2)^2 + \dots + (a_n + \lambda b_n)^2 \geq 0$$

$$a_1^2 + a_2^2 + \dots + a_n^2 + 2(a_1 b_1 + a_2 b_2 + \dots + a_n b_n)\lambda + \qquad \forall \lambda$$
$$+ (b_1^2 + \dots + b_n^2)\lambda^2 \geq 0$$

$$(a_1 b_1 + \dots + a_n b_n)^2 - (a_1^2 + \dots + a_n^2)(b_1^2 + \dots + b_n^2) \leq 0$$

$$\left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=1}^{n} b_i^2\right) \geq \left(\sum_{i=1}^{n} a_i b_i\right)^2 .$$

1) $\in \mathbb{R}$

2) $=$ se $a_i = t b_i \quad \forall i$

$$a_1 \dots a_n \qquad b_1 = 1 \quad b_2 = 1 \dots b_n = 1$$

$$\left(\sum_{i=1}^{n} a_i^2\right) \cdot n \geq \left(\sum a_i\right)^2 \qquad \sqrt{\frac{\sum_{i=1}^{n} a_i^2}{n}} \geq \frac{\sum_{i=1}^{n} a_i}{\cancel{\sqrt{n}}\ n}$$

QM $\qquad$ AM

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

$$v=(a,b,c) \qquad w=(b,c,a)$$

$$\sqrt{a^2+b^2+c^2}\cdot\sqrt{b^2+c^2+a^2} \geq |ab+bc+ca|.$$

Nesbitt: $\dfrac{a}{b+c}+\dfrac{b}{c+a}+\dfrac{c}{a+b} \geq \dfrac{3}{2}$

$a+b=y$
$b+c=y$
$c+a=z$
riarrang.

$$\left(\sqrt{\frac{a}{b+c}},\sqrt{\frac{b}{c+a}},\sqrt{\frac{c}{a+b}}\right)$$

$$\left(\sqrt{a}\sqrt{b+c},\sqrt{b}\sqrt{c+a}\ \sqrt{c}\sqrt{a+b}\right)$$

$$\left(\frac{a}{b+c}+\cdots\right)\left(2(ab+bc+ca)\right) \geq (a+b+c)^2$$

$$\frac{a}{b+c}+\cdots \geq \frac{a^2+b^2+c^2}{2(ab+bc+ca)}+\frac{2(ab+bc+ca)}{2(ab+bc+ca)}$$

$$\geq \frac{1}{2} \qquad + \qquad 1 \qquad = \frac{3}{2}$$

Dis. raggruppamento o bunching o Muirhead.

$a_1 \cdots a_n \qquad \sum_{cyc} a_i^2 a_{i+1} \qquad \sum_{cyc}^{a,b,c} a^2b = a^2b+b^2c+c^2a$

$$\sum_{sym}^{a,b,c} a^2b = a^2b+b^2c+c^2a+ab^2+bc^2+ca^2$$

2, 1, 0
a b c
b c a
c a b

2 1 0
a b c
a c b
b a c
b c a
c a b
c b a

2 1 1
a b c a^2bc
a c b a^2cb

1 1 1
a b c
b a c

$$\sum_{sym} abc = 6abc$$

su $\mathbb{R}^+$

Le somme simmetriche più grandi sono quelle con gli esponenti più concentrati.

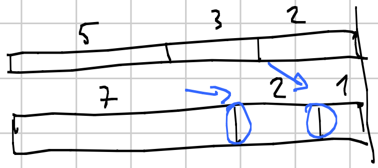
$\overline{k}$ $\quad k_1 \geq \dots \geq k_n$

$\overline{h}$ $\quad h_1 \geq \dots \geq h_n$

$\overline{k} \geq \overline{h}$ se

$k_1 \geq h_1$ e $k_1+k_2 \geq h_1+h_2$ e

$k_1+k_2+k_3 \geq h_1+h_2+h_3$ e.. $\sum k_i = \sum h_i$



$$\sum_{sym} x^4 y^2 z \geq \sum_{sym} x^3 y^2 z^2$$

$4 > 3$

$4+2 > 3+2$

$4+2+1 = 3+2+2$

$\mathbb{R}^+$

$=$ se e solo se tutte le variabili uguali

omog. di vari gradi

$$\sum_{sym} x^3 + \sum_{sym} xyz \geq 2\sum_{sym} x^2 y \qquad \text{Schur}$$

$$a(a-b)(a-c) + b(b-c)(b-a) + c(c-b)(c-a) \geq 0$$

$\geq 0 \quad \leq 0 \quad \geq 0$

$a \geq b \geq c$.

$a(a-c) - b(b-c) \geq 0$? Ovviamente sì

$\mathbb{R}^+$

$=$ due var. $=$ e 1 è 0

$$a^k(a-b)(a-c) + b^k(b-c)(b-a) + c^k(c-b)(c-a) \geq 0.$$

$$\frac{1}{a^3+b^3+1}+\frac{1}{b^3+c^3+1}+\frac{1}{c^3+a^3+1}\le 1$$

$$abc=1$$

$$\frac{1}{a^3+b^3+abc}+\frac{}{+abc}+\frac{}{+abc}\le\frac{1}{abc}$$

$$\sum a^6b^3 \ge \sum a^5b^2c^2$$

A3 BASIC -Maria-

Titolo nota 10/09/2010

- Identità
- Successioni
- Eq funzionali.

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

$$\begin{aligned} (a^2+b^2)(c^2+d^2) &= |a+ib|^2 \cdot |c+id|^2 = |(a+ib)(c+id)|^2 \\ &= |(ac-bd) + i(bc+ad)|^2 \end{aligned}$$

Es: $p \in \mathbb{R}[x]$: $P(x) \geq 0 \ \forall x$

$\Rightarrow \exists\, q, r \in \mathbb{R}[x]$:
$p(x) = q(x)^2 + r(x)^2$

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

$$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + \dots + y^{n-1}) \text{ (con } n \text{ dispari)}$$

$$x^n + y^n = x^n - (-y)^n$$

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

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

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

Se n è dispari $\frac{n-1}{2}(n+1) + \frac{n+1}{2} = \frac{n(n+1)}{2}$

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

Dim 1: per induz.

Dim 2: $(n+1)^3 - 1 = \sum_{i=1}^{n} (i+1)^3 - i^3$

$$= \sum_{i=1}^{n} 3i^2 + 3i + 1$$

$$= 3\sum i^2 + 3\underbrace{\sum i}_{\frac{n(n+1)}{2}} + n$$

$$\sum i^2 = \frac{(n+1)^3 - 1 - 3\frac{n(n+1)}{2} - n}{3}$$

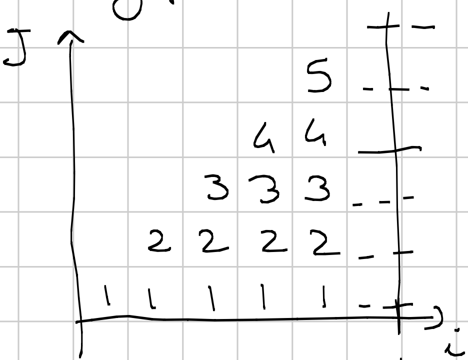
Oss $p(m) = \frac{n(n+1)(2n+1)}{6}$

$p(m)$	1	5	14	30	55	91	...
m^2		4	9	16	25	36	...
$2m+1$			5	7	9	11	...
			2	2	2	2	...

$\deg(p(m+1) - p(m)) \leq$ ~~$\deg p - 1$~~

Dim 3:

$\sum i^2$



$$\sum_{J=1}^{n}\left(\sum_{i=J}^{n} J\right) = \text{SOMMA FATTA} \times \text{RIGHE}$$

$$= \sum_{J=1}^{n} J(n+1-J) = (n+1)\sum_{J=1}^{n} J - \sum J^2$$

$$\sum_{i=1}^{n}\left(\sum_{J=1}^{i} J\right) = \text{SOMMA FATTA} \times \text{COLONNE}$$

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

$$(n+1)\frac{n(n+1)}{2} - \sum_{j=1}^{n} j^2 = \sum \frac{j(j+1)}{2} = \frac{1}{2}\sum_{j=1}^{n} j^2 + \frac{1}{2}\sum_{j=1}^{n} j$$

$$= \frac{1}{2}\sum j^2 + \frac{n(n+1)}{4}$$

Oss: $\sum_{i=1}^{\infty} \frac{1}{i} = +\infty$

$$\sum_{i=1}^{\infty} \frac{1}{i} = \underbrace{1}_{} + \underbrace{\frac{1}{2}}_{} + \underbrace{\frac{1}{3} + \frac{1}{4}}_{} + \underbrace{\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}}_{} + \dots$$

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

$$= 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \dots \longrightarrow +\infty$$

SUCCESSIONI

$$a_n = \begin{cases} 0 & \text{se } n \text{ dispari} \\ 1 & \text{se } n \text{ pari} \end{cases}$$

$$\begin{cases} a_{n+1} = 2a_n & \text{(ricorrenza)} \\ a_0 = 3 & \text{(dato iniziale)} \end{cases}$$

Succ di Fibonacci: $\begin{cases} a_{n+1} = a_n + a_{n-1} \\ a_0 = 0 \\ a_1 = 1 \end{cases}$

$$a_{n+1} = 2n\, a_n + a_{n-5}$$

Progr aritm e geometriche

$$a_n = a + dn \qquad a_n = a_{n-1} + d$$

$$\sum_{n=1}^{N} a_n = \sum_{n=1}^{N} a + dn = aN + d \sum_{n=1}^{N} n = aN + d\,\frac{N(N+1)}{2}$$

$$a_n = a r^n \qquad \begin{cases} a_n = r\, a_{n-1} \\ a_0 = a \end{cases}$$

$$\sum_{i=1}^{N} a_i = \sum_{n=1}^{N} a r^n$$

$$a \sum r^n = a\,(1 + r + r^2 + \dots + r^N)$$

$$a r \sum r^n = a\,(\ \ r + r^2 + \dots + r^{N+1})$$

$$a \cdot \sum_{n=1}^{N} r^n = \frac{a\,(1 - r^{N+1})}{1-r} \qquad \text{se } r \neq 1$$

$$\text{Se } r = 1 \qquad a_n = a \qquad \sum_{n=1}^{N} a_n = aN$$

Oss: se $r < 1$

$$\sum_{n=1}^{\infty} r^n = \lim_{N \to +\infty} \frac{1 - r^{N+1}}{1-r} = \frac{1}{1-r}$$

$$\begin{cases} x_{n+1} = a x_n + b \\ x_0 \text{ fissato} \end{cases}$$

$$x_0$$
$$x_1 = a x_0 + b$$
$$x_2 = a x_1 + b = a(a x_0 + b) + b$$
$$\vdots \qquad = a^2 x_0 + ab + b$$

$$x_n = a^n x_0 + a^{n-1} b + a^{n-2} b + \dots + b$$
$$= a^n x_0 + b\,\frac{a^{n-1} - 1}{a-1}$$

Ricorrenze da due termini precedenti:

Esercizio: $a_1 > a_0 + 1 > 0$ fissati.

$a_2 = 3a_1 - 2a_0$, $a_3 = 3a_2 - 2a_1$, ---

Dimostrare che $a_{100} > 2^{99}$

$a_2 - a_1 = 2(a_1 - a_0)$, $a_3 - a_2 = 2(a_2 - a_1)$, --

$a_{100} - a_{99} = 2(a_{99} - a_{98}) = \dots = 2^{99}(a_1 - a_0)$

$\Rightarrow a_{100} = \underbrace{a_{99}}_{>0} + 2^{99}(a_1 - a_0) > 2^{99} \cdot 1$

In generale:

$$\begin{cases} x_0 \\ x_1 \quad \text{fissati} \\ x_{n+1} = \alpha x_n + \beta x_{n-1} \end{cases}$$

Formula chiusa per x_n.

Dimentichiamo i dati iniziali.

$\{a_n\}$, $\{b_n\}$ verificano, dati $A, B \in \mathbb{R}$

$\Rightarrow \{A a_n + B b_n\}$ verifica la ricorrenza.

$$A a_{n+1} + B b_{n+1} \overset{?}{=} \alpha(A a_n + B b_n) + \beta(A a_{n-1} + B b_{n-1})$$

$x_n = r^n$ verifica la ric per qualche n?

$r^{n+1} = \alpha r^n + \beta r^{n-1} \iff r^2 - \alpha r - \beta = 0$

$r = \begin{cases} r_1 \\ r_2 \end{cases}$ radici.

$A r_1^n + B r_2^n$ verifica la ricorrenza.

$$\begin{cases} x_0 \\ x_1 \quad \text{fissati} \\ x_{n+1} = \alpha x_n + \beta x_{n-1} \end{cases}$$

$$\begin{cases} x_0 = A + B \\ x_1 = A r_1 + B r_2 \end{cases} \Rightarrow \text{ trovo } A \text{ e } B.$$

$$\begin{cases} x_0 = 1 \\ x_1 = 2 \\ x_{n+1} = 2x_n + x_{n-1} \end{cases}$$

$x_3 = 2 \cdot 2 + 1 = 5$

$x_4 = 2 \cdot 5 + 2 = 12$

$\vdots$

Vale se $r_1 \neq r_2$

Se $r_1 = r_2$ $\begin{cases} x_0 = A+B \\ x_1 = r_1 (A+B) \end{cases}$

Provare $n \cdot r^n = x_n$

Se $r_1 = r_2 = r$

$x_{n+1} = \alpha x_n + \beta x_{n-1}$

$x^2 - \alpha x - \beta = (x - r)^2$

$\alpha = 2r \quad \beta = -r^2$

$x_{n+1} = 2r x_n - r^2 x_{n-1}$

$n r^n = x_n \longrightarrow (n+1) r^{n+1} = 2 r^{n+1} \cdot n - r^2 (n-1) r^{n-1}$

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

$A r^n + B n r^n$ sono sol.

$$\begin{cases} x_0 \\ x_1 \end{cases} \text{ fissati} \qquad x_{n+1} = \alpha x_n + \beta x_{n-1}$$

$$\begin{cases} x_0 = A \\ x_1 = A r + B \cdot r \end{cases} \Rightarrow \text{ trovo } A \text{ e } B.$$

Esempio $\begin{cases} a_0 = 1 \\ a_1 = 2 \\ a_{n+1} = 3a_n - 2a_{n-1} \end{cases}$

(1) Trovo le radici di $x^2-3x+2=0$
Sono $r_1=1$ e $r_2=2$.

(2) Deduco che $A\cdot 1^n + B\cdot 2^n$ è sol. della ricorrenza

(3) Impongo i dati iniziali

$$\begin{cases} 1 = A+B \\ 2 = A+2B \end{cases} \qquad \begin{cases} A = 1-B \\ 2 = 1+B \end{cases} \Rightarrow \begin{cases} A = 0 \\ B = 1 \end{cases}$$

La succ che verifica il dato iniziale è 2^n.

Esempio (numeri di Fibonacci)

Succ di Fibonacci: $\begin{cases} a_{n+1} = a_n + a_{n-1} \\ a_0 = 0 \\ a_1 = 1 \end{cases}$

$x^2-x-1=0 \qquad r_{1,2} = \dfrac{1\pm\sqrt{5}}{2}$

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

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

Esercizio: vedere perchè la formula esplicita, pur avendo coeff compl., restituisce numeri reali

Esercizio:
n Bambini in riga.
Permutazioni in cui ogni bambino dista al + 1 dalla sua posiz originale?

a_n //

0

1

$$\begin{cases} a_1 = 1 \\ a_2 = 2 \\ a_3 = 3 \end{cases}$$

$n = 3$

1 2 3

1 3 2

2 1 3

$a_{n+1} = a_n + a_{n-1}$

ultimi 2 si scambiano -

ultimo rimane fermo

$a_n = (n+1)$- n° numero di Fibonacci

Esercizio: bambini in cerchio -

EQUAZIONI FUNZIONALI

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

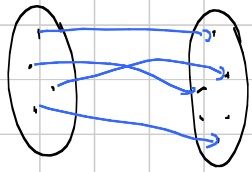
$f: \mathbb{R} \to \mathbb{R}$ $\quad f(x) = ax \quad a \in \mathbb{R}$

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

Iniettività, surgettività, ...

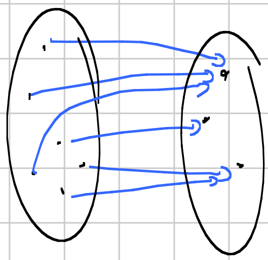
f iniettiva $\quad a \neq b \Rightarrow f(a) \neq f(b)$

f surgettiva $\quad \forall y \in Y \quad \exists x: f(x) = y$



f biunivoca $\Leftrightarrow$ iniett e surg.

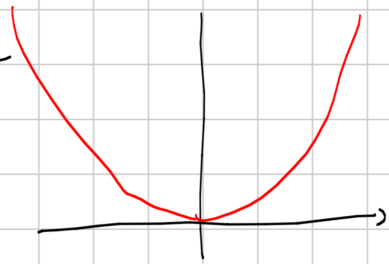
Si può invertire



Esempi: $f(x) = x$ biiettiva

$f(x) = x^2$

$\searrow$ non è iniettiva
non è surg.



$x^2|_{(0,+\infty)}$ è iniettiva

Come funzione $\mathbb{R} \to \mathbb{R}_{\geq 0}$ è surg.

$\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ è biunivoca.

f crescente $\Leftrightarrow$ $a \leq b \Rightarrow f(a) \leq f(b)$

(strett) $\quad <$ $\quad <$

Oss: $f: \mathbb{R} \to \mathbb{R}$ strett crescente è iniettiva.

Esercizio: $f:\mathbb{R}\to\mathbb{R}$ crescenti t.c.

$f(f(x)) = x$.

Dim: senza hp di crescenza

$0 \to 1 \quad 1 \to 0$

$0.5 \to 7 \quad 7 \to 0.5$

$$f(x) = \begin{cases} x & \text{se } x \in \mathbb{Q} \\ -x & \text{se } x \in \mathbb{R}\setminus\mathbb{Q} \end{cases}$$

$f(x) = x$ verifica

Supponiamo per assurdo esista un'altra f

- $f(x) > x$ oppure $f(x) < x$

$\Downarrow$

$f(f(x)) > f(x)$

$\shortparallel$

x

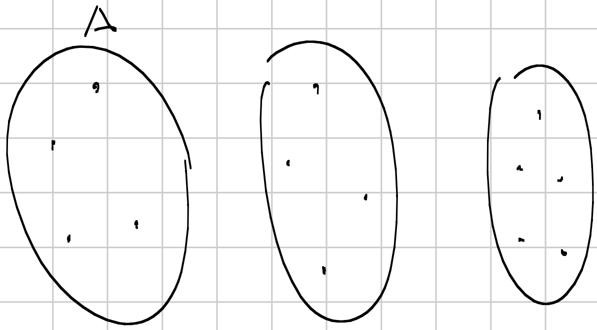
contraddizione.

COMPOSIZIONE

f, g funzioni

f, g iniettive

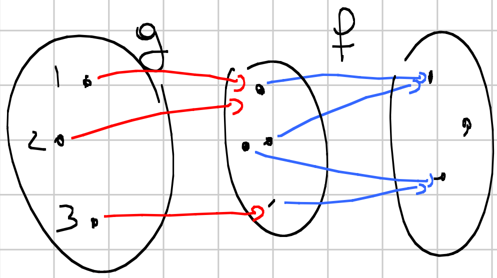
$\Rightarrow f \circ g$ è iniett.



f, g surgettive $\Rightarrow f\circ g$ surg

Esercizio: f iniett g surg $\Rightarrow$ non posso conclu.

dove né iniett né surgett su $f\circ g$ e $g \circ f$.



Supponiamo

$f \circ g$ surg.

$\Rightarrow f$ surg.

$f \circ g$ iniettiva

$\Rightarrow g$ iniettiva

$f_1 \circ \dots \circ f_k$ surg $\Rightarrow f_1$ è surg

iniett $\Rightarrow f_k$ è iniett

$$f(f(x)^2+5) = 2x+7$$

$\Rightarrow f$ iniett? $\quad g(y) = y^2+5 \quad f(g(f(x))) = 2x+7$

f surgett? OK $\quad \Downarrow$

f iniettiva.

$$\begin{cases} a_0 = 2 \\ a_1 = 3 \\ a_{n+1} = 2^{n+1} + a_n + a_{n-1} \end{cases}$$

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

$\{a_n\}$ sol particolare

$$x_n = \underbrace{A\left(\frac{1+\sqrt5}{2}\right)^n + B\left(\frac{1-\sqrt5}{2}\right)^n}_{\text{sol generale dell'omogenea}} + \underbrace{a_n}_{\text{sol particolare}}.$$

$$\begin{cases} a_0 = 5 \\ a_1 = 14 \\ a_{n+1} = 2^n + \frac{1}{2}a_n + a_{n-1} \end{cases}$$

$$a_n = 2^n$$

① SOSTITUZIONI

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

Pongo $x=0$ $y=0$:

$$f(0) = 2f(0) \Rightarrow f(0)=0$$

Pongo $y=-x$

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

$\Rightarrow$ f è DISPARI (ovvero verifica $f(-x) = -f(x)$)

f è PARI se $f(-x) = f(x)$

Ossia f dispari $\Rightarrow$ $f(0)=0$

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

$$\frac{f(x) - f(y)}{x-y} = 3 \qquad \forall x, y \in \mathbb{R}$$

Sostituisco $y=0$

$$\frac{f(x) - f(0)}{x} = 3 \Rightarrow f(x) = 3x + \underset{\overset{\parallel}{A}}{f(0)}$$

$$= 3x + A$$

Verifica!!! $\dfrac{3x+A-3y-A}{x-y} = 3$ ok.

IMO 2008 - 4

$f: (0,+\infty) \to (0,+\infty)$ t.c.

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

$\forall x,y,z,w$ che verifica $wx = yz$.

① $w = x = y = z = 1$

$$\frac{2f(1)^2}{2f(1)} = 1 \implies f(1)^2 = f(1)$$

$$\implies f(1) = 1$$

② $w = y = z = x$

$$f(x)^2 = f(x^2) \qquad \forall x$$

③ $$\frac{f(w^2)+f(x^2)}{f(y^2)+f(z^2)} = \frac{w^2+x^2}{y^2+z^2}$$ $\forall$.. t.c $wx = yz$

$\overline{w} = w^2$

$$\frac{f(\overline{w})+f(\overline{x})}{f(\overline{y})+f(\overline{z})} = \frac{\overline{w}+\overline{x}}{\overline{y}+\overline{z}}$$

$\forall\ \overline{x}, \overline{y}, \overline{z}, \overline{w}$ $\overline{w}\,\overline{x} = \overline{y}\,\overline{z}$

perchè $\overline{w}$, — sono positivi e quindi si può trovare w t.c. $\overline{w} = w^2$, ...

Sostituisco $\overline{x} = x$ $\overline{w} = x$ $\overline{y} = x^2$ $\overline{z} = 1$

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

Allora $f(x)$ risolve eq di 2° grado!

$$2f(x)(x^2+1) = 2x\left(f(x)^2+1\right)$$

$$2xf(x)^2 - 2(x^2+1)f(x) + 2x = 0$$

$$f(x) = \frac{x^2+1 \pm \sqrt{(x^2+1)^2-4x^2}}{2x} = \begin{cases} 1/x \\ x \end{cases}$$

$$\forall x \quad f(x) = \begin{cases} o & x \\ o & 1/x \end{cases}$$.

Supponiamo che esistano $a, b \neq 1$

$f(a) = a \qquad f(b) = 1/b$

(altrimenti o $f(x) = x \ \forall x$ o $f(x) = \frac{1}{x} \ \forall x$)

$$\frac{f(\bar{w}) + f(\bar{x})}{f(\bar{y}) + f(\bar{z})} = \frac{\bar{w} + \bar{x}}{\bar{y} + \bar{z}} \qquad \forall \bar{x}, \bar{y}, \bar{z}, \bar{w} \quad \bar{w}\bar{x} = \bar{y}\bar{z}$$

Sostituiamo $\bar{w} = a \quad \bar{x} = b \quad \bar{y} = ab \quad \bar{z} = 1$

$$\frac{a + 1/b}{f(ab) + 1} = \frac{a+b}{ab+1}$$

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

$\cancel{a} + 1/b = \cancel{a} + b \Rightarrow b = 1$ Assurdo .

$$\frac{a + 1/b}{\frac{1}{ab} + 1} = \frac{a+b}{ab+1}$$

$$\frac{ab\,(a + 1/b)}{\cancel{ab+1}} = \frac{a+b}{\cancel{ab+1}}$$

$$a + \cancel{1/b} = \cancel{\frac{1}{b}} + \frac{1}{a}$$

$\Rightarrow a = 1$ Assurdo .

Sostituendo, si verifica l'eq .

IMO 2010 - 1

Trovare $f: \mathbb{R} \to \mathbb{R}$ t.c.

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

- Sostituiamo $x = 0$

$$f(0) = f(0) \cdot \lfloor f(y) \rfloor$$

$$\Rightarrow \begin{cases} f(0) = 0 & \text{CASO 1} \\ \lfloor f(y) \rfloor = 1 \quad \forall y & \text{CASO 2} \end{cases}$$

CASO 2: $f(\lfloor x \rfloor y) = f(x) \cdot 1$

Sostituendo $y = 0$, $f(x) = C \in [1, 2)$.

CASO 1: $f(0) = 0$.

Sostituiamo $x = 1$

$$f(y) = f(1) \cdot \lfloor f(y) \rfloor \quad \forall y$$

$$\begin{cases} f(1) = 0 \Rightarrow f(y) = 0 \quad \forall y & \text{CASO 1.1 OK} \\ \lfloor f(y) \rfloor = \dfrac{f(y)}{f(1)} \quad \forall y & \text{CASO 1.2} \end{cases}$$

CASO 1.2:

$$f(\lfloor x \rfloor y) = \frac{f(x) \cdot f(y)}{f(1)} = f(\lfloor y \rfloor x)$$

IDEA: IL RHS È SIMMETRICO
POSSO EGUAGLIARE AL
"SIMMETRICO" DEL LHS ($x \to y$ $y \to x$)

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

Sostituiamo $x = 1/2 \quad y = 2$.

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

$$\Rightarrow f(y) = 0 \quad \forall y.$$

$f(x) = c \in [1,2)$.

$$c = c \cdot \underset{\overset{\shortparallel}{1}}{\lfloor c \rfloor}$$

Verifica ok.

RICONDURSI A CAUCHY.

Risolviamo l'eq di Cauchy:

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

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

Step 1: $f(0) = 0$ e f è dispari

Sostituisco $x = y = 0$ $\quad \cancel{f(0)} = \cancel{f(0)} + f(0)$, cioè $f(0) = 0$

Sostituisco $-x = y$ $\quad 0 = f(x) + f(-x)$

Osserviamo:

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

$f(3) = $ (sost $x=1$ $y=2$) $f(1) + f(2)$

$= 3f(1)$

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

Step 2: $f(mx) = m f(x) \quad \forall m \in \mathbb{N} \quad \forall x \in \mathbb{Q}$ -

$n=1$ è vero. X induzione su n -

$f((n+1)x) \overset{\uparrow}{=} f(x) + f(nx)$

(sostituendo $y = nx$)

$= f(x) + n f(x)$

$= (n+1) f(x)$ ok -

Step 3: $f(n) = a n \quad \forall n \in \mathbb{N}$, a cost fissato -

(discende da ~~Step~~ Step 2 con $x=1$) (a è $f(1)$) -

Step 4: $f\left(\frac{m}{n}\right) = a \frac{m}{n} \quad \forall m, n \in \mathbb{N}$

Sostituiamo $x = \frac{m}{n}$ nello step 2.

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

$\Rightarrow f\left(\frac{m}{n}\right) = \frac{f(m)}{n} \overset{\text{step 3}}{=} a \frac{m}{n}$.

Quindi: $\forall q \in \mathbb{Q} \quad f(q) = aq$ -

Sostituendo, si verifica che le funzioni lineari e nulle in 0 soddisfano e sono quindi le uniche -

Oss: $\mathbb{Q} + \sqrt{2}\mathbb{Q} = \{a + b\sqrt{2}, \text{ con } a, b \in \mathbb{Q}\}$

Allora le f che soddisfano Cauchy sono di più!

$f: a + \sqrt{2} b \longrightarrow a + 7b$ - $\quad x \longrightarrow Ax$ NO

Questa verifica Cauchy -

$a + \sqrt{2} b = a' + \sqrt{2} b' \longrightarrow \begin{matrix} a+7b \\ a'+7b' \end{matrix}$

$\Downarrow$

$a = a'$ e $b = b'$

$a - a' = \sqrt{2}(b - b')$

Se $b - b' \neq 0 \qquad \sqrt{2} = \frac{a-a'}{b-b'} \Rightarrow$ è raz.

$$b=b' \Rightarrow a=a'.$$

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

$$x = a+\sqrt{2}b \qquad y = c+\sqrt{2}d$$

Dobbiamo verificare

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

$$a+c+7(b+d) = a+7b + c+7d$$

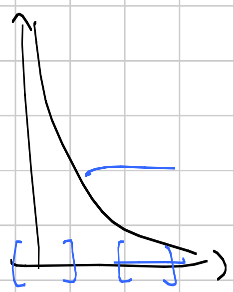
ok.

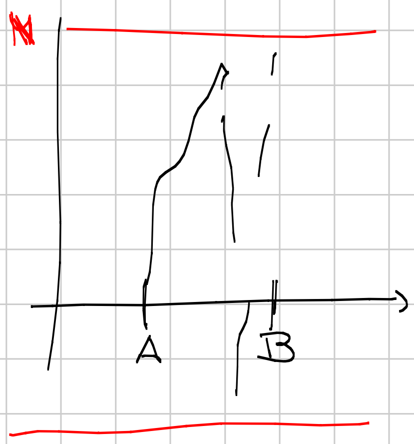
Diventa vero che $f:\mathbb{R}\to\mathbb{R}$ che risolve Cauchy è della forma $f(x)=Ax$ con $A\in\mathbb{R}$ se vale almeno una delle seguenti:

1. f continua
2. f crescente.
3. f localmente lim in un int

$\exists\, [A,B],\ M,N\in\mathbb{R} : \quad M \le f(x) \le N \quad \forall x\in[A,B]$

$f(x)=1/x$





Esempio: $f: \mathbb{Q} \to \mathbb{R}^+$ t.c.

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

Prendiamo il log di entrambi i membri

$$\ln_2 f(x) + \ln_2 f(y) = \ln_2 f(x+y)$$

Chiamiamo $g = \ln \circ f$

$g(x) + g(y) = g(x+y)$

$\Rightarrow$ (Cauchy) $g(x) = Ax$ per qualche $A \in \mathbb{R}$

$g(x) = \ln(f(x))$ $\qquad e^{g(x)} = f(x)$

$\qquad \qquad \qquad \qquad \quad \, \| $

$\qquad \qquad \qquad \qquad e^{Ax}$ $\quad f(x) = 2^{Ax} = e^{\ln 2 \cdot A \cdot x}$

Esempio $f: \mathbb{R} \to \mathbb{R}$ monotona t.c.

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

ES 10 LIBRETTO SENIOR

$f: \mathbb{R} \to \mathbb{R}$ t.c.

$f(x f(x) + f(y)) = f(x)^2 + y \qquad \forall x, y \in \mathbb{R}$ (0)

Sostituiamo $x = 0$

$f(f(y)) = \underbrace{f(0)^2 + y}$ (1) $\to$ è bigettiva

$\Rightarrow f$ è bigettiva.

$\exists\, a \in \mathbb{R}\ !\ \ f(a) = 0$.

Sostituiamo $x = a$.

$f(f(y)) = y$ (2)

Confrontando 1 e 2, $f(0) = 0$.

In particolare per (1) $f(f(y)) = y \quad \forall y$. (3).

$x = f(z)$

$f(f(z) \cdot f(f(z)) + f(y)) = f(f(z))^2 + y$

Usando (3), $f(f(z) z + f(y)) = z^2 + y$ (4)

Uguagliando (0) e (4)

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

$$f(x)^2 = x^2 \implies f(x) = \pm x \quad \forall x \in \mathbb{R}$$

Speriamo che le uniche sol siano
$f(x) = x \ \forall x$ e $f(x) = -x \ \forall x$
(è facile verificare che queste 2 funzionano)

Supponiamo che esistano $a, b \neq 0$ t.c
$f(a) = a \qquad f(b) = -b$.

Poniamo in (0) $x = a \quad y = b$.

$$f(a^2 - b) \stackrel{?}{=} a^2 + b$$

$$f(a^2-b) = \begin{cases} a^2 - b \longrightarrow \cancel{a^2} - b = \cancel{a^2} + b \Rightarrow b = 0 \quad \text{ASSURDO} \\ b - a^2 \longrightarrow \cancel{b} - a^2 = a^2 + \cancel{b} \Rightarrow a = 0 \quad \text{ASSURDO} \end{cases}$$

C1 BASIC (Anér)

Titolo nota 07/09/2010

1) QUANTI SONO?

2) COSA SONO?

$$A = \{a_1, a_2, \dots, a_n\} \qquad |A| = n$$

$$B = \{b_1, \dots, b_m\} \qquad |B| = m$$

$$A \times B = \{(a_i ; b_j) \text{ t.c. } a_i \in A, b_j \in B\}$$

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

$$\text{Th. } n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$$

quanti divisori ha n? $\tau(n)$

Come è fatto un div. di n?

Se $d \mid n$ allora posso scrivere $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$

$0 \leq \beta_i \leq \alpha_i$

$$\underset{\alpha_1+1 \text{ el.}}{\{0, \ldots, \alpha_1\}} \times \underset{\alpha_2+1}{\{0, \ldots \alpha_2\}} \times \ldots \times \underset{\ldots}{\{0, \ldots, \alpha_k\}} =$$

$$= (\alpha_1+1)(\alpha_2+1) \cdot \ldots (\alpha_k+1)$$

---

quante funzioni ci sono da A a B?

quanti elementi ha B^n?

Se ho $f: A \to B$ allora $(f(a_1), f(a_2) \ldots, f(a_n))$ appartiene a B^n. Viceversa se prendo una n-upla $(b_{j_1}, b_{j_2}, \ldots, b_{j_k})$ costruisco $F: A \to B$

$F(a_i) = b_{j_i}$

Le F da A a B m^n

TEST INIZIALE N° 6

$S = \{1, \ldots, 2010\}$ $\mathcal{P}(S) = \{X \text{ t.c. } X \subseteq S\}$

Quante sono le terne $(A, B, C) \in \mathcal{P}(S)^3$

t.c.

i) $|A \cap B| = |B \cap C| = |C \cap A| = 1$

ii) $|A \cap B \cap C| = 0$

Scelgo l'el. che appartiene nel $A \cap B$.
posso in 2010 modi

Posso scegliere i 3 elementi "quasi comuni" in

$2010 \cdot 2009 \cdot 2008$ modi

valendo 4^{2007} funzioni che associano a uno 2007 el. rimasti un insieme tra A, B, C, resto del mondo

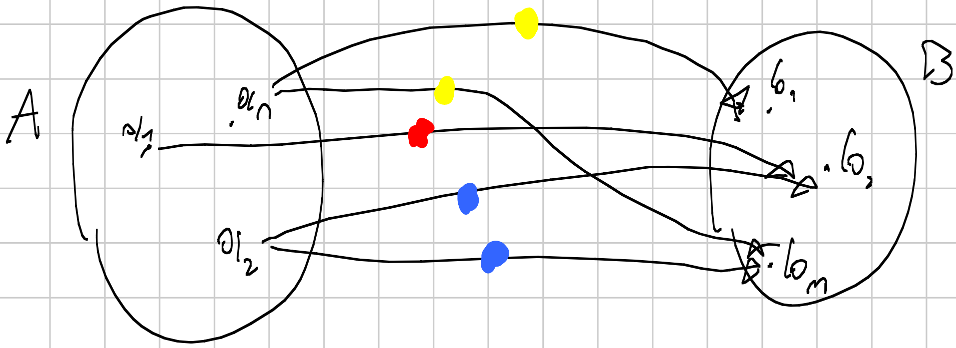
ho in tutto $2010 \cdot 2009 \cdot 2008 \cdot 4^{2007}$ terne.

