Stage Senior 2013 – Livello Basic

Stampato integrale delle lezioni

Autori vari

Indice

P - PRELIMINARI

Titolo nota 01/09/2013

INDUZIONE

$\mathbb{N} = \{0, 1, 2, \dots\}$

$p(n) = $ " ... n ... "

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

per ogni

passo base: $p(0)$ É VERA

passo induttivo: $p(n) \Rightarrow p(n+1)$

ESEMPIO 1 $\quad 1 + \dots + n = \dfrac{n(n+1)}{2}$

ESEMPIO 2 $\quad 1 + 3 + \dots + 2n - 1 = n^2$ $\quad p(n)$

dim.

passo base $\quad 1 = 1$ ok! $\quad p(1)$

passo induttivo $\quad (1 + \dots) + 2n + 1 =$

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

per hp. induttiva $= n^2$

TESI!

ESEMPIO 3 $\quad (1 + x)^n \geq 1 + nx \qquad (x > -1)$

Bernoulli

passo base $\quad 1 \geq 1$ ok! $\quad n = 0$

passo induttivo $\quad (1+x)^n \geq 1 + nx$

hp. ind.

$(1+x)(1+x)^n \geq (1 + nx)(1+x)$

$$(1+x)^{n+1} \geq nx^2 + nx + x + 1$$
è ≥ 0, ok! $\longrightarrow$ $$nx^2 + (n+1)x + 1$$
$$\geq (n+1)x + 1$$
$\rightarrow$ tesi

ESEMPIO 4 $\quad n+1 \leq 2^n \quad \forall n \in \mathbb{N}$

passo base $\quad n = 0 \quad 1 \leq 1$ ok!

passo induttivo $\quad n+2 = (n+1) + 1$
$$\underset{\text{hp. induttiva}}{\leq} 2^n + 1 \leq 2^n + 2^n = 2^{n+1}$$

$\rightarrow$ tesi

parentesi: n + un miliardo $\leq 2^n$ da un certo punto in poi.
prendo un passo base più "avanti"

$n = 10^9 \qquad \cancel{2} \cdot 10^9 \leq 2^{10^9 - 1}$ è vera per $n+1 \leq 2^n$

ESEMPIO 5 $\quad$ ogni naturale si scrive come somma di Fibonacci distinti non consecutivi.

per induzione (estesa)!

passo base + passo induttivo
$p(0) \qquad p(0), p(1), \dots, p(n) \Rightarrow p(n+1)$

passo base: $0 = 0$ ok!
ho n. Prendo il più grande Fibonacci che "ci stia", lo chiamo F_k.

Considero $n - F_k < n$ lo scrivo per hp. induttiva!

$n = F_k + (\dots) \to$ tesi!

→ se F_k compare nella scomp. di $n - F_k$, $n \geq 2F_k$ → potevo prendere $F_k + F_{k-1}$ al posto di F_k.

→ F_{k-1} potrebbe comparire in $n - F_k$. Ma allora in n ci sta $F_k + F_{k-1} = F_{k+1}$.

ESEMPIO 6 $\alpha + \frac{1}{\alpha} \in \mathbb{Q}$ allora $\forall n$ $\underset{\in \mathbb{Q}}{\alpha^n + \frac{1}{\alpha^n}}$.

passo base Ok!

$$\underbrace{\left(\alpha + \frac{1}{\alpha}\right)^2}_{\text{è razionale!}} = \underbrace{\boxed{\alpha^2 + \frac{1}{\alpha^2}}}_{\text{è razionale!}} + \underbrace{2}_{\text{è razionale!}}$$

$$\underbrace{\left(\alpha^2 + \frac{1}{\alpha^2}\right)\left(\alpha + \frac{1}{\alpha}\right)}_{\text{è raz}} = \alpha^3 + \frac{1}{\alpha^3} + \underbrace{\alpha + \frac{1}{\alpha}}_{\text{è raz.}}$$

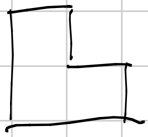
fantastico! Mi basta scrivere

$$\underbrace{\left(\alpha^n + \frac{1}{\alpha^n}\right)\left(\alpha + \frac{1}{\alpha}\right)}_{\in \mathbb{Q} \text{ per hp. induttiva }} = \overbrace{\alpha^{n+1} + \frac{1}{\alpha^{n+1}}}^{\text{tesi } \in \mathbb{Q}} + \underbrace{\left(\alpha^{n-1} + \frac{1}{\alpha^{n-1}}\right)}_{\text{per hp. } \in \mathbb{Q}}$$

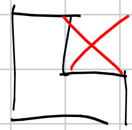
induttiva intera

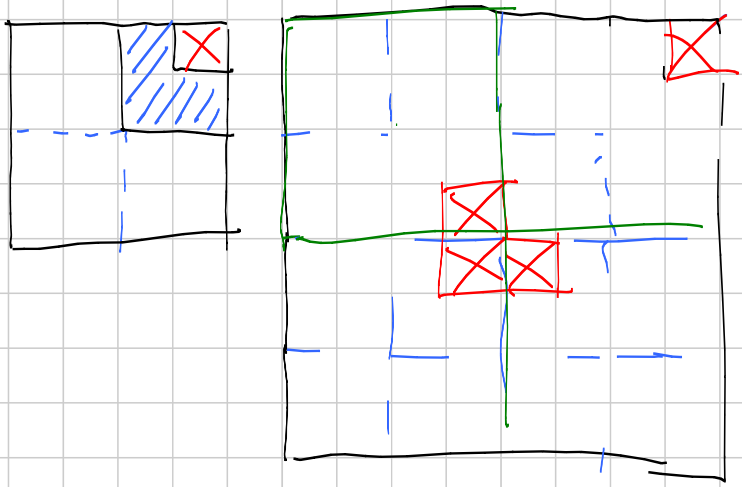
ESEMPIO 7

$2^n \times 2^n$ scacchiera, tolgo angolino. Posso tassellarla con "triomini" a L?



passo base: sì!





passo induttivo!

Attenzione!

tutti quanti hanno gli occhi azzurri.

$\forall n$ prendo n persone $\to$ tutte hanno gli occhi stesso colore

passo base. 1 persona ok.

passo induttivo

prendo gruppo di $n+1$

tolgo 1 $\to$ uso hp. ind sugli altri

tolgo 2 $\to$ "

$\longrightarrow$ vero per $n+1$.

OPS!! $n = 2$

D'altra parte se fosse stato vero per $n = 2$ $\Rightarrow$ vero sempre!

Tutti i fib. sono pari.

0 è pari.
passo base

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

pari pari
hp. induttiva

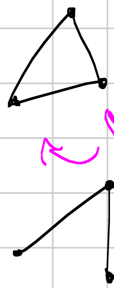
→ tesi!

Dovevo fare i primi due come passo base!

Tutti i grafi per cui ogni vertice ha $\geq$ 1 arco uscente sono connessi!

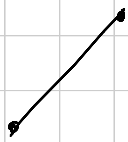
connesso

grafo



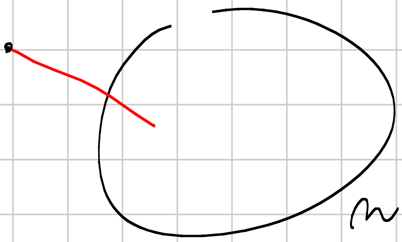
NON connessi

passo base: $n=2$



è connesso

passo induttivo:



n

sono connessi
hp induttiva!

→ è connesso!

L'hp. induttiva NON è necessariamente verificata!

PIGEONHOLE

n tane $n+1$ piccioni $\rightarrow$
$\exists$ almeno una "tana" con almeno due "piccioni".

n tane $nk+1$ piccioni $\rightarrow$
$\exists$ almeno una "tana" con almeno $k+1$ "piccioni"

Esempio "stupido" Siete 25. Quante persone siete sicuri di poter trovare che compiono gli anni lo stesso mese?
Sicuramente ce ne sono 3.

Esempio "meno stupido" Siete 25. Esistono due di voi che conoscono (fra voi) lo stesso # di persone.

$0, \ldots, 24 \downarrow$

tane = # amici quante? 25
piccioni = voi quanti? 25

faccio casi!
- se esiste un "solitario" non esiste un "popolare"
  $\rightarrow$ 24 tane
- se non esiste un "solitario"
  $\rightarrow$ 24 tane

$\rightarrow \exists$ 2 piccioni nella stessa tana!

ESEMPIO 3 $n+1$ numeri fra 1 e $2n$
interi

Allora ne esistono 2 primi fra loro.
2 uno divisore dell'altro

- esistono due consecutivi

$\boxed{1\ 2}\ \boxed{3\ 4}\ \boxed{5\ 6}\ \boxed{7\ 8}\ \dots\ \boxed{\ \ 2n}$

n tane, $n+1$ piccioni
$\rightarrow$ 2 nella stessa
$=$ 2 consecutivi

- Scrivo i numeri scelti come $2^{k_i} d_i$

Quanti sono i possibili d_i? n possibili
MA scelgo $n+1$ numeri!
Quindi scelgo $\underbrace{2^a d,\ 2^b d}_{\text{STESSO fattore } d}$

"divide"

MA allora se $a<b$ $\quad 2^a d \mid 2^b d$
$a>b$ $\quad 2^b d \mid 2^a d$
$a=b$ $\quad$ NO!

Algebra (Complessi & polinomi) mr_go

Titolo nota 03/09/2013

① Numeri complessi.

$z = x + iy$ x, y reali, i unità imm. $i^2 = -1$.

$= \rho(\cos\theta + i\sin\theta) = \rho e^{i\theta}$. ρ reale non-neg. θ reale

$z_1 = x_1 + iy_1$
$z_2 = x_2 + iy_2$ $z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$

$z_1 = \rho_1 e^{i\theta_1}$
$z_2 = \rho_2 e^{i\theta_2}$ $z_1 \cdot z_2 = \rho_1 \cdot \rho_2 \cdot e^{i(\theta_1 + \theta_2)}$

def Coniugio: $\overline{z} = x - iy = \rho e^{-i\theta}$.

es $\overline{i} = -i$
$\overline{37\pi} = 37\pi$.

oss $z = \overline{z}$ se e solo se z è reale.

$z = -\overline{z}$ se e solo se z è immaginario.

es: $\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$:

infatti $z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$

$\overline{z_1 + z_2} = (x_1 + x_2) - i(y_1 + y_2)$

- $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$

$\overline{z_1} = \rho_1 e^{-i\theta_1}$, $\overline{z_2} \cdot \ldots$

$\overline{z_1 \cdot z_2} = \rho_1 \cdot \rho_2 \cdot e^{-i(\theta_1+\theta_2)} = \overline{z_1} \cdot \overline{z_2}$

<u>Formule di de Moivre</u>

z^n dove $|z| = 1 = \sqrt{x^2+y^2} = \rho$

$z^n = (x+iy)^n$ = svil. col binomio di Newton.

$z = \cancel{\rho} \cdot e^{i\theta} \rightsquigarrow z^n = (e^{i\theta})^n = e^{i(n\theta)}$

se $|z| \neq 1 \rightsquigarrow |z^n| = |z|^n$.

$\cos(2x) = \cos^2 x - \operatorname{sen}^2 x$

$\cos(3x) = ?$ $\qquad \cos 4x$

$\cos(nx) = \operatorname{Re}(e^{i(nx)}) =$

$\qquad (e^{ix})^n = (\cos x + i \operatorname{sen} x)^n$

<u>es</u> Trovare la parte reale (in funzione di $\cos x$ e $\operatorname{sen} x$). Trovare $\operatorname{sen}(nx)$.

<u>pensare a</u>: come si trovano tutti i numeri complessi z tali che $z^m = 1$? (m intero positivo).

② Polinomi (basic)

Che cos'è un polinomio?

Un polinomio (in una variabile) è un'espressione formale

$$p(x) = \underbrace{a_d}\, x^d + a_{d-1} \cdot x^{d-1} + \dots + a_1 \cdot x + a_0.$$

$a_d \neq 0 \rightsquigarrow$ il polinomio ha grado d

$d = \deg p$ (~~∂p~~).

$a_d = 1 \rightsquigarrow p$ si dice monico.

a_i = coefficienti, a_d coeff. di testa,

a_0 = termine noto.

a_i possono essere interi (pol. a coeff. interi)

razionali (" " " raz.)

reali (reali)

complessi (" " " compl.)

classi di resto

polinomi

$$p(x,y) = 2x^2 y + 3x \cdot y + 23$$

domanda quando due polinomi sono uguali?

risp? ① $p(x) = q(x)$ se $p(a) = q(a)$ $\forall a \in \mathbb{R}$.

② due polinomi sono uguali se hanno gli stessi coefficienti

A p pol. associo una funzione.

I polinomi $p(x)=x$ e $q(x)=x^2$ a coeff. in $\mathbb{F}_2$ o $\mathbb{Z}/2\mathbb{Z}$ hanno la stessa funzione associata:

$$p(0)=0, \qquad q(0)=0$$
$$p(1)=1, \qquad q(1)=1$$

<u>Ma</u> sono diversi come polinomi.

1 è "sbagliata", ma 1 e 2 sono equivalenti sui reali/complessi/interi/razionali...

3 <u>Divisione tra polinomi</u>

Ho a e b polinomi a coeff. reali e voglio dividere a per b.

$$a(x) = x^3+3x^2+1$$
$$b(x) = x^2+2$$

Divido x^3 per x^2 ho x

$$a(x) - x\cdot b = x^3+3x^2+1 - x\cdot(x^2+2) =$$
$$= \cancel{x^3}+3x^2+1-\cancel{x^3}-2x =$$

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

Divido $3x^2$ per x^2 ho 3

$3x^2 - 2x + 1 - 3 \cdot b = \boxed{-2x-5}$

$$a(x) = \underbrace{(x+3)}_{\text{quoziente} = q} \cdot b(x) + \underbrace{(-2x-5)}_{\text{resto} = r}$$

Il resto e il quoziente della divisione di a per b sono univocamente determinati da:

- $a = q \cdot b + r$
- $\deg r < \deg b$ $\quad (\sim\ r < b)$.

<u>Oss</u> (Molto importante)

I polinomi a coeff (reali/interi/razionali) hanno la fattorizzazione unica.

<u>Cioè</u> $p(x)$ esistono e sono unici (a meno dell'ordine) $f_1(x), \dots, f_k(x)$ polinomi <u>irriducibili</u> tali che $p(x) = f_1(x) \cdot \ldots \cdot f_k(x) = \prod_{j=1}^{k} f_j(x)$.

<u>Oss</u> $p(x)$ è a coeff. interi, può benissimo essere: irriducibile <u>ma</u> riducibile sui reali.

$p(x) = x^2 - 2$ non irr. in $\mathbb{Z}[x]$ (es.)

$p(x) = (x-\sqrt{2})(x+\sqrt{2})$

$p(x)$ ha a coeff. reali, irrid. nei reali, ma riducibile sui complessi

$p(x) = x^2+2$
x^2+x+1
$x^2+1 = (x+i)(x-i)$.

thm (Lemma di Gauss)

Se $p(x) \in \mathbb{Z}[x]$ è riducibile in $\mathbb{Q}[x]$, allora è riducibile anche in $\mathbb{Z}[x]$.

es $p(x) = x^2+2x+1 = (2x+2)\left(\frac{1}{2}x + \frac{1}{2}\right)$

MCD (stessa definizione)

MCD(a, b) = pol. $\overset{\text{monico}}{\vee}$ di grado massimo che divide a e b.

Come si calcola: Algoritmo di Euclide.

thm (Bézout): se $d(x) = MCD(a(x), b(x))$, allora esistono $h(x), k(x)$ polinomi t.c.

$$h(x)\cdot a(x) + k(x)\cdot b(x) = d(x)$$

def Una radice (o zero) di un polinomio $p(x)$ è un numero α tale che $p(\alpha)=0$.

es $\sqrt{2}$ è una radice di x^2-2.
i è una radice di x^2+1 ...

es Se abbiamo un polinomio $f(x)=a_d x^d+\ldots+a_0$ a coeff. interi, e $\alpha = p/q$ è una sua radice razionale.
fraz. ridotta ai min termini
Cosa possiamo dire di p e q?

sol $q \mid a_d$, $p \mid a_0$.

$$0 = f(\alpha) = f(p/q) = a_d \cdot \left(\frac{p}{q}\right)^d + a_{d-1} \cdot \left(\frac{p}{q}\right)^{d-1} + \ldots + a_0$$

$$\leadsto \quad 0 = \underbrace{a_d \cdot p^d + \overbrace{a_{d-1} \cdot p^{d-1} \cdot q + \ldots + a_1 \cdot p \cdot q^{d-1} + a_0 \cdot q^d}}$$

Addendo rosso $= p \cdot (\underbrace{a_d \cdot p^{d-1} + \ldots + a_1 \cdot q^{d-1}}_{\text{intero}})$
$\downarrow$
div. per p. $\qquad a_0 \cdot q^d \leadsto$ divisibile per p.

Siccome $MCD(p,q)=1 \Rightarrow p \mid a_0$.

es $x^{35}+12x^{13}+17x+1$ trovare le radici razionali.
$\hookrightarrow$ non ha radici razionali (± 1 non sono radici).

es Se abbiamo un polinomio $p(x)$ a coeff. interi, ~~[illegible]~~

e abbiamo due interi $a \neq b$.

Cosa possiamo dire su $p(a) - p(b)$?

$$\boxed{(a-b) \mid (p(a)-p(b))}$$

perché? • Se $p(x) = x^k$, lo sappiamo dimostrare?

$$p(a)-p(b) = a^k - b^k = (a-b)\underbrace{(a^{k-1}+\ldots+b^{k-1})}_{\text{intero}}$$

• Se $p(x) = c_k \cdot x^k$ è vero?

• Se è vero per $p(x)$ e $q(x)$ è vero per $p(x)+q(x)$?

Sì: $(p+q)(a) - (p+q)(b) = p(a)+q(a)-(p(b)+q(b)) =$

$= (p(a)-p(b)) + (q(a)-q(b))$ ✓

• FINE. (per induzione).

thm (Ruffini)

Vogliamo dividere $p(x)$ per il polinomio $(x-a)$.

Qual è il resto?

(*) $p(x) = (x-a)\cdot q(x) + r\boxed{(x)}$ con $\deg r < 1$

Cioè r è una costante!

Ora sostituiamo $x=a$ in (*):

$$p(a) = \cancel{(a-a)\cdot q(a)} + r^{\nearrow r(a)}$$

Thm (Ruffini) Il resto della divisione di $p(x)$ per $(x-a)$ è $p(a)$.

es Resto della divisione di $x^{10}+1$ per $x-2$:

1025.

cor $x^{37}+x^{12}+x^5+13$. ha al più 37 radici.

Se α è una radice di p allora $(x-\alpha)$ divide p!

In particolare, ogni radice si mangia un pezzo di grado

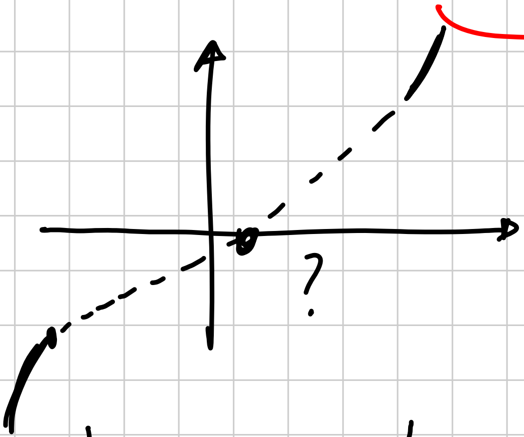
(occhio è vero solo su $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$). p primo

(4) Teorema fondamentale dell'algebra

Richiamento: se ho un polinomio di grado 3 a coefficienti reali:

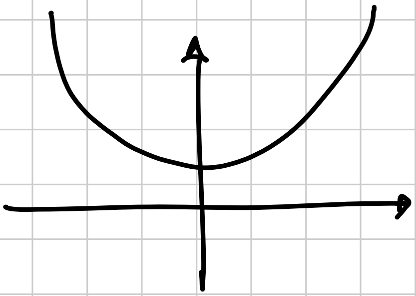
$$p(x) = x^3 + (ax^2+bx+c) =$$

$$= x^3 \cdot \Big(1 + \underbrace{\frac{a}{x} + \frac{b}{x^2} + \frac{c}{x^3}}_{\text{molto piccolo}}\Big) \text{ se } |x| >> 0.$$



unica cosa che conta

passo da negativo a positivo $\Rightarrow$ devo avere uno zero $\Rightarrow$ ho una radice



$\leftarrow \sim x^2+1$

<u>riscaldamento</u>/2 : $p(x) = x^2+ax+b$.

Ogni pol. di grado due ha almeno una radice.

(La sappiamo trovare esplicitamente.)

<u>thm</u> (Fondam. dell'algebra)

$p(x) \in \mathbb{R}[x]$ di grado n ha sempre n radici complesse.

<u>oss</u> Vero anche se $p(x) \in \mathbb{C}[x]$.

<u>cor</u> $p(x)$ è monico allora $p(x) = (x-\alpha_1)\cdot \ldots \cdot (x-\alpha_n)$

dove $\alpha_1, \ldots, \alpha_n$ sono <u>le</u> radici di $p(x)$.

Sia $p(x) \in \mathbb{R}[x]$: come sono fatti i fattori irr. della sua fattorizzazione?

p si spezza in fattori di grado 1 e 2.

Prendiamo α radice complessa di $p(x)$.

Cosa possiamo dire di $\bar{\alpha}$?

$$p(\bar{\alpha}) = \sum_{k=0}^{d} a_k \cdot \bar{\alpha}^k = \sum \bar{a}_k \cdot \overline{\alpha^k} = \sum \overline{(a_k \alpha^k)} =$$

$$= \overline{\sum a_k \alpha^k} = \overline{p(\alpha)} = 0.$$

Le radici di p sono reali o accoppiate a 2 a 2.

$$p(x) = (x-\alpha_1)\cdots(x-\alpha_h)\cdot(x-\beta_1)(x-\bar{\beta}_1)\cdots(x-\beta_\ell)\cdot(x-\bar{\beta}_\ell)$$

$$= \underbrace{(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_h)}_{\text{reali perché } \alpha_i \text{ reali}}\cdot\underbrace{\left(x^2-(\beta_1+\bar{\beta}_1)x+\beta_1\bar{\beta}_1\right)}_{\text{reale!}}\cdot\ldots\cdot\left(x^2-(\beta_\ell+\bar{\beta}_\ell)x+\beta_\ell\cdot\bar{\beta}_\ell\right)$$

$$z\cdot\bar{z} = (x+iy)(x-iy) = x^2-(iy)^2 =$$

$$= x^2 - i^2y^2 = x^2+y^2 = |z|^2 = \rho^2.$$

$$z\cdot\bar{z} = \rho e^{i\theta}\cdot\rho e^{-i\theta} = \rho^2 e^{i(\theta-\theta)} = \rho^2$$

Formule di Viète

Riscaldamento: $p(x) = (x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta$

$$\begin{aligned} &\parallel \\ &x^2 + ax + b \end{aligned}$$

$$\begin{cases} \alpha+\beta = -a \\ \alpha\beta = b \end{cases}$$

/2 : $p(x) = (x-\alpha)(x-\beta)(x-\gamma)$

$$\begin{aligned} &\parallel \\ &x^3 + ax^2 + bx + c \end{aligned}$$

$$\begin{cases} -\alpha-\beta-\gamma = a \\ \alpha\beta+\beta\gamma+\gamma\alpha = b \\ -\alpha\beta\gamma = c \end{cases}$$

In generale: $p(x) = x^d + \sum_{k=0}^{d-1} a_k x^k$

Se radici $\gamma_1, \dots, \gamma_d$, allora:

$$a_{d-1} = -(\gamma_1 + \dots + \gamma_d)$$

$$a_{d-2} = \gamma_1\gamma_2 + \dots + \gamma_1\gamma_d + \gamma_2\gamma_3 + \dots + \gamma_2\gamma_d + \dots + \dots + \gamma_{d-1}\gamma_d$$

$$\vdots$$

$$a_{d-3} = -(\gamma_1\gamma_2\gamma_3 + \dots + \dots + \gamma_{d-2}\cdot\gamma_{d-1}\cdot\gamma_d)$$

$$\vdots$$

$$a_0 = (-1)^d \gamma_1 \cdot \gamma_2 \cdot \dots \cdot \gamma_d$$

es $\alpha^3+\beta^3$ esprimere come funzione di

$\alpha+\beta$ e $\alpha\beta$.

$$\alpha^3+\beta^3 = (\alpha+\beta)(\alpha^2-\alpha\beta+\beta^2) =$$
$$\alpha^2+2\alpha\beta+\beta^2-3\alpha\beta =$$
$$= (\alpha+\beta)^3 - 3(\alpha+\beta)\alpha\beta.$$

es • $\alpha^2+\beta^2+\gamma^2$ esprimere in funz. di $\alpha+\beta+\gamma$
$\alpha\beta+\beta\gamma+\gamma\alpha$
$\alpha\beta\gamma$

$$(\alpha+\beta+\gamma)^2 - 2(\alpha\beta+\beta\gamma+\gamma\alpha)$$

• $$\alpha^3+\beta^3+\gamma^3 = (\alpha+\beta+\gamma)^3 - 3(\alpha^2\beta+\ldots+\beta^2\gamma+\ldots) - 6\alpha\beta\gamma$$

$$\alpha^2\beta+\alpha\beta^2+\beta\gamma^2+\beta^2\gamma+\gamma\alpha^2+\gamma^2\alpha =$$
$$(\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\gamma\alpha) - 3\alpha\beta\gamma$$

$$\alpha^3+\beta^3+\gamma^3 = (\alpha+\beta+\gamma)^3 - 3(\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\gamma\alpha)+3\alpha\beta\gamma$$

5 Radici di 1

Le radici n-esime di 1 sono le radici del polinomio X^n-1,

quindi sono al più n, e sono tutte distinte.

Stiamo cercando z t.c. $z^n = 1$:

$|z| = 1 \Rightarrow z = e^{i\theta}$.

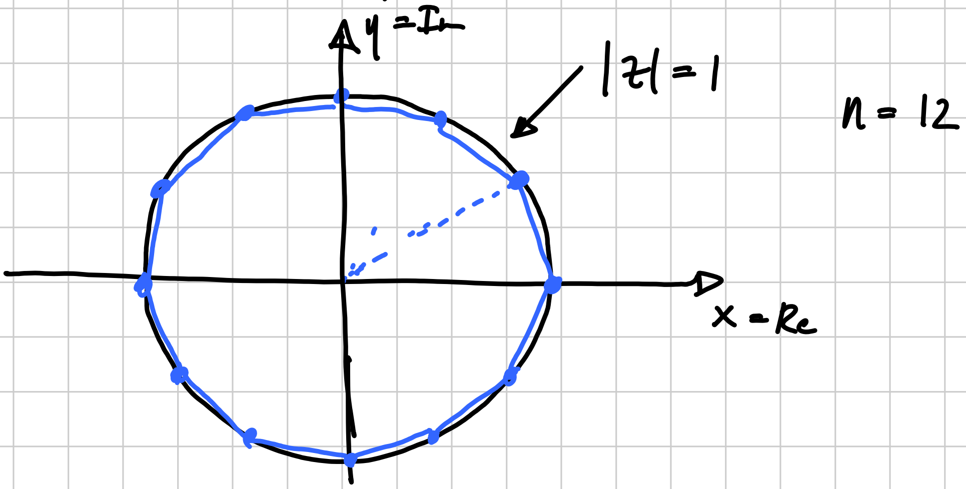
$$z^n = \left(e^{i\theta}\right)^n = e^{in\theta} = 1$$

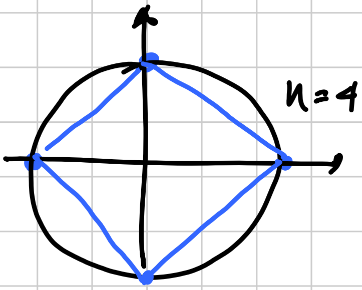
$$n\theta = 0,\ \pm 2\pi,\ \pm 4\pi,\ \ldots,$$

$$\theta = 0,\ 2\pi/n,\ 4\pi/n,\ 6\pi/n,\ \ldots,\ 2\pi n/n = 2\pi$$

hanno lo stesso arg.
a meno di 2π

Le radici n-esime di 1 sono $e^{2k\pi i/n}$ per $k = 0, \ldots, n-1$.





In generale, le radici di $x^n - 1$ stanno sulle circonf. $\{|z| = 1\}$ e formano un n-agono regolare con un vertice in 1.

1) $\alpha = e^{2\pi i/n}$ $\quad \alpha^0, \alpha^1, \dots, \alpha^{n-1}$

$$\sum_{k=0}^{n-1} \alpha^k = \frac{\alpha^n - 1}{\alpha - 1}$$

2) $S = \alpha^0 + \dots + \alpha^{n-1} = \alpha + \alpha^1 + \dots + \alpha^{n-1} + \alpha^n = \alpha \cdot S$

$\overset{\shortparallel}{1} = \alpha^n$

3) Formule di Viète!

$\alpha^0, \dots, \alpha^{n-1}$ sono (tutte e sole) le radici di $x^n - 1$.

