Stage Senior 2013 – Livello Medium

Stampato integrale delle lezioni

Autori vari

Indice

A1 MEDIUM pol

Titolo nota 03/09/2013

POLINOMI

$$a(x) = \sum_{i=0}^{d} a_i x^i \qquad \max\{i : a_i \neq 0\} = \deg a$$

coefficienti in un anello

$\mathbb{R}$ $\mathbb{C}$ $\mathbb{Z}$ F_m $\mathbb{Z}/(m\mathbb{Z})$ $\mathbb{Z}_m$

campo campo no campo se m primo $\Leftrightarrow \exists$ inversi molt. di ogni num $\neq 0$

$X^p - X$ $\mathbb{F}_p$ zero come funzione ma non come polinomio

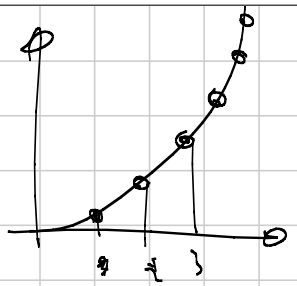
Principio di identità dei polinomi

dati $p(x)$, $q(x)$ poly. di grado $\leq d$

se $p(x_i) = q(x_i)$ per $d+1$ punti distinti

allora $p(x) = q(x)$ come polinomi

$x+y$ $x+y^2$ coincidono per ogni $x \in \mathbb{Z}$, $y = 0$



$p(x,y)$ $\quad p(n,n^2)=0$

$(y^2-x)\cdot q(x,y)$ sono tutti:

$(R[y])[x]$

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

$\underbrace{1+y}_{a_0} + \underbrace{1\cdot x}_{a_1} + \underbrace{y^2\cdot x^2}_{a_2}$

$p(x)$ $\quad$ Ruffini

$p(2)=5$ $\quad p(4)=5$ $\quad$ cosa so su $p(0)$?

(coefficienti interi)

$f(x)=p(x)-5$ si annulla in $x=2,\ x=4$

$f(x)=(x-2)(x-4)\,q(x)$

$p(x)=(x-2)(x-4)\,q(x)+5$

$\uparrow$

interi

$p(0)=-2\cdot -4\cdot q(0)+5$ $\quad p(0)\equiv 5 \mod 8$

$a-b \mid p(a)-p(b)$ $\forall$ p coeff. interi

$4-0 \mid p(4)-p(0) = 5-p(0)$ $\quad p(0) \equiv 5 \ (4.)$

$p(0) \equiv 5 \ (2)$

$(x_0, y_0), (x_1, y_1), \dots (x_d, y_d)$ | coeff. campo

$d+1$ pt con x_i distinte

$\exists!$ $p(x)$

$(9x+3)(6x+2) =$ $\quad F_{18}$ mod 18

$= 0 \cdot x^2 + 0 \cdot x + 6$

$\deg(p \cdot q) = \deg p + \deg q$ $\Leftarrow$ campo

- fatt. unica vale Campo$[x]$

Campo$[x, y, z, \dots]$

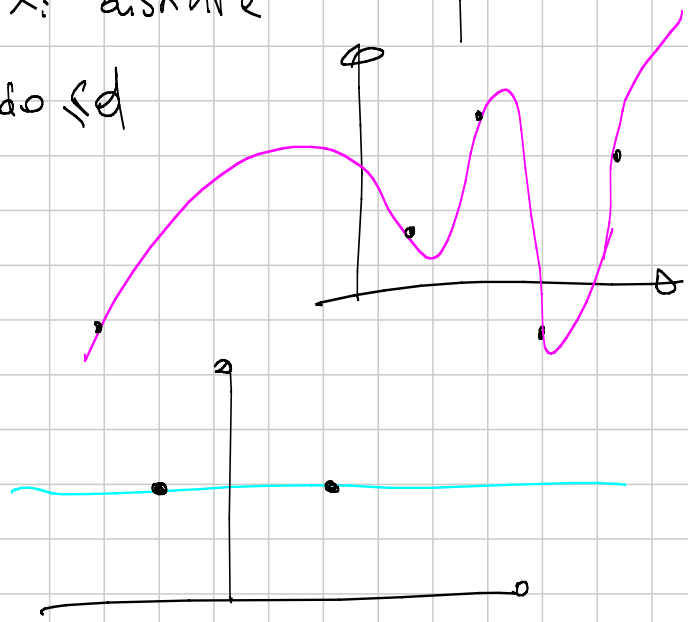
$\mathbb{Z}[x, y, z, \dots]$

Thm: Interpolazione (di Lagrange) | coeff. comp

$(x_0, y_0), (x_1, y_1), \dots (x_d, y_d)$

$d+1$ pt con x_i distinte

$\exists!$ $p(x)$ di grado $\leq d$



Come si dimostra?

1) caso facile

$(x_0, 1), (x_1, 0), (x_2, 0) \dots (x_d, 0)$

$L_0(x)$

$$\frac{(x-x_1)(x-x_2)\cdots(x-x_d)}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_d)} = L_0(x)$$

2) $L_i(x)$ t.c. $L_i(x_j) = \begin{cases} 1 & i=j \\ 0 & \text{altrimenti} \end{cases}$

3) $\sum_{i=0}^{d} y_i L_i(x)$ funziona!

4) unicità $f(x)$; $g(x)$

$f(x) - g(x)$ ha grado $\leq d$

Si annulla in $x_0, x_1, \dots x_d$

$$f(x) - g(x) = (x-x_0)(x-x_1)(x-x_2)\dots(x-x_d)\cdot q(x)$$

$$q(x) = \sum_{i=0}^{d} a_i x^i$$

a_i: incognite

$$\begin{cases} a_0 + a_1 x_0 + a_2 x_0^2 + \dots a_d x_0^d = y_0 \\ a_0 + a_1 x_1 + a_2 x_1^2 + \dots a_d x_1^d = y_1 \\ \vdots \qquad\qquad \vdots \end{cases}$$

$d+1$ eq. in $d+1$ incognite $a_0, a_1, \dots a_d$

$$\begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^d \\ 1 & x_1 & x_1^2 & & \\ 1 & x_2 & & \ddots & \\ \vdots & \vdots & & & \\ 1 & & & & x_d^d \end{bmatrix} = \text{matrice di Vandermonde}$$

$$\prod_{i<j} (x_j - x_i)$$

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 5 \pmod{14} \end{cases}$$

1) si risolve prima $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 0 \pmod 5 \\ x \equiv 0 \pmod{14} \end{cases}$

$5 \cdot 14 \cdot (\text{inverso di } 5 \cdot 14 \bmod 3) = L_i$

$$\sum_i y_i L_i$$

polinomi $\longleftrightarrow$ interi

in una var. coeff. in un campo

1) divisione TH dati $a(x), b(x), \exists\, q(x), r(x)$

$$a(x) = q(x) \cdot b(x) + r(x)$$

$$\deg r < \deg b$$

$\Rightarrow$ Algoritmo di Euclide

$\Rightarrow$ Bézout

TH dati $a(x), b(x)$ senza fattori comuni

$\exists\, p(x), q(x)$ t.c.

$$a(x)p(x)+b(x)q(x)=1$$

$a(x) \equiv b(x) \mod m(x)$

se $a(x)-b(x)$ è multiplo di $m(x)$

$x+a \mid x^m+a^m \iff m$ dispari

$x \equiv -a \quad x^m \equiv (-a)^m$ — m pari a^m; m dispari $-a^m$

$x^m \equiv -a^m$ per m dispari

$x+a \mid x^m+a^m$

$\mathbb{Z}[x] \subseteq \mathbb{C}[x]$

$a(x) = a_d(x-x_1)(x-x_2)\cdots(x-x_d)$

x_1, x_2 complessi

$d(x) \mid a(x)$

$d(x)\cdot q(x) = a(x)$

$d(x) \mid a(x)$ se $\exists\, q(x)$ t.c.

$d(x)\,q(x) = a(x)$

1) le radici di d sono radici di a
2) se sono in $\mathbb{C}$, d, a si spezzano in fattori lineari

$$(x-x_1)(x-x_2)\cdots(x-x_d)$$

$$3(x+1) \mid 2(x^2+2x+1)$$

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

$$x^{\phi(m)} = 1$$

$$x_1, x_2 \cdots x_{\phi(m)}$$

$$x\cdot x_1, x\cdot x_2 \cdots x\cdot x_{\phi(m)}$$

$$x_1 \cdot x_2 \cdots x_{\phi(m)}$$

$$x^{\phi(m)} x_1 x_2 \cdots x_{\phi(m)}$$

$\Rightarrow F_p$ funziona

$$p(x_0) = y_0$$

$$\begin{cases} p \equiv y_0 & (x-x_0) \\ p \equiv y_1 & (x-x_1) \\ \vdots & \\ p \equiv y_d & (x-x_d) \end{cases}$$

$p(x) \mid \mod(x-a)$

$p(x) \mid x-a$

$\vdots$

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

$a+b+c \mid$

$a^3+b^3+c^3-3abc$ ribattezziamo $c=x$

$a+b+x \mid a^3+b^3+x^3-3abx$

Divisione tra polinomi in $(\mathbb{R}[a,b])[x]$

$\underbrace{a^3+b^3+x^3-3abx}_{p(x)} = (a+b+x)\,q(x) + r(x)$

$r = p(-a-b)$

$a^3+b^3+(-a-b)^3-3ab(-a-b) =$

$= a^3+b^3-a^3-3a^2b-3ab^2-b^3+3ab(-a+b) =$

$=0$

Oss: quando faccio $a(x) : b(x)$

$a(x) \mid b(x)$

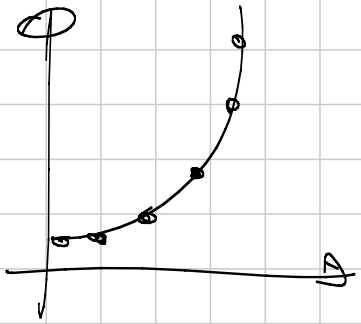
se $b(x)$ è monico, allora arrivo alla fine

senza dover fare divisioni
⇒ funziona anche in $\mathbb{Z}$, (e in un anello generico)
e $q(x)$, $r(x)$ hanno coefficienti nell'anello

$ax^3+3x^2+3x+1 \;|\; bx+1$
ax^3+ax^2
//

non sempre funziona

$p(x,y)$ per ogni $n \in \mathbb{N}$



$p(n, n^2) = 0$

Th $p(x,y) = (y-x^2) \cdot$ polinomio(x,y)

1) $p(z, z^2)$ polinomio nella sola z
si annulla per ogni $z = 1, 2, 3, \ldots \in \mathbb{N}$ (Hp)
⇒ $p(z, z^2)$ è il polinomio 0

2) Guardiamo x "coefficiente", y "indeterminata"
$(\mathbb{C}[x])[y]$
$y-x^2$ è un poly. di primo grado in y
Ruffini!
$p(x,y) = q(x,y) \cdot (y-x^2) + r(x,y)$
grado 1 in y grado 0 in y

per Ruffini, è $p(x, x^2)$ $\equiv 0$

polinomio in (x,y) perché $y - x^2$ è monico $\Rightarrow$ non servono divisioni

$x^3 + 1$

Qual è il resto della divisione

$$x^{2013} + x^{1000} + x + 1 \quad \big| \; x^3 + 1 \qquad ?$$

$x^3 \equiv -1$

$$(x^3)^{\text{roba}} \equiv (-1)^{\text{roba}} \equiv -1$$

$$x^{2013} \equiv (x^3 + 1)\, x^{2010} - x^{2010}$$

congruenze $\Leftrightarrow$ somme/sottrazioni multipli

$$x^{2013} + x^{1000} + x + 1 \equiv -1 + x \cdot x^{1111999} + x + 1 \equiv (x^3 + 1)$$

$$\equiv -1 - x + x + 1 = 0$$

congruenze modulo $x^3 - x + 2$: faccio i conti normalmente, tutte le volte che trovo x^3 lo rimpiazzo con $x - 2$

ogni $f \in \mathbb{R}[x]$ ha un "rappresentante privilegiato" modulo (x^3-x+2) del tipo ax^2+bx+c

$$\frac{\mathbb{R}[x]}{(x^3-x+2)} = \{\text{classi di resto dei polinomi mod } x^3-x+2\}$$

Se il polinomio $p(x)$ è irriducibile in $F(x)$ (F campo) allora $\dfrac{F(x)}{(x^3-x+2)}$ è un campo

Dim: Bézout

$$a(x)p(x) + (x^3-x+2)q(x) = 1$$

$$a(x)p(x) \equiv 1 \pmod{x^3-x+2}$$

Irriducibili in $\mathbb{C}[x]$: solo i polinomi di grado 1!

$$p(x) = a(x-x_1)(x-x_2)\cdots(x-x_d)$$

Irriducibili in $\mathbb{R}[x]$?

$$(x-x_0)(x-x_1)\cdots(x-x_r)\,(x-c_1)(x-\bar{c}_1)(x-c_2)(x-\bar{c}_2)\cdots(x-c_s)(x-\bar{c}_s)$$

Ruffini

- grado 1
- grado 2 con $\Delta < 0$

$$\frac{\mathbb{R}[x]}{(x^2+1)}$$

$$(a+bx) \cdot (c+dx)$$

$$(a+bx)(c+dx) = ac + bcx + adx + bdx^2$$
$$\equiv (ac - bd) + (bc + ad)x$$

$$\frac{\mathbb{Q}[x]}{(x^3-x+2)} = \{ ax^2+bx+c \,;\, a,b,c \in \mathbb{Q} \}$$

(campo)

perché lui è irriducibile?

Rational root theorem: in $\mathbb{Z}[x]$
se un polinomio ha radici razionali p/q,
allora p | termine noto, q | coeff. grado massimo

(Achtung: no radici $\neq$ irriducibile in generale)

$$(x^2+1)(x^2+5)$$

Irriducibile $\stackrel{\text{def}}{=}$ non posso scriverlo come $a(x)b(x)$
(con a,b non costanti)

$\mathbb{F}_7$, 5 no residuo quadratico

x^2-5 irriducibile in $\mathbb{F}_7$

$$\frac{\mathbb{F}_7[x]}{(x^2-5)} = \{ a+bx \;:\; a,b \in \mathbb{F}_7 \}$$

Faccio i conti normalmente, quando ho x^2 lo rimpiazzo con 5

Invece di x, posso chiamarlo "$\sqrt{5}$"

Fibonacci:

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

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

Cosa succede ai Fibonacci mod p?

1) se 5 è un residuo quadratico, allora $\exists\, a$ classe di resto t.c. $a^2 = 5$

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

Es. $p=11$, $4^2=5$

2) se 5 non è res. quadratico,

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

Fate i conti sostituendo $(\sqrt{5})^2$ con 5

3) $p=5$

Corollario

$\forall n,\ F_{n+p} \equiv F_{n+1}$ per i primi di Tipo 1

$\Rightarrow$ periodo (un divisore di) $p-1$

Tipo 2 Abbiamo aggiunto $\sqrt{5}$; non vale più piccolo th. Fermat per gli "oggetti" che abbiamo aggiunto

$$y^p - y \in \left[\frac{F_p[x]}{(x^2-5)}\right][x]$$

$0, 1, 2, \dots p-1$

$\sqrt{2}$ $\longrightarrow$ radice dell'equazione $x^2-2=0$

"$-\sqrt{2}$" $\longleftarrow$

$\sqrt{2}$ $\quad -\sqrt{2}$

Qual è il resto mod 5 di

$$\left\lfloor (\sqrt{2}+1)^{2013} \right\rfloor ?$$

$$Q_{2013} = \left\lfloor (\sqrt{2}+1)^{2013} + (-\sqrt{2}+1)^{2013} \right\rfloor = \left\lfloor (\sqrt{2}+1)^{2013} \right\rfloor$$

piccolissimo

$\S\S$

$0,000\dots 01$

$a_0 = \dots$

$a_1 = \dots$

$a_{n+1} = ?\,a_n + ?\,a_{n-1}$ $\qquad a_{2013} = ?\lambda_1^{2013} + ?\lambda_2^{2013}$

Lavoriamo al contrario!

$a_n := (\sqrt{2}+1)^n + (-\sqrt{2}+1)^n$

$a_0 = 2$

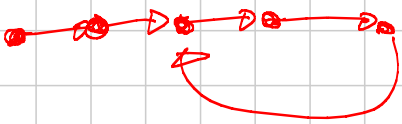
$a_1 = 2$

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

$$\begin{vmatrix} a_n \\ a_{n+1} \end{vmatrix} = \begin{vmatrix} a_n \\ a_{n+1} \end{vmatrix}$$

$(x-1)^2 = 2$

$x^2 - 2x - 1 = 0$



$\cos(15°) + \cos(30°) + \cos(45°) + \dots + \cos(315°)$

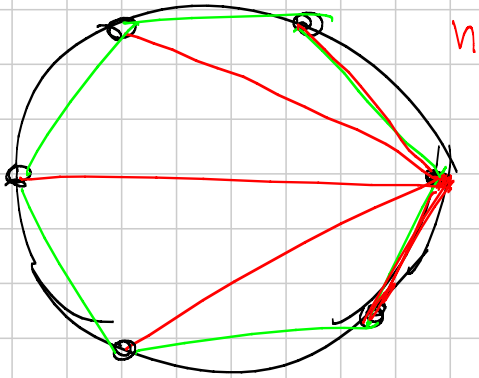
$\cos x + \cos 2x + \dots + \cos(nx) +$

$+ i\sin x + i\sin 2x + \dots + i\sin(nx)$

$= e^{ix} + e^{2ix} + \dots e^{nix} = \dfrac{1 - e^{nix}}{1 - e^{ix}} e^{ix}$

$$\Rightarrow \cos x + \dots + \cos nx = \mathrm{Re}\left[\frac{1+e^{nix}}{1-e^{ix}}\, e^{ix}\right]$$

Es

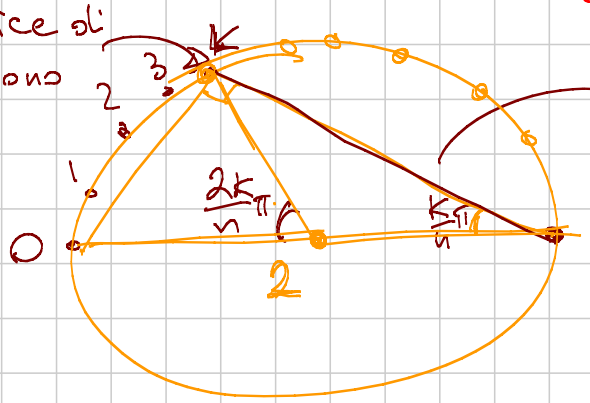


n-agono regolare in cerchio di raggio 1

Diagonali che partono da un vertice;

Quanto vale la somma delle loro lunghezze?

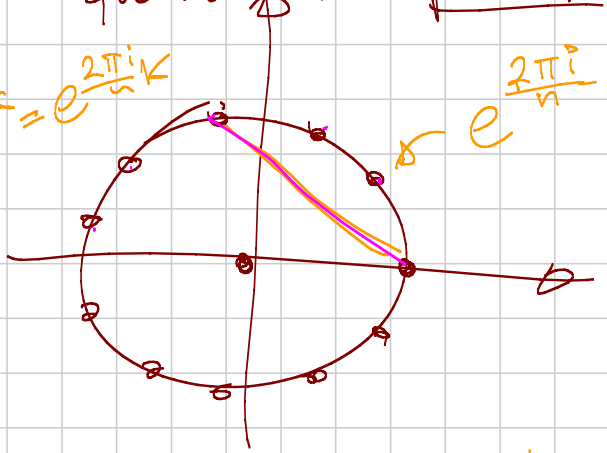
k-vertice di un n-agono



$$\to 2\cdot\cos\frac{k}{n}\pi$$

Es quanto vale prodotto delle diagonali?

$$w^k = e^{\frac{2\pi i}{n}k} \qquad e^{\frac{2\pi i}{n}} = w$$



$$|w^k - 1|$$

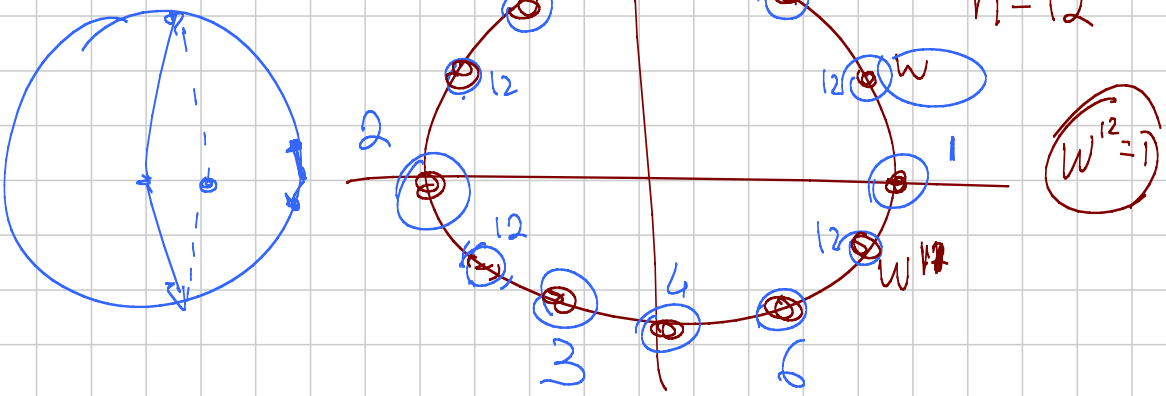
$$\prod_{k=1}^{n-1} |w^k - 1| = \left|\prod_{k=1}^{n-1} (w^k - 1)\right| = n$$

Chi è $\prod_{k=1}^{n-1}(X-w^k)$? è $\dfrac{(X^n-1)}{X-1} = 1+X+X^2+\dots+X^{n-1}$

Chi è $\prod_{k=1}^{n-1}(1-w^k)$? è $1+1+\dots+1 = n$

$$\prod_{k=1}^{n-1} 2\cos\frac{2\pi k}{n} = n$$

Ciclotomici



$a5 + b12 = 1 \Rightarrow 1 = (w^5)^a \cdot (w^{12})^b = w^{5a+12b} = w$

$$X^{12}-1 = (X^4)^3 - 1 = (X^4-1)(X^8+X^4+1)$$
$$= (X-1)(1+X+X^2+\dots+X^{11})$$
$$= (X^6-1)(X^6+1)$$
$$(X-1)(X^5+X^4+\dots)$$

$\Phi_1(x) = (x-1)$ ← radice con periodo 1 $w^0 = 1$

$\Phi_2(x) = (x+1)$ ← radice con periodo 2, $w^6 = -1$

$\Phi_4(x) = (x+i)(x-i) = x^2+1$ ← radici con periodo 4 $w^3 = i$, $w^4 = -1$

x^2+x+1 — 3, 6, 12

$\Phi_{12}(x) = (x-w)(x-w^5)(x-w^7)(x-w^{11})$

Formalmente,

$$\Phi_n(x) := \prod_{\substack{w \text{ radice} \\ n\text{-esima primitiva} \\ \text{di } 1}} (x-w) = \prod_{\substack{(k,n)=1 \\ k=1,2,\dots n}} \left(x - e^{\frac{2\pi i}{n}\cdot k}\right)$$

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

$$(x^6-1) = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$$

$$\Phi_1(x)\ \Phi_2(x)\ \Phi_3(x)\ \Phi_6(x)$$

1) i $\Phi(x)$ hanno tutti coeff. interi

Dim: induzione estesa!

Supponiamo che tutti fino a $n-1$ abbiano coeff. interi

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X) = \Phi_1(X)\,\Phi_d(X) \cdots \Phi_{\frac{n}{d}}(X)\,\Phi_n(X)$$

divisore, monico, a coeff. interi per hp. induttiva

$$\Rightarrow \Phi_n(X) = \frac{X^n - 1}{\text{roba (monica)}}$$

$\Phi_1(X) \quad \Phi_2(X)$

$(X-1)\,(X+1)$

$\Phi_4(X)$

$$X^{12} - 1 = (X^6 - 1)(X^6 + 1) = (X^3 - 1)(X^4 + X^2 + 1)(X^2 + 1) \cdot$$

$$\cdot (X^4 - X^2 + 1) = \Phi_{12}(X)$$

$(X^2 + X + 1)(X^2 - X + 1)$

$\Phi_3(X) \quad \Phi_6(X)$

Fatto: sono irriducibili sui razionali

$a(X) \cdot b(X) \quad a, b \in \mathbb{Q}[X]$

Fatto falso: i coeff. sono solo $-1, 0, 1$

(se andate alla lezione avanzata vedrete controesempi)

$$\Phi_n(X) = \varphi(n)$$

In particolare, $\boxed{\sum_{d \mid n} \varphi(d) = n}$

Pol. ciclotomici si possono usare per dimostrare che $\exists$ infiniti primi t.c. $p \equiv 1 \ (n)$ per ogni n

---

n fisso

Fatto 1) esistono ∞ primi t.c.

$p \mid \Phi_n(a)$ per qualche a intero

$p_1 \cdot p_2 \cdot p_3 \cdots p_u = b$

$\Phi_n(b) = b^n + \cdots \pm 1 \equiv 1 \ (p_i)$

assurdo

In generale, $\forall$ polinomio a coeff. interi, esistono ∞ primi che dividono $f(a)$ per qualche $a \in \mathbb{N}$

---

2) $p \mid \Phi_n(a) \Rightarrow p \equiv 1 \ (n)$

$p \nmid n$ voglio dire che $p \nmid a^d - 1$ per ogni $d \mid n$

Se $p \mid a^d - 1$, $a^d \equiv 1 \mod p$

$p \mid \Phi_n(a) \mid \frac{a^n - 1}{a^{n/d} - 1} = 1 + a^d + \cdots + a^{n - n/d} \equiv \frac{n}{d}$ assurdo!

Ora, $p \mid a^n - 1$ $\quad p \nmid a^d - 1$ $\forall d \mid n$

$\Rightarrow \operatorname{ord}_p(a) = n \quad n \mid p - 1 \Rightarrow p \equiv 1 \ (n)$

Lemma di Gauss $\mathbb{Z}[X]$

$p(x)$ a coefficienti interi,

$p(x) = a(x)\,b(x) \qquad a(x), b(x) \in \mathbb{Q}[X]$

Allora $p(x) = c(x)\,d(x) \quad c(x), d(x) \in \mathbb{Z}[X]$

$$x^2 - 4 = (x-2)(x+2) = \underbrace{(3x-6)}\cdot\underbrace{\left(\tfrac{1}{3}x + \tfrac{2}{3}\right)}$$

$$(9x^2 - 4) = (3x-2)(3x+2)$$

$x^5 + x^4 + 1$ irriducibile (su $\mathbb{Q}$)

$$(x^2 + ax + 1)(x^3 + bx^2 + cx + 1)$$

$$(x^2 + ax - 1)(x^3 + bx^2 + cx - 1)$$

---

dato $f(x)$ a coeff. interi, definiamo

$\mathrm{mcd}(a_0, a_1, \dots a_n) =: c(f) \qquad f = \sum_{i=0}^{d} a_i x^i$

$c(f \cdot g) = c(f) \cdot c(g)$

$\sum f_i g_{k-i}$

$f = c(f) \cdot f'$

f' → coeff. interi, contenuto 1

$g = c(g) \cdot g'$

$c(f \cdot g) = c\left(c(f)\, c(g)\, f' g'\right) = c(f)\, c(g)\, c(f' g')$

Mi manca da dimostrare che se
$c(f') = c(g') = 1 \Rightarrow c(f'g') = 1$

$p \mid c(f'g') \Leftrightarrow$ ogni coeff. di $f'g'$ è multiplo di p

$f'g' \equiv 0 \mod p$

f', g' non sono il polinomio 0

(idea: coeff. di grado più alto!)

$f' = ax^d + \dots \qquad g' = bx^D + \dots$

$\boxed{a \cdot b}\, x^{d+D}$ □

Dim. Lemma di Gauss:

$$p(x) = f(x)\,g(x) = \frac{a(x)}{m} \cdot \frac{b(x)}{n} \qquad (*)$$

(f, g razionali; $a(x)$: coeff. interi; $b(x)$: coeff. interi; m, n: den. comuni)

$$m \cdot n \cdot p(x) = a(x) \cdot b(x)$$

$$m \cdot n \cdot c(p) = c(a) \cdot c(b)$$

posso supporre 1

$$\Rightarrow m \cdot n = c(a) \cdot c(b)$$

$$(*) \quad p(x) = \frac{a(x)\,b(x)}{mn} = \frac{a(x)}{c(a)} \cdot \frac{b(x)}{c(b)}$$

($\frac{a(x)}{c(a)}$, $\frac{b(x)}{c(b)}$: coeff. interi)

Idea da tenere a mente: proiettare modulo p e cercare un assurdo

---

Criterio di Eisenstein

$f \in \mathbb{Z}[x]$

$$f = 1 \cdot x^d + a_{d-1} \cdot x^{d-1} + \dots + a_2 x^2 + a_1 x + a_0$$

$a_{d-1}, \dots, a_2$: multipli di p; a_1: multiplo di p; a_0: multiplo di p, ma non di p^2

$p \,\|\, a_0$

Allora f irriducibile

Dim: proietta modulo p!

Supponiamo $f(x) = a(x) \cdot b(x)$

$\mod p \to x^d = \bar{a}(x) \cdot \bar{b}(x)$

$\frac{1}{t} x^c \cdot t x^{d-c}$

$a(x) = a_c x^c + a_{c-1} x^{c-1} + \dots + a_1 x + a_0$

$a_c \equiv 0 \pmod p$, $a_{c-1} \equiv 0 \pmod p$, $a_1 \equiv 0 \pmod p$, $a_0 \equiv 0 \pmod p$

$b(x) = b_{d-c} x^{d-c} + b_{d-c-1} x^{d-c-1} + \dots + b_1 x + b_0$

$b_{d-c} \equiv 0 \pmod p$, $b_{d-c-1} \equiv 0 \pmod p$, $b_1 \equiv 0 \pmod p$, $b_0 \equiv 0 \pmod p$

$p_0 = a_0 \cdot b_0$ multiplo di p^2

a_0 multiplo di p, b_0 multiplo di p

assurdo

Es $\Phi_p(x)$ irriducibile per p primo

$\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1 = \frac{x^p - 1}{x - 1}$

trick: cambio di var $y \to \frac{x+1}{x-1}$

$a_d x^d + \dots$

$b_D x^D + \dots$

$a_d b_D x^{d+D} + \dots$

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

$a^3+b^3+c^3-3abc = (a+b+c)(\text{roba})$

$\text{roba} = A\cdot(a^2+b^2+c^2) + B\cdot(ab+bc+ca)$

$A = 1$ $\quad B = -1$

Polinomi di Chebyshev

$\cos(x) = \cos(x)$

$\cos(2x) = 2\cos^2(x)-1$

$\cos(3x) = \cos(2x+x) = \cos 2x\cdot\cos x - \sin 2x \sin x =$

$\sin 2x \sin x = 2\sin x\cos x\cdot\sin x = 2\cos x(1-\cos^2 x) =$

$= (2\cos^2 x - 1)\cos x - 2\cos x(1-\cos^2 x) =$

$= 2\cos^3 x - \cos x - 2\cos x + 2\cos^3 x =$

$= 4\cos^3 x - 3\cos x$

$\cos(nx)$ è un polinomio in $\cos x$

$\cos(nx) = T_n(\cos(x))$ per un opportuno T_n

$T_0(x) = 1$

$T_1(x) = x$

$T_2(x) = 2x^2 - 1$

$T_3(x) = 4x^3 - 3x$

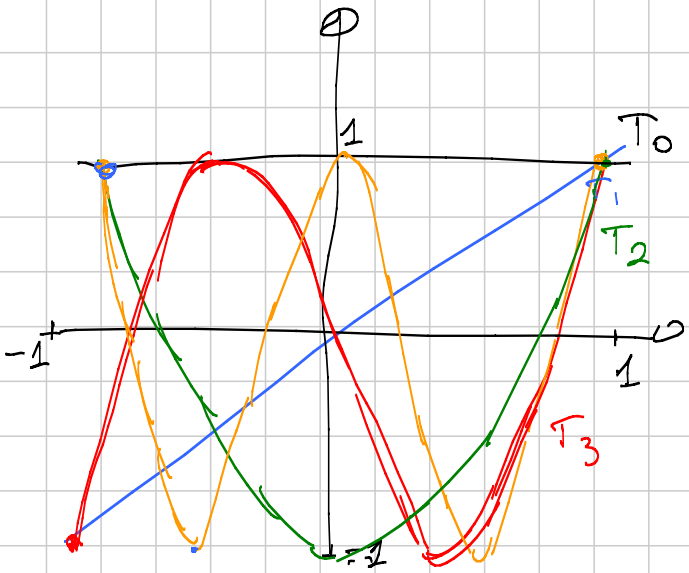
In gen $T_{n+1} = 2x\,T_n(x) - T_{n-1}(x)$

$\cos((n+1)x) = 2\cos x \cos nx - \cos((n-1)x)$

(Werner)

$\cos((n+1)x) + \cos((n-1)x) = 2\cos x \cos nx$

$\cos x$: semi di differenza; nx: semi somma



$T_n(x) = \cos n \cdot (\cos^{-1} x)$

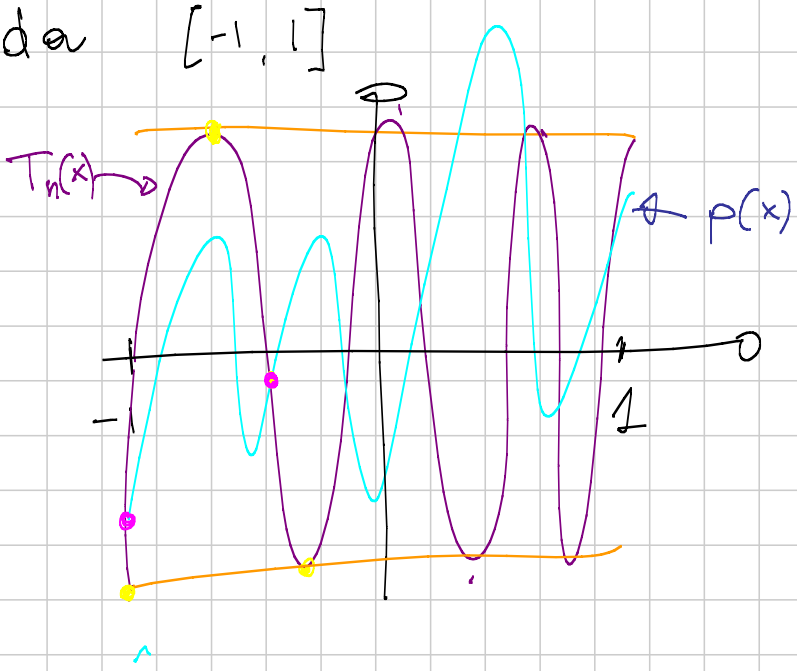
Quando $\cos n\vartheta = \begin{cases} 1 \\ -1 \end{cases}$?