— o — o —

Quanti sottoinsiemi ha A?
quante sono le funzioni da A a $\{+, -\}$?

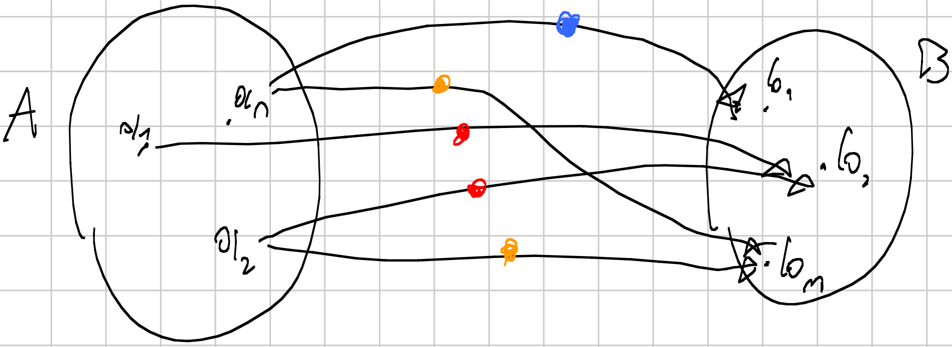
2^n.

DOUBLE COUNTING



Una relazione $R : A \to B$ è un sottoinsieme di $A \times B$.

$$\text{n° di frecce} = \sum_{\substack{\text{colori} \\ \text{iniziali}}} \text{n° di frecce con quel colore}$$



$$\text{n° di frecce} = \sum_{\substack{\text{colori} \\ \text{finali}}} \text{n° di frecce con quel colore}$$

DOUBLE COUNTING (VARIANTE).

1		2							3
				6				3	9
	4					15			19
			2						2
				8					8
								0	0
1	4	2	2	14	0	15	0	3	

Somma$_1$ (row sums)

Somma$_2$ (column sums)

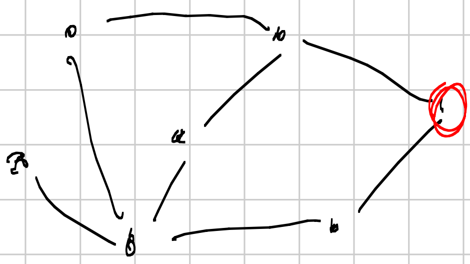
$$\text{Somma}_1 = \text{Somma}_2$$

GRAFI

Un grafo è una coppia di insiemi (V, E).

V contiene un po' di elementi detti VERTICI

E contiene un po' di coppie non ordin. di el. di V detti ARCHI



2 archi dal vertice ○

$$\deg(\circ) = 2$$

LEMMA DELLE STRETTE DI MANO

In un grafo il n° di vertici dispari è pari.

D.C. sulle coppie del tipo (vertice; arco che parte da quel vertice)

1° CONTO (PER VERTICI)

$$\sum_{v \in V} \deg(v)$$

2° conto (PER ARCHI)

sia e il numero di archi

allora ottengo $2e$

$$\sum_{v \in V} \deg(v) = 2e$$

$$\sum_{\substack{v \in V \\ \text{con grado pari}}} \deg(v) + \sum_{\substack{v \in V \\ \text{con grado dispari}}} \deg(v) = 2e$$

$$\sum_{\substack{v \in V \\ \text{con grado dispari}}} \deg(v) \longleftarrow \text{è pari}$$

poiché la somma di un numero dispari di
numeri dispari è dispari, l'ultima sommatoria
deve avere un numero pari di addendi.

— o —

[TEST INIZIALE 7]

Grafo su 2010 vertici, metà hanno grado 4 e metà
grado 5. È possibile? NO
perché ...

— o —

1) Dato un grafo G con almeno un arco
dim. che posso dividere i vertici di G in 2
insiemi V_1 e V_2 tali che la maggior parte
de i archi vadano da una parte all'altra.
v è il numero di vertici
e è il num. di archi

Faccio la media di tutte le bipartizioni
Le bipartizioni sono 2^v, sarà il denominatore

Mi serve $\sum_{\text{bipartizioni}}$ n° di archi da una parte all'altra nella bipartizione.

Sto contando le coppie ordinate del tipo

(bipartizione ; arco che va da una parte all'altra)

ora riconto secondo gli archi.

Prendo un arco $v_i — v_j$

Scelgo in 2 modi se mandare v_i in V_1 o in V_2

v_j va dall'altra parte.

Gli altri $v-2$ vertici fanno come vogliono in 2^{v-2} modi

$2 \cdot 2^{v-2} = 2^{v-1}$ è il n° di bipart. in cui $v_i — v_j$ va da una parte all'altra.

$$\sum_{\text{bipart.}} \text{n° di archi} \ldots = 2^{v-1} \cdot e$$

La media sarà $\dfrac{2^{v-1} \cdot e}{2^v} = \dfrac{e}{2}$

se metto tutti i vertici in V_1 non ho archi che vanno da V_1 a V_2, dunque esiste una bipartizione con più della metà degli archi da V_1 a V_2

Per casa] Dim. che se prendo $r > 0$ allora esistono grafi che comunque bipartiti hanno meno di $\left(\frac{1}{2}+r\right)e$ archi da V_1 a V_2

FATTORIALE]

In quanti modi posso ordinare in fila gli elementi di A? In $n!$ modi

---

Lemma $(n+1)! = (n+1)\, n!$ $\quad \forall n \geq 1$

Prendo A e un elemento esterno t

Scelgo un elemento che sia il più a sinistra.

$$\sum_{x \in A \cup \{t\}} n! = (n+1)\, n!$$

E per induzione (occhio al passo base, banale ma da fare) $n! = \prod_{i=1}^{n} i$

—— . ——

Quante sono le funzioni iniettive da A a B? Sia F il numero

Supponiamo $n \leq m$

D.C. sul numero di ordinamenti di B,

1° conto $m!$

2° conto Scelgo una funzione iniettiva da A a B

ordino così: $f(a_1), f(a_2) \ldots f(a_n)$ e poi gli altri

$(m-n)$ in uno dei $(m-n)!$ modi possibili

$$m! = F \cdot (m-n)! \qquad F = \prod_{i=m-n+1}^{m} i$$

— o — o —

BINOMIALI

Dato un intero p, quanti sono i sottoinsiemi di p elementi contenuti in A?

Sono $\binom{n}{p}$

Se $p < 0$ $\binom{n}{p} = 0$

Se $p > n$ $\binom{n}{p} = 0$

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

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

Ma forse $\binom{n}{p} = \binom{n}{n-p}$ sì

I sottoinsiemi da p sono in biiezione con i complementari, che sono quelli da $n-p$.

Formula di ricorrenza

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

Prendiamo A e aggiungiamo t

Se prendiamo un sott. da $p+1$ tra gli $n+1$, possiamo includere t oppure no.

1° caso $\binom{n}{p}$ scelte

2° caso $\binom{n}{p+1}$ scelte

Salvo casi disperati ($n<0$, $p<0$, $p>n$) vale la seguente formula: $\binom{n}{p} = \frac{n!}{p!\,(n-p)!}$

D. C. sul numero di ordinamenti di A.

1° conto: $n!$

2° conto: Scelgo in $\binom{n}{p}$ modi l'insieme dei primi p, li ordino in $p!$ e ordino gli altri in $(n-p)!$ modi

$$n! = \binom{n}{p} \cdot p! \cdot (n-p)!$$

$\binom{n}{p}$ = quello che deve essere

$p=0$ $\quad p=1$ $\quad p=2$

Somma righe		
1	0 0 1 0 0	← $n=0$ $\quad 2^0$
2	0 1 1 0	← $n=1$ $\quad 2^1$
4	1 2 1 0	← $n=2$ $\quad 2^2$
8	1 3 3 1	
	1 4 6 4 1	
	1 5 10 10 5 1	
	1 6 15 20 15 6 1	

20 è la somma dei ○

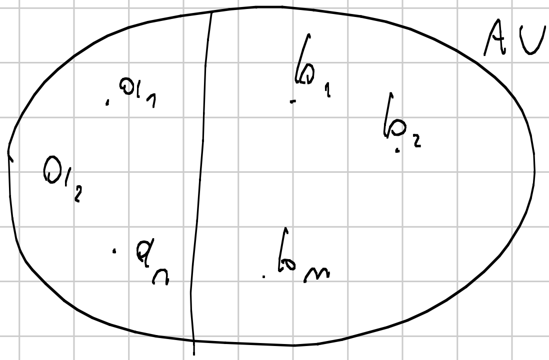
$$\sum_{i=0}^{n} \binom{n}{i} = 2^n \qquad \sum_{i=p}^{q} \binom{i}{p} = \binom{q+1}{p+1}$$

IDENTITÀ DI VAN DER MONDE Dato $k \in \mathbb{N}$

$$\sum_{i=0}^{k} \binom{n}{i}\binom{m}{k-i} = \binom{m+n}{k}$$

A e B sono disgiunti

Prendo $A \cup B$



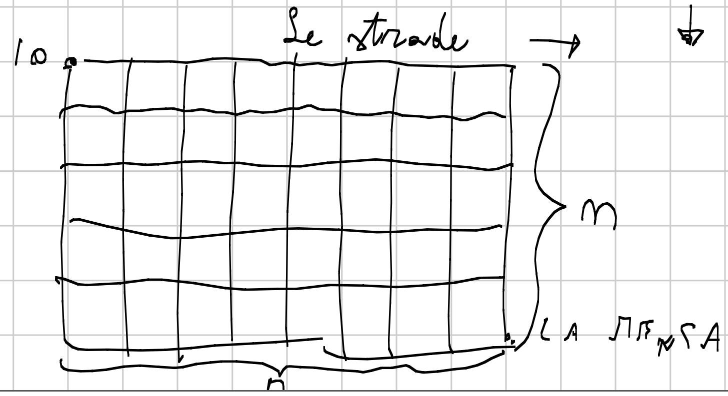
$A \cup B$ ha $m+n$ elementi

Conto i sottoins. di k el. dentro $A \cup B$.

Se ci sono i elementi da A, gli altri $k-i$ vengono da B. Se fisso i, $\binom{n}{i}\binom{m}{k-i}$

$$\sum_{i=0}^{k} \binom{n}{i}\binom{m}{k-i} = \binom{m+n}{k}$$

— o —



In quanti modi posso raggiungere la mensa?

Devo fare n spostam. $\rightarrow$ e m $\downarrow$, in tutto $m+n$

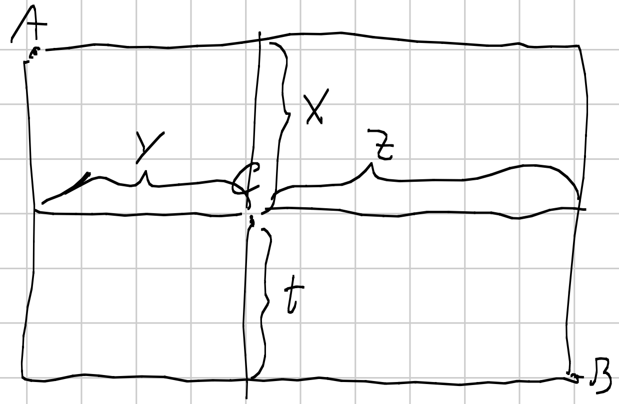
Supponiamo che io debba fare gli spostamenti $s_1, s_2, \dots, s_{m+n}$

Se scelgo n indici e decido che uso gli spostamenti corrispondenti per andare ad est. $\rightarrow$, formo un percorso.

Dunque devo scegliere n elementi fra $m+n$, dunque ho $\binom{m+n}{n}$ possibilità.

TEST INIZIALE 5

Devo andare da A a B senza passare per C. Quanti percorsi?



$$\binom{x+t+y+z}{x+t} - \binom{x+y}{x}\binom{z+t}{t}$$

BINOMIO DI NEWTON

$(x+1)^n$ come si sviluppa?

quanti sono i sottoinsiemi da p elementi di A?

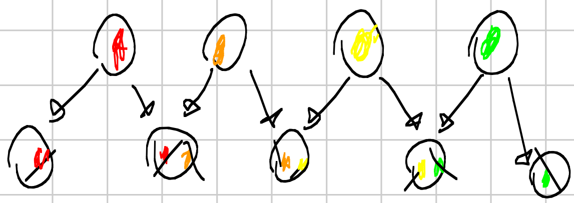
$$\underbrace{(x+1)(x+1)(x+1)\,\dots\,(x+1)}_{n \text{ fattori}}$$

per avere x^p devo scegliere p volte la x e $n-p$ volte l'1

posso farlo in $\binom{n}{p}$ modi

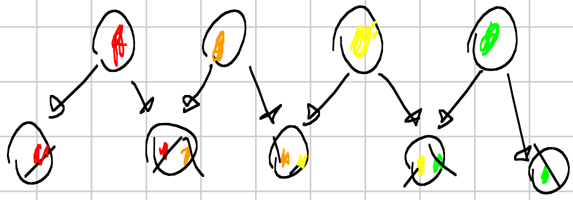
Il polinomio diventa $\sum_{i=0}^{n} \binom{n}{i} x^i = (x+1)^n$

Se $x = -1$ allora $\sum_{i=0}^{n} (-1)^i \binom{n}{i} = 0$



riga $n-1$ esima del triangolo di Tartaglia

$\sum_{i=0}^{k} (-1)^i \binom{n}{i}$ è positiva o negativa? dipende dal segno dell'ultimo termine della somma.



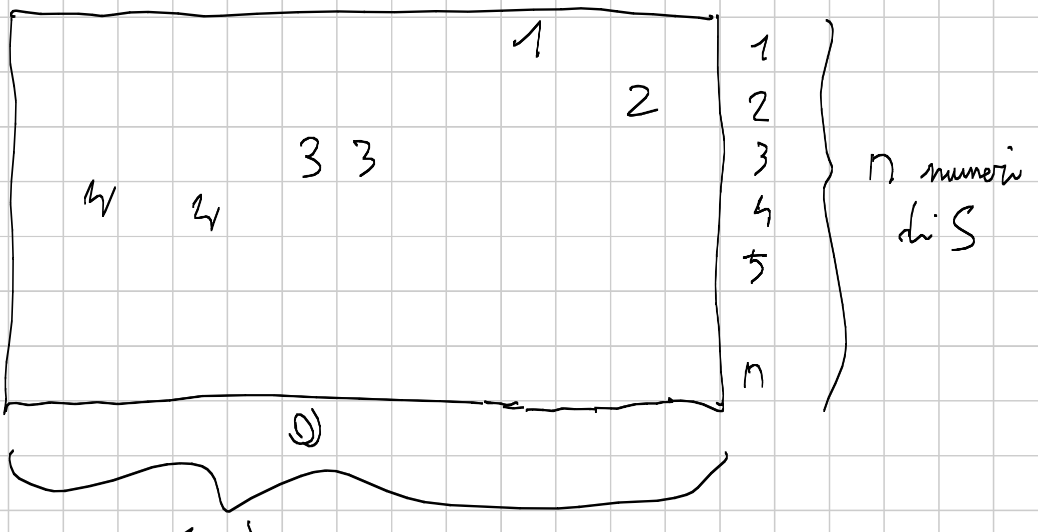
$+ \quad - \quad + \quad -$

rimane $- \bullet < 0$

IMO 1981/2 | Abbiamo S con n elementi $\{1, 2, \dots, n\}$. Prendiamo $1 \le r \le n$, e per ogni sottoinsieme di r elementi di S, consideriamo il minimo elemento del sottoinsieme. Allora la media dei minimi di tutti tali sottoinsiemi è $\frac{n+1}{r+1}$

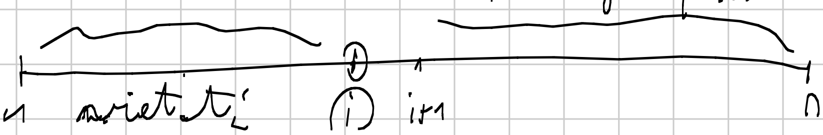
Qual è la somma dei minimi dei vari sottoinsiemi?

D.C.



$\binom{n}{r}$ sott. di S da r elem.

Scelgo un minimo i e conto in quanti sottoinsiemi da r è il minimo



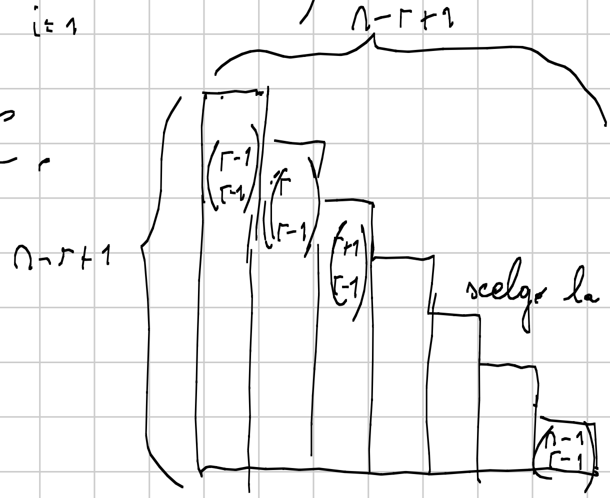
i è minimo in $\binom{n-i}{r-1}$ sottoinsiemi

i può essere minimo se e solo se $i \le n-r+1$

$$\sum_{i=1}^{n-r+1} i \binom{n-i}{r-1}$$

è la somma delle caselle di questa "tabella"

D. C.



scelgo la riga lunga K

la riga lunga k ha somma

$$\sum_{i=1}^{k} \binom{r+i-2}{r-1} = \binom{r+k-1}{r}$$

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

è la somma dei minimi tanto desiderata

$$\frac{\binom{n+1}{r+1}}{\binom{n}{r}} = \frac{n+1}{r+1}$$

IMO 1998/2 Abbiamo a concorrenti $(\alpha_1, \alpha_2, \dots, \alpha_a)$ in una competizione e b giudici $(g_1, g_2, \dots g_b)$

Ogni giudice può bocciare o promuovere ogni concorrente. K è un naturale t.c. comunque si scelgano 2 giudici g_i, g_j, i loro pareri coincidono su al più K concorrenti. In più b è dispari ≥ 3.

Dim che $\dfrac{K}{a} \geq \dfrac{b-1}{2b}$

$n = \dfrac{b-1}{2}$ $\quad b = 2n+1 \quad$ $\dfrac{K}{a} \geq \dfrac{n}{2n+1}$ nuova tesi equivalente

$f(g_i, g_j) =$ n° di concorrenti su cui g_i e g_j concordano

$f(g_i, g_j) \leq K$

$h(\alpha_i) =$ n° di giudici che hanno promosso α_i

D.C. Contiamo le coppie ordinate del tipo

(concorrente ; coppia di giudici che era d'accordo su di lui)
non ordinata

1° conto $\displaystyle \sum_{\alpha_i \text{ concorrente}} \binom{h(\alpha_i)}{2} + \binom{2n+1-h(\alpha_i)}{2}$

2° conto $\displaystyle \sum_{\substack{g_i g_j \\ \text{coppie non ord. di giudici}}} F(g_i, g_j)$

$$\sum_{g_i g_j \text{ coppie}} F(g_i, g_j) = \sum_{\alpha_i \text{ conc.}} \binom{h(\alpha_i)}{2} + \binom{2n+1-h(\alpha_i)}{2}$$

$$\binom{\alpha}{2} = \frac{\alpha(\alpha-1)}{2}$$

$$\sum_{g_i g_j \text{ coppie}} k = \binom{2n+1}{2} k$$

$$\sum_{\alpha_i \text{ conc}} \frac{h(\alpha_i)\left(h(\alpha_i)-1\right) + \left(2n+1-h(\alpha_i)\right)\left(2n+1-h(\alpha_i)-1\right)}{2}$$

$$\frac{1}{2}\sum_{\alpha_i \text{ conc.}} h(\alpha_i)^2 - \cancel{h(\alpha_i)} + \left(2n+1-h(\alpha_i)\right)^2 - \cancel{\left(2n+1-h(\alpha_i)\right)}$$

$$\| $$

$$= \frac{1}{2}\alpha(2n+1) + \frac{1}{2}\sum h(\alpha_i)^2 + (2n+1-h(\alpha_i))^2)$$

$$\geq ?$$

AM-QM sarebbe comoda ma non funzionerà

SMOOTHING: se $x+y=n$ ha somma fissata

allora x^2+y^2 sarà più piccola se avvicino x e y

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

$$= \frac{1}{2}\alpha(2n+1) + \frac{1}{2}\sum_{\alpha_i \text{ conc}} h(\alpha_i)^2 + (2n+1-h(\alpha_i))^2)$$

sostituisco $h(\alpha_i)$ e $2n+1-h(\alpha_i)$ con n e $n+1$

$$\geq$$

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

Abbiamo ottenuto $\binom{2n+1}{2}k \geq \alpha n^2$ da cui la tesi

ANAGRAMMI E ANNESSI & CONNESSI

Quanti anagrammi ha la parola SASSARI?

Ho 7 carte e 4 bambini che si chiamano S, A, R, I. Devo distribuirle, ma S è ingordo e ne vuole 3, A ne vuole 2, R, I una ciascuno. In quanti modi?

Ho un insieme di 7 elementi e devo partizionarlo in 4 insiemi S, A, R, I con risp. 3, 2, 1, 1 elementi. In quanti modi?

$(s+a+r+i)^7$ → qual è il coeff. di $s^3 a^2 r i$?

Sembrano 4, ma il problema è uno solo e la risposta dico che è il COEFFICIENTE MULTINOMIALE $\binom{7}{3,\ 2,\ 1,\ 1}$

Dato $n \in \mathbb{N}$ e $a_1, a_2, \dots, a_k$ interi t.c. $\sum a_i = n$ il coeff. mult. $\binom{n}{a_1,\ a_2,\ \dots,\ a_k}$ è il numero di partizioni di un insieme di n elementi in k sottoinsiemi di cui il primo con a_1 elementi, ..., l'ultimo con a_k elem.

$$\binom{n}{a_1, a_2, \ldots, a_k} = \frac{n!}{a_1! \cdot a_2! \cdot \ldots \cdot a_k!}$$

RICORRENZA

$$\binom{n-1}{a_1-1, a_2, \ldots, a_k} + \binom{n-1}{a_1, a_2-1, a_3, \ldots, a_k} +$$

$$+ \ldots + \binom{n-1}{a_1, a_2, \ldots, a_{k-1}, a_k - 1} =$$

$$= \binom{n}{a_1, a_2, \ldots, a_k}$$

Ho 11 giocatori in una squadra di calcio. Devo scegliere un portiere, 4 dif, 4 centrocampisti e 2 attaccanti. In quanti modi?

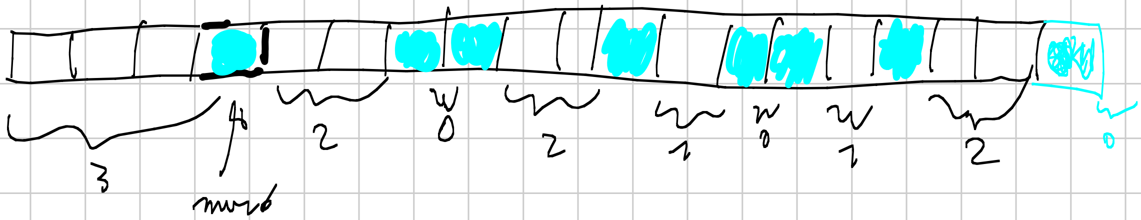
$$\binom{11}{4\ 4\ 2\ 1} = \frac{11!}{4!\,4!\,2\cdot 1} = \frac{11 \cdot \ldots \cdot 5}{4! \cdot 2 \cdot 1}$$

$$= \frac{11 \cdot 10 \cdot 9 \ldots \cdot 5}{16 \cdot 3} = 11 \cdot 10\, 9 \cdot 7 \cdot 5$$

fare il conto

Dati n e k, devo scrivere n come somma di k numeri naturali $a_1, a_2, \ldots, a_k$. In quanti modi posso farlo? ordinati (infatti c'è l'indice)

Data una stringa di $n+k-1$ caselle bianche, ne coloro $k-1$ di turchese. In quanti modi?



Dunque colorando $k-1$ caselle divido le n rimanenti in k gruppi, e viceversa posso decidere prima le lunghezze dei gruppi e poi colorare.

La risposta è $\binom{n+k-1}{k-1}$

PRINCIPIO DI INCLUSIONE-ESCLUSIONE

Se abbiamo un po' di insiemi $A_1, A_2, \ldots, A_n$, allora

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{1\le i\le n} |A_i| - \sum_{1\le i<j\le n} |A_i\cap A_j| + \sum_{1\le i<j<k\le n} |A_i\cap A_j\cap A_k| - \ldots$$

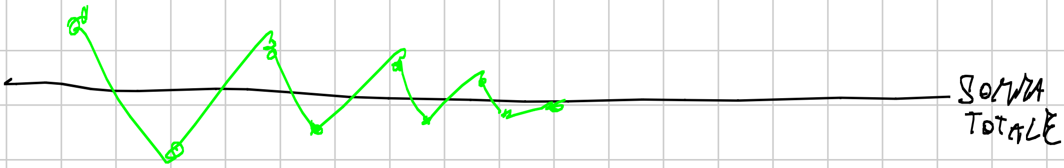
$$+(-1)^{n+1}\left|\bigcap_{i=1}^{n} A_i\right|$$

$$\left|\bigcap_{i=1}^{n} A_i\right| = \sum_{1\le i\le n}|A_i| - \sum|A_i\cup A_j| + \sum|A_i\cup A_j\cup A_k| - \dots$$

vale anche questa

$$+(-1)^{n+1}\left|\bigcup_{i=1}^{n} A_i\right|$$

nella prima, se uno fa la somma parziale questa è $\geq$ o $\leq$ di quella totale a seconda del segno $+$ o $-$ dell'ultimo termine preso.



ESERCIZIO Determinare nella 2ª formula come si comportano le somme parziali

Dim.

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{1\le i\le n}|A_i| - \sum_{1\le i<j\le n}|A_i\cap A_j| + \sum_{1\le i<j<k\le n}|A_i\cap A_j\cap A_k| - \dots$$

$$+(-1)^{n+1}\left|\bigcap_{i=1}^{n} A_i\right|$$

Siano $a_1, a_2, \dots, a_p$ gli elementi di $\bigcup_{i=1}^{n} A_i$

e sia b_i il numero di A_j che contengono a_i

D.C. ogni somma la conto secondo gli a_i

e non secondo gli A_i

TESI

$$p \stackrel{?}{=} \sum_{i=1}^{p} \binom{b_i}{1} - \sum_{i=1}^{p}\binom{b_i}{2} + \sum_{i=1}^{p}\binom{b_i}{3} - \dots + (-1)^{n+1}\sum_{i=1}^{p}\binom{b_i}{n}$$

$b_i \le n \quad \forall i$ perché n sono tutti gli A_j e b_i una parte.

$$\sum_{i=1}^{p}\left(\underbrace{\binom{b_i}{1} - \binom{b_i}{2} + \binom{b_i}{3} - \binom{b_i}{4} + \dots + (-1)^{n+1}\binom{b_i}{n}}_{1 \text{ (perché se togliessi } \binom{b_i}{0} \text{ farebbe } 0)}\right)$$

$$\sum_{i=1}^{p} 1 = p \quad \text{ok}$$

Se mi fermo alla q-esima sommatoria

$$\sum_{i=1}^{p}\left(\binom{b_i}{1}-\binom{b_i}{2}+\dots+(-1)^{q+1}\binom{b_i}{q}\right)$$

$$\|$$

$$\sum_{i=1}^{p}\left(-\binom{b_i}{0}+\binom{b_i}{1}-\binom{b_i}{2}+\dots+(-1)^{q+1}\binom{b_i}{q}+\binom{b_i}{0}\right)$$

$$p+\sum\left(-\binom{b_i}{0}+\binom{b_i}{1}-\dots+(-1)^{q+1}\binom{b_i}{q}\right)$$

se $q+1$ è pari ottengo una somma $\geq p$
″ ″ ″ dispari ″ ″ $\leq p$

È SFORATO IL TEMPO!

PER CASA (O DURANTE IL LUPUS DI NOTTE)

Dimostrare o confutare quanto scritto a pag. 21 del Goblino:

“ $\sum_{i=0}^{m}(-1)^{i}\binom{m}{i}(m-i)^{n}$ è il n° di funzioni suriettive da A a B ”

BST 08 (o 07?) N°1

COMBINATORIA 2

Titolo nota 10/09/2010

Permutazioni

σ biiettive da un insieme in sé

$$S_n = \{\sigma : \{1, \dots n\} \to \{1, \dots, n\}\}$$

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

σ, τ permutazioni $\qquad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$\sigma \circ \tau$ permutazione $\qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

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

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$$

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2)$$

Ciclo

$(a_1\ a_2\ \dots\ a_n)$

$a_1 \mapsto a_2 \mapsto a_3 \mapsto \ a_{n-1} \mapsto a_n \mapsto a_1$

$\exists k$ t.c.

$1 \quad \sigma(1) \quad \sigma(\sigma(1)) = \sigma^2(1) \quad \dots\dots \quad \sigma^k(1) = 1$

Sia k il min t.c. $\sigma^k(1)$ c'era già nella successione

$\sigma^k(1) = \sigma^h(1) \quad h < k \qquad h \neq 0 \to \sigma^{k-1}(1) = \sigma^{(h-1)}(1)$

$\left(1, \sigma(1), \sigma^2(1), \ldots \sigma^{k-1}(1)\right)$

Ogni permutazione è prodotto di cicli disgiunti

Cicli disgiunti commutano

→ scomposizione unica a meno dell'ordine

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

$$= (1\ 2\ 4\ 3)(5\ 6) = (5\ 6)(1\ 2\ 4\ 3)$$

2-cicli: trasposizioni

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

σ^{-1} è una perm t.c. $\sigma^{-1} \circ \sigma = \sigma \circ \sigma^{-1} = id$

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

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

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

$\tau(j) < \tau(i)$

$$\frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)}$$

$j > i \quad \sigma(j) < \sigma(i)$: inversione

il segno conta la parità del numero di inversioni

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

$$(1\ 2\ 3) = (1\ 2)(2\ 3)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

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

$a < b$

$$\dots (a{+}2\ a{+}1)(a{+}1\ a)$$

Segno : $\displaystyle\prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}$

- parità del numero di inversioni
- parità del numero di trasposizioni per una scomposizione di σ in trasposizioni

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Non si può portare a posto con mosse legali

$n!$ permutazioni in S_n

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

$$+ \dots + (-1)^n \binom{n}{n} \underbrace{0!}_{1} = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!}\right)$$

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

Senza punti fissi

$id, \sigma, \sigma^2, \dots$ qual'è il min k intero t.c. $\sigma^k = id$?