• Sez. 3.1, 3.2 (pp. 12 - 13)

esercizi: • 3, (7), 8, 9 p. 20

• Dimostrare che

$$\cos\frac{\pi}{7} - \cos\frac{2\pi}{7} + \cos\frac{3\pi}{7} = \frac{1}{2}.$$

es 3 p. 20. $S = \cos 15° + \cos 35° + \dots + \cos 355°$.

$$\cos 15° = \cos\frac{\pi}{12} = \cos\frac{2\pi}{24} = \mathrm{Re}\left(e^{\frac{2\pi}{24}\cdot i}\right)$$

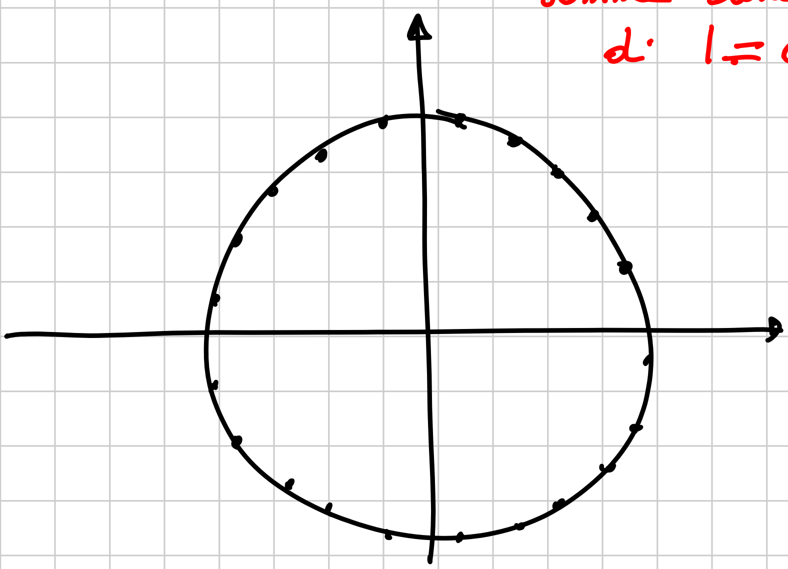
$$\cos 35° = \cos(15°+20°) = \mathrm{Re}\left(e^{\left(\frac{2\pi}{24}+\frac{2\pi}{18}\right)i}\right)$$

$$\cos 55° = \mathrm{Re}\left(e^{\left(\frac{2\pi}{24}+\frac{2\pi}{18}\cdot 2\right)i}\right) \dots$$

$$S = \sum_{k=0}^{17} \mathrm{Re}\left(e^{\left(\frac{2\pi}{24}+\frac{2\pi}{18}\cdot k\right)i}\right) =$$

$$= \mathrm{Re}\left(\sum e^{\left(\frac{2\pi}{24}+\frac{2\pi}{18}k\right)i}\right) =$$

$$= \mathrm{Re}\left(e^{\frac{2\pi}{24}i}\cdot \underbrace{\sum e^{\frac{2\pi}{18}\cdot k i}}_{\text{somma delle radici 18-esime di } 1 \,=\, 0}\right) = 0$$



es 7 p. 20 (Interpolazione di Lagrange)

Stiamo cercando un pol di grado al più 3 che faccia 2 in 0, 4 in 1 ...

Uno dei modi possibili:

trovo un pol di grado 3 che fa 1 in 0, 0 in 1, 2, 3, ⇝ $a(x-1)(x-2)(x-3)$

Impongo che $p(0)=1$ ⇝ $a=-1/6$.

$$p_0(x) = \frac{(x-1)(x-2)(x-3)}{(0-1)(0-2)(0-3)}$$

$$p_1(x) = \frac{(x-0)(x-2)(x-3)}{(1-0)(1-2)(1-3)}$$

$\vdots$

$$p(x) = a_0 \cdot p_0 + a_1 \cdot p_1 + a_2 \cdot p_2 + a_3 \cdot p_3 .$$

$p(0) = a_0$ $\quad$ $p(2) = a_2$

$p(1) = a_1$ $\quad$ $p(3) = a_3$

es 8

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 2$$
$$\alpha + \beta + \gamma + \delta = 1$$

→ quanto fa $\alpha\beta + \alpha\gamma + \alpha\delta + \beta\gamma + \beta\delta + \gamma\delta$?

$$(\alpha+\beta+\gamma+\delta)^2 = (\alpha^2+\dots+\delta^2) + 2(\overset{b}{\alpha\beta}+\dots+\gamma\delta)$$

$$\alpha^3+\dots+\delta^3 = (\alpha+\dots+\delta)^3 - 3(\quad)(\alpha+\dots+\delta) + 3(\alpha\beta\gamma+\alpha\dots)$$

VIÈTE

<u>es 9</u> Supponiamo che a sia una radice intera di P.

$(a-b) \mid (P(a)-P(b))$ per ogni b.

se $b=0$? $a-0 \mid P(b)$ dispari

$\Rightarrow a$ dispari.

$(\underset{\text{pari}}{a-13}) \mid (0-P(13))$ dispari. ↯.

<u>sol alt.</u> Se $P(a)=0$, allora $P(a)\equiv 0 \pmod 2$

però se a è pari $P(a)\equiv P(0) \pmod 2$, $P(0) \equiv 1 \neq 0$

se a è dispari, $P(a) \equiv P(1) \equiv P(13) \equiv 1 \neq 0 \pmod 2$

IMO 1969: Dim che $S=\cos\frac{\pi}{7}-\cos\frac{2\pi}{7}+\cos\frac{3\pi}{7}=\frac{1}{2}$.

$$\cos\alpha = -\cos(\pi-\alpha)$$

$$-\cos\frac{2\pi}{7} = \cos\left(\pi-\frac{2\pi}{7}\right) = \cos\left(\frac{5\pi}{7}\right)$$

$$\underset{\cos\frac{13\pi}{7}}{\overset{\shortparallel}{\cos\frac{\pi}{7}}}+\underset{\cos\frac{11\pi}{7}}{\overset{\shortparallel}{\cos\frac{3\pi}{7}}}+\underset{\cos\frac{9\pi}{7}}{\overset{\shortparallel}{\cos\frac{5\pi}{7}}} = \frac{1}{2}\cdot\left(\cos\frac{\pi}{7}+\dots+\cos\frac{13}{7}\pi+1\right)$$

$$2S = \left(\cos\frac{\pi}{7}+\cos\frac{2\pi}{7}+\dots+\cos\frac{13\pi}{7}\right) - \overset{\overset{-1}{\shortparallel}}{\cos\frac{7\pi}{7}}$$

$$\shortparallel$$

$$\sum \mathrm{Re}\left(e^{\left(\frac{\pi}{7}+\frac{2\pi}{7}\cdot k\right)i}\right) = 0$$

$$2S = 0-(-1) \Rightarrow 2S = 1.$$

:)

Algebra 2 - $\leq$

ma_go

Titolo nota 05/09/2013

Cosa vuol dire "Dimostrare una disuguaglianza"?

Dim che per ogni x, y, z reali >0 $\frac{x^3+y^3+z^3}{3} \geq \left(\frac{x+y+z}{3}\right)^3$.

Non è una disequazione.

$\Leftrightarrow$ dim che la funzione $F(x,y,z)=\frac{x^3+y^3+z^3}{3}-\left(\frac{x+y+z}{3}\right)^3$

è non-negativa $\Leftrightarrow$ $\min F \geq 0$.

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

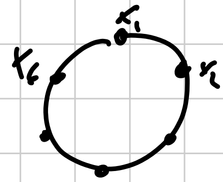
0) Notazione (somme cicliche e somme simmetriche)

A) $x_1, \dots, x_n$ variabili $x_1+\dots+x_n = S$

$S = \sum_{k=1}^{n} x_k = \sum_{cyc} x_1 \rightsquigarrow$ somma ciclica.

↳ parto da x_1 e sommo tutti i termini facendo crescere 1.

$x_1+x_2+x_3+\dots+x_n$.



es $\sum_{cyc} x_1^2 x_2 = \sum_{k=1}^{n-1} x_k^2 x_{k+1} + x_n^2 \cdot x_1$.

$a_1, \dots, a_n$

es $\sum_{cyc} a_1 a_2 a_3^2 = a_1 a_2 a_3^2 + a_2 a_3 a_4^2 + \dots$

$+ a_{n-2} a_{n-1} a_n^2 + a_{n-1} a_n a_1^2 + a_n a_1 a_2^2$

(★) $\sum_{sym} x_1 = \sum_{\sigma\in S_n} x_{\sigma(1)} = \sum_{k=1}^{n!} x_{\sigma_k(1)} =$

$= (n-1)!\,x_1 + (n-1)!\,x_2 + \dots =$

$= (n-1)!\sum x_i = (n-1)!\sum_{cyc} x_i .$

$S_n = \{\sigma_1, \sigma_2, \dots, \sigma_{n!}\}$

In un polinomio, $\underbrace{a_{d-2}}_{\text{ha } \binom{n}{2} \text{ addendi}} = \underbrace{\sum_{cyc} \alpha\beta}_{\text{ha } n \text{ addendi}} = \ell \underbrace{\sum_{sym} \alpha\beta}_{\text{ha } n!}$

$a_{d-2} = \frac{1}{(n-2)!\,2!}\sum_{sym} \alpha\beta = \frac{n!}{(n-2)!\,2!} = \binom{n}{2}$ se $\alpha=\beta=\dots=1$

<u>check</u> Cosa succede se $\alpha=\beta=\dots=\gamma=1$?

(1) <u>Riarrangiamento</u>

Ho due n-uple di reali $a_1,\dots,a_n$, $b_1,\dots,b_n$.

Come costruire rettangoli con base a_i e altezze b_j di modo da massimizzare l'area totale?
E se le voglio minimizzare?

WLOG possiamo supporre $a_1 \le a_2 \le \dots \le a_n$
$b_1 \le b_2 \le \dots \le b_n$.

Somma aree $= \sum_{i=1}^{n} a_i \cdot b_{\sigma(i)} = \sum_{cyc} a_1 b_{\sigma(1)}$ per $\sigma \in S_n$.

$S_n = \{\sigma : \{1,\dots,n\} \circlearrowleft \text{ bigettive}\}$

<u>thm</u> (R.) $\frac{1}{n}\sum_i a_i b_{n-i+1} \le \frac{1}{n}\sum_i a_i b_{\sigma(i)} \le \frac{1}{n}\sum_i a_i b_i$

$\forall \sigma \in S_n$. Vale per ogni scelta di

$a_1 \le \dots \le a_n$
$b_1 \le \dots \le b_n$ reali qualunque.

<u>dim</u> Prendiamo una perm. a caso, supp. per comodità che $\le \longrightarrow <$.

E supponiamo che <u>non</u> sia l'identità e dim. che ce n'è una più grande.

<u>oss</u> Se $\sigma \in S_n$ <u>non</u> è l'identità, esistono due indici k e l tali che $k < l$ e $\sigma(k) > \sigma(l)$.
(dim per casa – INDUZIONE).

$\sum_i a_i b_{\sigma(i)}$ e la modifichiamo per ottenere un valore più grande.

$\tilde{\sigma}(i) = \sigma(i)$ se $i \ne k, l$, e $\tilde{\sigma}(k) = \sigma(l)$ e $\tilde{\sigma}(l) = \sigma(k)$.

Voglio dim. che $\underbrace{\sum_i a_i b_{\tilde{\sigma}(i)}}\ \overset{?}{\geq}\ \underbrace{\sum_i a_i b_{\sigma(i)}}$.

quanto sono diversi?!

Rimane $a_k b_{\underbrace{\tilde{\sigma}(k)}_{n}} + a_l b_{\underbrace{\tilde{\sigma}(l)}_{m}} \overset{?}{\geq} a_k b_{\underbrace{\sigma(k)}_{m}} + a_l b_{\underbrace{\sigma(l)}_{n}}$

$$a_k b_n + a_l b_m - a_k b_m - a_l b_n \overset{?}{\geq} 0$$

$$\underbrace{(a_k - a_l)}\underbrace{(b_n - b_m)} \overset{?}{\geq} 0$$

<0 perché $k<l$ $\quad$ <0 perché $m>n$ $\quad\quad \square$

es Dimostrare l'altra metà.

esempi $\quad \sum_{cyc} ab \leq \sum_{cyc} a^2 \quad\quad a,b,c$

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

WLOG posso supporre $a \leq b \leq c$.

$ab + bc + ca \leq a \cdot a + b \cdot b + c \cdot c.$

$a \leq b \leq c$

$a \leq b \leq c$

riarrangiamento!

cor (della dimostr.) $\quad$ $a_1 \leq \dots \leq a_n$, $b_1 \leq \dots \leq b_n$, $c_1 \leq \dots \leq c_n$ $\quad \sum_i a_i b_{\sigma(i)} c_{\tau(i)} \leq \sum_i a_i b_i c_i$.

es $\quad a^b b^c c^a \leq a^a b^b c^c$.

$\Updownarrow \log(a^b b^c c^a) \leq \log(a^a b^b c^c)$

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

$a \leq b \leq c$ WLOG $\Rightarrow \log a \leq \log b \leq \log c$.

per riarrangiamento. $\quad \square$.

$$\sum_{cyc} \frac{x_1}{x_2} \geq n \qquad x_1, x_2, \dots, x_n > 0$$

$$\sum_{cyc} x_1 \cdot \frac{1}{x_2} \qquad \text{WLOG } x_1 \leq x_2 \leq \dots \leq x_n$$

$$\Downarrow$$

$$\frac{1}{x_1} \geq \frac{1}{x_2} \geq \dots \geq \frac{1}{x_n}$$

se li accoppiamo $1 \leftrightarrow 1, \dots, n \leftrightarrow n$ otteniamo il MIN

$$\sum = n$$

se li accoppiamo $1 \leftrightarrow n, \dots, n \leftrightarrow 1$ otteniamo il MAX

Per l'altra dis. del riarrangiamento, abbiamo vinto.

<u>thm</u> (Chebycheff) $\frac{1}{n} \sum a_i b_{n+1-i} \leq \left(\frac{1}{n}\sum a_i\right)\left(\frac{1}{n}\sum b_i\right) \leq \frac{1}{n}\sum a_i b_i$

(sotto le stesse ipotesi del riarr.)

MIN media dei prodotti. prod. delle medie MAX media dei prodotti

<u>dim</u> Sommate riarrangiamenti. (per casa).

<u>Cor</u> (Riarr.) <u>Dis. di Schur</u>

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

$$\| $$

$$(x+y+z)\left((x+y+z)^2 - 3(xy+yz+zx)\right).$$

<u>dim</u> Si ricava da $\sum_{cyc} x^t (x-y)(x-z) \geq 0$. (per casa) $\square$

$t > 0$.

② Medie

Chiamiamo medie p-esime di n reali positivi $a_1, \dots, a_n$

$$M_p = \left(\frac{a_1^p + \dots + a_n^p}{n}\right)^{1/p}.$$

AM = media aritm. = M_1
QM = " quad. = M_2
HM = " armonica = M_{-1}

$M_0 = GM = \left(\prod a_i\right)^{1/n}$
$M_{-\infty} = \min\{a_i\}$
$M_{+\infty} = \max\{a_i\}$

thm Se $p<q$, allora $M_p \leq M_q$,

e $M_p = M_q$ se e solo se $a_1 = a_2 = \dots = a_n$.

cor (AM-GM) AM $\geq$ GM
$M_1 \geq M_0$ $\quad \frac{\sum a_i}{n} \geq \left(\prod a_i\right)^{1/n}$.

dim Caso base: $n=2$. $\quad \frac{a+b}{2} \geq \sqrt{ab}$

$$\frac{(\sqrt{a}-\sqrt{b})^2}{2} = \frac{a - 2\sqrt{ab} + b}{2} \overset{?}{\geq} 0$$

sì, vero, = se e solo se $a=b$.

Passo induttivo: $n \rightsquigarrow 2n$.

Dobbiamo dim che $\frac{a_1 + \dots + a_n + a_{n+1} + \dots + a_{2n}}{2n} \geq \left(\prod_1^n a_i \cdot \prod_{n+1}^{2n} a_i\right)^{1/2n}$

$$AM = \frac{\overbrace{\frac{a_1 + \dots + a_n}{n}}^{x} + \overbrace{\frac{a_{n+1} + \dots + a_{2n}}{n}}^{y}}{2} \geq \sqrt{\left(\prod_1^n a_i\right)^{1/n} \cdot \left(\prod_{n+1}^{2n} a_i\right)^{1/n}}$$

$\Downarrow$ AM>GM quando ho 2 elementi

$AM(x,y) \geq GM(x,y)$

$$AM \geq \sqrt{\underbrace{\left(\frac{a_1+\dots+a_n}{n}\right)}_{\geq GM(a_1,\dots,a_n)} \cdot \underbrace{\left(\frac{a_{n+1}+\dots+a_{2n}}{n}\right)}_{GM(a_{n+1},\dots,a_{2n})}} \overset{P.I.}{\geq} \sqrt{\left(\prod a_i\right)^{1/n} \cdot \left(\prod a_i\right)^{1/n}}$$

Dobbiamo tornare indietro:

dovete dim $AM(a_1,\dots,a_{n-1}) \geq GM(a_1,\dots,a_{n-1})$

(*) e sapere $AM(x_1,\dots,x_n) \geq GM(x_1,\dots,x_n)$ $\forall x_i > 0$.

Applichiamo (*) a $x_1 = a_1, \dots, x_{n-1} = a_{n-1}$, $x_n = ?$

da scegliere in modo furbo. (per casa).

<u>es</u> $x + 2y + 3z \geq 6$ se $xy^2z^3 = 1$ $(x,y,z>0)$.

$$AM(\dots) = \frac{x+y+y+z+z+z}{6} \geq 1 = \sqrt[6]{1} = \sqrt[6]{xy^2z^3} = GM(\ )$$

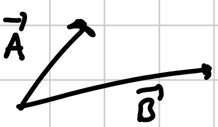
$x + 2y + 3z \geq ?$ se $xyz = 1$ $(x,y,z>0)$

$\frac{x+2y+3z}{3} \geq \sqrt[3]{6} \Rightarrow$? ottimale è $3\sqrt[3]{6}$.

(per casa) $x + 2y + 3z \geq ?$ se $x^3y^2z = 9$ $(x,y,z>0)$.

③ Cauchy-Schwarz

<u>thm</u> (C-S). $\left(\sum a_i b_i\right)^2 \leq \left(\sum a_i^2\right)\left(\sum b_i^2\right)$ $\forall a_i, b_i$.

<u>dim</u> 

, $\vec{A} \cdot \vec{B} = x_A x_B + y_A y_B$. (in coord.)

Un vettore n-dim. è una n-upla di num. reali.

$$\vec{A} = (x_1, x_2, \ldots, x_n), \quad \vec{B} = (y_1, y_2, \ldots, y_n) \quad \Big\} \ \vec{A}\cdot\vec{B} = x_1 \cdot y_1 + \ldots + x_n \cdot y_n.$$

$\vec{C}\cdot\vec{C}$ = somma di quad. $\geq 0 \quad \forall \vec{C}$.

$\|\vec{C}\|^2 = \vec{C}\cdot\vec{C} = 0$ se e solo se $\vec{C} = 0$.

$$\vec{A} = (a_1, \ldots, a_n), \quad \vec{B} = (b_1, \ldots, b_n) \Rightarrow LHS = (\vec{A}\cdot\vec{B})^2$$

$$RHS = \|\vec{A}\|^2 \cdot \|\vec{B}\|^2.$$

oss $(\vec{x}+\vec{y})\cdot\vec{z} = \vec{x}\cdot\vec{z} + \vec{y}\cdot\vec{z}$.

$\vec{x}\cdot\vec{y} = \vec{y}\cdot\vec{x}$ (verificare)

$\vec{C} = \vec{A} - t\cdot\vec{B}$ dove $t \in \mathbb{R}$.

$$0 \leq \|\vec{C}\|^2 = \|\vec{A} - t\cdot\vec{B}\|^2 = \|\vec{A}\|^2 - 2t\,\vec{A}\cdot\vec{B} + t^2\|\vec{B}\|^2.$$

$$\Updownarrow$$

$$\frac{\Delta}{4} \leq 0$$

$$\frac{b^2 - 4ac}{4} = \boxed{(\vec{A}\cdot\vec{B})^2 - \|\vec{A}\|^2\cdot\|\vec{B}\|^2 \leq 0}$$

C-S!

= in C-S. ce l'ho se e solo se per qualche t

$\vec{A} - t\vec{B} = \vec{C} = 0 \iff \vec{A}$ e $\vec{B}$ paralleli $\iff$

$\vec{A}$ e $\vec{B}$ sono multipli. $\square$

<u>es</u> $ab + bc + ca \le a^2 + b^2 + c^2$

$$\underbrace{a_1 = a}_{b_1} \quad \underbrace{a_2 = b}_{b_2} \quad \underbrace{a_3 = c}_{b_3}$$

<u>es</u> Prendiamo $x, y, z \ge 1$ t.c. $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 2$

Dim. che $\sqrt{x+y+z} \ge \sqrt{x-1} + \sqrt{y-1} + \sqrt{z-1}$.

$$\sqrt{x-1} = \underbrace{\sqrt{\frac{x-1}{x}}}_{a_1} \cdot \underbrace{\sqrt{x}}_{b_1} \quad \text{e cicliche.}$$

$$\underbrace{\sum_{cyc} \sqrt{x-1}}_{RHS} = \sum_{cyc} \sqrt{\frac{x-1}{x}} \cdot \sqrt{x} \underset{C-S}{\le} \sqrt{\left(\sum \left(\sqrt{\frac{x-1}{x}}\right)^2\right) \cdot \left(\sum (\sqrt{x})^2\right)} =$$

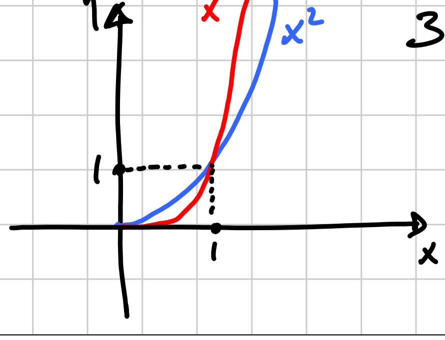
$$= \sqrt{\left(\underbrace{\frac{x}{x}}_{1} - \frac{1}{x} + \underbrace{\frac{y}{y}}_{1} - \frac{1}{y} + \underbrace{\frac{z}{z}}_{1} - \frac{1}{z}\right) \cdot (x+y+z)} = \sqrt{(1+1+1-2)(x+y+z)} = LHS$$

<u>non</u> esempio

Dimostrare che

$ab + bc + ca \le a^3 + b^3 + c^3$ per $a, b, c > 0$.

$a = b = c = t$

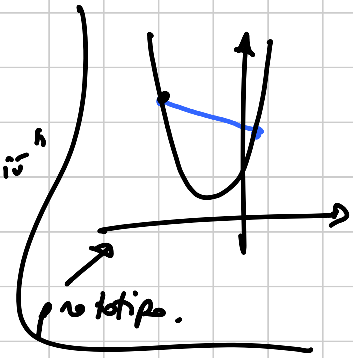


$3t^2 \le 3t^3$ non può essere vera

4 Convessità/concavità e Jensen

Che cos'è una funzione convessa?

"È una funzione con la pancia in giù"

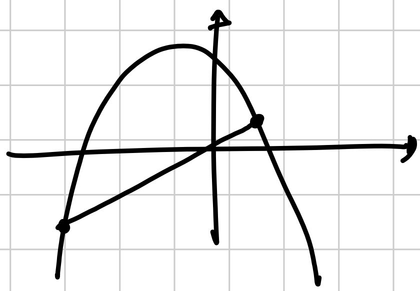


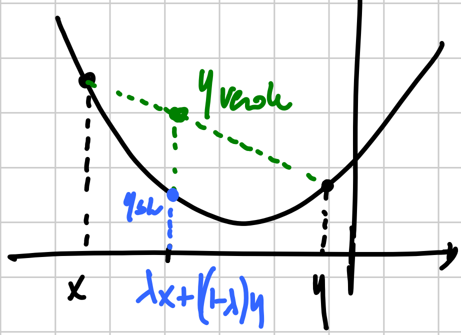
def f funzione reale si dice <u>convessa</u> se $\forall x, y$ e $\forall \lambda \in [0,1]$

$$y_{blu} = \boxed{f(\lambda x + (1-\lambda) y)} \le \boxed{\lambda f(x) + (1-\lambda) f(y)} = y_{verde}$$

f si dice concava se c'è $\ge$. cioè se

$y_{blu} \ge y_{verde}$.





es Le seguenti funzioni sono convesse:

$f(x) = x$

$f(x) = x^2$

$f(x) = x^\alpha$ per $\alpha > 1$ reale, $x > 0$

$f(x) = e^x$

$f(x) = 1/x$ per $x > 0$

$f(x) = \operatorname{tg} x$ per $x \in (0, \pi/2)$

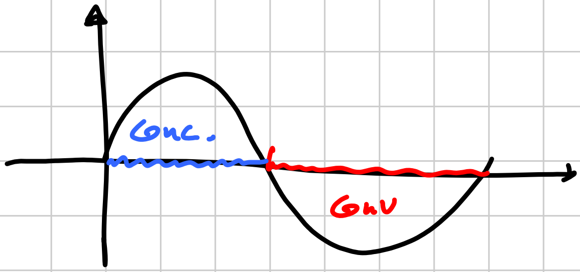
$f(x) + g(x)$ è conv. se lo sono f e g

$f(g(x))$ è convessa se f e g sono convesse e f è <u>crescente</u>.

Le seguenti funzioni sono concave:

$\sqrt{x}$ ($x \geq 0$), x, x^3 per $x \leq 0$, $\cos x$ $(-\pi/2, \pi/2)$, $\operatorname{sen} x$ $(0, \pi)$,

$1/x$ per $x < 0$, $\log x$, $-f(x)$ se x è convessa.



<u>es</u> (per casa) $f(x)$ è sia concava sia convessa se e solo se $f(x) = ax + b$.

<u>dis</u> (JENSEN) Se f è convessa e $x_1, \dots, x_n$ sono nell'int. di convessità, allora

$$f\left(\frac{x_1 + \dots + x_n}{n}\right) \leq \frac{f(x_1) + \dots + f(x_n)}{n}.$$

<u>dim</u> Per induzione (per casa: $x = x_1$, $y = \frac{x_2 + \dots + x_n}{n-1}$, $\lambda = \frac{1}{n}$, e applicate la def.)

<u>dis</u> (J2) Con le stesse hp, $\lambda_1 + \dots + \lambda_n = 1$, $\lambda_i \geq 0$

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

Es Dim la dis. tra le medie ($M_p \geq M_q$ se $p,q>0$).

claim (per casa) basta dim $M_p \geq M_1$ se $p>1$.

Se abbiamo il claim, applichiamo Jensen a $f(x) = x^p$.

$$\text{RHS} = \frac{f(x_1)+\dots+f(x_n)}{n} = \frac{x_1^p+\dots+x_n^p}{n} = M_p^p.$$

$$\text{LHS} = f\left(\frac{x_1+\dots+x_n}{n}\right) = \left(\frac{x_1+\dots+x_n}{n}\right)^p = AM^p = M_1^p$$

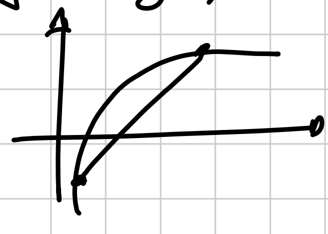
$$M_1^p \leq M_p^p \iff M_1 \leq M_p. \qquad \square$$

thm (Dis. di Young) Se $a,b>0$, $p,q>0$ t.c. $\frac{1}{p}+\frac{1}{q}=1$,

allora $\frac{a^p}{p}+\frac{b^q}{q} \geq ab$.

dim Applichiamo Jensen a $f(x)=\log x$, $x=a^p$, $y=b^q$.

$\log x$ è concava



$$f(\lambda x+(1-\lambda)y) \geq \lambda f(x) + (1-\lambda) f(y)$$

$$\log(\lambda x+(1-\lambda)y) \geq \lambda \log x + (1-\lambda) \log y$$

$$\log(\lambda a^p+(1-\lambda)b^q) \geq \lambda p \log a + (1-\lambda) q \log b$$

$$\lambda = \frac{1}{p} \Rightarrow 1-\lambda = \frac{1}{q}$$

$$\log\left(\frac{a^p}{p} + \frac{b^q}{q}\right) \geq \log a + \log b = \log ab$$

$$\frac{a^p}{p} + \frac{b^q}{q} \geq ab \qquad \square$$

Esercizi: lez. 3.3, 3.4 pp. 13-15

pp. 21-22: n. 1, 4, 5, 9

1. $x_1, \dots, x_n > 0$ e sappiamo

$HM(x_i) = 6$, $GM(x_i) = 7$, $AM(x_i) = 8$.

$$y_i = \prod_{j \neq i} x_j$$

HM, GM, AM degli y_i?

$$y_i = \prod_{i \neq j} x_j = \prod_{j=1}^{n} x_j \Big/ x_i = 7^n / x_i$$

$$AM(y_i) = \left(\sum y_i\right)\Big/ n = \frac{7^n \cdot \sum \frac{1}{x_i}}{n} = 7^n \cdot \left(\frac{\sum \frac{1}{x_i}}{n}\right) =$$

$$= 7^n \cdot HM(x_i)^{-1} =$$

$$= 7^n / 6$$

$$GM(y_i) = \left(\prod y_i\right)^{1/n} = \left(\prod\left(7^n \cdot \frac{1}{x_i}\right)\right)^{1/n} = \left(7^{n^2} \cdot \frac{1}{\prod x_i}\right)^{1/n} =$$

$$= \left(7^{n^2}/7^n\right)^{1/n} = 7^{\frac{n^2-n}{n}} = 7^{n-1}$$

$$AM(y_i) = \left(\frac{\sum_i \frac{1}{y_i}}{n}\right)^{-1} = \left(\frac{\sum x_i}{7^n \cdot n}\right)^{-1} = 7^n \cdot AM(x_i)^{-1} =$$
$$= 7^n/8.$$

$y_i' := y_i/7^n$: es. $M_p(a \cdot y_i) = a \cdot M_p(y_i)$.