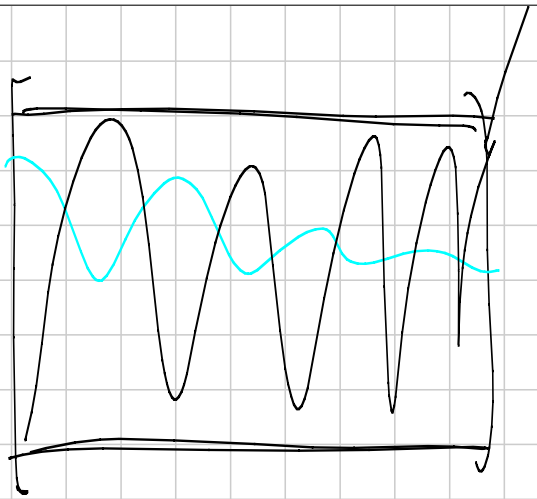
$n\vartheta = k \cdot \pi \qquad \vartheta = \frac{k}{n}\pi$

$\cos^{-1} x$ varia fra 0 e π quando x varia fra -1 e 1

$\cos^{-1}\left(\frac{k}{n}\pi\right)$

Thm: ogni altro polinomio di grado n con coeff. dom. 2^{n-1} "cosca fuori" da $[-1, 1]$





DISUGUAGLIANZE

Titolo nota 05/09/2013

$$\left(\sum a_i b_i\right)^2 \leq \left(\sum a_i^2\right)\left(\sum b_i^2\right)$$

Proof:

1) $a_i a_j b_i b_j$ $\qquad$ $a_i^2 b_j^2$

$$\sum_{i,j} (a_i b_j - a_j b_i)^2 \geq 0$$

$$\sum_{i,j} a_i^2 b_j^2 + a_j^2 b_i^2 - 2 a_i b_j a_j b_i \geq 0$$

2) Disomogeneizzare

$f(a,b,c,\dots)$ omogenea

$$f(\lambda a, \lambda b, \lambda c, \dots) = \lambda^g f(a,b,c)$$

$$\sum_c a\sqrt{\frac{b^2+ac}{2}} \qquad g=2$$

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c} \qquad g=-1$$

$$\frac{a}{b}+\frac{b}{c}+\frac{c}{a} \qquad g=0$$

Th $f(a,b,c,\dots) \geq 0$ omogenea di grado d_f

è vera se e solo se è vera per tutte le n-uple che soddisfano un qualche vincolo omogeneo $g(a,b,c) = 1$ (di grado $d_g \neq 0$)

Dim: f $a^3+b^3+c^3 - 3abc \geq 0$ $\quad$ g $a+b+c = 1$

$\Rightarrow$) ovvia

$\Leftarrow$) $a, b, c, \dots \quad g(a,b,c) = K$

$\alpha \quad \beta \quad \gamma$

$g(\lambda a, \lambda b, \lambda c) = \lambda^{d_g} \cdot K = 1$

scelgo λ in modo che

$a+b+c = 1$?

$\frac{a}{a+b+c}, \frac{b}{a+b+c}, \frac{c}{a+b+c}$

$\alpha \quad \beta \quad \gamma$

$0 \leq f(\alpha, \beta, \gamma) = f(\lambda a, \lambda b, \lambda c) = \lambda^{d_f} f(a,b,c)$

se $abc = 1$

$(abc)^{1/3}(a^2+b^2+c^2)+3 \geq 3(ab+bc+ca)(a+b+c)$

abc

più avanti vedremo tecniche per trattare disug. omogenee

Perché non ci sono disug. fatte così?

$$a^3+b^3+c^3 \geq a^2+b^2+c^2 \qquad a=b=c=\frac{1}{N}$$

$$a^3+b^3+c^3 \leq a^2+b^2+c^2 \qquad a=b=c=N$$

$$a^2+1 \geq 2a$$

$$\left(\sum a_i b_i\right)^2 \leq \left(\sum a_i^2\right)\left(\sum b_i^2\right)$$

Disomogeneizzo: $\sum a_i^2 = 1$, $\sum b_i^2 = 1$ (∗)

Devo dim. che $\sum a_i b_i \leq 1$ se vale (∗)

$$\sum_i a_i b_i \leq \sum_i \frac{a_i^2+b_i^2}{2} = \frac{\sum a_i^2 + \sum b_i^2}{2} \overset{*}{=} 1$$

$$\sum_i a_i b_i c_i \leq \left(\sum a_i^3\right)^{1/3} \left(\sum b_i^3\right)^{1/3} \left(\sum c_i^3\right)^{1/3}$$

(each factor $= 1$: disomogeneizzo)

$$\sum a_i b_i c_i \leq \sum \frac{a_i^3+b_i^3+c_i^3}{3}$$

TST 09

$$(a_1 a_2 \cdots a_n + b_1 b_2 \cdots b_n)^n \leq (a_1+b_1)^n (a_2+b_2)^n \cdots (a_n+b_n)^n$$

$$(a_1,b_1) \quad (a_2,b_2) \quad \ldots \quad (a_n,b_n)$$

Hölder: se $\frac{1}{p}+\frac{1}{q}=1$

$$\sum_i a_i b_i \leq \left(\sum_i a_i^p\right)^{1/p}\left(\sum_i b_i^q\right)^{1/q}$$

$$\sum_i a_i b_i \leq$$

$$ab \leq \frac{1}{p}a^p + \frac{1}{q}b^q \qquad \frac{1}{p}+\frac{1}{q}=1$$

$w_1 = \frac{1}{p}$ $w_2 = \frac{1}{q}$ $\quad x = a^{\frac{1}{p}}$, $y = b^{\frac{1}{q}}$

$$\sqrt[w_1+w_2]{x^{w_1} y^{w_2}} \leq \frac{w_1 x + w_2 y}{w_1 + w_2}$$

$\underbrace{x, x, x, x}_{w_1}$ $\quad \underbrace{y, y, y, y, y}_{w_2}$

$$\sum a_i b_i c_i \leq \left(\sum a_i^p\right)^{1/p}\left(\sum b_i^q\right)^{1/q}\left(\sum c_i^r\right)^{1/r}$$

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

---

a_1 a_1 a_2 a_3 a_3 a_3

$\underbrace{b_1}_{w_1}$ $\underbrace{b_1}_{w_1}$ $\underbrace{b_2}_{w_2}$ $\underbrace{b_3}_{w_3}$ b_3 b_3

$$\left(\sum w_i \cdot a_i b_i\right)^2 \leq \left(\sum w_i a_i^2\right)\left(\sum w_i b_i^2\right)$$

Nesbitt a,b,c

$$\sum_{cyc} \frac{a}{b+c} \geq \frac{3}{2}$$

$$\sum_{cyc} \frac{a}{b+c} = \sum_{cyc} \frac{a^2}{ab+ac}$$

$$a_i = \frac{\sqrt{a}}{\sqrt{b+c}} \qquad b_i = \sqrt{b+c}\sqrt{a}$$

$$\left(\sum_{cyc} a\right)^2 \leq \left(\sum_{cyc} \frac{a}{b+c}\right)\left(\sum_{cyc} (b+c)a\right)$$

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

$$a^2+b^2+c^2+2ab+2bc+2ca \geq 3(ab+bc+ca)$$

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

$$\sum a^2 \geq \sum ab$$

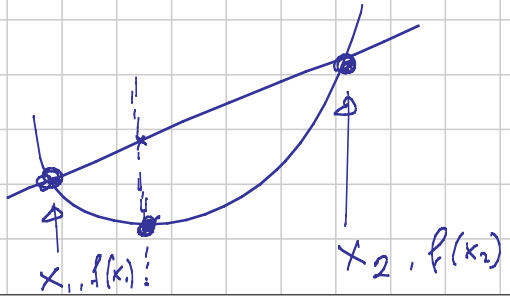
C.S.

$$\sum \frac{a}{b+c} \overset{C.S.}{\geq} \frac{\left(\sum_{cyc} a\right)^2}{\sum_{cyc} (b+c)a} = \frac{\sum_{cyc} a^2 + 2\sum ab}{2\sum_{cyc} ab} \geq \frac{3\sum ab}{2\sum ab}$$

$\geq$ $\geq$ $\leq$

Convessità

Def: f convessa se "tiene l'acqua" "sorride"



$\lambda x_1 + (1-\lambda) x_2 \qquad \lambda \in [0,1]$

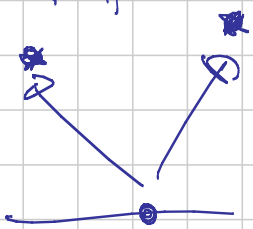
$$f(\lambda x_1 + (1-\lambda) x_2) \leq \lambda f(x_1) + (1-\lambda) f(x_2)$$

$n=14$

$2 \to 4 \to 8 \to 16 \to 15 \to 14$

Jensen $w_1 + w_2 + \dots + w_n = 1$, f convessa
$x_1, x_2, \dots x_n$ nel dominio di f

$$f\left(\sum w_i x_i\right) \leq \sum w_i f(x_i)$$

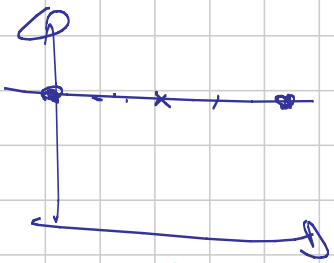


$$m \leq \sum w_i f(x_i) \leq \sum w_i M = M$$

Rmk: f convessa assume massimo sui **bordi**

f convessa su $[-1, 1]$

$$\max f = \begin{cases} f(1) \\ f(-1) \end{cases}$$



(Così hanno di speciale i punti $-1, 1$? Sono gli unici che non si scrivono come $w_1 x_1 + w_2 x_2$ in modo non banale

$$f\left(w_1x_1+\dots+w_nx_n+\quad w_{n+1}x_{n+1}\right)=$$

$\alpha=w_1+w_2+\dots+w_n \qquad \beta=w_{n+1} \qquad \alpha+\beta=1$

$$A=\frac{w_1x_1+\dots+w_nx_n}{\alpha}$$

J2, Jn, pesi $=\frac{w_n}{\alpha}$

$$=f(\alpha A+\beta B)\le\alpha f(A)+\beta f(B)\le$$

$$\le\alpha\cdot\sum_{i\le n} f(x_i)\cdot\frac{w_i}{\alpha}+\beta f(x_{n+1})$$

__Es__: f convessa, a,b,c nel dominio

$$\frac{4}{3}\left(f\left(\frac{a+b}{2}\right)+f\left(\frac{b+c}{2}\right)+f\left(\frac{c+a}{2}\right)\right)\le$$

$$\le f(a)+f(b)+f(c)+f\left(\frac{a+b+c}{3}\right)$$

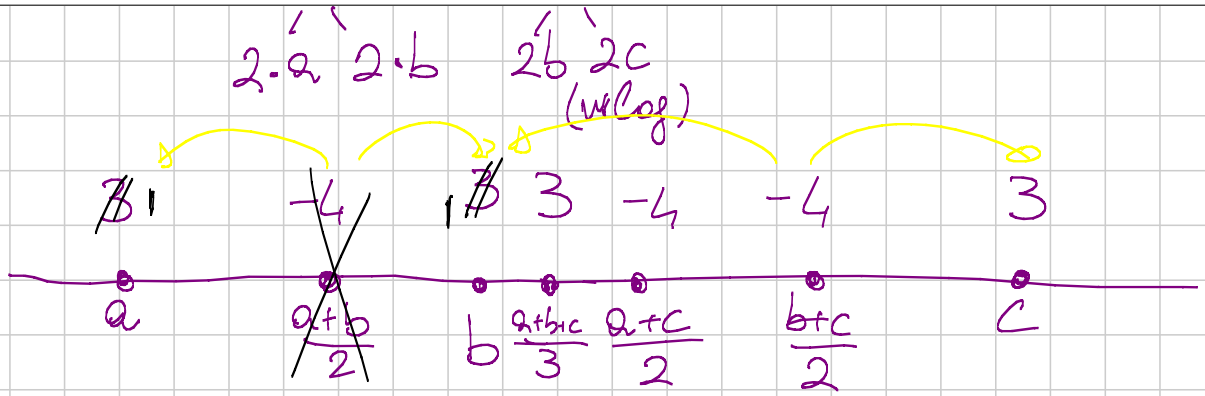
$f(x)=x$

$$4\left(\frac{a+b}{2}+\frac{b+c}{2}+\frac{c+a}{2}\right)=3\left(a+b+c+\frac{a+b+c}{3}\right)$$

$$4f\left(\frac{a+b}{2}\right)\le 4\tfrac{1}{2}f(a)+4\tfrac{1}{2}f(b)$$

$$f\left(\frac{b+c}{2}\right)\le\tfrac{1}{2}f(b)+\tfrac{1}{2}f(c)$$

-4	-4	-4	$+3$	$+3$	$+3$	$+3$
$\frac{a+b}{2}$	$\frac{b+c}{2}$	$\frac{c+a}{2}$	a	b	c	$\frac{a+b+c}{3}$



$$4\,\frac{a+c}{2} = 2a+2c = a + \frac{a+b+c}{3}\cdot\lambda + \left(3-\lambda\right)c$$

$$2a+2c-a-3c = \left(\frac{a+b+c}{3}-c\right)\lambda$$

$$a-c = \left(\frac{a+b-2c}{3}\right)\lambda$$

$$\lambda = 3\,\frac{c-a}{2c-b-a}$$

$$3-\lambda = 3\left(1-\frac{c-a}{2c-b-a}\right) = 3\cdot\frac{c-b}{2c-b-a}$$

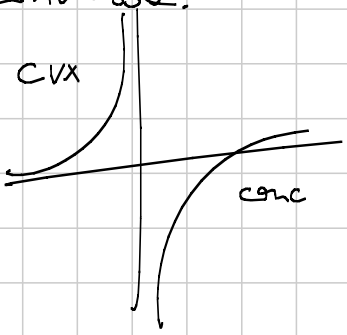
$$4f\left(\frac{a+c}{2}\right) \le f(a) + \frac{3c-a}{2c-b-a}\,f\left(\frac{a+b+c}{3}\right) + 3\,\frac{c-b}{2c-b-a}\,f(c)$$

≤ 3

se ho uso troppi c

Come si riconosce una f. convessa?

$y = x^2$ convessa



$\frac{a+bx}{c+dx}$

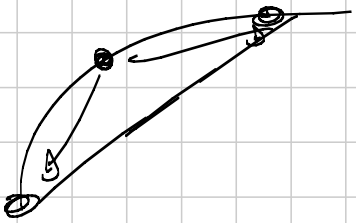
$f(x)+g(x)$ convessa

$f(x) \cdot g(x)$ non sempre!

rette = concave convesse

$f(x)$ concava $-f(x)$ convessa

Es. per $\sqrt{x}$ vale "Jensen al contrario"



Oppure: derivata seconda positiva $\cup$ $\cap$

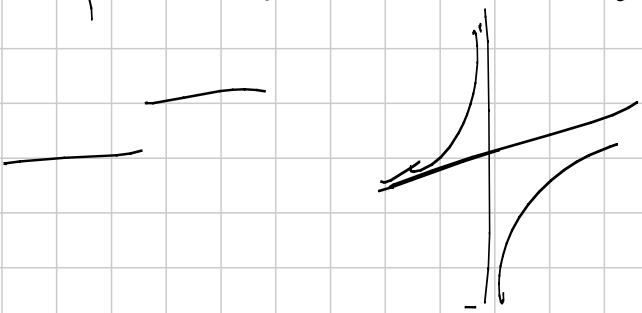
f. continua

"Si disegna senza staccare la penna"

→ polinomi → funzioni razionali

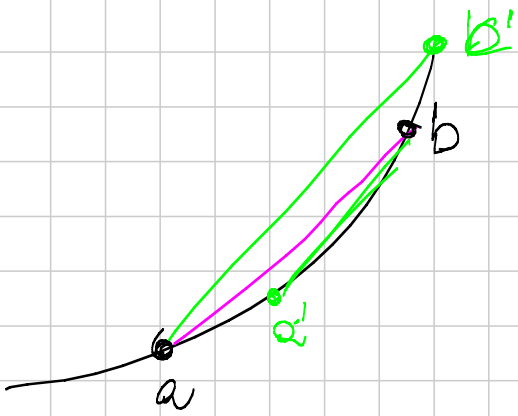
→ somme → prodotti → valori assoluti

→ tutto quello che non annulla denominatori



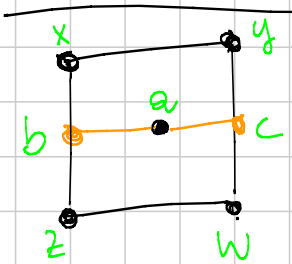
f continua è convessa $\Leftrightarrow$ "midpoint convex"

$$f\left(\frac{x+y}{2}\right) \leq \frac{f(x)+f(y)}{2}$$



$$M(a,b) \quad \frac{f(b)-f(a)}{b-a}$$

f convessa $\Leftrightarrow$ $M(a,b)$ crescente in a, b



$$f(a) \leq \square \cdot f(b) + \square \cdot f(c) \leq$$

$$\leq \square \cdot f(x) + \square \cdot f(z) + \square f(y) + \square f(w)$$

Bunching:

$$\sum_{sym} a^2 b = a^2b + a^2c + b^2a + b^2c + c^2a + c^2b$$

$$\sum_{sym} a^3 = 2a^3 + 2b^3 + 2c^3$$

Def p, q vettori di numeri ordinati in modo decrescente

p maggiorizza q $(p \succ q)$ se

$p_1 \geq q_1$, $p_1 + p_2 \geq q_1 + q_2$ .... fino all'ultimo

dove vale uguaglianza

$$p_1 + p_2 + \dots + p_n = q_1 + q_2 + \dots + q_n$$

Thm (Bunching) Se $p \succ q$, allora

$$\sum_{sym} a^{p_1} b^{p_2} c^{p_3} \dots \geq \sum_{sym} a^{q_1} b^{q_2} c^{q_3} \dots$$

per ogni n-upla $(a, b, c, \dots) \geq 0$

$$\sum_{sym} a^3 \geq \sum_{sym} a^2 b$$

Come altro si dimostra?

Riarrangiamento $\begin{pmatrix} a^2 & b^1 & c^2 \\ b & c & a \end{pmatrix}$

AM-GM PESATA

$$a^2b \leq \frac{2}{3}a^3 + \frac{1}{3}b^3$$

$$\sum_{sym} a^5 b \geq \sum_{sym} a^3 b^2 c$$

$$[5,1,0] \qquad [3,2,1]$$

$$5 \geq 3$$

$$5+1 \geq 3+2$$

$$5+1+0 = 3+2+1$$

A cosa serve? Smonda coi conti disuguaglianze omogenee simmetriche, polinomiali

$$\sum_{cyc} \frac{a}{b+c} \stackrel{?}{\geq} \frac{3}{2}$$

$$2\sum_{cyc} a(a+b)(a+c) \stackrel{?}{\geq} 3(a+b)(b+c)(c+a)$$

$$2\sum_{cyc}\left(a^3 + a^2b + a^2c + 2abc\right) \geq 3\left[2abc + \sum a^2b\right]$$

$$\sum_{sym} a^3 + 2\sum_{sym} a^2b + \sum_{sym} abc \geq \sum_{sym} abc + 3\sum_{sym} a^2b$$

$$7\cdot[3,1,0] + 2\cdot[3,2,1] \stackrel{?}{\geq} 3\cdot[4,2,0] + 6\cdot[2,2,2]$$

$$3\cdot[3,1,0] \geq 3\cdot[4,2,0]$$

$4[5,1,0] \geq 4\cdot[2,2,2]$

$2\cdot[3,2,1] \geq 2[2,2,2]$

Qualche volta non funziona

$$[3,0,0]+[1,1,1] \geq 2[2,1,0]$$

"esponenti concentrati battono esponenti sparpagliati"

Disuguaglianza di Schur:

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

per ogni $a,b,c \geq 0$

vale l'= se sono tutti uguali o ci sono due uguali e il terzo zero

Dim $a \geq b \geq c$

$$a(a-b)(a-c)+b(b-c)(b-a)+c(c-b)(c-a) \overset{?}{\geq} 0$$

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

$(+)$ I $\qquad (-)$ II $\qquad (+)$ III

I + II ≥ 0 $\qquad$ III ≥ 0

$$(a-b)\left[a^2-ac+bc-b^2\right]=(a-b)(a-b)(a+b-c) \geq 0$$

$$\sum_{cyc} a^r (a-b)(a-c) \geq 0$$

se x, y, z sono ordinati nello stesso modo di a, b, c

allora $\sum_{cyc} x(a-b)(a-c) \geq 0$ [Schur-Vornicu]

Schur:

$$0 \leq \sum_{cyc} a(a-b)(a-c) = \sum_{sym} a^3 - a^2 b - a^2 c + abc$$

$$\sum_{sym} a^3 + abc \geq 2 \sum_{sym} a^2 b$$

$$[3,0,0] + [1,1,1] \geq 2[2,1,0]$$

$$[r+2,0,0] + [r,1,1] \geq 2[r+1,1,0]$$

(E) Bundi/Schur: BMO 2012 -2

$$\sum_{cyc} (x+y)\sqrt{(z+y)(z+x)} \geq 4(xy+yz+zx)$$

($x+y$ = c, $z+y$ = a, $z+x$ = b)

Ravi substitution
Se ho disuguaglianza su a, b, c lati di un triangolo
$a \to x+y$ e cicliche
e mi semplifica le condizioni $x \geq 0$, $y \geq 0$, $z \geq 0$

$$\sum_{cyc} c\sqrt{ab} \overset{?}{\geq} 4\sum_{cyc} \frac{(b+c-a)}{2}\frac{(c+a-b)}{2} \qquad (a,b,c\geq 0)$$

$$a \to p^2$$
$$b \to q^2$$
$$c \to r^2$$

$$\sum_{\cancel{cyc}\ sym} r^2pq \overset{?}{\geq} \sum_{\cancel{cyc}\ sym} (p^2+q^2-r^2)(r^2+p^2-q^2)$$

$$2\sum_{sym} r^4 + \sum_{sym} r^2pq + roba \geq \sum_{sym} p^4 + 2\sum_{sym} p^2q^2$$

$$[4,0,0] + [2,1,1] \geq 2\cdot[2,2,0]$$

$$\vee\vee \qquad \geq$$

$$2\cdot[3,1,0]$$

$$\max_{\sigma} \sum a_i a_{\sigma(i)}$$

$$a_i a_{\sigma(i)} + a_j a_{\sigma(j)} < a_i a_{\sigma(j)} + a_j a_{\sigma(i)}$$

se $a_i > a_j$

$a_{\sigma(i)} < a_{\sigma(j)}$

$(a, b, c, \dots)$ A somma fissata $a+b+c+\dots$, quando massimizzo il prodotto?

Supponiamo che ci sia un max e che non sono tutti uguali

wlog $a < b$

li rimpiazzo con $\frac{a+b}{2}, \frac{a+b}{2}$

$$\frac{(a+b)^2}{4} \geq ab$$

Thm: il più grande numero naturale è 1

Supponiamo che sia $a > 1$

$a^2 > a$ assurdo!

"Smoothing": se devo dimostrare che una cosa ha max per $a=b=c=\dots$,
provo ad avvicinarli e vedo cosa succede

"Unsmoothing"

Come si aggiusta la prof. di AM-GM?

$$1,1,5 \to 3,3 \to 2,2,3 \to 2,\tfrac{5}{2},\tfrac{5}{2} \dots \dots \left(\tfrac{7}{3},\tfrac{7}{3},\tfrac{7}{3}\right)$$

A media aritmetica

$(a,b) \not\to \left(\frac{a+b}{2}, \frac{a+b}{2}\right)$ (A, A)

$\to (A, a+b-A)$

$abcd \leq Abcd \leq AAcd \leq \dots \leq (A\cdot A\cdot A\cdot A)^n$

Altro modo di aggiustarlo: dimostrare che $\exists$ massimo!

Weierstress Weierstraß

Funzione continua su un compatto assume un valore massimo M e un minimo m (e assume anche tutti i valori in mezzo almeno una volta, se è connesso)

compatto insieme chiuso + limitato

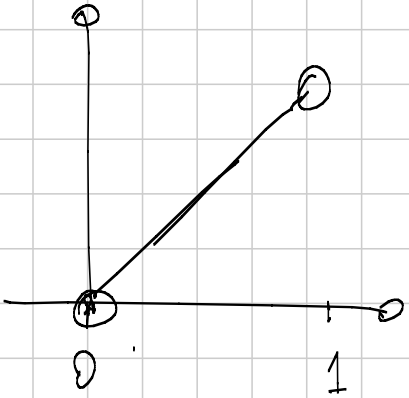
Limitato: le variabili non crescono troppo

$$S: \begin{cases} a+b+c+d=1 \\ a\geq 0 \quad d\geq 0 \\ b\geq 0 \\ c\geq 0 \end{cases} \qquad f(a,b,c,d) = a\cdot b\cdot c\cdot d$$

$abc = 1$

$M^2 \cdot \frac{1}{M} \cdot \frac{1}{M}$

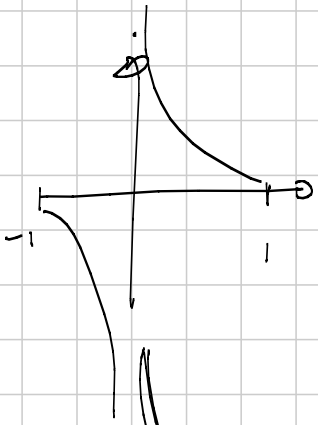
Chiuso: "definito solo con = e ≥ e ≤"



$S = (0, 1)$

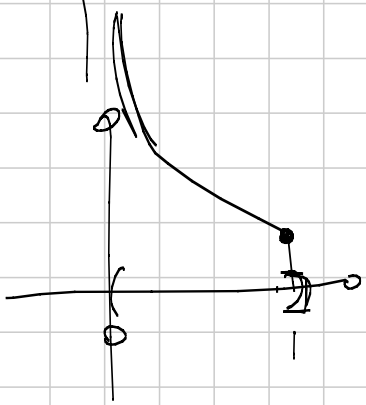
$f(x) = x$

$0 < x \leq 1$



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

$x = [-1, 1]$

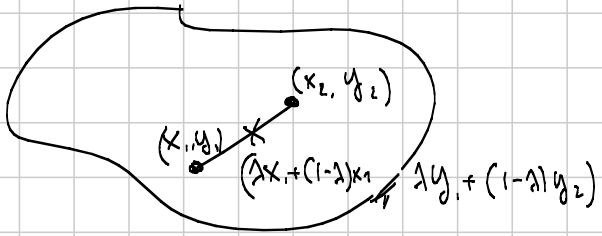


$(0, 1]$ $0 < x \leq 1$

$$C_1 \leq \frac{x_1}{x_2} + \frac{x_2}{x_3} + \frac{x_3}{x_4} + \frac{x_4}{x_5} + \frac{x_5}{x_1} \leq C_2$$

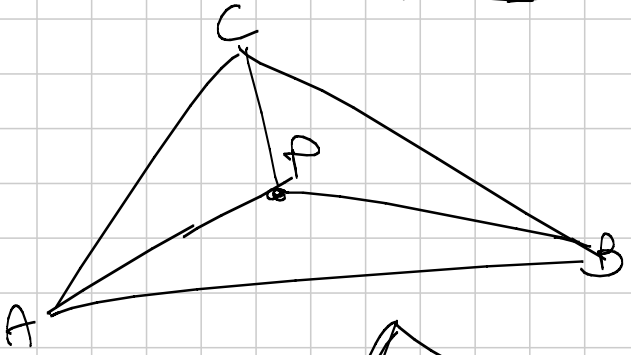
$x_1, x_2, x_3, x_4, x_5 \in \mathbb{R}^+$

$$C_1 \leq \frac{a}{a+b} + \frac{b}{b+c} + \frac{c}{c+a} \leq C_2$$

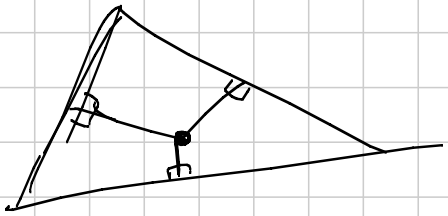


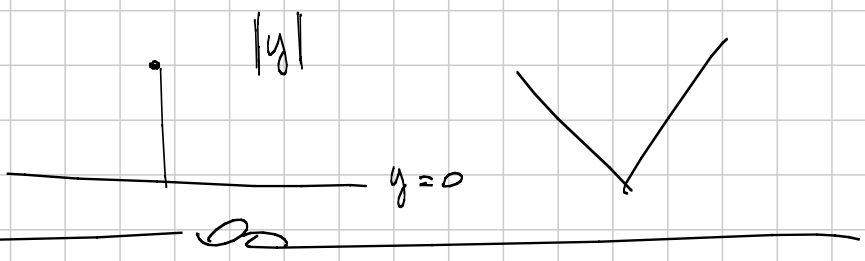
$$\lambda f(x_1, y_1) + (1-\lambda) f(x_2, y_2) \geq f(\lambda x_1 + (1-\lambda)x_2, \lambda y_1 + (1-\lambda) y_2)$$

distanza da un punto è convessa



$PA + PB + PC$





ABC, PQR, PQS

$$\sum_{cyc} a(a-b)(a-c) \geq 0$$

$$\sum_{sym} a^3 - 2a^2b + abc \geq 0$$

$$\begin{cases} S = a+b+c \\ Q = ab+bc+ca \\ P = abc \end{cases}$$

$$\sum a^2 = S^2 - 2Q$$

$$S^3 - 2QS = \sum a^2(a+b+c) = \sum_{cyc} a^3 + \sum_{cyc} a^2b + \sum_{cyc} a^2c =$$

$$= \frac{1}{2}\sum_{sym} a^3 + \sum_{sym} a^2b$$

$$S \cdot Q = \sum_{cyc} ab(a+b+c) = \sum_{cyc} abc + ab^2 + a^2b =$$

$$= \sum_{sym} a^2b + \frac{1}{2}\sum_{sym} abc$$

$$\boxed{\sum_{sym} a^2b = SQ - 3P}$$

$$S^3 - 2QS = a^3 + b^3 + c^3 + SQ - 3P$$

Schur: $\sum_{cyc} a^3 - a^2b - a^2c + abc \geq 0$

$$= S^3 - 2QS - 2\sum_{cyc}(a^2b + a^2c) + 3P \geq 0$$

$$= S^3 - 2QS - 2(QS - 3P) + 3P =$$

$$= \boxed{S^3 - 4SQ + 9P \geq 0}$$

Newton Maclaurin

$$\sqrt[3]{abc} \leq \sqrt{\frac{ab+bc+ca}{3}} \leq \frac{a+b+c}{3}$$

$$\sqrt[4]{abcd} \leq \sqrt[3]{\frac{abc+abd+acd+bcd}{4}} \leq \sqrt{\frac{ab+bc+cd+\dots}{6}} \leq$$

$$\leq \frac{a+b+c+d}{4}$$

$$abc\left(\frac{a+b+c}{3}\right) \leq \left(\frac{ab+bc+ca}{3}\right)^2$$

$$d_k = \frac{\sum(\text{tutti i } k \text{ delle } n \text{ variabili})}{\binom{n}{k}}$$

(controllo segno)

$$\sqrt[k]{d_k} \leq \sqrt[k-1]{d_{k-1}} \qquad d_{k+1}\, d_{k-1} \leq d_k^2$$

$$S^3 - 4SQ + 9P \geq 0$$

Metodo ABC

Th: Fissati S, Q, P di una certa terna a, b, c di reali positivi, esiste una terna di reali positivi (a', b', c') che ha gli stessi S, Q, P maggiore (o minore, a nostra scelta) e vale una di queste condizioni: $\begin{cases} a'=b' \\ c'=0 \end{cases}$ (*)

Perché serve?
Per esempio, per dimostrare Schur!

$$S^3 - 4SQ + 9P \geq 0$$

Supponiamo di aver dimostrato Schur per terne del tipo (*); allora,
(a, b, c)
prendo a', b', c' tali che $S' = S$, $Q' = Q$, $P' \leq P$

allora

$$S^3 - 4SQ + 9P \geq \underbrace{S^3 - 4SQ + 9P'}_{\text{Questo è Schur per } (a', b', c')} \overset{!}{\geq} 0$$

Se so dimostrare Schur per terne (*) allora ho vinto!