$(a_1 \qquad a_k)$

$\sigma(a_1) = a_2 \quad \sigma(a_2) = a_3 \quad \dots$

$\sigma(a_i) = a_{i+1} \pmod k$

$\sigma^2(a_1) = a_3$

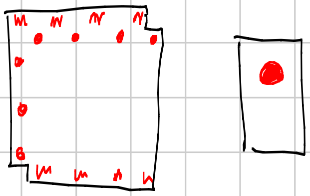
$\sigma^h(a_i) = a_{i+h} \pmod k$

Un ciclo ha per ordine la sua lunghezza

$ord(\sigma) = mcm($ordini dei cicli che la compongono$)$

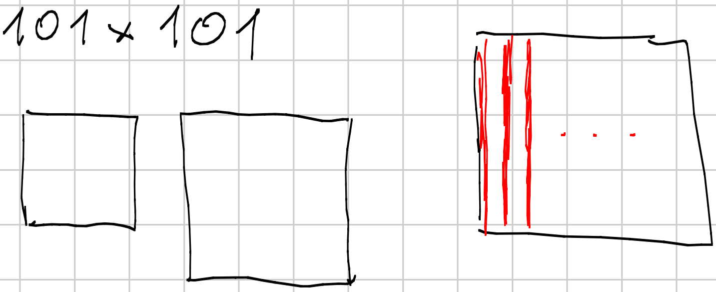
(In)varianti e colorazioni

$2n \times 2n$

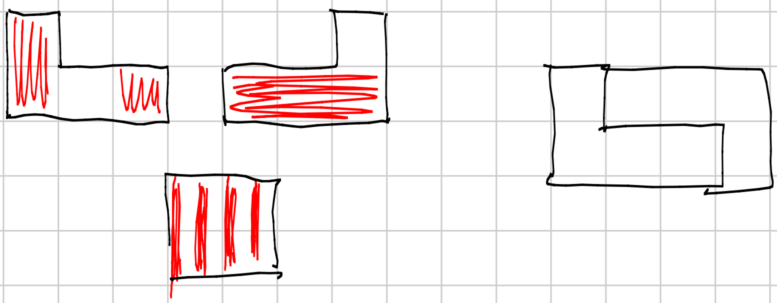


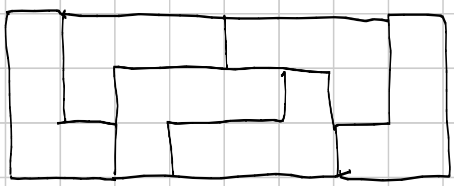
NO

101×101

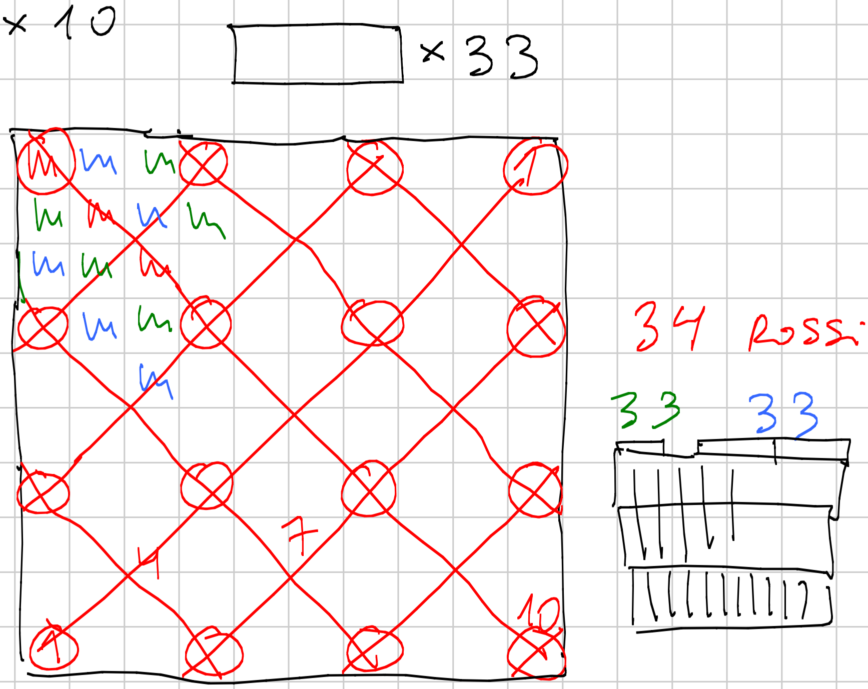


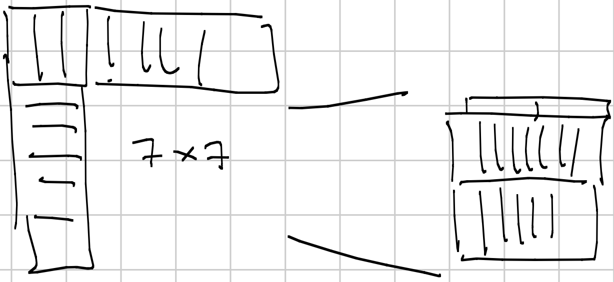
NO

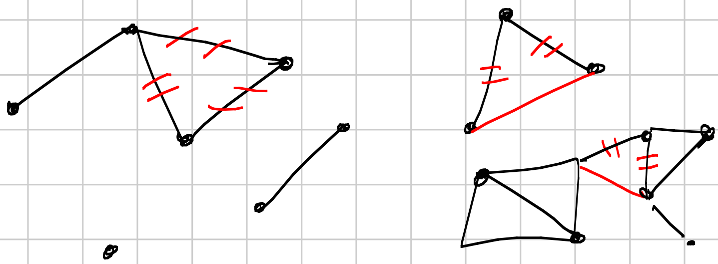




10 × 10







INVARIANTE: PARITÀ ARCHI DA UN VERTICE

„VARIANTE": PARITÀ ARCHI TOTALI

VI È UN NUMERO PARI DI VERTICI „DISPARI"

N° coppie di vertici dispari = archi finali

---

12 gnomi, alcuni amici

amicizia simmetrica

Case ROSA o AZZURRE

Si ridipinge se la maggioranza stretta degli amici di uno gnomo ha casa di colore diverso

Felicità (gnomo) := N° amici con casa dello stesso colore del proprio − N° amici con casa di colore diverso

$$F_{tot} = \sum_{\text{gnomi}} \text{Felicità (gnomo)}$$

+ gnomo cambia di segno la propria +

m amici con stesso colore

n amici con colore diverso

$n > m$

$2(n - m)$

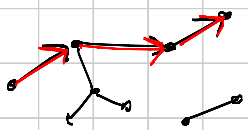
Ogni volta che si ridipinge F_{tot} cresce strettamente

$$F_{tot} \leq \sum_{\text{gnomi}} \text{N° amici (gnomo)}$$ $\Rightarrow$ NON SI RIDIPINGE ALL'INFINITO

Basi per affrontare giochi:
cercare invarianti e partire dalla fine

Grafi

Cammino



Grafo connesso

$\forall$ coppia di vertici $\exists$ cammino che li unisce

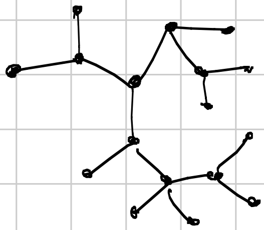
Ciclo: cammino con inizio = fine

Albero : connesso senza cicli

+ arco : acquista un ciclo

– arco : non connesso

Grafo ad albero



$V = e + 1$

edges

– Ci sono foglie : se no un ciclo

Tolgo una foglia e ipotesi induttiva

Base : •

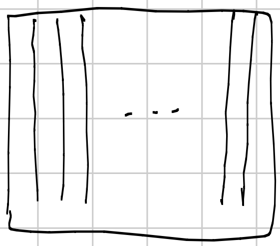
Castello 2010 × 2010, porta tra quadratini adiacenti

Max porte chiuse in modo che si possa arrivare da una stanza all'altra?

$V = 2010 \times 2010$

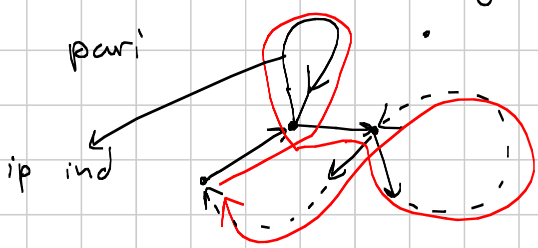
$2010 \times 2010 - 1$ porte aperte

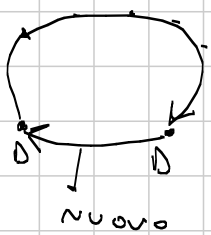
Totale porte $2 \cdot 2009 \cdot 2010$

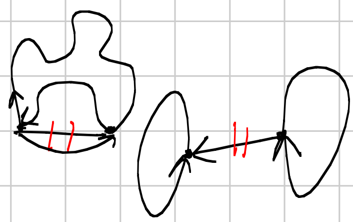


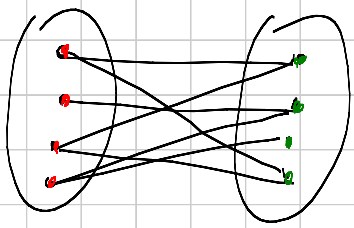
Circuito euleriano: ciclo che percorre tutti gli archi una e una sola volta

Esiste sse ogni vertice ha ordine pari

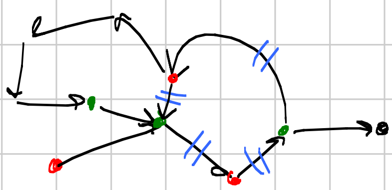


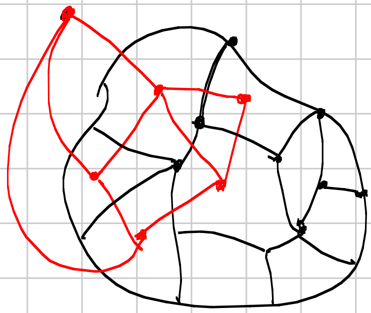






Grafo bipartito sse ogni ciclo ha lunghezza pari

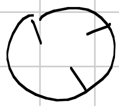


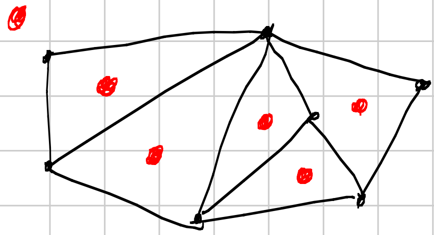


1: ferrovia a ciclo euleriano sui confini

2: Ing e astronauti, mai due professioni uguali da stati confinanti

2 $\Rightarrow$ grafo stati ha cicli pari $\Rightarrow$ 1

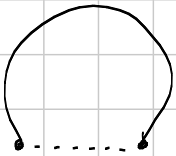




v vertici

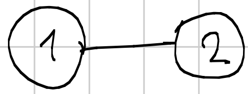
e archi

f



$$f + v = e + 2$$

$$-1 \qquad\qquad -1$$



$$f_1 + v_1 = e_1 + 2$$

$$f_2 + v_2 = e_2 + 2$$

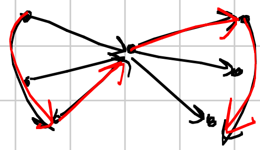
$$f_1 + f_2 \qquad + v_1 + v_2 = e_1 + e_2 + 2 + 2$$

Grafi orientati

ASSURDO

Cammino Hamiltoniano

Completo: ogni coppia di vertici è connessa



G 1 TRIGONOMETRIA Morandin / Pernazza

Titolo nota 06/09/2010

Sintetico ♡

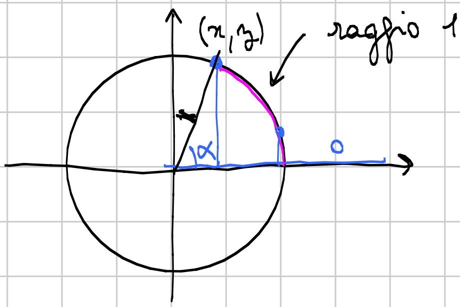
Analitico

Trigonometria — fare i conti = algebrizzare

Vettori

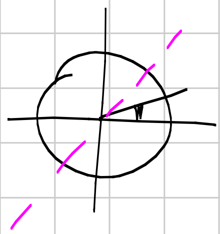
Complessi

GONIOMETRIA



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

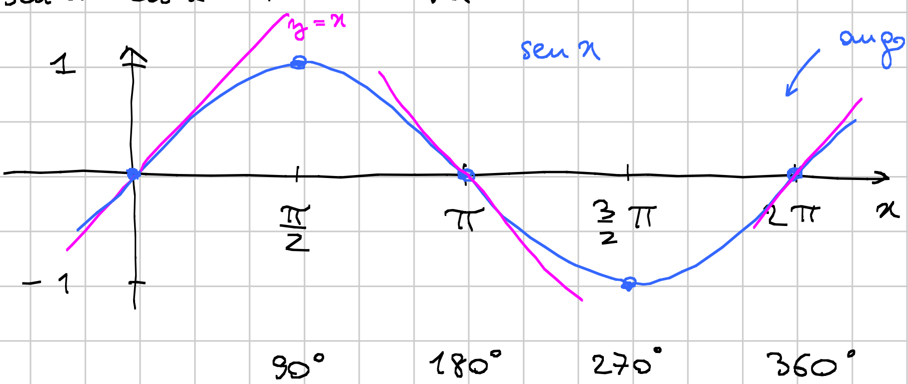
$$\begin{cases} x = \cos\alpha \\ y = \sin\alpha \end{cases}$$



$\operatorname{sen}\alpha, \cos\alpha \in [-1, 1] \quad \forall\alpha$

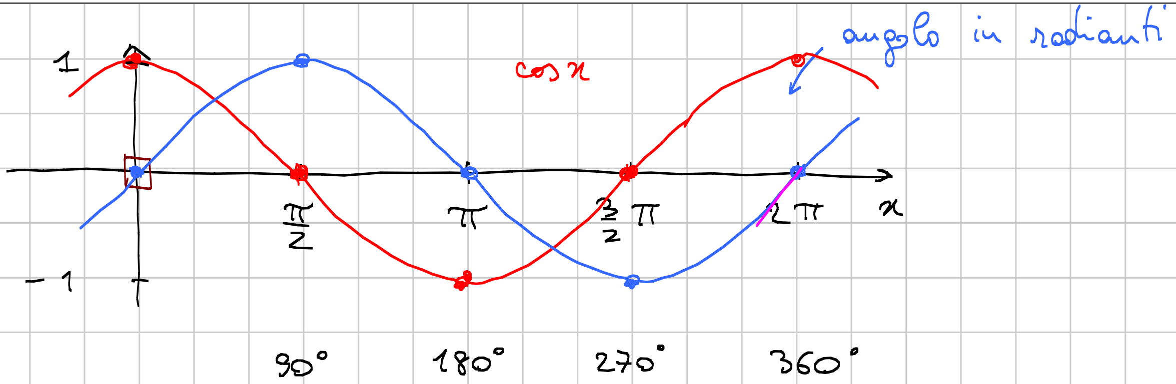
$\operatorname{sen}^2\alpha + \cos^2\alpha = 1 \quad \forall\alpha$

angolo in radianti



$370° \approx 10°$

$\boxed{x \geq 0 \quad \operatorname{sen} x \leq x}$ solo in radianti



- **Periodicità e simmetrie**

  - $\operatorname{sen}(\alpha+2\pi) = \operatorname{sen}\alpha$, $\cos(\alpha+2\pi) = \cos\alpha = \cos(\alpha+2k\pi)$ $\forall k \in \mathbb{Z}$
  - $\cos(\alpha) = \operatorname{sen}\left(\alpha+\frac{\pi}{2}\right)$
  - $\operatorname{sen}(-\alpha) = -\operatorname{sen}\alpha$ (dispari) x^3 $(-x)^3 = -x^3$, $\cos(-\alpha) = \cos\alpha$ (pari) x^8 $(-x)^8 = x^8$
  - $\operatorname{sen}(\pi-\alpha) = \operatorname{sen}\alpha$ angoli supplementari
  - $\cos(\pi-\alpha) = -\cos\alpha$
  - $\operatorname{sen}\left(\frac{\pi}{2}-\alpha\right) = \cos\alpha$ $\cos\left(\frac{\pi}{2}-\alpha\right) = \operatorname{sen}\alpha$

- **Valori speciali**

  $\frac{\sqrt{2}}{2} = \frac{1}{\sqrt{2}}$ $45°$ ...

  $\frac{1}{2}$, $\frac{\sqrt{3}}{2}$ $30°$, $60°$, ...

- **Sviluppo di Taylor**

$$\operatorname{sen} x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots \qquad \forall x$$

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \dots$$

- **Altre funzioni trig:**

$$-\ \operatorname{tg}\alpha := \frac{\operatorname{sen}\alpha}{\cos\alpha} \qquad \cot\alpha := \frac{\cos\alpha}{\operatorname{sen}\alpha}$$

$$1+\operatorname{tg}^2\alpha = \frac{\operatorname{sen}^2\alpha + \cos^2\alpha}{\cos^2\alpha} = \frac{1}{\cos^2\alpha} \qquad \boxed{1+\operatorname{tg}^2\alpha = \frac{1}{\cos^2\alpha}}$$

TRIGONOMETRIA BASE

notazione standard

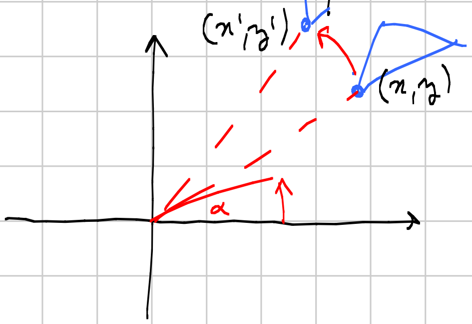
$$\beta = \frac{\pi}{2}$$

$$\boxed{\begin{aligned} c &= b\cos\alpha \\ a &= b\operatorname{sen}\alpha \end{aligned}}$$

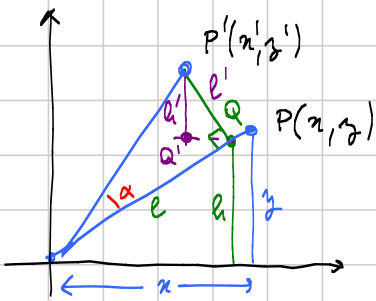
$$\boxed{\operatorname{tg}\alpha = \frac{a}{c}}$$

FORMULE

- **Rotazioni del piano**



$$\boxed{\begin{cases} x' = x\cos\alpha - y\operatorname{sen}\alpha \\ y' = x\operatorname{sen}\alpha + y\cos\alpha \end{cases}}$$



Dim (problemi di config)

$Q = (?, h)$ $\quad l = \overline{OQ}$ $\quad r = \overline{OP}$

$l' = \overline{P'Q}$

$y' = h + h'$

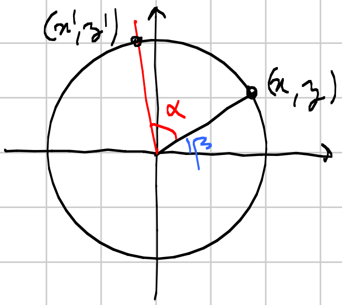
$h : l = y : r \qquad l = r\cos\alpha \qquad h = y\cos\alpha$

$h' : l' = x : r \qquad l' = r\operatorname{sen}\alpha \qquad h' = x\operatorname{sen}\alpha$

$y' = x\operatorname{sen}\alpha + y\cos\alpha$

- Addizione

$$\begin{cases} x' = x\cos\alpha - y\,\mathrm{sen}\,\alpha \\ y' = x\,\mathrm{sen}\,\alpha + y\cos\alpha \end{cases}$$

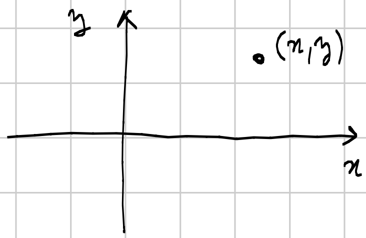


$$(x,y) = (\cos\beta, \mathrm{sen}\,\beta)$$

$$(x',y') = (\cos(\alpha+\beta), \mathrm{sen}(\alpha+\beta))$$

$$\boxed{\begin{aligned} \cos(\alpha+\beta) &= x' = \cos\alpha\cos\beta - \mathrm{sen}\,\alpha\,\mathrm{sen}\,\beta \\ \mathrm{sen}(\alpha+\beta) &= y' = \mathrm{sen}\,\alpha\cos\beta + \mathrm{sen}\,\beta\cos\alpha \\ \mathrm{tg}(\alpha+\beta) &= y'/x' = \frac{\mathrm{tg}\,\alpha + \mathrm{tg}\,\beta}{1 - \mathrm{tg}\,\alpha\,\mathrm{tg}\,\beta} \end{aligned}}$$

- Numeri complessi



piano $\mathbb{R}^2$ $\Rightarrow$ numeri complessi $\mathbb{C}$

i tale che $i^2 = -1$

$$(x,y) \longmapsto x + iy$$

$$(x+iy)(s+it) = xs + ixt + iys + \underset{-1}{i^2}yt = \underbrace{xs - yt}_{\text{“}x\text{”}\ \ x'} + i\underbrace{(xt+ys)}_{\text{“}y\text{”}\ \ y'}$$

$$\begin{cases} x' = xs - yt \\ y' = xt + ys \end{cases}$$

(x,y) e (s,t) sulla circ. goniometrica

$(x,y) = (\cos\alpha, \mathrm{sen}\,\alpha)$ $\quad (s,t) = (\cos\beta, \mathrm{sen}\,\beta)$

$$\begin{aligned}(x',y') &= (\cos\alpha\cos\beta - \mathrm{sen}\,\alpha\,\mathrm{sen}\,\beta, \ \mathrm{sen}\,\beta\cos\alpha + \mathrm{sen}\,\alpha\cos\beta) \\ &= (\cos(\alpha+\beta), \mathrm{sen}(\alpha+\beta))\end{aligned}$$

"Moltiplicare per un complesso che sta sulla circ. goniom. equivale a ruotare"

$$e^{i\alpha} := (\cos\alpha, \mathrm{sen}\,\alpha) =: \cos\alpha + i\,\mathrm{sen}\,\alpha$$
$$e^{i\beta} := (\cos\beta, \mathrm{sen}\,\beta) =: \cos\beta + i\,\mathrm{sen}\,\beta$$

$$e^{i\alpha}e^{i\beta}=(\cos\alpha+i\,\mathrm{sen}\,\alpha)(\cos\beta+i\,\mathrm{sen}\,\beta)=\cos(\alpha+\beta)+i\,\mathrm{sen}(\alpha+\beta)=e^{i(\alpha+\beta)}$$

$$e^{x}=1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\dots$$

$$\cos\alpha=1-\frac{\alpha^2}{2!}+\frac{\alpha^4}{4!}-\dots$$

$$i\,\mathrm{sen}\,\alpha=i\alpha-i\frac{\alpha^3}{3!}+i\frac{\alpha^5}{5!}-\dots$$

$$\cos\alpha+i\,\mathrm{sen}\,\alpha=1+i\alpha-\frac{\alpha^2}{2!}-i\frac{\alpha^3}{3!}+\frac{\alpha^4}{4!}+i\frac{\alpha^5}{5!}-\dots$$

$$e^{i\alpha}=1+i\alpha+\left(-\frac{\alpha^2}{2!}\right)+\left(-\frac{i\alpha^3}{3!}\right)+\frac{\alpha^4}{4!}\dots$$

FORMULE DI DUPLICAZIONE, BISEZIONE, TRIPLICAZIONE...

$$\boxed{\cos 2\alpha=\cos(\alpha+\alpha)=\cos^2\alpha-\mathrm{sen}^2\alpha=2\cos^2\alpha-1=1-2\,\mathrm{sen}^2\alpha}$$

$$\boxed{\mathrm{sen}\,2\alpha=\mathrm{sen}(\alpha+\alpha)=2\,\mathrm{sen}\,\alpha\cos\alpha}$$

$$\mathrm{tg}\,2\alpha=\frac{\mathrm{sen}\,2\alpha}{\cos 2\alpha}=\frac{2\,\mathrm{sen}\,\alpha\cos\alpha}{1-2\,\mathrm{sen}^2\alpha}=\frac{2\,\mathrm{tg}\,\alpha}{\frac{1}{\cos^2\alpha}-2\,\mathrm{tg}^2\alpha}=\boxed{\frac{2\,\mathrm{tg}\,\alpha}{1-\mathrm{tg}^2\alpha}}$$

☆ Dim form somma tg

$$\cos(\alpha+\beta)=x'=\cos\alpha\cos\beta-\mathrm{sen}\,\alpha\,\mathrm{sen}\,\beta$$

$$\mathrm{sen}(\alpha+\beta)=y'=\mathrm{sen}\,\alpha\cos\beta+\mathrm{sen}\,\beta\cos\alpha$$

$$\mathrm{tg}(\alpha+\beta)=\frac{y'}{x'}=\frac{\mathrm{sen}\,\alpha\cos\beta+\mathrm{sen}\,\beta\cos\alpha}{\cos\alpha\cos\beta-\mathrm{sen}\,\alpha\,\mathrm{sen}\,\beta}=\frac{\mathrm{tg}\,\alpha+\mathrm{tg}\,\beta}{1-\mathrm{tg}\,\alpha\,\mathrm{tg}\,\beta}$$

$$\cos 2\alpha=2\cos^2\alpha-1=1-2\,\mathrm{sen}^2\alpha$$

$$\boxed{\cos\alpha=\sqrt{\frac{1+\cos 2\alpha}{2}}}\qquad\boxed{\mathrm{sen}\,\alpha=\sqrt{\frac{1-\cos 2\alpha}{2}}}$$

$$\boxed{\operatorname{tg}\alpha = \sqrt{\frac{1-\cos 2\alpha}{1+\cos 2\alpha}}}$$

$$\cos 3\alpha = \cos(\alpha + 2\alpha) = \cos\alpha\cos 2\alpha - \operatorname{sen}\alpha\operatorname{sen}2\alpha$$
$$= \cos\alpha(\cos^2\alpha - \operatorname{sen}^2\alpha) - \operatorname{sen}\alpha(2\operatorname{sen}\alpha\cos\alpha)$$
$$= \cos\alpha(\cos^2\alpha - 3\operatorname{sen}^2\alpha) = \cos\alpha(4\cos^2\alpha - 3) = 4\cos^3\alpha - 3\cos\alpha$$

$$\boxed{\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha}$$

$\operatorname{sen}3\alpha = ???$

- $\cos(x+y) = \cos x\cos y - \operatorname{sen}x\operatorname{sen}y$
  $\cos(x-y) = \cos x\cos y + \operatorname{sen}x\operatorname{sen}y$

$$\cos x\cos y = \frac{\cos(x+y)+\cos(x-y)}{2}$$

$$\operatorname{sen}x\operatorname{sen}y = -\frac{\cos(x+y)-\cos(x-y)}{2}$$

$$\operatorname{sen}(x+y) = \operatorname{sen}x\cos y + \cos x\operatorname{sen}y$$
$$\operatorname{sen}(x-y) = \operatorname{sen}x\cos y - \cos x\operatorname{sen}y$$

$$\boxed{\begin{aligned}
\operatorname{sen}x\cos y &= \frac{\operatorname{sen}(x+y)+\operatorname{sen}(x-y)}{2}\\
\cos x\operatorname{sen}y &= \frac{\operatorname{sen}(x+y)-\operatorname{sen}(x-y)}{2}\\
\cos x\cos y &= \frac{\cos(x+y)+\cos(x-y)}{2}\\
\operatorname{sen}x\operatorname{sen}y &= -\frac{\cos(x+y)-\cos(x-y)}{2}
\end{aligned}}$$

"cento rose sono belle"

Scrittura parametrica

$7\cos\alpha - 8\,\mathrm{sen}\,\alpha = 1 \qquad \alpha = ?$

$7\cos\alpha - 8\sqrt{1-\cos^2\alpha} = 1$

$8\sqrt{1-\cos^2\alpha} = 7\cos\alpha - 1$

?? $64(1-\cos^2\alpha) = 49\cos^2\alpha - 14\cos\alpha + 1$

... eq II grado in $\cos\alpha$

$$\boxed{t := \mathrm{tg}\frac{\alpha}{2} \qquad \cos\alpha = \frac{1-t^2}{1+t^2} \qquad \mathrm{sen}\,\alpha = \frac{2t}{1+t^2}}$$

$\cos 2\beta = 1 - 2\,\mathrm{sen}^2\beta = \cos^2\beta\left(\frac{1}{\cos^2\beta} - 2\,\mathrm{tg}^2\beta\right) = \cos^2\beta\left(1-\mathrm{tg}^2\beta\right)$

$= \frac{1-\mathrm{tg}^2\beta}{1/\cos^2\beta} = \frac{1-\mathrm{tg}^2\beta}{1+\mathrm{tg}^2\beta} = \frac{1-\mathrm{tg}^2\alpha/2}{1+\mathrm{tg}^2\alpha/2} = \frac{1-t^2}{1+t^2} \qquad \beta = \frac{\alpha}{2}$

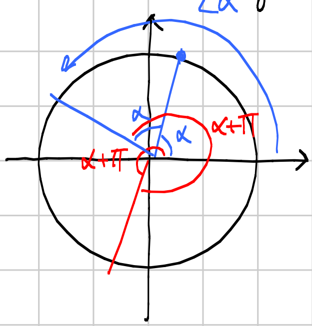
$\mathrm{sen}\,2\beta = 2\,\mathrm{sen}\beta\cos\beta = \cos^2\beta\,(2\,\mathrm{tg}\,\beta) = \frac{2\,\mathrm{tg}\,\beta}{1+\mathrm{tg}^2\beta} = \frac{2\,\mathrm{tg}\,\alpha/2}{1+\mathrm{tg}^2\alpha/2} = \frac{2t}{1+t^2}$

$7\cos\alpha - 8\,\mathrm{sen}\,\alpha = 1$

$7\,\frac{1-t^2}{1+t^2} - 8\,\frac{2t}{1+t^2} = 1 \qquad 7(1-t^2) - 8\cdot 2t = 1+t^2$

eq II grado più semplice

★ Occhio a dividere gli angoli



$2\alpha = \alpha+\alpha = (\alpha+\pi)+(\alpha+\pi) = 2(\alpha+\pi)$

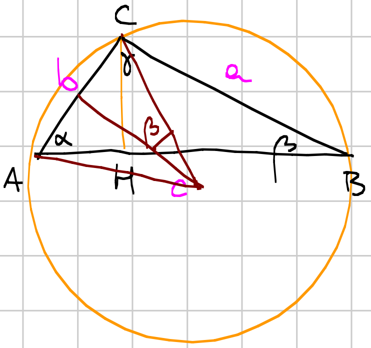
$\frac{\beta}{2}$ non è univoco

$3\alpha = \alpha+\alpha+\alpha = (\alpha+\frac{2}{3}\pi)\cdot 3 = (\alpha+\frac{4}{3}\pi)\cdot 3$

$\mathrm{tg}\,\alpha = \mathrm{tg}\,\alpha+\pi \quad \Rightarrow \mathrm{tg}\,\frac{\beta}{2}$ è univoco $\Rightarrow \beta$ è univoco

TRIGONOMETRIA

- teor dei seni



$b \operatorname{sen} \alpha = HC = a \operatorname{sen} \beta$

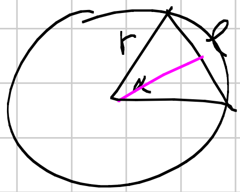
$$\boxed{\frac{a}{\operatorname{sen}\alpha} = \frac{b}{\operatorname{sen}\beta} = \frac{c}{\operatorname{sen}\gamma} = 2R}$$

$$\frac{b}{2} = R \operatorname{sen} \beta$$

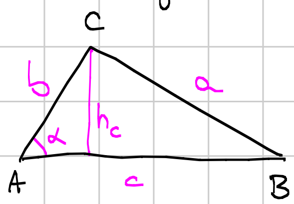
★ es: determinare il minimo perimetro di un triangolo con lati tutti interi e due angoli uno il doppio dell'altro
(Bocconi 2010 finale)

- lunghezza corda

$$\ell = 2 \cdot r \operatorname{sen} \frac{\alpha}{2}$$



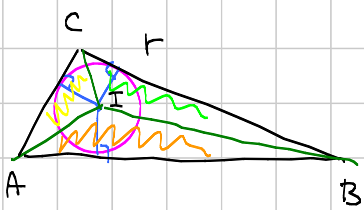
- area trigonometrica



$$\frac{c \cdot h_c}{2} = \boxed{\frac{c \cdot b \operatorname{sen}\alpha}{2} = [ABC]}$$

$$[ABC] = \frac{c \cdot b \cdot \frac{a}{2R}}{2} = \frac{abc}{4R}$$

$$\boxed{R = \frac{abc}{4[ABC]}}$$



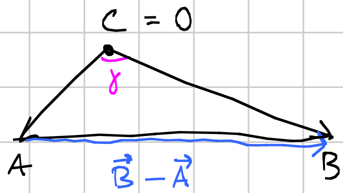
semiperimetro

$$[ABC] = \frac{c \cdot r}{2} + \frac{a \cdot r}{2} + \frac{b \cdot r}{2} = r \cdot p$$

$$\boxed{r = \frac{[ABC]}{p}}$$

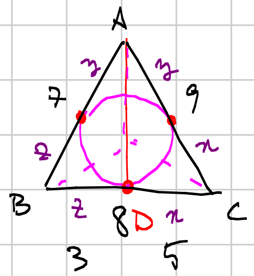
- Carnot (o coseno)

$$\boxed{c^2 = a^2 + b^2 - 2ab\cos\gamma}$$

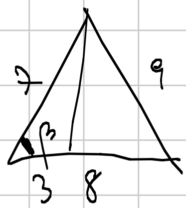


$$c^2 = \overline{AB}^2 = |\vec{B}-\vec{A}|^2 = (\vec{B}-\vec{A})\cdot(\vec{B}-\vec{A})$$
$$= \vec{B}\cdot\vec{B} + \vec{A}\cdot\vec{A} - \vec{B}\cdot\vec{A} - \vec{A}\cdot\vec{B}$$
$$= |\vec{B}|^2 + |\vec{A}|^2 - 2\vec{A}\cdot\vec{B} = a^2 + b^2 - 2ab\cos\gamma$$

✱ Es 9 :



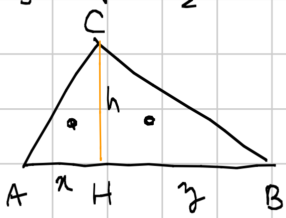
$$\underbrace{x+y+z}_{7} = 12$$
$$x = 5$$



$$9^2 = 7^2 + 8^2 - 2\cdot 7\cdot 8\cdot\cos\beta$$
$$AD^2 = 3^2 + 7^2 - 2\cdot 3\cdot 7\cdot\cos\beta$$
$$AD^2 = 46$$

- Formula di Erone

$$[ABC] = \sqrt{\frac{a+b+c}{2}\cdot\frac{a+b-c}{2}\cdot\frac{a-b+c}{2}\cdot\frac{-a+b+c}{2}}$$



$$h^2 + x^2 = b^2$$
$$h^2 + y^2 = a^2$$
$$y^2 - x^2 = a^2 - b^2$$
$$(y-x)\,c = a^2 - b^2$$
$$\begin{cases} y - x = \dfrac{a^2-b^2}{c} \\ y + x = c \end{cases}$$

$$y = \frac{a^2 - b^2 + c^2}{2c}$$

$$h^2 = a^2 - y^2 = \frac{4a^2c^2 - (a^2-b^2+c^2)^2}{4c^2}$$

$$[ABC] = \frac{ch}{2} = \frac{\sqrt{4a^2c^2 - (a^2-b^2+c^2)^2}}{4}$$

$$4a^2c^2 - a^4 - b^4 - c^4 + 2a^2b^2 + 2b^2c^2 - 2a^2c^2 = \sum_{cyc} a^2b^2 - \sum_{cyc} a^4$$

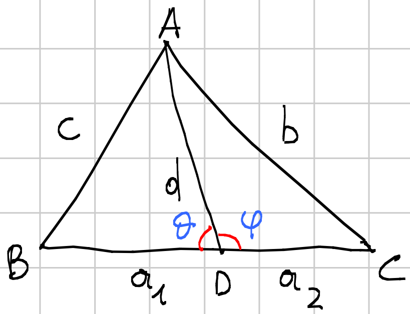
$$[ABC] = \frac{\sqrt{\sum_{cyc} a^2b^2 - \sum_{cyc} a^4}}{4}$$

$((a+b)^2 - c^2)(c^2 - (a-b)^2)$ sviluppo e viene ...