(4) MAX (x^5yz) sapendo che $x+y+z=1$.

$$x \cdot x \cdot x \cdot x \cdot x \cdot 5y \cdot 5z \underset{AM\text{-}GM}{\leq} \left(\frac{5x+5y+5z}{7}\right)^7$$

$$25x^5yz \leq \left[\frac{5}{7}(x+y+z)\right]^7 \Rightarrow x^5yz \leq \frac{5^5}{7^7}.$$

$$x = 5y = 5z \Rightarrow x = \frac{5}{7},\ y = z = \frac{1}{7}.$$

$$x^5yz = \left(\frac{5}{7}\right)^5 \cdot \frac{1}{7} \cdot \frac{1}{7} = \frac{5^5}{7^7} \leftarrow$$ il massimo è raggiunto!

(5) $a_i = x_i,\quad b_i = \sqrt{y_i}$

CS : $$\underbrace{\sum_i x_i\sqrt{y_i}}_{=9n} \leq \sqrt{\sum_i x_i^2} \cdot \underbrace{\sqrt{\sum_i y_i}}_{=\sqrt{8n}}$$

$$\sqrt{\sum_i x_i^2} \geq \frac{9\sqrt{n}}{2\sqrt{2}\cdot\cancel{\sqrt{n}}} \Rightarrow \sqrt{\frac{\sum_i x_i^2}{n}} \geq \frac{9}{2\sqrt{2}} \Rightarrow$$

$$QM(x_i) \geq \frac{9}{2\sqrt{2}}.$$

$x = y_i = y_j = 8 \rightsquigarrow x_i = x_j = x$

$x\sqrt{y} = 7 \implies x = \frac{9}{2\sqrt{2}}$ $\underline{\underline{\text{ok}}}$.

9 Chebych. $M_1(a_i b_{n+1-i}) \leq M_1(a_i) \cdot M(b_i) \leq M_1(a_i b_i)$

WLOG $x_1 \leq x_2 \leq \ldots \leq x_n$

$\frac{1}{\sqrt{1-x_1}}, \ldots, \frac{1}{\sqrt{1-x_n}}$?

$\sqrt{1-x_2} \leq \sqrt{1-x_1}$

$\frac{1}{\sqrt{1-x_1}} \leq \frac{1}{\sqrt{1-x_2}} \leq \ldots \leq \frac{1}{\sqrt{1-x_n}}$

$\frac{1}{n}\sum_i \frac{x_i}{\sqrt{1-x_i}} \underset{\text{cheby}}{\geq} M_1(x_i) \cdot M_1\left(\frac{1}{\sqrt{1-x_i}}\right)$ $\quad y_i = \frac{1}{\sqrt{1-x_i}}$

$M_1(x_i) \to \frac{1}{n}$, $\quad M_1\left(\frac{1}{\sqrt{1-x_i}}\right) \to$?

$$M_{-2}(y_i) = \left(\frac{\sum_i \frac{1}{y_i^2}}{n}\right)^{-1/2} = \left(\frac{\sum_i 1-x_i}{n}\right)^{-1/2} = \left(\frac{n-1}{n}\right)^{-1/2} =$$

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

$$\cancel{\frac{1}{n}}\sum_i \geq \cancel{\frac{1}{n}} \cdot M_1(y_i) \geq \cancel{\frac{1}{n}} M_{-2}(y_i) = \cancel{\frac{1}{n}} \cdot \frac{\sqrt{n}}{\sqrt{n-1}} = \sqrt{\frac{n}{n-1}}.$$

SUCCESSIONI / FUNZIONI

Titolo nota 06/09/2013

$a_0 = \square$

$a_1 = \square$

$a_2 = \square$

$a_3 = \square$

successioni $\neq$ formule

$a_n = \{$numero di persone al mondo con n capelli$\}$

$a_n = \{$numero di "e" che ci sono nel nome di un numero$\}$ ...

1, 2, 3, 4, 5, ...

$a_0 = 0 \qquad a_1 = 1 \qquad a_2 = 1+2$

$$a_n = 1+2+3+\dots+n = \sum_{i=0}^{n} i$$

$$\sum_{i=2}^{5} (i^2+1) = (2^2+1)+(3^2+1)+(4^2+1)+(5^2+1)$$

DOUBLE-COUNTING:

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & \dots & n \\ n & n-1 & n-2 & \dots & & 1 \\ \shortparallel & \shortparallel & & & & \shortparallel \\ n+1 & n+1 & & & & n+1 \end{array} \qquad \begin{array}{l} = a_n \\ = a_n \end{array}$$

$$2 \cdot a_n = n \cdot (n+1)$$

$$\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{k=1}^{n} 0 = k^3$$

$$\sum_{i=0}^{n} (i+1)^3 - i^3$$

$$(n+1)^3 = \boxed{\sum_{k=0}^{n} (k+1)^3 - k^3} = \sum_{k=0}^{n} (\cancel{k^3} + 3k^2 + 3k + 1) - \cancel{k^3} =$$

telescopica

$(\cancel{1^3} - 0^3)$

$\cancel{2^3} - \cancel{1^3}$

$\cancel{3^3} - \cancel{2^3}$

$4^3 - \cancel{3^3}$

$$= \sum_{k=0}^{n} 3k^2 + \sum_{k=0}^{n} 3k + \sum_{k=0}^{n} 1 =$$

$$= 3\sum_{k=0}^{n} k^2 + 3\sum_{k=0}^{n} k + n + 1$$

$$= 3\sum_{k=0}^{n} k^2 + 3\frac{n(n+1)}{2} + n + 1$$

$$(n+1)^3 = 3\sum_{k=0}^{n} k^2 + 3\frac{n(n+1)}{2} + n + 1$$

$$\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

In questo modo, anche $\sum_{k=1}^{n} k^3$, $\sum_{k=1}^{n} k^4$, eccetera

In generale, no formule belle

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

$a, b \qquad x_n = an + b$

$$\sum_{k=1}^{n} x_k = \sum_{k=1}^{n} ak+b = a\left(\sum_{k=1}^{n} k\right) + b\cdot n =$$

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

$$1 + x + x^2 + \dots + x^n = \frac{x^{n+1}-1}{x-1}$$

$x_n = an+b$ $\Updownarrow$

$$k=1,2,3,\dots \quad \begin{cases} x_0 = b \\ x_{k+1} = x_k + a \end{cases}$$

$x_n = a^n$ $\Updownarrow$

$$\begin{cases} x_0 = 1 \\ x_{k+1} = x_k \cdot a \end{cases} \quad k=1,2,3,\dots$$

$$\circledast \begin{cases} x_0 = c \\ x_{k+1} = a\cdot x_k + b \end{cases} \qquad \begin{cases} x_0 = 37 \\ x_{n+1} = 2x_n + 1 \end{cases} \quad n = \dots$$

<u>Idea</u>: senza b lo so fare, trasformo ed elimino b:

$$y_k = x_k + \alpha$$

$$\circledast \begin{cases} y_0 = c + \alpha \\ y_{k+1} = x_{k+1} + \alpha = a x_k + b + \alpha = \end{cases}$$

$$= a(x_k+\alpha) - a\alpha + b + \alpha = a y_k + \underbrace{b + (1-a)\alpha}_{\text{t.n.}}$$

Posso scegliere α in modo che $\underbrace{\text{t.n.}}$ $= 0$

$$\alpha = -\frac{b}{1-a}$$

$$\begin{cases} y_0 = c - \frac{b}{1-a} \\ y_{k+1} = a y_k \end{cases} \Rightarrow y_n = \left(c - \frac{b}{1-a}\right) \cdot a^n$$

$$\forall n \in \mathbb{N} \quad x_n = y_n - \alpha = \left(c - \frac{b}{1-a}\right) a^n + \frac{b}{1-a}$$

$$\begin{cases} x_0 = 37 \\ x_{n+1} = 2x_n + 1 \end{cases} \rightarrow \begin{cases} y_0 = 38 \\ y_{n+1} = x_{n+1} + 1 = 2x_n + 2 = 2(x_n+1) = 2y_k \end{cases}$$

$$\boxed{y_n = x_n + 1}$$

$$\begin{cases} x_0 = \dots \\ x_1 = \dots \\ x_{n+2} = a x_{n+1} + b x_n + c \end{cases} \qquad n = 0, 1, 2, \dots$$

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

c si fa sparire col trucco di prima

$y_n = x_n +$ qualcosa,

scelgo bene "qualcosa"

ignoriamole per un attimo

$$\begin{cases} x_0 = \dots & (1) \\ x_1 = \dots & (2) \\ x_{n+2} = a x_{n+1} + b x_n & (3) \end{cases}$$

Trucco: proviamo a cercare soluzioni del tipo

$$x_n = \lambda^n$$

$$\lambda^{\cancel{n}+2} = a\lambda^{\cancel{n}+1} + b\lambda^{\cancel{n}}$$

$$\Updownarrow$$

$$\lambda^2 = a\lambda + b \quad \begin{cases} \lambda_1 \\ \lambda_2 \end{cases} \text{ soluzioni}$$

$x_n = \lambda_1^n$ | $x_n = \lambda_2^n$ soddisfano (3)

$x_0 = 1$ | $x_0 = 1$

$x_1 = \lambda_1$ | $x_1 = \lambda_2$

Trucco n. 2: se ho due soluzioni di (3), x_n y_n

allora per ogni $p, q \in \mathbb{R}$ (o complessi...)

$z_n = p \cdot x_n + q \cdot y_n$ è anche lei soluzione di (3)

$$\begin{aligned} p \cdot &\left(x_{n+2} = a x_{n+1} + b x_n \right. \\ q \cdot &\left. y_{n+2} = a y_{n+1} + b y_n \right) \end{aligned}$$

$$\underbrace{p x_{n+2} + q y_{n+2}}_{} = a\left(p x_{n+1} + q y_{n+1}\right) + b\left(p x_n + q y_n\right)$$

$$z_{n+2} = a z_{n+1} + b z_n$$

In part. $z_n = p \cdot \lambda_1^n + q \cdot \lambda_2^n$ sono soluzioni

Se io vi do α e β, sapete trovarne una che ha $z_0 = \alpha$ $z_1 = \beta$

$$\begin{cases} \alpha = p + q \\ \beta = p \cdot \lambda_1 + q \cdot \lambda_2 \end{cases}$$

Risolvo il sistema, trovo p, q

Esempio: Fibonacci!

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

1) Trovo sol. speciali

$$\lambda^{n+2} = \lambda^{n+1} + \lambda^n \iff \underbrace{\lambda^2 = \lambda + 1}_{\text{polinomio caratteristico}}$$

$$\lambda^2 - \lambda - 1 = 0 \qquad \lambda_{12} = \frac{1 \pm \sqrt{5}}{2}$$

2) aggiusto cond. iniziali: trovo p, q

$z_n = p \cdot \lambda_1^n + q \cdot \lambda_2^n$ tale che

$$\begin{cases} 0 = F_0 = z_0 = p + q \\ 1 = F_1 = z_1 = p \cdot \lambda_1 + q \cdot \lambda_2 \end{cases}$$

$$\begin{cases} p + q = 0 \\ p\left(\frac{1+\sqrt{5}}{2}\right) + q\left(\frac{1-\sqrt{5}}{2}\right) = 1 \end{cases}$$

$q = -p \quad p\left(\frac{\cancel{1}+\sqrt{5}}{2} - \frac{\cancel{1}-\sqrt{5}}{2}\right) = 1$

$p \cdot \sqrt{5} = 1 \quad p = \frac{1}{\sqrt{5}} \quad q = -\frac{1}{\sqrt{5}}$

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

Magicamente, per ogni n i $\sqrt{5}$ si semplificano e viene un numero intero (provate per es. per $n=2,3$)

<u>Dettaglio</u>: $\begin{cases} z_0 = 0 \\ z_1 = 1 \\ z_{n+2} = z_{n+1} + z_n \end{cases} \overset{?}{\Longrightarrow} z_n = F_n\ ?$

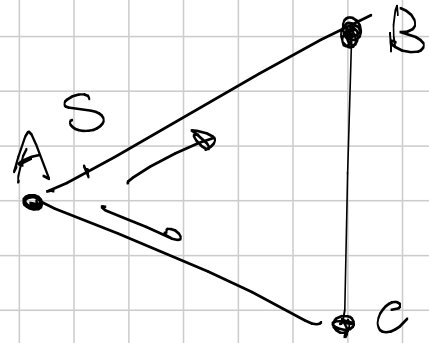
sì: induzione!

Cosa può andare storto nel metodo sopra?

1) l'eq. di 2° grado non ha sol. reali
→ uso i complessi

2) $\lambda_1 = \lambda_2$ <u>Trucco</u>: $x_n = \lambda_1^n \quad y_n = n \cdot \lambda_1^n$

3) Il sistema per p, q non ha sol.
no mai! $\lambda_1 \neq \lambda_2$ (claim)



S gira tra i bar A, B, C

Parte da A al tempo 0

Ad ogni "passo" prende una strada a caso delle due e va al bar in fondo a quella strada

Qual è la probabilità che sia in A (o B o C) dopo 2013 passi?

$A_k = \text{Prob}(\text{al bar } A \text{ al tempo } k)$

B_k, C_k analoghi

$A_0 = 1 \qquad B_0 = 0 \qquad C_0 = 0$

$$\begin{cases} A_{k+1} = \frac{1}{2} B_k + \frac{1}{2} C_k \\ B_{k+1} = \frac{1}{2} A_k + \frac{1}{2} C_k \\ C_{k+1} = \frac{1}{2} A_k + \frac{1}{2} B_k \end{cases}$$

$B_k = C_k$ (simmetria, o induzione)

shift!

$$\begin{cases} A_{k+1} = B_k \; (+\alpha A_k) \leftarrow A_k = B_{k-1} \\ B_{k+1} = \frac{1}{2} A_k + \frac{1}{2} B_k \end{cases}$$

$$\boxed{B_{k+1} = \frac{1}{2}B_k + \frac{1}{2}B_{k-1}}$$

$$\lambda^2 = \frac{1}{2}\lambda + \frac{1}{2}$$

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

$$\lambda_{1,2} = \frac{1 \pm \sqrt{1+8}}{4} = \begin{cases} 1 \\ -\frac{1}{2} \end{cases}$$

$$B_k = p \cdot 1^k + q \cdot \left(-\frac{1}{2}\right)^k$$

$$B_0 = 0 \qquad B_1 = \frac{1}{2}$$

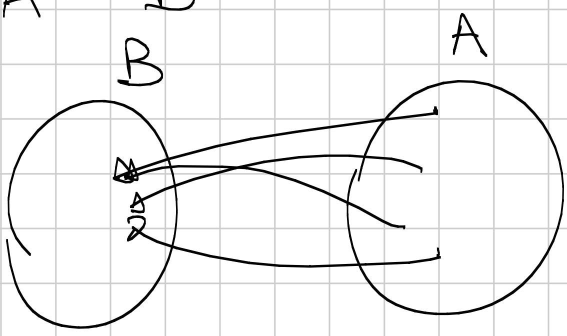
risolvo, $B_k = \frac{1}{3} - \frac{1}{3}\left(-\frac{1}{2}\right)^k$

FUNZIONI

cosa <u>non</u> è una funzione

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

$f : A \to B$



$f: \mathbb{N} \to \mathbb{N}$ {numero di volte che la lettera "e" compare nel nome del numero}

$f: \mathbb{R} \to \mathbb{R}$ $f(x) = \begin{cases} 1 & \text{se } x \leq 37 \\ 2 & \text{se } x > 38 \\ 3 & \text{se } 37 < x \leq 38 \end{cases}$

$f: \mathbb{R} \to \mathbb{R}$ $f(x) = \begin{cases} 0 & \text{se } x \in \mathbb{Q} \\ 1 & \text{se } x \notin \mathbb{Q} \end{cases}$

Devo associare un elemento di B a <u>ogni</u> elemento di A

~~$f(x) = 1/x$ $f: \mathbb{R} \to \mathbb{R}$~~

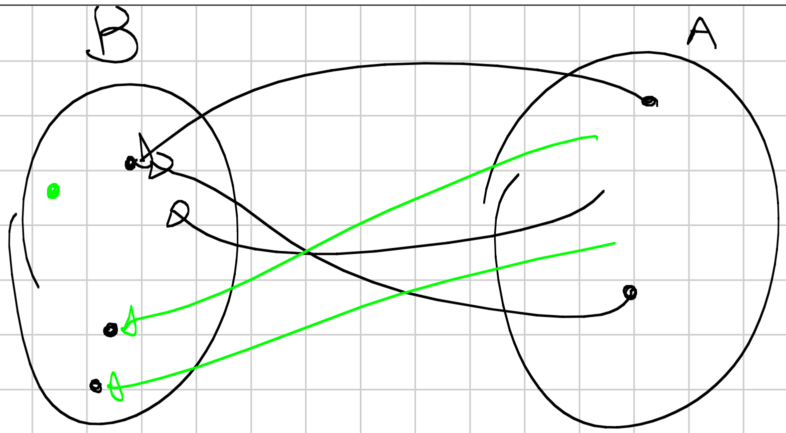
$f: \mathbb{R} \to \mathbb{R}$ $[0, \infty) \to (-1, 1)$

$f: A \to B$

obbligo indicazione

$f(x) = x^2$ $f: \mathbb{R} \to \mathbb{R}$

però -2 non viene preso mai



Iniettività: non esiste $b \in B$ su cui arrivano due frecce
Suriettività: ogni el. di B raggiunto da una freccia

In: $\forall a_1, a_2 \in A \quad a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$

Sur: $\forall b \in B \quad \exists a$ t.c. $f(a) = b$

$f(x) = x^2 \qquad \mathbb{R} \to \mathbb{R}$

$f(-1) = f(1) \Rightarrow$ no iniettiva

-1 non è $f(\text{niente}) \Rightarrow$ no suriettiva

Immagine di f: insieme dei val. raggiunti $[0, \infty)$

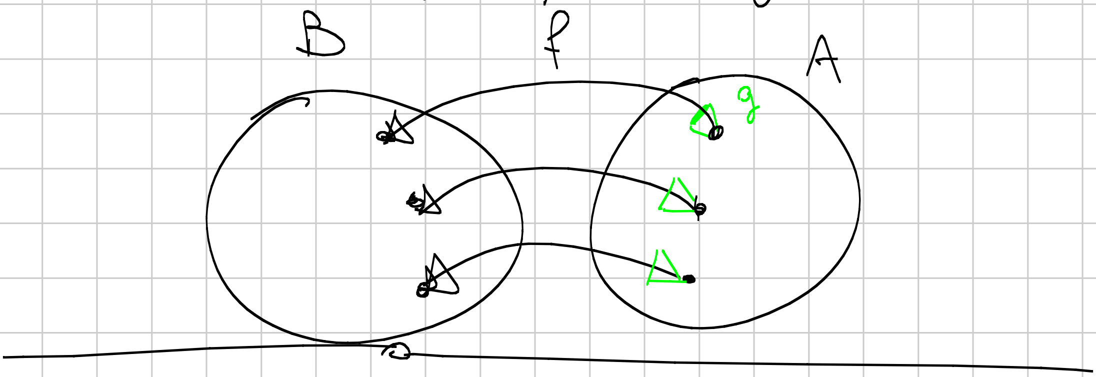
$f(x) = x^2 \qquad f: [0, \infty) \to [0, \infty)$

suriettiva: sì!
iniettiva: sì!

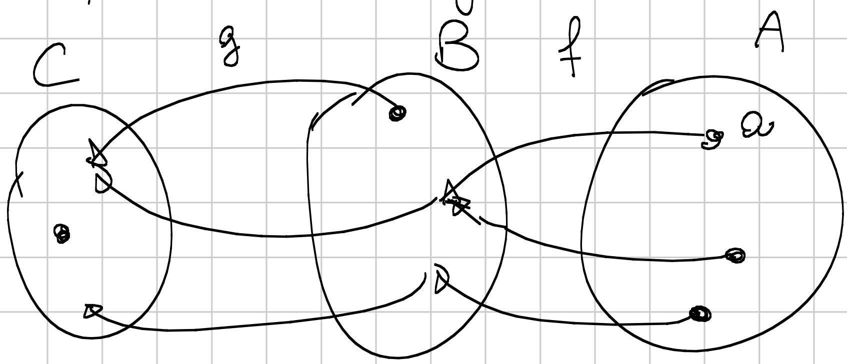
suriettiva + iniettiva = invertibile

$f_{:A \to B}$ in + surj $\Rightarrow$ esiste $g: B \to A$

tale che $f(g(b)) = b$ $\quad g(f(a)) = a$



$f: A \to B \qquad g: B \to C$



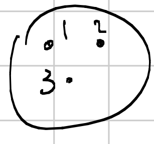
Dato $a \in A$, faccio

$$a \mapsto g(f(a)) \qquad g \circ f$$

$h: A \to C$

Occhio all'ordine!

$g \circ f$ vuol dire "prima f"



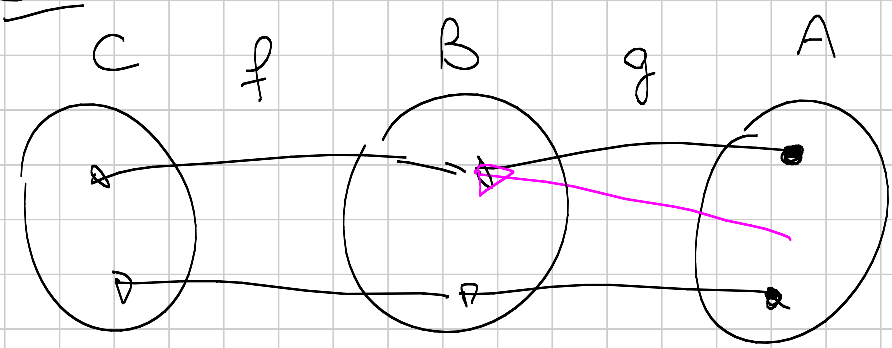
$f: \{1, 2, \dots 10\} \to \{1, 2, \dots 8\}$

$g: \{1, \dots 8\} \to \{1, \dots 10\}$

Th: $f \circ g$ iniettiva $\Rightarrow$ g iniettiva

$f \circ g$ suriettiva $\Rightarrow$ f suriettiva

Dim:



Monotonia: monotono $<$ crescente / decrescente

f crescente: $a \le b \Rightarrow f(a) \le f(b)$

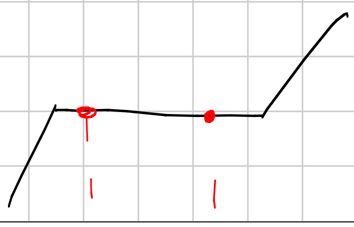
f strettamente crescente $a < b$ $\quad f(a) < f(b)$

decrescente $a \le b$ $\quad f(a) \ge f(b)$

str. dec. $a < b \Rightarrow f(a) > f(b)$

f str. cr. $\quad f(a) < f(b) \Leftrightarrow a < b$

f cr. $\quad f(a) \le f(b) \cancel{\Leftrightarrow} a \le b$



Equazione funzionale

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

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

Trovare tutte le $f:\mathbb{R}\to\mathbb{R}$ che soddisfano (*)

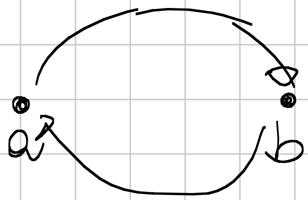
$f:\mathbb{Z}\to\mathbb{Z}$

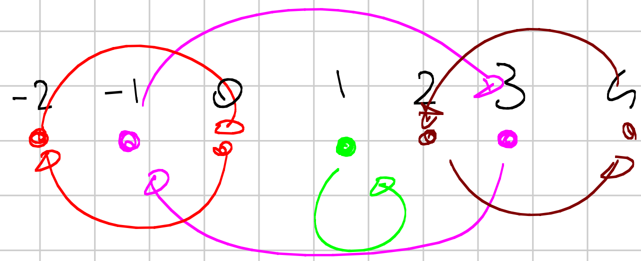
$$f(f(x)) = x$$

$f(x)=x$ funziona

$f(x)=-x$

Ce n'è una marea!





$f(-2)=0$ $\qquad$ $f(1)=1$

$f(-1)=3$ $\qquad$ $\vdots$

$f(0)=-2$

Equazione di Cauchy:

Trovare $f: \mathbb{R} \to \mathbb{R}$ tale che

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

Dim: i) Dimostro che $f(0) = 0$

Uso $P(0,0)$

$$f(0+0) = f(0) + f(0)$$
$$\Downarrow$$
$$f(0) = 2f(0)$$
$$\Downarrow$$
$$f(0) = 0$$

quando scrivete le formule "presentate" le variabili

~~$P(0,y)$: $f(0+y) = f(0) + f(y)$~~ $\boxed{\forall y \in \mathbb{R}}$

ii) Provo che $f(-x) = -f(x)$

$P(x,-x)$:

$$0 = f(0) = f(x-x) = f(x) + f(-x) \quad \forall x \in \mathbb{R}$$
$$\Downarrow$$
$$f(-x) = -f(x)$$

Diamo un nome a $f(1)$: $\quad f(1) = a$

iii) Provo che $f(2) = 2a$

$P(1,1)$: $f(1+1)=f(1)+f(1)=2a$

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

iv) Dimostro che $f(n)=an \quad \forall n\in\mathbb{N}$

Passo base ...

Passo ind. $P(n,1)$: $f(n+1)=f(n)+f(1)=na+a$

v) $f(n)=an \quad \forall n\in\mathbb{Z}$

Per (ii), $f(-n)=-f(n)=-an \quad \forall n\in\mathbb{N}$

quindi $f(x)=ax$ anche per x int. negativo.

vi) (**) $f(x_1+x_2+x_3+\dots+x_n)=f(x_1)+f(x_2)+\dots+f(x_n)$
$\forall x_1,x_2,\dots x_n\in\mathbb{R}$

<u>Per induzione</u>:

$P(x_1+x_2+\dots+x_n,\ x_{n+1})$

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

vii) $f\left(\frac{1}{n}\right)=a\cdot\frac{1}{n}$

Applico (**) con $x_1=x_2=\dots=x_n=\frac{1}{n}$

$$f(\underbrace{\tfrac{1}{n}+\tfrac{1}{n}+\dots+\tfrac{1}{n}}_{n\text{ volte}})=\underbrace{f\left(\tfrac{1}{n}\right)+f\left(\tfrac{1}{n}\right)+\dots+f\left(\tfrac{1}{n}\right)}_{n\text{ volte}}$$

$a = f(1) = n\, f(\frac{1}{n})$

vii) $f(\frac{k}{n}) = a \cdot \frac{k}{n}$ razionali positivi

$$f(\underbrace{\tfrac{1}{n}+\tfrac{1}{n}+\tfrac{1}{n}+\ldots+\tfrac{1}{n}}_{k \text{ volte}}) = \underbrace{f(\tfrac{1}{n})+f(\tfrac{1}{n})+\ldots+f(\tfrac{1}{n})}_{k \text{ volte}}$$

$$f(k/n) = k\,a \cdot \frac{1}{n}$$

ix) raz. negativi

x) verifica sui razionali $a(x+y) = f(x+y)$

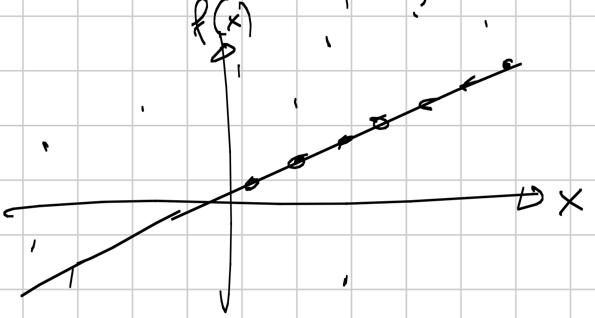
$f(x)+f(y) = ax+ay$

Manca da $\mathbb{Q}$ a $\mathbb{R}$

no ci sono tante funzioni (anche brutte)

che soddisfano $f(x+y) = f(x)+f(y)$, su $\mathbb{R}$

non solo $f(x) = a \cdot x$



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

Th: se esiste un quadratino del piano su cui il grafico di f non passa, allora

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

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

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

$$P(x,0): \quad f(x^2) = [f(x)]^2 + \cancel{f(0)}$$

$$P(0,0): \quad \cancel{f(0)} = f(0)^2 + \cancel{f(0)} \quad \Rightarrow \quad f(0) = 0$$

$$(*) \quad f(x^2) = [f(x)]^2$$

$$Q(x,y): f(x^2+y) = f(x^2) + f(y) \qquad x^2 =: z$$

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

$\forall z \geq 0 \leftarrow$ occhio!