Dimostriamolo per terne ⊛:

1) $a=b$

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

$c(c-a)^2$

2) $c=0$

$$a^2(a-b)+b^2(b-a)\geq 0$$

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

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

Questo trucco funziona se la disug. è monotona in P

$$f(S,Q,P)\geq f(S,Q,P')\geq 0$$

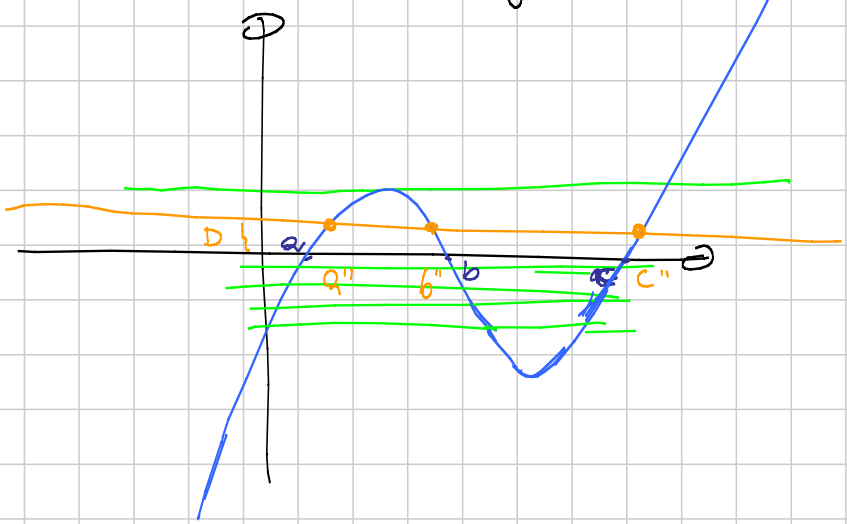
monotonia — caso facile

Dim. teorema PQS

a,b,c sono radici di

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

Com'è fatto il grafico di $p(x)$?



a'', b'', c'' sono radici $p(x) - D =$

$$= x^3 - Sx^2 + Qx - P - D$$

Faccio "salire o scendere la retta" finché non trovo una terna non più valida

Cosa succede nei casi estremi?

- $c = 0$ (una delle due sol. smette di essere positiva)
- $a = b$ (pto di tangenza, se alzo/abbasso ancora non ho più sol. reali)

$f(S, Q, P)$ monotona in P

Se il poly. simmetrico in a, b, c da cui parto ha grado al più 5, allora ha grado in P al più 1 (perché P^2 ha già grado 6)

$\Rightarrow$ Questo trucco funziona sempre se il poly. simmetrico ha grado ≤ 5

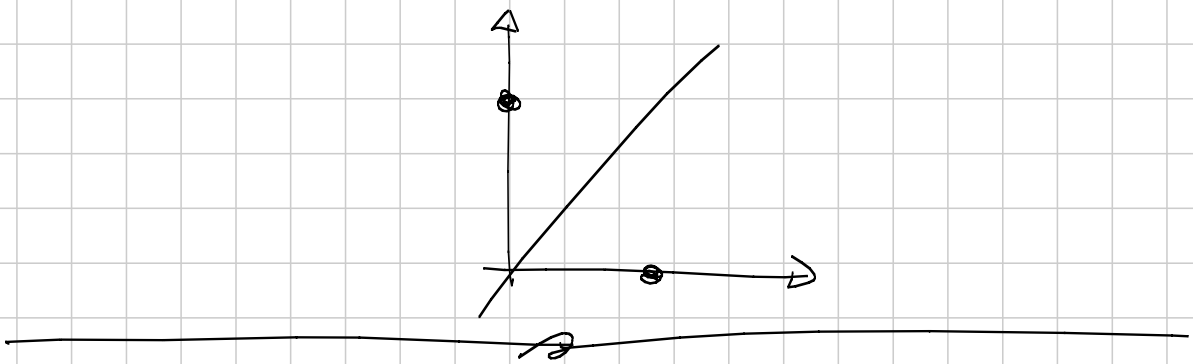
Data disuguaglianza simmetrica polinomiale di grado ≤ 5 in 3 variabili, allora mi basta dimostrarla nei due casi particolari: < due uguali / uno zero

$$\sum p^2 - \cancel{2sp} + 5$$

$$\sum \frac{a}{b+c} \geq \frac{3}{2}$$

Se io ho una disuguaglianza di grado $d \geq 2$ in n variabili, allora per vedere se vale per tutte le n-uple $(a_1, a_2 \dots a_n) \geq 0$, mi basta verificare che vale per tutte le n-uple che hanno al più $\left\lfloor \frac{d}{2} \right\rfloor$ valori positivi distinti

"half-degree principle"



IMO 01-2

$$\sum \frac{a}{\sqrt{a^2+8bc}} \geq 1$$

CS su $\frac{\sqrt{a}}{\sqrt[4]{a^2+8bc}}$, $\sqrt{a}\sqrt[4]{a^2+8bc}$

$$LHS \geq \frac{\left(\sum a\right)^2}{\sum a\sqrt{a^2+8bc}}$$

Mi manca

$$\sum a\sqrt{a^2+8bc} \leq \left(\sum a\right)^2$$

Provo...

$$a\sqrt{a^2+8bc} \leq \frac{a^2+a^2+8bc}{2} \quad (*)$$

$$LHS \geq \text{roba} \geq \text{roba} \geq \text{riba} \geq 1$$

Se uguaglianza, tutti $=$

Ma $(*)$ non soddisfa le stesse...

AM-GM su

$$3a \cdot \sqrt{a^2+8bc} \leq \frac{9a^2+a^2+8bc}{2}$$

"Pol" Point of incidence

$$a\sqrt{a^2+8bc} \le \frac{1}{3}\left(5a^2+4bc\right)$$

$$\sum a\sqrt{a^2+8bc} \le (a+b+c)^2$$

x_i y_i

$$\sum a\sqrt{a^2+8bc} \le \left(\sum a^2\right)^{1/2}\left(\sum a^2+8bc\right)^{1/2} \overset{\text{HOPE}}{\le} (a+b+c)^2$$

$$\left(\sum_{\text{sym}} a^2\right)\left(\sum_{\text{sym}} a^2+8bc\right) \overset{\text{HOPE}}{\le} (a+b+c)^4$$

$1\cdot(a^4+b^4+c^4)$ ✓ $\qquad 1\cdot(a^4+b^4+c^4)$

$8\sum_{\text{sym}} a^3b \qquad 4a^3b$

CS

$$\sum \sqrt{a}\sqrt{a^3+8abc}$$

x_i y_i

Questa volta funziona! =)

Senior 2013. Algebra 3

Titolo nota 06/09/2013

Eq. funzionali

Es. (Cauchy) Trovare tutte le funzioni

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

tali che

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

Sol.

$P(a,b)$: $f(a+b) = f(a) + f(b)$

$P(x,0)$: $f(x+0) = f(x) + f(0) \quad (\forall x \in \mathbb{Z})$

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

$f(0) = 0.$

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

$f(-x) = -f(x)$ (f è dispari)

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

$P(x,x)$: $f(2x) = 2f(x)$

$P(x,1)$: $f(x+1) = f(x) + f(1)$ $(x \in \mathbb{Z})$

Possiamo provare per induzione che $f(x) = xf(1)$

Dim. Passo base $x=0$ ok.

Passo induttivo : $f(n) = nf(1)$

$\rightsquigarrow f(n+1) \overset{?}{=} (n+1)f(1)$ (Hp. ind.)

- con $x=n$ $\rightsquigarrow$ $f(n+1) = f(n)+f(1) = (n+1)f(1)$.

Abbiamo dimostrato che $f(n) = nf(1)$ $\forall n \in \mathbb{N}$

$f(-n) = -f(n) \longrightarrow f(z) = zf(1)$ $\forall z \in \mathbb{Z}$.

Abbiamo trovato che $f(x) = xf(1)$. Chi può essere $f(1)$? Sappiamo che $f(1) \in \mathbb{Z}$ $(f : \mathbb{Z} \to \mathbb{Z})$; va bene qualunque intero.

$f(x) = ax$ $(a \in \mathbb{Z})$

(verifico che funziona) ← SEMPRE.

$f : \mathbb{Q} \longrightarrow \mathbb{Q}$ $\quad f(nx) = nf(x)$ (ind. su n.)

Se $x = \frac{p}{q}$ $\quad pf(1) = f\left(q \cdot \frac{p}{q}\right) = qf\left(\frac{p}{q}\right)$

$f\left(\frac{p}{q}\right) = \frac{p}{q} f(1)$ $\quad \left(f(x) = xf(1) \ \forall x \in \mathbb{Q}\right)$.

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

$\Rightarrow \quad f(x) = ax \quad$ per qualche a. $\left(x \in \mathbb{Z}/\mathbb{Q}\right)$

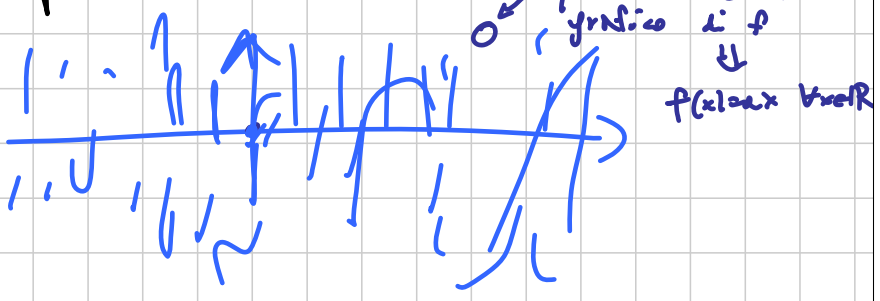
$f : \mathbb{R} \longrightarrow \mathbb{R}$ $\quad \exists a: f(x+y) = f(x)+f(y)$.

posso dire che $f(x) = ax \quad \forall\ x \in \mathbb{R}$?

NO!! Esistono funzioni brutte a piacere che sono "lineari" ma non sono delle rette. (basi di Hamel).

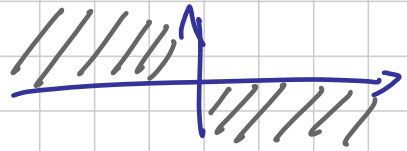
Remark. Appena ho su f una ipotesi di "regolarità" ottengo $f(x) = ax \quad \forall\ x \in \mathbb{R}$.

Es.
- f crescente (o decrescente)
- f limitata in un intervallo
- il grafico di f non contiene una pallina in $\mathbb{R}^2$:



(Es. se f è crescente $\Rightarrow$ $f(x) \le f(0) \ \forall x \le 0$, $f(x) \ge f(0) \ \forall x \ge 0$.

il grafico non può stare qui $\rightarrow$)



Ex. • $f(x^2+y) = f(x)^2 + f(y)$ $\quad f: \mathbb{R} \to \mathbb{R}$. $\quad \forall\, x, y \in \mathbb{R}$

$P(0,0)$ $\quad f(0) = f(0)^2 + f(0) \rightsquigarrow f(0) = 0$

$P(x,0)$ $\quad f(x^2) = f(x)^2$

$\overset{1}{\Rightarrow}$ $f(x^2+y) = f(x^2) + f(y)$

$\overset{2}{\Rightarrow}$ $f(a+y) = f(a) + f(y)$ $\quad (x^2 = a \geq 0,\ y \in \mathbb{R})$

f è crescente : perché?

f è positiva sui positivi $\quad (f(x) = (f(x))^2 \geq 0)$

$f(a-a) = f(a) + f(-a) \rightsquigarrow f(a) = -f(-a)$ (dispari).

$x, y \in \mathbb{R}$

$f(x+y) = f(x) + f(y)$ $\quad$ (se almeno uno tra x e y è ≥ 0) (2)

$x, y \leq 0$

$f(x+y) \overset{f \text{ dispari}}{=} -f((-x)+(-y)) \overset{(2)}{=} -(f(-x) + f(-y)) \overset{f \text{ dispari}}{=} f(x) + f(y)$.

Cauchy con $f(a) \geq 0$ se $a \geq 0$. fine.

Esistono funzioni brutte!!

$f : [0,1] \to [0,1]$

$f(f(x)) = x$

$$\left\{ \begin{array}{l} f(f(\underbrace{f(f(x))}_{\text{"}x\text{"}})) = f(f(x)) = x \\ f^{(2n)}(x) = x \end{array} \right\}$$

$f(x) = x$ funziona

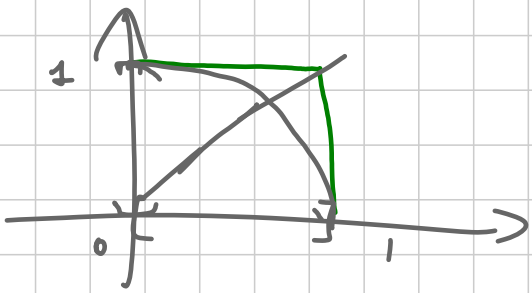
$f(x) = 1 - x$ (funziona)

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

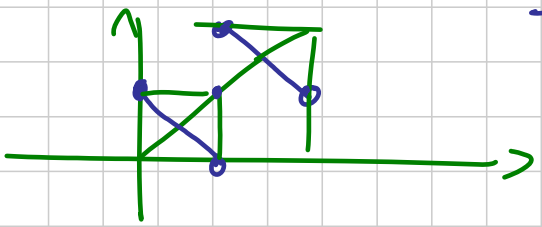
$f(a) = b \iff f(b) = a$

$(a,b) \in \Gamma_f \iff (b,a) \in \Gamma_f$

f risolve $\Leftrightarrow$ Γ_f è simmetrico rispetto a $y = x$



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



$$f(x) = \begin{cases} \frac{1}{2} - x & x < \frac{1}{2} \\ \frac{1}{2} & x = \frac{1}{2} \\ \frac{3}{2} - x & x > \frac{1}{2} \end{cases}$$

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

I012 (B1). $f : \mathbb{Z} \to \mathbb{Z}$

$$f(a)^2 + f(b)^2 + f(c)^2 = 2\left(f(a)f(b) + f(b)f(c) + f(c)f(a)\right)$$

$\forall\, a,b,c$ t.c. $a+b+c = 0$.

$P(0,0,0)$: $\quad 3f(0)^2 = 6f(0)^2 \Rightarrow f(0) = 0$

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

$$(f(a) - f(-a))^2 = 0 \qquad f(a) = f(-a)$$

(f è pari).

$c = a+b$

$$\cdot\ f(a)^2 + f(b)^2 + f(a+b)^2 = 2\left(f(a)f(b) + (f(a)+f(b))f(a+b)\right)$$

($f(a+b) \in \mathbb{Z} \rightsquigarrow \Delta$ eq. quadratica DEVE essere un quadrato)

$$f(a+b) = f(a) + f(b) \pm \sqrt{(f(a)+f(b))^2 - (f(a)-f(b))^2}$$

$$\cdot\ f(a+b)^2 - 2(f(a)+f(b))f(a+b) + (f(a)^2 - 2f(a)f(b) + f(b)^2) = 0$$

$$f(a+b) = f(a) + f(b) \pm 2\sqrt{f(a)f(b)} \qquad \forall\ a,b \in \mathbb{Z}$$

~~$k(a+b)^2 = k^2(a) + k^2(b) \pm 2k(a)k(b)$~~

$f(a)f(b) = \square$ per ogni a,b

$f(a)f(1) = \square \qquad f(a) = \square \cdot k$

$f(1) = n^2 \cdot m$ (m squarefree) $\qquad m = p_1 p_2 \cdots p_j$ (tutti distinti)

$f(a) f(1) = 0 \qquad f(a) \cdot m = 0$ ($p_1 \cdots p_j$)

$m \mid f(a) \qquad f(a) = m \cdot g(a)$

$m^2 g(a) = 0 \rightsquigarrow g(a) = k(a)^2$

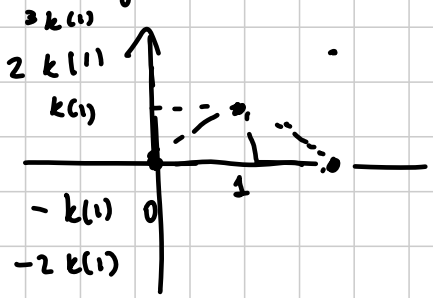
$f(a) = m \cdot k(a)^2$

$k(a+b)^2 = k(a)^2 + k(b)^2 \pm 2k(a)k(b)$

$k(a+b)^2 = (k(a) \pm k(b))^2$ (mi restringo a $k \geq 0$)

fittizio: $\rightsquigarrow$ $\boxed{k(a+b) = \pm k(a) \pm k(b)}$ $\qquad k(n+1) = \pm k(n) \pm k(1)$

ho già dim. che $f(a) = f(-a)$ $\qquad k(1) > 0 \Rightarrow f \equiv 0$



$k(2) < 2k(1)$ $\qquad \pm k(1)$

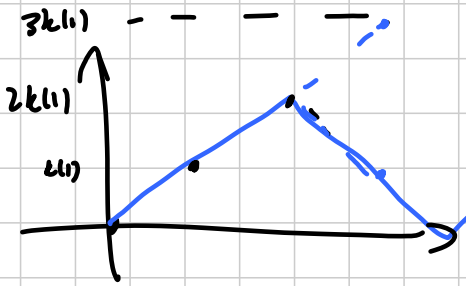
$k(3) =$

$k(4) =$

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

$k(2) = 2k(1)$

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



$k(3) = 3k(1) \to k(n) = nk(1)$

$k(3) = k(1) \to \begin{cases} k(2) = k(1) \\ k(2) = 2k(1) \\ k(3) = k(1) \end{cases} \pmod 4$

3 tipi di soluzioni

- $f(n) = an^2 \qquad a \in \mathbb{Z}$
- $f(n) = \begin{cases} 0 & n \text{ pari} \\ a \in \mathbb{Z} & n \text{ dispari} \end{cases}$
- $f(n) = \begin{cases} 0 & 4 \mid n \\ a & n \text{ dispari} \\ 4a & \text{negli altri casi.} \end{cases}$

Succ. per ricorrenze lineari

$$\begin{cases} x_{n+2} = 3x_{n+1} + x_n \\ x_0 = 0 \\ x_1 = 1 \end{cases} \qquad (*)$$

$$\left(x_{2009} > 2^{2009} \; ? \right)$$

1ª cosa: Se y_n risolve $(*)$ e z_n ris. $(*)$ allora $w_n = \alpha y_n + \beta z_n$ risolve $(*)$.

$$w_{n+2} = \alpha y_{n+2} + \beta z_{n+2} = \alpha(3y_{n+1} + y_n) + \beta(3z_{n+1} + z_n) =$$

$$= 3w_{n+1} + w_n \qquad \text{(linearità)}$$

IP provo a trovare sol. della forma $x_n = \rho^n$

cosa deve essere verificato?

$$\rho^{n+2} = 3\rho^{n+1} + \rho^n$$

↓ divido per ρ^n

$$\rho^2 = 3\rho + 1$$

$$\rho^2 - 3\rho - 1 = 0 \leftarrow \text{(eq. caratteristica della succ. per ricorrenza)}$$

$$\rho_{1,2} = \begin{cases} \frac{3+\sqrt{13}}{2} \\ \frac{3-\sqrt{13}}{2} \end{cases}$$

$y_n = \rho_1^n$ $\quad z_n = \rho_2^n$ risolvono (*); scegliendo opportunamente α e β ho che

$$\alpha\rho_1^n + \beta\rho_2^n = w_n$$

sono TUTTE le possibili soluzioni di (*).

$$\alpha + \beta = 0 \qquad \alpha = -\beta$$

$$\alpha\rho_1 + \beta\rho_2 = 1$$

$\alpha(\rho_1 - \rho_2) = 1$ $\qquad \alpha = \frac{1}{\sqrt{13}}$

$\beta = -\frac{1}{\sqrt{13}}$

$$x_n = \frac{1}{\sqrt{13}}\left(\frac{3+\sqrt{13}}{2}\right)^n - \frac{1}{\sqrt{13}}\left(\frac{3-\sqrt{13}}{2}\right)^n$$

$|t| < 1$

$\frac{3+\sqrt{13}}{2} > 3$ $\qquad x_n \geq \frac{1}{\sqrt{13}} 3^n \geq 2^n \quad (n \geq 10)$.

chi è $\left\lfloor (2+\sqrt{3})^{2013} \right\rfloor$ modulo 5 ?

$(2+\sqrt{3})^{2013} + (2-\sqrt{3})^{2013} = a_{2013}$
(ρ_1, ρ_2)

a_{2013} è intero.

eq. per ρ_1, ρ_2 $\rightarrow$ $x^2 - 4x + 1$

$a_{n+2} = 4a_{n+1} - a_n$

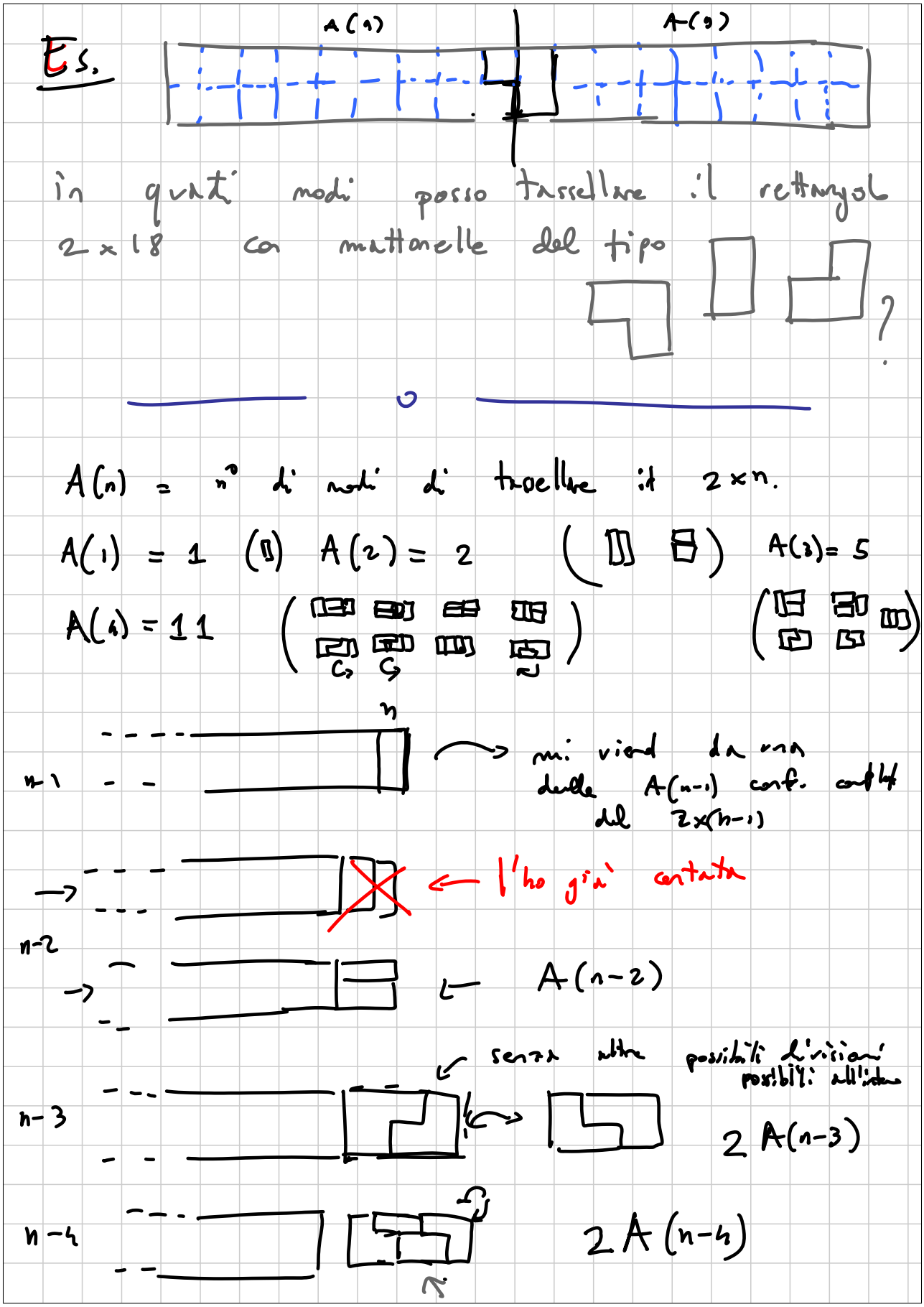
$$\begin{cases} a_{n+2} = -a_{n+1} - a_n \\ a_0 = 2 \\ a_1 = -1 \end{cases}$$

2, −1, −1, 2, −1, −1, 2, ⋮

$\left\lfloor (2+\sqrt{3})^{2013} \right\rfloor \equiv 1 \pmod 5$.

$B(n)^2 + A(n)^2 \rightarrow A(n)^2 + 2B(n)A(n-1) = A(2n)$

$A(1)^2 + \frac{B(9)^2}{2} + A(8)^2 + 2A(8)\cdot B(9) = A(18)$


Es.
A(n)
A(3)
in quanti modi posso tassellare il rettangolo 2 x 18 con mattonelle del tipo ?
A(n) = n° di modi di tassellare il 2 x n.
A(1) = 1
A(2) = 2
A(3) = 5
A(4) = 11
n
n-1
mi viene da una delle A(n-1) conf. con il 2x(n-1)
← l'ho già contata
n-2
A(n-2)
n-3
senza altre possibili divisioni possibili all'interno
2 A(n-3)
n-4
2 A(n-4)

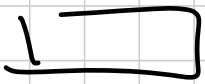
$A(n) = A(n-1) + A(n-2) + 2\left(A(n-3) + \dots + A(1) + 1\right)$

$A(n-1) = A(n-2) + A(n-3) + 2\left(A(n-4) + \dots + A(1) + 1\right)$

$A(n) - A(n-1) = A(n-1) + A(n-3)$

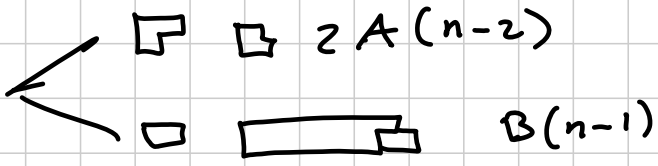
$x_n = 2x_{n-1} + x_{n-3}$ $\qquad \rho^3 - 2\rho^2 - 1 = 0$

$\left(x_n \sim c \cdot \rho^n + \varepsilon_n\right)$

$A(n)$ n° modi  $2 \times n$

$B(n)$ n° modi 

$A(n) =$ 

$B(n) =$ 

$$\begin{cases} A(n) = A(n-1) + A(n-2) + B(n-1) \leftarrow \\ B(n) = 2A(n-2) + B(n-1) \end{cases}$$

stesso int. di $A(n)$

$B(n-1) = A(n) - A(n-1) - A(n-2)$

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

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

$A(n) = \alpha \rho_1^n + \beta \rho_2^n + \gamma \rho_3^n .$

Trovare tutte le $g : \mathbb{N} \to \mathbb{N}$ t.c.

$(g(m)+m)(g(n)+m)$

è un quadrato $\forall\ m,n \in \mathbb{N}$.

$P(n,n)$ $(g(n)+n)^2$ è un quadrato

vero.

$P(0,n)$ $(g(0)+n)\ g(n)$ è un quadrato.

$m = A^2 - g(n)$ $A > g(n)$

$g(A^2 - g(n)) + n$ è un quadrato

$g(n) = n$ funziona $g(n) = n + a$

$(n + a + m)(n + m + a)$ è un quadrato

$g(n) = g(n+1)$?

$((g(n)+n+1)(g(n+1)+n)$ è quadrato.)

$(g(n)+n)^2 < (g(n)+n+1)(g(n)+n) < (g(n)+n+1)^2$

Now può essere

$g(n) = g(n+2)$?

$(g(n)+n+2)(g(n)+n) = (g(n)+n+1)^2 - 1 \neq \square$

$|g(n) - g(n+1)| > 1$ $\quad \nmid \quad g(n) - g(n+1)$

$d = g(n+1) - g(n)$.

$(g(n)+m)(g(m)+n) = \square$

$(g(n)+m+d)(g(m)+n+1) = \square$

prendo m t.c. $p \mid g(n)+m$ $\quad p^{2k+1} \| g(n)+m$

$v_p(g(n)+m) = 2k+1 > v_p(d)$ $\quad$ b)

$p \mid g(m)+n$

$v_p(g(n)+m+d) = v_p(d)$

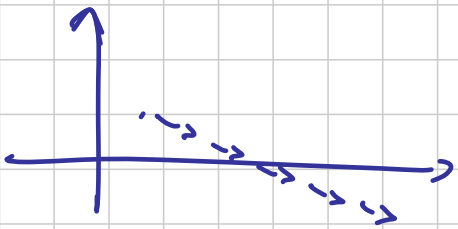
se $v_p(d)$ è dispri ok se $v_p(d)$ è pari: allora $v_p(d) \geq 2$ $\quad k=0$

$v_p(g(n)+m+d) = 1$ ok.