★ α, β, γ angoli di un triangolo

$$\operatorname{tg}\alpha + \operatorname{tg}\beta + \operatorname{tg}\gamma = \operatorname{tg}\alpha \operatorname{tg}\beta \operatorname{tg}\gamma$$

Teorema di Stewart



$$a(a_1a_2 + d^2) = a_1b^2 + a_2c^2$$

$$\cos\vartheta = \frac{a_1^2 + d^2 - c^2}{2a_1d} \qquad \cos\varphi = \frac{a_2^2 + d^2 - b^2}{2a_2d}$$

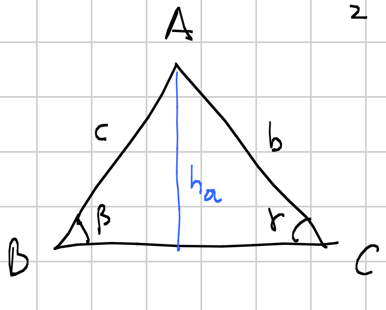
$$a_2(a_1^2 + d^2 - c^2) + a_1(a_2^2 + d^2 - b^2) = 0$$

$$a_1a_2(a_1 + a_2) + (a_1 + a_2)d^2 = a_2c^2 + a_1b^2$$

$$a(a_1a_2 + d^2) = a_2c^2 + a_1b^2$$

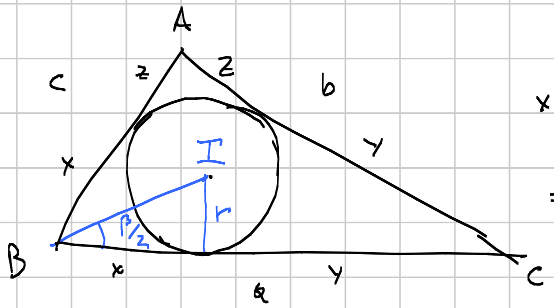
$$a_1 = a_2 = \frac{a}{2} \qquad \cancel{a}\left(\frac{a}{2}\cdot\frac{a}{2}+d^2\right) = \frac{\cancel{a}}{2}\left(c^2+b^2\right)$$

$$d^2 = \frac{b^2}{2}+\frac{c^2}{2}-\frac{a^2}{4} \qquad d = \sqrt{\frac{2b^2+2c^2-a^2}{4}} = m_a$$

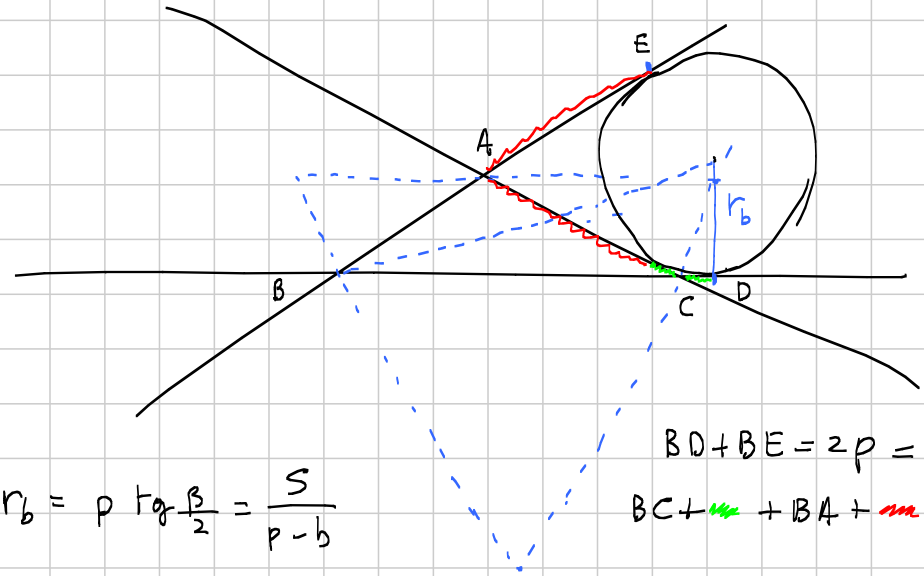


$$h_a = \frac{2S}{a} = c\,\mathrm{sen}\,\beta = b\,\mathrm{sen}\,\gamma = \frac{2}{a}\sqrt{p(p-a)(p-b)(p-c)}$$

$$r = \frac{S}{p} = (p-a)\,\mathrm{tg}\frac{\alpha}{2} = (p-b)\,\mathrm{tg}\frac{\beta}{2} = (p-c)\,\mathrm{tg}\frac{\gamma}{2}$$



$$x = \frac{a+c-b}{2} = \frac{a+c+b-2b}{2} = p-b$$



$$BD + BE = 2p = BC + + BA + $$

$$r_b = p\,\mathrm{tg}\frac{\beta}{2} = \frac{S}{p-b}$$

$$S = \sqrt{r\cdot r_a\cdot r_b\cdot r_c}$$

$$\frac{1}{r} = \frac{1}{r_a}+\frac{1}{r_b}+\frac{1}{r_c}$$

$$\frac{p}{S} = \frac{p-a}{S}+\frac{p-b}{S}+\frac{p-c}{S}$$

$$r_a + r_b + r_c - r = 4R$$

d_a bisettrice di α $\qquad a_1 : b = a_2 : c$

$$d_a = \frac{2bc}{b+c} \cos\frac{\alpha}{2} = \sqrt{bc - a_1 a_2} = \qquad a_1 : b = a : (b+c)$$

$$= \sqrt{bc\left(1 - \frac{a^2}{(b+c)^2}\right)}$$

$$\cos\alpha = \frac{b^2+c^2-a^2}{2bc} = \frac{b^2+c^2-2bc+2bc-a^2}{2bc} =$$

$$= \frac{2bc + (b-c)^2 - a^2}{2bc} = \frac{2bc + (b-c-a)(b-c+a)}{2bc} =$$

$2p - 2c$

$$= \frac{bc - 2(p-b)(p-c)}{bc} = 1 - 2\frac{(p-b)(p-c)}{bc}$$

$$\cos\alpha = 1 - 2\operatorname{sen}^2\frac{\alpha}{2}$$

$$\operatorname{sen}^2\frac{\alpha}{2} = \frac{(p-b)(p-c)}{bc}$$

Formula di Briggs

$$\boxed{\operatorname{sen}\frac{\alpha}{2} = \sqrt{\frac{(p-b)(p-c)}{bc}}}$$

$$\cos\frac{\alpha}{2} = \sqrt{\frac{bc-(p-b)(p-c)}{bc}} = \sqrt{\frac{p(p-a)}{bc}}$$

$$S = \frac{1}{2} bc \operatorname{sen}\alpha = \sqrt{p(p-a)(p-b)(p-c)} =$$

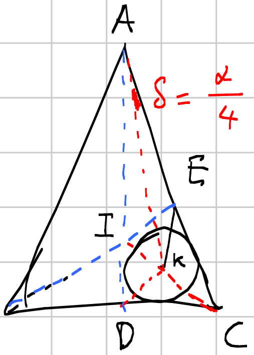
$$\operatorname{sen}\alpha = 2\sqrt{\frac{p(p-a)}{bc} \; \frac{(p-b)(p-c)}{bc}}$$

IMO 4/2009

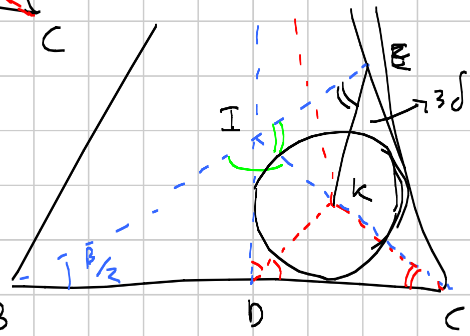
$AB = AC$

$B\hat{E}K = 45°$

Quali valori può assumere $B\hat{A}C$?



CKI allineati.



$$\frac{\beta}{2} = \frac{180-\alpha}{4} = 45-\delta$$

$$C\hat{D}K = 45°$$

$$B\hat{E}C = 180 - 3\frac{\beta}{2} = 45 + 3\delta$$

$$\beta = 90 - \frac{\alpha}{2}$$

$$\frac{IK}{KC} = \frac{ID}{DC} = tg(45-\delta)$$

Teorema dei seni su IEK $\quad \frac{IK}{KE} = \frac{sen\,45}{sen\,E\hat{I}K} =$

$$\frac{sen\,45}{sen\,\beta} = \frac{sen\,45}{sen(90-2\delta)} = \frac{sen\,45}{cos\,2\delta}$$

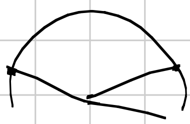
Teorema dei seni su EKC $\quad \frac{KC}{KE} = \frac{sen\,3\delta}{sen(45-\delta)}$

$$\frac{IK}{KC} = \frac{\frac{IK}{KE}}{\frac{KC}{KE}} = \frac{\frac{sen\,45}{cos\,2\delta}}{\frac{sen\,3\delta}{\cancel{sen(45-\delta)}}} = \frac{\cancel{sen(45-\delta)}}{cos(45-\delta)}$$

$$sen\,45 \cdot cos(45-\delta) = cos\,2\delta\; sen\,3\delta$$

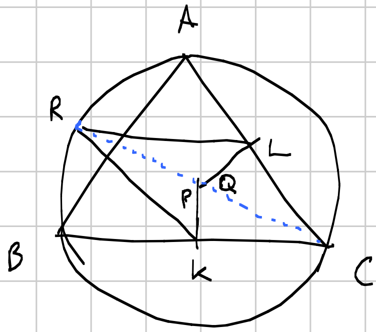
$$\frac{sen(90-\delta) + \cancel{sen\,\delta}}{\cancel{2}} = \frac{sen\,5\delta + \cancel{sen\,\delta}}{\cancel{2}}$$

$$\delta = 15° + \cancel{k30°} \qquad \delta = 22{,}5°$$



IMO
4/2007

$\alpha = 60^\circ$ $\alpha = 90^\circ$



Area RPK = Area RQL

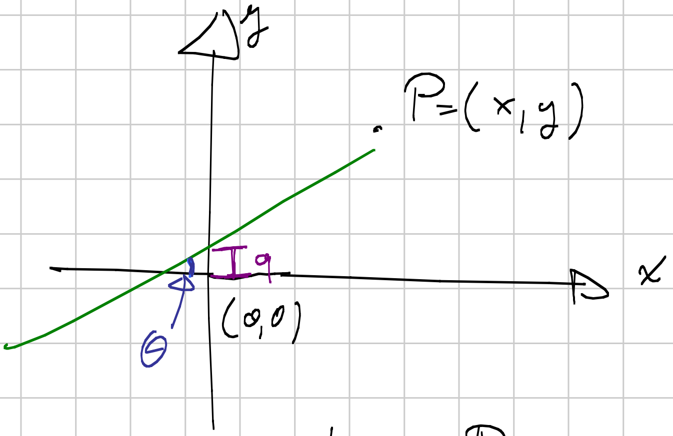
G2 - Metodi algebrici - Basic

Titolo nota 08/09/2010

1 - Coordinate cartesiane

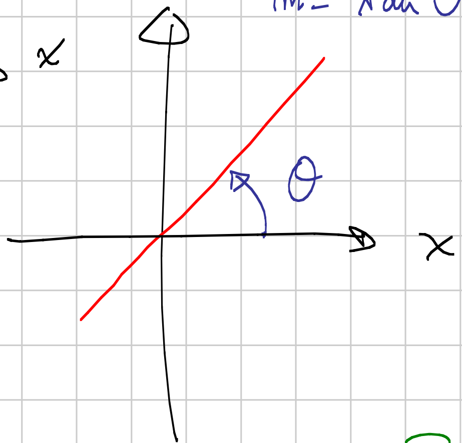
2 - Vettori

3 - Complessi



$$y = mx + q$$

$$m = \tan\theta$$

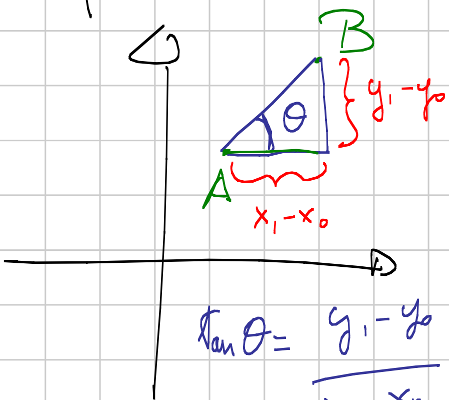


$a, b, c \in \mathbb{R}$

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

$A = (x_0, y_0)$ $B = (x_1, y_1)$

$$y = \frac{y_0 - y_1}{x_0 - x_1}(x - x_1) + y_1$$



$$\tan\theta = \frac{y_1 - y_0}{x_1 - x_0}$$

Oss: $p(x,y)=0 \qquad \deg p = 3$

$$p(x,y) = (x^2+1)\,y \quad \leftarrow$$

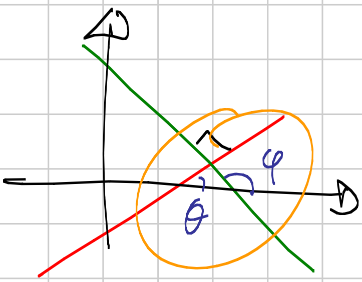
$$p(x,y)=0 \iff (x^2+1)\,y=0 \iff y=0$$

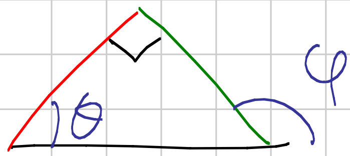
$$p(x,y) = y^2 + 2xy + x^2 = (x+y)^2$$

$y = mx + q \qquad mn = -1 \iff$ perpendicolari

$y = nx + r \qquad m = \tan\theta$

$n = \tan\varphi$



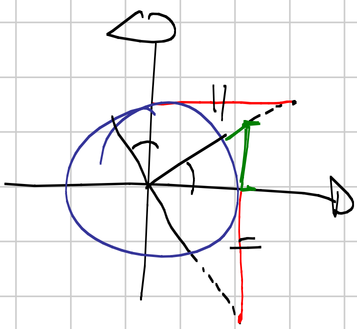


$$\varphi = \frac{\pi}{2} + \theta$$

$$\tan\varphi = -\cot\theta = -\frac{1}{\operatorname{tg}\theta}$$

$$\tan\varphi \cdot \tan\theta = -1$$

$$n \cdot m = -1$$



parallele $\iff m = n$

C'è una distanza

$$d(A,B) = \sqrt{(x_0-x_1)^2+(y_0-y_1)^2}$$

- bisettrice: bisett. dell'angolo tra r, s

$$\mathcal{L} = \{ P : d(P,r) = d(P,s) \}$$

- circonferenza: $\mathcal{C} = \{ P : d(P,O) = r \}$

$$(x-x_0)^2 + (y-y_0)^2 = r^2$$

- asse di un segmento

$$\mathcal{L} = \{ P : d(P,A) = d(P,B) \}$$

$$\sqrt{(x-x_0)^2+(y-y_0)^2} = \sqrt{(x-x_1)^2+(y-y_1)^2}$$

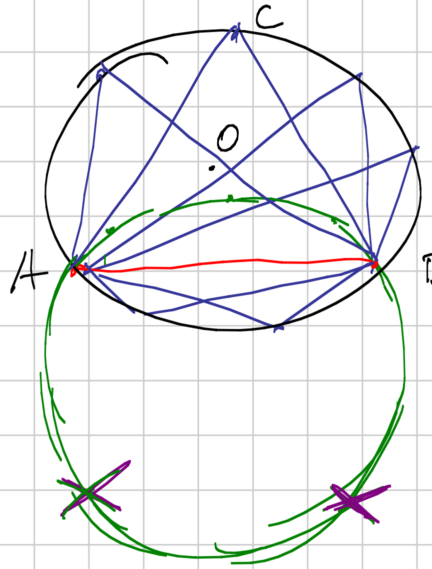
$$(x-x_0)^2+(y-y_0)^2 = (x-x_1)^2+(y-y_1)^2$$

$$\cancel{x^2}+x_0^2-2xx_0+\cancel{y^2}+y_0^2-2yy_0 = \cancel{x^2}+x_1^2-2xx_1+\cancel{y^2}+y_1^2-2yy_1$$

$$\boxed{2x(x_1-x_0)+2y(y_1-y_0)+x_0^2-x_1^2+y_0^2-y_1^2=0}$$

pt. medio di $AB = \left(\frac{x_0+x_1}{2}, \frac{y_0+y_1}{2}\right)$

Es:

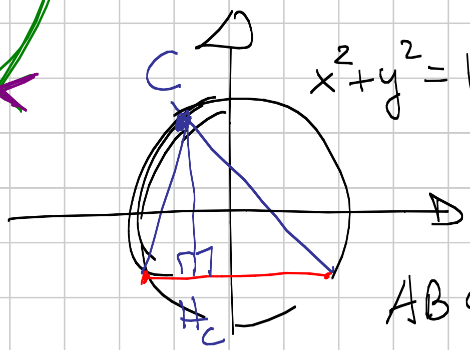


1- Origine in O

2- Origine in A, B

3 - Origine nel pt. medio di AB

$\boxed{\text{Scegliamo 1}}$



$x^2+y^2=1$

$AB \subset \{y=k\}$

$-1<k\leq 0$

Calcolo A, B

$$\begin{cases} y=k \\ x^2+y^2=1 \end{cases} \qquad x^2+k^2=1$$

$$x^2=1-k^2 \longrightarrow x=\pm\sqrt{1-k^2}$$

$A(\sqrt{1-k^2}, k) \qquad B(-\sqrt{1-k^2}, k) \qquad C=(x_0, y_0)$

Dobbiamo trovare H

Altezza da C: $x=x_0$

Lato AC: $y=\underbrace{\frac{k-y_0}{\sqrt{1-k^2}-x_0}}_{=m}(x-x_0)+y_0$

$$-\frac{1}{m}=-\frac{\sqrt{1-k^2}-x_0}{k-y_0}=\frac{\sqrt{1-k^2}-x_0}{y_0-k}$$

Altezza da B: $y=\frac{\sqrt{1-k^2}-x_0}{y_0-k}\left(x+\sqrt{1-k^2}\right)+k$

$H=$ alt. da C $\cap$ alt da B

$$H = \begin{cases} x = x_0 \\ y = \dfrac{\sqrt{1-k^2} - x_0}{y_0 - k}\left(x + \sqrt{1-k^2}\right) + k \end{cases}$$

$$y = \frac{\sqrt{1-k^2} - x_0}{y_0 - k}\left(x_0 + \sqrt{1-k^2}\right) + k =$$

$$= \frac{1-k^2-x_0^2 + ky_0 - k^2}{y_0 - k}$$

$$x = x_0 \qquad H = \left(x_0, \frac{1-2k^2-x_0^2+ky_0}{y_0-k}\right)$$

$$C \in \Gamma \Rightarrow x_0^2 + y_0^2 = 1 \qquad x_0^2 = 1 - y_0^2$$

$$H = \left(x_0, \frac{\cancel{1}-2k^2-\cancel{1}+y_0^2+ky_0}{y_0-k}\right) =$$

$$= \left(x_0, \frac{y_0^2-k^2-k^2+ky_0}{y_0-k}\right) =$$

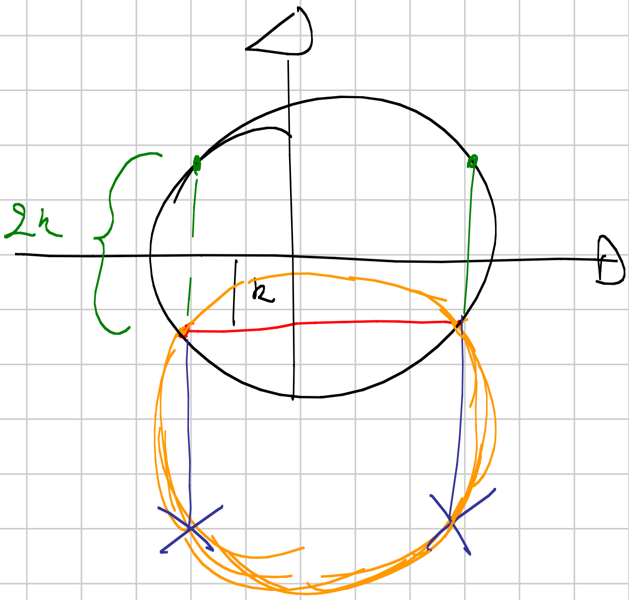
$$= \left(x_0, y_0+k+k\right) = \left(x_0, y_0+2k\right)$$

$y_0 + k + k$

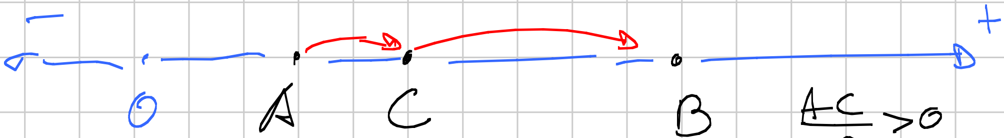
$x_0 + \sqrt{1-k^2} - \sqrt{1-k^2}$

$$\underset{(x_0,y_0)}{C} \in \Gamma \dashrightarrow H = (x_0, y_0+2k)$$

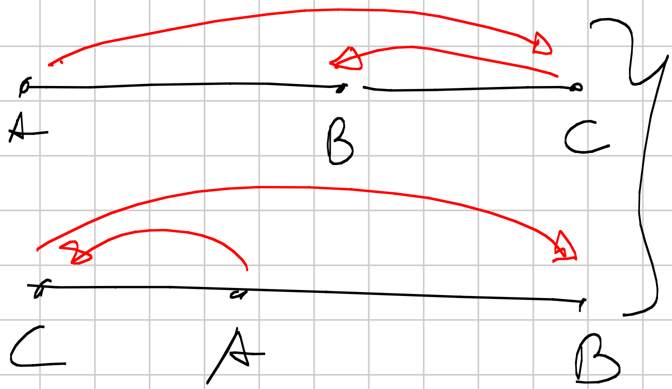
$$f(x,y) = (x, y+2k)$$



Rapporti: A, B, C allineati $\frac{AC}{CB}$



$\frac{AC}{CB} > 0$

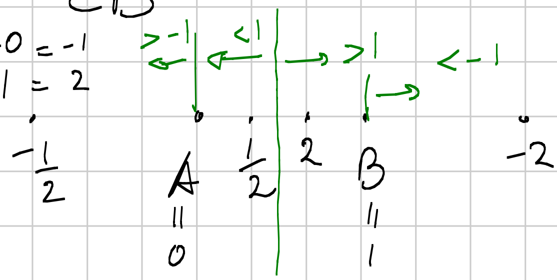


$\frac{AC}{CB} < 0$

Es: $\frac{AC}{CB} = 2, \frac{1}{2}, -2, -\frac{1}{2}$

$AC = -1-0 = -1$

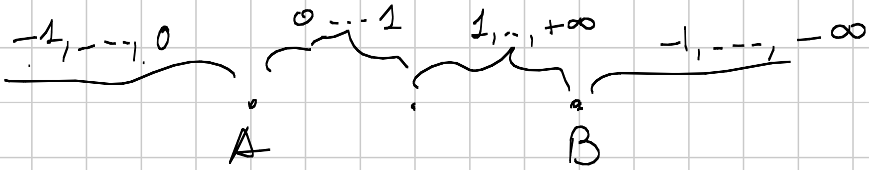
$CB = 1+1 = 2$

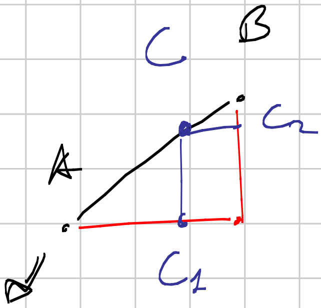


$AC = 2-0$

$CB = 1-2$

$= -2$





Es: $A(x_0, y_0)$ $B(x_1, y_1)$

Voglio C t.c. $\dfrac{AC}{CB} = \lambda$

mi riduco a 1 coordinata

A	B	C
$x_0,$	x_1	x t.c.

$$\frac{AC}{CB} = \frac{x - x_0}{x_1 - x} = \lambda$$

$$x - x_0 = \lambda x_1 - \lambda x$$

$$x = \frac{\lambda x_1 + x_0}{1 + \lambda} =$$

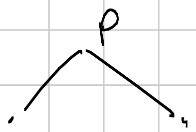
$$= \frac{1}{1+\lambda} x_0 + \frac{\lambda}{1+\lambda} x_1$$

$$\underbrace{\frac{1}{1+\lambda} + \frac{\lambda}{1+\lambda}}_{= 1}$$

$$C = \left(\frac{x_0}{1+\lambda} + \frac{\lambda x_1}{1+\lambda}, \frac{y_0}{1+\lambda} + \frac{\lambda y_1}{1+\lambda} \right)$$

Es: $\mathcal{L} = \{ d(P, A) = k \cdot d(P, B) \}$ $\qquad k \in \mathbb{R}^+ - \{0, 1\}$

$k > 0$
$k \neq 1$.



$PA = k \cdot PB$

$A = (x_0, y_0)$ $\qquad B = (x_1, y_1)$

Sol:
$$\sqrt{(x-x_0)^2 + (y-y_0)^2} = k \cdot \sqrt{(x-x_1)^2 + (y-y_1)^2}$$

$$(x-x_0)^2 + (y-y_0)^2 = k^2 \left[(x-x_1)^2 + (y-y_1)^2 \right]$$

$$x^2(1-k^2) + y^2(1-k^2) - 2x(x_0 - k^2 x_1) - 2y(y_0 - k^2 y_1) +$$
$$+ x_0^2 + y_0^2 - k^2 x_1^2 - k^2 y_1^2 = 0$$

$$x^2+y^2-2x\boxed{\frac{x_0-k^2x_1}{1-k^2}}-2y\boxed{\frac{y_0-k^2y_1}{1-k^2}}+\frac{x_0^2-k^2x_1^2}{1-k^2}+\frac{y_0^2-k^2y_1^2}{1-k^2}=0$$

$$\| $$

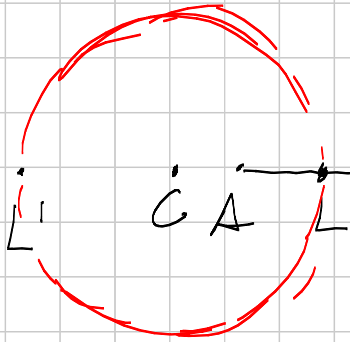
$$\frac{x_0}{1+(-k^2)}+\frac{(-k^2)\,x_1}{1+(-k^2)}=\frac{x_0}{1+\lambda}+\frac{\lambda x_1}{1+\lambda}$$

$\Rightarrow$ il centro divide AB in rapporto $-k^2$

$\|$

C

$$\frac{AC}{CB}=-k^2$$

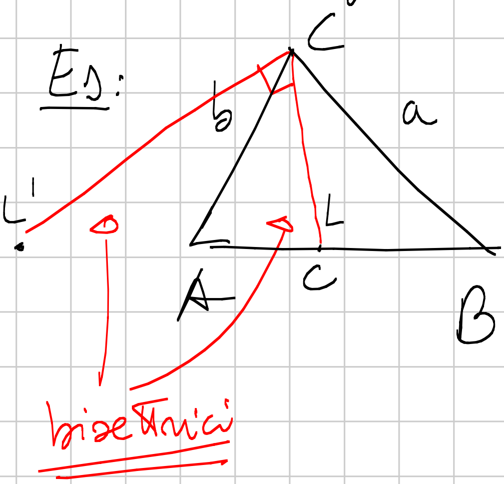


$$\frac{AL}{LB}=k \Rightarrow L,L'\in\mathcal{L}$$

$$\frac{AL'}{L'B}=-k$$

$\mathcal{L}$ si chiama Cfr. di Apollonio del seg. AB con parametro k.

Es:



$$\mathcal{L}=\left\{P:\ PA=\frac{b}{a}\cdot PB\right\}$$

1) $C\in\mathcal{L}$

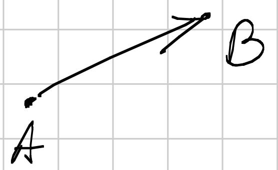
2) $L,L'\in\mathcal{L}$ $\quad \frac{AL}{LB}=\frac{b}{a}$

$$\frac{AL'}{L'B}=-\frac{b}{a}$$

——— ooo ———

Un vettore è una cosa che si somma e si sottrae, si allunga e si accorcia.

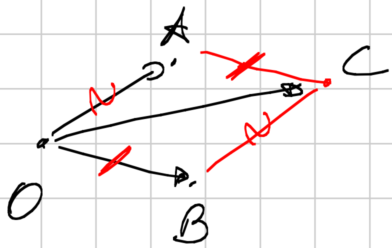
Un vettore è una freccia: un punto di applicazione (origine), una lunghezza, una direzione, un verso.



$\overrightarrow{AB}$

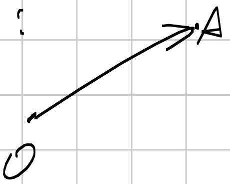
$\vec{A} = \overrightarrow{OA}$ se ho fissato prima O come origine.

<u>Somma</u>:



$\vec{A} + \vec{B} = \vec{C}$

<u>Allungamento</u>/<u>Accorciamento</u>:



$k \in \mathbb{R}$

$k \cdot \vec{A} = \vec{B}$

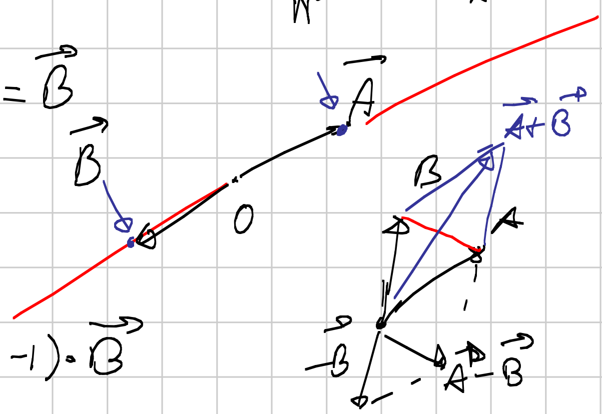
t.c. i) $\overline{OB} = |k| \cdot \overline{OA}$

ii) O, A, B sono allineati

iii) se $k > 0$ $\vec{B}$ ha lo stesso verso di $\vec{A}$

se $k < 0$ $\vec{B}$ ha verso opposto ad $\vec{A}$

<u>Es</u>: $-\vec{A} = (-1) \cdot \vec{A} = \vec{B}$



Es: $\vec{A} - \vec{B} = \vec{A} + (-1) \cdot \vec{B}$

Notazione: $\|\vec{A}\| = OA$ $\qquad \|\cdot\| =$ norma

$|\vec{A}| = OA$ $\qquad$ la lunghezza del vettore

Es: $\|k\cdot\vec{A}\| = |k|\cdot\|\vec{A}\|$

Es: $\mathcal{L} = \{ k\cdot\vec{A} ;\ k\in\mathbb{R} \}$ = retta per A e O =

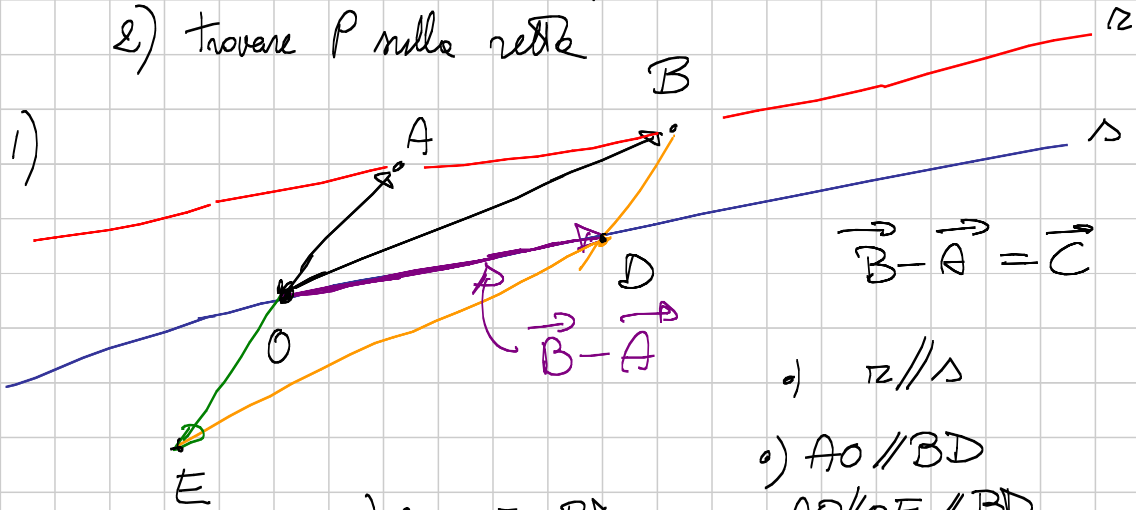
= direzione di $\vec{A}$

Es: P t.c. $\dfrac{AP}{PB} = \lambda$

1) descrivere la retta per A, B

2) trovare P sulla retta

1)



$\vec{B}-\vec{A} = \vec{C}$

•) $r /\!/ s$

•) $AO /\!/ BD$

$AO /\!/ OE /\!/ BD$ $\Leftarrow$ $OEDB$ parall.

•) $AO = OE = BD$

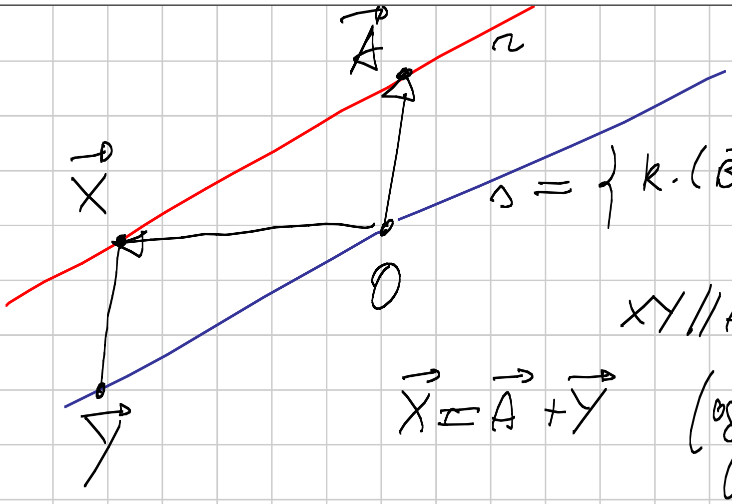
$\Downarrow$

$AODB$ parall.

$\Rightarrow D\in s$ $\Rightarrow$ s è la direzione di $\vec{B}-\vec{A}$

$(D=C)$

$s = \{ k\cdot(\vec{B}-\vec{A}) \mid k\in\mathbb{R} \}$



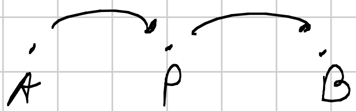
$$s = \{ k\cdot(\vec{B}-\vec{A}) \mid k \in \mathbb{R} \}$$

$XY \parallel AO$

$\vec{X} = \vec{A} + \vec{Y}$ (ogni punto di r è la somma di $\vec{A}$ e di un ~~vettore~~ su s)

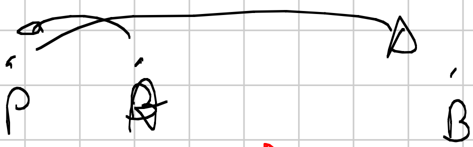
$$r = \{ k\cdot(\vec{B}-\vec{A}) + \vec{A} \mid k \in \mathbb{R} \}$$

2) $\dfrac{AP}{PB} = \lambda$ $\qquad \lambda > 0$



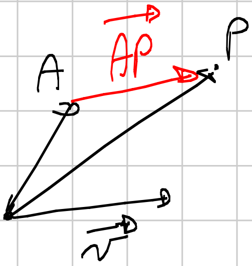
$\Downarrow$

$\vec{AP} = \lambda \cdot \vec{PB}$



$\vec{P} - \vec{A} = \vec{v}$

$\vec{P} = \vec{OP}$, $\vec{A} = \vec{OA}$



$\|\vec{v}\| = \|\vec{AP}\|$

$\vec{v} \parallel \vec{AP}$

hanno lo stesso verso.