Dati z, y ($z \geq 0$), scelgo

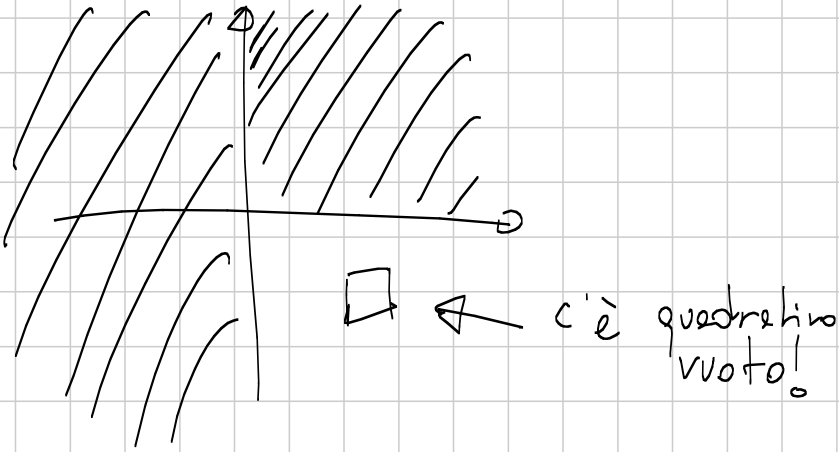
$$Q(\sqrt{z}, y) \quad : \quad f(z+y) = f(z) + f(y)$$

$$R(t,-t) \quad : \quad f(-t) = -f(t) \quad \forall t \in \mathbb{R}$$

$$(*) \quad f(x^2) = [f(x)]^2 \geq 0$$

$\Rightarrow \forall z \geq 0$ z

$$f(z) = f\left((\sqrt{z})^2\right) \overset{!}{=} \left[f(\sqrt{z})\right]^2 \geq 0$$



→ crescenza, monotonia

→ continuità

Riepilogo degli errori comuni:

→ $ffx = x$ non segue $f(x) = x$

$$ffx = f(x+8)$$

$\cancel{\Downarrow}$ iniettività

$$f(x) = x+8$$

→ $f(f(x)) = f(x) + 8 \quad \forall x \in \mathbb{R} \quad f(x) = z$

$f(z) = z + 8 \quad \cancel{\forall z \in \mathbb{R}}$

a meno che non sia suriettiva

$$f(f(x)) = 3x^3 + 5$$

biiettive = iniett + surj

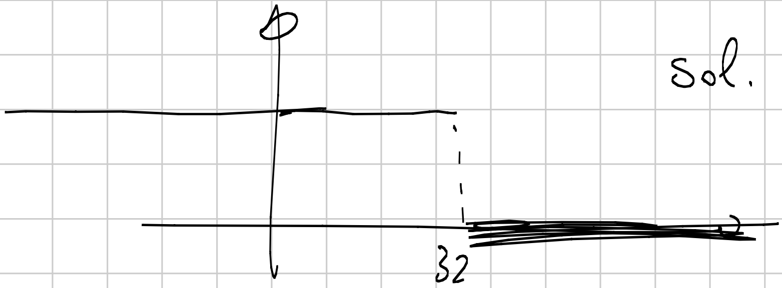
bigettiva   bijective
biiettiva

bi

$$f(x) = [f(x)]^2 \Rightarrow \begin{array}{l} f(x)=0 \\ f(x)=1 \end{array}$$

Allora le sol. sono $f(x)=1$ $f(x)=0$ No!

sol. miste



Prendo a $f(a)=0$
b $f(b)=1$

$$f((x+y)+z) \qquad f(x+(y+z))$$

$$f\left(x+y^2+2xf(x)f(y^2)\right) = \underline{\underline{f(x)}}\,f(y)$$

$$f\left(y+x^2+2y\,f(y)f(x^2)\right)$$

Tanti esempi sui senior scorsi...

Combinatoria 1 Basic (LAB)

Titolo nota 03/09/2013

Fattoriale

Podio 3 classificati con 10 partecipanti

$$10\cdot 9\cdot 8 = \frac{10!}{7!}$$

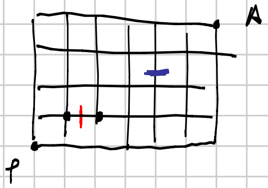
Borse ai primi tre $\frac{10!}{7!\,3!} = \binom{10}{3} = \binom{10}{7}$

Anagrammi

SCATOLE $7!$ SC adiacenti $\longrightarrow$ X $6!$

S prima di C $\frac{7!}{2}$

$* \underbrace{S \_ C}_{Y} *$ $5\cdot 5!$



$6\times\rightarrow$ $4\times\uparrow$ $\frac{10!}{6!\,4!}\left[=\binom{10}{6}=\binom{10}{4}\right]$

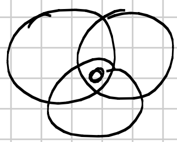
Con posto di blocco

$$\frac{10!}{6!\,4!} - 2\cdot 1\cdot\frac{7!}{4!\,3!}$$

Con 2 posti di blocco

T $-$ {Vie per 1° blocco} $-$ {Vie per 2° blocco} $+$ {Vie per entr.}

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



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

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & & 1 & & \\ & 1 & & 2 & & 1 & \\ 1 & & 3 & & 3 & & 1 \\ \_ & & \_ & & \_ & & \_ \end{array}$$

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

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

In quanti modi posso scrivere 15 come somme ordinate di 5 interi positivi?

$$\circ \mid \circ \mid \circ \ \circ \ \circ \ \circ \ \circ \ \circ \mid \circ \ \circ \ \circ \ \circ \ \circ \ \circ \mid \circ$$

$\binom{14}{4}$

n come somme ord. di k int >0

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

Ex: in quanti modi posso scr. 15 come somme ord. di 5 interi ≥ 0.

Probl. 30 giocatori con maglie 1 — 30.
In quanti modi posso scegliere 11 giocatori senza maglie con # cons.?

$1 \dots n$ ne prendo k non consecutivi

$1 \dots m$ ne prendo k $\qquad \binom{m}{k}$

$s_1, \ s_2+1, \ s_3+2, \ \dots, \ s_k+(k-1)$ stanno in $1, \dots, m+k-1$

$m+k-1 = n \qquad m = n-k+1$

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

1 3 19 79 r_1
· 25 r_2

$c_1\ c_2 \ldots$

$\sum c_i = \sum r_i$

Probabilità

$$P = \frac{\# F}{\# T}$$

P di vincere alla lotteria $= \frac{1}{2}$

NO

Casi equiprobabili .... definizione ricorsiva

$P(U) = 1$ $\quad$ $P(A^c) = 1 - P(A)$

$P(\phi) = 0$

2 d 12 risultato del prodotto 5 &

$\cancel{\frac{1}{3}}$ $\quad$ $\frac{1}{3} - \frac{1}{36} = \frac{11}{36}$ $\quad$ $\cancel{\frac{1}{6}}$

||| $\quad$ ||| $\quad$ |||

$$\frac{1}{6} \cdot 1 + \frac{5}{6} \cdot \frac{1}{6} = \frac{11}{36}$$

$P(A \cup B) = P(A) + P(B) - P(A \cap B)$

$P(A \cap B \cap C) =$ inc. escl. $\quad$ $P(A \cap B)$ non nec. $= P(A)P(B)$

1/2 |

1/3 |||

1/4 ||||

1/12

Altro | 2/3

MM	MF
FM	~~FF~~

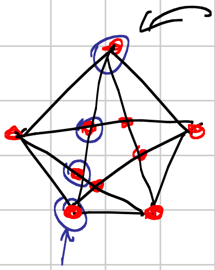
Titolo nota 04/09/2013

COMBINATORIA 2 basic

Problema 1. Drago a 100 teste.
Spada taglia 15, 17, 20, 5 teste.
Gli ricrescono 24, 2, 14, 17 ".
Per ucciderlo devo tagliargli tutte le teste.

Idea a ogni colpo di spada
+9, −15, −6, 12 teste.
→ non cambia il resto nella divisione per 3.

Problema 2.



lampadine accese

Posso cambiare stato a lati/diagonali.

Voglio spegnere tutto.

Ad ogni mossa cambiano 2 lampadine sul perimetro → parità del # di lampadine spente sul perimetro è INVARIANTE → da 0 spente non arrivo a 5!

Problema per dopo: esagono regolare.

Problema 3. Un gioco fra A e B

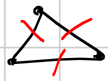
vertici archi

$G = (V, E)$

semplice

coppie di el. di V

A turno una mossa del tipo

-  cancello triangolo   oppure
-  inverto ✓

Domanda: come si gioca per vincere?
(Chi non può più muovere perde.)

OSS #1. il gioco finisce perché gli archi diminuiscono.

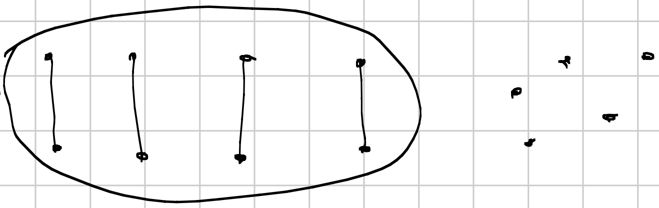
OSS #2. quanti archi incidono su v
$= d(v)$
↑ grado di v

ad ogni mossa 3 oppure 1 vertice hanno il grado diminuito di 2.

→ CANDIDATO INVARIANTE!
parità del grado di ogni vertice.

→ OSS #3. Quando il gioco finisce?
Quando i gradi sono 0 o 1;
una situazione del genere:

quelli che avevano d disp. $= m$



$\frac{m}{2}$ archi

PARENTESI: m era necessariamente PARI.

$$\sum_{x \in V} d(x) = 2|E|$$

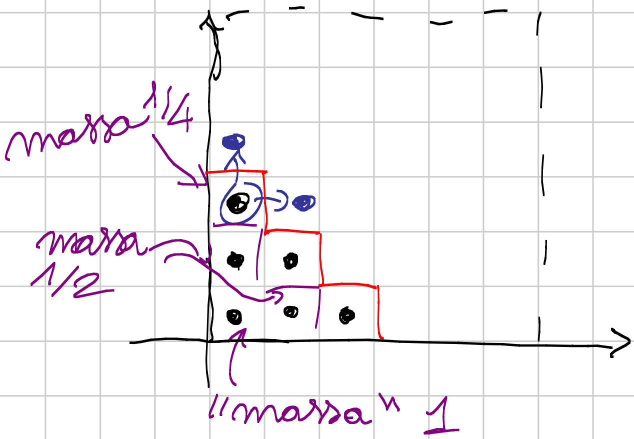
↑ # archi

→ m = # vertici di d disp
dev'essere pari.

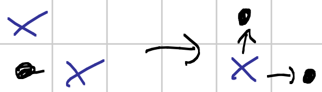
OSS #4 Quanti archi devo togliere?
$|E| - \frac{m}{2}$.

Il vincitore è determinato!
Tolgo $m/2$ archi a colpi di 1 o di 3: ad ogni mossa tolgo dispari $\longrightarrow$ la parità delle mosse è la stessa di $m/2$.

Problema 4



massa:



posso "pulire" la zona coperta all'inizio?

diagonale $n \longrightarrow$ massa $\frac{1}{2^{n-1}}$

la massa totale delle caselle con • sulla scacchiera è invariante! In partenza era $2 + \frac{3}{4}$.

Vorrei dim. che non basta il complementare della mia zona per prendersi tutta la massa.

La massa della prima colonna è $1 + \frac{1}{2} + \frac{1}{4} + \dots = 2$

2^a

$\frac{1}{2} + \frac{1}{4} + \dots = 1 = \frac{1}{2} \cdot 2$

3^a

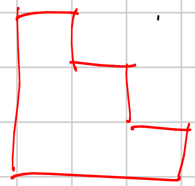
$\frac{1}{2} = \frac{1}{4} \cdot 2$

...

La massa totale $2\left(1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots\right) = 4$

Quindi NON potrò mandare i • in una zona che ha massa totale
$4 - 2 - 3/4 < 2$ → ho perso! :(

Problema per dopo: c'è un solo pallino in $(0,0)$. Volete pulire



Ce la fate?

Problema 5. 12 nani. Alcuni hanno la casa altri
A gennaio il nano corrispondente si adegua alla maggioranza degli altri. A un certo punto smetteranno di ridipingere?
Variante. Ogni nano si adegua alla maggioranza dei SUOI amici.

"invariante"

\# coppie con casa di colore diverso.

A ogni passaggio diminuisce o sta fermo.

→ ma forse meglio

\# coppie di amici con case di colore diverso

→ se tizio non cambia colore
rimane uguale
→ se tizio cambia colore
diminuisce.

Da un certo punto in poi quella quantità rimane fissa! Ma allora i nani non stavano cambiando colore alle case.

Problema per dopo:

Avete un grafo con almeno un arco. Dimostrate che esiste una partizione dei suoi vertici in due parti in modo che ci siano più archi fra le due parti che "dentro".

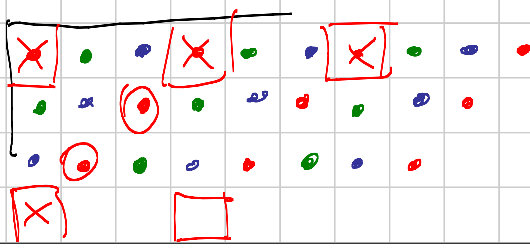
Problema 6. Scacchiera $n \times n$, tolgo 2 angolini opposti. Posso tassellarla con tessere del domino?

(n dispari → n^2-2 è dispari → non si tassella)

No! Perché coloro "a scacchiera" e ho tolto 2 angoli dello stesso colore ma ...

Problema 7. Scacchiera 10×10, tasselli

"tassello" con 33 pezzi.
Dove può stare il buco?



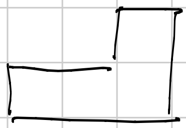
Sulla scacchiera c'è un • in più
→ il buco dev'

essere •.

In ENTRAMBE le colorazioni; le caselle □ POSSONO rimanere

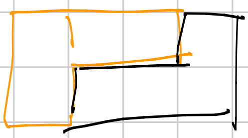
devo dimostrarlo! (esempio)

Problema 8. Quali rettangoli $m \times n$ posso tassellare con "



" ?

- $4h \times 2k$ SI



- mn dev'essere multiplo di 4
- Ma pare anche di 8 ... perché?

$2d_1 \times 2d_2$ $\qquad$ $4d_1 \times d_2$

lato pari

coloro a strisce

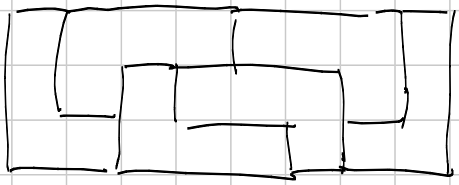
* una L copre 1 bianca e 3 nere (o viceversa)

\# caselle bianche = # caselle nere $= 2d_1 d_2$ ← PARI!

Quanti pezzi servono?
Servono in # pari per *
In totale però $\frac{4d_1 d_2}{4}$ pezzi ← DISPARI!

Quindi non riesco a tassellare se $8 \nmid mn$

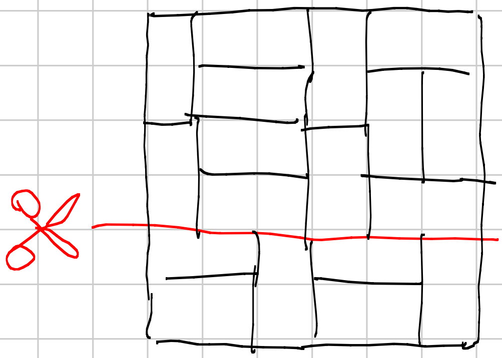
– Riesco a tassellare $8h \times d$? $d \geq 3$

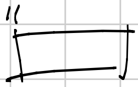


ho vinto :)

CONCLUSIONE: riesco a tassellare $\Leftrightarrow$ $8 \mid mn$, $m, n \geq 2$.

Problema extra:



6×6 tassellata con "".

Dimostrare che (comunque tassellata) esiste un "taglio"

Problemi $d(n) =$ "somma cifre di n"

Risolvere $n + d(n) + d(d(n)) = 2014$.

ho un'eq. di 2° grado $ax^2 + bx + c$; posso scambiare a con c oppure sostituire a "x" "$x+t$" (con $t \in \mathbb{R}$ a mia scelta). Posso portare $x^2 - x - 2$ in $x^2 - x - 1$?

+ problemi sopra (esagono, bipartizioni, tagli pulire angolo della scacchiera)

"Soluzioni"

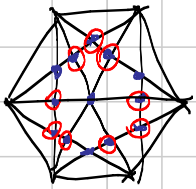
$$\Delta^2 = b^2 - 4ac$$

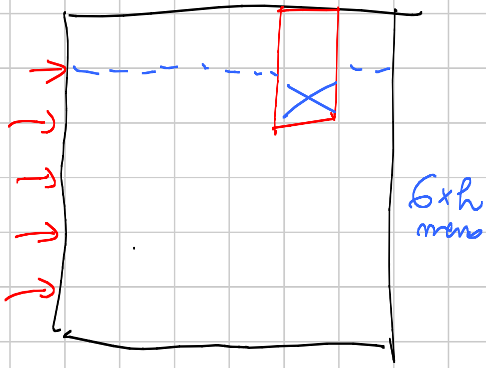
– scambiare a e c è chiaro;

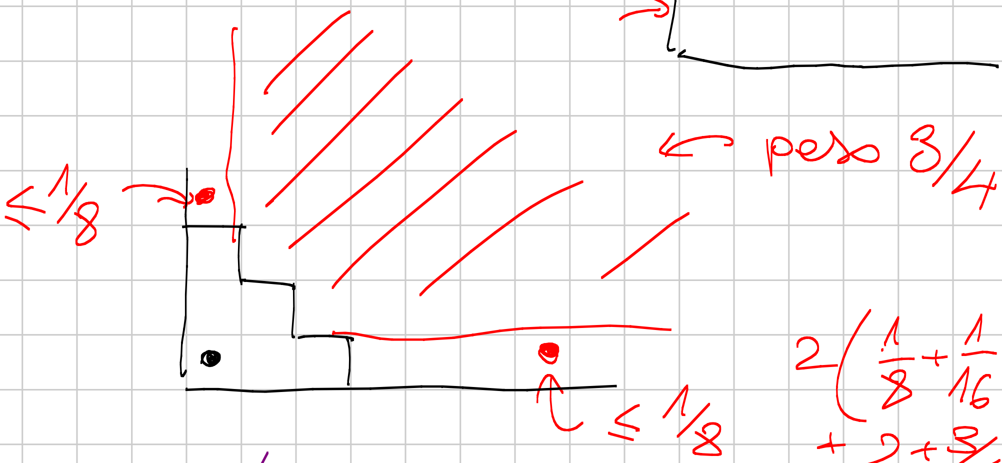
– $\Delta^2 = a^2\left(\frac{b^2}{a^2} - 4c/a\right) = a^2(S^2 - 4P)$

$$= a^2(x_1^2 + x_2^2 - 2x_1x_2) =$$
$$= a^2(x_1 - x_2)^2$$

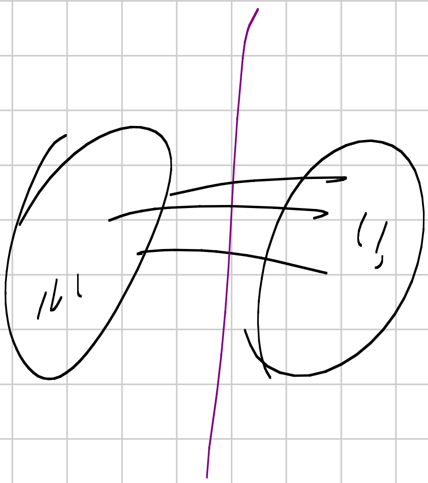
Esagono



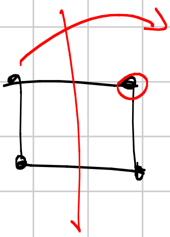




$$2\left(\frac{1}{8} + \frac{1}{16} + \dots\right) + 2 + 3/4 =$$
$$= 2 + \frac{1}{2} + 3/4$$
$$4 - \dots = 3/4$$



$$\sum_x \#\text{amici}(x) - \#\text{nemici}(x)$$



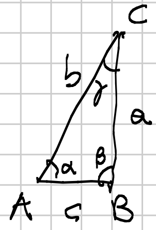
$= 2\,\#$archi "interni" $- 2\,\#$archi "esterni"

→ la faccio diventare negativa?

Geometria 1 Basic (LAB)

Titolo nota 02/09/2013

$\downarrow$ Geom Sintetica G3 $\uparrow$
Analitica ... G2
Trigonometria G1



$\beta = 90°$

$\alpha + \gamma = 90° \Rightarrow \alpha, \gamma < 90°$ ACUTI

$$\cos\alpha = \frac{c}{b} = \frac{AB}{AC} = \frac{\text{cateto adiacente ad } \alpha}{\text{ipotenusa}}$$

$$\sin\alpha = \frac{a}{b} = \frac{CB}{AC} = \frac{\text{cat. opposto } \alpha}{\text{ipotenusa}}$$

$$\cos\gamma = \frac{a}{b} = \sin\alpha \qquad \cos(90° - \alpha) = \sin\alpha$$

$$\sin\gamma = \frac{c}{b} = \cos\alpha \qquad \sin(90° - \alpha) = \cos\alpha$$

$$\operatorname{tg}\alpha = \tan\alpha = \frac{\text{cateto opposto}}{\text{cat. adiacente}} = \frac{a}{c} = \frac{a}{b} \cdot \frac{b}{c}$$

$$= \frac{\sin\alpha}{\cos\alpha}$$

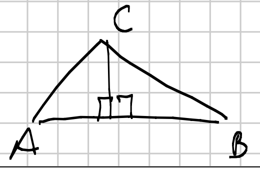
$$\operatorname{tg}\gamma = \frac{c}{a} = \frac{1}{\operatorname{tg}\alpha} =: \operatorname{cotg}\alpha \qquad \operatorname{tg}(90° - \alpha) = \operatorname{cotg}\alpha$$

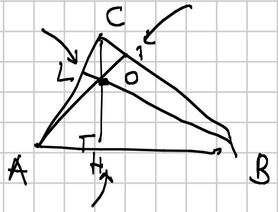
$a = b \cdot \sin\alpha \qquad c = b \cdot \cos\alpha$

$= b \cdot \cos\gamma \qquad = b \cdot \sin\gamma$

$$a^2 + c^2 = b^2 \longrightarrow \cancel{b^2} \cdot \sin^2\alpha + \cancel{b^2} \cdot \cos^2\alpha = \cancel{b^2}\ 1$$

$$\boxed{\sin^2\alpha + \cos^2\alpha = 1}$$





. Distanza di un vertice dall'ortocentro

. " " " lato " "

$AO = ?$ $\qquad T_{AOH}$ retto in H

$$\frac{AH}{AO} = \cos(O\hat{A}H) = \cos(90° - \beta) = \sin\beta$$

$$OA = \frac{AH}{\sin\beta} \qquad AH = b \cdot \cos\alpha$$

$$= c - a \cdot \cos\beta$$

$$= b \cdot \frac{\cos\alpha}{\sin\beta}$$

$$= \frac{c - a \cdot \cos\beta}{\sin\beta}$$

$OI = ?$ 1. per differenze

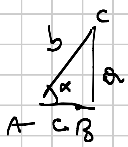
2. diretto $\qquad O\hat{C}B = 90° - \beta$

$$\frac{OI}{CI} = tg(O\hat{C}B) = cotg(\beta)$$

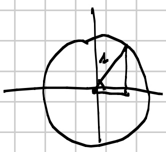
$$OI = (a - c \cdot \cos\beta) \cdot cotg\,\beta$$

$$CI = a - c \cdot \cos\beta$$

Torniamo indietro



$a = b \cdot \sin\alpha$ $\qquad$ caso interessante $b = 1$



Come misuriamo gli angoli

gradi vs lunghezza arco sotteso

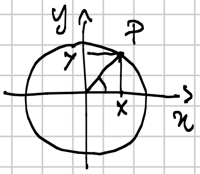
$$\alpha° \longleftrightarrow \alpha^{rad}$$

$$\frac{\alpha°}{360°} = \frac{\alpha^{rad}}{2\pi}$$

N.B. Stiamo considerando gli angoli con segno

↺ positivo $\qquad$ ↻ negativo

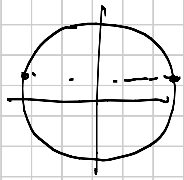
Come sono qu. $\sin\alpha$ e $\cos\alpha$



$x = \cos\alpha$
$y = \sin\alpha$

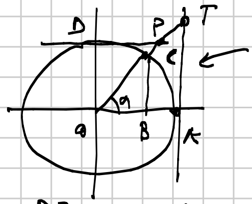
$360° \longleftrightarrow 2\pi$
$180° \longleftrightarrow \pi$
$90° \longleftrightarrow \pi/2$

Simmetrie & periodicità



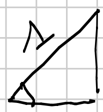
$$\sin(\alpha + 2\pi) = \sin\alpha$$
$$\cos(\alpha + 2\pi) = \cos\alpha$$
$$\sin(\pi - \alpha) = \sin\alpha$$
$$\cos(\pi - \alpha) = -\cos\alpha = \cos(\pi + \alpha)$$
$$\sin(\pi + \alpha) = -\sin\alpha = \sin(-\alpha)$$
$$\cos(-\alpha) = \cos\alpha$$
$$\cos\left(\frac{\pi}{2} - \alpha\right) = \sin\alpha \qquad \cos\left(\frac{\pi}{2} + \alpha\right) = -\sin\alpha$$
$$\sin\left(\frac{\pi}{2} - \alpha\right) = \cos\alpha \qquad \sin\left(\frac{\pi}{2} + \alpha\right) = \cos\alpha$$

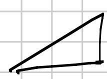
Tangente e cotangente

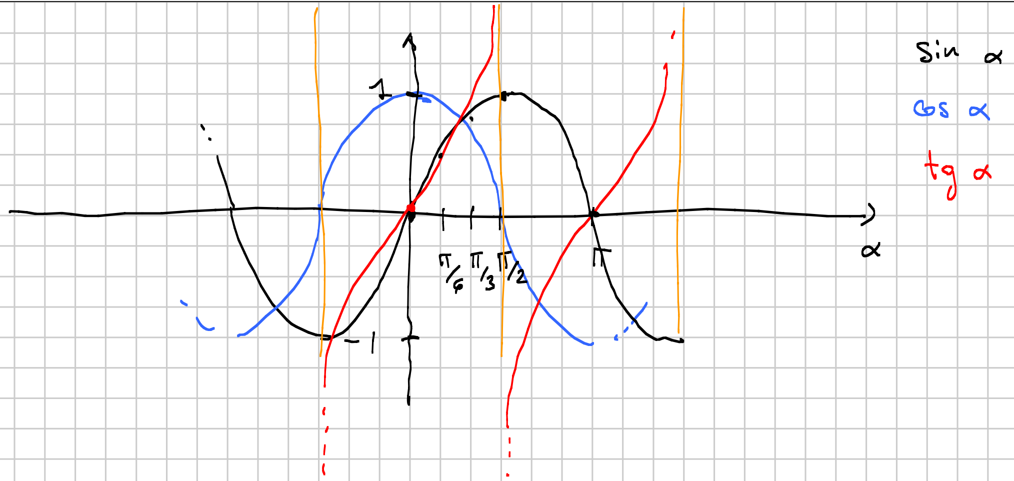


$$\operatorname{tg}\alpha = TA = \frac{TA}{OA} = \frac{PB}{BO} = \frac{\sin\alpha}{\cos\alpha}$$

		sin	cos	tg
	0	0	1	0
	$\pi/2$	1	0	?
	π	0	-1	0
	$\frac{3}{2}\pi$	-1	0	?
(45°)	$\pi/4$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{2}}{2}$	1
(60°)	$\pi/3$	$\sqrt{3}/2$	$1/2$	$\sqrt{3}$
(30°)	$\pi/6$	$1/2$	$\sqrt{3}/2$	$\frac{\sqrt{3}}{3}$







Q: È vero che $\sin x = \sin y \Rightarrow x = y$? NO

Restringere $\pi/2$, $\frac{3}{2}\pi$

$\left[\frac{\pi}{2} + 2k\pi, \frac{3}{2}\pi + 2k\pi\right]$ è monotona decresc

$\Rightarrow$ iniettiva ☺

$\left[-\frac{\pi}{2} + 2k\pi, \frac{\pi}{2} + 2k\pi\right]$ è monot. cresc.

$\Rightarrow$ iniettiva

Stessa cosa ma int. diversi per il coseno

Se le voglio entrambe $\longrightarrow \left[0 + \frac{k\pi}{2}, \frac{\pi}{2} + \frac{k\pi}{2}\right]$

La tangente? In $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ è monot. cres

$\Rightarrow$ iniettiva

ma è anche suriettiva

$\Downarrow$ invertibile

Funzioni inverse

$\operatorname{atan} x = \arctan x = \operatorname{arctg} x$ "arco la cui tangente è x"

$\mathbb{R} \longrightarrow \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$

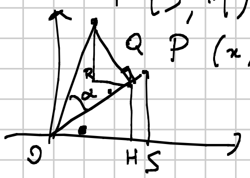
$\arcsin x = \operatorname{asin} x$

$[-1, 1] \longrightarrow \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$

$\arccos x = \operatorname{acos} x$

$[-1, 1] \longrightarrow [0, \pi]$.