$|g(n) - g(n+1)| \leq 1$

$g(n+1) = g(n) \pm 1$

$g(n+2) = g(n)$



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

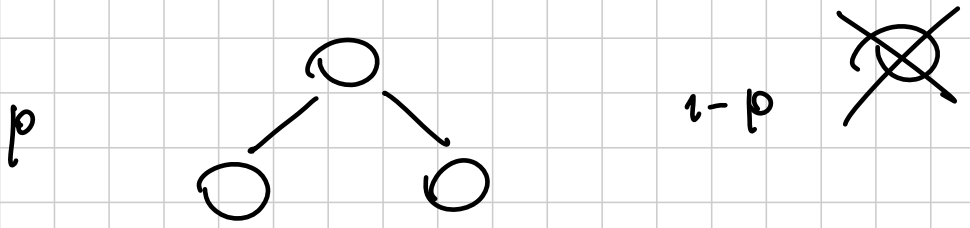
$g(n) = n + a.$

IMO 2010 / 3

C1 MEDIUM

Titolo nota 03/09/2013

PROBLEMA 1 UN BATTERIO



Sia q la prob. che la specie si estingua

$$q = 1 - p + pq^2$$

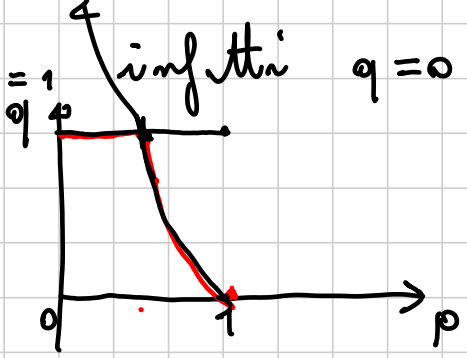
$$pq^2 - q + (1-p) = 0$$

$$q = \begin{cases} 1 \\ \dfrac{1-p}{p} \end{cases}$$

Se $\frac{1-p}{p} \geq 1$ $\left(\text{Se } p \leq \frac{1}{2}\right)$

Se $p > \frac{1}{2}$? $q = \frac{1-p}{p}$

Se $p = 1$ infatti $q = 0$



FUNZIONI GENERATRICI

Data $(a_n)_{n \in \mathbb{N}}$ successione a valori in $\mathbb{R}$ (o in $\mathbb{C}$)

$a_0, a_1, a_2, \ldots$

$$\text{o.g.F.}(a_n) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots$$

$ogF(a_n) + ogF(b_n) = ogf(a_n + b_n)$

$(a_0 + a_1 x + \dots)(b_0 + b_1 x + \dots) =$

$= a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \dots$

$ogf(a_n) \cdot ogf(b_n) = ogF(c_n)$

$c_n = \sum_{i=0}^{n} a_i b_{n-i}$

Per quali $ogf(a_n)$ esiste $ogF(b_n)$ tale che

$$\underbrace{ogf(a_n)}_{A(x)} \cdot \underbrace{ogF(b_n)}_{B(x)} = 1 \quad ?$$

Se $a_0 = 0$

$$c_0 = a_0 b_0 = 0 \neq 1$$

Se $a_0 \neq 0$ allora esiste $B(x)$

Si pone $b_0 = \frac{1}{a_0}$

Vogliamo che per $n \geq 1$ $\sum_{i=0}^{n} a_i b_{n-i} = 0$

$a_0 b_n + \sum_{i=1}^{n} a_i b_{n-i} = 0$

Prendiamo una frazione algebrica $\frac{p(x)}{q(x)}$ con $q(0) \neq 0$

Allora esiste $q(x)^{-1}$ nelle fonz. gener

Associo a $\frac{p(x)}{q(x)}$ la funz. gen. $p(x) \cdot q(x)^{-1}$

Quanto vale $\frac{1}{1-x}$? $\quad 1+x+x^2+\dots$

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

$$1-x+x-x^2+x^2-x^3+\dots$$

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

$$F(x)=\sum_{n=0}^{\infty} F_n x^n = x+x^2+2x^3+3x^4+5x^5+\dots$$

$$xF(x)=\text{ogf}(F_{n-1})$$

$F_{n+2}=F_{n+1}+F_n \qquad \text{ogf}(F_{n+2})=\text{ogf}(F_{n+1})+\text{ogf}(F_n)$

$$\frac{F(x)}{x}+F(x)=\frac{\frac{F(x)}{x}-1}{x}$$

$$xF(x)+x^2F(x)=F(x)-x \qquad F(x)=\frac{x}{1-x-x^2}$$

α_1, α_2 le radici di $1-x-x^2=-(x-\alpha_1)(x-\alpha_2)$

Esistono $c_1, c_2 \quad F(x)=\frac{c_1}{x-\alpha_1}+\frac{c_2}{x-\alpha_2}$

$$c_1+\frac{c_2(x-\alpha_1)}{x-\alpha_2}=(x-\alpha_1)F(x)=\frac{x}{\alpha_2-x}$$

$$F(x)=\frac{c_1/\alpha_1}{\frac{x}{\alpha_1}-1}+\frac{c_2/\alpha_2}{\frac{x}{\alpha_2}-1}=-\frac{c_1}{\alpha_1}\sum_{n=0}^{\infty}\left(\frac{x}{\alpha_1}\right)^n+$$

$$-\frac{c_2}{\alpha_2}\sum_{n=0}^{\infty}\left(\frac{x}{\alpha_2}\right)^n$$

$$F_n=-\frac{c_1}{\alpha_1}\left(\frac{1}{\alpha_1}\right)^n-\frac{c_2}{\alpha_2}\left(\frac{1}{\alpha_2}\right)^n$$

NOTA Se $\deg(p) < \deg(q)$ e sono coprimi

$$\frac{p(x)}{q(x)} = \frac{c_{11}}{x-\alpha_1} + \frac{c_{12}}{(x-\alpha_1)^2} + \dots \frac{c_{1k_1}}{(x-\alpha_1)^{k_1}} + \frac{c_{21}}{x-\alpha_2} + \dots$$

$$q(x) = \prod (x-\alpha_i)^{k_i}$$

BINOMIO DI NEWTON

$$(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i \qquad n \in \mathbb{N}$$

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

Definiamo $\binom{x}{i} = \frac{x(x-1)\cdots(x-i+1)}{i!}$

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

$$\left((1+x)^n\right)^m = (1+x)^{nm}$$

$n, m \in \mathbb{N}$

$$\left(\sum_{i=0}^{\infty} \binom{n}{i} x^i\right)^m = \sum_{i=0}^{\infty} \binom{nm}{i} x^i$$

$r = \frac{a}{m} \in \mathbb{Q}^+$ $\qquad \left(\sum_{i=0}^{\infty} \binom{r}{i} x^i\right)^m \stackrel{?}{=} \sum_{i=0}^{\infty} \binom{rm}{i} x^i$

$$\left(\sum \binom{a/m}{i} x^i\right)^m = \sum \binom{a}{i} x^i = (1+x)^a$$

$$(1+x)^{a/m} = \sum_{i=0}^{\infty} \binom{a/m}{i} x^i$$

$$(1+x)^n \cdot (1+x)^m = (1+x)^{n+m} \qquad \forall n, m \in \mathbb{N}$$

$$\left(\sum_{i=0}^{\infty}\binom{n}{i}x^i\right)(1+x)^m = \sum_{i=0}^{\infty}\binom{n+m}{i}x^i$$

$$(1+x)^{-m} = \sum_{i=0}^{\infty}\binom{-m}{i}x^i$$

PROBLEMA In quanti modi si scrive n come somma di k addendi ordinati ≥ 0 ? $\binom{n+k-1}{k-1}$

Sia a_n tale numero

k fattori

$$(1+x+x^2+\dots)(1+x+x^2+\dots)\cdot\dots\cdot(1+x+x^2+\dots)$$

$$\text{OGF}(a_n) = (1+x+x^2+\dots)^k = \left(\frac{1}{1-x}\right)^k = (1-x)^{-k}$$

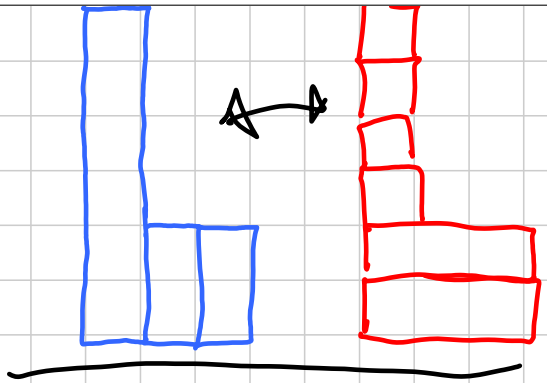
$$= \sum_{i=0}^{\infty}\binom{-k}{i}(-x)^i$$

$$a_n = (-1)^n\binom{-k}{n} = (-1)^n\frac{(-k)(-k-1)(-k-2)\cdot\dots\cdot(-k-n+1)}{n!}$$

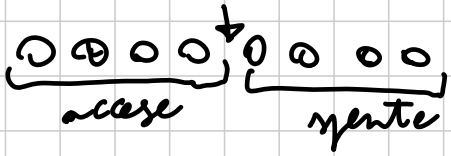
$$= \frac{(n+k-1)(n+k-2)\cdot\dots\cdot k}{n!} = \binom{n+k-1}{n}$$

PROBLEMA Dati $n, k \geq 1$, sia a_{nk} il numero di modi di scrivere n come somma di k addendi ≥ 1 non ordinati. Sia b_{nk} il n° di modi di scrivere n come Σ di alcuni addendi ≥ 1 non ordinati, tra cui il più grande vale k. Dimostrare che $a_{nk} = b_{nk}$

$n = 10 \quad k = 3 \quad 10 = 6+2+2 = 2+6+2$



IMO 2008/5 2n lampade $k \geq n$ mosse
spente $k-n$ pari



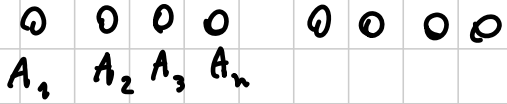
k mosse, ad ogni mossa cambiamo di stato una lampadina

Sia a_{nk} il n° di modi per passare dalla 1ª all'ultima configurazione; sia b_{nk} il n° di modi senza toccare gli ultimi n interruttori
Calcolare a_{nk}/b_{nk}

Prendiamo un modo del primo tipo

Creo una sequenza del 2° tipo: ogni volta che devo toccare una lampadina della 2ª metà, tocco la corrispondente della prima metà.

Dalla sequenza del 2° tipo



$A_i \subseteq \{1, \dots, k\}$ è l'insieme delle mosse in cui ho toccato l'interruttore i

$|A_i|$ è dispari $\sum_{i=1}^{n} |A_i| = k$ $|A_i| = a_i$

Per ogni A_i scelgo un sottoinsieme puro
posso farlo in $2^{a_i - 1}$ modi
In tutto ho $\prod_{i=1}^{n} 2^{a_i - 1} = 2^{k-n}$

$\Omega \neq \emptyset$ insieme finito, insieme di "esiti"

$P : \Omega \to [0,1]$ $\quad \sum_{\omega \in \Omega} P(\omega) = 1$

A "evento"
$A \subseteq \Omega \quad P(A) = \sum_{\omega \in A} P(\omega)$

$F : \Omega \to \mathbb{R}$ è una variabile aleatoria

Definiamo il valore atteso di F

$$E[F] = \sum_{\omega \in \Omega} P(\omega) \cdot F(\omega)$$

$$E[F+g] = \sum_{\omega \in \Omega} P(\omega) \cdot (F+g)(\omega) = \sum_{\omega \in \Omega} P(\omega) F(\omega) + P(\omega) g(\omega)$$
$$= E[F] + E[g]$$

$$E[\lambda \cdot F] = \lambda E[F] \qquad \lambda \in \mathbb{R}$$

F e g sono indip. se $\forall x, y \in \mathbb{R}$

$$P(\{F(\omega) = x\}) \cdot P(\{g(\omega) = y\}) = P\left(\begin{matrix}\{F(\omega)=x \text{ e}\\ g(\omega)=y\end{matrix}\right)$$

Se F, g sono indipendenti, allora
$E[Fg] = E[F] \cdot E[g]$

Sia $A = \mathrm{Im} F$, $B = \mathrm{Im} g$

$$E[Fg] = \sum_{\omega \in \Omega} P(\omega) \cdot F(\omega) g(\omega) = \sum_{(a,b) \in A \times B} a \cdot b \cdot P(\{F(\omega)=a, g(\omega)=b\})$$

$$= \sum_{(a,b)} a \cdot b \, P(\{F(\omega)=a\}) \cdot P(\{g(\omega)=b\}) = \left(\sum_{a \in A} a \cdot P(\{F(\omega)=a\}) \right) \cdot \left(\sum_{b \in B} b \cdot P(\{g(\omega)=b\}) \right) = E[F] \cdot E[g]$$

PROBLEMA n amici che vivono in n città diverse. Per ogni coppia (a,b) di amici c'è un numero $F(a,b) = F(b,a)$ di ore al giorno in cui a e b parlano tra loro al Telefono.

Dim. che si possono dividere in 2 gruppi in modo che più della metà del traffico telefonico sia da un gruppo all'altro.

Disponiamo ogni ragazzo con prob. $\frac{1}{2}$ nel 1° gruppo e con prob $\frac{1}{2}$ nel 2°.

Ω = insieme delle disposizioni dei ragazzi nei gruppi

$$|\Omega| = 2^n$$

$$\forall \omega \in \Omega \quad P(\omega) = \frac{1}{2^n}$$

Scelti $a \neq b$, chiamiamo $g_{a,b}(\omega) = F(a,b)$ se a,b sono in gruppi diversi in ω, 0 altrimenti

$$E[g_{a,b}] = \frac{1}{2} F(a,b)$$

$$E\left[\sum_{1\le a<b\le n} g_{a,b}\right] = \frac{1}{2}\sum_{1\le a<b\le n} F(a,b)$$

Dunque per almeno un ω $\quad \sum g_{a,b}(\omega) \ge \frac{1}{2}\sum_{1\le a<b\le n} F(a,b)$

Dato che $\exists\, \omega$ con $\sum g_{a,b}(\omega) = 0 < \frac{1}{2}\sum F(a,b)$, deve esistere anche un caso con il $>$.

$R(n,n)$ è il più piccolo $k \in \mathbb{N}$ t.c. comunque colorisco di blu o di rosso gli archi di un grafo completo su k vertici, esiste almeno un K_n monocromatico.

$$R(n,n) \le \binom{2n-2}{n-1} \sim \frac{4^{n-1}}{\sqrt{\pi(n-1)}}$$

$$R(n,n) \ge \sim$$

Idea Prendo un grafo completo su k vertici e lo colorisco casualmente di R e B; ogni arco è blu con prob. $\frac{1}{2}$, rosso con prob $\frac{1}{2}$

$\binom{k}{2}$ archi $\Rightarrow 2^{\binom{k}{2}}$

$F(\omega)$ = n° di K_n monocromatici in ω

$V = \{1, \dots, k\}$ $\quad A \subseteq V$ $\quad |A| = n$

Qual è la prob. che A sia monocromatico?

$\frac{1}{2^{\binom{n}{2}-1}}$ $\quad F_A(\omega)$ $\begin{cases} 1 \text{ se } A \text{ è monocr.} \\ 0 \text{ altrimenti} \end{cases}$.

$$E[F_A] = \frac{1}{2^{\binom{n}{2}-1}} \qquad F = \sum_{\substack{A \subseteq \{1,\dots,k\} \\ |A|=n}} F_A$$

$$\cdot E[F] = \frac{1}{2^{\binom{n}{2}-1}} \cdot \binom{k}{n} = \frac{k(k-1)\cdots(k-n+1)}{n! \cdot 2^{\frac{n^2-n}{2}-1}} <$$

$$< \frac{k^n \cdot 2}{\frac{n^n}{e^n}\sqrt{2\pi n}\sqrt{2}^{n^2-n}} < \frac{k^n}{\frac{n^n}{e^n}\sqrt{2}^{n^2-n}} < 1$$

$$k < \frac{n}{e}\sqrt{2}^{n-1}$$

$F : \Omega \to \mathbb{N}$

$$ogf(F) = \sum_{n=0}^{\infty} P(\{F=n\}) \cdot x^n$$

$$ogf(F)(1) = 1$$

$$ogf(F)'(1) = E[F]$$

Se F e g sono indipendenti

$$ogf(F+g) = ogf(F) \cdot ogf(g)$$

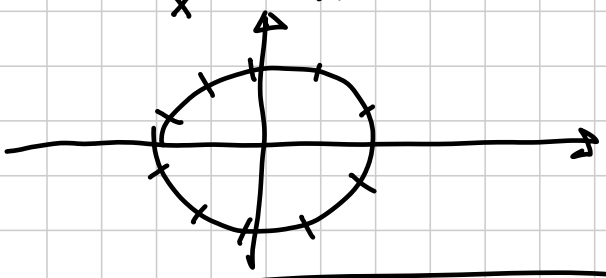
Abbiamo 2 dadi a 6 facce; è possibile truccarli in modo che le 11 somme possibili siano equiprobabili?

D_1, D_2 $\qquad q_1(x) = p_{11}x + p_{12}x^2 + \dots + p_{16}x^6$

$q_2(x) = p_{21}x + \qquad\qquad + p_{26}x^6$

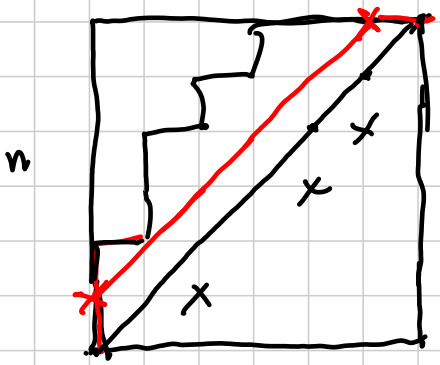
$$q_1(x) \cdot q_2(x) = \frac{1}{11}\left(x^2 + x^3 + \dots + x^{12}\right)$$

$$\frac{q_1(x)}{x} \cdot \frac{q_2(x)}{x} = \frac{1}{11}\left(1 + \dots + x^{10}\right)$$



X CASA ESISTONO 2 DADI A 6 FACCE NON EQUIL. TALI CHE LA SOMMA SI COMPORTI COME QUELLA DI 2 DADI EQUILIBRATI ?

NUMERI DI CATALAN



C_n

$C_0 = 1 \quad C_1 = 1$

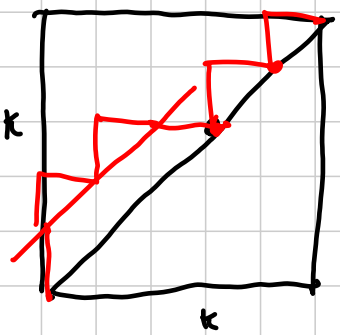
$C_2 = 2$

2 CASI: -NON TORNO MAI SULLA DIAG. SE NON ALLA FINE

C_{n-1} possibilità

-TORNO PER LA 1ª VOLTA SULLA DIAG. DOPO $2k$ PASSI

$C_{k-1} \cdot C_{n-k}$



$$C_n = \left(\sum_{k=1}^{n-1} C_{k-1} \cdot C_{n-k}\right) + C_{n-1} C_0$$

$$C_n = \sum_{k=1}^{n} C_{k-1}\, C_{n-k} \qquad n \geq 1$$

$$C(x) = ogf(C_n) \qquad = \sum_{k=0}^{n-1} C_k \, C_{n-1-k}$$

$$C(x)^2 = ogf\left(\sum_{i=0}^{n} C_i C_{n-i}\right) = ogf(C_{n+1}) =$$

$$= \frac{ogf(C_n) - 1}{x} = \frac{C(x) - 1}{x}$$

$$x\,C(x)^2 - C(x) + 1 = 0$$

$$4x^2 C(x)^2 - 4x C(x) + 4x + 1 - 1 = 0$$

$$(2x\,C(x) - 1)^2 = 1 - 4x$$

$$1 - 2x\,C(x) = \sqrt{1-4x}$$

$$C(x) = \frac{1 - \sqrt{1-4x}}{2x}$$

$$\sqrt{1-4x} = \sum_{i=0}^{\infty} \binom{1/2}{i} (4x)^i$$

$$\binom{1/2}{i} = \frac{\frac{1}{2} \cdot \left(-\frac{1}{2}\right) \cdot \left(-\frac{3}{2}\right) \cdot \ldots \cdot \left(\frac{3-2i}{2}\right)}{i!} =$$

$$= \frac{(2i-3)!! \cdot \frac{1}{2^i} \cdot (-1)^{i-1}}{i!} = \frac{(2i-2)! \cdot \frac{1}{2^i} (-1)^{i-1}}{i! \cdot 2^{i-1} \cdot (i-1)!}$$

$$\frac{(2i-2)!}{i\cdot(i-1)!^2}\cdot\frac{1}{2^{2i-1}}\cdot(-1)^{i-1}$$

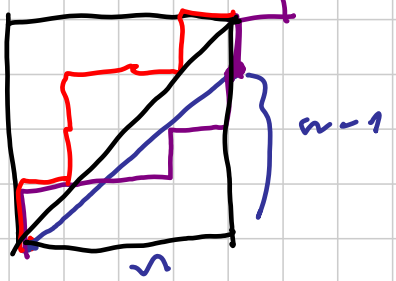
$$\frac{1}{i}\binom{2i-2}{i-1}$$

$$\sqrt{1-4x}=\sum_{i=0}^{\infty}\frac{1}{i}\binom{2i-2}{i-1}\cdot(-2)\cdot x^i$$

$$1-\sqrt{1-4x}=x\cdot\sum_{i=0}^{\infty}2\cdot\frac{1}{i+1}\binom{2i}{i}x^i$$

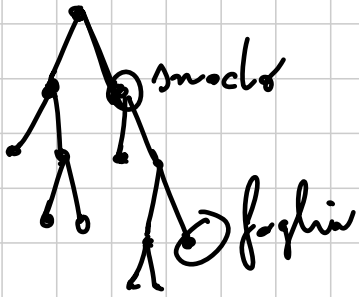
$$C_n=\frac{1}{n+1}\binom{2n}{n}$$

IDEA



C_n = n° di triangolazioni di un $n+2$-agono regolare

C_n = n° di alberi binari con $n+1$ foglie e n nodi



BATTERIO Un albero binario con $n+1$ foglie e n snodi ha prob. $p^n \cdot (1-p)^{n+1}$

$$q = \sum_{n=0}^{\infty} C_n \, p^n (1-p)^{n+1} = (1-p) \cdot \frac{1 - \sqrt{1 - 4p(1-p)}}{2p(1-p)}$$

$$= \frac{1 - \sqrt{(2p-1)^2}}{2p} = \frac{2-2p}{2p} = \frac{1-p}{p}$$

ULTIMA IDEA Qual è la prob. che la colonia si estingua entro la n-esima generazione? q_n

$$q_1 = (1-p) \qquad q_{n+1} = (1-p) + p \cdot q_n^2$$

ESERCIZIO. Se $p > \frac{1}{2}$ q_n è crescente e

$$\lim_{n \to \infty} q_n = \frac{1-p}{p}$$

C2 MEDIUM

Titolo nota 04/09/2013

IMO SL 2005 / C4

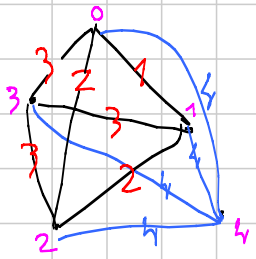
K_n GRAFO COMPLETO SU n VERTICI
$r \geq 1$

VOGLIAMO SCRIVERE SU OGNI ARCO UN NUMERO TRA 1 E r IN MODO CHE

- OGNI NUMERO VIENE USATO ALMENO UNA VOLTA
- IN OGNI TRIANGOLO DUE LATI HANNO LO STESSO NUMERO, PIÙ GRANDE DEL TERZO LATO

QUAL È IL MASSIMO r PER CUI È POSSIBILE?

K_4

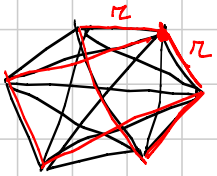


PER $n=4$ $r=3$ VA BENE

$r = n-1$ VA BENE:

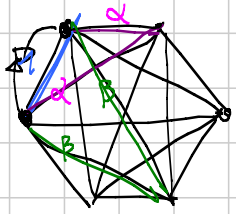
NUMERO I VERTICI DA 0 A $n-1$ E SUL LATO a/b METTO IL NUMERO $\max\{a,b\}$

K_n

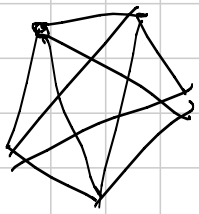


CONSIDERO UN LATO CON IL NUMERO r

$n-1$ ARCHI (ALMENO) SONO SEGNATI CON r:
QUELLO INIZIALE E ALTRI $n-2$ PER OGNI VERTICE



$\longrightarrow K_{n-1}$

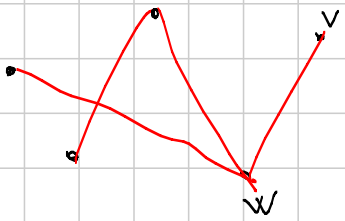


HO r OPPURE $r-1$ ETICHETTE.

SE $r \geq n \Rightarrow r-1 \geq n-1$ ASSURDO (IP. INDUTTIVA)

PER COMPLETARE $n=1$ AL PIÙ 2 COLORI

GRAFI V insieme (finito) di vertici E insieme di archi cioè di coppie di vertici distinte (e non ordinate)

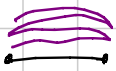


deg (v) = n° di archi che hanno v come estremo

= 1

deg (w) = 3

CAMMINO SEQUENZA $v_1\ e_{1,2}\ v_2\ e_{2,3}\ v_3 \dots v_k$ DI VERTICI E ARCHI T.C. TRA v_i E v_{i+1} C'È L'ARCO $e_{i,i+1}$



CAMMINO SEMPLICE SE v_i SONO TUTTI DISTINTI

CAMMINO CHIUSO CAMMINO IN CUI IL 1° E L'ULTIMO VERTICE COINCIDONO

CICLO CAMMINO CHIUSO "SEMPLICE" (SOLO IL 1° E L'ULTIMO COINCIDONO)

GRAFO CONNESSO DATI DUE VERTICI v E w ESISTE SEMPRE UN CAMMINO DA v A w

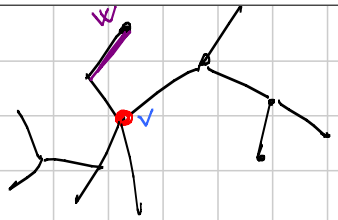
ALBERO GRAFO CONNESSO SENZA CICLI

o EQUIVALENTEMENTE, SUPPONENDO CHE ABBIA n VERTICI

- CONNESSO CON n-1 ARCHI
- ACICLICO SENZA CICLI CON n-1 ARCHI
- ACICLICO MASSIMALE (COMUNQUE AGGIUNGO UN ARCO CREO UN CICLO)
- CONNESSO MINIMALE (COMUNQUE TOLGO UN ARCO SCONNETTO IL GRAFO)

ESERCIZIO IN UN ALBERO DATI v E w ESISTE ESATTAMENTE UN CAMMINO SEMPLICE DA v A w.

V = S + 1



SCELGO UNA RADICE v

AD OGNI w ASSOCIO IL PRIMO ARCO DEL CAMMINO SEMPLICE DA w A v

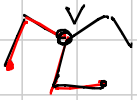
QUESTA È UNA BIGEZIONE

ESERCIZIO ABBIAMO UN ALBERO.

- DIMOSTRARE CHE IL CAMMINO SEMPLICE PIÙ LUNGO CONGIUNGE DUE FOGLIE (DUE VERTICI DI GRADO 1)

SUPPONIAMO CHE TALE LUNGHEZZA MASSIMA SIA PARI, = 2K

PRENDIAMO UN CAMM. SEMPL. LUNGO 2K E SIA v IL VERTICE CENTRALE



- DIMOSTRARE CHE OGNI CAMM. SEMPL. LUNGO 2K PASSA PER v

COSA SI PUÒ DIRE SE LA MAX LUNGHEZZA È DISPARI?

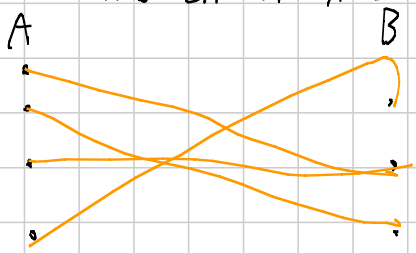
UNA "FOGLIA" È UN VERTICE DI GRADO 1 IN UN GRAFO QUALSIASI. IN UN ALBERO (CON ≥2 VERTICI) CI SONO SEMPRE ALMENO 2 FOGLIE (ESERCIZIO)

CIRCUITO EULERIANO: CAMMINO CHIUSO CHE PASSA ESATTAMENTE UNA VOLTA PER OGNI ARCO

QUANDO ESISTE? QUANDO IL GRAFO È CONNESSO E OGNI VERTICE HA GRADO PARI.

GRAFI BIPARTITI

UN GRAFO SI DICE BIPARTITO SE È POSSIBILE DIVIDERE IN DUE SOTTOINSIEMI A E B IN MODO CHE TUTTI GLI ARCHI VADANO DA A A B.



UN GRAFO ① È BIPARTITO ⟺ OGNI ② CAMMINO CHIUSO HA LUNGHEZZA PARI ⟺ OGNI CICLO HA LUNGHEZZA PARI ③

DIM. ① ⇒ ② E ③

SE UN GRAFO È BIPARTITO, OGNI CAMMINO CHIUSO PASSA ALTERNATIVAMENTE PER A E PER B

② ⇒ ① (SUPPONGO IL GRAFO CONNESSO)

FISSO V E METTO IN A IL VERTICE V E TUTTI I VERTICI CHE SI RAGGIUNGONO DA V CON UN NUMERO PARI DI PASSI, IN B GLI ALTRI

. OGNI VERTICE STA DA ALMENO UNA PARTE (IL GRAFO È CONNESSO)

. W NON PUO' STARE SIA IN A CHE IN B, ALTRIMENTI C'È UN CAMMINO CHIUSO DI LUNGHEZZA DISPARI (DA V A W CON # PARI DI PASSI E POI DA W A V CON # DISPARI DI PASSI)

CI PUO' ESSERE UN ARCO TRA $v_1, v_2 \in A$? NO, ALTRIMENTI v_2 STAREBBE ANCHE IN B (DA V A v_1 CON # PARI DI PASSI, PIÙ $v_1 v_2$)

IDEM PER $v_1 v_2 \in B$

③ ⇒ ② PER ASSURDO C'È ALMENO UN CAMMINO CHIUSO DISPARI. PRENDIAMO ALLORA

$v_1 \; e_{12} \; v_2 - \cdots - v_{2k} \; e_{2k\,2k+1} \; v_{2k+1} \; e_{2k+1} \; v_1$

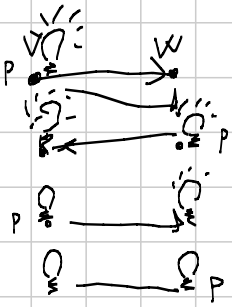
CAMMINO CHIUSO DI LUNGHEZZA MINIMA POSSIBILE

ALLORA È UN CICLO: SE v_i FOSSE UGUALE A v_j $i \neq j$

ALLORA $v_i - \cdots - v_j$ E $v_j - \cdots - v_i$ SAREBBERO CAMMINI CHIUSI PIÙ PICCOLI, DI CUI UNO PARI E L'ALTRO DISPARI

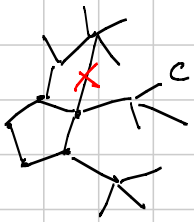
HO UN GRAFO G CONNESSO E UNA LAMPADA SU OGNI VERTICE ALL'INIZIO LE LAMPADE SONO ALCUNE ACCESE E ALCUNE SPENTE. PIERINO CAMMINA LUNGO GLI ARCHI DEL GRAFO E CAMBIA STATO A UNA LAMPADA QUANDO RAGGIUNGE UN VERTICE. PIERINO PARTE DAL VERTICE C E DEVE SPEGNERE TUTTE LE LAMPADE, TORNANDO

IN P. PER QUALI GRAFI PIERINO RIUSCIRÀ NELL'IMPRESA?

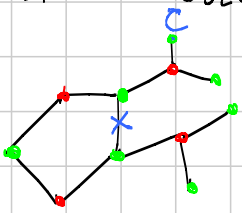


SE IL GRAFO È BIPARTITO, PIERINO NON RIUSCIRÀ SEMPRE NELL'IMPRESA. INFATTI PIERINO PREMERÀ UN N° PARI DI INTERRUTTORI (PER TORNARE IN C), E SE ALL'INIZIO C'È UN NUMERO DI SPARI DI LAMPADE ACCESE NON C'È SPERANZA PER LUI.

SE IL GRAFO NON È BIPARTITO



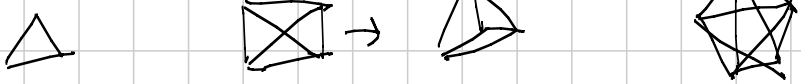
BASTA IL CASO DI UN SOLO CICLO DISPARI



PIERINO PUÒ "AGGIUSTARE" LA PARITÀ DI LAMPADE ACCESE

GRAFO PLANARE

GRAFO CHE SI PUÒ DISEGNARE NEL PIANO SENZA FAR SOVRAPPORRE DUE ARCHI



UN GRAFO PLANARE (DISEGNATO) DIVIDE IL PIANO IN F REGIONI

SE UN GRAFO PLANARE È CONNESSO (E NON VUOTO)

$F + V = S + 2$

F = # di facce, V = # di vertici, S = # di archi, 2

INDUZIONE • VERO SE C'È UN SOLO PUNTO

PASSO INDUTTIVO SE C'È UN CICLO, ELIMINO UN ARCO DEL CICLO: DUE FACCE DISTINTE (PERCHÉ?) VENGONO SALDATE (F CALA DI 1) E S CALA DI 1. IL GRAFO NON SI SCONNETTE

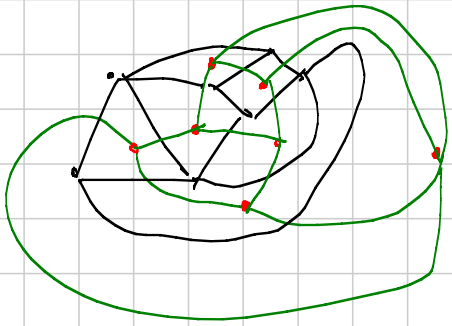
SE HO A CHE FARE CON UN ALBERO ALLORA $F = 1$ $V = n$ $S = n - 1$

IN CASI UMANI (GRANDE) OGNI FACCIA HA ALMENO 3 LATI $3F \leq 2S$

$$S + 2 = F + V \leq \frac{2}{3}S + V \qquad \frac{1}{3}S + 2 \leq V$$

$$3V - 6 \geq S$$

DUALE DI UN GRAFO PLANARE



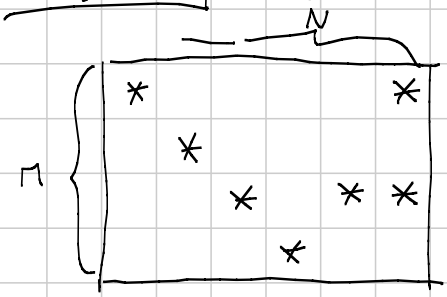
FACCE → VERTICI
ARCHI → ARCHI
VERTICI → FACCE

OCCORRE CHE
- UNA FACCIA NON CONFINI CON SE STESSA
- DUE FACCE NON CONFININO PER PIÙ DI UN ARCO

AD ESEMPIO UN POLIEDRO CONVESSO VA SEMPRE BENE

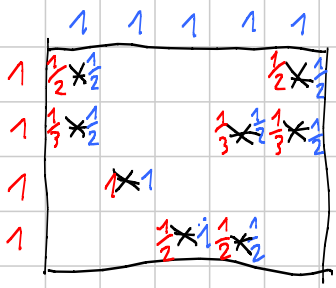
PROBLEMA PER CASA ABBIAMO UN POLIEDRO CONVESSO SONO EQUIVALENTI
- ESISTE UN CIRCUITO EULERIANO
- POSSO COLORARE CON 2 COLORI LE FACCE IN MODO CHE FACCE ADIACENTI ABBIANO COLORI DIVERSI

PROBLEMA TABELLA $M \times N$ SEGNO DEGLI ASTERISCHI IN ALCUNE CASELLE, ALMENO UNO PER OGNI RIGA E COLONNA



SO CHE, SCELTO UN $*$, IL N° DI $*$ SULLA SUA RIGA È $\geq$ DEL N° DI ASTERISCHI SULLA SUA COLONNA

ALLORA $N \geq M$



SE SCELGO UN $*$ IL SUO NUMERO BLU È $\geq$ DEL NUMERO ROSSO

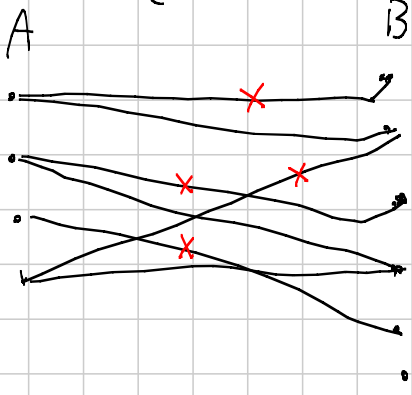
$\sum$ NUMERI BLU $\geq \sum$ NUMERI ROSSI

$\quad\;\; \| \qquad\qquad \|$

$\quad\;\; N \qquad\quad M$

LEMMA DEI MATRIMONI (TEOREMA DI HALL)

ABBIAMO UN INSIEME A DI RAGAZZI E UN INSIEME B DI RAGAZZE (INSIEMI FINITI). AD OGNI RAGAZZO PIACCIONO ALCUNE RAGAZZE. POSSIAMO DARE UNA MOGLIE AD OGNI RAGAZZO FRA LE RAGAZZE CHE GLI PIACCIONO (SENZA DARE LA STESSA MOGLIE A PIÙ RAGAZZI)?