$\vec{AP} = \lambda\cdot\vec{PB} \qquad \vec{P}-\vec{A} = \lambda(\vec{B}-\vec{P})$

$$\vec{P} = k\cdot(\vec{B}-\vec{A}) + \vec{A}$$

$$k\cdot(\vec{B}-\vec{A}) \cancel{+\vec{A}} \cancel{-\vec{A}} = \lambda\vec{B} - \lambda k(\vec{B}-\vec{A}) - \lambda\vec{A}$$

$$k(\vec{B}-\vec{A}+\lambda\vec{B}-\lambda\vec{A})=\lambda\vec{B}-\lambda\vec{A}$$

$$k(\lambda+1)(\vec{B}-\vec{A})=\lambda(\vec{B}-\vec{A})$$

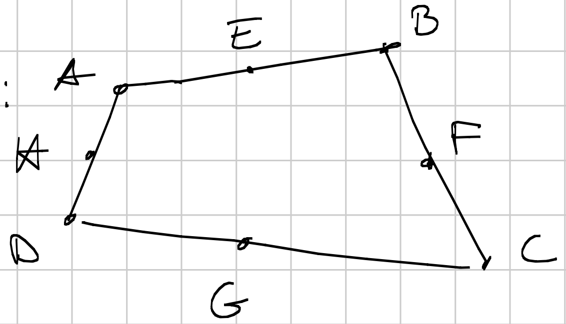
$$k(\lambda+1)=\lambda \qquad k=\frac{\lambda}{\lambda+1}$$

$$\vec{P}=\frac{\lambda}{\lambda+1}(\vec{B}-\vec{A})+\vec{A}=\frac{\lambda}{\lambda+1}\vec{B}+\frac{1}{\lambda+1}\vec{A}$$

Es: $\vec{A},\vec{B}$ $\quad M$ pt. medio $\quad \frac{AM}{MB}=1$

$$\vec{M}=\frac{\vec{A}+\vec{B}}{2}$$

Es:



$$\vec{E}=\frac{\vec{A}+\vec{B}}{2}$$
$$\vec{F}=\frac{\vec{B}+\vec{C}}{2}$$
$$\vec{G}=\frac{\vec{C}+\vec{D}}{2}$$
$$\vec{H}=\frac{\vec{D}+\vec{A}}{2}$$

pt. medio di $EG=\frac{\vec{A}+\vec{B}+\vec{C}+\vec{D}}{4}$

pt. medio di $FH=\frac{\vec{A}+\vec{B}+\vec{C}+\vec{D}}{4}$

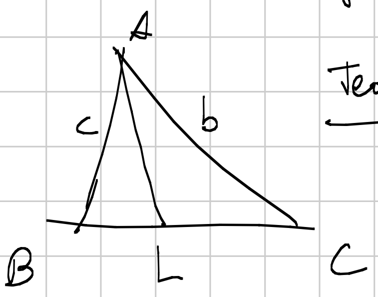
pt. medio di $AC=\frac{\vec{A}+\vec{C}}{2}$ $\qquad$ pt. medio di $BD=\frac{\vec{B}+\vec{D}}{2}$

$\quad\ \ \| \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \|$

$\quad\ M \qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad N$

pt. medio di $MN=\frac{\vec{A}+\vec{B}+\vec{C}+\vec{D}}{4}$

Es: $\overset{\Delta}{ABC}$ triangolo AL bisettrice

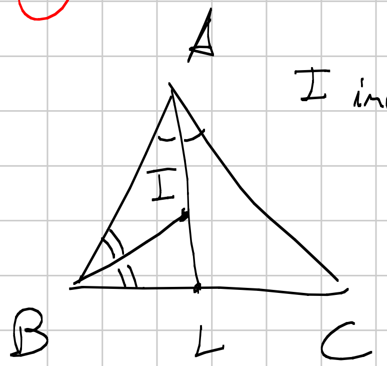


Teo bisett.: $\dfrac{BL}{LC} = \dfrac{AB}{AC} = \dfrac{c}{b}$

$$\vec{L} = \frac{\frac{c}{b}\cdot\vec{C} + \vec{B}}{1 + \frac{c}{b}} = \frac{c\cdot\vec{C} + b\cdot\vec{B}}{b+c}$$

$$\frac{BL}{LC} = k \implies \vec{L} = \frac{k\cdot\vec{C} + \vec{B}}{1+k}$$

Es:



I incentro teo bisett $\Rightarrow \dfrac{AI}{IL} = \dfrac{AB}{BL} = \dfrac{c}{BL}$

$$\|\vec{L} - \vec{B}\| = \left\| \frac{c\vec{C} + b\vec{B}}{c+b} - \vec{B} \right\| =$$

$$= \left\| \frac{c\vec{C} - c\vec{B}}{c+b} \right\| =$$

$$= \frac{c}{c+b}\|\vec{C} - \vec{B}\| = \frac{ac}{c+b}$$

$$\frac{AI}{IL} = \frac{\cancel{c}}{\frac{a\cancel{c}}{c+b}} = \frac{c+b}{a}$$

$$\vec{I} = \frac{\frac{c+b}{a}\vec{L} + \vec{A}}{1 + \frac{c+b}{a}} = \frac{(c+b)\vec{L} + a\vec{A}}{a+b+c} =$$

$$= \frac{\frac{c\vec{C} + b\vec{B}}{c+b}\cdot(c+b) + a\vec{A}}{a+b+c} = \frac{a\vec{A} + b\vec{B} + c\vec{C}}{a+b+c}$$

Es: G = baricentro $\overset{\Delta}{ABC}$ triangolo M pt medio di BC

$$\vec{M} = \frac{\vec{B} + \vec{C}}{2} \qquad \frac{AG}{GM} = 2$$

$$\vec{G} = \frac{2\vec{M} + \vec{A}}{3} = \frac{\cancel{2}\frac{\vec{B}+\vec{C}}{\cancel{2}} + \vec{A}}{3} = \frac{\vec{A}+\vec{B}+\vec{C}}{3}.$$

Es: centro della cf. di Apollonio nel Tri $\overset{\Delta}{ABC}$ sul lato AB

$$N_1 \text{ t.c. } \frac{AN_1}{N_1B} = -k^2 = -\left(\frac{AC}{CB}\right)^2 = -\frac{b^2}{a^2}$$

$$\vec{N}_1 = \frac{\vec{B}\left(-\frac{b^2}{a^2}\right) + \vec{A}}{1 - \frac{b^2}{a^2}} = \frac{a^2\vec{A} - b^2\vec{B}}{a^2 - b^2}$$

$$BC \ni \vec{N}_2 = \frac{b^2\vec{B} - c^2\vec{C}}{b^2 - c^2} \qquad \underset{AC}{\underset{\uparrow}{N_3}} = \frac{c^2\vec{C} - a^2\vec{A}}{c^2 - a^2}$$

$$\vec{N}_1 - \vec{N}_2 = \left(a^2b^2\vec{A} - a^2c^2\vec{A} - b^4\vec{B} + b^2c^2\vec{B} + a^2b^2\vec{B} - b^4\vec{B}\right.$$
$$\left. - a^2c^2\vec{C} + b^2c^2\vec{C}\right) \cdot \frac{1}{(b^2-c^2)(a^2-b^2)} =$$

$$= \frac{1}{(\ )(\ )}\left(\vec{A}(a^2b^2 - a^2c^2) + \vec{B}(a^2b^2 + b^2c^2 - 2b^4) + \right.$$
$$\left. + \vec{C}(-a^2c^2 + b^2c^2)\right) =$$

$$= \frac{1}{(\ )(\ )}\left(a^2\vec{A}(b^2-c^2) + b^2\vec{B}(a^2+c^2-2b^2) + c^2\vec{C}(-a^2+b^2)\right)$$

Es: (noioso) trovare k t.c. $k(\vec{N}_1 - \vec{N}_2) + \vec{N}_1 = \vec{N}_3$.

Prodotto scalare: è un coso che mangia due vettori e sputa un numero. (Tra vett. con la stessa origine)

$$\langle \vec{A}, \vec{B} \rangle \qquad (\vec{A}, \vec{B}) \qquad \vec{A} \bullet \vec{B}$$

(i) $\langle \vec{A}, \vec{B} \rangle = \langle \vec{B}, \vec{A} \rangle$

(ii) $\langle \vec{A}+\vec{B}, \vec{C} \rangle = \langle \vec{A}, \vec{C} \rangle + \langle \vec{B}, \vec{C} \rangle$

(iii) $\langle \lambda\vec{A}, \vec{B} \rangle = \lambda \cdot \langle \vec{A}, \vec{B} \rangle$

(iv) $\langle \vec{A}, \vec{B} \rangle = 0 \iff OA \perp OB$

(v) $\langle \vec{A}, \vec{A} \rangle = \|\vec{A}\|^2$

$$\boxed{\langle \vec{A}, \vec{B} \rangle = OA \cdot OB \cdot \cos(\widehat{AOB})}$$

$O = (0,0)$

$\vec{A} = (x_0, y_0)$

$\vec{B} = (x_1, y_1)$

$\langle \vec{A}, \vec{B} \rangle =$

$= x_0 x_1 + y_0 y_1$.

Es: $\langle \vec{A}-\vec{B}, \vec{A}-\vec{B} \rangle = \langle \vec{A}, \vec{A}-\vec{B} \rangle - \langle \vec{B}, \vec{A}-\vec{B} \rangle =$

$\| \vec{A}-\vec{B} \|^2 = AB^2$

$= \langle \vec{A}, \vec{A} \rangle - \langle \vec{A}, \vec{B} \rangle - \langle \vec{B}, \vec{A} \rangle + \langle \vec{B}, \vec{B} \rangle =$

$= \|\vec{A}\|^2 + \|\vec{B}\|^2 - 2\langle \vec{A}, \vec{B} \rangle =$

$= OA^2 + OB^2 - 2 OA \cdot OB \cdot \cos \widehat{BOA}$

T. di Carnot

Es: $\langle \vec{A}-\vec{B}, \vec{A}+\vec{B} \rangle = \|\vec{A}\|^2 - \|\vec{B}\|^2$

Oss: $\langle \vec{A} \cdot \vec{B} \rangle^2 = OA^2 \cdot OB^2 \cdot \cos^2 \widehat{BOA} \leq OA^2 \cdot OB^2 = \|\vec{A}\|^2 \cdot \|\vec{B}\|^2$

$$|\langle \vec{A}, \vec{B} \rangle| \leq \|\vec{A}\| \cdot \|\vec{B}\|$$

disug. di Cauchy-Schwarz.

$$|x_0x_1+y_0y_1| \le \sqrt{(x_0^2+y_0^2)(x_1^2+y_1^2)}$$

Es: Se l'origine è il circocentro di $\overset{\triangle}{ABC}$ allora $\vec{H} = \vec{A}+\vec{B}+\vec{C}$ è l'ortocentro.

Dim: $HA \perp BC \iff \langle \vec{A}-\vec{H}, \vec{C}-\vec{B} \rangle = 0$ $\quad \|\vec{B}\| = OB = R$

$HB \perp AC \iff \langle \vec{B}-\vec{H}, \vec{C}-\vec{A} \rangle = 0$ $\quad \|\vec{C}\| = OC = R$

$HC \perp AB \iff \langle \vec{C}-\vec{H}, \vec{B}-\vec{A} \rangle = 0$

$$\langle \vec{A}-\vec{H}, \vec{C}-\vec{B} \rangle = \langle -\vec{B}-\vec{C}, \vec{C}-\vec{B} \rangle =$$

$$= \langle \vec{B}+\vec{C}, \vec{B}-\vec{C} \rangle = \|\vec{B}\|^2 - \|\vec{C}\|^2 = R^2 - R^2 = 0$$

$$\langle \vec{B}-\vec{H}, \vec{A}-\vec{C} \rangle = \langle \vec{A}+\vec{C}, \vec{C}-\vec{A} \rangle = \|\vec{A}\|^2 - \|\vec{C}\|^2 = R^2 - R^2 = 0$$

idem per l'altra $\Rightarrow$ $\vec{A}+\vec{B}+\vec{C}$ è l'ortocentro. $\square$

Es: O origine e circocentro $\Rightarrow$ $H = \vec{A}+\vec{B}+\vec{C}$

inoltre sempre $\vec{G} = \dfrac{\vec{A}+\vec{B}+\vec{C}}{3}$ $\qquad \vec{G} = \dfrac{1}{3}\cdot\vec{H}$

$\Rightarrow$ O, G, H allineati e $\dfrac{OG}{GH} = \dfrac{1}{2}$

retta di Eulero.

Es: $GH = ???$

$$\|\vec{H}-\vec{G}\|^2 = \langle \vec{H}-\vec{G}, \vec{H}-\vec{G} \rangle = \text{(origine nel circocentro)}$$

$$= \left\langle \vec{A}+\vec{B}+\vec{C} - \left(\frac{\vec{A}+\vec{B}+\vec{C}}{3}\right), \vec{A}+\vec{B}+\vec{C} - \left(\frac{\vec{A}+\vec{B}+\vec{C}}{3}\right) \right\rangle =$$

$$= \left\langle \frac{2}{3}(\vec{A}+\vec{B}+\vec{C}), \frac{2}{3}(\vec{A}+\vec{B}+\vec{C}) \right\rangle =$$

$$= \frac{4}{9}\left[\underbrace{\|\vec{A}\|^2+\|\vec{B}\|^2+\|\vec{C}\|^2}_{3R^2} + 2\langle\vec{A},\vec{B}\rangle + 2\langle\vec{B},\vec{C}\rangle + 2\langle\vec{C},\vec{A}\rangle\right]$$

$$c^2 = AB^2 = \langle\vec{A}-\vec{B},\vec{A}-\vec{B}\rangle = \underbrace{\|\vec{A}\|^2+\|\vec{B}\|^2}_{2R^2} - 2\langle\vec{A},\vec{B}\rangle$$

$$\boxed{2R^2 - c^2 = 2\langle\vec{A},\vec{B}\rangle}$$

$$= \frac{4}{9}\left[3R^2 + 2R^2 - c^2 + 2R^2 - a^2 + 2R^2 - b^2\right] =$$

$$= \frac{4}{9}\left[9R^2 - a^2 - b^2 - c^2\right] =$$

$$= 4R^2 - \frac{4}{9}(a^2+b^2+c^2) = GH^2$$

Oss: $OH^2 = 9R^2 - (a^2+b^2+c^2)$

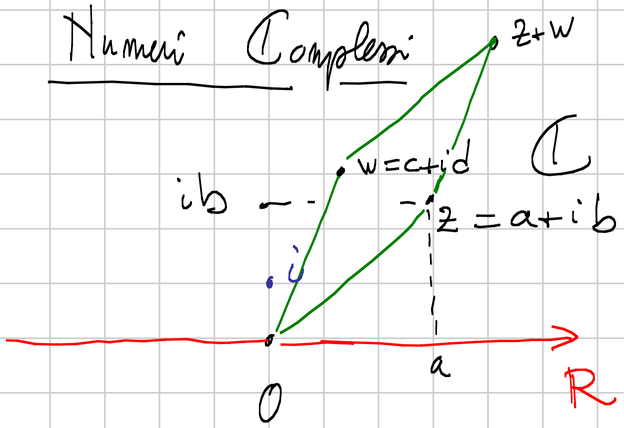
Oss: $OH^2 \geq 0 \qquad 9R^2 \geq a^2+b^2+c^2$

$$9\cancel{R^2} \geq 4\cancel{R^2}\sin^2\alpha + 4\cancel{R^2}\sin^2\beta + 4\cancel{R^2}\sin^2\gamma$$

$$\frac{9}{4} \geq \sin^2\alpha + \sin^2\beta + \sin^2\gamma \geq 0$$

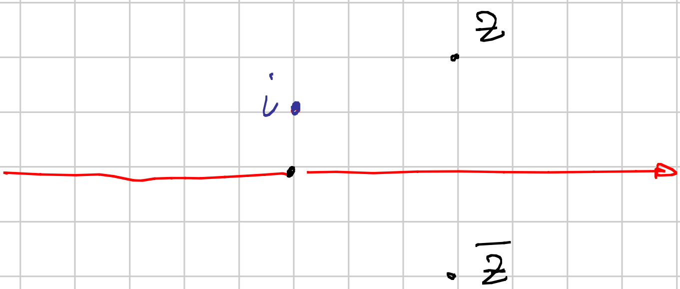
Oss: $OI^2 = R^2 - 2Rr = R(R-2r) \qquad R \geq 2r$

Numeri Complessi



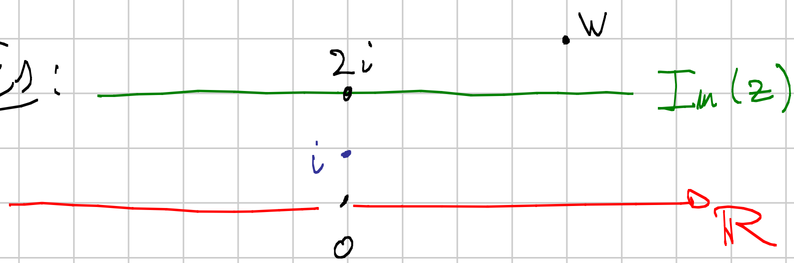
$z+w = (a+c) + i(b+d)$

Somma tra complessi
‖
Somma tra vettori con origine nello ZERO
‖
Traslazioni.



z
$\downarrow$ simmetria rispetto all'asse reale
$\bar z$

Es:



Simm di w rispetto alla retta verde $= \bar w + 4i$

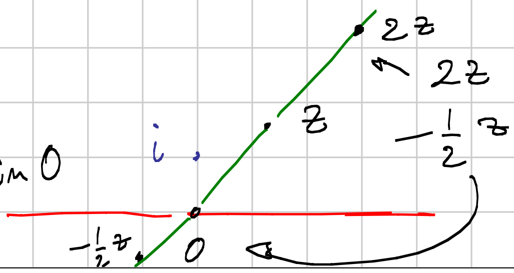
$\zeta \longrightarrow \zeta - 2i$

$w \longrightarrow w - 2i$ simm. risp. all'asse reale $= \overline{w-2i} =$
$= \bar w + 2i$

$\zeta' \longrightarrow \zeta' + 2i$ $\bar w + 4i$

Oss: $k \in \mathbb{R}$ $k \cdot z$

$k \cdot \vec A$ ↗ omotetia in 0



Es: z omotetia di fattore $-\frac{1}{3}$ rispetto al punto $1+i$

$$z \longrightarrow z-1-i \longrightarrow -\frac{1}{3}(z-1-i) \longrightarrow -\frac{1}{3}(z-1-i)+1+i$$

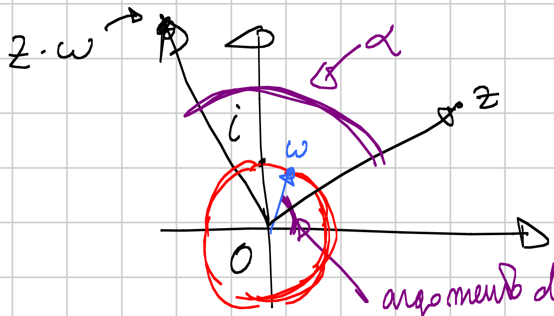
$$ = -\frac{1}{3}z+\frac{2}{3}(1+i)$$

Es: $\omega \in S^1 \quad \|\omega\|=1.$

$$\|w\| = \sqrt{w\cdot\overline{w}} = \sqrt{a^2+b^2}$$

$w = a+ib$

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



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

argomento di ω = $\arctan\frac{b}{a} = \alpha$

$z = \rho(\cos\theta + i\,\mathrm{sen}\,\theta)$ $\qquad \rho$ = modulo, norma

$\omega = \cos\alpha + i\,\mathrm{sen}\,\alpha$ $\qquad \theta$ = argomento

$$zw = \rho\left(\cos\theta\cos\alpha - \mathrm{sen}\,\theta\,\mathrm{sen}\,\alpha + i\left(\cos\alpha\,\mathrm{sen}\,\theta + \cos\theta\,\mathrm{sen}\,\alpha\right)\right) =$$

$$= \rho\left(\cos(\alpha+\theta) + i\,\mathrm{sen}(\alpha+\theta)\right)$$

$$\Rightarrow \arg(zw) = \arg(z) + \underbrace{\arg(\omega)}_{} = \text{rotazione di } \underset{\arg(\omega)}{\overset{\shortparallel}{\alpha}}$$

Es: Voglio ruotare z di $30°$ attorno a $2-\frac{i}{2}$

$$z \longrightarrow z-2+\frac{i}{2} \longrightarrow \left(z-2+\frac{i}{2}\right)\left(\cos 30° + i\,\mathrm{sen}\,30°\right) \Longrightarrow$$

$$\Longrightarrow \left(z-2+\frac{i}{2}\right)\left(\frac{\sqrt{3}}{2}+\frac{i}{2}\right) \longrightarrow \left(z-2+\frac{i}{2}\right)\left(\frac{\sqrt{3}}{2}+\frac{i}{2}\right)+2-\frac{i}{2}=$$

$$= z\left(\frac{\sqrt{3}}{2}+\frac{i}{2}\right)+\left(2-\frac{i}{2}\right)\left(1-\frac{\sqrt{3}}{2}+\frac{i}{2}\right)$$

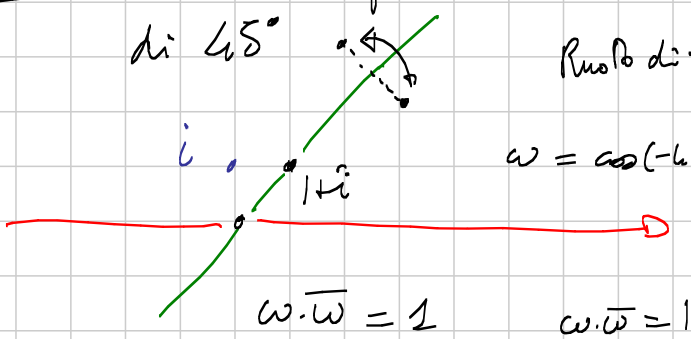
Es: Ruoto z di $45°$ attorno a $1+i$ e poi faccio la simmetria rispetto a $\mathrm{Im}(z)=-2i$

$$z \longrightarrow (z-1-i) \longrightarrow (z-1-i)\left(\frac{1}{\sqrt{2}}+\frac{i}{\sqrt{2}}\right) \longrightarrow (z-1-i)\left(\frac{1+i}{\sqrt{2}}\right)+1+i$$

$$\longrightarrow (z-1-i)\left(\frac{1+i}{\sqrt{2}}\right)+1+i+2i \longrightarrow (\bar{z}-1+i)\left(\frac{1-i}{\sqrt{2}}\right)+1-3i$$

$$\longrightarrow (\bar{z}-1+i)\left(\frac{1-i}{\sqrt{2}}\right)+1-3i-2i=(\bar{z}-1+i)\left(\frac{1-i}{\sqrt{2}}\right)+1-5i$$

Es: Simmetria rispetto alla retta per $1+i$ inclinata di $45°$



Ruoto di $-45°$ $\longrightarrow$ simmetria risp. a $\mathbb{R}$ $\longrightarrow$ Ruoto di $45°$

$$\omega=\cos(-45°)+i\,\mathrm{sen}(-45°)=$$

$$=\frac{1}{\sqrt{2}}-\frac{i}{\sqrt{2}}$$

$$\omega\cdot\bar{\omega}=1 \qquad 1=\|\omega\|^2$$

$$\omega\cdot\bar{\omega}=1 \Longrightarrow \bar{\omega}=\frac{1}{\omega}$$

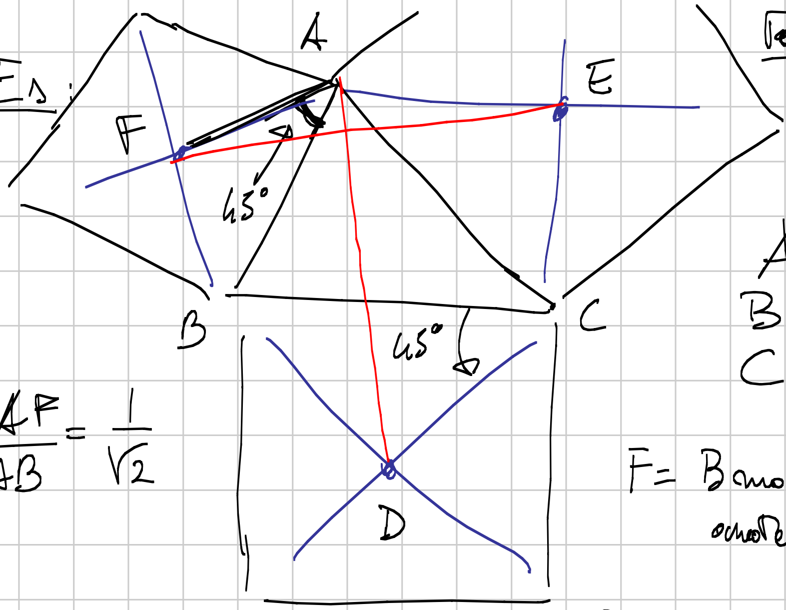
$$z \longrightarrow z\left(\frac{1}{\sqrt{2}}-\frac{i}{\sqrt{2}}\right) \longrightarrow \bar{z}\left(\frac{1}{\sqrt{2}}+\frac{i}{\sqrt{2}}\right) \longrightarrow \bar{z}\left(\frac{1}{\sqrt{2}}+\frac{i}{\sqrt{2}}\right)^2$$

Ruot di $-45°$ — simm. risp a $\mathbb{R}$ — Ruot di $45°$

Simm risp. a una retta per O inclinata di θ

$$z \longrightarrow \bar{z}\left(\cos\theta+i\,\mathrm{sen}\,\theta\right)^2$$

Es:



Tesi: $AD \perp EF$
$AD = EF$

$\frac{AF}{AB} = \frac{1}{\sqrt{2}}$

$A = 0$
$B = b$
$C = c$

$F =$ B ruotato di $-45°$ e omotetizzato di $\frac{1}{\sqrt{2}}$

$$f = b\left(\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}\right)\cdot\frac{1}{\sqrt{2}} = b\,\frac{1-i}{2}$$

$$e = c\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right)\frac{1}{\sqrt{2}} = c\,\frac{1+i}{2}$$

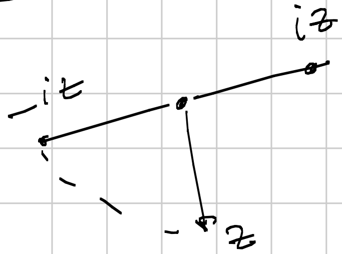
$$d = (b-c)\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right)\cdot\frac{1}{\sqrt{2}} + c = $$
$$= (b-c)\left(\frac{1+i}{2}\right) + c$$

$$\left.\begin{array}{l} AD \perp EF \\ AD = EF \end{array}\right\} \Longleftrightarrow d = \pm i\,(e-f)$$

$$(b-c)\left(\frac{1+i}{2}\right) + c = \left[\frac{c-b}{2} + i\,\frac{(c+b)}{2}\right](\pm i)$$

$$\frac{b-c}{2} + c + \frac{i}{2}(b-c) \qquad\qquad \pm i\,\frac{c-b}{2} \mp \frac{(c+b)}{2}$$

$$= \frac{b+c}{2} + \frac{i}{2}(b-c) \;=\!=\!=\; -\left(\frac{c-b}{2}\right)i + \left(\frac{c+b}{2}\right)$$



G3 BASIC

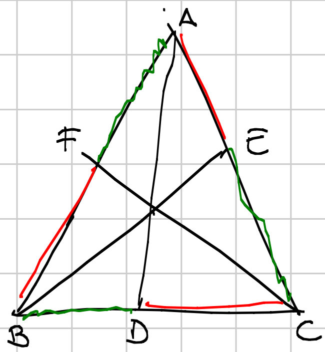
-Maria-

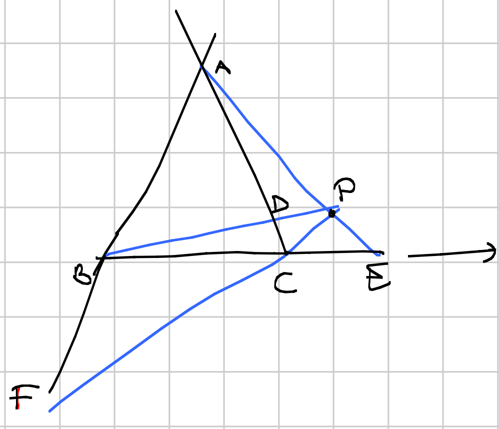
Titolo nota 09/09/2010

- Allineamenti e concorrenze: Ceva, Menelao, Carnot, ...
- Circonferenze: angoli, potenze...
- Trasformazioni geometriche
- Retta di Eulero, Feuerbach
- Excerchi ...

Teo di Ceva:
AD, BE, CF concorrono

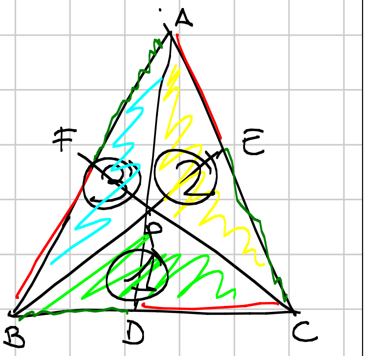
$$\iff \frac{AF}{FB} \cdot \frac{BD}{DC} \cdot \frac{CE}{EA} = 1$$





$\Rightarrow$) Dim (Aree)

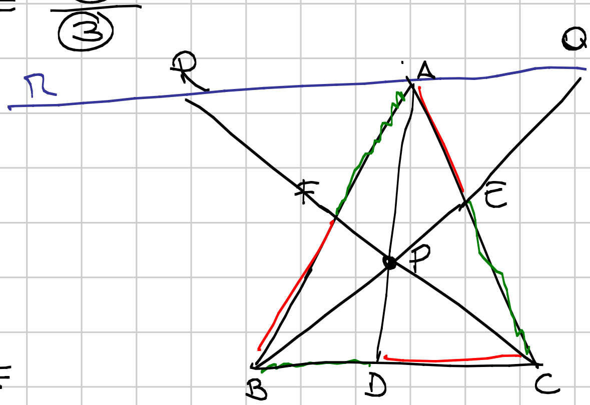
$$\frac{AF}{FB} = \frac{[AFC]}{[BFC]} = \frac{[AFP]}{[BFP]} \overset{?}{=} \frac{[APC]}{[BPC]}$$



$$\frac{[APC]}{[BPC]} = \frac{[AFC]-[AFP]}{[BCF]-[BFP]} = \frac{[AFC]}{[BFC]}\left(\underbrace{\frac{1-\frac{[AFP]}{[AFC]}}{1-\frac{[BFP]}{[BFC]}}}_{=1}\right)$$

$$= \frac{AF}{FB} = \frac{2}{1}$$

$$\frac{BD}{DC} = \frac{3}{2} \qquad \frac{CE}{EA} = \frac{1}{3}$$



Dim:

$r \parallel BC$.

$$\frac{AF}{FB} = \frac{AR}{BC}$$ simili $AFR \sim BCF$

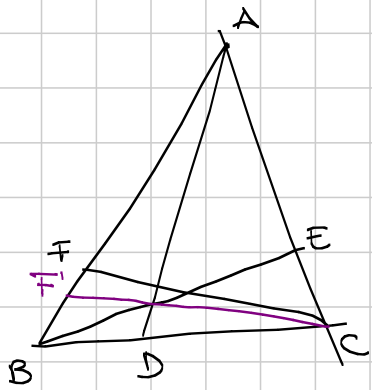
$$\frac{BD}{DC} = \frac{QA}{AR}$$

$$\frac{CE}{EA} = \frac{BC}{AQ}$$ $BCE \sim AEQ$

($\Leftarrow$) $$\frac{AF}{FB}\cdot\frac{BD}{DC}\cdot\frac{CE}{EA} = 1$$

$$\frac{AF'}{F'B}\cdot\frac{BD}{DC}\cdot\frac{CE}{EA} = 1$$

$$\Rightarrow \frac{AF}{FB} = \frac{AF'}{F'B}$$

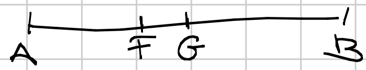


$F \longrightarrow \dfrac{AF}{FB}$

$G > F$

$$\frac{AF}{FB} < \frac{AG}{GB}$$

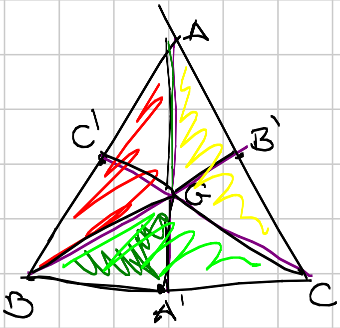
$AF < AG$, $FB > GB$



$\Longrightarrow \quad F = F'$

Esempio: baricentro

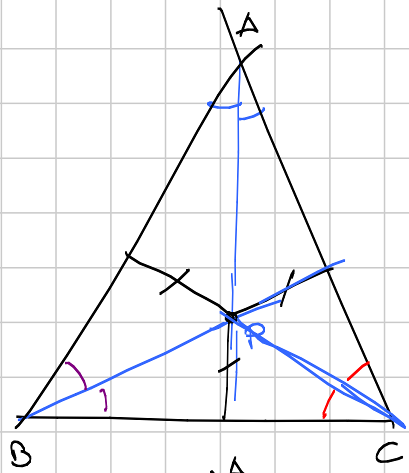
$$\underbrace{\frac{AC'}{C'B}}_{=1} \cdot \underbrace{\frac{BA'}{A'C}}_{=1} \cdot \underbrace{\frac{CB'}{B'A}}_{=1} = 1$$



$[AGC] = [BCG] = [ABG]$

$$\frac{AG}{GA'} = \frac{[ABG]}{[A'BG]} = \frac{2 \text{ triangolini}}{1 \text{ triangolino}} = 2$$

Esempio: incentro.

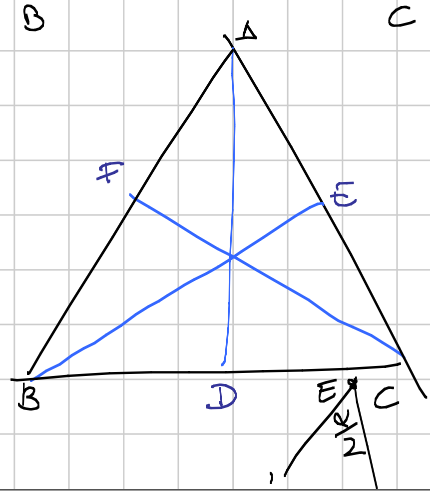


$$\frac{BD}{DC} = \frac{c}{b}$$

$$\frac{CE}{EA} = \frac{a}{c}$$

$$\frac{AF}{FB} = \frac{b}{a}$$

$$\frac{\cancel{c}}{\cancel{b}} \cdot \frac{\cancel{a}}{\cancel{c}} \cdot \frac{\cancel{b}}{\cancel{a}} = 1$$

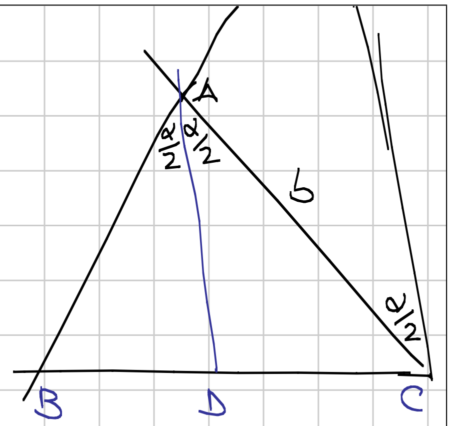


Lemma

$$\frac{BD}{DC} = \frac{c}{b}$$

$$\frac{BD}{DC} = \frac{AB}{AE} = \frac{c}{AE}$$

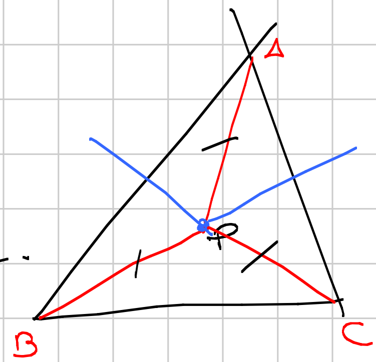
ACE è isoscele $\Rightarrow$ $AE = b$



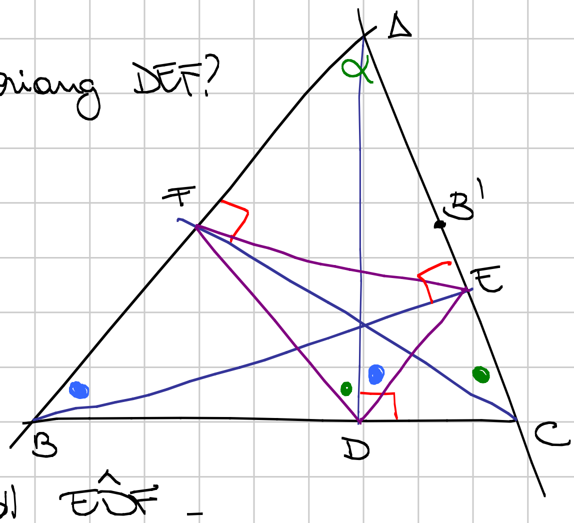
Circocentro?

$$\underbrace{BP = AP}_{\Downarrow} = PC$$

P sta sull'asse di BC.