Rotazioni $P'(\xi, \eta)$



Vogliamo ξ, η in termini di x, y, α

$$\rho^2 = x^2 + y^2 = \xi^2 + \eta^2$$

$$OQ = OP \cdot \cos\alpha$$

$$\frac{QH}{OQ} = \frac{PS}{OP} = \frac{y}{\rho}$$

$$\eta = P'R + QH$$

$$\boxed{QH = y \cdot \cos\alpha}$$

$$O\hat{P}S = O\hat{Q}H = 90^\circ - \bullet$$

$$90^\circ = O\hat{Q}P' = O\hat{Q}R + R\hat{Q}P = \bullet + R\hat{Q}P \implies O\hat{P}S = R\hat{Q}P$$

$$\frac{P'R}{P'Q} = \frac{OS}{OP} = \frac{x}{\rho} \qquad P'Q = \rho \cdot \sin\alpha$$

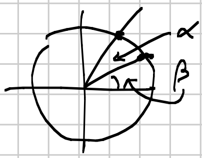
$$P'R = x \cdot \sin\alpha$$

$$\text{(EX)} \quad \begin{cases} \eta = x \cdot \sin\alpha + y \cdot \cos\alpha \\ \xi = x \cdot \cos\alpha - y \cdot \sin\alpha \end{cases}$$

Se $P \in B(0,1)$ $\quad x = \cos\beta \quad y = \sin\beta$

$$\xi = \cos(\alpha+\beta) = \cos\beta \cdot \cos\alpha - \sin\beta \cdot \sin\alpha$$

$$\eta = \sin(\alpha+\beta) = \cos\beta \cdot \sin\alpha + \sin\beta \cos\alpha$$



"EX" $\cos(\alpha-\beta) = ?$

$\sin(\alpha-\beta) = ?$

$$\cos(2\alpha) = \cos^2\alpha - \sin^2\alpha = 1 - 2\sin^2\alpha = 2\cos^2\alpha - 1$$

$$\sin(2\alpha) = 2\sin\alpha\cos\alpha$$

"EX" $\cos\left(\frac{\alpha}{2}\right)$

$\sin\left(\frac{\alpha}{2}\right)$

Tangenti

$$\operatorname{tg}(\alpha+\beta) = \frac{\sin(\alpha+\beta)}{\cos(\alpha+\beta)} = \dots = \frac{\operatorname{tg}\alpha + \operatorname{tg}\beta}{1 - \operatorname{tg}\alpha \operatorname{tg}\beta}$$

$$\operatorname{tg}(2\alpha) =$$

$$\operatorname{tg}\left(\frac{\alpha}{2}\right) = \dots = \frac{\sin\alpha}{1+\cos\alpha}$$

modo geom.

Formule parametriche $\quad t = \operatorname{tg}\left(\frac{\alpha}{2}\right)$

$$\sin\alpha = \frac{2t}{1+t^2} \qquad \cos\alpha = \frac{1-t^2}{1+t^2}$$

Proprietà interessante

$$0 < \alpha, \beta, \gamma < \pi$$

$$\alpha+\beta+\gamma = \pi \iff \operatorname{tg}\frac{\alpha}{2}\operatorname{tg}\frac{\beta}{2} + \operatorname{tg}\frac{\beta}{2}\operatorname{tg}\frac{\gamma}{2} + \operatorname{tg}\frac{\alpha}{2}\cdot\operatorname{tg}\frac{\gamma}{2} = 1 \qquad (*)$$

$[\Rightarrow]$

$$\operatorname{tg}\frac{\gamma}{2} = \operatorname{tg}\frac{\pi-\alpha-\beta}{2} = \operatorname{tg}\left(\frac{\pi}{2} - \frac{\alpha+\beta}{2}\right)$$

$$= \frac{1}{\operatorname{tg}\left(\frac{\alpha}{2}+\frac{\beta}{2}\right)} = \frac{1 - \operatorname{tg}\frac{\alpha}{2}\operatorname{tg}\beta/2}{\operatorname{tg}\frac{\alpha}{2} + \operatorname{tg}\beta/2}$$

che si ottiene da $(*)$ raccogliendo

$[\Leftarrow]$

$$\operatorname{tg}\left(\frac{\pi}{2} - \frac{\alpha+\beta}{2}\right) = \frac{1 - \operatorname{tg}\frac{\alpha}{2}\operatorname{tg}\beta/2}{\operatorname{tg}\frac{\alpha}{2} + \operatorname{tg}\beta/2} = \operatorname{tg}\frac{\gamma}{2}$$

$$\Downarrow$$

tg è iniettiva in $0, \frac{\pi}{2}$ & $\gamma \in (0,\pi) \Rightarrow \frac{\gamma}{2} \in (0, \pi/2)$

$$\Rightarrow \gamma/2 = \frac{\pi}{2} - \frac{\alpha}{2} - \frac{\beta}{2} \Rightarrow \text{tesi} \qquad \boxtimes$$

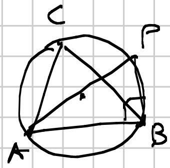
Ex: $\quad \alpha+\beta+\gamma = \pi \Rightarrow \operatorname{tg}\alpha + \operatorname{tg}\beta + \operatorname{tg}\gamma = \operatorname{tg}\alpha\cdot\operatorname{tg}\beta\cdot\operatorname{tg}\gamma$

$$\Rightarrow \sin\alpha + \sin\beta + \sin\gamma = 4\cos\frac{\alpha}{2}\cdot\cos\frac{\beta}{2}\cdot\cos\frac{\gamma}{2}$$

Teo dei Seni

$$\frac{a}{\sin\alpha} = \frac{b}{\sin\beta} = \frac{c}{\sin\gamma} = 2R$$

raggio circ. circoscritta



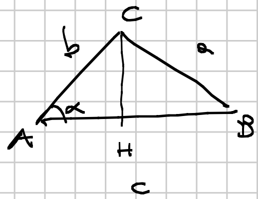
$$\hat{APB} = \gamma$$

$$c = 2R \cdot \sin\gamma$$

Teorema di Carnot (o dei Coseni o Pitagora general.)

Dati b, c lati e angolo α tra essi

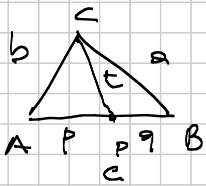
$$a^2 = b^2 + c^2 - 2bc \cdot \cos\alpha$$



Dim

$$\begin{aligned} a^2 &= BH^2 + CH^2 \\ &= BH^2 + b^2\sin^2\alpha \\ &= (c - b\cdot\cos\alpha)^2 + b^2\sin^2\alpha \\ &= c^2 - 2bc\cos\alpha \underbrace{+ b^2\cos^2\alpha + b^2\sin^2\alpha}_{= b^2} \end{aligned}$$

Teo Stewart

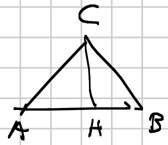


$$c\cdot(t^2 + p\cdot q) = b^2 q + a^2 p$$

Dim (EX) hint Carnot ..

Mediana (cor.)

$$t^2 = \frac{a^2 + b^2}{2} - \frac{c^2}{4}$$



Area

$$\begin{aligned} S_{ABC} &= \frac{AB \cdot CH}{2} \\ &= \frac{1}{2}\, c \cdot b \cdot \sin\alpha \\ &\overset{(\text{seni})}{=} \frac{a\cdot b\cdot c}{4R} \end{aligned}$$

<u>Erone</u> $p = \frac{a+b+c}{2}$ $S = \sqrt{p(p-a)(p-b)(p-c)}$

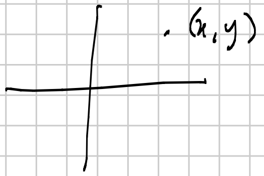
<u>Dim</u> $\cos\gamma = \frac{a^2+b^2-c^2}{2a\cdot b}$

$\sin\gamma = \ldots$

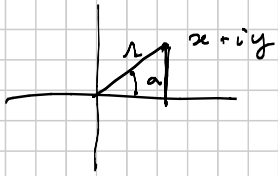
$S = \frac{1}{2} a\cdot b\cdot \sin\gamma = \ldots$

<u>Complessi</u>

$\mathbb{R}^2$



$\mathbb{C}$



i t.c. $i^2 = -1$

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

$z \in \mathbb{C}$ $\quad \mathrm{Re}(z) = \mathrm{Re}(z) = a$

$\shortparallel$

$a+ib$ $\quad \mathrm{Im}(z) = \mathrm{Im}(z) = b$

$(a+ib)\cdot(c+id) = ac + iad + ibc + i^2bd$

$= (ac - bd) + i(ad + bc)$

$|x+iy| = \sqrt{x^2+y^2}$

$\alpha = \arctan\left(\frac{y}{x}\right)$

se $x=0$ problem ..

$|z|\cdot(\cos\alpha + i\sin\alpha)$

$(\cos\alpha + i\sin\alpha)(x+iy) =$

$= x\cos\alpha - y\sin\alpha + i(x\sin\alpha + y\cos\alpha)$

$(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) =$

$= \cos(\alpha+\beta) + i\sin(\alpha+\beta)$

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

$$e^{i\alpha} \cdot e^{i\beta} = e^{i(\alpha+\beta)}$$

$$\boxed{z = |z| e^{i\alpha}}$$

$(x+iy)^n = ? = (EX)$ de Moivre

$n \in \mathbb{N}$

Esercizi

- $\sin\alpha \cdot \cos\beta = \frac{1}{2}\left(\sin(\alpha+\beta) + \sin(\alpha-\beta)\right)$
- $5\cos x + 2\sin x = 1$ risolvere (trovare x)
- Pag 29 esercizi 4 e 9

$$\sin\left(\frac{\alpha}{2}\right) = \pm\sqrt{\frac{1-\cos\alpha}{2}}$$

- $5X + 2Y = 1$

$t = tg\,\frac{x}{2}$ $\qquad 5\,\frac{1-t^2}{1+t^2} + 2\,\frac{2t}{1+t^2} = 1$

$$5 - 5t^2 + 4t - 1 - t^2 = 0$$

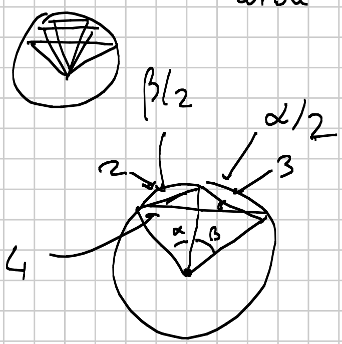
$$6t^2 - 4t - 4 = 0$$

$$tg\,\frac{x}{2} = t = \frac{1 \pm \sqrt{7}}{3}$$

$$\frac{x}{2} = \operatorname{atan}\left(\frac{1 \pm \sqrt{7}}{3}\right) + k\pi$$

corde lunghe 2, 3, 4

$\alpha \quad \beta \quad \alpha+\beta$



Dobbiamo calcolare $\cos\alpha$

Carnot

$$2^2 = 3^2 + 4^2 - 2 \cdot 3 \cdot 4 \cdot \cos\frac{\alpha}{2}$$

$$\cos\frac{\alpha}{2} = \frac{7}{8}$$

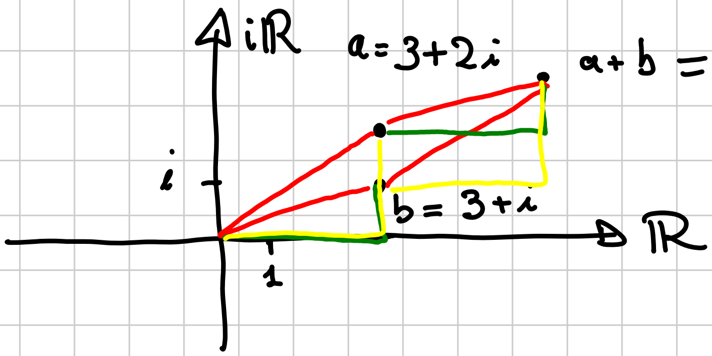
+ formula duplicazione ..

$$\cos\alpha = \frac{17}{32}$$

G 2 - Basic

Sam

Titolo nota 04/09/2013

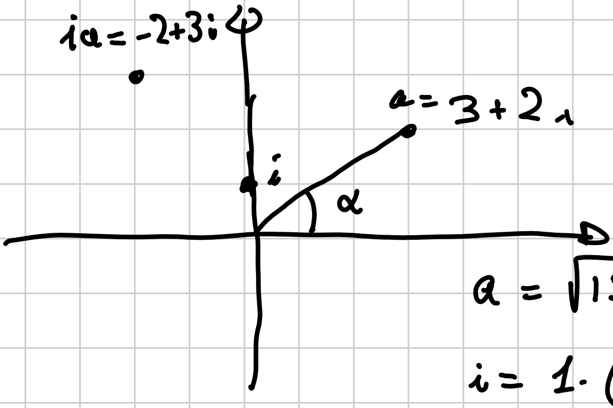


$A = (3, 2)$

$B = (3, 1)$

$C = (6, 3)$

t.c. OACB è un parallelogramma



$ia = -2+3i$

$a = \sqrt{13}\,(\cos\alpha + i\,\mathrm{sen}\,\alpha)$

$i = 1\cdot\left(\cos\frac{\pi}{2} + i\,\mathrm{sen}\,\frac{\pi}{2}\right)$

$a = x+iy$

$b = u+iv$

$ab = xu + ixv + iyu + i^2 yv =$

$= (xu - yv) + i(xv + yu)$

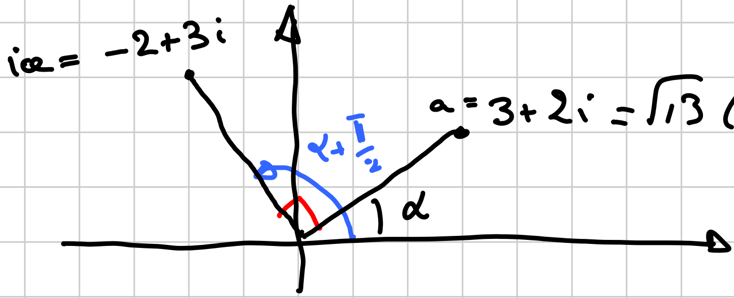
$a = r\cdot(\cos\alpha + i\,\mathrm{sen}\,\alpha)$

$b = R\cdot(\cos\beta + i\,\mathrm{sen}\,\beta)$

$ab = rR\big(\cos\alpha\cos\beta - \mathrm{sen}\,\alpha\,\mathrm{sen}\,\beta +$

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

$= rR\big(\cos(\alpha+\beta) + i\,\mathrm{sen}\,(\alpha+\beta)\big)$



$a = 3+2i = \sqrt{13}\,(\cos\alpha + i \operatorname{sen}\alpha)$

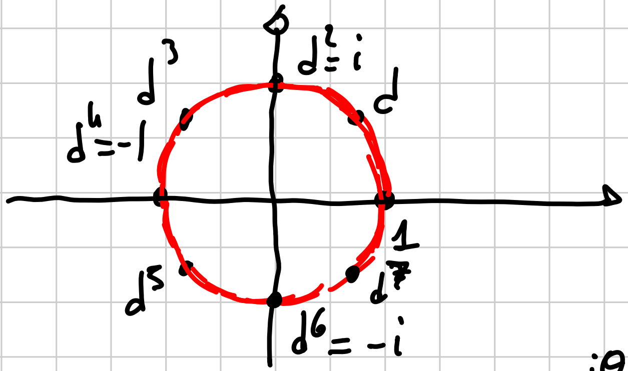
$i = 1\left(\cos\frac{\pi}{2} + i \operatorname{sen}\frac{\pi}{2}\right)$

$$ia = \sqrt{13}\left(\cos\left(\alpha+\frac{\pi}{2}\right) + i \operatorname{sen}\left(\alpha+\frac{\pi}{2}\right)\right)$$

dist da 0 — angolo formato con il semiasse reale positivo

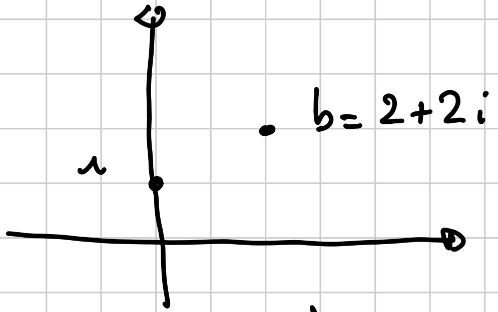
$$d = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}} = 1\left(\cos\frac{\pi}{4} + i \operatorname{sen}\frac{\pi}{4}\right)$$

$1, d, d^2, d^3, d^4, d^5, \ldots \quad d^8 = 1$



$c \longrightarrow c\,e^{i\theta}$ rot. in senso antiorario attorno all'origine di un angolo θ.

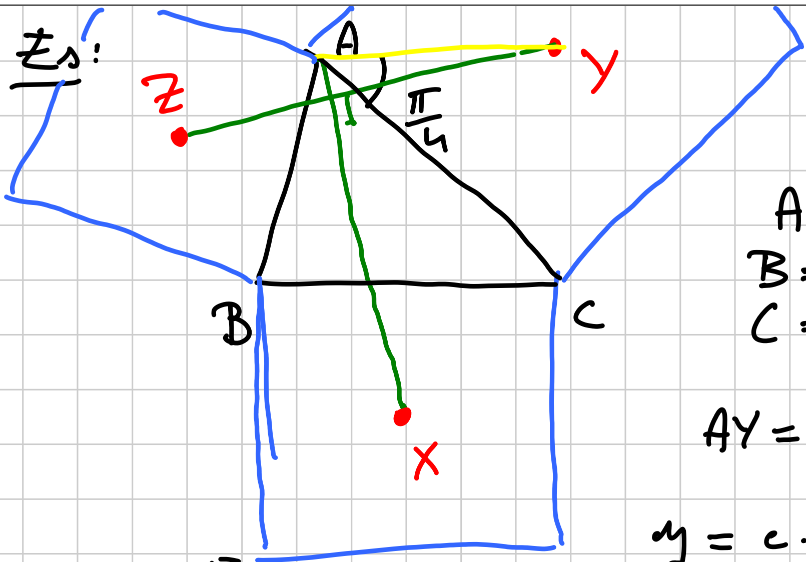
$$e^{i\theta} = \cos\theta + i \operatorname{sen}\theta$$



rotare b attorno a i di $\frac{\pi}{4}$.

$$b \xrightarrow[\text{Traslazione di } i \text{ nell'origine}]{} b-i \xrightarrow[\text{rot.}]{} (b-i)e^{i\frac{\pi}{4}} \xrightarrow[\text{Trasl. indietro}]{} (b-i)e^{i\frac{\pi}{4}}+i$$

Es:



$AX \perp ZY$

$A = 0$
$B = b$
$C = c$

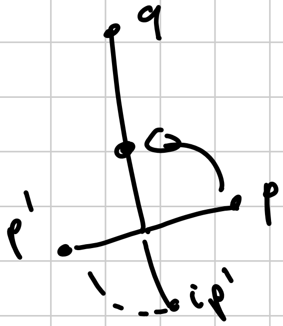
$$AY = \frac{AC}{2}\sqrt{2}$$

$$y = c \cdot e^{i\frac{\pi}{4}} \cdot \frac{\sqrt{2}}{2}$$

$$z = b \cdot e^{-i\frac{\pi}{4}} \cdot \frac{\sqrt{2}}{2}$$

$$(b-c)\,e^{i\frac{\pi}{4}} \cdot \frac{\sqrt{2}}{2} + c = x$$

Per verificare la $\perp$, portiamo uno tra Z e Y in A



$$Op \perp Oq \iff ip = kq$$
$$\Updownarrow$$
$$\frac{p}{q} = \frac{k}{i} = -ki$$
$$\Updownarrow$$
$\frac{p}{q}$ è immaginario puro.

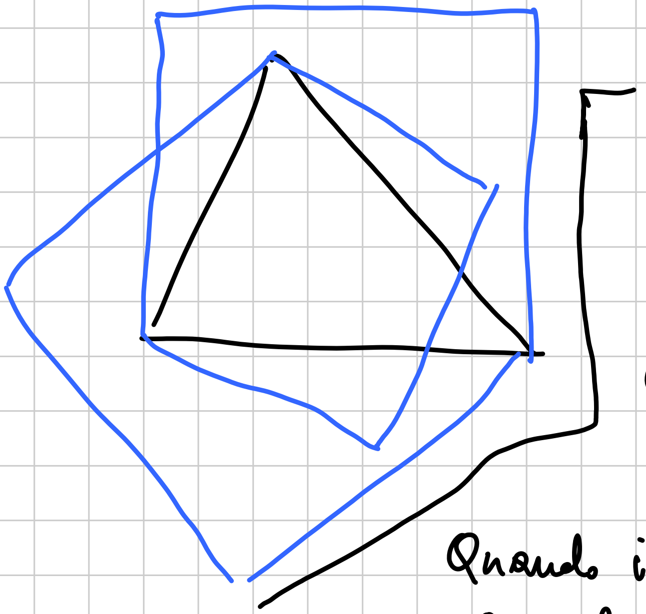
Concludendo
$$z - y = b e^{-i\frac{\pi}{4}} \frac{\sqrt{2}}{2} - c e^{i\frac{\pi}{4}} \frac{\sqrt{2}}{2}$$
$$x = (b-c)\,e^{i\frac{\pi}{4}} \frac{\sqrt{2}}{2} + c$$

$$z - y = b\left(\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}\right)\frac{\sqrt{2}}{2} - c\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right)\frac{\sqrt{2}}{2} =$$
$$= \frac{b}{2} - \frac{bi}{2} - \frac{c}{2} - \frac{ci}{2}$$

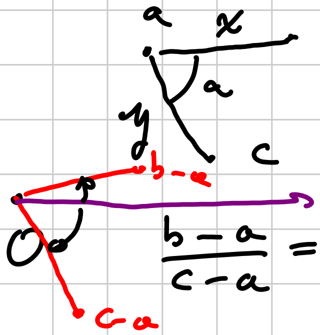
$$x = (b-c)(1+i)\frac{1}{2} + c = \frac{b}{2} + \frac{ib}{2} - \frac{c}{2} - \frac{ic}{2} + c =$$

$$= \frac{b}{2} + \frac{ib}{2} + \frac{c}{2} - \frac{ic}{2} =$$

$$= i\left(\frac{b}{2} - \frac{ib}{2} - \frac{c}{2} - \frac{ic}{2}\right) = i(z-y)$$



——— o ———



$$\frac{b-a}{c-a} = \frac{x}{y}e^{i\alpha}$$

Quando il Triangolo a, b, c è equilatero?

Quando $\frac{b-a}{c-a} = e^{i\frac{\pi}{3}}$

$$b - a = e^{i\frac{\pi}{3}}(c-a)$$

$$b + a\left(e^{i\frac{\pi}{3}} - 1\right) - c e^{i\frac{\pi}{3}} = 0$$

$$\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i - 1\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = e^{i\frac{2}{3}\pi}$$

$$-e^{i\frac{\pi}{3}} = e^{i\pi}\cdot e^{i\frac{\pi}{3}} = e^{i\frac{4}{3}\pi}$$

$$b + a e^{i\frac{2}{3}\pi} + c e^{i\frac{4}{3}\pi} = 0.$$

$$\omega = e^{i\frac{2}{3}\pi}$$

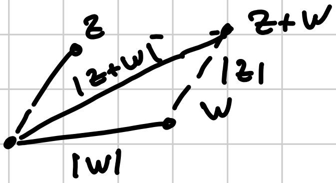
a, b, c formano un tr. equilatero

se e solo se $b + \omega a + \omega^2 c = 0$

oppure

$a + \omega b + \omega^2 c = 0$

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



Oss 2: z e $\overline{z}$ sono simmetrici rispetto alla retta reale.

Oss 3: z, w, t sono allineati se $t = kz + (1-k)w$ con $k \in \mathbb{R}$

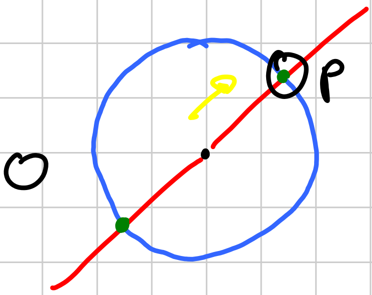
se e solo se $\frac{z-t}{w-t} \in \mathbb{R}$.

Vettori

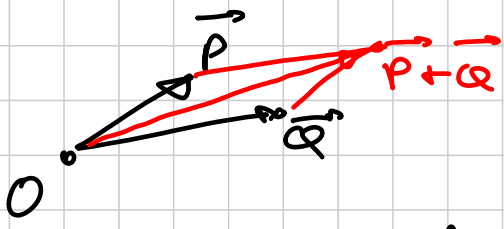
Fisso un'origine O. Ad ogni punto P corrisponde un vettore ($\overrightarrow{OP}$, $\vec{P}$), che è una freccia.

Vettore = direzione, intensità e verso

$\|\vec{P}\|$ = intensità = modulo = $\overline{OP}$



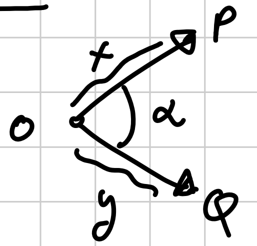
I vettori si sommano



I vettori si moltiplicano per un numero reale

$k \in \mathbb{R}$, $\vec{P}$ vettore $\quad k\vec{P}$ = stessa direzione
modulo pari a $|k| \cdot \|\vec{P}\|$
verso uguale a $\vec{P}$ se $k>0$
verso opposto se $k<0$

<u>Prodotto scalare</u>: $\vec{P}\cdot\vec{Q} = \|\vec{P}\|\cdot\|\vec{Q}\|\cdot\cos(P\hat{O}Q)$



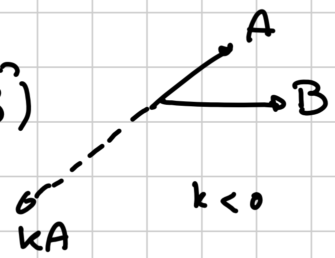
$xy\cos\alpha$

$OP \perp OQ \iff \vec{P}\cdot\vec{Q} = 0.$

<u>Proprietà</u>: 1) $(\vec{A}+\vec{B})\cdot\vec{C} = \vec{A}\cdot\vec{C} + \vec{B}\cdot\vec{C}$

2) $\vec{A}\cdot\vec{B} = \vec{B}\cdot\vec{A}$

3) $(k\vec{A})\cdot\vec{B} = k(\vec{A}\cdot\vec{B})$



4) $\vec{A}\cdot\vec{A} = \|\vec{A}\|^2$

$k<0$

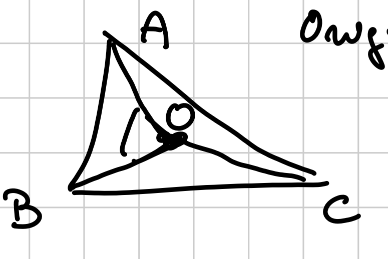
<u>Es</u>: $\|\vec{A}+\vec{B}\|^2 = (\vec{A}+\vec{B})\cdot(\vec{A}+\vec{B}) =$

$= (\vec{A}+\vec{B})\cdot\vec{A} + (\vec{A}+\vec{B})\cdot\vec{B} =$

$= \vec{A}\cdot\vec{A} + \vec{B}\cdot\vec{A} + \vec{A}\cdot\vec{B} + \vec{B}\cdot\vec{B} =$

$= \|\vec{A}\|^2 + 2\vec{A}\cdot\vec{B} + \|\vec{B}\|^2$

<u>Es</u>:



Origine nel circocentro

$\|\vec{A}\|^2 = R^2 = \|\vec{B}\|^2 = \|\vec{C}\|^2$

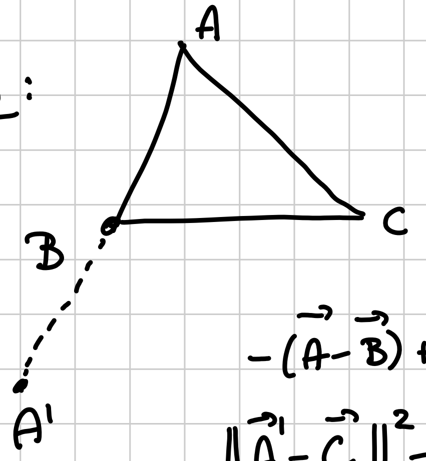
$\vec{A}\cdot\vec{B} = R^2\cos A\hat{O}B = R^2\cos 2\gamma$

$\|\vec{A}-\vec{B}\|^2 = c^2$

$$\begin{array}{ccccccc} \|\vec{A}-\vec{B}\|^2 & = & \|\vec{A}\|^2 & + & \|\vec{B}\|^2 & - & 2\vec{A}\cdot\vec{B} \\ \| & & \| & & \| & & \\ c^2 & = & R^2 & + & R^2 & - & 2\vec{A}\cdot\vec{B} \end{array}$$

$$\vec{A}\cdot\vec{B} = \frac{2R^2 - c^2}{2} = R^2 - \frac{c^2}{2}$$

Es:



$BA' = BA$

$A'C = ?$

Origine nel circocentro

$$-(\vec{A} - \vec{B}) + \vec{B} = 2\vec{B} - \vec{A} = \vec{A}'$$

$$\|\vec{A}' - \vec{C}\|^2 = \|\vec{A}'\|^2 + \|\vec{C}\|^2 - 2\vec{A}'\cdot\vec{C} =$$

$$= \|2\vec{B} - \vec{A}\|^2 + R^2 - 2(2\vec{B} - \vec{A})\cdot\vec{C} =$$

$$= \|2\vec{B}\|^2 + \|\vec{A}\|^2 - 2(2\vec{B})\cdot\vec{A} + R^2 -$$

$$- 4\vec{B}\cdot\vec{C} + 2\vec{A}\cdot\vec{C} =$$

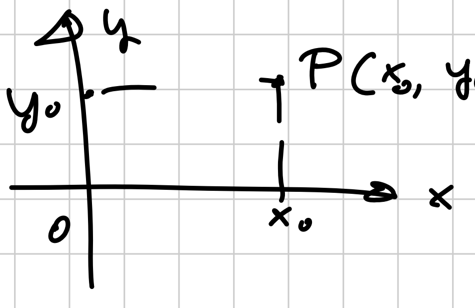
$$= 4R^2 + R^2 - 4\left(R^2 - \frac{c^2}{2}\right) + R^2 - 4\left(R^2 - \frac{a^2}{2}\right) +$$

$$+ 2\left(R^2 - \frac{b^2}{2}\right) =$$

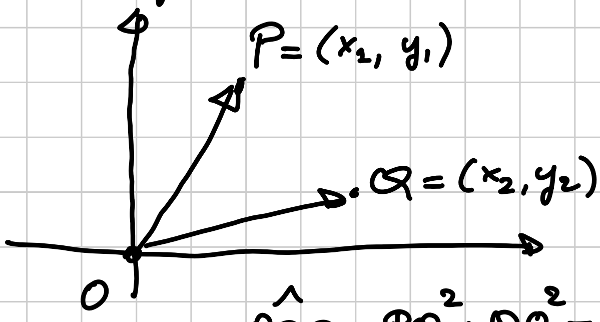
$$= 6R^2 - 4R^2 - 4R^2 + 2R^2 + 2c^2 + 2a^2 - b^2 =$$

$$= 2c^2 + 2a^2 - b^2.$$

Coordinate cartesiane



come si fa il prodotto scalare?



$$\vec{P}\cdot\vec{Q} = \|\vec{P}\|\cdot\|\vec{Q}\| \cos P\hat{O}Q = \sqrt{x_1^2+y_1^2}\cdot\sqrt{x_2^2+y_2^2}\cos P\hat{O}Q$$

$$\cos P\hat{O}Q = \frac{PO^2+QO^2-PQ^2}{2PO\cdot QO}$$ (Teo di Carnot)

$$\vec{P}\cdot\vec{Q} = \frac{PO^2+QO^2-PQ^2}{2} = \frac{1}{2}\Big[(x_1^2+y_1^2)+(x_2^2+y_2^2) -$$

$$-(x_1-x_2)^2-(y_1-y_2)^2\Big] =$$

$$= \frac{1}{2}\Big[\cancel{x_1^2}+\cancel{y_1^2}+\cancel{x_2^2}+\cancel{y_2^2}-\cancel{x_1^2}-\cancel{x_2^2}+2x_1x_2-\cancel{y_1^2}-\cancel{y_2^2}+2y_1y_2\Big] =$$

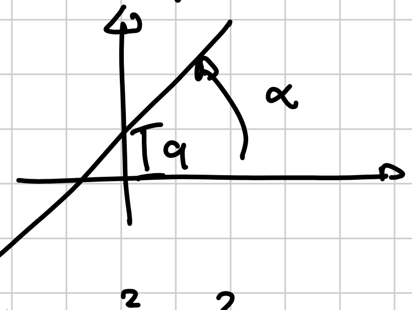
$$= \frac{1}{2}\big[2x_1x_2+2y_1y_2\big] = x_1x_2+y_1y_2$$

- eq. della retta $\quad y = mx+q.$ $\quad m = \operatorname{tg}\alpha$

$\qquad ax+by+c=0$ $\qquad q = \text{intercetta}$

rette $//$ $\Leftrightarrow$ stessa m

rette $\perp$ $\Leftrightarrow$ $m\cdot m' = -1$



- <u>circonferenza</u>: $(x-x_0)^2+(y-y_0)^2 = r^2$

$$x^2+y^2+2\alpha x+2\beta y+\gamma = 0$$

$$\alpha = -x_0 \qquad \beta = -y_0 \qquad \gamma = x_0^2+y_0^2-r^2$$

$$r^2 = x_0^2 + y_0^2 - \gamma = \alpha^2 + \beta^2 - \gamma > 0$$

$$\{x^2 + y^2 + 2x + 2y + 3 = 0\}$$

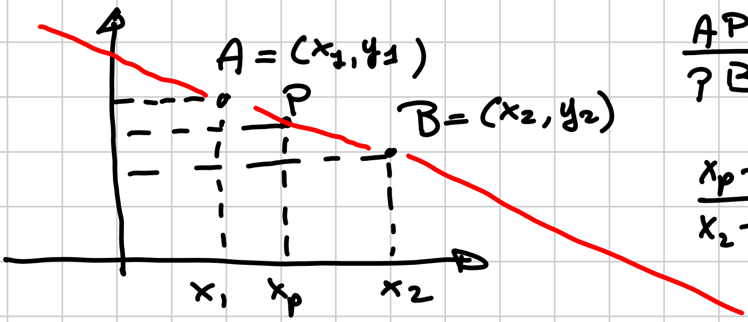
$1 + 1 - 3 = -1 < 0$ non è una cfr.

$$pow_\Gamma(P) = OP^2 - R^2 = (x - x_0)^2 + (y - y_0)^2 - r^2$$

Γ: centro O e raggio R

per ottenere la pot. di P basta sostituire le sue coord nell'eq della cfr.

— • —



$$\frac{AP}{PB} = k$$

$$\frac{x_p - x_1}{x_2 - x_p} = k$$

$$x_p(1+k) = x_1 + k x_2$$

$$x_p = \frac{x_1 + k x_2}{1+k}$$

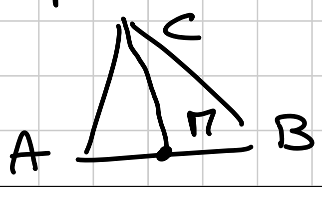
$$y_p = \frac{y_1 + k y_2}{1+k}$$

$$(x_p, y_p) = \frac{(x_1, y_1) + k(x_2, y_2)}{1+k} \Longleftarrow$$

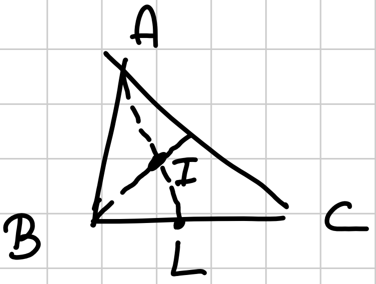
$$\vec{P} = \frac{\vec{A} + \boxed{k\vec{B}}}{1+k} \qquad \frac{AP}{PB} = k$$

$p = x_p + i y_p \quad a = x_1 + i y_1 \quad b = x_2 + i y_2 \quad p = \dfrac{a + kb}{1+k}$

A, B, C triangolo pt. medio di AB è $\dfrac{\vec{A} + \vec{B}}{2} = \vec{M}$



$$\frac{CG}{GM} = 2 \Rightarrow \vec{G} = \frac{\vec{C} + 2\vec{M}}{3} = \frac{\vec{A}+\vec{B}+\vec{C}}{3}$$



$$\frac{BL}{LC} = \frac{BA}{AC} = \frac{c}{b}$$

$$L = \frac{\vec{B} + \frac{c}{b}\vec{C}}{1 + \frac{c}{b}} = \frac{b\vec{B} + c\vec{C}}{b+c}$$

$$I = \frac{a\vec{A} + b\vec{B} + c\vec{C}}{a+b+c}$$

<u>Fatto vero</u>: Se l'origine è nel circocentro, allora $\vec{H} = \vec{A} + \vec{B} + \vec{C}$ è l'ortocentro.

———— o ————

Esercizi

$X = (1,1) \quad Y = (0,2)$

$\{P : XP = 2PY\}$

$X = (x_1, y_1) \quad Y = (x_2, y_2)$

$\{P : XP = \lambda YP\} \quad \lambda \neq 1, 0$

$P = (x,y)$

$$(x-x_1)^2 + (y-y_1)^2 = \lambda^2\left[(x-x_2)^2 + (y-y_2)^2\right]$$

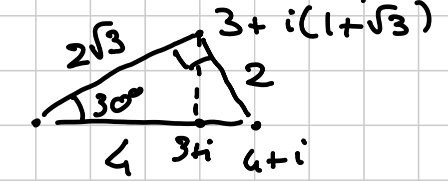
$$x^2 + x_1^2 + y^2 + y_1^2 - 2xx_1 - 2yy_1 = \lambda^2 x^2 + \lambda^2 x_2^2 + \lambda^2 y^2 + \lambda^2 y_2^2 - 2\lambda^2 yy_2 - 2\lambda^2 xx_2$$

$$x^2(1-\lambda^2)+y^2(1-\lambda^2)-2x(x_1-\lambda^2x_2)-2y(y_1-\lambda^2y_2)$$
$$+x_1^2+y_1^2-\lambda^2(x_2^2+y_2^2)=0$$ circonferenza di Apollonio

$$x_0=\frac{x_1-\lambda^2x_2}{1-\lambda^2}\qquad y_0=\frac{y_1-\lambda^2y_2}{1-\lambda^2}$$

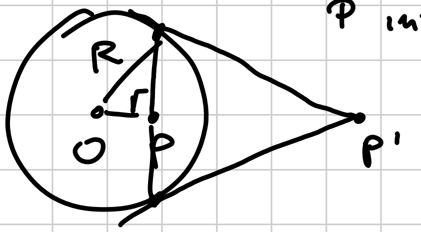
C t.c. X, Y, C sono all. e $\frac{XC}{CY}=-\lambda^2$

$\boxed{C}$ $\frac{a+b}{2}, \dots, \dots$



$$(2\sqrt3)^2+2^2=12+4=16=4^2$$

$$\frac{-a\vec{A}+b\vec{B}+c\vec{C}}{-a+b+c}, \dots, \dots$$



P' inverso di P se O, P, P' sono allin.
e $OP\cdot OP'=R^2$
e P, P' stanno sulla stessa semiretta da O.

$\vec{N}$ t.c. $\vec{N}=k\cdot\vec{m_a}$ $k>0$

$$Om_a\cdot ON=R^2\qquad ON=\|\vec{N}\|=\frac{R^2}{\|\vec{m_a}\|}$$

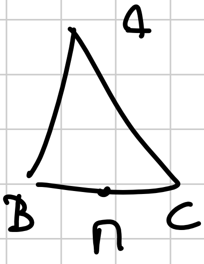
$$m_a=\frac{\vec{B}+\vec{C}}{2}\qquad \|m_a\|^2=\frac{1}{4}(R^2+R^2+2R^2-a^2)=R^2-\frac{a^2}{4}$$

$$\frac{ON}{Om_a}=\frac{R^2}{\|m_a\|^2}=\frac{R^2}{R^2-\frac{a^2}{4}}=1+\frac{a^2}{4R^2-a^2}$$

$$\vec{M} = \left(1 + \frac{a^2}{4R^2-a^2}\right)\frac{\vec{B}+\vec{C}}{2}$$

---

6) $\sum$ mediane^2



$$\vec{M} = \frac{\vec{B}+\vec{C}}{2}$$

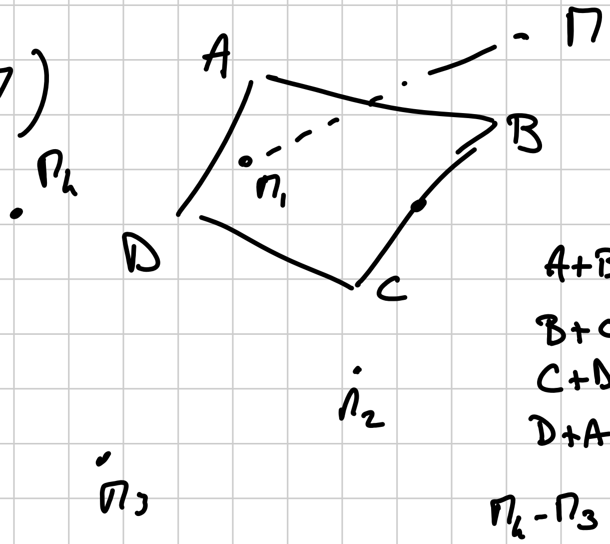
$$AM^2 = \left\|\vec{A} - \frac{\vec{B}+\vec{C}}{2}\right\|^2 =$$

$$a^2 = \|\vec{B}-\vec{C}\|^2 = \|\vec{B}\|^2 + \|\vec{C}\|^2 - 2\vec{B}\cdot\vec{C}$$

$$= \left\|\frac{\vec{A}-\vec{B}}{2} + \frac{\vec{A}-\vec{C}}{2}\right\|^2 = \frac{1}{4}(c^2+b^2) + \frac{1}{2}(\vec{A}-\vec{B})\cdot(\vec{A}-\vec{C})$$

$$\frac{3}{4}(a^2+b^2+c^2)$$

7)

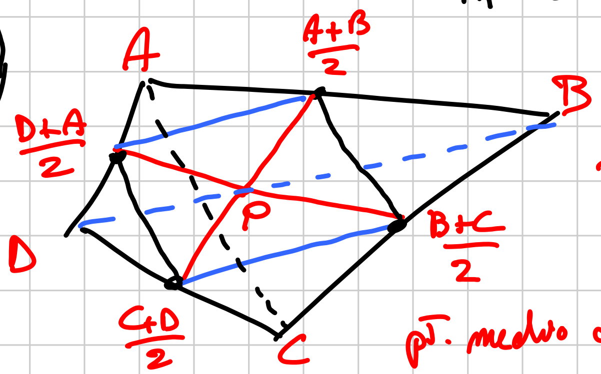


$$\frac{A+B}{2}$$

$$A+B-M = M_1$$
$$B+C-M = M_2$$
$$C+D-M = M_3$$
$$D+A-M = M_4$$

$$M_4 - M_3 = D+A-M-C-D+M = A-C$$
$$M_1 - M_2 = A+B-M-B-C+M = A-C$$

8)



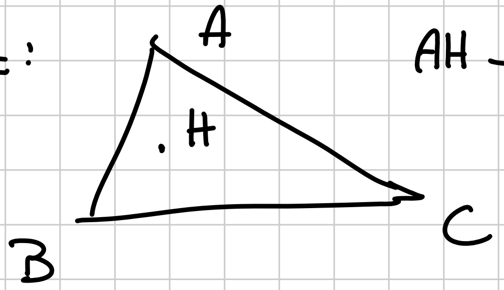
$$P = \frac{\frac{A+B}{2} + \frac{C+D}{2}}{2} = \frac{A+B+C+D}{4}$$

pt. medio di $BD = \frac{B+D}{2}$

pt medio di $AC = \frac{A+C}{2}$

$\Rightarrow$ pt medio tra i pt. medi $= \dfrac{A+B+C+D}{4}$

Vediamo cosa:



$AH \perp BC \quad (*)$

Se l'origine è in O, $\vec{H} = \vec{A}+\vec{B}+\vec{C}$ soddisfa $(*)$

$$(\vec{H}-\vec{A})\cdot(\vec{B}-\vec{C}) = (\vec{B}+\vec{C})\cdot(\vec{B}-\vec{C}) =$$

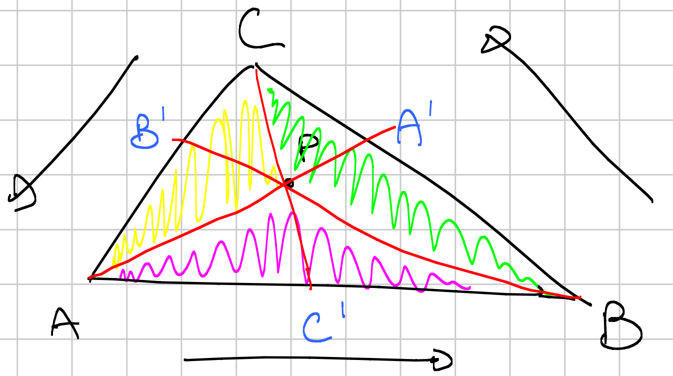
$$= \|\vec{B}\|^2 - \|\vec{C}\|^2 = R^2 - R^2 = 0$$

$\Rightarrow$ Se l'origine è nel circocentro, $\vec{H} = \vec{A}+\vec{B}+\vec{C}$ sta sulle altezze $\Rightarrow$ è l'ortocentro.

G 3 - Basic - Geom. Sintetica (Pdfkk)

Titolo nota 05/09/2013

CEVA MENELAO



Th (CEVA) $\dfrac{AC'}{C'B} \cdot \dfrac{BA'}{A'C} \cdot \dfrac{CB'}{B'A} = 1$

Dim: Idea: considera aree! $\dfrac{AC'}{C'B} = \dfrac{[ACC']}{[BCC']} = \dfrac{[APC']}{[BPC']} =$ ⊛

$= \dfrac{[ACC'] - [APC']}{[BCC'] - [BPC']} = \dfrac{[APC]}{[BPC]}$ (I) ⊛

Ora, stessa costruzione sugli altri lati!

⊛ $\begin{array}{l|l} A \to B & A' \to B' \\ B \to C & B' \to C' \\ C \to A & C' \to A' \end{array}$ $\to \dfrac{BA'}{A'C} = \dfrac{[BPA]}{[CPA]}$ (II)

$\to \dfrac{CB'}{B'A} = \dfrac{[CPB]}{[APB]}$, (III)

Tesi: (I) $\cdot$ (II) $\cdot$ (III) $= 1$

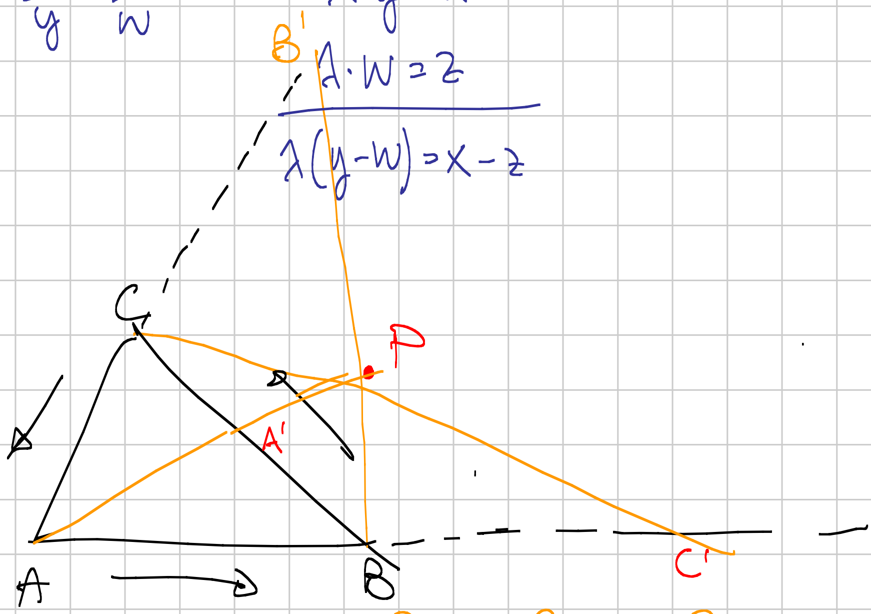
perché le 3 aree si semplificano

(*) $\dfrac{x}{y} = \dfrac{z}{w} = \dfrac{x-z}{y-w}$

$\uparrow$ Hp $\quad\uparrow$ Th

Dim: $\lambda = \dfrac{x}{y} = \dfrac{z}{w}$

$$\lambda \cdot y = x$$
$$\lambda \cdot w = z$$
$$\lambda(y-w) = x - z$$



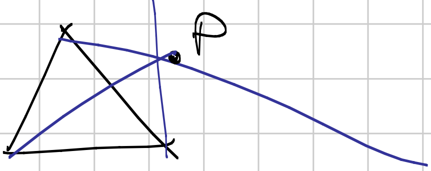
lunghezze con segno!

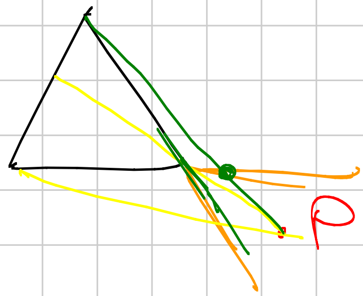
$$\underset{\ominus}{\overset{\oplus}{\frac{AC'}{C'B}}} \cdot \underset{\oplus}{\overset{\oplus}{\frac{BA'}{A'C}}} \cdot \underset{\oplus}{\overset{\ominus}{\frac{CB'}{B'A}}} = 1$$

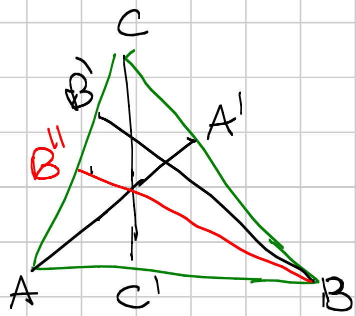
Th: questo rapporto fa $+1$ anche se il punto P è esterno al triangolo (a patto di usare lunghezze orientate)

dim: i) se rifacciamo la dim. sopra, rifunziona a patto di cambiare "−" in "+"

ii)







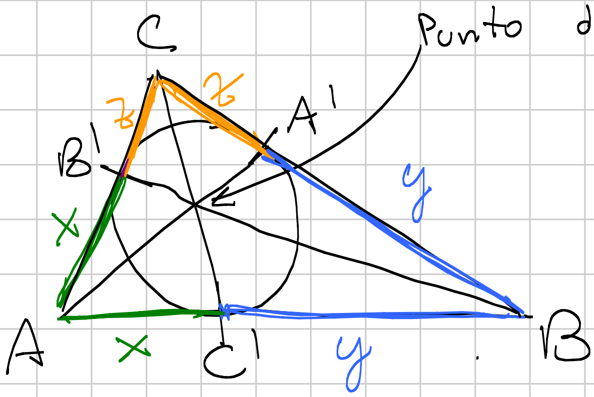
$$\frac{AC'}{C'B}\cdot\frac{BA'}{A'C}\cdot\frac{CB'}{B'A}=1$$

$\neq$

$$\frac{AC'}{C'B}\cdot\frac{BA'}{A'C}\cdot\frac{CB''}{B''A}=1$$

ASSURDO

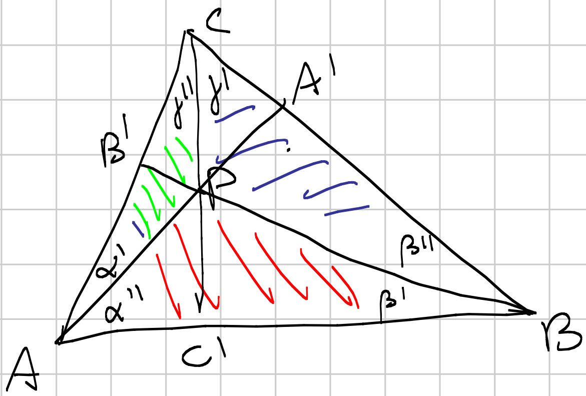
Punto di Gergonne



$$\frac{\cancel{x}}{\cancel{y}}\cdot\frac{\cancel{y}}{\cancel{z}}\cdot\frac{\cancel{z}}{\cancel{x}}=1$$

Compito per casa: trovare x, y, z in funzione delle lunghezze dei lati

Compito per casa (dopo lungo allenamento di base): Coniugato isotomico



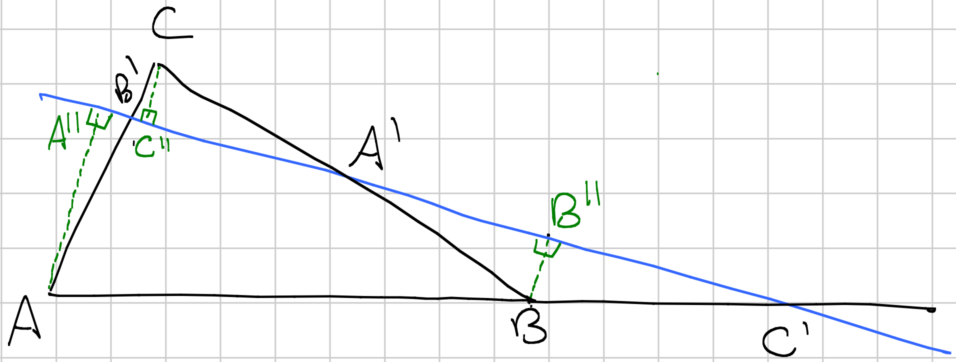
AA', BB', CC' concorrono se e solo se

$$\frac{\sin\alpha'}{\sin\alpha''}\cdot\frac{\sin\beta'}{\sin\beta''}\cdot\frac{\sin\gamma'}{\sin\gamma''}=1$$

$$1=\frac{\text{Area } APB}{\text{Area } BPC}\cdot\frac{\text{Area } BPC}{\text{Area } CPA}\cdot\frac{\text{Area } CPA}{\text{Area } APB}=$$

$$=\frac{\cancel{AB}\cdot\cancel{PB}\cdot\sin\beta'}{\cancel{CB}\cdot\cancel{PB}\cdot\sin\beta''}\cdot\frac{\cancel{BC}\cdot\cancel{PC}\cdot\sin\gamma'}{\cancel{AC}\cdot\cancel{PC}\cdot\sin\gamma''}\cdot\frac{\cancel{CA}\cdot\cancel{PA}\cdot\sin\alpha'}{\cancel{BA}\cdot\cancel{PA}\cdot\sin\alpha''}$$

Coniugato isogonale



A', B', C' allineati se e solo se

$$\frac{AC'}{C'B}\cdot\frac{BA'}{A'C}\cdot\frac{CB'}{B'A}=-1$$

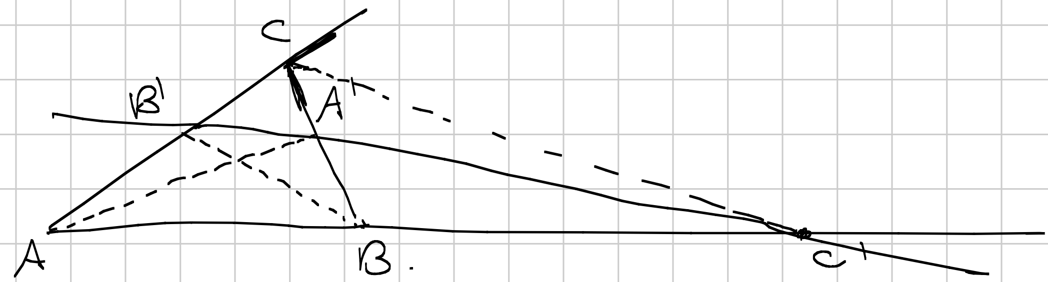
$AA'' \parallel BB'' \parallel CC''$. (Talete)

$$\frac{AC'}{C'B}=\frac{AA''}{B''B}\qquad\frac{BA'}{A'C}=\frac{BB''}{C''C}$$

$$\frac{CB'}{B'A} = \frac{CC''}{A''A}$$

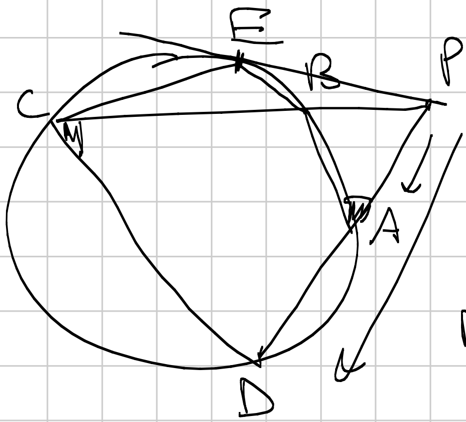
$$\frac{\cancel{AA''}}{\cancel{B''B}} \cdot \frac{\cancel{BB''}}{\cancel{C''C}} \cdot \frac{\cancel{CC''}}{\cancel{A''A}} = -1$$

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



A', B', C' sono allineati.