SERVE $|B| \geq |A|$

- SERVE CHE $\forall X \subseteq A \quad |X| \leq |\Gamma(X)|$ OVE $\Gamma(X)$ È L'INSIEME DELLE RAGAZZE CONOSCIUTE DA QUALCUNO IN X

DIMOSTRIAMO CHE LA CONDIZIONE è SUFFICIENTE.
INDUZIONE ESTESA SUL NUMERO DI RAGAZZI

PASSO BASE 1 RAGAZZO

PASSO INDUTTIVO PER IPOTESI SAPPIAMO CHE

$$\forall X \subseteq A \qquad |X| \leq |\Gamma(X)|$$

SI HANNO DUE CASI

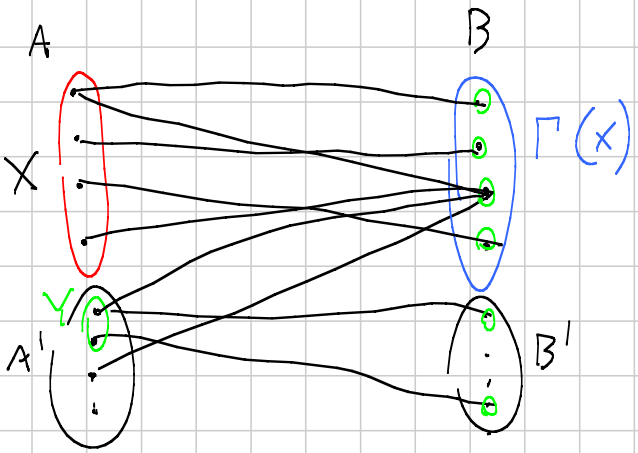
1. $\forall X \subseteq A \quad X \neq \emptyset, X \neq A \qquad |X| < |\Gamma(X)|$
2. $\exists X \subseteq A \quad X \neq \emptyset, X \neq A \qquad |X| = |\Gamma(X)|$

1) SCEGLIAMO UN RAGAZZO Z E FACCIAMOLO SPOSARE CON UNA DELLE ALMENO 2 RAGAZZE CHE CONOSCE.

SIA $X \subseteq A \setminus \{z\}$ $\quad |\Gamma(X) \setminus \{s\}| \geq |\Gamma(X)| - 1 \geq |X|$

DUNQUE AVENDO UN RAGAZZO IN MENO POSSO CONCLUDERE PER IP. INDUTTIVA

2)



Se $Y \subseteq X$ $\quad \Gamma(Y) \subseteq \Gamma(X)$ E $|\Gamma(Y)| \geq |Y|$

Se $Y \subseteq A \setminus X = A'$

IO SO CHE $\quad |Y \cup X| = |Y| + |X| \leq |\Gamma(X \cup Y)| =$

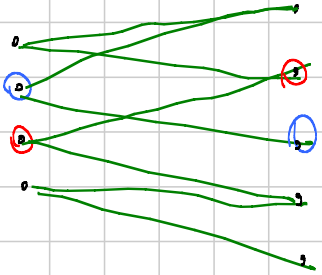
$= |\Gamma(X)| + |\Gamma(X \cup Y) \setminus \Gamma(X)|$

$|Y| \leq |\Gamma(X \cup Y) \setminus \Gamma(X)|$

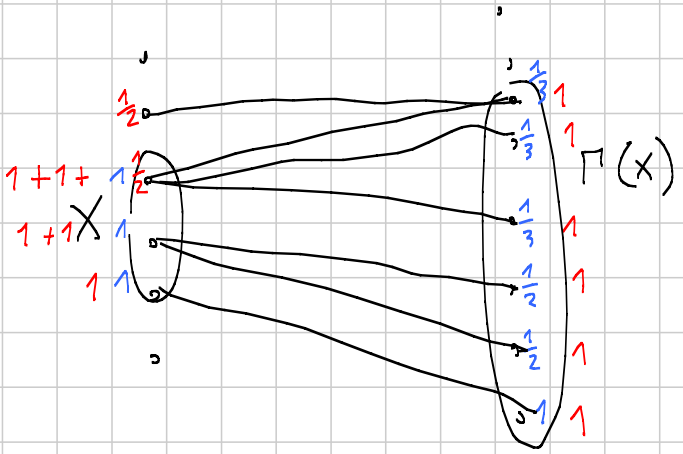
RAGAZZE CONOSCIUTE DA Y FUORI DA $\Gamma(X)$

SUPPONIAMO CHE $\forall z \in \forall S$ CHE SI CONOSCONO

ALLORA $\deg(z) \geq \deg(s)$



ALLORA VALGONO LE IPOTESI DEL LEMMA DEI MATRIMONI



$|X| = \sum_{s \in \Gamma(X)}$ PESO BLU DIS PROVENIENTE DA X $\leq \sum_{z \in X}$ PESI ROSSI DI $z \leq$ ΣPESI DISTRIBUITI DA $\Gamma(X)$ $= |\Gamma(X)|$

CASO PARTICOLARE

OGNI RAGAZZO CONOSCE h RAGAZZE, OGNI RAGAZZA CONOSCE k RAGAZZI CON $h \geq k$

IMO SL 2006 / C6

DIAMANTE

ESISTE UN TASSELLAMENTO IN ◇ SSE ∀ {K

CI SONO AL PIÙ K BUCHI.

▽ RAGAZZI

△ RAGAZZE

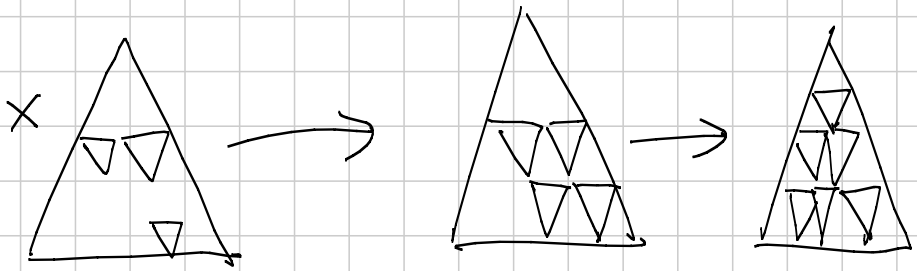
ALL'INTERNO ITA ▽ > △

Sia $X \subseteq \{\nabla\}$

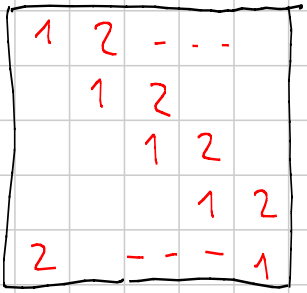
PER ASSURDO

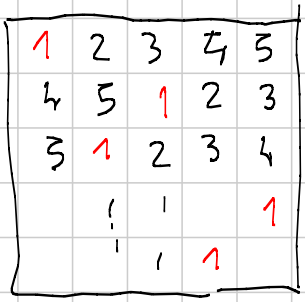
Ora SUPPONIAMO CHE ESISTA $X \subseteq \{\nabla\}$ t.c. $|X| > |\Gamma(X)|$

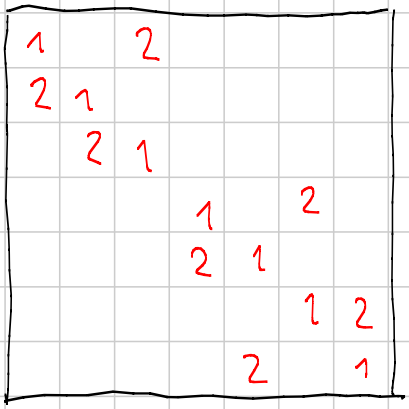
PRENDIAMO IL PIÙ GRANDE X CON QUESTA PROPRIETÀ ($>$ SBAGLIATA)



ALTRO ESEMPIO TABELLA $n \times n$ VOGLIO SCRIVERE I NUMERI DA 1 A n IN MODO CHE OGNI RIGA E OGNI COLONNA CONTENGANO NUMERI DIVERSI







VOGLIAMO FAR SPOSARE RIGHE E COLONNE (METTERE 1 3)

SE HO GIÀ MESSO I NUMERI DA 1 A k
OGNI RIGA CONOSCE $n-k$ COLONNE
OGNI COLONNA // $n-k$ RIGHE

$n-k \geq n-k$

$|S| = n$ $\mathcal{P}(A)$ $S = \{1, \dots, n\}$

$\emptyset$

$\{1\}$ $\{n\}$

$\{1,2\}$ $\{n-1, n\}$

⋮

Prendiamo i sottoinsiemi di cardinalità k e quelli di cardinalità $k+1$.

$A = \{\text{ragazzi}\} = \{\text{sott. di card. } k\}$

$B = \{\text{sott. di card. } k+1\}$

un r conosce S se $r \subseteq S$

Per $k \leq \left\lfloor \frac{n-1}{2} \right\rfloor$ si può

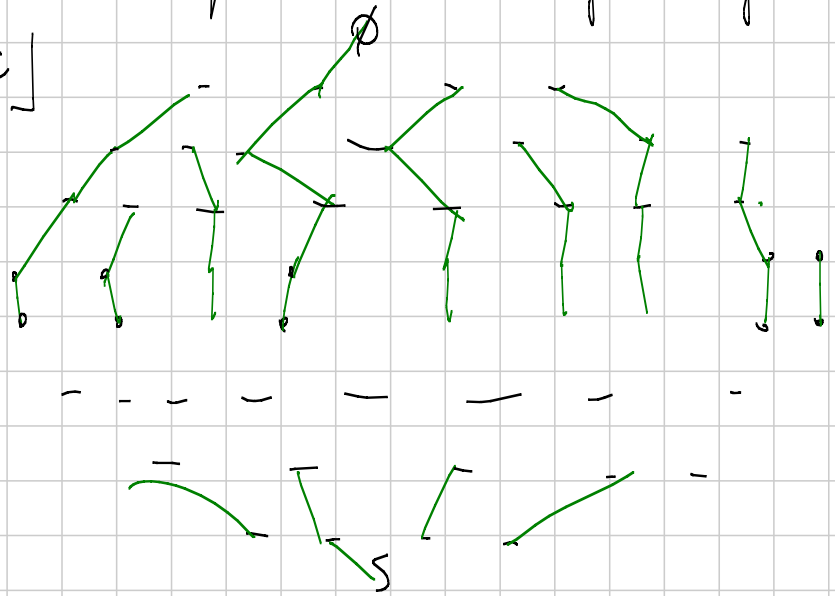
ogni ragazzo conosce $n-k$ ragazzi
ogni ragazza conosce $k+1$ ragazzi

$n-k \geq k+1$ allora si può

altrimenti si può dare ad ogni ragazza un maschio

ESEMPIO

in dimensione



ORDINE PARZIALE

ABBIAMO UN INSIEME S. UN ORDINE PARZIALE SU S È UNA LEGGE CHE DATE ALCUNE COPPIE DI ELEMENTI DISTINTI DI S, DICE QUAL È IL PIÙ GRANDE

$S = \{1, \dots, n\}$ $a \prec b$ lo stesso per $\mathbb{N}, \mathbb{Z}, \mathbb{R} \dots$

$S = \{1, \dots, n\}$ $a \prec b$ se $a \mid b$ e $a \neq b$

CHIEDIAMO CHE SE $a \prec b$, ALLORA $b \not\prec a$

E SE $a \prec b \prec c$ ALLORA $a \prec c$

a E b SONO INCONFRONTABILI SE $a \not\prec b$ E $b \not\prec a$ E $a \neq b$

UN ORDINE È TOTALE SE $\forall a \neq b$ $a \prec b$ OPPURE $b \prec a$

ABBIAMO ALCUNE CITTÀ COLLEGATE DA STRADE A SENSO UNICO

SAPPIAMO CHE $\forall a, b$, È POSSIBILE ANDARE DA a A b O VICEVERSA (O ENTRAMBE)

DIMOSTRARE CHE C'È UNA CITTÀ DA CUI SI RAGGIUNGONO TUTTE LE ALTRE

DICIAMO CHE a E b SONO EQUIVALENTI SE SI PUÒ ANDARE DA a A b E DA b A a. $a \sim b$

ALLORA LE CITTÀ RAGGIUNGIBILI DA a SONO LE STESSE RAGGIUNGIBILI DA b $\quad a \sim a$, $a \sim b \Rightarrow b \sim a$, $a \sim b \sim c \Rightarrow a \sim c$

DICIAMO CHE $a > b$ (CLASSE(a) $\succ$ CLASSE(b)) SE SI PUÒ ANDARE DA a A b MA NON DA b AD a.

SULLE CLASSI $>$ È UN ORDINE PARZIALE

L'IPOTESI DEL PROBLEMA CI DICE CHE L'ORDINE È TOTALE

ALLORA PRENDO LA CLASSE MASSIMA E OGNI CITTÀ CONTENUTA IN ESSA SODDISFA LA RICHIESTA

CATENA SOTTOINSIEME TOTALMENTE ORDINATO

ES. $\mathbb{N}$, $\quad 0$ È IL MASSIMO, 1 È IL MINIMO

$\{2^n\}$ È UNA CATENA

ANTICATENA SOTTOINSIEME TOTALMENTE DISORDINATO

NELL'ESEMPIO DI PRIMA, $\{p \text{ primo}\}$ È UN'ANTICATENA

TEOREMA DI DILWORTH

Sia $(S, \prec)$ un ordine parziale. Sia k la massima cardinalità (CARDINALITÀ) di un'anticatena.

Allora è possibile spezzare S come unione di k catene.

DILWORTH 2

Stessa cosa, ma k è la max cardinalità di una catena e spezziamo S in k anticatene

---

Abbiamo $x_1, \dots, x_{ab+1}$ numeri reali distinti

allora c'è una succ. $\nearrow$ lunga $a+1$ oppure una $\searrow$ lunga $b+1$

Sia $S = \{x_1, \dots, x_n\}$ definiamo un ordine parziale

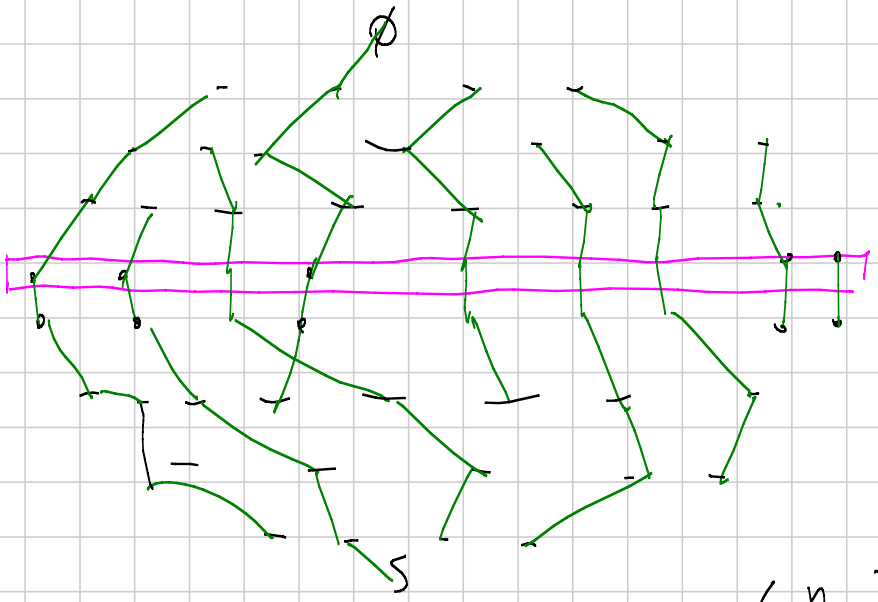
$x_i \prec x_j$ se e solo se $i < j$ $x_i < x_j$

Sia k la più grande dimensione di una anticatena (sottosequenza decrescente).

Se $k \geq b+1$ ok

altrimenti divido S in $\leq b$ catene e quindi ce ne sta una lunga almeno $\left\lceil \frac{ab+1}{b} \right\rceil = a+1$

$|A| = n$ $\mathcal{P}(A)$ è parzialmente ordinato per $\subseteq$



ABBIAMO TROVATO UN'ANTICATENA LUNGA $\binom{n}{\lfloor \frac{n}{2} \rfloor}$

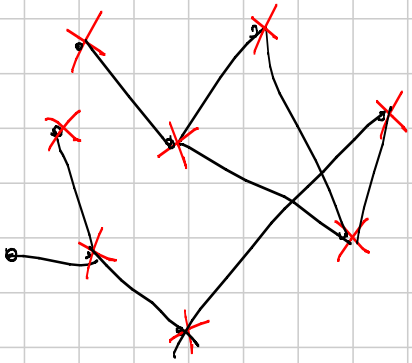
E ABBIAMO DIVISO $\mathcal{P}(A)$ IN $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ CATENE

TEOREMA DI SPERNER

Se $|A| = n$ e $\mathcal{Q} \subseteq \mathcal{P}(A)$ è un'anticatena per $\subseteq$

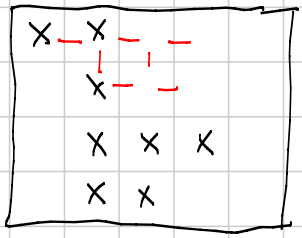
allora $|\mathcal{Q}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$

ALBERTO E BARBARA

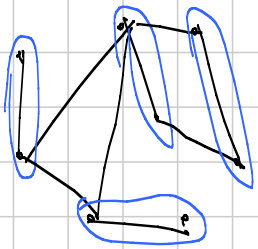


GRAFO CONNESSO G

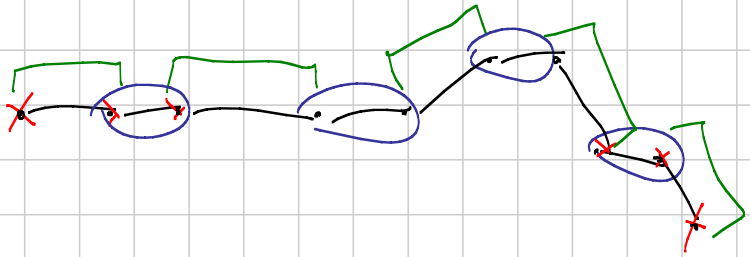
A TURNO SI METTE UNA CROCE SU UN VERTICE ADIACENTE ALL'ULTIMO E NON ANCORA USATO. INIZIA ALBERTO METTENDO DOVE VUOLE LA PRIMA CROCE. PERDE CHI NON PUÒ PIÙ MUOVERE



n intero positivo
Alberto dice un divisore d_1 di n
Barbara dice un altro divisore d_2 t.c. $d_1 \mid d_2$ oppure $d_2 \mid d_1$
e così via, usando solo i divisori di n (ciascuno al più una volta)



Se esiste un accoppiamento vince Barbara, che può sempre rispondere a ogni mossa di Alberto completando la coppia



PROBLEMA Sia un grafo con $|V|$=vertici e $|E|$=lati
UN SOTTOINSIEME STABILE dei vertici è un sottoinsieme in cui nessun vertice è collegato a nessun altro.
IDEA Ordino i vertici a caso $v_1, \dots, v_n$
Comincio a scorrere i vertici a partire dal primo

- Prendo v_1 e lo metto da parte
- Se v_2 non è collegato a v_1 lo metto da parte, altrimenti lo butto via

⋮

- Considero v_i: se è collegato a un vertice già preso lo butto via, altrimenti lo metto da parte

IN MEDIA quanti vertici prendo?

N è il n° di vertici presi N è la somma delle funzioni f_v per $v \in V$ $f_v = \begin{cases} 0 \text{ se ho scartato } v \\ 1 \text{ se l'ho messo da parte} \end{cases}$

$$E[N] = \sum_{v \in V} E[f_v] = \sum_{v \in V} P(\{\text{"}v \text{ viene messo da parte"}\}) \geq$$

$$\geq \sum_{v \in V} \frac{1}{\deg(v)+1} \geq n \cdot \frac{1}{1+\frac{2e}{n}} = \frac{n^2}{n+2e}$$

JENSEN su $\frac{1}{1+x}$

(TEOREMA DI TURÀN)

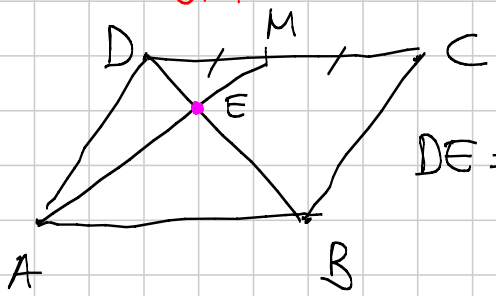
ESERCIZIO Se un grafo su n vertici non contiene K_r completi come sottografi, allora

$$e \leq \left(1 - \frac{1}{r-1}\right) \frac{n^2}{2}$$

GEOMETRIA 1 (medium)

Titolo nota 02/09/2013

VETTORI



parallelogramma :)
pto medio :)

$DE = \frac{1}{3} BD$:)

$$\vec{AE} = a\vec{AM} = \vec{AB} + b\vec{BD}$$

$\vec{AM} = \vec{AD} + \frac{1}{2}\vec{AB}$ (= $\vec{DM}$)

$\vec{BD} = \vec{AD} - \vec{AB}$

$$\Rightarrow \vec{AD}(a-b) = \vec{AB}\left(1-b-\frac{1}{2}a\right)$$

vorrei dire $= 0$: è vero?

Sì, perché A, B, D NON sono allineati.

ottengo $a=b$, $1-\frac{3}{2}b = 0 \to b = a = \frac{2}{3}$

→ abbiamo vinto!

Prodotto scalare

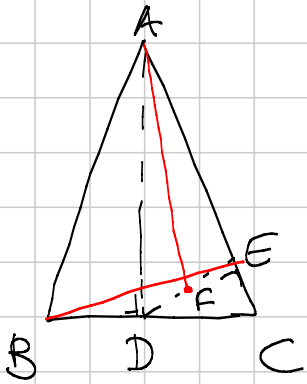
$$\vec{p}\cdot\vec{Q} = |\vec{p}||\vec{Q}|\cos\alpha$$

$$(x_1, y_1)\cdot(x_2, y_2) = x_1x_2 + y_1y_2$$

$\vec{p}\cdot\vec{Q} = 0$ quando sono ortogonali

$\vec{p}\cdot\vec{p} = |\vec{p}|^2$

Es.



$AB = AC$:) $DF = FE$:) proiezioni :) ortogonalità

tesi: $AF \perp BE$

$$\vec{AF}\cdot\vec{BE} = (\vec{AE}+\vec{EF})\cdot(\vec{BD}+\vec{DE}) =$$
$$= \vec{AE}\cdot\vec{BD} - \frac{1}{2}\vec{DE}\cdot\vec{BD} + \vec{AE}\cdot\vec{DE} - \frac{1}{2}\vec{DE}\cdot\vec{DE}$$

$\vec{AE}\cdot\vec{BD}$ ↑ $(\vec{AD}+\vec{DE})\cdot\vec{BD}$ $\vec{DE}\cdot\vec{BD}$

$\vec{AE}\cdot\vec{DE}$ ortogonali

$$= \frac{\vec{DE}}{2}\cdot(\vec{BD}-\vec{DE}) = \frac{\vec{DE}}{2}\cdot(\vec{DC}-\vec{DE})$$

$\vec{BD}-\vec{DE} = \vec{DC}$ ↑ isoscele! $\vec{DC}-\vec{DE} = \vec{EC}$ $= 0$ per hp.

Conti di lunghezze!

incentro ↖ $OI^2 = R^2 - 2rR$ ↑ circocentro

metto il centro in O come si scrive I ?

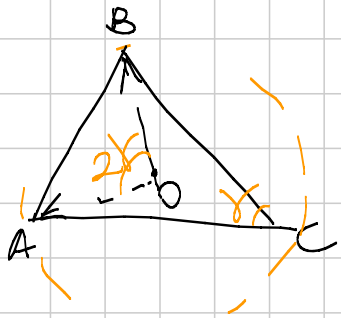
$$\frac{a\vec{A}+b\vec{B}+c\vec{C}}{a+b+c}$$

$$\left|\frac{a\vec{A}+b\vec{B}+c\vec{C}}{a+b+c}\right|^2 = \frac{1}{(2p)^2}\langle a\vec{A}+b\vec{B}+c\vec{C}, a\vec{A}+b\vec{B}+c\vec{C}\rangle =$$

$$= \frac{1}{(2p)^2}\left(a^2 \vec{A}\cdot\vec{A} + b^2 \vec{B}\cdot\vec{B} + c^2 \vec{C}\cdot\vec{C} + 2\sum_{cyc} ab\, \vec{A}\cdot\vec{B}\right) =$$

($\vec{A}\cdot\vec{A} = R^2$, $\vec{B}\cdot\vec{B} = R^2$, $\vec{C}\cdot\vec{C} = R^2$, $\vec{A}\cdot\vec{B} = R^2\cos 2\gamma$)

$\cos 2\gamma = \cos^2\gamma - \sin^2\gamma = 1 - 2\sin^2\gamma$



$$= \frac{1}{(2p)^2}\Big(R^2(a^2+b^2+c^2+2ab+2bc+2ca) - 4R^2(ab\sin^2\gamma + bc\sin^2\alpha + ac\sin^2\beta)\Big) =$$

$$= R^2 - \frac{4R^2}{4p^2}2S(\sin\alpha+\sin\beta+\sin\gamma)$$

$r = \frac{S}{p}$ $\quad 2R\sin\alpha = a$

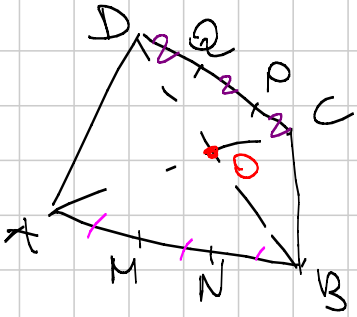
$\rightarrow 2R(\sin\alpha+\sin\beta+\sin\gamma)$

$= 2p$

$$OI^2 = R^2 - Rr\frac{2p}{p} = R(R-2r)$$

→ COROLLARIO $\quad R - 2r \geq 0$

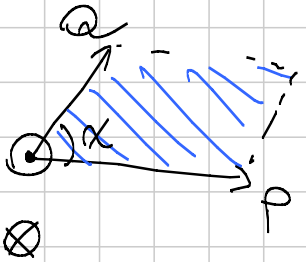
$R \geq 2r$



tesi: Area (MOP) = Area (NOQ)

posso farlo coi vettori?

Aree → :) PRODOTTI VETTORIALI



$\vec{P}, \vec{Q}$

$\vec{P} \times \vec{Q}$, modulo $S = |P||Q| \sin\alpha$

ortog al piano di $\vec{P}, \vec{Q}$ con verso dato dalla regola mano dx.

proprietà: $a \times b = -b \times a$

è 0 se a, b allineati

è prod dei moduli se ortogonali

$(\pm)$

$(a+b) \times c = a \times c + b \times c$

occhio: l'associatività è FALSA!

Risolviamo problema:

$\overrightarrow{OM} \times \overrightarrow{OP} \stackrel{?}{=} -(\overrightarrow{OQ} \times \overrightarrow{ON})$ ← $\frac{1}{3}\vec{A} + \frac{2}{3}\vec{B}$

$\frac{2}{3}\vec{A} + \frac{1}{3}\vec{B}$ $\quad$ $\frac{1}{3}\vec{D} + \frac{2}{3}\vec{C}$ $\quad$ $\frac{2}{3}\vec{D} + \frac{1}{3}\vec{C}$

$\frac{2}{3}\vec{A} \times \frac{1}{3}\vec{D} + \frac{2}{3}\vec{A} \times \frac{2}{3}\vec{C} + \frac{1}{3}\vec{B} \times \frac{1}{3}\vec{D} + \frac{1}{3}\vec{B} \times \frac{2}{3}\vec{C}$

A O C allineati

//

$-\left(\frac{2}{9}\vec{D} \times \vec{A} + \frac{2}{9}\vec{C} \times \vec{B}\right)$

Altro esempio (x es.)

BONUS: è vero per qualunque poligono regolare

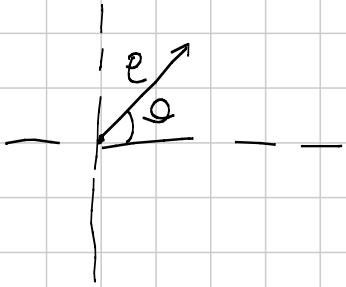
equilatero

"con segno"

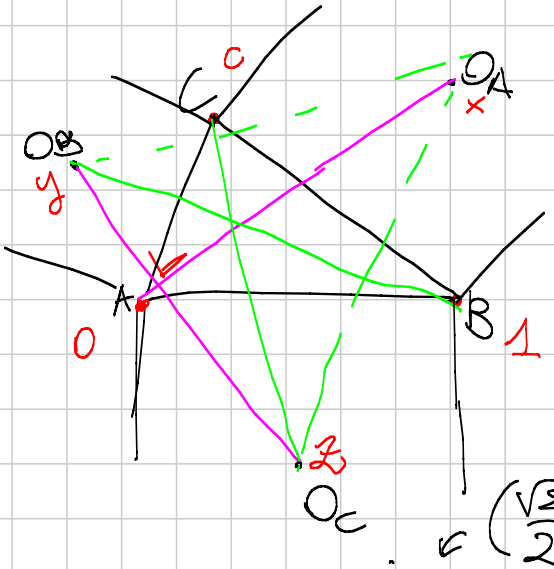
la somma delle distanze di P dai lati NON dipende da P!

COMPLESSI

$x + iy$ $\qquad \rho(\cos\vartheta + i\,\mathrm{sen}\,\vartheta) = \rho e^{i\vartheta}$



Esercizio 1



tesi

AO_A, BO_B, CO_C concorrono;

$AO_A = O_B O_C$

$z = c\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)$

$y = c\frac{\sqrt{2}}{2} e^{i\pi/4}$ $\qquad = c\left(\frac{1}{2} + \frac{i}{2}\right)$

$$z = 1\,\frac{\sqrt{2}}{2}\left(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) = \frac{(1-i)}{2}$$

$$x = (c-1)\frac{\sqrt{2}}{2}\left(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) + 1 =$$

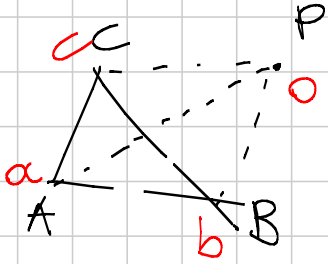
$$= (c-1)\frac{(1-i)}{2} + 1 =$$

$$= \frac{c+1+i(1-c)}{2}$$

$$y - z = \frac{c-1+i(c+1)}{2} = ix$$

$\Rightarrow y - z \perp x \rightarrow$ concorrenza "gratis"

Esercizio 2



tesi

$$\left(\frac{PA}{BC}\right)^2 + \left(\frac{PB}{AC}\right)^2 + \left(\frac{PC}{AB}\right)^2 \geq 1$$

$x \quad y \quad z$

$$x^2 + y^2 + z^2 \geq xy + yz + zx$$

$$\sum_{cyc} \frac{PA \cdot PB}{AC \cdot BC} \geq 1$$

metto il centro in P!

cosa diventa?

$$\sum_{cyc} \frac{|a||b|}{|a-c||c-b|} \quad *$$

$$\sum_{cyc} \frac{ab}{(a-c)(c-b)} = \sum_{cyc} \frac{ab(b-a)}{(a-c)(c-b)(b-a)}$$

$$= \frac{1}{(a-c)(c-b)(b-a)} \sum_{cyc} ab(b-a)$$

$ab^2 - a^2b$

$ab^2 + bc^2 + ca^2$

$-(a^2b + b^2c + c^2a)$

$abc - abc + a^2b + b^2c + c^2a - (ab^2 + bc^2 + ca^2)$

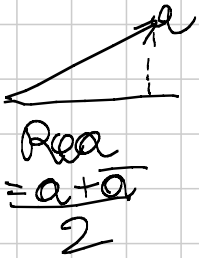
è l'espressione iniziale fa -1 !