Esempio: ortocentro
(con Ceva, esercizio)
Cos'è AD rispetto al triang DEF?
AD



Oss: $AFDC$ è ciclico.

$\hat{FDA} = F\hat{C}E = 90 - \alpha$

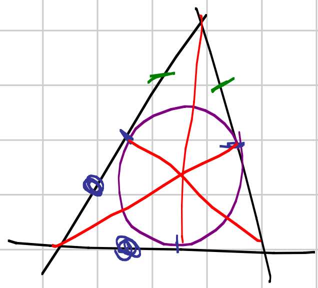
$\hat{ADE} = A\hat{B}E = 90 - \alpha$

$\Rightarrow$ AD è bisettrice di $E\hat{D}F$.

Oss: ortocentro di ABC = incentro DEF

Oss: centro della circo circoscr $AFDC$
= pto medio di AC

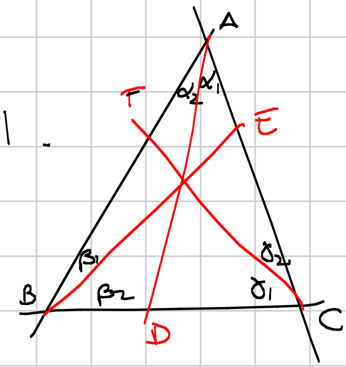
Esercizio pto di Gergonne



Ceva in vers trigo:

(1) AD, BE, CF concorrono

$\Leftrightarrow \quad \frac{\sin\alpha_1}{\sin\alpha_2} \cdot \frac{\sin\beta_1}{\sin\beta_2} \cdot \frac{\sin\gamma_1}{\sin\gamma_2} = 1.$ (2)



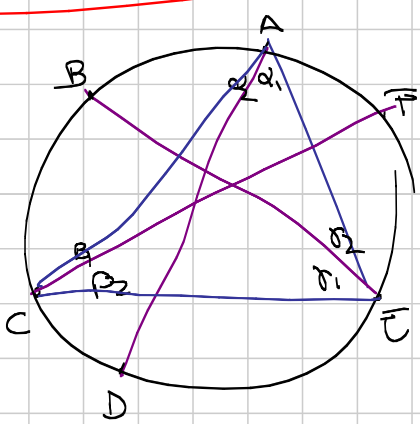
(1) $\Leftrightarrow \quad \frac{AF}{FB} \cdot \frac{BD}{DC} \cdot \frac{CE}{EA} = 1$

$\frac{DC}{\cancel{\sin\alpha_1}} = \boxed{\frac{AD}{\sin\gamma} \cdot \sin\alpha_1}$ (teo Seni su $\triangle ACD$)

$\frac{BD}{\cancel{\sin\beta_2}} = \boxed{\frac{AD}{\sin\beta} \cdot \sin\alpha_2}$ (teo Seni ABD)

$AF = \boxed{\frac{CF}{\sin\alpha} \cdot \sin\gamma_2}$ $\quad BF = \boxed{\frac{CF}{\sin\beta} \cdot \sin\gamma_1}$

$CE = \boxed{\frac{BE}{\sin\gamma} \sin\beta_2}$ $\quad AE = \boxed{\frac{BE}{\sin\alpha} \sin\beta_1}$



Esempio

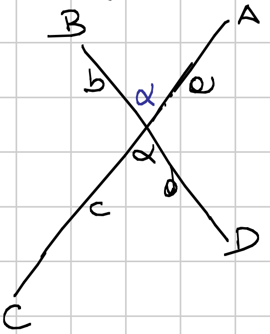
AD, BE, CE concorrono

$\Leftrightarrow \quad AB \cdot CD \cdot EF = BC \cdot DE \cdot FA$

$AB = 2R \sin\gamma_2$

Teorema di Carnot.

Lemma (metrica di perp)



$AC \perp BD \iff$
$AB^2 + CD^2 = AD^2 + BC^2$.
(1) (2)

Dim:

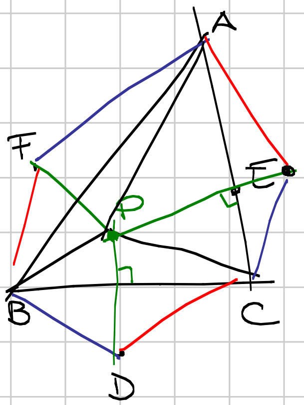
$\Rightarrow) = a^2+b^2+c^2+d^2$

$\Leftarrow) \overset{(1)}{=} a^2+b^2-2ab\cos\alpha +$
$c^2+d^2-2cd\cos\alpha$

$(2) = a^2+d^2+2ad\cos\alpha$
$+ b^2+c^2+2bc\cos\alpha$

$-2ab-2cd = 2ad+2bc$

Teo:
le perp da F ad AB,
da E a AC,
da D a BC
concorrono $\iff$
$AF^2 + BD^2 + CE^2 = AE^2 + BF^2 + CD^2$



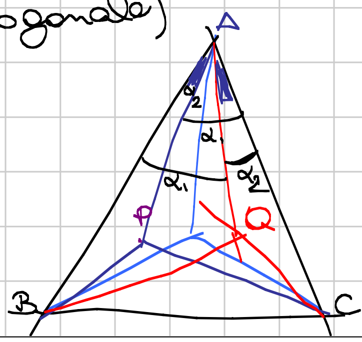
$\Rightarrow)$ $AF^2 + BP^2 = AP^2 + BF^2$
$BD^2 + CP^2 = BP^2 + CD^2$
$CE^2 + AP^2 = CP^2 + AE^3$

Esercizio (esistenza coniugato isogonale)

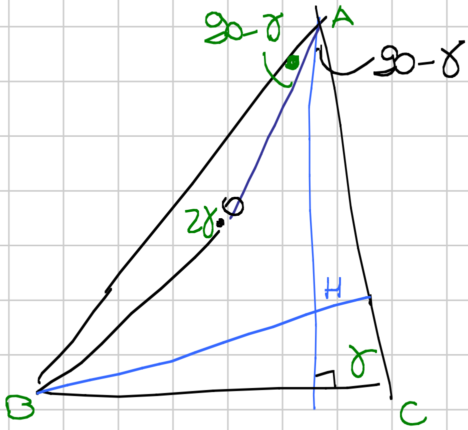
Q è coniugato isog di P.

Dim concorrenza:

$\frac{\sin\alpha_1}{\sin\alpha_2} \cdot \ldots = 1$



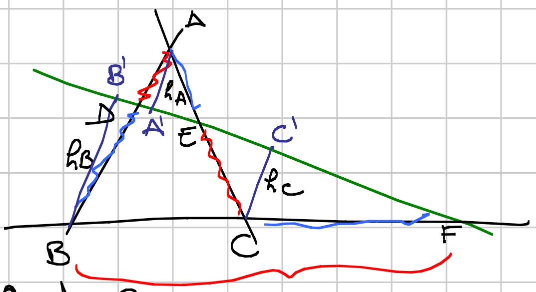
Oss: il coniug isog del circoc è l'ortoc



Teo di Menelao.

D, E, F sono all $\iff$

$$\frac{AD}{DB} \cdot \frac{BF}{FC} \cdot \frac{CE}{EA} = -1$$



Dim: esercizio: dedurlo da Ceva.

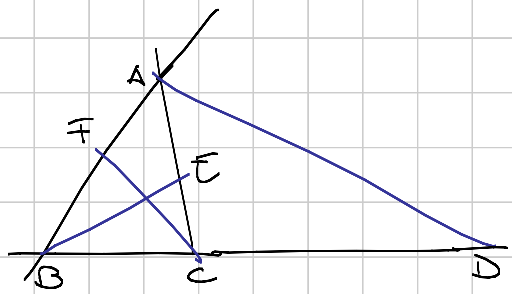
$\Rightarrow$) $\dfrac{AD}{DB} = \dfrac{h_A}{h_B}$ sim $AA'D \sim BB'D$

$$\frac{BF}{FC} = -\frac{h_B}{h_C}$$

$$\frac{CE}{EA} = \frac{h_C}{h_A}$$

Sostituisco, ok

Esercizio:
2 bisettrici interne, 1 esterna.
$\Rightarrow$ D, E, F allineati.



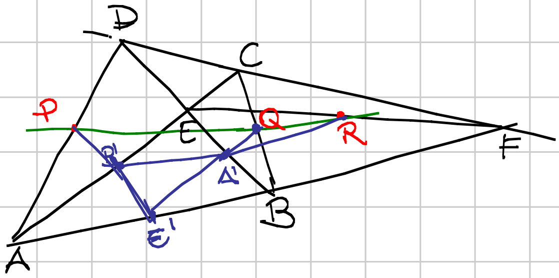
Esempio (linea di Gauss)

ABCD quadril.

R pto medio EF

P, Q di AD, BC.

$\Rightarrow$ P, Q, R allineati.



Dim

Consideriamo $A'E'B'$ mediale di ABE

$\Rightarrow$ E', A', Q sono allineati.

E', B', P

A', B', R

teo di Menelao con $A'B'E'$

P, Q, R sono all $\Longleftrightarrow$ $\frac{B'P}{PE'} \cdot \frac{E'Q}{QA'} \cdot \frac{A'R}{RB'} \overset{?}{=} -1$

$PE' \parallel BD \Rightarrow \frac{B'P}{PE'} = \frac{ED}{DB}$

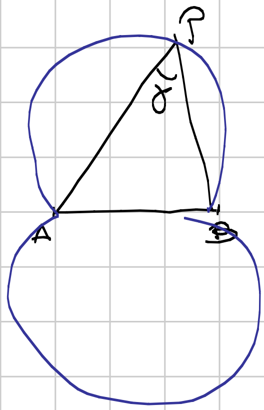
$E'A' \parallel AC \Rightarrow \frac{E'Q}{QA'} = \frac{AC}{CE}$

$A'B' \parallel AB \Rightarrow \frac{A'R}{RB'} = \frac{BF}{FA}$

$\frac{ED}{DB} \cdot \frac{AC}{CE} \cdot \frac{BF}{FA} \overset{?}{=} -1$

Ok per il teo di Menelao applicato a ABE rispetto alla retta C, D, F.

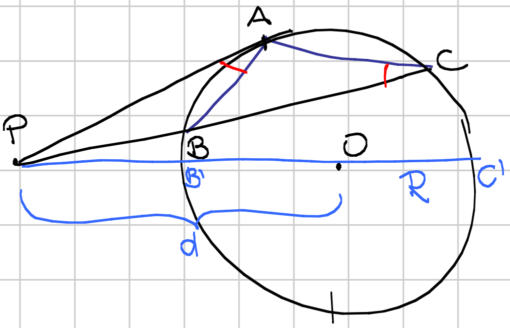
CIRCONFERENZE



$PA^2 = PB \cdot PC$

Cons i triangoli PAB e PCA. Sono simili.

$$\frac{PA}{PB} = \frac{PC}{PA}$$

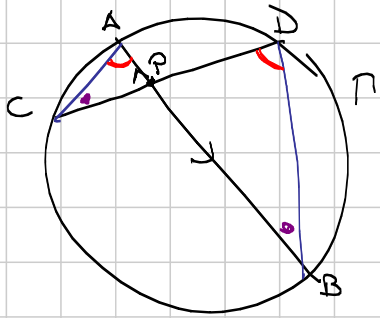


$Pow_\Gamma P = PB \cdot PC = (d-R)(d+R) = d^2 - R^2$.

$PA \cdot PB = PC \cdot PD$

I triangoli APC e BDP sono simili.

$$\frac{PA}{PC} = \frac{PD}{PB}$$ ok.

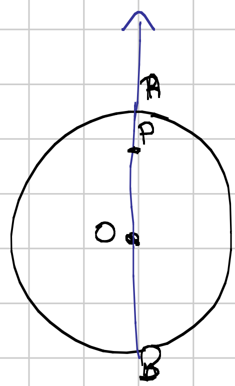


P interno:

$Pow_\Gamma P = PB \cdot PC < 0$

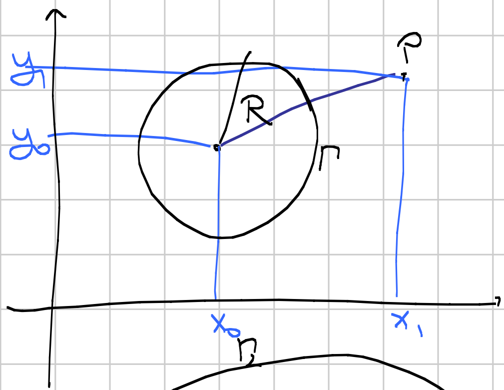
P è interno $\Leftrightarrow$ $Pow_\Gamma P < 0$

$Pow_\Gamma P = PA \cdot PB = (R-d)(-R-d)$
$= d^2 - R^2$



Oss:

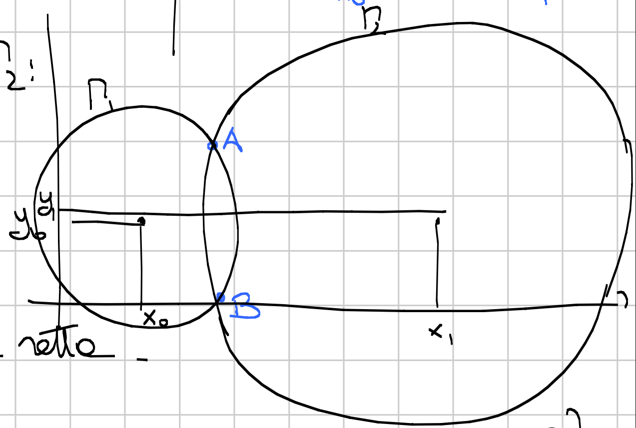
$$Pow_{\Gamma} P = d^2 - R^2$$
$$= (y_1 - y_0)^2 + (x_1 - x_0)^2 - R^2$$
$$(y - y_0)^2 + (x - x_0)^2 - R^2 = 0$$



Asse radicale di Γ_1 e Γ_2:

$$r = \{ P : Pow_{\Gamma_1} P = Pow_{\Gamma_2} P \}$$

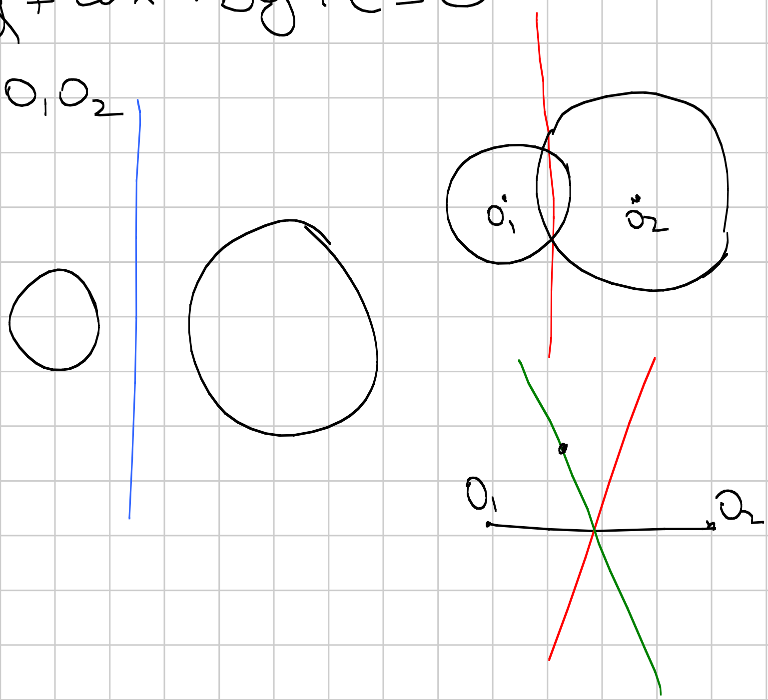
$A, B \in r$.



Prop: l'asse rad è una retta.

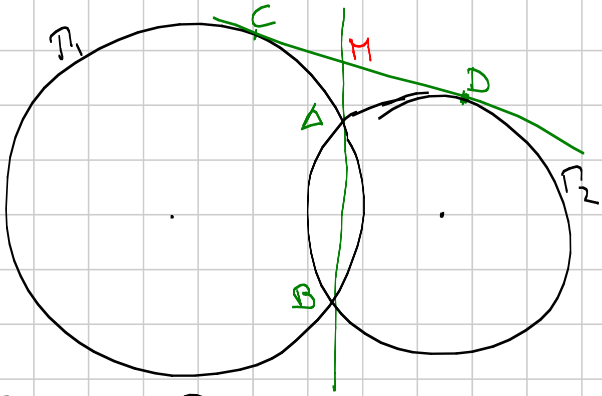
$$r = \{ (x,y) : (x - x_0)^2 + (y - y_0)^2 - r_1^2 = (x - x_1)^2 + (y - y_1)^2 - r_2^2 \}$$
$$\cancel{dx^2} + \cancel{ey^2} + ax + by + c = 0$$

Oss: $r \perp O_1 O_2$



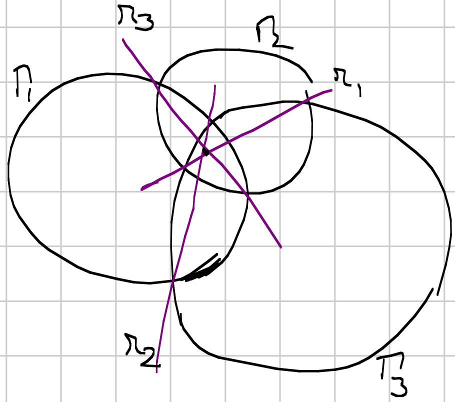
Oss 1:

M è pto medio di CD.



$$M \in AB \Rightarrow \underbrace{Pow_{\Gamma_1} M}_{= MC^2} = \underbrace{Pow_{\Gamma_2} M}_{= MD^2}$$

Oss 2: $\Gamma_1, \Gamma_2, \Gamma_3$ circo $\Rightarrow$ gli assi radicali concorrono

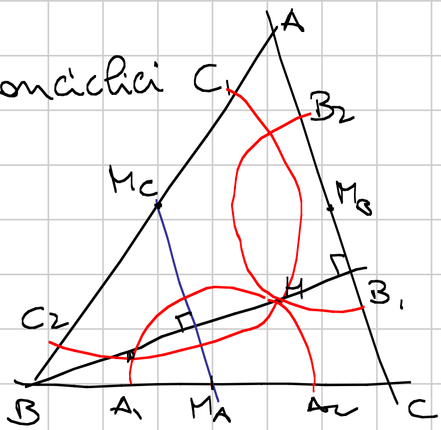


$r_2 \cap r_3 = P$: $\underbrace{Pow_{\Gamma_1} P}_{= Pow_{\Gamma_2} P} = Pow_{\Gamma_3} P$

$\Rightarrow P \in r_1$

Es: IMO 2008 – 1

Tesi: $A_i B_i C_i$, $i = 1, 2$, sono conciclici



Oss: se fossero conciclici, O sarebbe il centro.

BH • $\perp M_A M_C$
 • passa per H

BH è asse radicale

$$BC_1 \cdot BC_2 = BA_1 \cdot BA_2$$

$\Rightarrow A_1 A_2 C_1 C_2$ è ciclico.

Il centro della circo per) è O (sta sull'asse di A_1A_2, cioè AB, e di C_1C_2, cioè BC)

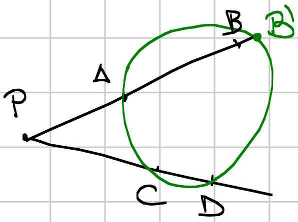
Oss: ABCD è ciclico

$\iff PA \cdot PB = PC \cdot PD$

$\Rightarrow$) ok

$\Leftarrow$) $PA \cdot PB' = PC \cdot PD$

$PB' = PB \Rightarrow B = B'$.



Oss:

I 3 cerchi concorrono.

$P = \Gamma_1 \cap \Gamma_2$

$P \in \Gamma_3 \iff$

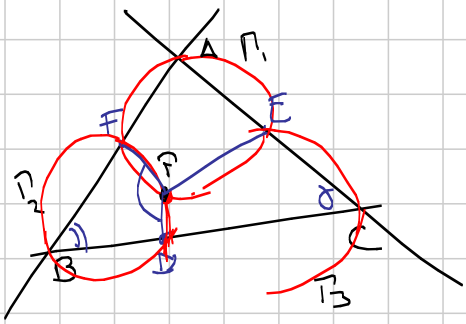
$D\hat{P}E + \gamma = 180$

$D\hat{P}F = 180 - \beta$

$F\hat{P}E = 180 - \alpha$

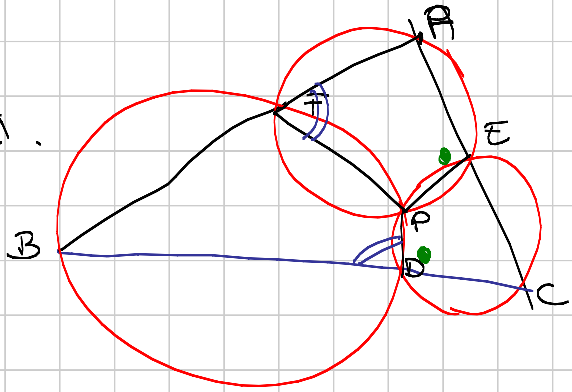
$\Rightarrow D\hat{P}E = 360 - D\hat{P}F - F\hat{P}E$

$= \alpha + \beta = 180 - \gamma$



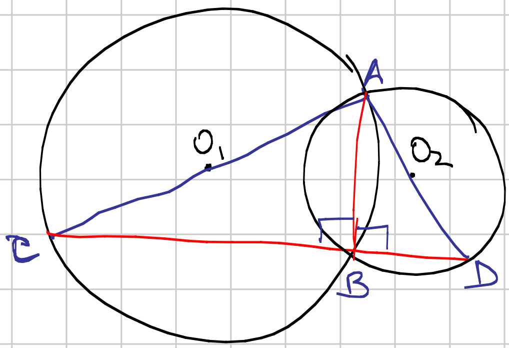
Oss:

$\Rightarrow$ B, D, C allineati.



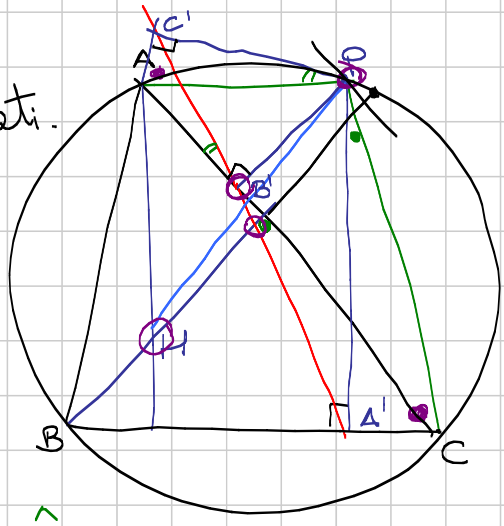
Oss:

C, B, D all.



Es: SIMSON LINE

$P \in \Gamma \Rightarrow A', B', C'$ allineati.



Sono allineati se
$A\hat{B'}C' = A'\hat{B'}C$

$AB'PC'$ è ciclico $\Rightarrow$
$A\hat{B'}C' = A\hat{P}C'$

$A'CPB'$ ciclico $\Rightarrow A'\hat{B'}C = A'\hat{P}C$

$\quad \| = 90 - \bullet$

$ABCP$ ciclico $\Rightarrow C'\hat{A}P = A'\hat{C}P$

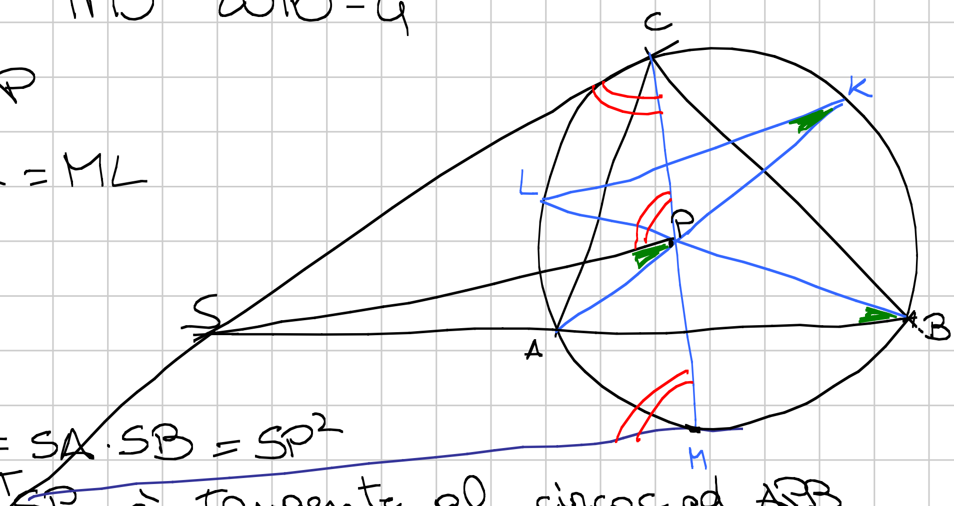
$\bullet = 90 - \bullet$

Esercizio: la SE di P passa per il pto medio di PH.

Esercizio IMO 2010-4

$SC = SP$

$\Rightarrow MK = ML$



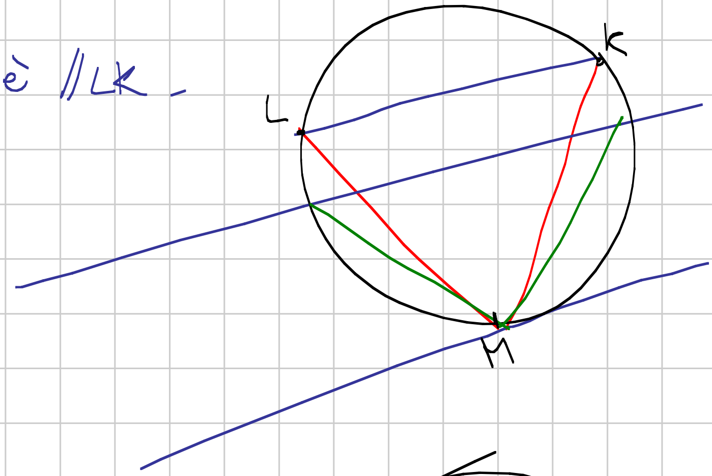
$SC^2 = SA \cdot SB = SP^2$

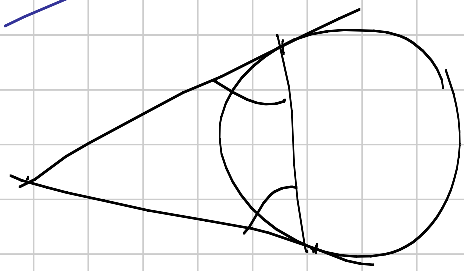
$\Rightarrow$ TSP è tangente al circoc ad APB

$\Rightarrow SP \parallel LK$

Manca: $TM \parallel SP$.

LM = MK $\iff$
la tang in M è // LK.



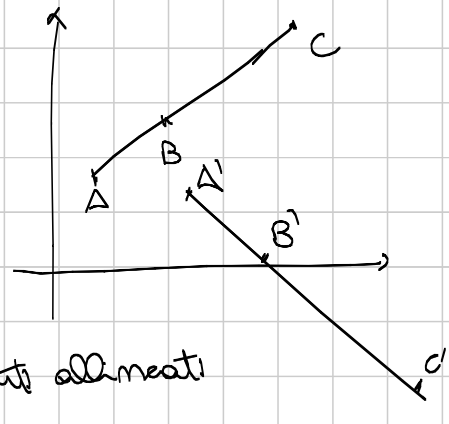


TRASFORMAZIONI GEOMETRICHE

AFFINITÀ:

$$\begin{cases} x \longrightarrow ax+by+c = x' \\ y \longrightarrow dx+ey+f = y' \end{cases}$$

(con $ae-db \neq 0$, invertibile)



- conserva: • concorr, parall,
  - rapporti di segmenti allineati
- non conserva: • similitudine
  - angoli
  - circonferenze

Oss A, B, C non all, A', B', C' non all

$\Rightarrow$ esiste affinità che manda $A \to A'$

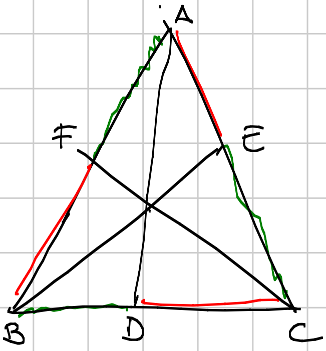
$B \to B'$

$C \to C'$

Teo di Ceva:

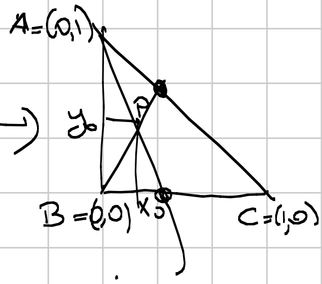
AD, BE, CF concorrono

$$\Longleftrightarrow \quad \frac{AF}{FB} \cdot \frac{BD}{DC} \cdot \frac{CE}{EA} = 1$$



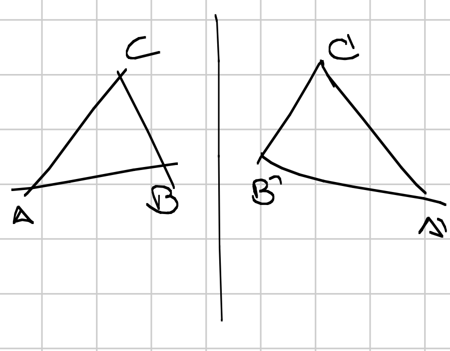
Dim:

A meno di affinità possiamo supporre

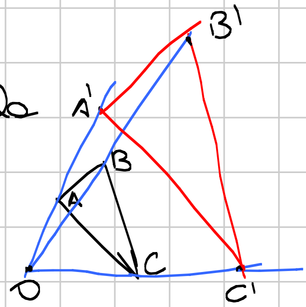


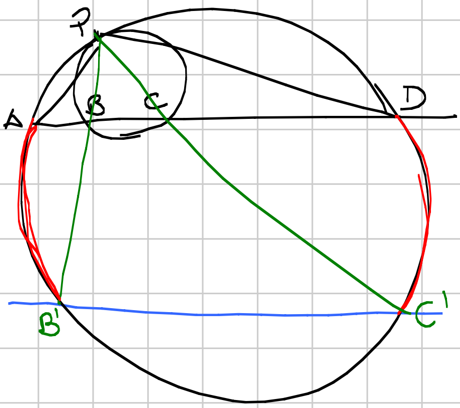
Riflessioni, rotazioni, traslazioni

Oss: rifl + rifl = $\begin{cases} \text{trasl (assi parall)} \\ \text{rotazione (non parall)} \end{cases}$



Omotetie:
Conserva gli angoli,
parall (e una retta è parall alla sua immagine)
rapporti di lunghezze



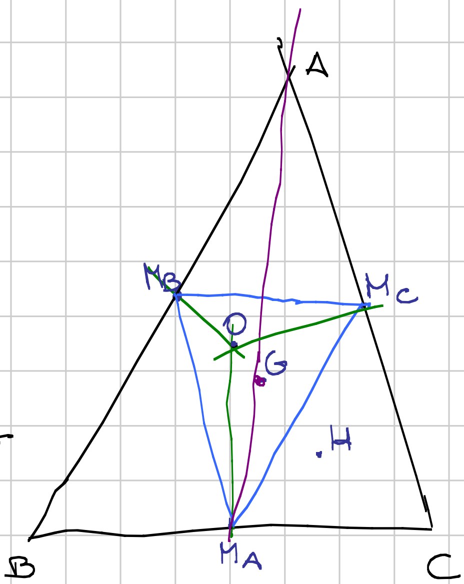


Esempio
$A\hat{P}C = B\hat{P}D$.

Omotetia di centro P.
$B'C' \parallel AD$

Tesi $\Leftrightarrow$ $A\hat{P}B = C\hat{P}D$

Retta di Eulero.
O, G, H sono all,
$\vec{OG} = \frac{1}{3}\vec{OH}$

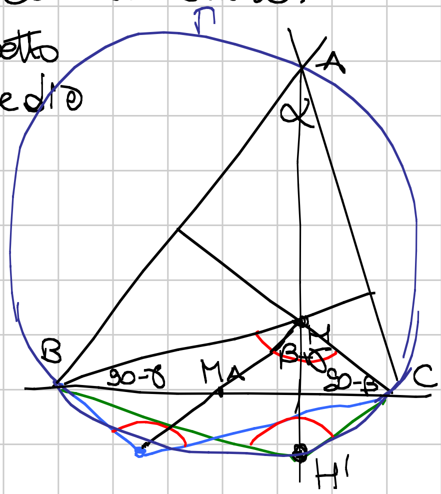


Dim:
Omotetia di centro G e rapporto $-1/2$.
$A \to M_A$
$H \to$ ortoc del triangolo $M_AM_BM_C$
$=$ circoc di ABC (altezza M_A a M_BM_C è

esse BC).

O $\quad G = \frac{A+B+C}{3} \quad H = A+B+C$

Lemma del simmetrico dell'ortocentro:
il simmetrico dell'ortoc rispetto a un lato o a un pto medio sta sulla circo circoscritta



Dim:
Caso Acutangolo
Devo verif
$B\hat{A}C + B\hat{H'}C = 180°$

$B\hat{H'}C = B\hat{H}C = \beta + \gamma$

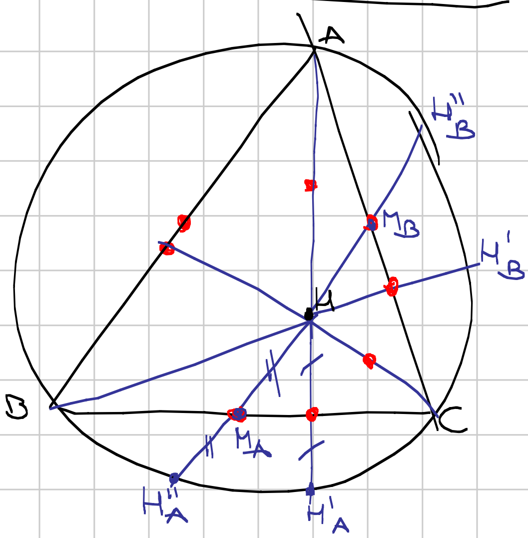
X i punti medi, quesi uguale.
Dim 2 pti medi

$$X \longrightarrow 2M_A - X$$

$$H \longrightarrow 2 \cdot \frac{B+C}{2} - (A+B+C) = -A$$

Omotetia di centro H e rapporto $\frac{1}{2}$.