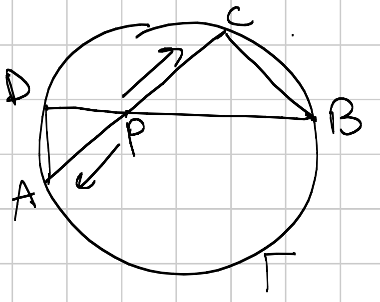
$$\underbrace{\frac{AC'}{C'B}}_{\cancel{\frac{AC}{CB}}} \cdot \underbrace{\frac{BA'}{A'C}}_{\cancel{\frac{BA}{AC}}} \cdot \underbrace{\frac{CB'}{B'A}}_{\cancel{\frac{CB}{BA}}} = -1$$



$PAB \sim PCD$

$$\frac{PA}{PC} = \frac{PB}{PD}$$

$$PA \cdot PD = PB \cdot PC = PE^2$$

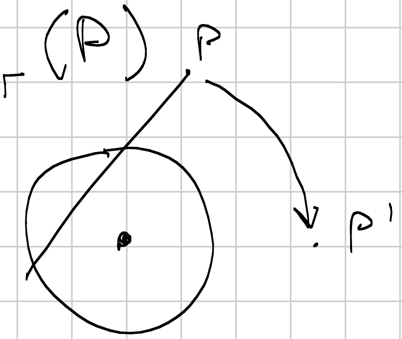


$PAD \sim PBC$

$$\frac{PA}{PB} = \frac{PC}{PD}$$

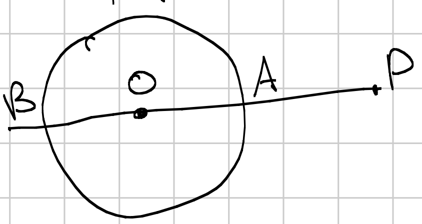
$$PA \cdot PC = PB \cdot PD$$

$Pow_\Gamma(P)$



$Pow_\Gamma(P)$ dipende solo dalla distanza di P dal centro

$Pow_\Gamma(\text{punto su } \Gamma) = 0$



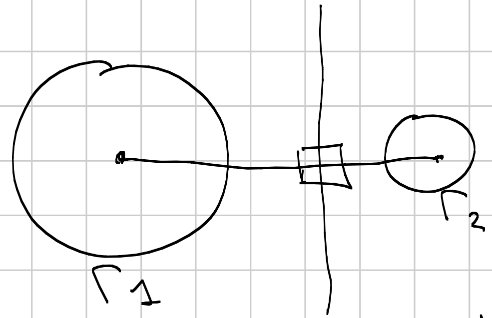
$$PA \cdot PB = (PO - \underset{R}{AO})(PO + \underset{R}{OB}) =$$
$$= PO^2 - R^2$$

P sta sulla circonferenza Γ di centro O e raggio R se e solo se

$$\underbrace{(x_P - x_O)^2 + (y_P - y_O)^2}_{OP^2} - R^2 = 0$$

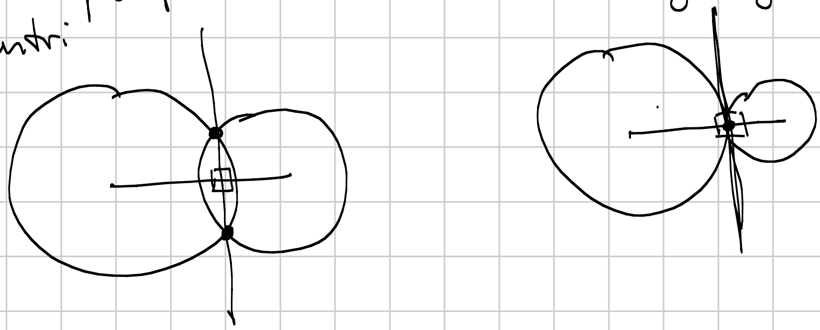
$$\underbrace{(x_P - x_O)^2 + (y_P - y_O)^2}_{OP^2} - R^2 = Pow_\Gamma(P)$$

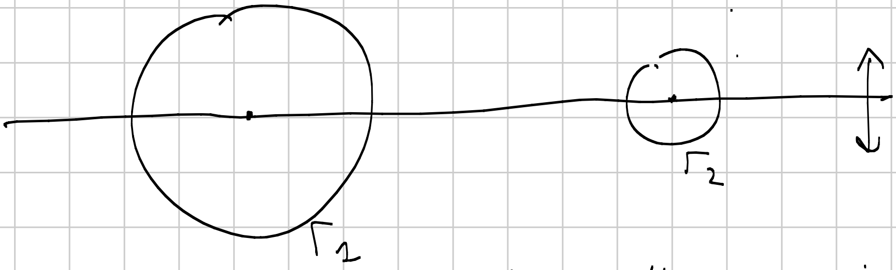
$x_P^2 + \ldots \quad y_P^2 + \ldots$



luogo dei punti P
per cui
$$\mathrm{Pow}_{\Gamma_1}(P) = \mathrm{Pow}_{\Gamma_2}(P)$$
?

asse radicale di Γ_1 e Γ_2
è perpendicolare alla congiungente i centri



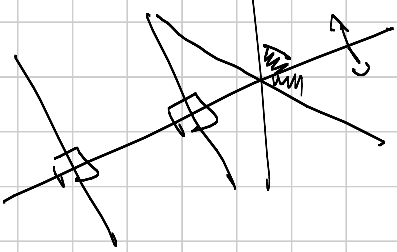


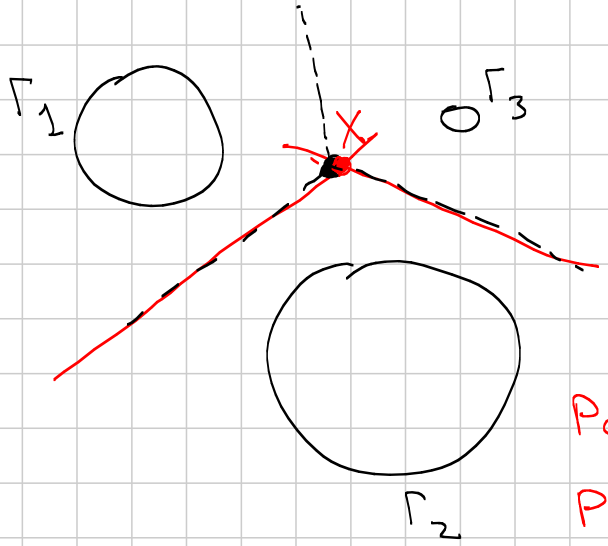
simmetria rispetto alla congiungente i centri

Γ_1 va in Γ_1, Γ_2 in Γ_2

Allora le potenze dei punti si conservano

Quindi asse radicale va nell'asse radicale
che quindi è ortogonale
alla congiungente i
centri





Asse radicale di Γ_1, Γ_2

Quello di $\Gamma_2 \Gamma_3$

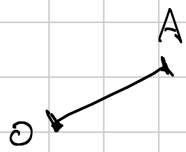
Quello di $\Gamma_3 \Gamma_1$

concorrono

$$\mathrm{Pow}_{\Gamma_1}(X) = \mathrm{Pow}_{\Gamma_2}(X)$$
$$\mathrm{Pow}_{\Gamma_2}(X) = \mathrm{Pow}_{\Gamma_3}(X)$$

Omotetie

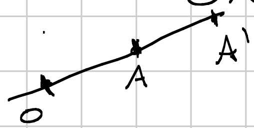
di centro O e ragione $\lambda \neq 0$



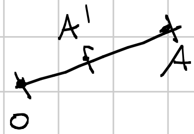
A va in A' tale che

- O, A, A' sono allineati
- $\dfrac{OA'}{OA} = \lambda$

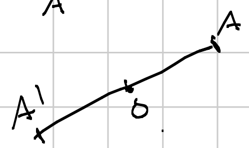
$\lambda = 2$



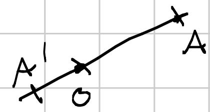
$\lambda = \frac{1}{2}$



$\lambda = -1$



$\lambda = -\frac{1}{3}$

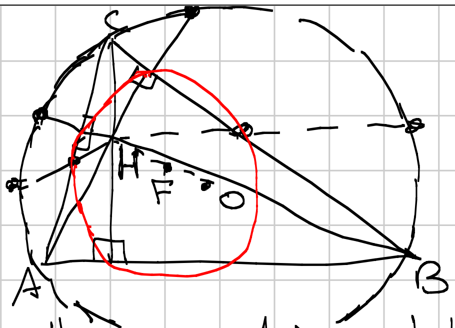


Le distanze vengono moltiplicate per $|\lambda|$

$$d(A', B') = |\lambda|\, d(A, B)$$

Rette vanno in rette parallele alle originali

Circonferenza di centro C e raggio r va in una circonferenza con centro l'immagine di C e raggio $|\lambda| r$



H ortocentro

Omotetia di centro H e ragione $\frac{1}{2}$

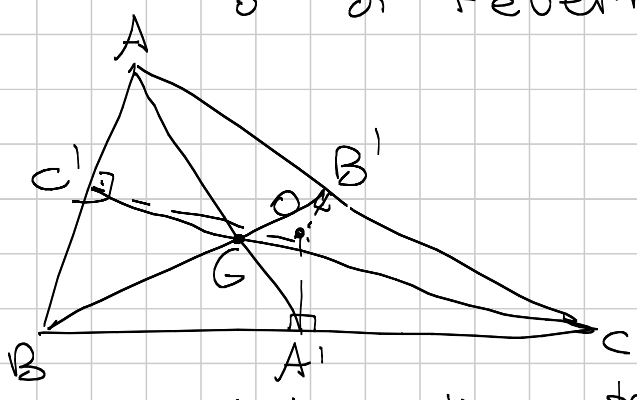
(1) Il simmetrico dell'ortocentro rispetto ad un lato sta sulla circonferenza circoscritta

(2) Il simmetrico dell'ortocentro rispetto al punto medio di un lato sta sulla cfr circoscritta

Con questa omotetia la circoscritta va in una circonferenza di centro F tale che H, F, O allineati e HF = FO raggio metà del raggio della circoscritta

Passa per:
- punti medi di HA, HB, HC
- piedi delle altezze
- punti medi dei lati

Circonferenza dei 9 punti o di Feuerbach



$BG = 2GB'$
$AG = 2GA'$
$CG = 2GC'$

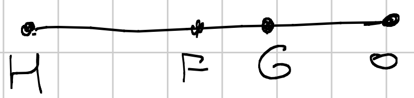
Omotetia di centro G e ragione $-\frac{1}{2}$

A va in A'
B in B'
C in C'

La circoscritta va nella circonferenza per A', B', C', che è sempre la cfr di Feuerbach

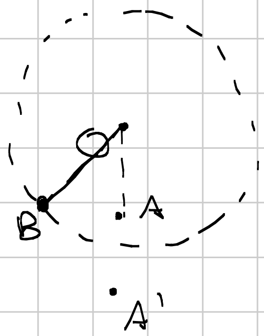
O, G, F sono allineati in quest'ordine e $OG = 2GF$

La retta per H, F, G, O è detta retta di Eulero



$HG = 2GO$
$HF = FO$
$OG = 2GF$

Circonferenza di centro O e raggio r



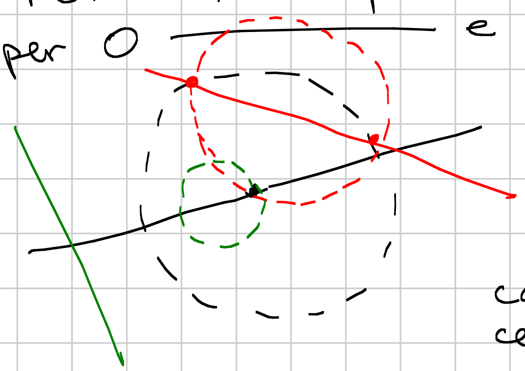
A va in A' tale che $\neq O$

- A, A', O sono allineati
- A, A' sono dalla stessa parte rispetto ad O
- $OA \cdot OA' = r^2$

Inversione di centro O e raggio r

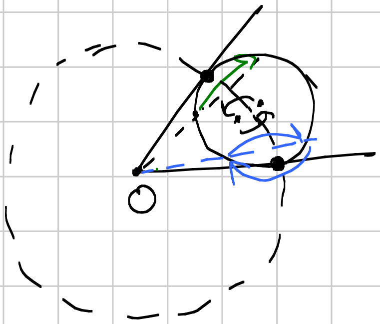
rette per O vanno in rette per O

rette NON per O vanno in circonferenze per O e viceversa

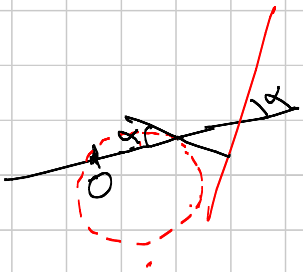


Circonferenze non per O vanno in circonferenze non per O

Achtung! In questo caso, il centro non va nel centro



Si conservano gli angoli tra le tangenti



Teorema di Tolomeo

ABCD quadrilatero, allora

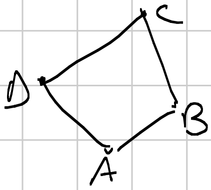
$AB \cdot CD + BC \cdot AD \geq AC \cdot BD$ e vale $=$ se e solo se ABCD ciclico

Facciamo un inversione di centro D e raggio R

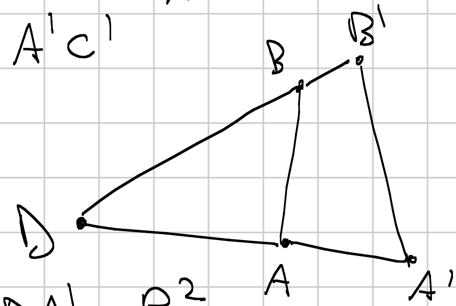
A va in A'

B va in B'

C va in C'



$A'B' + B'C' \geq A'C'$



$DB \cdot DB' = DA \cdot DA' = R^2$

$\dfrac{DB}{DA} = \dfrac{DA'}{DB'}$ allora $\quad DAB \sim DB'A'$

$$\frac{A'B'}{AB} = \frac{DB'}{DA} = \frac{DB' \cdot DB}{DA \cdot DB} = \frac{R^2}{DA \cdot DB}$$

$$A'B' = AB \cdot \frac{R^2}{DA \cdot DB}$$

$$A'B' + B'C' \geq A'C'$$

$$DC \cdot AB \cdot \frac{\cancel{R^2}}{\cancel{DC} \cancel{DA} \cdot \cancel{DB}} + DA \cdot BC \cdot \frac{\cancel{R^2}}{DA \cdot \cancel{DB} \cancel{DC}} \geq DB\,AC \cdot \frac{\cancel{R^2}}{\cancel{DB}\,\cancel{DA} \cdot \cancel{DC}}$$

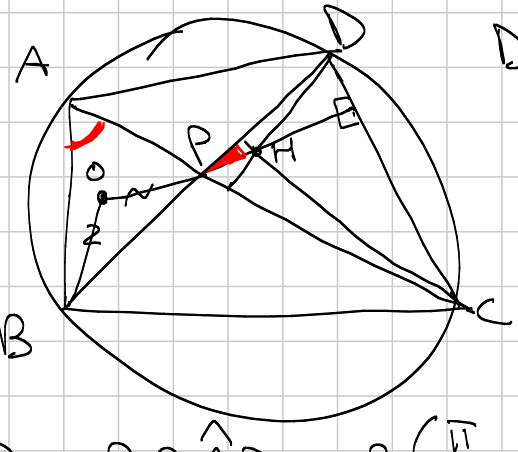
$$DC \cdot AB + DA \cdot BC \geq BD \cdot AC$$

se A', B', C' allineati A, B, C e D stanno sulla stessa circonferenza

Parte 1
12, 14, 15, 16, 18, 19 (e altri, se volete)

Parte 2
Esercizi 1, 3, 6, 8, 9 (e altri, se volete)

1

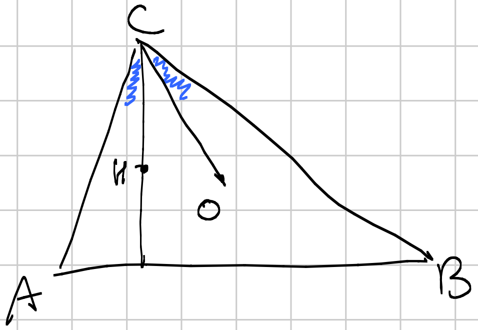


$$DPH \stackrel{?}{=} OPB$$

$$\frac{\pi}{2} - P\hat{D}C = \frac{\pi}{2} - B\hat{A}C$$

$$B\hat{O}P = 2B\hat{A}P = 2\left(\frac{\pi}{2} - H\hat{P}D\right) =$$

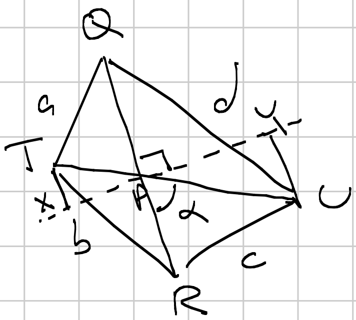
$$= \pi - 2H\hat{P}D \qquad \text{Allora } O\hat{P}B = H\hat{P}D$$



Fatto utile:

$$H\hat{C}A = O\hat{C}B$$

3



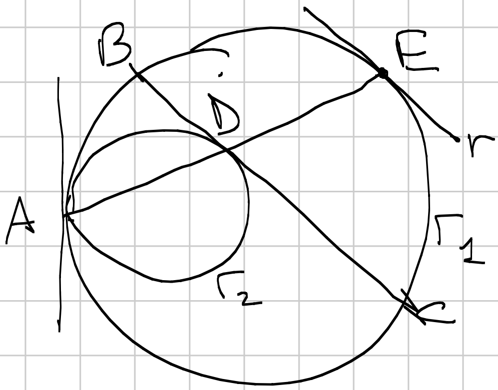
$ac + bd \geq$ prodotto lunghezze diagonali $\overset{?}{\geq} 2S$

$$2S = QR \cdot XY \leq QR \cdot TU =$$

$= ?$
- $=$ in Tolomeo (ciclico)
- Diagonali ortogonali

$$2S = QR \cdot TU \cdot \sin\alpha$$

6



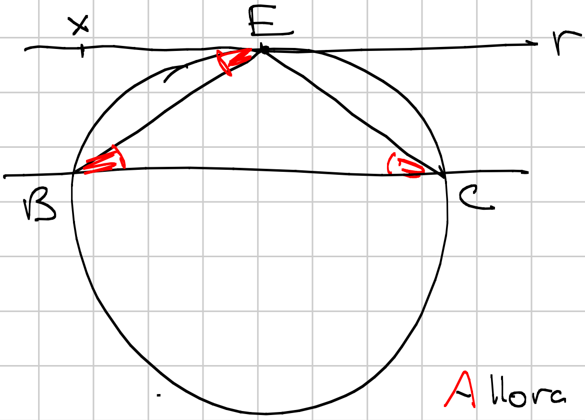
$$\overset{\frown}{BE} \overset{?}{=} \overset{\frown}{EC}$$

$r \parallel BC$?

Omotetia di centro A e ragione $\frac{AE}{AD}$

$A \to A$ $D \to E$ $\Gamma_2 \to \Gamma_1$ $BC \to$ Tangente a Γ_1 in E, cioè r

Allora $BC \parallel r$



$x\hat{E}B = E\hat{B}C$

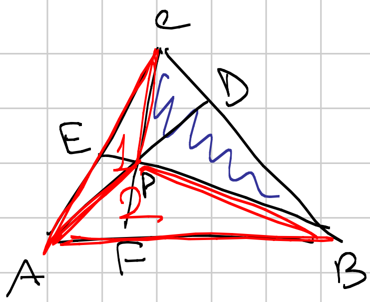
(parallelismo)

$x\hat{E}B = E\hat{C}B$

(insistono su EB)

Allora $EB = EC$

e $\overset{\frown}{EB} = \overset{\frown}{EC}$

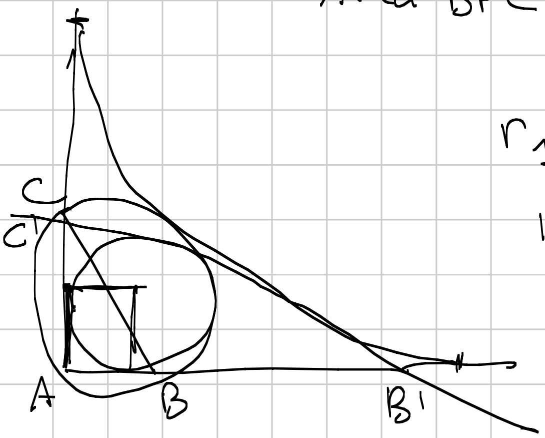


$$\frac{AF}{FB} = \frac{\text{Area } APC}{\text{Area } CPB}$$

$$\frac{AE}{EC} = \frac{\text{Area } APB}{\text{Area } CPB}$$

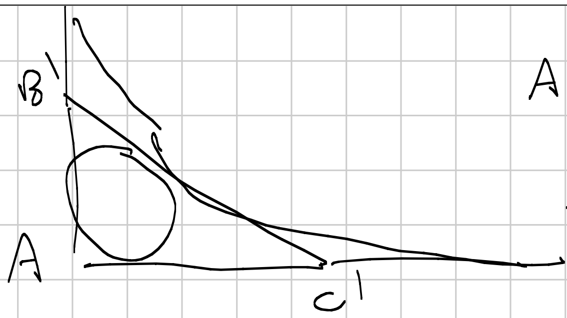
$$\frac{AF}{FB} + \frac{AE}{EC} = \frac{\text{Area } ABPC}{\text{Area } BPC} = \frac{AP}{PD}$$

9



$r_1 \quad r_2$

Inversione di centro A e raggio $\sqrt{r_1 r_2}$



$$AB' = \frac{r_1 r_2}{AB}$$

$$AC' = \frac{r_1 r_2}{AC}$$

Sapendo Area ABC sapete Area $AB'C'$

Dovete dimostrare che

Area $AB'C' = r_1 r_2$

Teoria dei Numeri 1

Titolo nota 02/09/2013

Naturali $= \mathbb{N} = \{0, 1, 2, \dots\}$

Interi $\mathbb{Z}$ $\{\dots, -2, -1, 0, 1, 2, \dots\}$

Un intero a divide un intero b

(e si scrive $a \mid b$)

se esiste un intero k t.c. $b = ka$

Oss: $a \mid b \Rightarrow |a| \leq |b|$

$|b| = |k| \cdot |a| \geq |a|$

Fatto essenziale: $a \mid b$ $a \mid c$

$a \mid b \cdot c$ $a \mid b + c$

$a \mid k \cdot b$

Quindi $a \mid hb + kc$

Numero primo p è divisibile solo per $\pm 1, \pm p$ e non è ± 1

p è primo se e solo se $p \mid a \cdot b$ $\Rightarrow$ $p \mid a$ oppure $p \mid b$

Supponiamo $a \mid p$, cioè $p = a \cdot b$
In particolare $p \mid a \cdot b$; WLOG (= senza perdita di generalità) $p \mid a$
$|a| \leq |p| \leq |a|$ $\Rightarrow$ $a = \pm p$

Teorema fondamentale dell'Aritmetica

Ogni intero ≥ 2 si scrive in maniera unica come prodotto di primi (con ripetizioni)

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$$

$$m = q_1^{b_1} \cdot \ldots \cdot q_h^{b_h}$$

Quand'è che $m \mid n$?

1) Tutti i q_i devono dividere anche n

A meno dell'ordine, $p_1 = q_1, \ldots, p_h = q_h$

2) $b_1 \le a_1, \ldots, b_h \le a_h$ $\boxed{h \le k}$

Massimo comun divisore

Dati a, b interi, il massimo comun divisore – che si scrive (a,b) – e' il piu' grande intero che divida entrambi

Algoritmo di Euclide

$$d = (a,b)$$

$$c \mid a \text{ e } c \mid b \iff c \mid a \text{ e } c \mid a-b$$

$$(144, 27) = (144-27, 27) = (144-27\cdot 2, 27)$$
$$= \ldots = (9, 27) = (27-3\cdot 9, 9)$$
$$= (0, 9) = 9$$

Es. $(a^2+a+1, a+1) = 1$?

Coprimi a, b sono coprimi se $(a,b) = 1$

$$(a^2+a+1, a+1) = (a^2+a+1-a(a+1), a+1)$$
$$= (1, a+1) = 1$$

Identità di Bézout

Esiste sempre una scrittura di (a,b) come combinazione (a coeff. interi) di a e b

$$9 = 144h + 27k$$
$$h=1, \quad k=-5$$

$(44, 17) = 1$

$$44 = 17 \cdot 2 + 10 \qquad (17, 10)$$
$$17 = 10 \cdot 1 + 7 \qquad (10, 7)$$
$$10 = 7 \cdot 1 + 3 \qquad (7, 3)$$
$$7 = 3 \cdot 2 + 1 \qquad (3, 1) = 1$$

$$1 = 7 - 3 \cdot 2 = 7 - 2 \cdot (10 - 7) =$$
$$= -2 \cdot 10 + 3 \cdot 7 = -2 \cdot 10 + 3 \cdot (17 - 10)$$
$$= 3 \cdot 17 - 5 \cdot 10 = 3 \cdot 17 - 5 \cdot (44 - 2 \cdot 17) =$$
$$= -5 \cdot 44 + 13 \cdot 17$$

Diofantee lineari in due variabili

$$44x + 17y = 5$$

$$44x - 72y = 5$$ ha grossi problemi ad avere soluzioni.

$$44x + 17y = 1$$

$$44 \cdot (5x) + 17(5y) = 5$$

In generale $ax + by = c$, dove a, b, c sono interi fissati ed x, y le incognite hanno soluzioni se e solo se $(a,b) \mid c$

Ex Quali sono TUTTE le soluzioni?

Diofantee

$$3x^2 = 141 y^5 + 5$$

$$3x^2 - 141 y^5 = 5$$

$$\| $$

$$3(x^2 - 47 y^5)$$

No! Perché $3 \nmid 5$ (3 non divide 5)

Fattorizzazioni algebriche forniscono fattorizzazioni aritmetiche

$$x^2 - y^2 = 7$$

$$(x-y)(x+y) = 7 \longrightarrow x+y \mid 7$$

Wlog $x \geq 0$, $y \geq 0$

$$x+y = \begin{cases} 1 & \Rightarrow x-y = 7 \\ 7 & \Rightarrow x-y = 1 \end{cases}$$

Soluzione $x = \pm 4$, $y = \pm 3$

$5p + 49 = n^2$, n intero e p primo

$$5p = (n+7)(n-7)$$

$\pm 1, \pm 5, \pm p, \pm 5p$

$n+7 = p$, $n-7 = 5$

$n+7 = 5p$, $n-7 = 1$

Ex $m^3 - n^3 = 7004 = 2^2 \cdot 17 \cdot 103$

Risolvere $p^x = x^y$

1) x è una potenza di p

$$x = p^a$$

2) $p^{p^a} = p^{ay} \Rightarrow p^a = a \cdot y$

3) $a \mid p^a \Rightarrow a = p^b$

$$p^{p^b} = p^b \cdot y \Rightarrow y = p^{p^b - b}$$

Ex $p^b - b \geq 0$ per ogni p primo, $b \geq 0$

Congruenze

Che giorno sarà fra 400 giorni?

$$400 = 57 \cdot 7 + 1$$

$$400 \rightsquigarrow 50 \rightsquigarrow 1$$

Def Diciamo che a e b sono congrui modulo n se lasciano lo stesso resto nella divisione per n

Si denota $a \equiv b \pmod{n}$

$a \equiv b \quad (n)$

ed è equivalente a dire che $n \mid (a-b)$

$$400 \equiv 50 \equiv 1 \pmod 7$$

1) $a \equiv b \pmod n \Rightarrow a + k \equiv b + k \ (n)$

2) $a \equiv b \ (n) \Rightarrow ha \equiv hb \ (n)$

3) $a \equiv b \ (n) \quad c \equiv d \ (n) \Longrightarrow ac \equiv bd \ (n)$

$$400 \equiv 1 \ (7) \Rightarrow 400 \cdot 400 \equiv 1 \cdot 1 \equiv 1 \ (7)$$

Cosa vogliamo? $n \mid ac - bd =$

$= c(a-b) - bd + bc =$

$$= \underbrace{c(a-b)}_{\text{multiplo di } n} + b\underbrace{(c-d)}_{\text{multiplo di } n}$$

Rappresentanti privilegiati $= \{0, 1, 2, \dots, n-1\}$

Un'altra scelta possibile e'

$$\{ \quad -3, -2, -1, 0, 1, 2, 3 \}$$

Resto della divisione di 398^2 per 400?

$$398 \equiv -2 \pmod{400}$$

$$398^2 \equiv (-2)^2 \equiv 4$$

ACHTUNG: COSA NON FUNZIONA?

$$6 \equiv 2 \pmod 4 \qquad 4 \mid 6-2$$

$$\cancel{\Downarrow}$$

$$3 \equiv 1 \pmod 4 \qquad 4 \mid \frac{6-2}{2}$$

$$3 \equiv 1 \pmod 2 \qquad \frac{4}{2} \mid \frac{6-2}{2}$$

$$4 \cdot 7 \equiv 88 \pmod{15}$$

$$\Downarrow$$

$$7 \equiv 22 \pmod{15}$$

Potenze

Funziona: $a \equiv b \ (n) \Rightarrow a^k \equiv b^k \ (n)$

NON funziona: $h \equiv k \pmod{n}$

$$\Rightarrow \quad 2^h \equiv 2^k \pmod{n}$$

FALSISSIMO

$1 \equiv 6 \pmod{5} \overset{?}{\Rightarrow} 2^1 \equiv 2^6 \ (5)$

$$2 \not\equiv 64 \ (5)$$

Applicazione alle Diofantee

$$3x^2 = 141y^2 + 2$$

Uguaglianza $\Longrightarrow$ congruenza

Idea: far sparire variabili

$$0 \equiv 3x^2 \equiv 141y^2 + 2 \pmod 3$$
$$\equiv 0 \cdot y^2 + 2 \quad (3)$$

$$2^x - 5y^2 = 64$$

Modulo 2: $-5y^2 \equiv 0 \pmod 2$

$y^2 \equiv 0 \pmod 2$

y è pari

Modulo 5: $2^x \equiv 4 \pmod 5$

$x = 0 \qquad 2^x = 1 \equiv 1 \quad (5)$

$1 \qquad 2^1 \equiv 2$

$\boxed{2 \qquad 2^2 \equiv 4}$ + periodicità di periodo 4

$3 \qquad 2^3 \equiv 3$

$4 \qquad 2^4 \equiv 1$

$5 \qquad 2^5 \equiv 2^4 \cdot 2 \equiv 2 \quad (5)$

Quindi $x = 2 + 4k$, quindi x è pari

$$x^2 + y^2 = z^4 + 6$$

Quadrati sono belli modulo 8

$0^2 \quad 1^2 \quad 2^2 \equiv 4 \quad 3^2 \equiv 1 \pmod 8$

$4^2 \equiv 0 \ (8) \quad 5^2 \equiv 1 \pmod 8 \quad 6^2 \equiv 4 \ (8)$

$7^2 \equiv (-1)^2 \equiv 1 \ (8)$

$a \equiv 0, 1, 2, 3, \dots, 7 \pmod 8$

$a^2 \equiv 0^2, 1^2, \dots, 7^2 \quad (8)$

$x^2 + y^2 = z^4 + 6$

Cosa può fare $x^2+y^2 \bmod 8$?