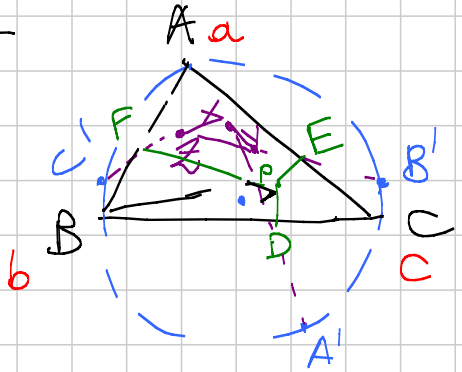
$* \sum_{cyc} | \quad | \geq \left| \sum_{cyc} \ldots \right| = 1$ → tesi!

Esercizio 3 (CHINA TST '11)

ABC O circocentro
A', B', C' simmetrici rispetto a O
pto P, proiezioni D, E, F sui lati di ABC, X, Y, Z simmetrici di A', B', C' risp. a D, E, F.

$XYZ \sim ABC$



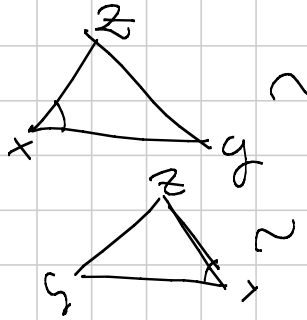


O è in O, $R = 1$

$a\bar{a} = b\bar{b} = c\bar{c} = 1$

PIANO:
calcolarmi x
in f. di a, b, c, p

condizione di somiglianza



$\frac{c-a}{b-a} \stackrel{?}{=} \frac{z-x}{y-x}$

(oppure $\frac{c-a}{b-a} \stackrel{?}{=} \frac{\bar{z}-\bar{x}}{\bar{y}-\bar{x}}$)

calcolo d.

$$d = \left[\frac{\left(\frac{p-b}{c-b}\right) + \overline{\left(\frac{p-b}{c-b}\right)}}{2}\right](c-b) + b =$$

$$2d = p - b + \frac{\bar{p}-\bar{b}}{\bar{c}-\bar{b}}(c-b) + 2b =$$

$$= p + b + \frac{bc}{b-c}(c-b)(\bar{p}-\bar{b}) =$$

$$\frac{bc}{b-c} \cdot \frac{c-b}{\bar{c}-\bar{b}} = -1$$

$$= p + b - bc\bar{p} + c$$

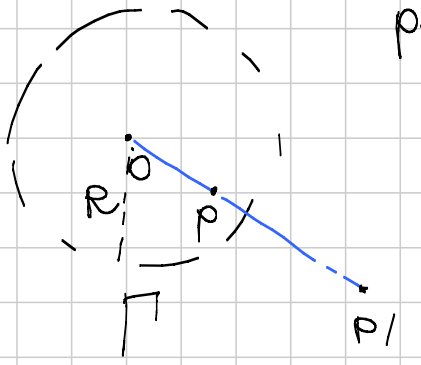
$$x + a' = 2d = p + b + c - bc\bar{p}$$

$$x = p + a + b + c - bc\bar{p} \qquad z = p + a + b + c - ab\bar{p}$$

$$\frac{z-x}{y-x} = \frac{bc\bar{p} - a\bar{b}p}{p(b\bar{c} - a\bar{c})} = \frac{abc(b\bar{c} - a\bar{b})}{abc(b\bar{c} - a\bar{c})}$$

$$\frac{a-c}{a-b} = \frac{c-a}{b-a}$$

INVERSIONE circolare



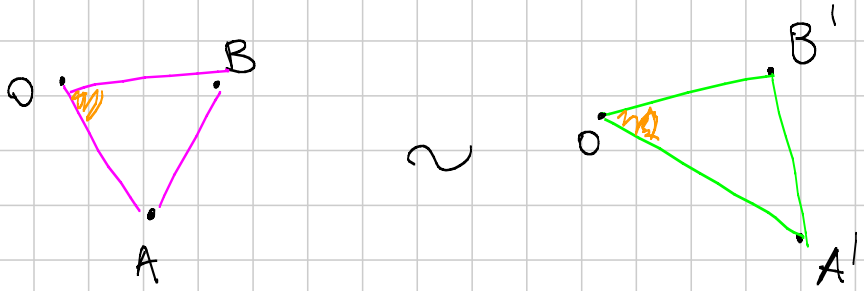
piano $\setminus \{O\} \to$ piano $\setminus \{O\}$

P va in P' sulla semiretta OP

$OP \cdot OP' = R^2$

rette per O → se stesse
circonferenze per O ↔ rette non per O
circonferenze non per O ↔

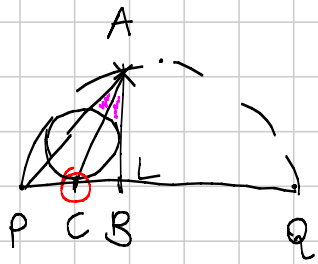
angoli "si mantengono"
(fra rette/circonferenze e loro immagini)



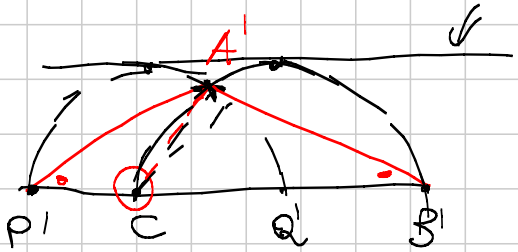
$$\frac{OA'}{OB'} = \frac{R^2}{OA}\frac{OB}{R^2} = \frac{OB}{OA}$$

$$A'B' = AB \cdot \frac{OA'}{OB} = \frac{AB \cdot R^2}{OA \cdot OB}$$

Es. 1



$\widehat{PAC} \cong \widehat{CAB}$



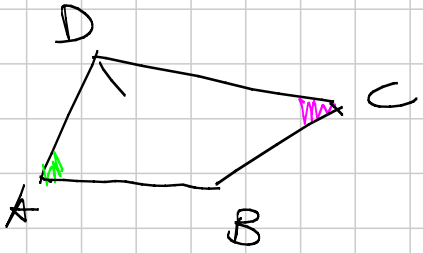
$\widehat{CAP} \cong \widehat{A'P'C}$
$\widehat{CAB} \cong \widehat{A'B'C}$ ↕ 1?

$\widehat{CAP} \sim \widehat{CP'A'}$
$\widehat{A'B'C} \sim \widehat{BAC}$

Es. 2

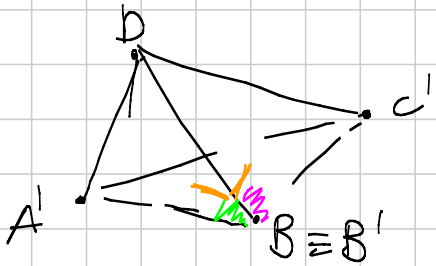
ABCD quad. convesso $\hat{A} + \hat{C} = \pi/2$

$$(AB \cdot DC)^2 + (AD \cdot BC)^2 = (AC \cdot DB)^2$$



$\alpha + \alpha = \pi/2$

inverto in D e cerchio fermo B



$\triangle DA'B \sim \triangle DBA$

$\triangle DC'B \sim \triangle DBC$

pitagora in $\triangle A'BC'$

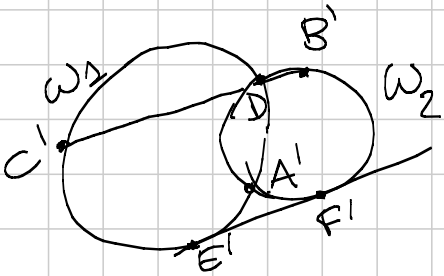
$$A'C' = \frac{AC \cdot BD^2}{AD \cdot DC} \qquad A'B = \frac{AB \cdot BD^2 \cdot DC}{AD \cdot BD \cdot DC}$$

$$C'B = \frac{BC \cdot BD^2 \cdot AD}{BD \cdot DC \cdot AD}$$

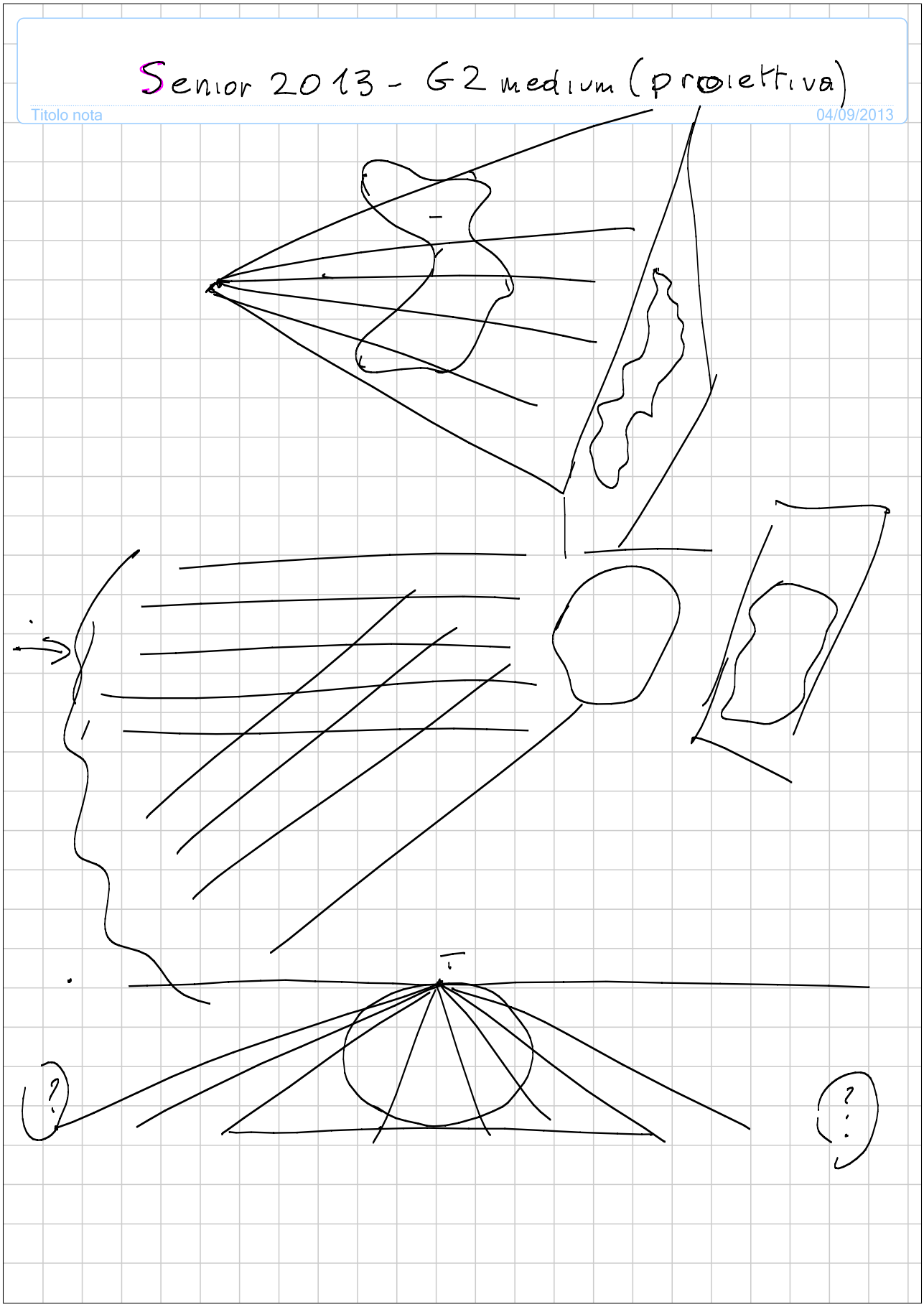
$$A'B^2 + C'B^2$$

$$\frac{BD^4}{(BD \cdot DC \cdot AD)^2}\left((AB \cdot DC)^2 + (BC \cdot AD)^2\right) = \frac{(AC \cdot BD)^2 \cdot BD^4}{(AD \cdot DC \cdot BD)^2}$$

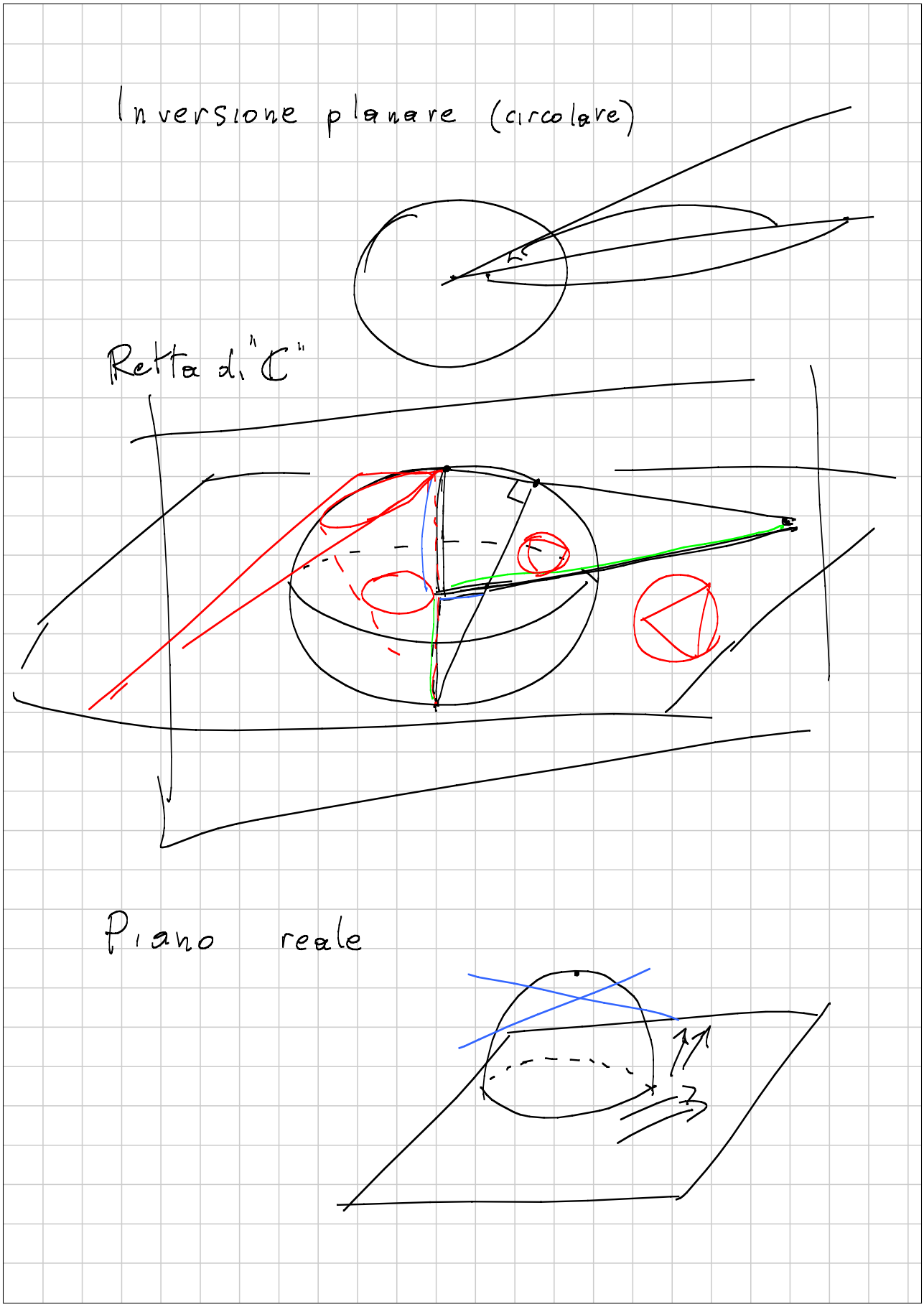
Esercizio

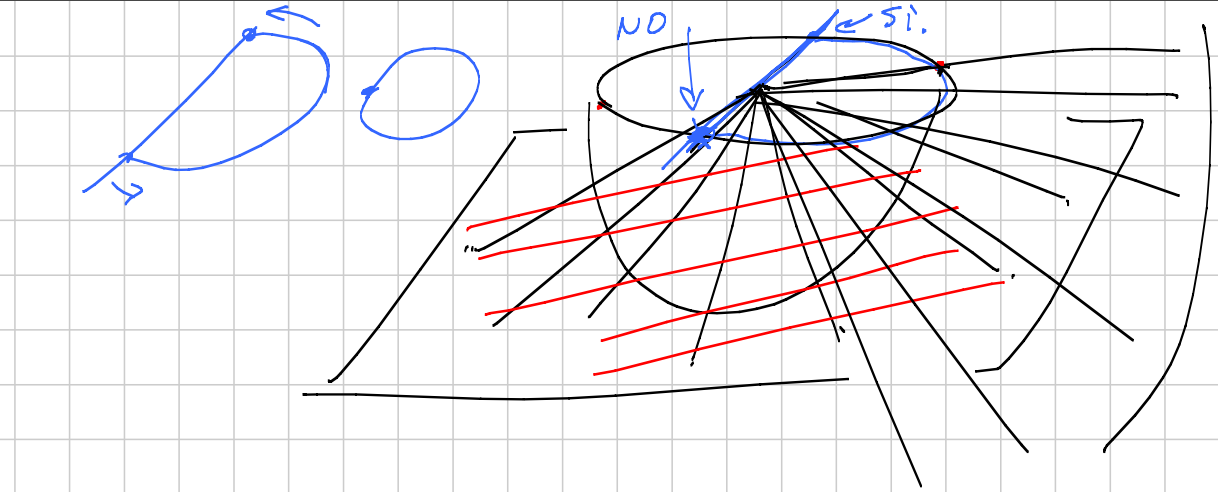


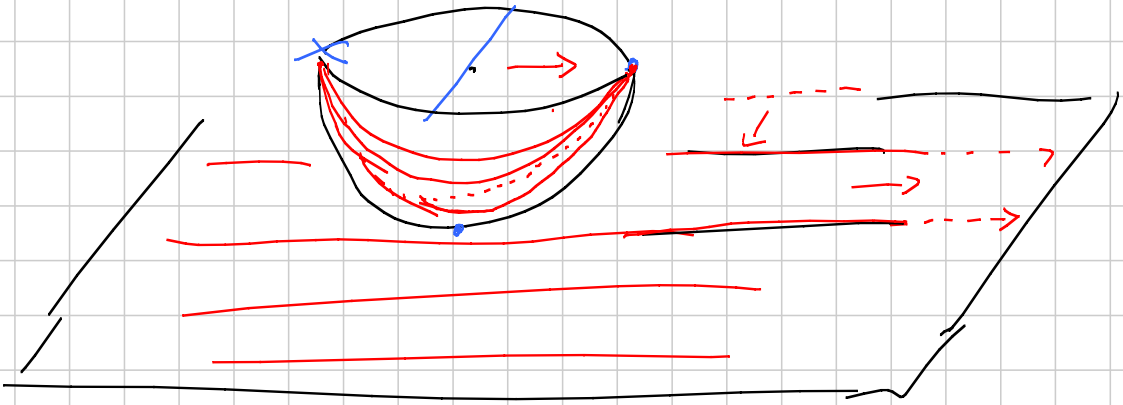
tesi circ. circoscritte a $B'DE'$ e $C'DF'$ si incontrano su $A'D$ (di nuovo)



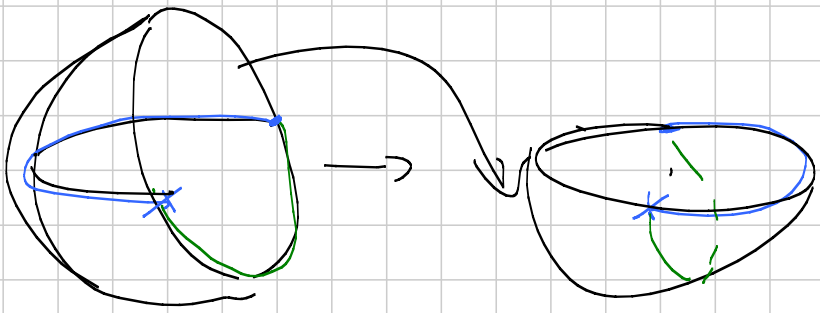
Geometria 2 (Medium) – Ludovico Pernazza

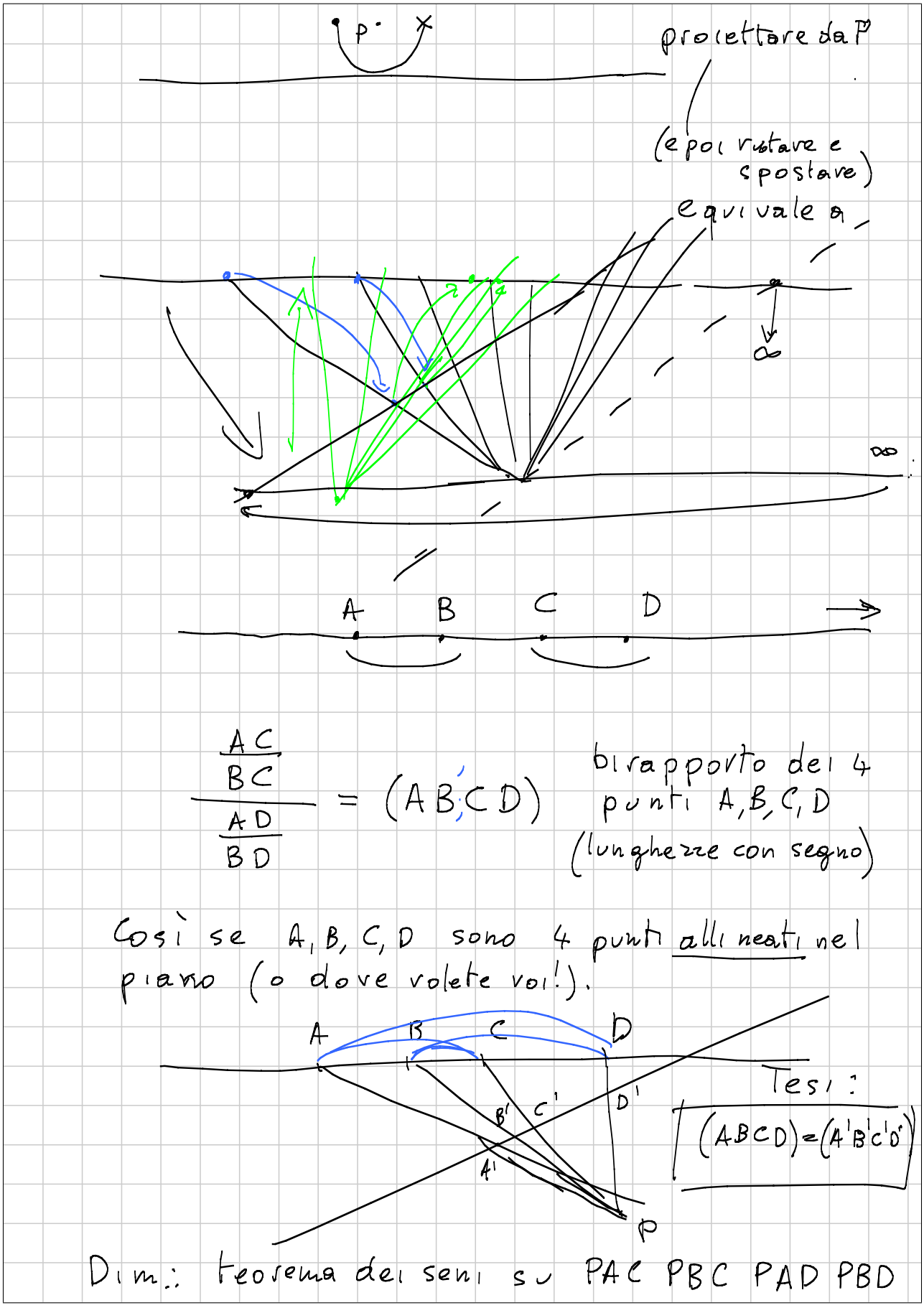

Inversione planare (circolare)
Retta di "C"
Piano reale



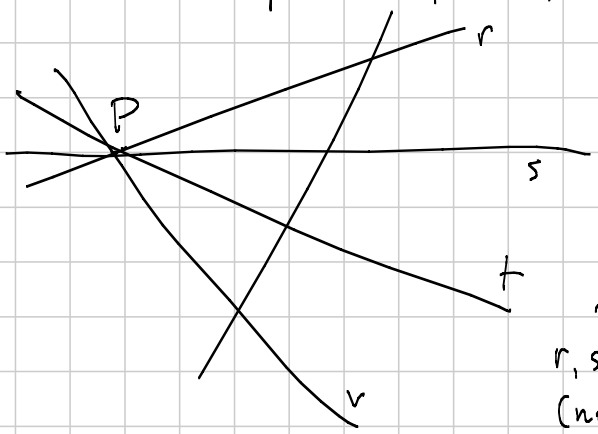


Nel piano proiettivo, tutte le rette (distinte) si intersecano in 1 punto.




P
X
proiettare da P
(e poi ruotare e spostare)
equivale a
∞
∞
A
B
C
D
$\frac{\frac{AC}{BC}}{\frac{AD}{BD}} = (AB;CD)$
birapporto dei 4 punti A, B, C, D
(lunghezze con segno)
Così se A, B, C, D sono 4 punti allineati nel piano (o dove volete voi!).
A
B
C
D
A'
B'
C'
D'
P
Tesi:
$(ABCD) = (A'B'C'D')$
Dim.: teorema dei seni su PAC PBC PAD PBD

$(ABCD) = \dfrac{\operatorname{sen} A\hat{P}C}{\operatorname{sen} B\hat{P}C} : \dfrac{\operatorname{sen} A\hat{P}D}{\operatorname{sen} B\hat{P}D}$, quindi è indipendente dalla retta su cui lo calcolo (se non passa per P, almeno).



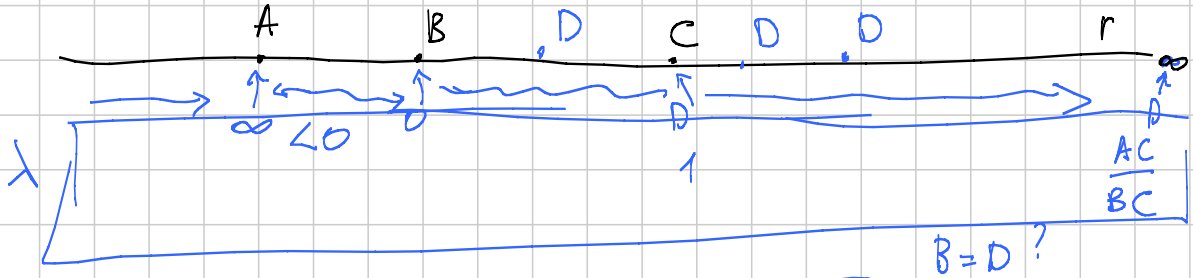
$(rstv)$ birapporto di 4 rette concorrenti

birapporto di 4 punti ottenuti intersecando r, s, t, v con una trasversale (non per P magari).

$(ABCD) = \lambda \qquad (ABDC) = \dfrac{1}{\lambda} = (BACD)$

$(ACBD) \overset{?}{=} 1-\lambda \qquad (ADCB)$

$$\left(\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{\lambda}{1-\lambda}, \frac{1-\lambda}{\lambda}, \frac{1}{1-\lambda}\right)$$



$D = \infty$? $\quad \dfrac{AC}{BC} \cdot \dfrac{BD}{AD} = \dfrac{AC}{BC} \cdot \dfrac{B\infty}{A\infty} = \dfrac{AC}{BC} > 1$

Importante oss.: è una biiezione tra $\lambda \in \mathbb{R} \cup \{\infty\}$ e le posizioni di D su $r \cup \{\infty\}$

$(ABCD) + (ACBD) = 1$

$A\ B\ C\ D\ D'$ allineati

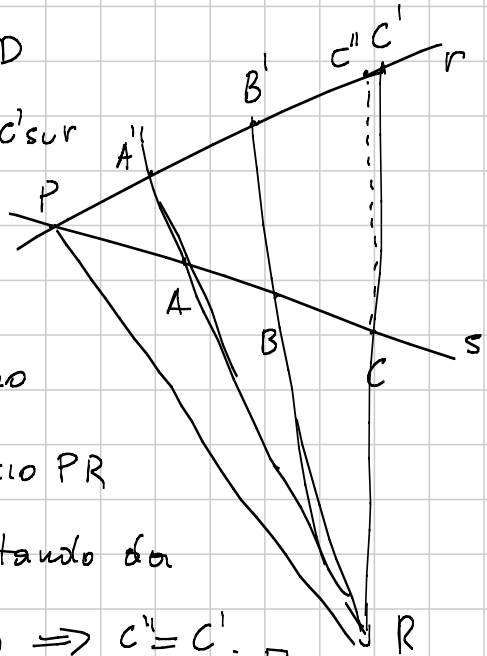
$(ABCD) \cdot (ABDD')$

$$\frac{(ABCD)}{(ABDD')} = (ABCD') \qquad \frac{(ABCD)}{(ABEF)} = (CDEF)$$

$(ABCD) = 1 \iff C = D$

Teorema P, A, B, C su s; P, A', B', C' sur

$(PABC) = (PA'B'C')$



Allora le rette AA', BB' e CC' concorrono

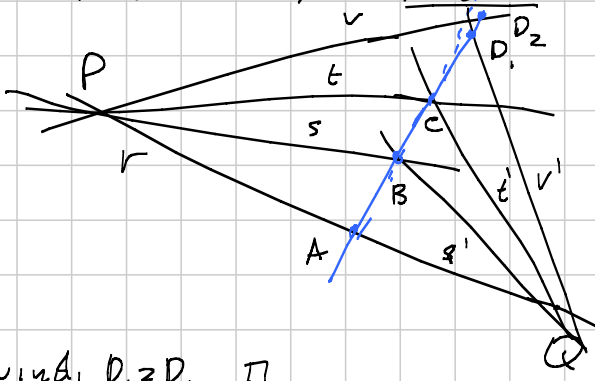
Dim.: $R = AA' \cap BB'$. Traccio PR

$RC \cap r = C''$; ma proiettando da R su r $(PA'B'C'') = (PABC) \Rightarrow C'' = C'$. □

[r, s, t, v 4 rette concorrenti, e così r, s', t', v' in Q

$(r,s,t,v) = (r,s',t',v')$. Allora in P $s \cap s'$, $t \cap t'$, $v \cap v'$ sono allineati.

Dim



Considero la retta per $s \cap s'$ e $t \cap t'$:

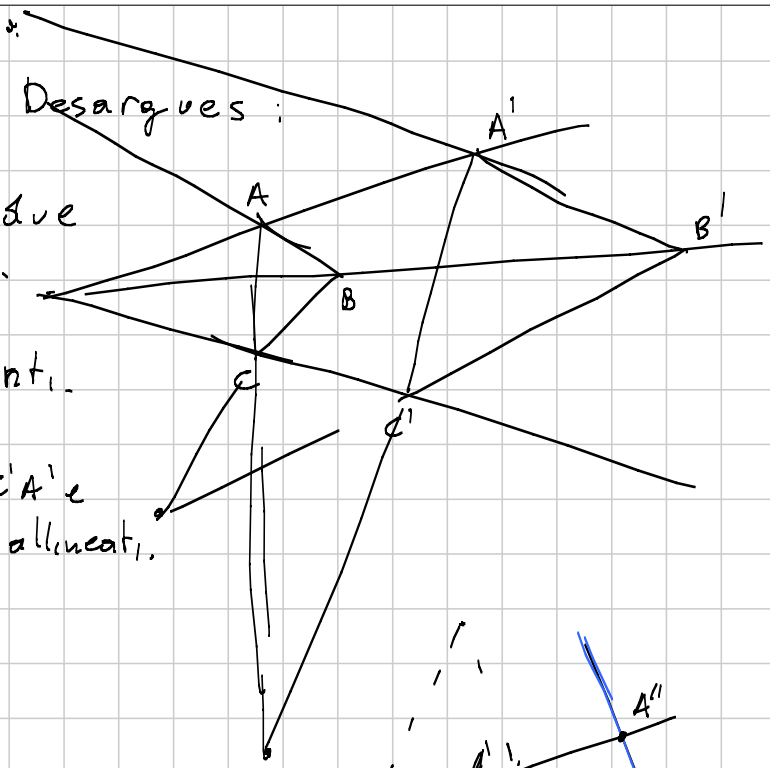
$(rstv) = (ABCD_2)$

$(rs't'v') = (ABCD_1)$.