$H'_A \to$ piede altezze
$H''_A \to M_A$
$A \to$ pto medio di AH

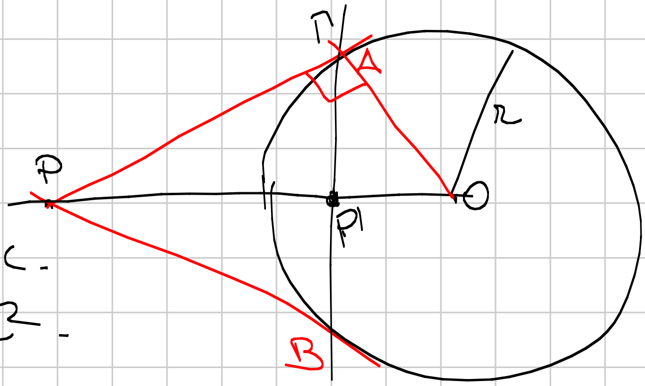


M_A, M_B, M_C, piedi delle alt

Sono conciclici

È detto CIRCONFERENZA DI FEUERBACH!

Inversione



$P \to P'$ su OP t.c.

$OP \cdot OP' = r^2$.

P' si ottiene $AB \cap OP$

Dim: chiamiamo "P" e verifichiamo

$OP \cdot OP'' = r^2$.

È il 1° teo di Euclide sul triangolo AOP.

Punti fissi: Γ

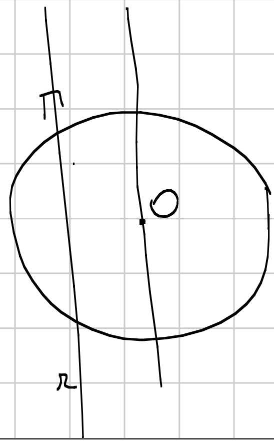
Retta per O → sé

Retta non per O →

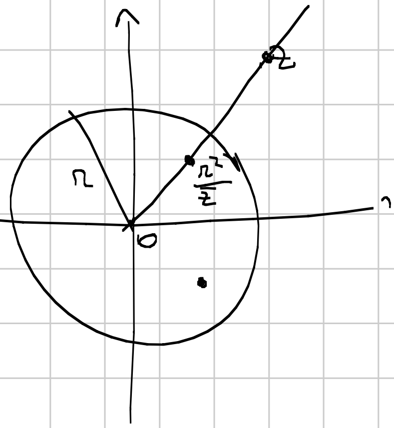
circonferenza per O

$a \operatorname{Re} z + b \operatorname{Im} z + c = 0$

$z \longrightarrow \frac{r^2}{\bar{z}}$



$$\frac{r^2}{|z|} \qquad |z|\cdot|w| = r^2$$



$$\frac{r^2}{z} \qquad z \longrightarrow \frac{1}{z}$$

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

$$a \operatorname{Re}\frac{r^2}{\bar z} + b \operatorname{Im}\frac{r^2}{\bar z} + c = 0$$

$$a \operatorname{Re}\frac{r^2 z}{|z|^2} + b \operatorname{Im}\frac{r^2 z}{|z|^2} + c = 0$$

$$a\, r^2 \operatorname{Re} z + b\, r^2 \operatorname{Im} z + c|z|^2 = 0$$

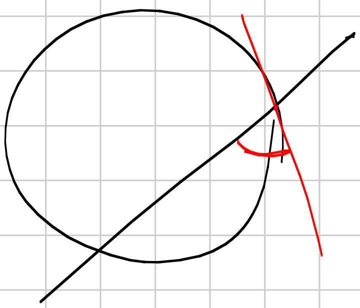
$\operatorname{Re} z = x \qquad \operatorname{Im} z = y$

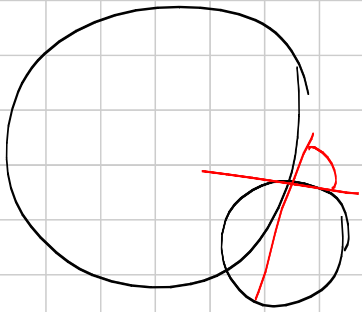
$$a r^2 x + b r^2 y + c(x^2+y^2) = 0$$

Circonferenze non per O $\longrightarrow$ circonferenze non per O.

Attenzione: i centri non vanno necess nei centri.

Oss: conservo gli angoli tra rette e circonf.





Ossi:

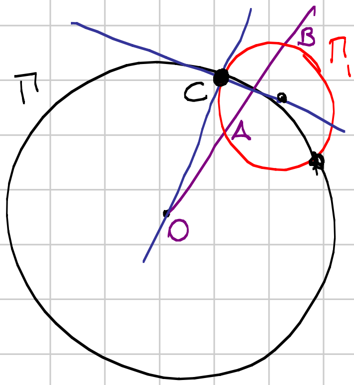
Se inverto rispetto a Γ,

Γ_1 resta fermo

Immagine di Γ_1

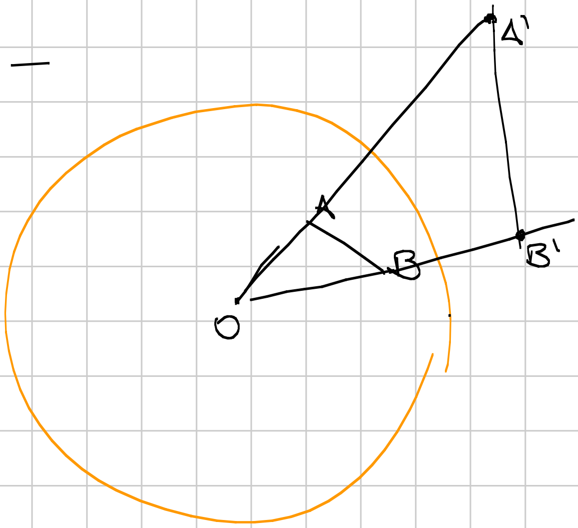
B e A si scambiano?

$$OA \cdot OB = r^2$$
$$\text{Pow}_{\Gamma_1} O = OC^2$$



Teorema di Tolomeo —

$A'B' = ?$



$$OA \cdot OA' = r^2$$
$$OB \cdot OB' = r^2$$
$$\frac{OA}{OB} = \frac{OA'}{OB'}$$

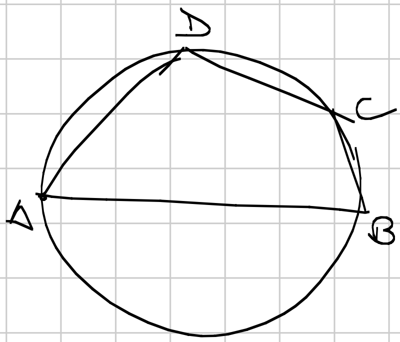
$\Rightarrow$ similitudine di OAB e $OB'A'$

$$\boxed{\frac{A'B'}{AB} =} \frac{OA'}{OB} = \boxed{\frac{r^2}{OB \cdot OA}}$$

Teo di Tolomeo:

$AB \cdot CD + BC \cdot AD \geq AC \cdot AD$,

con uguaglianza ($\Leftrightarrow$) A, B, C, D sono conciclici.



Dim: Invertiamo rispetto ad A con raggio 1

$\cdot D'$

$B'C' + C'D' \geq B'D'$

con $=$ $\Leftrightarrow$

B', C', D' sono all

$\Leftrightarrow$ A, B, C, D conciclici

$\cdot C'$

$\cdot B'$

$$\frac{BC}{AB \cdot AC} + \frac{CD}{AC \cdot AD} \geq \frac{BD}{AB \cdot AD}$$

DARKCRYSTAL

Teoria dei Numeri 1 (Basic)

Titolo nota 06/09/2010

$x^2 + x + 1 = y^2$ $\quad x, y$ interi positivi

Equazione diofantea

$x \longrightarrow x^2 \neq x^2 + x + 1$ (piccolo)

$(x+1) \longmapsto x^2 + 2x + 1$ (grosso)

Rappresentazioni in base

$322_{10} = 3 \cdot 10^2 + 2 \cdot 10^1 + 2 \cdot 10^0$

$\shortparallel$

102221_3

$1, 3, 9, 27, 81, 243, \cancel{729}$

Resto $\begin{array}{r} 79 - \\ 54 \\ \hline 25 \end{array}$

(IMO) $f : \mathbb{N} \longrightarrow \mathbb{N}$ (f va dagli interi ≥ 0 agli interi ≥ 0)

$f(0) = f(1) = 0, \quad f(2n) = 2f(n) + 1,$

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

f e' ben definita su $\{0, 1, \ldots, m\}$

$f(m+1) = ?$

	n	$f(n)$	
0	0	0	0
1	1	0	0
10	2	1	(0)1
11	3	0	(00)
100	4	3	(0)11
101	5	2	(0)10
110	6	1	(00)1

Fissato n $\exists\, m$ t.c.

$$f^m(n) = 0$$

$$n_2 = \underbrace{1\ \ldots}_{k \text{ cifre}}$$

$f(n)$ = al più $k-1$ cifre

FORMALIZZATA?

Per induzione sul numero di cifre di n_2

- 1 cifra (verifica)
- Passo induttivo $n_2 = \underbrace{a_1 \dots a_k}\ \begin{matrix} 0 & (a) \\ 1 & (b) \end{matrix}$

a) $f(n) = f(2_{10}\ \underbrace{a_1 \dots a_k}) = 2 f(a_1 \text{---} a_k) + 1 =$

$\underset{\substack{\uparrow \\ \text{ipot. indutt.}}}{=} \overline{a_1}\ \overline{a_2} \dots \overline{a_k}\ 0 + 1 = \overline{a_1}\ \overline{a_2} \dots \overline{a_k}\ \overline{0}$

b) ---

DIVISIONE EUCLIDEA

$23 : 5 = 4$ resto 3 (?)

$23 = 5 \cdot 4 + 3$

a, b interi positivi, e $b \neq 0$, allora

$\exists!\ q, r$ t.c.

$a = bq + r, \qquad 0 \leq r \leq b-1$

$3 \mid 12$ ("3 divide 12")

$a \mid b \iff b = ka$ per qualche k intero

- $d \mid a,\ d \mid b \longrightarrow d \mid ka + hb$

  $a = md,\ b = nd$
  $a + b = (m+n)d$

- $d \mid a \implies |d| \leq |a|$

- $a - b \mid a^n - b^n \qquad \forall a, b, n$

$$\frac{a^n - b^n}{a - b} = a^{n-1} + a^{n-2} \cdot b + \dots + b^{n-1}$$

- $a + b \mid a^n + b^n$ (n dispari)

Def. Un numero p e' primo se:

- $p = ab \longrightarrow a = \pm 1$ o $b = \pm 1$ (irriduc.)
- $p \mid ab \quad \begin{matrix} \nearrow p \mid a \\ \searrow p \mid b \end{matrix} \qquad \begin{pmatrix} 5 \mid 4 \cdot \underline{5} \\ 10 \mid 8 \cdot 5 \end{pmatrix}$

Es $2^n - 1^n$ e' primo, allora n e' primo.

Dim Diciamo che n non sia primo, $n = a \cdot b$
$a > 1$, $b > 1$

$$\underset{\substack{\shortparallel \\ X}}{X - 1} \;\Big|\; (2^a)^b - 1^b \leftarrow \text{primo}$$

$X - 1 \neq 1 \qquad 2^a \neq 2 \qquad$ si! (perche' $a \neq 1$)

Es $2^n + 1$ e' primo $\longrightarrow n = 2^k$

Dim Supp. di no. Allora $\exists\, p \neq 2$, $p \mid n$

$n = pb$

$$\underbrace{2^b + 1}_{\neq 1} \;\Big|\; (2^b)^p + 1^p \qquad (p \text{ dispari})$$

$2^b + 1 \neq 1$; $\quad 2^b + 1 \neq 2^{bp} + 1 \quad$ (ok)

Teo (Fattorizz. unica) Ogni intero > 1 si scrive in modo unico come prodotto di numeri primi

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$$

$\alpha_1 = v_{p_1}(n)$ "Valutazione p_1-adica"

- $v_p(a \cdot b) = v_p(a) + v_p(b)$
- $v_p(a) < v_p(b) \longrightarrow v_p(a+b) = v_p(a)$

$$a = p_1^{c} \cdot q \qquad b = p_1^{c} \cdot (p_1^{d} \cdot r)$$

$$a + b = p_1^{c} (\underbrace{q + r \cdot p_1^{d}}_{\text{NON è divisib. per } p_1})$$

MCD e mcm

Dati due numeri a, b il $MCD(a,b) =$

$= (a,b)$ è

- il max tra i d che dividono sia a che b
- un numero d t.c. $d \mid a$, $d \mid b$ e se $c \mid a$, $c \mid b$ allora $c \mid d$

$$a \cdot b = (a,b) \cdot mcm(a,b)$$

$(a,b) = (a - hb, b)$ per ogni h.

$d \mid a,\ d \mid b \longrightarrow d \mid a - hb$

$d \mid (a-hb)+hb \longleftarrow d \mid a - hb,\ d \mid b$

$(20, 15) = (20-15, 15) = (5, 15) = 5$

$(64, 13) =$ $\qquad 64 = 13 \cdot 4 + 12$

$= (\underline{64 - 13 \cdot 4}, 13) = (12, 13) = (12, 13-12)$

$= (12, 1) = 1$

$\quad\; \| \quad (12-12, 1)$

Algoritmo di Euclide

Il resto è < divisore. Il minore dei due decresce ad ogni passo.

$(0, m) = m$

Teorema di Bézout Se a, b sono interi, esistono h, k t.c. $h \cdot a + k \cdot b = (a,b)$

$(a|b \rightarrow |a| \leq |b|)$

Dim $(23, 15) = 1$

$23 = 15 \cdot 1 + 8$

$15 = 8 \cdot 1 + 7$

$8 = 7 \cdot 1 + 1$

$7 = 7 \cdot 1 + 0$ /

$23a + 15b = 1$

$1 = 2 \cdot 23 - 3 \cdot 15$

$1 = (23 - 15) - (15 - 23 + 15)$

$1 = 8 - (15 - 8)$

$1 = 8 - 7$

In generale, $a_1, \dots, a_n$ sono interi,

$$(a_1, \dots, a_n) = h_1 a_1 + h_2 a_2 + \dots + h_n a_n$$

IMO 1959/1) $\dfrac{21n+4}{14n+3}$ è sempre irriduc.

Sol. $(21n+4, 14n+3) = (21n+4-14n-3, 14n+3)$

$= (7n+1, 14n+3) = (14n+3-2\cdot(7n+1), 7n+1) =$

$= (1, 7n+1) = 1$

Es $d_n = \text{mcd}(n^2+100, (n+1)^2+100)$.

Max d_n?

Dim $(n^2+2n+1+100-(n^2+100), n^2+100) =$

$= (\underbrace{2n+1}_{\text{dispari}}, 2(n^2+100)) = (2n^2+200-n(2n+1), 2n+1)$

$= (200-n, 2n+1) =$

$= (2n+1+2\cdot(200-n), 200-n) =$

$= (401, 200-n) \to 1, \ 401$

$n = 200 \qquad n = 200+401$

Def. a, b si chiamano "coprimi" $(a,b)=1$

CONGRUENZE

Fissato m, "lavoriamo mod m"

$$580 \equiv 4 \quad (12) \qquad (\text{mod } 12)$$

$\uparrow$ "congruo"

$$\overline{abcd} = a\cdot 10^3 + b\cdot 10^2 + c\cdot 10^1 + d\cdot 10^0 \equiv a\cdot(1)^3 + b\cdot 1^2 + c\cdot 1 + d \ (9)$$

$$a\cdot b = c \quad \Longrightarrow \quad a\cdot b \equiv c \ (9)$$

$$3x + 9y = 2 \qquad \text{mod } 3$$

$$0 + 0 \equiv 2 \ (3) \qquad \underline{\underline{\text{NO}}}$$

IMO 2009/1) $a_1, \ldots, a_k$ sono interi distinti presi in $\{1, \ldots, n\}$ t.c. $n \mid a_i \cdot (a_{i+1} - 1)$.
$i = 1, \ldots, k-1$

Dim. che $n \nmid a_k (a_1 - 1)$

<u>Dim</u> $n \mid a_1(a_2 - 1) \iff a_1 a_2 \equiv a_1 \ (n) \qquad (i)$

$$a_2 a_3 \equiv a_2 \ (n) \qquad (ii)$$

$$\vdots$$

$$a_1 a_3 \overset{(i)}{\equiv} a_1(a_2 a_3) \overset{(ii)}{\equiv} a_1 a_2 \overset{(i)}{\equiv} a_1 \quad (\text{mod } n)$$

$\cdot\, a_4$

$$a_1 a_4 \equiv a_1 a_3 a_4 \overset{(iii)}{\equiv} a_1 a_3 \equiv a_1$$

Per induz., $a_1 a_m \equiv a_1 \ (\text{mod } n) \quad m = 1, 2, \ldots, k$

Tesi: $a_1 a_k \not\equiv a_k \pmod n$

Supponiamo falsa la tesi. Allora $\begin{cases} a_1 a_k \equiv a_k \ (n) \\ a_1 a_k \equiv a_1 \ (n) \end{cases}$

$a_k \equiv a_1 \ (n) \longrightarrow n \mid a_1 - a_k$

$|n| \leq |a_1 - a_k| \longrightarrow a_1 = a_k$

<u>Es</u> $\dfrac{n^2+3n-2}{n+11}$ e' intero? $(*)$

$$= \frac{(n+11)(n-8)+86}{n+11}$$

$$\begin{array}{l|l} n^2+3n-2 & n+11 \\ \cline{2-2} n^2+11n & n-8 \\ \quad -8n-2 & \\ \quad -8n-88 & \\ \cline{1-1} \qquad 86 & \end{array}$$

SSe $86/(n+11)$ e' intero

$(*) \iff n+11 \mid n^2+3n-2 \iff n^2+3n-2 \equiv 0 \ (n+11)$

$$(\underbrace{n+11}_{\equiv 0}-11)^2+3(\underbrace{n+11}_{\equiv 0}-11)-2 \equiv 0 \ (n+11)$$

$$11^2-3\cdot 11-2 \equiv 0 \ (n+11)$$

$$86 \equiv 0 \ (n+11)$$

$\begin{cases} a \equiv b \pmod m \\ c \equiv d \pmod m \end{cases} \longrightarrow \begin{array}{l} a+c \equiv b+d \pmod m \\ a\cdot c \equiv b\cdot d \pmod m \end{array}$

$4 \equiv 10 \pmod 6$

$2 \equiv 5 \pmod 6$ <u>NO</u>!

$4 - 10 = 6k$

$2 - 5 = 3k \qquad 2 \equiv 5 \ (3)$

$15 \equiv 5 \ (10)$

$3 \equiv 1 \ (2)$

$2 \equiv 24 \ (11) \qquad 2 \cdot 6 \equiv 1 \ (11)$

$2 \equiv 2 \cdot 12 \ (11)$

$1 \cdot 2 \equiv 2^{1} \cdot 12 \ (11)$

$1 \equiv 12 \ (11)$

Quando esiste l'inverso?

Fissato a, so risolvere $a \cdot x \equiv 1 \pmod m$

se e solo se $(a, m) = 1$

Supp. che $(a, m) = 1$. $\qquad h \cdot a + k \cdot m = 1$

$h \cdot a \equiv 1 \pmod m$

Supp. di saper risolvere $a \cdot x \equiv 1 \ (m)$.

$1 = a \cdot x + h \cdot m$

$d \mid a,\ d \mid m \longrightarrow d \mid 1 \Rightarrow (a, m) = 1$

Modulo i primi? Sia p primo. a si inverte mod p $\Leftrightarrow$ $(a, p) = 1$

- a è multiplo di p, ma allora $a \equiv 0\ (p)$
- a NON è mult. di p, e allora si inverte

$5 \cdot 3x \equiv 1 \cdot 5\ (7)$

$x \equiv 5\ (7)$

$\frac{1}{2} - \frac{1}{3} \equiv \frac{1}{6} \quad (\mathrm{mod}\ p) \qquad p \neq 2, 3$

$\left(\underset{a}{\tfrac{1}{2}} - \underset{b}{\tfrac{1}{3}} - \underset{c}{\tfrac{1}{6}}\right) \equiv 0\ (p) \iff 3 - 2 - 1 \equiv 0\ (p)$

$a - b - c \equiv 0\ (p) \iff 6(a-b-c) \equiv 0\ (p)$

Mod m "rappr. privilegiati" $\to \{0, 1, \dots, m-1\}$

$\to \left\{\text{"}-\frac{m}{2}\text{"}, -\frac{m}{2}+1, \dots, 0, \dots, \text{"}+\frac{m}{2}\text{"}\right\}$

Mod 7 $\{0, 1, 2, \dots, 6\} \cdot 3$

$= \{0, 3, 6, 2, 5, 1, 4\}$

$x \not\equiv y \qquad 3x \equiv 3y \quad (7) \qquad$ <u>NO</u>

$\Downarrow$

$x \equiv y$

Mod m, moltiplicare per a dove $1 = (a, m)$ è una funzione bigettiva (perché è <u>iniett.</u>)

Questo ci dice che $\exists$ una soluz. all'eq.

$\underline{a \cdot x \equiv 1\ (\mathrm{mod}\ m)}$

$\Downarrow$

$a \cdot x = 1 + hm$

$$1 = a \cdot \overset{\downarrow}{x} - h \cdot m \quad (\text{Bézout})$$

$$ax \equiv ay \ (m) \iff m \mid ax - ay$$

$$\iff m \mid a(x-y) \iff m \mid x-y$$

NO FATTORI COMUNI

$$\Updownarrow$$

$$x \equiv y \ (m)$$

Struttura moltiplicativa

$$x \longmapsto ax$$

$$x \longmapsto x^a \quad ??$$

Mod p: $\nearrow$ $x \equiv 0 \ (p)$, allora $x^1 \equiv x^2 \equiv x^n \equiv 0 \ (p)$

$\searrow$ $x^1, x^2, x^3, \ldots, x^p, x^{p+1} \ldots$

$$\exists\, a, b \ \text{ t.c. } \ x^a \equiv x^b \ (p) \quad (\text{PIGEONHOLE})$$

$b > a$

$$\underbrace{(x^{-1})^a x^a}_{1 \equiv x^{-1} \cdot x \cdot x^{-1} \cdot x \cdot \ldots} \equiv (x^{-1})^a x^b \ (p)$$

$$\equiv x^{b-a} \ (\text{mod } p)$$

Per ogni $x \not\equiv 0 \ (p)$, $\exists\, c > 0$ t.c. $x^c \equiv 1 \ (\text{mod } p)$.

Def. L' "ordine" (moltiplicativo) di x mod p

$=$ il più piccolo $c > 0$ t.c. $x^c \equiv 1 \ (p)$

$$c = \text{ord}_p(x)$$

Supponiamo che $x^d \equiv 1 \ (p)$. Dico che $c \mid d$.

$$\begin{cases} x^d \equiv 1 \quad (p) \\ x^c \equiv 1 \quad (p) \end{cases} \qquad d = k \cdot c + r, \quad 0 \leq r \leq c-1$$

$$x^{c\cdot k + r} \equiv 1 \ (p) \longrightarrow (\underbrace{x^c}_{\equiv 1})^k \cdot x^r \equiv 1 \ (p)$$

$$\longrightarrow x^r \equiv 1 \ (p), \quad \text{con} \quad r < c \implies \boxed{r = 0}$$

Piccolo Teorema di Fermat

$$a^p \equiv a \ (p) \quad \begin{cases} a \equiv 0 \ (p) \\ a \not\equiv 0 \quad a^{p-1} \equiv 1 \ (p) \end{cases}$$

$$\operatorname{ord}_p(a) \mid (p-1) \qquad a^y \equiv 1 \ (p) \qquad \operatorname{ord}_p(a) \mid y$$

Dim 1. Per induzione su a.

$*$ $a = 0$, $a = 1$ ok

$*$ $(a+1)^p \equiv \sum_{n=0}^{p} \binom{p}{n} a^n \equiv \binom{p}{0} a^0 + \binom{p}{p} a^p \overset{\text{ip. ind.}}{\equiv} 1 + a \pmod p$

$\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1} \equiv 0 \ (p)$

$\dfrac{p!}{n!(p-n)!}$ ← 1 fattore p ; ↖ no fattori p

2. $\{1, 2, \ldots, p-1\}$ $\qquad \underbrace{\{a, 2a, 3a, \ldots, (p-1)a\}}$

permutazione di $\{1, 2, \ldots, p-1\}$
perché $(a, p) = 1$.

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \quad (p)$$

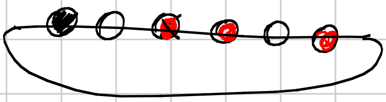
$$(p-1)! \equiv a^{p-1} \cdot (p-1)! \pmod p$$

$(p-1)! \not\equiv 0 \ (p)$

$1 \equiv a^{p-1} \pmod p$

$a \equiv a^{p} \pmod p$

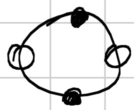
3. Collane con p perline di a colori



Collane aperte $= a^p$

* Collana monocromatica ($\to$ sono a)
* " NON monocrom. ($\to$ sono $a^p - a$) APERTE

Sono $\frac{a^p-a}{p}$.



Se ruotandola di d scatti torna uguale, anche $2d$, $3d$ ... $kd = p \to d \mid p$ $\to d=1$, $\to d=p$

$\underbrace{\frac{a^p-a}{p}}_{\text{intero}}$ collane non mon. chiuse

$\Updownarrow$

$p \mid a^p - a \iff a^p - a \equiv 0 \ (p)$ ∎

Teo. Wilson $(p-1)! \equiv -1 \pmod p$

Mod 7 $\quad 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$

Mod p $\quad 1 \cdot \underbrace{2 \cdot 3 \cdot \ldots \cdot (p-2)}_{1} \underset{\Uparrow}{(p-1)} \equiv -1 \ (p)$

1 e -1 sono gli unici numeri t.c. $a^{-1} \equiv a \ (p)$

$\Rightarrow \quad 1 \equiv a^2 \ (p) \quad \Leftrightarrow \quad (a+1)(a-1) \equiv 0 \ (p)$

$a+1 \equiv 0 \ (p) \qquad a-1 \equiv 0 \ (p)$

Es $\quad \{ p^4 - q^4 \}$ con p, q primi di almeno 2 cifre

$p, q > 10$

Quanto è mcd di tutti?

Svolg. $\quad a = \ .$ Quali fattori primi ha a?

Dico che in a NON compaiono primi > 10.
Diciamo che $r \mid a$, $r \geq 10$, primo.

$a \mid r, \quad a \mid p^4 - r^4 \longrightarrow a \mid p^4 \quad \forall p$

$\longrightarrow a = 1 \quad$ (NO)

$p^4 - q^4 \equiv 0 \quad (2) \longrightarrow 2 \mid a \quad (a \geq 2)$

$p^4 - q^4 \equiv (p^2)^2 - (q^2)^2 \overset{FLT}{\equiv} 1^2 - 1^2 \equiv 0 \quad (3)$

$a^{p-1} \equiv 1 \ (p) \qquad a^2 \equiv 1 \ (3)$

$p^4 - q^4 \overset{FLT}{\equiv} 1 - 1 \equiv 0 \quad (5)$

$13^4 - 11^4 = 3 \cdot 5 \cdot 29 \cdot 2^5 \qquad$ (7 NON c'è)

$p^4 - q^4 \equiv 0 \quad (2^4) \qquad p^4 \equiv 1 \quad (16)$

$p^2 \equiv 1 \quad (8) \qquad 1^2 \equiv 1 \ (8) \quad 5^2 \equiv (-3)^2 \equiv 9 \equiv 1 \ (8)$

$3^2 \equiv 1 \ (8) \quad 7^2 \equiv (-1)^2 \equiv 1 \ (8)$

$$p^2 = 1 + 8k \Rightarrow p^4 = (1+8k)^2 =$$
$$= 1 + 16k + 64k^2 \equiv 1 \ (16)$$

$17^4 - 11^4 = 2^4 \cdot$ dispari

$a = 2^4 \cdot 3 \cdot 5$

Residui quadratici. Quando è che $x^2 \equiv a$ ha soluzioni mod p?

3 è $\sqrt{2}$ mod 7 $\qquad 3^2 \equiv 2 \ (7)$

$x^2 \equiv 6 \ (7)$ $\qquad 4^2 \equiv (-3)^2 \equiv 2 \ (7)$

$5^2 \equiv (-1)^2 \equiv 1 \ (7)$

Mod 3: $x^2 \to 0 \ (x \equiv 0)$, $x^2 \to 1 \ (x \not\equiv 0)$

$$3x^2 + 2 = y^2$$
$$\downarrow$$
$$2 \equiv y^2 \ (3) \quad \text{IMPOSSIBILE}$$

Mod 4: $0^2 \equiv 0$, $2^2 \equiv 0$, $1^2 \equiv 1$, $3^2 \equiv 1$ (mod 4)

$\exists$ 2006 2006 ... 2006 che siano quadrati?

$\equiv$ 06 $\equiv 2 \ (4)$

Mod 8: $0^2 \equiv 0$, $2^2 \equiv 4$, $4^2 \equiv 0$, $6^2 \equiv 4 \ (8)$

$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \ (8)$

$$x^2 \equiv (-x)^2 \qquad a^2 \equiv b^2 \pmod m$$
$$\downarrow ?$$
$$a \equiv \pm b$$

$$a^2 \equiv b^2 \pmod p \iff (a-b)(a+b) \equiv 0 \ (p)$$
$$\Updownarrow$$
$$p \mid a-b \qquad p \mid a+b$$
$$a \equiv b \ (p) \qquad a \equiv -b \ (p)$$

Corollario: mod p ci sono $\underbrace{\frac{p-1}{2}}_{\substack{\text{accoppiati} \\ a \leftrightarrows -a}} + \underbrace{1}_{0}$ residui quad.

Es. $15x^2 - 7y^2 = 9$ $\quad x, y$ interi posit.

Dim $\quad -7y^2 \equiv 0 \ (3) \rightarrow y^2 \equiv 0 \ (3) \rightarrow 3 \mid y$

$\quad y^2 \equiv 0 \ (9) \not\Rightarrow 9 \mid y$

$y = 3k. \qquad 15x^2 - 7 \cdot 9 \cdot k^2 = 9$

$$5x^2 - 21k^2 = 3$$

La leggo mod 3 $\rightarrow 5x^2 \equiv 0 \ (3) \rightarrow 3 \mid x$

$x = 3a \qquad 5 \cdot 9 \cdot a^2 - 21k^2 = 3$

$$15a^2 - 7k^2 = 1$$

$$-7k^2 \equiv 1 \ (3)$$

$$-k^2 \equiv 1 \ (3) \rightarrow k^2 \equiv 2 \ (3) \qquad \text{IMPOSS.}$$

Cubi mod 7

$$\begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 1 & -1 & 1 & -1 & -1 \end{array}$$

elevo al cubo

$$x^3 + 2 = 7y^5$$

Leggo mod 7 $\quad x^3 + 2 \equiv 0 \pmod 7$

$$x^3 \equiv 5 \pmod 7 \qquad \underline{\text{NO}}$$

Mod 9 : $\begin{array}{l} 0, 1, -1 \\ 0, 1, -1 \\ 0, 1, -1 \end{array}$

$$(a+3)^3 \equiv a^3 + 3a^2 \cdot 3 + 3 \cdot 9 \cdot a + 27$$

$$\equiv a^3 \pmod 9$$

Quarte potenze: 0 o 1 mod 16

$4^a + 4^b + 4^c$ = un quadrato $= q^2$

1) È simmetrica in $a, b, c \longrightarrow a \le b \le c$

2) $\underbrace{4^a}_{\text{quadr.}} \cdot \underbrace{\left(1 + 4^{b-a} + 4^{c-a}\right)}_{\longrightarrow \text{ quadrato}} = q^2$

$$\text{quadrato} = q^2/2^{2a} = (q/2^a)^2$$

3) $1 + 4^x + 4^y = z^2 \qquad (x \le y)$

$$4^x\left(1+4^{y-x}\right) = z^2 - 1 = (z+1)(z-1)$$

$$\operatorname{mcd}\left(4^x, 1+4^{y-x}\right) = 2^e$$

$\nearrow$ $1+4^{y-x}$ è pari

$\searrow$ $1+4^{y-x}$ è $\equiv 1\ (2)$

- $y = x$ $\qquad$ (Se $x=0$, $1+1+4^y = z^2$, $2 + 2^{2y} = z^2$)
- mcd $=1$

Se mcd $=1$,

Ricaviamo che $z = 2k+1$

$$4^{x-1}\left(1+4^{y-x}\right) = 4k(k+1)$$

$$2^{2x-2} \cdot \left(1+4^{y-x}\right)$$

Dico che serve $1+4^{y-x} \ge 4^{x-1} - 1$.

$4^{x-1} = k \qquad 1+4^{y-x} = k+1$

$$1+4^{y-x} \ge 4^{x-1}$$

$$2+4^{y-x} \geqslant 4^{x-1} \rightarrow \begin{cases} x=1 \\ y \geqslant 2x-1 \end{cases}$$

$y = 2x-1$

$$1+4^x+4^y =$$
$$= 1+4^x+\frac{1}{4}4^{2x} =$$
$$= \left(1+2\cdot 2^{2x-1}+2^{4x-2}\right)$$
$$= \left(1+2^{2x-1}\right)^2$$

$y > 2x-1$ $\quad 1+4^x+4^y < (2^y+1)^2$

$$4^y = (2^y)^2$$

$$\cancel{1}+4^x+\cancel{4^y} < \cancel{1}+\cancel{4^y}+2\cdot 2^y$$

$$2^{2x} < 2^{y+1}$$

<u>Probl.</u> (Cese 1995/6) $x^2 + 615 = 2^y$

<u>Dim.</u> $x^2 \equiv 2^y \pmod 3$

Puo' essere $x \equiv 0\ (3)$? NO

$1 \equiv 2^y\ (3)$ $\quad 1 \equiv (-1)^y\ (3)$

y e' pari! $\quad 2^y = 2^{2z} = a^2$

$a^2 - x^2 = 615$ $\quad x = 59,\ y = \ldots$

$\parallel$

$(a-x)(a+x),$

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

<u>Prob</u> (Cesenatico 1994/2) $y^2 = x^3 + 16$

$y^2 - 16 = x^3$

<u>Dim</u>

$$(y+4)(y-4) = x^3$$

- y dispari

$$(y+4, y-4) = (8, y+4) = 1$$

Allora, siccome sono coprimi, sono entrambi cubi

$$y+4 = a^3, \qquad y-4 = b^3$$

$$a^3 - b^3 = 8$$

$$(a-b)(a^2+ab+b^2) = 8$$

potenze di 2

$a - b = 1 \qquad (b+1)^3 - b^3 = 8 \qquad$ No

$a - b \geq 2 \qquad a^3 = (b+2)^3 > b^3 + 8$

$8 = a^3 - b^3 > 8 \qquad$ No

- y pari $\quad y^2 = x^3 + 16$

Mod 2: x e' pari

Mod 8: $y^2 \equiv x^3 \equiv 0 \ (8) \longrightarrow \underline{y \equiv 0 \ (4)}$

$y = 4k$

$$16(k^2 - 1) = x^3$$

$$4 + v_2(k^2-1) = v_2(x^3) = 3\,v_2(x)$$

$\hookrightarrow$ k e' dispari $= 2m+1$

$$16 \cdot 2m \cdot 2 \cdot (m+1) = x^3$$

$$64\, m(m+1) = x^3$$

cubo

$$\downarrow$$

$m(m+1)$ è un cubo

$m=0,\ k=1,\ y=4 \longrightarrow x=0$

IMO 2006/4) Risolvere $1+2^x+2^{2x+1}=y^2$ negli interi ≥ 0

$x=0 \to y=2$ ✓

<u>Sol.</u> $1 \equiv y^2 \pmod{2^x}$

$$\Downarrow$$

$2^x \mid (y+1)(y-1)$ $\qquad \gcd(y+1,\, y-1) = 2$

$$\overset{\shortparallel}{(2,\ y-1)}$$

$y \equiv \pm 1 \pmod{2^{x-1}}$

Quanto sarà grosso y? • $y \geq 3 \cdot 2^{x-1}$

$$y^2 \geq 9 \cdot 2^{2x-2} = \cancel{2^{2x+1}} + 2^{2x-2} \overset{?}{=} \cancel{2^{2x+1}} + 2^x + 1$$

$9 = 1+2^3$

Se $x \geq 3$, LHS > RHS $\qquad x = 0, 1, 2$

• $y \leq 2^{x-1}$ $\qquad y^2 = 2^{2x-2} \overset{<}{=} 2^{2x+1} + 2^x + 1$ No

Quindi: o $y = 2^{x-1}+1,\ 2 \cdot 2^{x-1} \pm 1,$

$3 \cdot 2^{x-1} - 1$

Test iniziale 13.

x, y interi, $y > x$, $11x + 7y = 2010$

$\min(y - x)$.