$0, 1, 4, 5, 2$

z dispari

Cosa fa z^4 ? $\quad z^4 \equiv (z^2)^2 \equiv \begin{cases} 1^2 & (8) \\ 0 & (8) \end{cases}$

z pari

Cosa fa z^4+6 ? $\quad 6$ o 7

Caso fortunato

Lavorando modulo n, ho trovato una cosa della forma

$$a \cdot (\underset{\text{incognite}}{\text{roba contenente}}) \equiv b \ (n)$$

Quindi voglio sapere se si può risolvere

$$ax \equiv b \pmod n$$

$\iff n \mid (ax - b) \iff$ esiste un intero y tale che $ax - b = y \cdot n$

$\iff$ la diofantea $(\star)$ $ax + ny = b$ si risolve $\iff (a, n) \mid b$

a meno di cambiare il segno di y

E come trovo la soluzione?

La soluzione di $(\star)$ è esattamente la soluzione della congruenza:

se guardo $ax + ny = b$ modulo n

trovo $ax \equiv b \pmod n$

Ex L'equazione $8x \equiv 7 \pmod{15}$ quante soluzioni ha?

Troviamo almeno una soluzione

$$8x \equiv 6 \ (15)$$

$\iff 15 \mid 8x-6 \iff 8x-6 = -15y$

$\iff 8x + 15y = 6$

$(8,15) \mid 6$ OK

$15 = 8 + 7$

$8 = 7 + 1$

$1 = 8 - 7 = 2 \cdot 8 - 15$

$\times 6$

$12 \cdot 8 - 6 \cdot 15 = 6$

$12 \cdot 8 \equiv 6 \pmod{15}$

$M = n^4 + n^3 + n^2 + n + 1$

$n \in \mathbb{Z}^+$, trovare n affinché M sia quadrato perfetto

Diofantee lineari in 2 variabili: tutte le soluzioni

$$ax + by = c$$

$$az + bw = c$$

$$a(x-z) + b(y-w) = 0$$

$$a(x-z) = -b(y-w)$$

Wlog $(a,b)=1$. $\quad a \mid b(y-w)$

$\Downarrow$ perché $(a,b)=1$

$a \mid (y-w)$

$$\Rightarrow \begin{cases} \boxed{w = y + ka} \\ a(x-z) = -b(-ka) \end{cases}$$

$$\Rightarrow x - z = kb \Rightarrow \boxed{z = x - kb}$$

$$mn + 2m - n - 8 = 0$$

$$(m-1)(n+2) - 6$$

$$(m-1)(n+2) = 6$$

$x^3 - y^3 = 7004$

7005

Osservazione $(x+3)^3 = x^3 + 9x^2 + 27x + 27$

$\equiv x^3 \pmod 9$

$0^3 \equiv 0 \quad 1^3 \equiv 1 \quad 2^3 \equiv -1 \ (9)$

$7005 \equiv 12 \equiv 3 \ (9)$

Quindi $x^3 - y^3 \equiv 3 \pmod 9$ non ha soluzioni

$$7004 = (x-y)\underbrace{(x^2+xy+y^2)}_{\substack{(x-y)^2+3xy \\ \geq (x-y)^2}}$$

$x \geq 0$, $y \geq 0$

$8000 > 7004 \geq (x-y)^3 \Rightarrow 20 > x-y$

Lavorando modulo 2 (mah...) trovo

$x \equiv y \ (2)$

Possono essere entrambi pari?

Se sì, $8 \mid x^3 - y^3 = 7004$, il che non è vero. Quindi $x \equiv y \equiv 1 \ (2)$, e

$x - y \equiv 0 \pmod 4$, siccome x^2+xy+y^2 è dispari

$4 \mid (x-y) \mid 7004 = 4 \cdot 17 \cdot 103$

E $x - y < 20$. Mmmh...

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

$x^2 \equiv 2 \pmod 3$

ma x^2 e' 0 o 1 modulo 3, assurdo

$3^y - x^2 = 41$

Parita' : x e' pari

Mod 4 : $3^y \equiv 1 \pmod 4$

$\Rightarrow$ y e' pari

$\Rightarrow$ scrivo $y = 2a$,

$(3^a - x)(3^a + x) = 41$

$3^y - 2^x = 41$

Se $x \leq 1$ non è interessante

Altrimenti $2^x \equiv 0 \pmod 4$, da cui

$$3^y \equiv 1 \pmod 4$$

$\Rightarrow$ y è pari

$-2^x \equiv 2 \pmod 3$

$2^x \equiv 1 \pmod 3 \Rightarrow x$ pari

$$4^x - 2^y = 4094 \qquad 4096 - 2 = 4094$$

$$0 - 2^y \equiv 2 \mod 4$$

$$\Rightarrow y \leq 1$$

(Esercizio 42)

$$4^x + 4^y + 4^z = 9 \cdot \text{qualcosa} + 1$$

Per parità, uno tra x, y, z è zero, diciamo z.

$$4^x + 4^y = \text{numerone} = 2^3 \cdot \text{dispari}$$

Quindi x e y non possono essere entrambi ≥ 2, e poi casi...

Altrimenti, contraddizione modulo 3

IMO 2009/1

Sia n un intero >0 e $a_1, \dots, a_k$ $(k \geq 2)$ interi distinti in $\{1, \dots, n\}$

Supponiamo che $n \mid a_i(a_{i+1} - 1)$ per $i = 1, \dots, k-1$.

Tesi: $n \nmid a_k(a_1 - 1) \iff a_1 a_k \not\equiv a_k$

$$a_i \cdot a_{i+1} \equiv a_i \mod n$$

$$a_1 a_2 \equiv a_1 \quad (n)$$

$$a_2 a_3 \equiv a_2 \quad (n) \rightarrow a_1 a_2 a_3 \equiv a_1 a_2 \equiv a_1$$

$$a_3 a_4 \equiv a_3 \quad (n)$$

$$a_1 a_2 a_3 a_4 \equiv a_1 a_2 a_3 \equiv a_1 a_2 \equiv a_1$$

$$\begin{cases} \overbrace{a_1 a_2}^{a_1} \cdots a_k \equiv a_1 \pmod{n} \\ a_1 a_k \equiv a_k \pmod{n} \end{cases}$$

Se per assurdo $\uparrow$ fosse vera, $a_k \equiv a_1 \ (n)$

Ma $a_1, \dots, a_k \in \{1, \dots, n\}$ e sono distinti, assurdo!

Teoria dei Numeri 2 (darkcrystal)

Titolo nota 06/09/2013

Inverso moltiplicativo

$ax \equiv b \pmod{n}$

$ax \equiv 1 \pmod{n}$ ammette soluzione

$\Updownarrow$

$ax + ny = 1$ ammette soluz.

$\Updownarrow$

$(a, n) = 1$

Supponiamo di avere una soluzione, chiamiamola s: $a \cdot s \equiv 1 \pmod{n}$

Come risolvo $a \cdot x \equiv b \pmod{n}$?

Moltiplico per "a^{-1}" (cioè s)

e trovo $(sa)x \equiv sb \ (n)$

$x \equiv sb \pmod{n}$

$s = a^{-1} =$ inverso moltiplicativo di a mod n

Quindi, in generale?

$$ax \equiv b \pmod{n}$$

$d = (a, n)$ $\qquad n' = n/(a,n)$

Condizione necessaria: $d \mid b$

$$(a,n) \underbrace{\frac{a}{(a,n)}}_{a'} x \equiv (a,n) \underbrace{\frac{b}{(a,n)}}_{b'} \pmod{n}$$

$\Leftrightarrow$

$$a' x \equiv b' \pmod{n'}$$

$$\Longleftrightarrow \qquad x \equiv (a')^{-1} b' \pmod{n'}$$

Oss importante

Supponiamo di sapere $ax \equiv ay \mod n$ con $(a, n) = 1$. Allora $x \equiv y \pmod{n}$

Dim: moltiplico per a^{-1} entrambi i membri

$$3x \equiv 3 \pmod{10} \Rightarrow x \equiv 1 \ (10)$$

(Peraltro, $3^{-1} \equiv 7 \pmod{10}$)

Se invece ho $3x \equiv 13 \pmod{10}$, non posso "dividere per 3", ma posso "molt.

per $7 \equiv 3^{-1}$ ", quindi:

$$21x \equiv 91 \pmod{10}$$

$$x \equiv 1 \pmod{10}$$

Teorema Cinese del Resto

Cosa succede se ho 2 (o più) congruenze modulo cose diverse?

$$\begin{cases} x \equiv 13 \pmod 8 \\ x \equiv 1000 \pmod{96} \end{cases}$$

Un tale x non esiste! (parità)

$$\begin{cases} x \equiv 3 \mod 4 \\ x \equiv 7 \mod 5 \end{cases} \qquad x = 7$$

$$\iff \begin{cases} x \equiv 7 \mod 4 \\ x \equiv 7 \mod 5 \end{cases}$$

$$\iff 4 \mid x-7 \quad \text{e} \quad 5 \mid x-7$$

$$\iff 20 \mid x-7 \iff x \equiv 7 \pmod{20}$$

Con Bézout: $x = 3 + 4k$

$$x - 7 = (-4 + 4k) = 5h$$

$$\iff 4k + 5h' = 4$$

TEO: Un sistema di congruenze

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$$

in cui $(m, n)=1$ ammette una ed una sola soluzione modulo $m \cdot n$

$$\begin{cases} x \equiv 13 \pmod{96} \\ x \equiv 27 \pmod{8} \end{cases}$$

Vogliamo moduli coprimi

$$x \equiv 13 \pmod{\underset{3 \cdot 32}{\underset{\parallel}{96}}} \iff \begin{cases} x \equiv 13 \pmod{3} \\ x \equiv 13 \pmod{32} \end{cases}$$

$$\begin{cases} x \equiv 13 \pmod{3} \\ x \equiv 13 \quad (\ 32) \\ x \equiv 27 \quad (\ 8) \end{cases} \rightsquigarrow \quad \begin{matrix} x \equiv 13 \pmod{8} \\ x \equiv 27 \pmod{8} \end{matrix}$$

Il sistema non ha soluzione. Invece

$$\begin{cases} x \equiv 13 \pmod{96} \\ x \equiv 5 \pmod{8} \end{cases}$$

$$\iff \begin{cases} x \equiv 13 & (3) \\ x \equiv 13 & (32) \\ x \equiv 5 & (8) \quad \text{inutile} \end{cases}$$

Esempio

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 5 \quad (\ 6) \\ x \equiv 6 \quad (\ 7) \\ x \equiv 7 \quad (\ 8) \\ x \equiv 8 \quad (\ 9) \end{cases}$$

$$\Longleftrightarrow \begin{cases} x \equiv 4 & (5) \\ \cancel{x \equiv 1} & (2) \\ \cancel{x \equiv 2} & (3) \\ x \equiv 6 & (7) \\ x \equiv 7 & (8) \\ x \equiv 8 & (9) \end{cases} \Longleftrightarrow \begin{cases} x \equiv 4 & (5) \\ x \equiv 6 & (7) \\ x \equiv 7 & (8) \\ x \equiv 8 & (9) \end{cases}$$

Esiste un'unica soluz, della forma

$$x \equiv \ ? \qquad (\bmod\ 5 \cdot 7 \cdot 8 \cdot 9)$$

$$\Longleftrightarrow \begin{cases} x \equiv -1 & (5) \\ & (7) \\ \quad '' & (8) \\ & (9) \end{cases}$$

LA soluzione è quindi $x \equiv -1 \ (5 \cdot 7 \cdot 8 \cdot 9)$

Altro esempio Trovare il resto della divisione di 10^{100} per 144

$$x \equiv 10^{100} \quad (\bmod\ 2^4 \cdot 3^2)$$

$$\Longleftrightarrow \begin{cases} x \equiv 10^{100} & (\bmod\ 2^4) \\ x \equiv 10^{100} & (\bmod\ 3^2) \end{cases}$$

$$\Longleftrightarrow \begin{cases} x \equiv 0 & (\bmod\ 2^4) \\ x \equiv 1 & (\bmod\ 3^2) \end{cases}$$

$$\Longleftrightarrow \quad x \equiv 64 \quad \bmod\ 144$$

Comportamento delle potenze

$1, a, a^2, a^3, \dots \mod n$

Per pigeonhole, esistono due esponenti h e k con $a^h \equiv a^k \mod n$ $(\star)$

Diciamo $k > h$

Supponiamo che $\boxed{(a, n) = 1.}$ ⚠

Allora esiste un b t.c. $ab \equiv 1 \pmod n$,

e da $\star$ trovo $b^h a^h \equiv b^h a^h a^{k-h} \ (n)$

$\iff (ba)^h \equiv (ba)^h \cdot a^{k-h} \pmod n$

$\iff 1 \equiv a^{k-h} \pmod n$

Se non ho $(a, n) = 1$?

Potenze di 2 mod 16 : $\underbrace{1, 2, 4, 8,}$ $0, 0, 0, \dots$

Potenze di 2 mod 48:

$\underbrace{1, 2, 4, 8,}$ $16, 32, 16, 32, \dots$

$2^k \mod 48 \longleftrightarrow \begin{cases} 2^k \mod 3 \\ 2^k \mod 16 \end{cases}$

$\begin{cases} 2^0 \equiv 1 & \pmod 3 \\ 2^0 \equiv 1 & \pmod{16} \end{cases}$

$$\begin{cases} 2^1 \equiv 2 & (\bmod 3) \\ 2^1 \equiv 2 & (\quad 16) \end{cases}$$

$$\vdots$$

per $k \geq 4$ $\begin{cases} 2^k \equiv (-1)^k & (\bmod 3) \\ 2^k \equiv 0 & (\bmod 16) \end{cases}$

Potenze di 6 mod $2^5 \cdot 3^7$: prima o poi fanno zero...

Ordine moltiplicativo $(a, n) = 1$. Sappiamo che esiste $h > 0$ t.c. $a^h \equiv 1 \pmod n$

L' **ord. molt.** di a mod n – $\mathrm{ord}_n(a)$ – e' il più piccolo h con questa proprietà.

Prop. fondamentale $a^x \equiv 1 \pmod n$

$$\iff \mathrm{ord}_n(a) \mid x$$

$\Leftarrow$ ovvio: $a^x = \left(a^{\mathrm{ord}}\right)^{\text{qualcosa}} \equiv 1^q \equiv 1$

$\Rightarrow$ Scriviamo $x = \mathrm{ord}_n(a) \cdot h + r$,

dove $0 \leq r < \mathrm{ord}_n(a)$

$$1 \equiv a^x \equiv \left(a^{\mathrm{ord}_n(a)}\right)^h \cdot a^r \pmod n$$

$$\equiv 1^h \cdot a^r \pmod n$$

Quindi $a^r \equiv 1 \pmod n$, e siccome

$r < \text{ord}_n(a)$ r deve essere 0,

cioè $\text{ord} \mid x$.

Ordine moltiplicativo = periodo della successione

Cosa può essere $\text{ord}_p(a)$?

Piccolo Teorema di Fermat: se $(a, p) = 1$,

$$a^{p-1} \equiv 1 \pmod p,$$

ovvero $\text{ord}_p(a) \mid (p-1)$

Sempre $a^p \equiv a \pmod p$

Dimostrazione Considero $\{1, 2, 3, \dots, p-1\}$

e $\{a, 2a, 3a, \dots, (p-1)a\}$

Dico che modulo p sono lo stesso insieme

$p = 5$, $a = 3$ $\{1, 2, 3, 4\}$

$\{3, 6, 9, 12\}$

Basta verificare che $i \neq j \Rightarrow i \cdot a \not\equiv j \cdot a \ (p)$

Infatti

* $ia \not\equiv 0 \ (p)$, perché per ipotesi $p \nmid a$ e $i = 1, \dots, p-1$, quindi $p \nmid i$
* se sono tutti diversi mod p, i loro rappr. privilegiati sono tutti diversi: ma questi sono $p-1$ numeri compresi tra 1 e $p-1$, quindi sono (in un qualche ordine) $1, 2, \dots, p-1$

Verifichiamolo: $ia \equiv ja \pmod p$

$$\Rightarrow i \equiv j \pmod p$$

$$\Rightarrow i = j \quad (\text{perché entrambi } < p)$$

Allora

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv a \cdot (2a) \cdot (3a) \cdots (p-1)a \quad (p)$$

$$(p-1)! \equiv (p-1)!\, a^{p-1} \pmod p$$

$$\Leftrightarrow 1 \equiv a^{p-1} \mod p$$

Ex $(p-1)! \equiv -1 \pmod p$

E con n generico? "Teorema di Eulero - Fermat"

Siano a, n coprimi. Allora $a^{\varphi(n)} \equiv 1 \ (n)$.

Cos'è $\varphi(n)$?

$$\varphi(n) = \#\{1 \leq k \leq n \ \text{ t.c. } (k,n)=1\}$$

$\varphi(6)$? $\quad 1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6} \quad \varphi(6) = 2$

$\varphi(p) = p-1 \quad$ ($\Rightarrow$ piccolo t. Fermat)

$\varphi(3^{100}) =$ tutti $-$ multipli di 3

$= \text{tutti} - 3^{99} = 3^{99} \cdot 2$

$$\varphi(p^k) = p^k - \frac{1}{p} p^k = p^{k-1} \cdot (p-1)$$

Fatto: Se $(m,n) = 1$, $\quad \varphi(m \cdot n) = \varphi(m)\varphi(n)$

$$\varphi(144) = \varphi(2^4 \cdot 3^2) = \varphi(2^4)\varphi(3^2)$$
$$= 2^3 \cdot 3 \cdot (3-1) = 3 \cdot 2^4$$

Es. $\quad 5^{48} \equiv 1 \pmod{144}$

Oss: se $(a,n)=1$, $\quad \mathrm{ord}_n(a) \mid \varphi(n)$

Ex $x^{19} - y^{19} \equiv 0 \mod 31$

* 31 e' primo. Se $31 \mid x$, $31 \mid y$, quindi

$x \equiv 0 \ (31) \iff y \equiv 0 \ (\mathrm{mod}\ 31)$

* Se $31 \nmid y$, esiste l'inverso di y mod 31, chiamiamolo z. $x^{19}z^{19} - y^{19}z^{19} \equiv 0 \ (31)$

$\Rightarrow \ (xz)^{19} - 1 \equiv 0 \ (31)$

$\Rightarrow \ \boxed{(xz)^{19} \equiv 1 \ (\mathrm{mod}\ 31)}$

* $\mathrm{ord}_{31}(xz) = ?$ $\quad \mathrm{ord}_{31}(xz) \mid 19$

Eulero - Fermat $\Rightarrow$ $\mathrm{ord}_{31}(xz) \mid \varphi(31) = 30$

$\mathrm{ord}_{31}(xz) = 1$

* Quindi $(xz)^1 \equiv 1 \ (\mathrm{mod}\ 31)$: moltiplico per y e trovo $x \equiv y \ (\mathrm{mod}\ 31)$

Generatori

La stima del FLT e' la migliore possibile?

Cioe': esiste un a t.c. $\mathrm{ord}_p(a) = p-1$?

Risposta: si, cioe' per ogni p esiste una classe di resto g t.c. $\mathrm{ord}_p(g) = p-1$, e un tale elemento si chiama GENERATORE

$p = 7, \quad a = 3$

$$\underbrace{1,\ 3,\ 2,\ 6,\ 4,\ 5,}_{6 = p-1}\ 1, \dots$$

Tutte le classi di resto modulo p si scrivono come una potenza di un generatore

Ex Esistono esattamente $\varphi(\varphi(p))$ generatori.

Un elemento $a = g^i$ che ordine ha?

$$a^x \equiv 1 \pmod p \iff g^{ix} \equiv 1 \pmod p$$

$$\underset{g \text{ generatore}}{\iff} (p-1) \mid ix$$

$p = 7$, $g = 3$: se considero 3^2, questo non ha speranze: $(3^2)^3 = 3^6 \equiv 1 \pmod 7$

Sia $d = (i, p-1)$

Allora $p-1 \mid ix \iff \frac{p-1}{d} \mid \frac{i}{d} \cdot x$

$\iff \frac{p-1}{d} \mid x$

Quindi $\mathrm{ord}_p(a) = \mathrm{ord}_p(g^i) = \frac{p-1}{(i, p-1)}$.

Se voglio che a sia un generatore, è nec. e suff. che $(i, p-1) = 1$. Quanti interi esistono coprimi con $p-1$ e minori di p? $\varphi(p-1) = \varphi(\varphi(p))$

Esistenza di un generatore in generale

Esiste un generatore mod n, cioè un g con

$$\mathrm{ord}_n(g) = \varphi(n),$$

se e solo se $n = 2, 4, p^k$ o $2p^k$ con p primo dispari

Fatto Se g è un generatore mod p, allora o g o $g+p$ è un generatore mod p^k per ogni k

Residui quadratici

Cioè: quand'è che $x^2 \equiv a \pmod p$ ha soluzioni?

* $a = 0$
* Se $y^2 \equiv z^2 \bmod p$, allora $(y-z)(y+z) \equiv 0\ (p)$,

quindi $p \mid x-y$ oppure $p \mid x+y$

$$\Updownarrow \qquad\qquad \Updownarrow$$

$$x \equiv y\ (p) \qquad\qquad x \equiv -y\ (p)$$

* In particolare,

$$1 \quad 2 \quad 3 \cdots \frac{p-1}{2} \quad \underbrace{\frac{p+1}{2} \cdots p-1}_{\frac{p-1}{2}}$$

quadrati

$$1^2 \quad 2^2 \quad 3^2 \cdots \left(\frac{p-1}{2}\right)^2 \quad \left(-\frac{p-1}{2}\right)^2 \quad \left(-\frac{p-3}{2}\right)^2 \cdots (-1)^2$$

$$1 \quad 2 \quad 3 \quad (-3) \quad (-2) \quad (-1)$$

$$1 \quad 4 \quad 9 \quad 9 \quad 4 \quad 1$$

Morale: ci sono

lo zero $\rightarrow 1 + \dfrac{p-1}{2} \leftarrow$ residui non-zero

residui quadratici

Quadrati vs generatore

$$1, g, g^2, g^3, g^4, \dots, g^{p-2}$$

quadrati

Residui quadratici = generatore elevato alla numero pari

Ma allora, cosa sono le potenze 19-esime mod 31? TUTTO!

Prendiamo una classe di resto mod 31,

$$a \equiv g^i \pmod{31}$$

Dico che posso scegliere $i \equiv 0 \pmod{19}$

Infatti posso sostituire i con $i+30$, ed in generale con qualunque esponente congruo ad i mod 30.

Ma $\begin{cases} x \equiv i \pmod{30} \\ x \equiv 0 \pmod{19} \end{cases} \xRightarrow{\text{TCR}}$ ha soluzione

$\Rightarrow$ posso scegliere i multiplo di 19.

Esercizi 32 p. 10, 33, 46, 48, 50

pag. 33 4, 7 e 10

Esistono 2013 interi consecutivi ognuno divisibile per una quinta potenza perfetta

$$\begin{cases} x \equiv 0 & (p_0^5) \\ x+1 \equiv 0 & (p_1^5) \\ x+2 \equiv 0 & \\ \vdots & \vdots \\ x+2012 \equiv 0 & (p_{2012}^5) \end{cases}$$

$p_0, p_1, \ldots, p_{2012}$ primi tutti distinti.

TCR $\Longrightarrow$ esiste una soluzione (unica modulo $(p_0 \cdots p_{2012})^5$)

Per ogni p primo, esistono infiniti n per cui $p \mid 2^n - n$

* Può succedere che $p \mid n$? Allora $p \mid 2^n$, e $p=2$ (posso prendere n pari)

* $2^n \equiv n \pmod{p}$

"periodico di periodo p"

periodico, di un periodo che divide $p-1$

Se sostituisco n con $n + Kp(p-1)$ che succede?

$$2^{n+Kp(p-1)} \equiv 2^n \cdot \big(\underbrace{2^{p-1}}_{1 \text{ FLT}}\big)^{Kp} \equiv 2^n \pmod{p}$$

$$n + Kp(p-1) \equiv n \pmod{p}$$

* Basta trovare una soluzione

* Sappiamo che 2^n può fare 1.
Succede (perlomeno) se $n = h(p-1)$
Il membro destro è $\equiv 1$ se (sorpresa) $n \equiv 1 \ (p)$

Funzionano gli n con $\begin{cases} n \equiv 0 & (p-1) \\ n \equiv 1 & (p) \end{cases}$

Uno esplicito e' dato da $(1-p) + p(p-1)$

$= (p-1)^2$

Ultime 5 cifre di $5^{5^{5^{5}}} = x$

Voglio $x \bmod 10^5$

$$\iff \begin{cases} x \equiv 0 \mod 5^5 \\ x \quad \mod 2^5 \end{cases}$$

Cosa sappiamo? $5^{\varphi(32)} \equiv 1 \pmod{32}$

$$5^{\text{mostro}} \bmod 32 \equiv 5^{(\text{mostro} \bmod \varphi(32))} \ (32)$$

$\varphi(32) = 16$: voglio $5^{5^{5^5}} \bmod 16$

voglio $5^{5^5} \bmod 8$

Siccome $5^5 \equiv 1 \pmod 4$, $5^{5^5} \equiv 5^1 \pmod 8$,

da cui $5^{5^{5^5}} \equiv 5^5 \pmod{16}$

$\equiv 5 \pmod{16}$

Oss: x dispari $\Rightarrow x^2 \equiv 1 \pmod 8$

$\Rightarrow x^2 = 8k+1 \Rightarrow x^4 = 1 + 16k + 64k^2$

$x^4 \equiv 1 \pmod{16}$

$$\begin{cases} x \equiv 5^5 \mod 32 \\ x \equiv 5^5 \mod (5^5) \end{cases} \Rightarrow x \equiv \overset{03125}{\overset{\parallel}{5^5}} \pmod{10^5}$$

$D = \{ n \text{ t.c. } n \mid 2^n + 1 \}$

PIÙ PICCOLO PRIMO (ppp)

Sia p il ppp di n.

$$p \mid 2^n + 1 \iff 2^n \equiv -1 \pmod p$$
$$\Downarrow$$
$$2^{2n} \equiv 1 \pmod p$$

$$\begin{cases} \mathrm{ord}_p(2) \mid 2n \\ \mathrm{ord}_p(2) \mid (p-1) \end{cases} \Rightarrow \mathrm{ord}_p(2) \mid (p-1, 2n) = 2$$

Perché $(p-1, 2n) = 2$? Se $q \mid n$ e $q \mid p-1$, allora $q \leq p-1 < p = \mathrm{ppp}(n)$ e quindi non esiste

$$\mathrm{ord}_p(2) = \begin{cases} 1 \Rightarrow 2^1 \equiv 1 \pmod p \Rightarrow \text{assurdo} \\ 2 \Rightarrow 2^2 \equiv 1 \pmod p, \end{cases}$$

quindi $p = 3$.

b) $3^k \in D$? $\quad 3^k \mid 2^{3^k} + 1$

Per induzione su k. $k = 1$ ok

Se è vero per k, $2^{3^k} + 1 = 3^k \cdot q$

Cosa fa $2^{3^{k+1}}+1 = (2^{3^k})^3+1$

$= (3^k \cdot q - 1)^3 + 1 =$

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

$\equiv 0 \pmod{3^{k+1}}$

$3^{k+1} \parallel 2^{3^k}+1$

Ancora residui d-esimi (mod p)

Fatto: ce ne sono esattamente

$$1 + \frac{p-1}{(p-1, d)}$$

Quali sono le classi di resto mod p?

$$1 = g^0, g^1, g^2, \ldots, g^{p-2}$$

Ci chiediamo se l'equazione $a \equiv x^d \ (p)$ (per a fissato) ha soluzione.

Scrivo $a = g^i$ e $x = g^y$: allora l'equazione diventa $g^i \equiv g^{yd} \bmod p$

$\Longleftrightarrow (p-1) \mid yd - i \Longleftrightarrow yd \equiv i \ (p-1)$

$\Longleftrightarrow dy + (p-1)z = i$

Bézout

$\Longleftrightarrow$ ha soluzione se e solo se $(d, p-1) \mid i$

Quindi $a = x^i$ è residuo d-esimo $\Longleftrightarrow$ $(d, p-1) \mid i$. Quindi i residui d-esimi $\neq 0$ sono in corrispondenza con gli esponenti $i = 0, \ldots, p-2$ divisibili per $(d, p-1)$, e quindi sono $\dfrac{p-1}{(d, p-1)}$

Esempio $y^2 = x^5 - 4$ non ha soluz mod 11.