Quindi $D_1 = D_2$ □

Teorema di Desargues:

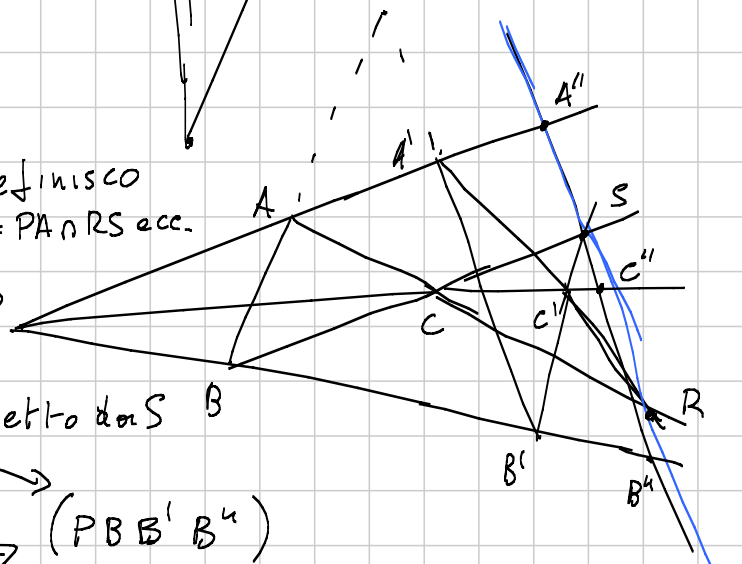
ABC $A'B'C'$ due triangoli t.c. AA', BB' e CC' sono concorrenti. Allora $AB \cap A'B'$, $CA \cap C'A'$ e $BC \cap B'C'$ sono allineati.



Dim

Dimostrerò che AB, $A'B'$ e RS concorrono.

Definisco $A'' \equiv PA \cap RS$ ecc.



$(PCC'C'')$ proietto da S $\rightarrow$ $(PBB'B'')$

$(PCC'C'')$ proietto da R $\rightarrow$ $(PAA'A'')$

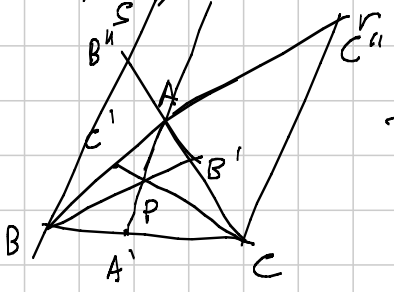
$(PAA'A'')$ e $(PBB'B'')$ sono uguali: quindi AB, $A'B'$ e $A''B''$ concorrono

$A''B'' = RS$

□

Teorema di Ceva: ABC triangolo, $A' \in BC$, $B' \in CA$, $C' \in AB$. AA', BB', CC' concorrono $\iff \frac{BA'}{CA'} \cdot \frac{CB'}{AB'} \cdot \frac{AC'}{BC'} = -1$

Dim.



Traccio le parallele a AA' per B e C (concorrono con AA')

proietto da B

$(A' B A \infty) = (C B' A B'') = \frac{CA}{CB''} \cdot \frac{B'B''}{B'A}$ $\quad (A C B' B'')$ $\quad \shortparallel$

↳ proj. da C

$(B C' A C'') = \frac{BA}{BC''} \cdot \frac{C'C''}{C'A}$ $\quad$ Così, $\quad (A B C' C'')$

e quindi

$$\frac{AB'}{CB'} \cdot \frac{BC'}{AC'} = \frac{AB''}{CB''} : \frac{AC''}{BC''} = \frac{A'B}{CB} : \frac{A'C}{BC} = \quad \text{(Talete su se } AA' \text{ e } r\text{)}$$

$$= -\frac{A'B}{A'C} \qquad \frac{AB'}{CB'} \cdot \frac{BC'}{AC'} \cdot \frac{CA'}{BA'} = -1$$

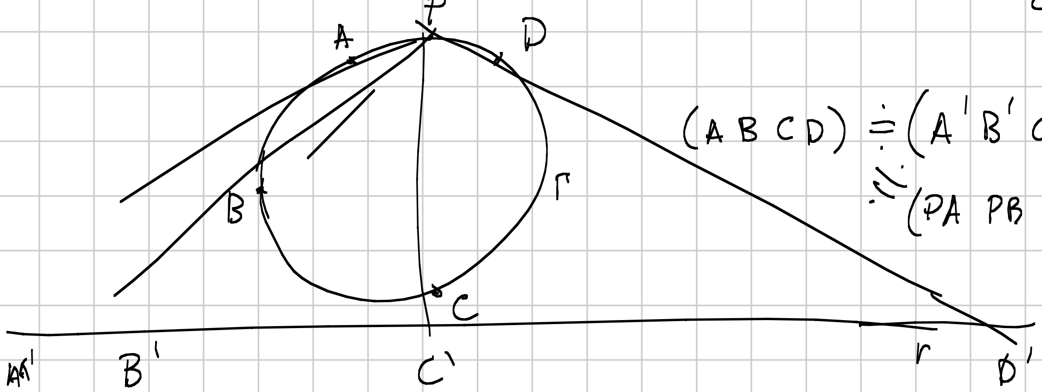
Teorema di Menelao: $\overset{r,s,t}{ABC}$ triangolo $\exists$ retta v per tre punti di r, s, t A', B', C'

$\underset{v \cap r}{A'}$, $\underset{v \cap s}{B'}$, $\underset{v \cap t}{C'}$

$$\Longleftrightarrow \frac{A'B}{A'C} \cdot \frac{B'C}{B'A} \cdot \frac{C'A}{C'B} = -1$$

Dim. idem. □

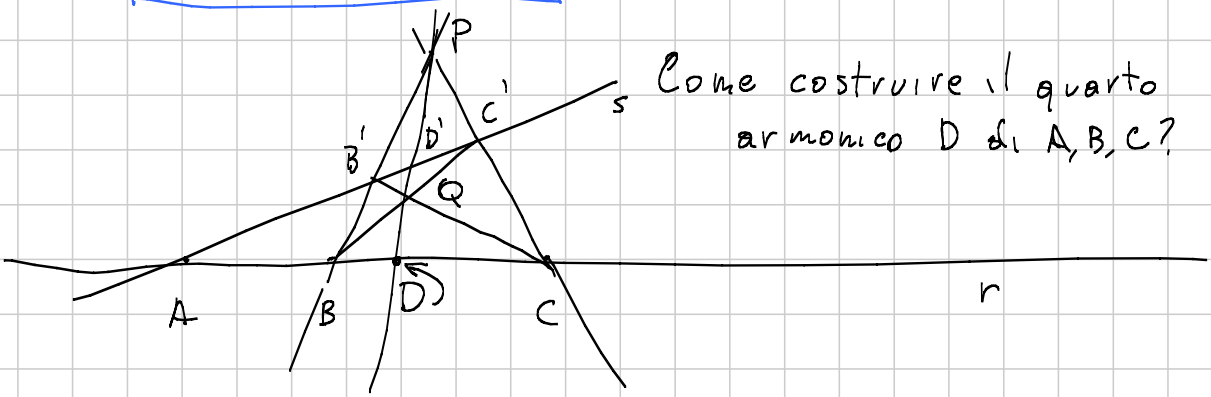
Birapporto su una circonferenza (o su una conica)



$(A B C D) \doteq (A' B' C' D')$
$\doteq (PA\ PB\ PC\ PD)$

Qualunque sia P, qualunque sia r il birapporto $(A'B'C'D')$ è lo stesso!

A, B, C, D allineati t.c. $(ABCD) = -1$ si dicono **quaterna armonica**



Come costruire il quarto armonico D di A, B, C?

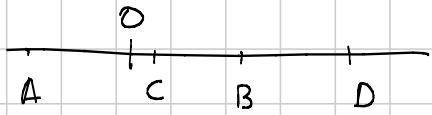
Scelgo s per A, $P \notin r \cup s$; traccio PB e PC, chiamo $B' = PB \cap s$ $C' = PC \cap s$ e $Q = CB' \cap BC'$; sia $D = r \cap PQ$ e $D' = s \cap PQ$.

$$(ADBC) = (AD'B'C') = (ADCB) = \frac{1}{(ADBC)}$$

$\Rightarrow (ADBC) =$ ~~+1~~ no perché A, B, C, D distinti, -1

D è anche detto coniugato di A rispetto a BC

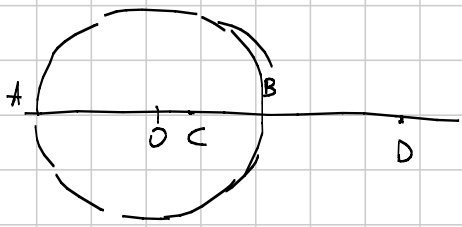
Proprietà: A, B, C, D quat. armonica, O = p. medio di AB



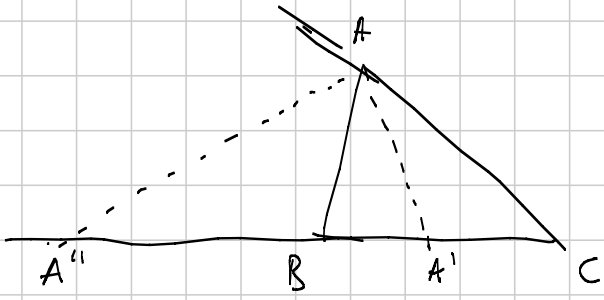
① $\frac{2}{AB} = \frac{1}{AC} + \frac{1}{AD}$

② $CA \cdot CB = CO \cdot CD$

③ $OC \cdot OD = OA^2 = OB^2$ ⟶



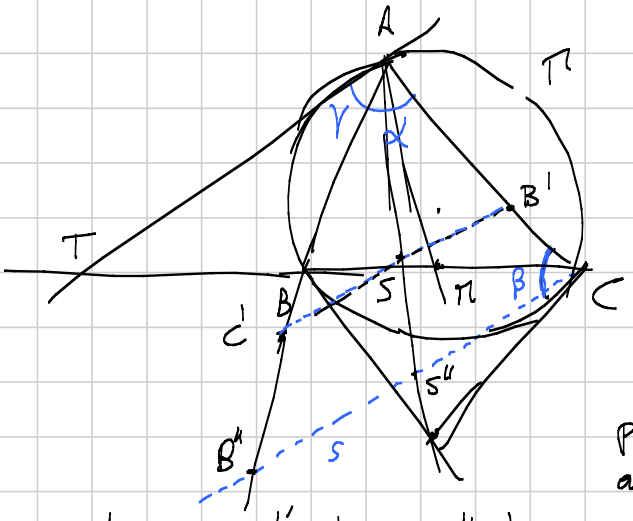
④ $\frac{OC}{OD} = \left(\frac{AC}{AD}\right)^2 = \left(\frac{BC}{BD}\right)^2$



AA', AA'' bisettrici

$(A''A'BC) = -1$.

(calcolo con seni o teo. bisettrice).



AT tangente in A a Γ

AS simmediana.

$(T\ S\ BC) = -1$

Simmediana = luogo dei p. medi delle antiparallele al lato opposto

Simmetrizzo: l'antiparallela per C a BC fa con AC un angolo β. AT con AC fa un angolo $\pi - \beta$

$\Rightarrow$ AT e s sono parallele. S'' è p. medio di $B''C$.

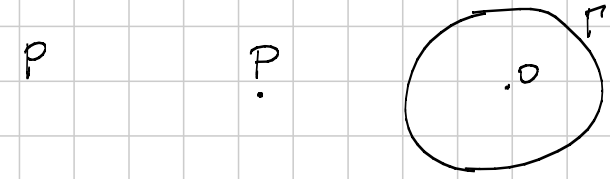
Ma il p. medio è il coniugato armonico di ∞

$$(\infty\ S''B''C) = \left(\frac{S''B''}{S''C}\right)^{-1} = -1$$

$\Rightarrow$ $TSBC$ è armonica. $\square$

Polo e polare

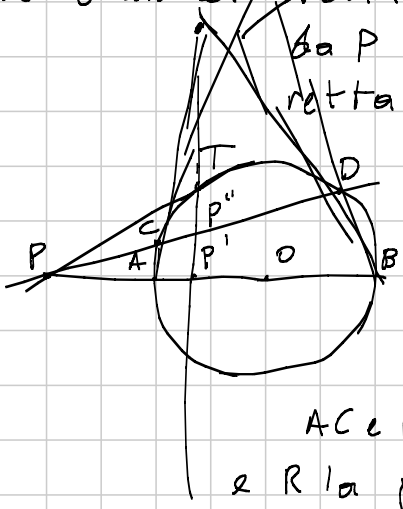
C conica (circonferenza, o 2 rette)



Il luogo dei punti Q quarti armonici di P e delle due intersezioni delle rette per P con Γ è una retta, chiamata **polare di P**

La polare è anche: retta per i punti di tangenza da P

retta $\perp$ PO per l'inverso di P.

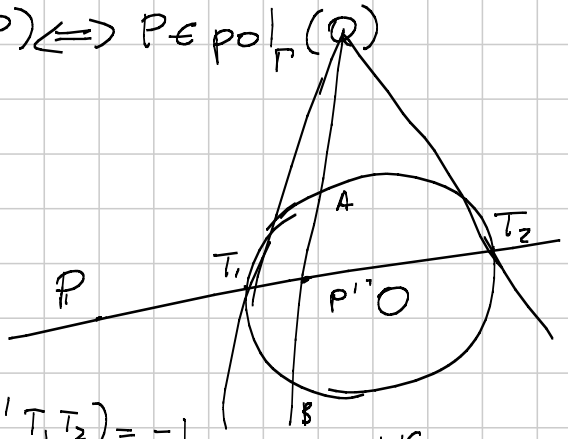


$(PP'AB) = -1$

$(PTTT) = -1$

$(PP''CD) = -1$ perché AC e BD si intersecano su $P' \in T_1 R$ e R la proietta su $(PP'AB)$.

Dualità: $Q \in pol_\Gamma(P) \iff P \in pol_\Gamma(Q)$



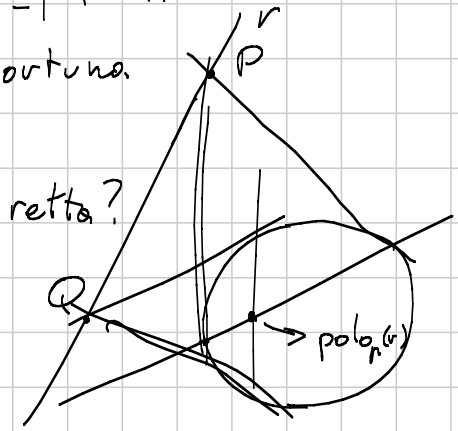
$(QPAB) = -1$

Quanto vale (PQX_1X_2) ? $= (PP'T_1T_2) = -1$ proiettando dal punto opportuno.

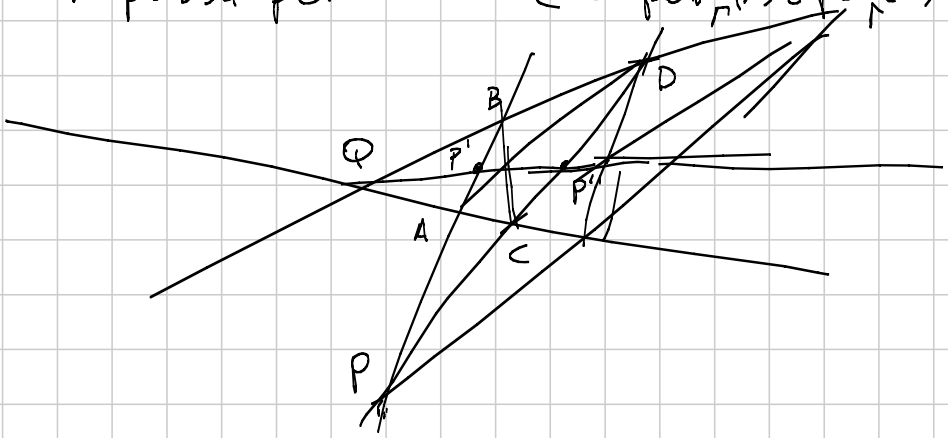
Come calcolo il polo di una retta?

Per $pol_\Gamma(r) \in pol_\Gamma(P)$

$pol_\Gamma(r) \in pol_\Gamma(Q)$



r passa per P e Q $\longleftrightarrow$ polo$_r$(r) $\in$ pol$_r$(P) $\cap$ pol$_r$(Q)

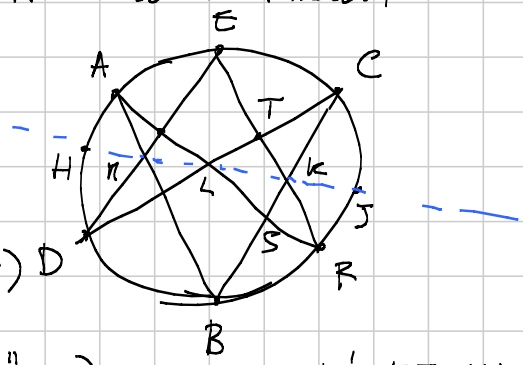


Teorema di Pappo: $A,B,C \in r$ $A',B',C' \in s$

$AB' \cap BA'$ $AC' \cap CA'$ $BC' \cap CB'$ sono allineati

Teorema di Pascal: $ABCDEF$ su conica

$AB \cap DE$ $BC \cap EF$ $CD \cap FA$ sono allineati



$H, J = \pi L \cap \Gamma$

$(H \pi L J) \overset{D}{=} (HECJ) \overset{T}{=} (HK'LJ)$ D

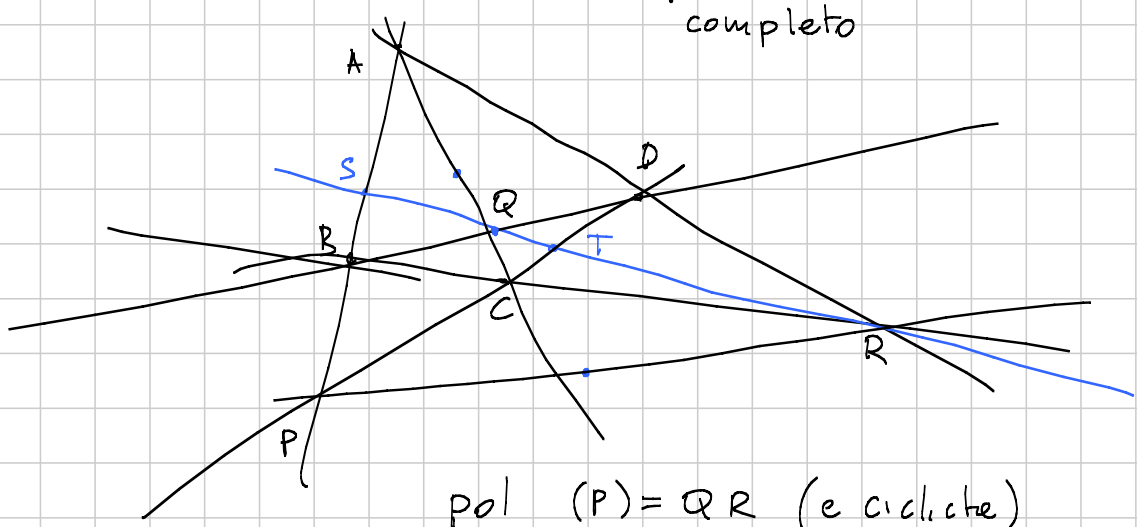
$(H \pi L J) \overset{A}{=} (HBFJ) \overset{S}{=} (HK''LJ)$

$K' = ET \cap \pi L$

$K'' = BS \cap \pi L$

Quindi $K' = K'' \Rightarrow BC \cap EF \in \pi L$

quadrilatero completo

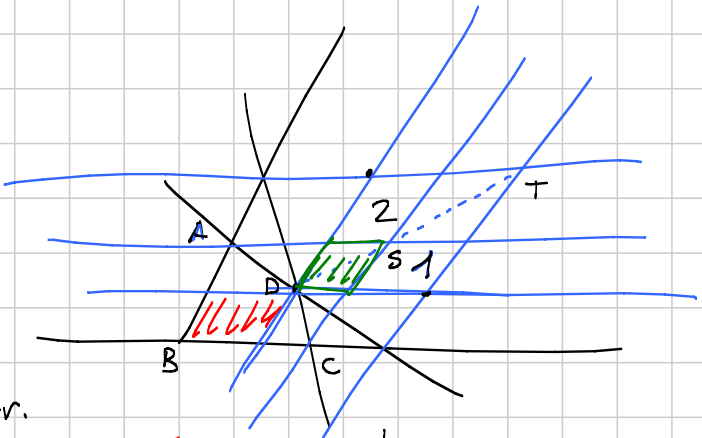


$\underset{AD,BC}{pol}(P) = QR$ (e cicliche P,Q,R)

$(STQR) = -1 \quad (PSBA) = -1 \quad (PTCD) = -1$

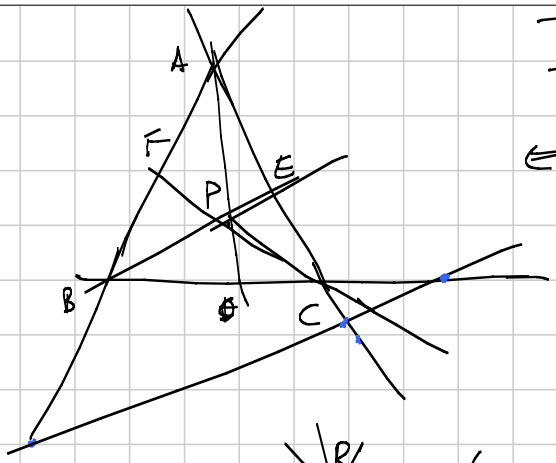
Diagonali: AC, BD, PR

Es. r_1 r_2 r_3 (p. medi di AC, BD e PR) sono allineati



DST allineati:
$S \in$ diag. parallelogr.
$\Leftrightarrow \quad 1 = 2$: ma $1 + \text{▨} = \text{▨} = 2 + \text{▨}$!

r_1 r_2 r_3 sono p. medi di BD, BS, BT



Teorema (Ceva $\overleftarrow{\text{vs}}$ Menelao)

AD BE CF concorrono

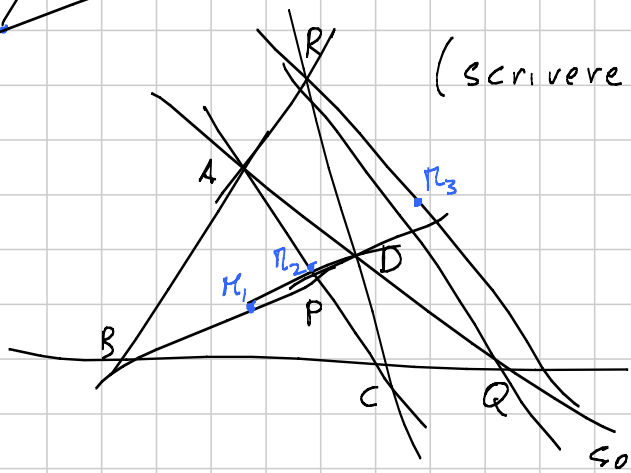
$\Leftrightarrow$ i quarti armonici di

A risp. BC

E AC

F AB

sono allineati



(scrivere i birapporti)

In BQR

BD RC e AQ

concorrono in D

$\Rightarrow$ i quarti armonici

delle terne sui lati

sono allineati.

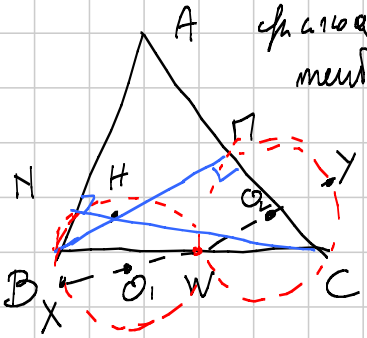
I rapporti di Menelao sono quelli della formula (4)

$\Rightarrow$ il prodotto dei quadrati fa 1 $\Rightarrow$ r_1, r_2 e r_3 sono allineati.

GEOMETRIA SINTETICA – G3M

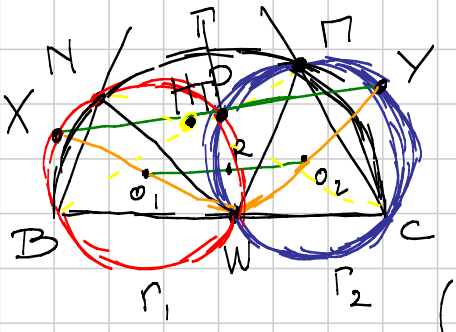
Titolo nota 05/09/2013

IMO 2013 – B1



Sia $\triangle ABC$ e Γ la sua circonferenza considerata. Siano W, X e Y i punti diametralmente opposti a W, X e Y. Allora X, H, Y allineati.

Dim: Notiamo $BC\Gamma N$ ciclico (due angoli retti)



$\text{pow}_{\Gamma}(A) = AN \cdot AB = A\Gamma \cdot AC$

$\text{pow}_{\Gamma_1}(A) = AN \cdot AB$

$\text{pow}_{\Gamma_2}(A) = A\Gamma \cdot AC$

(altrimenti: AB asse rad tra Γ e Γ_1)
AC asse rad tra Γ e Γ_2

$\Rightarrow A \in$ asse rad tra Γ_1 e Γ_2

se $\Gamma_1 \cap \Gamma_2 = \{W, P\} \Rightarrow A \in PW$

$\Rightarrow AP \perp O_1O_2$

Ma $XY \parallel O_1O_2$ per Talete $\Rightarrow AP \perp XY$

Inoltre per simmetria, se $PW \cap O_1O_2 = R$, si ha $PR = WR$

$\Rightarrow P$ sta su XY (sempre per Talete)

Hope: $H\hat{P}A = \frac{\pi}{2}$

$ANHP$ ciclico con diam. AH. Se P sta sulla sua circ. abbiamo finito. Questo è vero per il Teorema di Miquel.

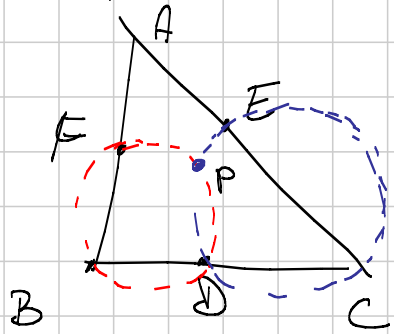
Oppure, da ignorarsi, calcolo anche

$$N\hat{P}\Pi = 2\pi - N\hat{P}W - \Pi\hat{P}W = 2\pi - (\pi-\beta) - (\pi-\gamma) =$$

$$= \beta+\gamma \Rightarrow ANP\Pi \text{ ciclico} \Rightarrow \text{tesi}. \square$$

Teo (Miquel): Dato un Triangolo ABC con tre punti D, E, F sui suoi lati, le circonferenze circoscritte a AEF, BDF, CED concorrono.

Dim:



Traccio le ch per B, D, F e C, E, D che si incontrano, oltre che in D, in un punto P.

$$F\hat{P}E = 2\pi - F\hat{P}D - E\hat{P}D =$$

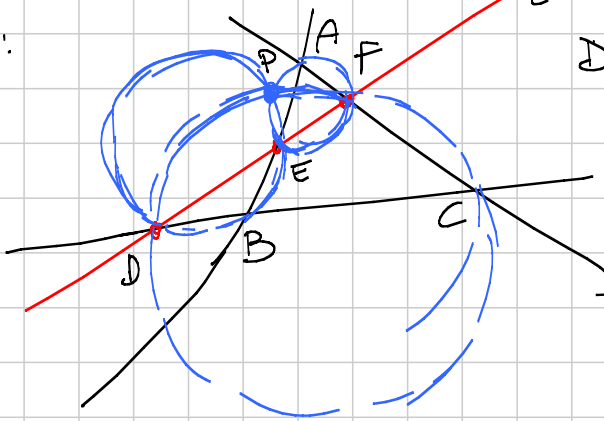
$$= 2\pi - (\pi-\beta) - (\pi-\gamma) = \beta+\gamma$$

$\Rightarrow AFPE$ ciclico. $\square$

Oss: Il Teo di Miquel vale per qualunque configurazione.

Teo (di Miquel): Date 4 rette r_1, r_2, r_3, r_4, a 3 a 3 non concorrenti, sia Γ_i la ch. circ. al Tri formato da $r_j r_k r_l$ per $\{i,j,k,l\} = \{1,2,3,4\}$. Allora $\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4$ concorrono.

Dim:



ch. blu $\Leftarrow$ ABC Tri, BEF punti ex bar

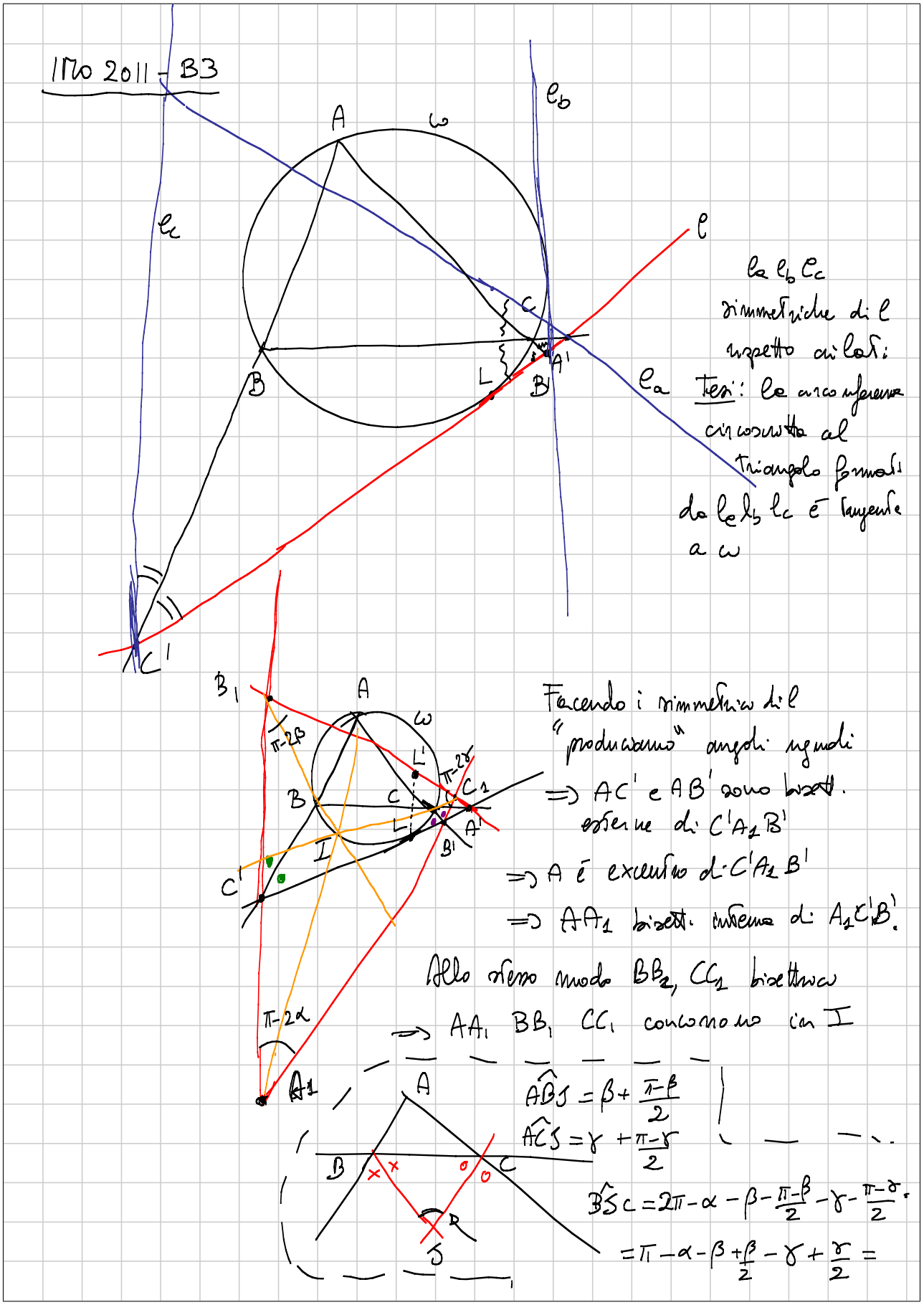
DCF Tri, AEB punti simili

$\Downarrow$

circa CAB, AEF, DBE concorrono

$\Rightarrow$ circa CAB passa per l'inverso dell'inverso della circa a AEF e DBE.

ovvero P. $\square$


IMO 2011 - B3
A
ω
ℓ_b
ℓ_c
ℓ
ℓ_a
B
C
L
B'
A'
C'
la ℓ_b ℓ_c simmetriche di ℓ rispetto ai lati: Tesi: la circonferenza circoscritta al triangolo formato da ℓ_a ℓ_b ℓ_c è tangente a ω
B_1
$\pi-2\beta$
L'
$\pi-2\gamma$
C_1
A_1
I
$\pi-2\alpha$
Facendo i simmetrici di ℓ "producono" angoli uguali
$\Rightarrow$ AC' e AB' sono bisett. esterne di $C'A_1B'$
$\Rightarrow$ A è excentro di $C'A_1B'$
$\Rightarrow$ AA_1 bisett. interna di $A_1C'B'$.
Allo stesso modo BB_1, CC_1 bisettrici
$\Rightarrow$ AA_1 BB_1 CC_1 concorrono in I
$A\hat{B}S = \beta + \frac{\pi-\beta}{2}$
$A\hat{C}S = \gamma + \frac{\pi-\gamma}{2}$
$B\hat{S}C = 2\pi - \alpha - \beta - \frac{\pi-\beta}{2} - \gamma - \frac{\pi-\gamma}{2}$
$= \pi - \alpha - \beta + \frac{\beta}{2} - \gamma + \frac{\gamma}{2} =$

$\Rightarrow C\hat{A}B = \frac{\pi}{2} - \frac{C'\hat{A}_1B'}{2}$

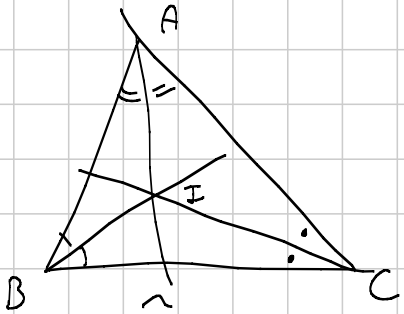
$C_1\hat{A}_1B_1 = C'\hat{A}_1B' = \pi - 2C\hat{A}B = \pi - 2\alpha$

$B_1\hat{I}C_1 = \frac{\pi}{2} + \frac{B_1\hat{A}_1C_1}{2} =$

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

$\Rightarrow B\hat{I}C = \pi - \alpha \Rightarrow$ BICA ciclico.