$2 \cdot 11 - 7 \cdot 3 = 1$ $\qquad$ $2 \cdot 2010 = x_0$

$-3 \cdot 2010 = y_0$

$x = x_0 + a, \quad y = y_0 + b$

$$\underbrace{11x_0} + 11a + \underbrace{7y_0} + 7b = \underbrace{2010}$$

$11a + 7b = 0$ $\qquad$ $a = -7k$, $b = +11k$ $\qquad$ k intero

$-3 \cdot 2010 + 11k - 2 \cdot 2010 + 7k = y - x$

$-5 \cdot 2010 + 18k = y - x \equiv -5 \cdot 2010 \pmod{18}$

$\equiv -150 \equiv 30 \equiv 12 \quad (18)$

Teoria dei Numeri 2 - Basic

DARKCRYSTAL

Titolo nota 08/09/2010

$$\begin{cases} x \equiv 0 \ (m_1) \\ x \equiv 0 \ (m_2) \end{cases}, \quad (m_1, m_2) = 1$$

$$m_1 \mid x, \quad m_2 \mid x \implies m_1 m_2 \mid x$$

$$x \equiv 0 \ (m_1 \cdot m_2) \qquad a \equiv b \ (m_1 \cdot m_2)$$

$$\Updownarrow$$

$$m_1 \cdot m_2 \mid a - b$$

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \quad e \quad (m_1, m_2) = 1$$

$$\Updownarrow$$

$$x \equiv a \pmod{m_1 \cdot m_2}$$

$$x = a + k \cdot m_1 \cdot m_2$$

Teorema Cinese del Resto

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \quad e \quad (m_1, m_2) = 1$$

$$x = a_1 + h m_1, \qquad x = a_2 + k \cdot m_2$$

$$a_1 + h m_1 = a_2 + k \cdot m_2$$

$$a_1 - a_2 = k \cdot m_2 - h \cdot m_1 \qquad (A)$$

$c \cdot m_2 - d \cdot m_1 = 1$ (Bézout)

$c \cdot (a_1 - a_2)$, $d \cdot (a_1 - a_2)$

(k_0, h_0) soluz di ⊛

$k = k_0 + \overline{x}$, $h = h_0 + y$

$m_2 \cdot \overline{x} - m_1 \cdot y = 0 \to m_2 \mid y$, $m_1 \mid \overline{x}$

$$X = \underbrace{a_1 + m_1 h_0} + \underbrace{m_1 y}_{\text{divisibile per } m_1 \cdot m_2}$$

Come trovo esplicit. le soluz?

$$\begin{cases} X \equiv a_1 \ (m_1) \\ X \equiv a_2 \ (m_2) \end{cases} \qquad X = A \cdot m_1 + B m_2$$

$$\begin{cases} \cancel{A \cdot m_1} + B m_2 \equiv a_1 \ (m_1) \\ A \cdot m_1 + \cancel{B \cdot m_2} \equiv a_2 \ (m_2) \end{cases} \qquad B \equiv m_2^{-1} \cdot a_1 \ (m_1)$$

$$\begin{cases} X \equiv 3 \ (7) \\ X \equiv 2 \ (5) \end{cases} \qquad X = 7A + 5B$$

$$\Updownarrow$$

$$X \equiv 17 \ (35) \qquad \begin{cases} 5B \equiv 3 \ (7) \\ 7A \equiv 2 \ (5) \end{cases} \qquad \begin{cases} B \equiv 9 \equiv 2 \ (7) \\ A \equiv 1 \ (5) \end{cases}$$

$X = 7 + 10 = 17$

B è scelto a meno di multipli di 7, $5B$ a meno di multipli di 35.

$$\begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \\ \vdots \\ x \equiv a_n \ (m_n) \end{cases} \qquad x \equiv b_1 \ (m_1 \cdot m_2)$$

con gli m a due a due coprimi.

$$\Updownarrow$$

$$x \equiv a \ (m_1 \cdot m_2 \cdot \ldots \cdot m_n)$$

$$X = A\, m_2 m_3 \ldots m_n + B\, m_1 m_3 \ldots m_n + \ldots$$

$$\begin{cases} X \equiv 5 \ (20) \\ X \equiv 6 \ (30) \end{cases} \xrightarrow{\text{TCR}} \begin{cases} X \equiv 0 \ (5) \\ X \equiv 1 \ (4) \\ x \equiv 0 \ (2) \\ x \equiv 0 \ (3) \\ x \equiv 1 \ (5) \end{cases}$$

IMPOSSIBILE

$$\begin{cases} x \equiv 4 \ (20) \\ X \equiv 14 \ (30) \end{cases} \xrightarrow{\text{TCR}} \begin{cases} X \equiv 0 \ (4) \\ X \equiv 4 \ (5) \\ \cancel{X \equiv 0 \ (2)} \\ X \equiv 2 \ (3) \\ \cancel{X \equiv 4 \ (5)} \end{cases} \longleftrightarrow X \equiv 44 \ (60)$$

Esercizi

1) Esistono 2010 interi consecutivi di cui il prim[o] è divis. per 2^2, il secondo $\equiv 0 \ (3^3)$, il terzo $\equiv 0 \ (5^5)$, ...

$$\begin{cases} n \equiv 0 \ (4) \\ n+1 \equiv 0 \ (3^3) \\ n+2 \equiv 0 \ (5^5) \\ \vdots \end{cases} \longleftrightarrow \begin{cases} n \equiv 0 \ (2^2) \\ n \equiv -1 \ (3^3) \\ \vdots \end{cases}$$

Il TCR dice che $\exists$ una soluz., ed è unica mod $2^2 \cdot 3^3 \cdot 5^5 \cdot 7^7 \cdot \ldots$

2) Esistono 2010 interi consec. di cui esattam. 1 è una potenza perfetta.

Supponiamo che $n, n+1, \ldots, n+2009$ che NON sono potenze perfette. $\exists$ il più piccolo intero $m > n+2009$ che è una potenza perfetta.
Ma allora $\underbrace{n, n+1, \ldots, m}_{\text{più di } 2010}$ di cui esatt. 1 è potenza. Scelgo gli ultimi 2010.

Se x è una pot. perfetta, $x \not\equiv p \ (p^2)$ per ogni scelta di p primo.

Se $x \equiv p \ (p^2) \longrightarrow x \equiv p \ (p) \rightarrow p \mid x$.

Allora $p^2 \mid x$, cioè $x \equiv 0 \ (p^2)$.

Scegliamo $p_1, p_2, \ldots, p_{2010}$ primi distinti:

$$\begin{cases} x \equiv p_1 \ (p_1^2) \\ x+1 \equiv p_2 \ (p_2^2) \\ x+2 \equiv p_3 \ (p_3^2) \\ \vdots \end{cases} \xrightarrow{\text{TCR}} \exists \text{ una soluz. } x$$

3) Esiste una progress. aritmetica di lunghezza ℓ, ragione d t.c. ogni elemento e' divisibile per almeno una potenza n-esima

---

φ di Eulero

$$\varphi(n) = \left| \{ 0 < m \le n \ : \ (m,n) = 1 \} \right|$$

$\varphi(1) = 1$. $\quad n = p$ primo? $\quad \varphi(p) = p - 1$

$$\varphi(p^k) = p^k - \frac{p^k}{p} = p^{k-1}(p-1) \qquad k \geq 1$$

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

$$(m,n) = 1 \longrightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

$$\varphi(\underbrace{p_1^{\alpha_1}} \cdot \underbrace{\ldots \cdot p_k^{\alpha_k}}) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}) =$$

$$= \ldots = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k})$$

$$\varphi(40) = \varphi(5) \cdot \varphi(8) = 4 \cdot 2^2 = 16$$

Funzione moltiplicativa $\quad (m,n) = 1 \rightarrow \varphi(m n) = \varphi(m) \cdot \varphi(n)$

Funz. completam. moltipl. $\quad f(m n) = f(m) \cdot f(n)$

$$6 = \varphi(9) \neq \varphi(3) \cdot \varphi(3) = 2 \cdot 2$$

$$X \equiv a \pmod{n \cdot m} \xleftrightarrow{\text{TCR}} \begin{cases} X \equiv a & (m) \\ X \equiv a & (n) \end{cases}$$

Se $1=(a, m \cdot n)$, allora i rappr. priv. saranno coprimi con m, n

$$X \equiv 4 \ (15) \longrightarrow \begin{cases} X \equiv 1 & (3) \\ X \equiv 4 & (5) \end{cases}$$

$$\begin{cases} X \equiv a_1 & (m) \\ X \equiv a_2 & (n) \end{cases} \longrightarrow X \equiv a \ (m \cdot n)$$

Bigezione tra $\varphi(m \cdot n)$ e i sistemi $\begin{cases} X \equiv a_1 & (m) \\ X \equiv a_2 & (n) \end{cases}$

con $(a_1, m) = 1$, $(a_2, n) = 1$, $0 \le a_1 < m$, $0 \le a_2 < n$

$$\varphi(m) \cdot \varphi(n) = \varphi(m \cdot n)$$

$$\varphi(p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}) =$$

$$= p_1^{\alpha_1 - 1}(p_1 - 1) \cdot p_2^{\alpha_2 - 1}(p_2 - 1) \cdot \ldots \cdot p_k^{\alpha_k - 1}(p_k - 1)$$

$$= n \left(\frac{p_1 - 1}{p_1} \right) \left(1 - \frac{1}{p_2} \right) \cdot \ldots \cdot \left(1 - 1/p_k \right)$$

φ di Eulero /2

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - \ldots - \frac{n}{p_k} +$$

$$+ \frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \ldots - \sum \frac{n}{p_i p_j p_k} + \sum \frac{n}{p_i p_j p_k p_l} \ldots$$

(Principio Incl - Esclus.)

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

$$\varphi(m \cdot n) = \underbrace{m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots}\ \cdot$$

$$\cdot\, \underbrace{n\left(1-\frac{1}{q_1}\right)\left(1-1/q_2\right)\cdots\left(1-1/q_k\right)}$$

$$= \varphi(m)\cdot\varphi(n)$$

$$\sum_{d|n}\varphi(d) = n$$

$$n = p^m \qquad \sum_{k=0}^{m}\varphi(p^k) = \varphi(1) + \sum_{k=1}^{m}(p-1)p^{k-1} =$$

$$= 1 + (p-1)\left(1+p+p^2+\dots+p^{m-1}\right) =$$

$$= 1 + \cancel{(p-1)}\,\frac{p^m-1}{\cancel{p-1}} = p^m = n$$

$$g(n) = \sum_{d|n}\varphi(d)$$ Hope: e' moltiplicativa?

$$g(p^k) = p^k \qquad g(n) = g(p_1^{\alpha_1})\cdot\ \dots\ \cdot g(p_k^{\alpha_k}) =$$

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

$$(m, n) = 1 \qquad g(m \cdot n) = \sum_{d \mid m \cdot n} \varphi(d) =$$

$$= \sum_{\substack{a \cdot b \mid m \cdot n \\ a \mid m \\ b \mid n}} \varphi(ab) = \sum_{a,b} \varphi(a)\varphi(b) =$$

$$= \sum_{a \mid m} \left[\sum_{b \mid n} \varphi(a)\, \varphi(b) \right] =$$

$$= \sum_{a \mid m} \left(\varphi(a) \sum_{b \mid n} \varphi(b) \right) = \left(\sum_{b \mid n} \varphi(b) \right) \left(\sum_{a \mid m} \varphi(a) \right) =$$

$$= g(m)\, g(n)$$

Struttura moltiplicativa mod m

$a^n \mod m$

$a^0, a^1, a^2, \dots, a^m, a^{m+1} \to$ periodica per pigeonhole

$a^k \equiv a^h \pmod m$

$2 = a, \mod 12$

$2, \underbrace{4, 8}, \underbrace{4, 8}, \dots$

1) Non ha un ordine : $\boxed{a^k \not\equiv 1 \ (12)}$

2) Non è periodica.

$$a^n \mod m \longleftrightarrow \begin{cases} a^n & \mod 4 \\ a^n & \mod 3 \end{cases}$$

$1, 2, 0, 0, \dots, 0$

Per quali a $\exists$ k t.c. $a^k \equiv 1 \pmod m$?

Per gli a t.c. $(a, m) = 1$

$a^k = 1 + h \cdot m$

Supponiamo che $(a, m) > 1$. Allora esiste $p \mid a$, $p \mid m$. Allora $p \mid a^k - h \cdot m = 1$

Viceversa, se $(a, m) = 1$, allora $a^h \equiv a^k \pmod m$

$$h < k \rightarrow \underbrace{(a^{-1})^h a^h}_{\equiv 1} \equiv a^{k-h} \pmod m$$

FLT (primi): $(a, p) = 1$ $\quad a^{p-1} \equiv 1 \ (p)$

Teorema di Eulero – Fermat Se $(a, m) = 1$, allora

$$a^{\varphi(m)} \equiv 1 \pmod m$$

$$\{1, a_2, a_3, \ldots, a_{\varphi(m)}\} = A$$

mod 8 : $\{1, 3, 5, 7\}$

$$\{1x, a_2 x, a_3 x, \ldots, a_{\varphi(m)} x\} = B \quad \text{se } (x, m) = 1$$

$$a_h x \equiv a_k x \pmod m \rightarrow a_h \equiv a_k \ (m)$$

$$\underbrace{1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_{\varphi(m)}}_{Z} \equiv (1x)(a_2 x) \ldots (a_{\varphi(m)} x) \quad (m)$$

$$Z \equiv Z \cdot x^{\varphi(m)} \pmod m$$

$$1 \equiv x^{\varphi(m)} \pmod m$$

Def $\operatorname{ord}_m(x)$ = min. intero positivo k t.c. $x^k \equiv 1 \pmod m$

$$\boxed{\mathrm{ord}_m(x) \mid \varphi(m)}$$

$$\mathrm{ord}_m(x) \leq \varphi(m) \leq m$$

Generatori Un generatore mod m e' un g t.c. $\mathrm{ord}_m(g) = \varphi(m)$

$\underbrace{g^1, g^2, \dots, g^{\varphi(m)}}_{\varphi(m) \text{ residui}}$ sono tutti distinti

coprimi con m

Mod 5 $\quad 2, 4, 3, 1$ generatore!

$4, 1$ NO

Teo Esiste un generatore se e solo se m e' uno tra $2, 4, p^n, 2p^n$ con p primo dispari

Mod 8 non esiste un generatore, perché

$$a^2 \equiv 1 \pmod 8 \qquad (a, 2) = 1$$

Se g fosse gener. mod 16, g^k genererebbe tutto mod 16 $\Rightarrow$ genererebbe tutto mod 8

Generatori mod p. $\operatorname{ord}(g) = p-1$.

$g^{p-1} \equiv 1 \ (p)$ (inutile)

$\operatorname{ord}_p(g) \mid p-1$. $g^m \not\equiv 1 \ (p)$ se $m < p-1$

$p-1 = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot \ldots \cdot q_k^{\alpha_k}$

$q_1^{\beta_1} \cdot \ldots \cdot q_k^{\beta_k}$ con almeno 1 $\beta < \alpha$.

Basta provare che $g^{\frac{p-1}{q}} \not\equiv 1 \ (p)$, per $q \mid p-1$.

$p = 19$, $p-1 = 18$ $g^{18} \equiv 1 \ (19)$

$1, 2, 3, 6, 9, 18$ $\frac{18}{9}$ $\frac{18}{3}$

Sia g gener. mod p. Allora

- o g o $g+p$ e' generatore mod p^2
- se h e' gener. mod p^2, allora e' generatore mod p^n per ogni n (p disp)

. $\operatorname{ord}_p g = p-1$ $g^{p-1} = 1 + kp$

Gener. mod p^2 ha ordine $\varphi(p^2) = p(p-1)$

$\operatorname{ord}_{p^2}(g)$ $g^h \equiv 1 \ (p^2) \to g^h \equiv 1 \ (p)$

$$\underset{\substack{\parallel \\ p-1}}{\operatorname{ord}_p g} \mid \operatorname{ord}_{p^2}(g) \mid p \cdot (p-1) = \varphi(p^2)$$

$$\operatorname{ord}_{p^2}(g) \begin{cases} \to p-1 & (1) \\ \to p\cdot(p-1) & \underline{\text{ok}} \end{cases}$$

(1) $g^{p-1} \equiv 1 \ (p^2) \longrightarrow g^{p-1} = 1 + h\cdot p^2$

$(g+p) \equiv g \ (p)$, $g+p$ e' un gen mod p

$\to p-1 \mid \operatorname{ord}_{p^2}(g+p) \mid p(p-1)$

$$(g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}\cdot p + p^2(\dots)$$

$$= 1 - p\cdot g^{p-2} + \cancel{p^2(\dots)}$$

$$\not\equiv 1 \quad (p^2)$$

$p\cdot g^{p-2} \not\equiv 0 \ (p^2)$

$\operatorname{ord}_{p^2}(g+p)$ e' $p(p-1)$, cioe' $g+p$ genera

Quando e' che -1 e' un residuo quadrat? (mod p)

$\Longleftrightarrow$ esiste a che risolve $a^2 \equiv -1 \ (p)$

$\Longrightarrow \quad a^4 \equiv 1 \ (p) \qquad \mathrm{ord}_p(a) = 4$

$\mathrm{ord} = 4 \mid \varphi(p) = p-1 \quad \Longrightarrow \quad p \equiv 1 \ (4)$ (NECESS.)

Sia $p \equiv 1 \ (4)$ e sia g un gener.

$a = g^{\frac{p-1}{4}} \qquad a^4 \equiv g^{p-1} \equiv 1 \ (p)$

$(a^2)^2 \equiv 1 \ (p), \qquad a^2 \equiv g^{\frac{p-1}{2}} \not\equiv 1 \ (p)$

$\downarrow$

$(a^2-1)(a^2+1) \equiv 0 \ (p) \rightarrow a^2+1 \equiv 0 \ (p)$

$\rightarrow a^2 \equiv -1 \ (p)$

Quanti sono i generatori?

Tutti i residui si scrivono $g, g^2, g^3, \dots, g^{p-1}$

g^k e' ancora un generatore?

Sia $a = \mathrm{ord}_p(g^k)$. $\quad g^{ak} \equiv 1 \ (p)$

$\Longleftrightarrow p-1 \mid ak$. Se $(k, p-1) = 1$,

allora $\searrow \ p-1 \mid a \mid p-1 \Longrightarrow a = p-1$

g^k è ancora generatore se $\boxed{(k, p-1) = 1}$

Se invece $(k, p-1) = b > 1$, allora

$$(g^k)^{\frac{p-1}{b}} = g^{(k/b)\cdot(p-1)} \equiv 1 \ (p)$$

ma $\frac{p-1}{b} < p-1$

I generatori sono $\varphi(p-1) = \varphi(\varphi(p))$.

Esercizi

1) È vero che $37 \mid 2^{17} - 1$?

Se fosse vero, $2^{17} \equiv 1 \ (37)$

$2^{36} \equiv 1 \ (37)$

$\mathrm{ord}_{37}(2) \ \begin{matrix} \mid 17 \\ \mid 36 \end{matrix} \longrightarrow \mathrm{ord}_{37}(2) = 1$

$\longrightarrow 2^1 \equiv 1 \ (37)$ NO

2) $X \equiv 1432^{1432} \bmod 1001 = 7 \cdot 11 \cdot 13$

$1432 \equiv 4 \pmod 6$

$$\downarrow$$

$$\begin{cases} X \equiv 4^{1432} \equiv 4^4 \equiv 4 & (7) \\ X \equiv 2^2 \equiv 4 & (11) \\ X \equiv 2^4 \equiv 3 & (13) \end{cases}$$

$1432 \equiv 4 \pmod{12}$

$$\downarrow$$

$$\begin{cases} X \equiv 4 & (77) \\ X \equiv 3 & (13) \end{cases} \longrightarrow X \equiv 81 \ (1001)$$

3) Le ultime 5 cifre di $x = 5^{5^{5^{5^5}}}$?

$$X \bmod 10^5 \to \bmod 2^5, \quad \to \bmod 5^5$$

$X \bmod 2^5$ $\qquad 5^{16} \equiv 1 \ (32)$

Ci basta $5^{5^{5^5}} \equiv 5^5 \bmod 16 \equiv 5 \bmod 16$

$5^{5^5} \equiv 5^1 \bmod 8$

$5^5 \equiv 1 \bmod 4$

$$\begin{cases} X \equiv 5^5 \bmod (32) \\ X \equiv 0 \equiv 5^5 \bmod 5^5 \end{cases} \qquad X \equiv 03125 \ (100000)$$

4) $\text{Torre}_n(a) = a^{a^{a^{\cdot^{\cdot^{a}}}}} \Big\}$ n volte

$\text{Torre}_n(a)$ e' costante mod m da un certo n in poi.

Idea $\underbrace{\text{Torre}_m(a)}_{\text{cost. mod } m} = a^{\text{torre}_{n-1}(a)]\bmod \varphi(m)}$

Induzione (estesa) su m. Per $m = 1, 2$ ok

Se lo so fare per $\{1, 2, \dots, m-1\}$ come lo faccio per m ?

Dico che $\text{torre}_n(a)$ sarà costante mod $\varphi(m)$

$\Longrightarrow \quad a^{\text{torre}_n(a)}$ è costante mod m

$\Rightarrow \quad \text{torre}_{n+1}(a)$ " " " "

$a^{\varphi(m)} \equiv 1 \pmod m$

$c \equiv d \ (\varphi(m)) \longrightarrow x^c \equiv x^d \ (m)$

$d = c + k\varphi(m) \qquad x^c \equiv x^c \cdot \underbrace{x^{k\varphi(m)}}_{1} \ (m)$

$(m, a) = b \qquad m = c \cdot n$

$\qquad (c, a) = 1$

- La congruenza mod c si fa
- " " " n si fa lo stesso

perché $a^{a^{a^{\cdot^{\cdot^{\cdot^{a}}}}}}$ prima o poi $\equiv 0 \ (n)$

$\text{torre}_n \, a$ è costante sia mod n $(\equiv 0)$ / sia mod c

Esercizi istruttivi

1) Sia $D = \{ n \in \mathbb{N} \mid n \mid 2^n + 1 \}$

a. Trovare primi $p \in D$

$p \mid 2^p + 1 \iff 2^p + 1 \equiv 0 \ (p)$

$\iff 2 + 1 \equiv 0 \ (p) \qquad p \mid 3$

b. Dimostr. che tutti gli elem. di D sono $\equiv 0 \ (3)$

$$n \mid 2^n+1 \iff 2^n+1 \equiv 0 \ (n) \qquad (*)$$

Idea: il più piccolo primo!! $p \mid n$

$$(*) \Rightarrow 2^n+1 \equiv 0 \ (p)$$

$$2^n \equiv -1 \ (p)$$

$$4^n \equiv 1 \ (p) \qquad \begin{cases} \mathrm{ord}_p(4) \mid n \\ \mathrm{ord}_p(4) \mid p-1 \end{cases}$$

$$\Rightarrow \mathrm{ord}_p(4) \mid (n, p-1) = 1 \quad (\text{p.p.p.})$$

$$4^1 \equiv 1 \ (p) \Rightarrow p \mid 3$$

Variante $n \mid 12^n+1$. Allora $13 \mid n$

c) Trova $n = p \cdot q$, $n \in D$.

$$n = 3q$$

$$3q \mid 2^{3q}+1$$

Caso 1: $q = 3$. $\quad 9 \overset{?}{\mid} 2^9+1 = 513$

Caso 2: $q \neq 3$ $\quad \begin{cases} 2^{3q}+1 \equiv 0 & (3) \\ 2^{3q}+1 \equiv 0 & (q) \end{cases}$

$$(-1)^q + 1 \equiv 0 \ (3)$$

$$8^q + 1 \equiv 0 \ (q) \longrightarrow 8 + 1 \equiv 0 \ (q)$$

$$q \mid 9 \to q = 3 \quad (\text{fatto})$$

d) $n = p^2 \cdot q, \quad p \neq q$ primi, $n \in D$

- $p = 3, \quad n = 9q \qquad 2^{9q} \equiv -1 \ (9q)$

$$\begin{cases} 2^{9q} \equiv -1 \ (9) \\ 2^{9q} \equiv -1 \ (q) \end{cases} \qquad \begin{cases} (-1)^q \equiv -1 \ (9) \\ (2^9)^q \equiv -1 \ (q) \end{cases}$$

$$\begin{cases} \text{ok} \\ 512 \equiv -1 \ (q) \end{cases} \qquad q \mid 513 = 9 \cdot 57 = 3^3 \cdot 19$$

$q = 19$

- $n = 3p^2 \qquad 2^{3p^2} \equiv -1 \ (3p^2)$

$$\Downarrow$$

$$2^{3p^2} \equiv -1 \ (p)$$

$$2^{3p^2} = (2^{3p})^p \equiv 2^{3p} \equiv 8^p \equiv 8 \ (p)$$

$$8 \equiv -1 \ (p) \to p = 3$$

e) Trova $n = p^k$, $n \in D$. $\quad n = 3^k$

Claim $\quad 3^k \mid 2^{3^k} + 1$

Induzione su k: $k = 1, 2$

$k \to k+1$: $3^{k+1} \mid 2^{3^{k+1}} + 1$?

$$\left(\underbrace{2^{3^k}}_{A}\right)^3 + 1 = \underbrace{(A+1)}_{3^k}\underbrace{(A^2 - A + 1)}_{\text{devo guad. un } 3}$$

Ip. indutt.: $3^k \mid 2^{3^k} + 1 = A + 1$

$A^2 - A + 1 \equiv 1 - 2 + 1 \equiv 0 \ (3)$

$3^{k+1} \parallel 2^{3^k} + 1 \qquad v_3\left(2^{3^k} + 1\right) = k+1$

2) $\dfrac{a^p - 1}{a - 1}$ con p primo dispari

$*$ $q \mid \dfrac{a^p-1}{a-1} \Longrightarrow q \mid a^p - 1$

$\Longrightarrow a^p \equiv 1 \ (q) \qquad \mathrm{ord}_q(a) \begin{cases} 1 \\ p \end{cases}$

- o $p \mid q - 1 \Rightarrow q \equiv 1 \ (p)$
- o $q \mid a - 1$

$*$ $a^p - 1 = (a-1)\left(\dfrac{a^p - 1}{a - 1}\right)$

$q \mid \mathrm{mcd}\left(a - 1, \dfrac{a^p-1}{a-1}\right)$

$q \mid a - 1, \quad q \mid \dfrac{a^p - 1}{a - 1} = 1 + a + a^2 + \dots + a^{p-1}$

$$a \equiv 1 \ (q)$$

$$\underbrace{1+1+1+\dots+1}_{p \text{ termini}} \equiv 0 \ (q) \qquad p \equiv 0 \ (q)$$

$$\left(a-1, \frac{a^p-1}{a-1}\right) = p^k$$

$$* \quad p \mid a-1 \longrightarrow a = hp+1$$

$$\frac{a^p-1}{a-1} = \frac{(1+hp)^p-1}{hp} = \qquad p \mid \binom{p}{m}$$

$$= \frac{\cancel{1}+\binom{p}{1}hp + h^2p^{2+1}(\dots)\cancel{-1}}{hp} \qquad p \geq 3$$

$$= p + hp^2(\dots) \equiv p \ (\mathrm{mod}\ p^2)$$

$$\Rightarrow \left(a-1, \frac{a^p-1}{a-1}\right) \begin{cases} 1 \\ p \end{cases}$$

$$\frac{a^p-1}{a-1} = p \qquad 1+a+a^2+\dots+a^{p-1} = p$$

Appena $a \geq 2$ $\underline{\text{NO}}$

$a=1$ NON HA SENSO

$$a = -b$$

$$\frac{+b^p+1}{+b+1} = p \qquad p = \frac{b^p+1}{b+1} > \frac{b^p}{b+1} \geq \left(\frac{2}{3}\right) b^{p-1}$$

$$p > (2/3)\, b^{p-1}, \quad \text{con } b \geq 2$$

$\boxed{p=3, \quad b=2}$ $\qquad 2^3+1=3^2$

3) $x^p+1=q^n$ con p, q primi dispari
$n \geq 2$

$$\underset{\parallel}{x^p+1} \qquad (x+1)\left(\frac{x^p+1}{x+1}\right) \qquad x+1=q^a, \quad \frac{x^p+1}{x+1}=q^b$$

- $p=q$
- $\frac{x^p+1}{x+1}$ ha un fattore primo che $x+1$ non ha, a meno $x=2$, $p=3 \to q=3$

$x=0$, $x=1$
$n=0$ NO

Test iniziale. 15) Determinare quale dei seguenti k è residuo quadratico mod 2^{2010}.

k ~~2000~~, ~~2005~~, ~~$\underline{\underline{2010}}$~~, ~~2015~~, 2020

$\equiv 2 (4)$

$$2^{2010} \mid x^2 - 2010 \rightarrow 4 \mid x^2 - 2$$

$$2^{2010} \mid x^2 - 2000 \qquad x = 4m$$

$$2^{2010} \mid 16(m^2 - 125)$$

$$2^{2006} \mid m^2 - 125 \longrightarrow 8 \mid m^2 - 125$$

$$m^2 - 5$$

$$2^{2010} \mid x^2 - 2020 \qquad 2^{2008} \mid x^2 - 505$$

Fatto a è residuo quadratico mod 2^k, $k \geq 3$

$\iff a \equiv 1 \ (8)$

Dim $a = y^2 + 2^k \cdot x \leftarrow$ ("a è un residuo quadr. mod 2^k")

- x è pari $\rightarrow$ ho vinto
- x è dispari.

$k \geq 3$

$$(y + 2^{k-1})^2 \equiv y^2 + 2y \cdot 2^{k-1} + \cancel{2^{2k-2}}$$

$$\equiv a - 2^k \cdot x + y \cdot 2^k \equiv$$

$$\equiv a + 2^k \underbrace{(y - x)}_{\text{fattore } 2} \equiv a \quad (2^{k+1})$$

16) $S_p = \{ n \in \mathbb{N} : n \leq p \text{ e } p \mid n^{35} + 1 \}$

Determinare i possibili valori di $|S_p|$ al variare di p primo ≥ 2010

$$n^{35} + 1 \equiv 0 \ (p) \qquad n = g^k$$

$$g^{35k} + 1 \equiv 0 \ (p)$$

$$g^{35k} \equiv -1 \ (p) \iff 35k \equiv \frac{p-1}{2} \ (p-1)$$

$$\left(g^{\left(\frac{p-1}{2}\right)}\right)^2 \equiv 1 \ (p) \qquad g^{\frac{p-1}{2}} \not\equiv 1 \ (p)$$

$$\Rightarrow g^{\frac{p-1}{2}} \equiv -1 \ (p) \qquad p - 1 = \mathrm{ord}_p(g) \leq \frac{p-1}{2}$$

Contare le soluz. di $35k \equiv \frac{p-1}{2} \ (p-1)$

$$(p-1, 35) \in \{1, 5, 7, 35\}$$

- $(p-1, 35) = 1 \qquad k \equiv (35)^{-1} \left(\frac{p-1}{2}\right) \ (p-1)$

$$g^k = -1$$

- $(p-1, 35) = 5 \qquad 5k \equiv 7^{-1} \cdot \frac{p-1}{2} \ (p-1)$

$$k \equiv 7^{-1} \cdot \frac{p-1}{2 \cdot 5} \ \left(\frac{p-1}{5}\right)$$

$$k_0, \ k_0 + \frac{p-1}{5}, \ k_0 + 2 \cdot \frac{p-1}{5}, \ \ldots, \ k_0 + 4 \cdot \frac{p-1}{5}$$

- $(p-1, 35) = 7 \to 7$ soluz.
- $(p-1, 35) = 35 \to 35$ soluz

$$|S_p| = (p-1, 35)$$

Teo (Dirichlet) Se $(a, b) = 1$, allora esistono infiniti primi della forma $an + b$

$n \cdot 35 + 1 \qquad \varphi(p) = 35 \cdot n$

$35n + 8 \qquad \varphi(p) = 35n + 7 \qquad 7 \mid \varphi(p)$

$5 \nmid \varphi(p)$

Lemmone Sia $q(x)$ è un polinomio di grado al più $p-2$ con p primo.

Allora $q(0) + q(1) + q(2) + \dots + q(p-1) \equiv 0 \ (p)$

Dim Idea: se è vero per i singoli monomi, sommando sui vari monomi lo sappiamo fare per $q(x)$ generico.

$ax \qquad \cancel{a}(1 + 2 + 3 + \dots + p-1) \equiv 0 \quad (p)$

- $\frac{(p-1)p}{2} \equiv 0 \quad (p)$
- $1 + (p-1) + 2 + (p-2) + \dots \equiv 0 \quad (p)$

X^n $\quad 1^n + 2^n + \dots + (p-1)^n \equiv 0 \pmod p$

$$1^n + 2^n + \dots + (p-1)^n \equiv (g^1)^n + (g^2)^n + \dots + (g^{p-1})^n$$

$$\equiv (g^n)^1 + (g^n)^2 + \dots + (g^n)^{p-2} + (g^n)^0 \equiv$$

$y = g^n$ $\quad \equiv y^0 + y^1 + \dots + y^{p-2} \equiv \dfrac{y^{p-1} - 1}{y - 1} \equiv \star$

ATTENZIONE!

Serve $y \neq 1$, per dividere.

$g^n \neq 1 \qquad n \leq p-2$

$\star \equiv (1-1) \cdot (y-1)^{-1} \equiv 0 \pmod p$