$= \frac{\beta}{2} + \frac{\gamma}{2} = \frac{\pi}{2} - \frac{\alpha}{2}$.

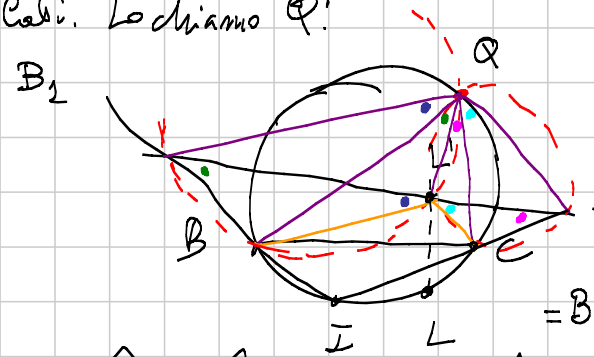


$B\hat{I}C = \pi - \frac{\beta}{2} - \frac{\gamma}{2} =$

$= \frac{\pi}{2} + \frac{\alpha}{2}$

Sia L' simm. di L rsp. a BC

considero il pf. di Miquel in B_1IC_1 dato dai punti B, C, L' ossia Q. Lo chiamo Q.



$B_1\hat{Q}B = B_1\hat{L}'B = B\hat{L}C' =$

$= B\hat{C}L = B\hat{C}L'$

$B_1\hat{Q}C_1 = B\hat{Q}L' + L'\hat{Q}C + B_1\hat{Q}B + C\hat{Q}C_1 =$

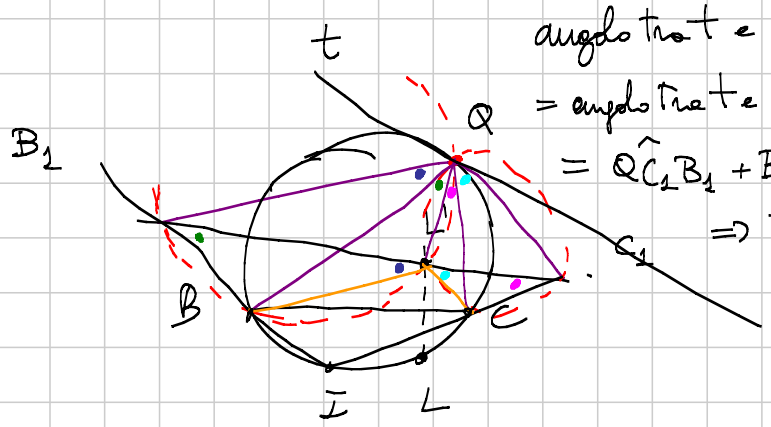
$= I\hat{B}_1C_1 + I\hat{C}_1B_1 + C\hat{B}L' + B\hat{C}L' =$

$= \pi - B_1\hat{I}C_1 + \pi - C\hat{L}'B = \pi - B_1\hat{I}C_1 + \pi - C\hat{L}B =$

$= \pi - B_1\hat{I}C_1 + \pi - B\hat{I}C = 2\pi - 2B_1\hat{I}C_1 =$

$= \pi - B_1\hat{A}_1C_1 \Rightarrow$ Q sta sulla cf. per $A_1B_1C_1$

$$\boxed{B_1\hat{Q}B + Q\hat{C}_1B_1 = B\hat{C}Q}$$



t tg alla ch per $A_1B_1C_1$ in Q

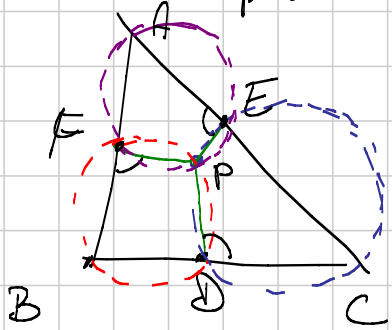
angolo tra t e QB =

= angolo tra t e QB_1 + $B_1\hat{Q}B$ =

= $Q\hat{C}_1B_1 + B_1\hat{Q}B = Q\hat{C}B$

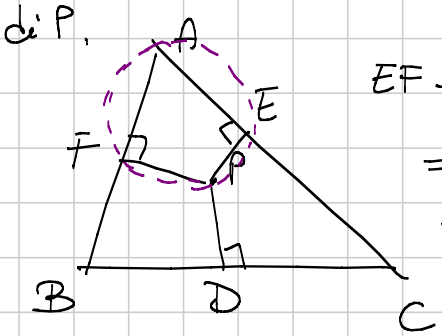
$\Rightarrow$ t è tangente a ω. □

Oss: P punto di Miquel per DEF $\Rightarrow P\hat{D}C \cong P\hat{E}A \cong P\hat{F}B$ (*)



Vale anche il contrario:
dato P, se costruisco D, E, F
in modo tale che valga (*)
$\Rightarrow$ P è il punto di Miquel
di DEF.

Oss 2: Se $P\hat{D}C = P\hat{E}A = P\hat{F}B = \frac{\pi}{2}$, DEF è detto triangolo podale di P.



$EF = 2R_{AFPE} \cdot \sin F\hat{A}E =$

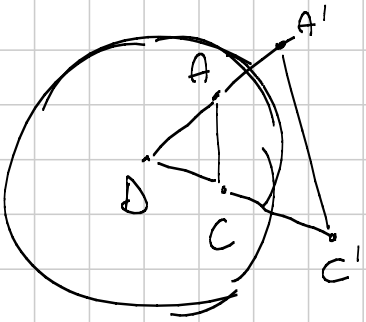
$= AP \cdot \sin\alpha = \frac{AP \cdot BC}{2R}$

$ED = \frac{CP \cdot AB}{2R}$

$DF = \frac{BP \cdot AC}{2R}$

Teo di Tolomeo: Un quadrilatero convesso ABCD è ciclico se e solo se $AB \cdot CD + BC \cdot DA = AC \cdot BD$.

Dim: Invertiamo in D!!!



$DA \cdot DA' = R^2$

$DC \cdot DC' = R^2$

$DC \cdot DC' = DA \cdot DA'$

$\frac{DC}{DA} = \frac{DA'}{DC'} \iff D\hat{C}A \sim D\hat{A}'C'$

$\iff \frac{A'C'}{AC} = \frac{DC'}{DA}$

$$A'C' = \frac{AC \cdot DC'}{DA} = R^2 \frac{AC}{DA \cdot DC}$$

La circonferenza per DCA diversa da retta $A'C'$ e il punto B va nel punto B'.

$ABCD$ ciclico $\iff B', A', C'$ allineati.

Se B' stanno tra le semirette DA e DC.

$\Rightarrow B', A', C'$ allineati $\iff A'B' + B'C' = A'C'$

$$\iff \frac{R^2 AB}{DA \cdot DB} + \frac{R^2 BC}{DB \cdot DC} = \frac{R^2 AC}{DA \cdot DC}$$

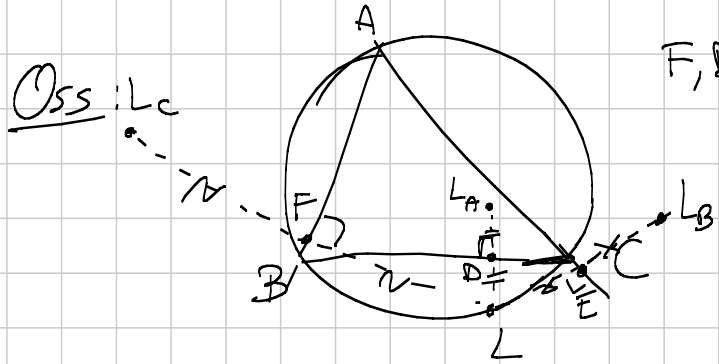
$$\iff AB \cdot DC + BC \cdot DA = DB \cdot AC \quad \square$$

Teo: P punto, le proiez. di P sui lati (D, E, F) sono allineate se e solo se P sta sulla circonferenza circoscritta ad ABC

Dim: Wlog $DE + EF = DF \iff \frac{CP \cdot AB}{2R} + \frac{AP \cdot BC}{2R} = \frac{BP \cdot AC}{2R}$

$\iff CP \cdot AB + AP \cdot BC = BP \cdot AC \iff CPAB$ ciclico $\square$

(Retta di Simson)



F, D, E allineati $\Leftrightarrow$ il Teo di Simson.

$\Downarrow$

L_A, L_B, L_C allineati.

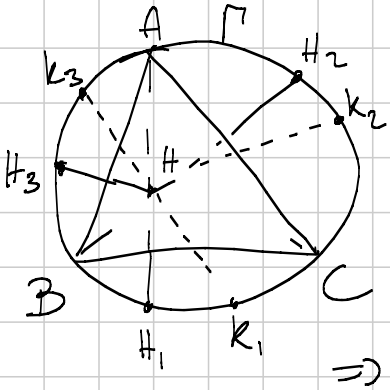
Se mettiamo l'origine nel circocentro e ovviamo

$$\ell_a = \left(\frac{\ell - b}{c-b}\right)(c-b) + b = \frac{\frac{1}{e} - \frac{1}{b}}{\frac{1}{c} - \frac{1}{b}}(c-b) + b =$$

$$= \frac{e-b}{c-b} \cdot \frac{cb}{eb}(c-b) + b = c + b - \frac{bc}{e}$$

Calcolando anche ℓ_b, ℓ_c si vede che $h = a+b+c$ sta sulla retta per ℓ_a, ℓ_b, ℓ_c.

Cor: la linea di Simson di L passa per il p.to medio tra L e H.



omot. di centro H e fattore $\frac{1}{2}$

K_1, K_2, K_3 $\longrightarrow$ p.ti medi dei lati

H_1, H_2, H_3 $\longrightarrow$ piedi delle altezze

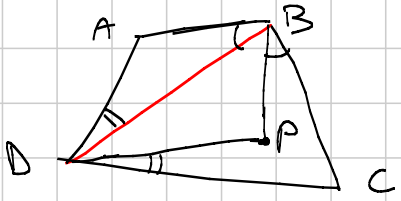
A, B, C $\longrightarrow$ p.ti medi di AH, BH, CH.

$\Rightarrow \Gamma \longrightarrow$ feuerbach

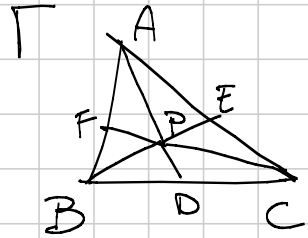
IMO 2004 – B2 $ABCD$ quad. convesso

P t.c. $A\hat{D}B = P\hat{D}C$ e $A\hat{B}D = P\hat{B}C$

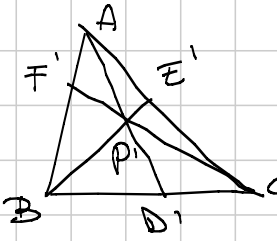
Dim che $ABCD$ è ciclico $\Longleftrightarrow$ $AP = PC$



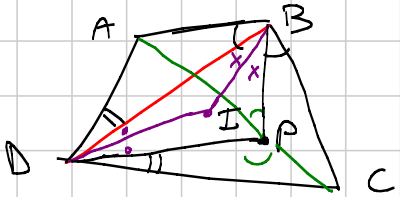
Dim: I punti A e C sono coniugati isogonali in $\triangle DPB$



sia AD' simm. di AD risp. alla bisett. int. in A
sia BE' " " BD " " " " in B
sia CF' " " CE " " " " in C



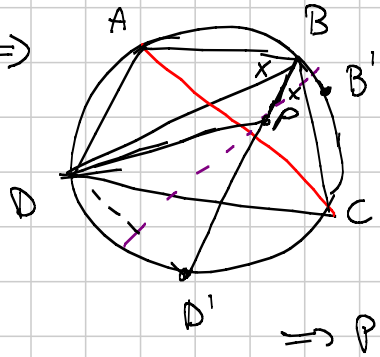
per Ceva Trig. inversa AD', BE', CF' concorrono. Il punto P' di conc. si dice coniugato isogonale di P



$\hat{ABI} = \hat{IBC}$
$\hat{ADI} = \hat{IDC}$
$\Rightarrow$ AP e PC sono simm. risp. alla bisett. uscente in P

$\Rightarrow \hat{APB} = \pi - \hat{DPC}$

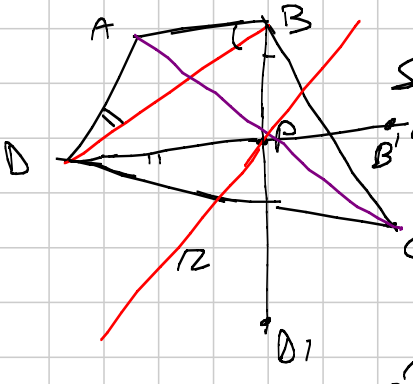
ciclico $\Rightarrow$



D', B' simm. risp all'asse di AC di D, B. stanno sulla cp. inoltre $\hat{DBA} = \hat{PBC} \Rightarrow B, P, D'$ sono allineati
allo stesso modo D, P, B' allineati.
$\Rightarrow P = DB' \cap D'B$
ma la simm. risp. all'asse di AC scambia DB' e $D'B \Rightarrow$ fissa $P \Rightarrow P$ sta sull'asse di $AC \Rightarrow AP = PC$.

$AP = PC \Rightarrow$ asse di AC passa per P e AP e CP sono simm. risp. a questo asse. Poiché A, C sono coniug isogonali,

PA, PC sono rimm. risp. alle bisettrici
$\Rightarrow$ asse di AC è bisettrice esterna di $B\hat{P}D$



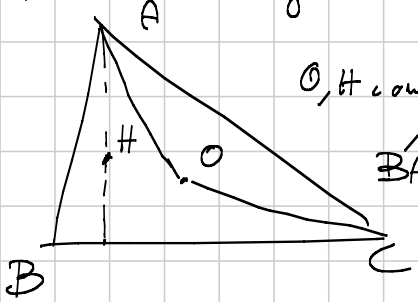
Se B' e D' sono rimm. di B, D rispetto a r
allora D', B, P allineati
D, B', P allineati.

$$\hat{ABP} = \hat{ABD'} = \hat{CBD} = \hat{AB'D'}$$
$\Rightarrow A, B, D', B'$ ciclico.

$$\hat{CBD} = \hat{ABD'} = \hat{CB'D} \Rightarrow CBB'D \text{ ciclico}$$

inoltre D, D', B, B' concicl. $\Rightarrow ABCD$ concicl. □

Oss: O, H sono coniugati isogonali



O, H con. isog $\Leftrightarrow B\hat{A}H = O\hat{A}C$ e cicliche

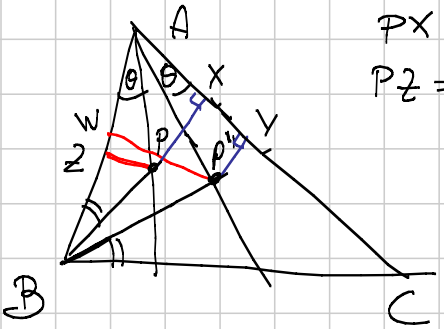
$$B\hat{A}H = \frac{\pi}{2} - \beta$$

$$O\hat{A}C = \frac{\pi - A\hat{O}C}{2} = \frac{\pi - 2\beta}{2} = \frac{\pi}{2} - \beta$$

$\Rightarrow$ ok.

Teo: Se P e P' sono coniugati isogonali, allora i loro triangoli pedali hanno la stessa circonferenza circoscritta, il cui centro è punto medio tra P e P'.

Dim:



$$P\hat{A}X$$
$$PX = AP \cdot \sin(\alpha - \theta)$$
$$PZ = AP \cdot \sin\theta$$
$$P\hat{A}Z$$
$$P'Y = AP' \sin\theta$$
$$P'W = AP' \sin(\alpha - \theta)$$

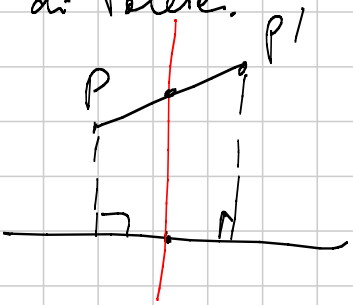
$$AX = AP \cdot \cos(\alpha - \theta) \qquad AY = AP' \cos\theta$$
$$AZ = AP \cos\theta \qquad AW = AP' \cos(\alpha - \theta)$$

$$AX \cdot AY = AP \cdot AP' \cos(\alpha - \theta)\cos\theta = AZ \cdot AW$$

$\Rightarrow X, Y, Z, W$ sono conciclici.

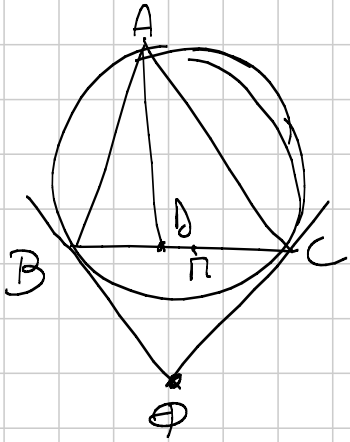
In questo modo ottengo 3 quadrilateri ciclici con circonferenze circoscritte che, se disegnate, hanno i 3 lati AB, AC, BC come assi radicali. Assurdo $\Rightarrow$ le 3 rette coincidono.

Il centro è il pt. medio di PP' per una banale applicazione del teo di Talete.



Coniugato isogonale del baricentro (punto di Lemoine)

Simm. di una mediana nella bisettrice = simmediana



PB, PC tangenti
AD simmediana
$\Rightarrow A, D, P$ allineati.

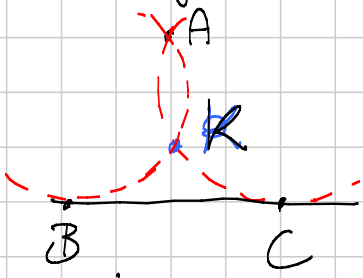
Teo $\Leftarrow$ AP è simmediana
$\Leftarrow$ AP è simm di AM
M pt medio di BC

Inversione in A di raggio $\sqrt{AB \cdot AC}$ $\quad B \to B' \quad AB' = AC$
$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad C \to C' \quad AC' = AB$
+
simmetria nella bisettrice di A

$B \to C$
$C \to B$

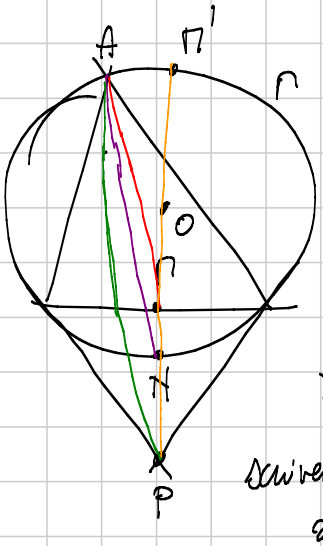
pt circ $\to$ retta BC
retta BC $\to$ pt circ.

$BP \to$ circ per A,B tg. a BC $\quad P \to K$
$CP \to$ circ per A,C tg a BC



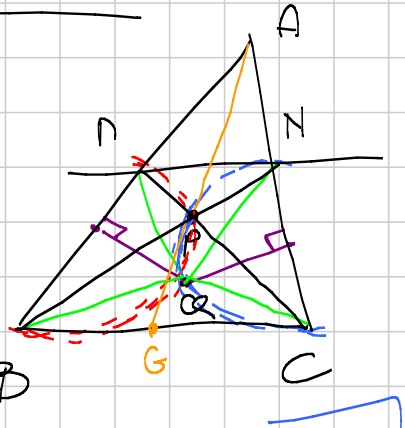
AK è asse radicale
BC è tg comune
$\Rightarrow AK$ passa per il pt medio di BC. fine

Dim 2:



$P \in pol_\Gamma(M)$
$\Downarrow$
$(M', N, M, P) = -1$
$(AM', AN, AM, AP) = -1$
$\hat{NAM'} = \frac{\pi}{2}$
scrivendo il birapporto con i seni si vede che $\hat{MAN} = \hat{NAP}$.

BMO 2009-2



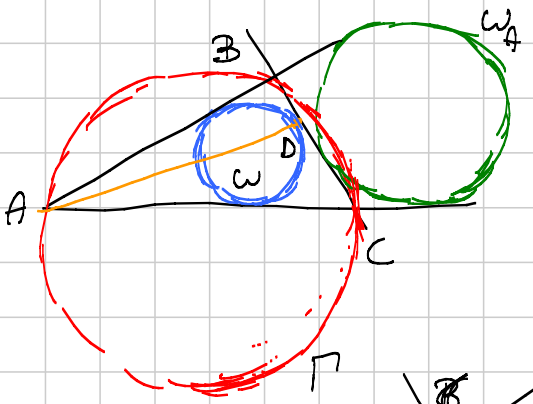
$MN \parallel BC$
$P = MC \cap NB$
circ a BPM e CPN si incontrano nuovamente in Q.
Dim che $\hat{BAQ} = \hat{CAP}$

× Ceva: $\frac{BG}{GC} \cdot \frac{CN}{NA} \cdot \frac{AM}{MB} = 1 \Rightarrow G$ pt. medio.
$\Downarrow$
1

Devo dim che AQ è simmediana.

conclusione × esercizio
(calcolo delle distanze L_1Q dai lati)

Coniugati isogonali di Nagel e Gergonne



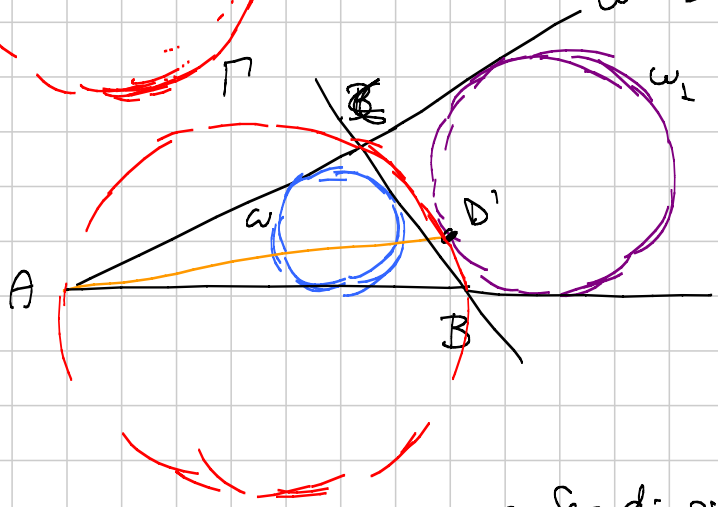
Inv. in A con raggio $\sqrt{AB \cdot AC}$ + simm. nella bisett. di A.

$\Gamma \to BC \qquad BC \to \Gamma$

$B \to C \qquad C \to B$

$\omega \to \omega_1 = $ tg a AB, AC, Γ esternamente

$D \to D'$



D' = centro di simil interno tra Γ e ω_1

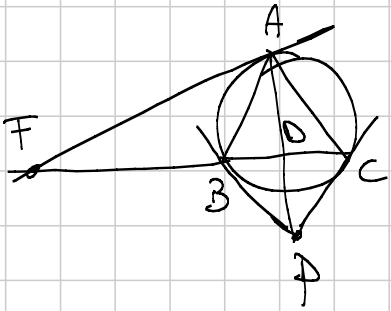
A = centro di simil esterno tra ω e ω_1

$\Rightarrow$ centro di simil interno tra ω e Γ sta su AD'.

$\Rightarrow AD'$ = simm. di AD risp alla bisett. interna.
= retta da A al centro di simil. interno tra ω e Γ.

$\Rightarrow$ centro di simil interno tra ω e Γ è coniug. isog. di Gergonne
" " " esterno tra ω e Γ " " " " Nagel.

Fatto:

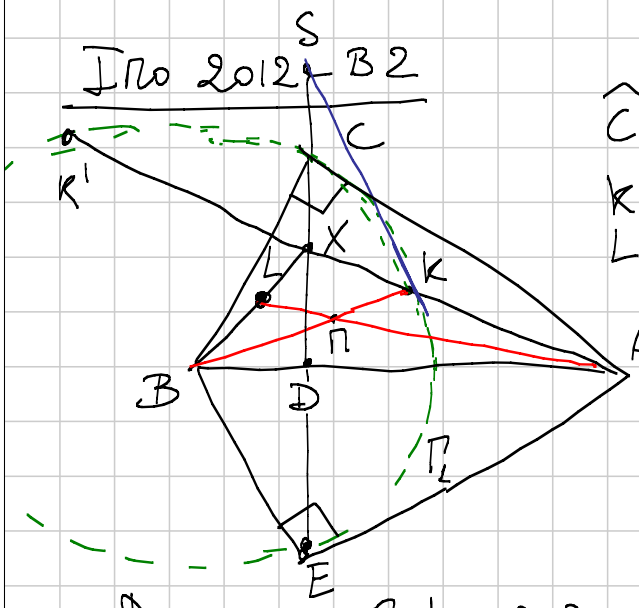


AD armonica

$(B, C, D, F) = -1$.

Fatto ieri!

IMO 2012 - B2



$\hat{C} = \frac{\pi}{2}$

$K \in AX$ t.c. $BC = BK$

$L \in BX$ t.c. $AC = AL$

$\Pi = BK \cap AL$

Tesi: $\Pi L = \Pi K$

Dim: Disegno Γ_1 di centro B per C, K. E l'altra intersez di CD con Γ_1

$(A, X, K, K') = -1$ (Ceviana della polare)

$(C, E, K, K')_{\Gamma} = -1$ $(KC, KE, KK, KK') = -1$ intersechiamo con CE

$(C, E, S, X) = -1$

Se ora rifaccio tutto in Γ_2 centro A e raggio AC, con $T = CE \cap LL$

$(C, E, T, X) = -1$

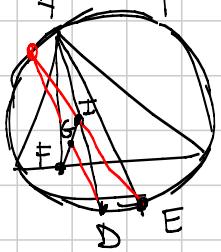
Ma, fissati 3 punti, ne esiste uno e uno solo che realizza un dato birapporto $\Rightarrow S = T$.

Ma CD è asse radicale delle due cfr

$\Rightarrow SL = SK$

$\Rightarrow S\hat{L}\Pi \cong S\hat{K}\Pi \Rightarrow L\Pi = K\Pi$.

ES per casa (IMO 2010 - A2)



$F\hat{A}B = E\hat{A}C$

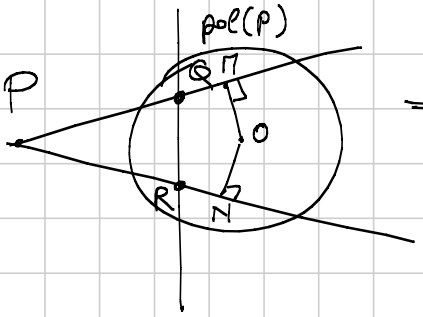
$GI = GF$

Th: $EI \cap DG \in \Gamma$

Inizio: Basta dim $A\hat{E}I = I\hat{D}G$ ....

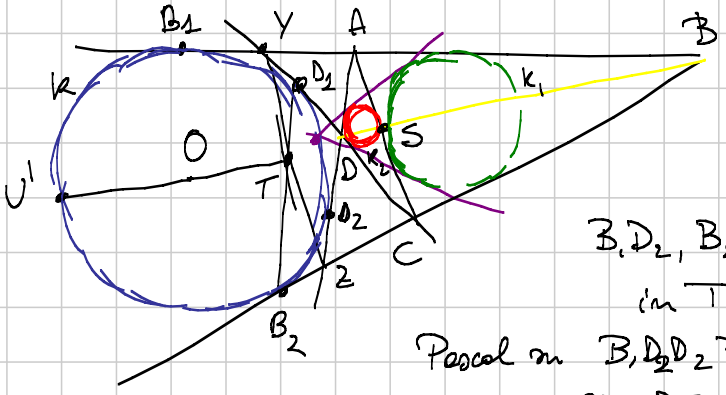
(usare I_a eccentro opposto ad A).

Es: P



$\Rightarrow$ RTNQ ciclico.

IMO 2008 - B3



tg. esterne comune a k_1, k_2 si incontrano su k.

B_1D_2, B_2D_1, YZ, BD concorrono in T.

Pascal su $B_1D_2D_2B_2D_1D_1$ $\quad = X$

$\Rightarrow B_1D_2 \cap D_2B_2$, D, $D_2B_2 \cap D_2B_1$ sono all. a T

$B_1B_1D_2B_2B_2D_1$ $\quad$ "T" lo T, D, X sono all.

$\hookrightarrow T, B, X$ sono all.

centro di simil tra k_1, k_2

$S = AC \cap BB$

$(ZB, ZS, ZA, ZY) = -1$ quad. completo $ABCD$

$(OB, OS, OA, OY) = -1$ $\quad \ell$ = retta per i centri O_1O_2 di k_1, k_2

$OB \cap \ell = O_1$, $\quad S \in \ell$, $\quad OT \cap \ell = U$

$\Rightarrow (O_1, O_2, S, U) = -1$

$\Rightarrow U$ centro est. di simil tra k_1, k_2

Si fanno conti con i birapporti fino a dim che se $OT \cap k = \{?, U'\}$ con U' + lontano da AC

$\Rightarrow (S, T, U, U') = -1$

+ $AC = pol(T) \Rightarrow U \in k$.

Senior 2013 N1 – Medium

SIMONE DI MARINO

IMO 2009/1 (CONGRUENZE)

Sia $n>0$ e $a_1, a_2, \dots, a_k$ ($k \geq 2$) interi distinti nell'insieme $\{1, 2, \dots, n\}$ (tutti e soli i residui modulo n) tali che

$$n \mid a_i(a_{i+1}-1) \qquad (i=1,2,\dots,k-1)$$

Dimostrare che $n \nmid a_k(a_1-1)$.

Dim. Proviamo a scrivere i dati sotto forma di congruenze (mod n). $1 \leq a_1, \dots, a_k \leq n$ e distinti, in particolare $a_1 \not\equiv a_2 \pmod n$,

l'altra ipotesi si scrive come

$$a_i(a_{i+1}-1) \equiv 0 \pmod n$$

$$a_i a_{i+1} - a_i \equiv 0 \pmod n$$

$$a_i a_{i+1} \equiv a_i \pmod n \qquad \forall\, i=1,\dots,k.$$

$$a_1 \equiv a_1 a_2 \qquad a_2 \equiv a_2 a_3 \qquad a_3 \equiv a_3 a_4 \quad \dots \quad a_{k-1} \equiv a_{k-1} a_k$$

$$a_1 \equiv a_1 a_2 \equiv a_1 a_2 a_3 \equiv a_1 a_2 a_3 a_4 \equiv \dots \equiv a_1 a_2 a_3 \dots a_{k-1} a_k$$

Suppl. per assurdo che $a_k a_1 \equiv a_k \pmod n$

$$a_2 \equiv a_2 a_3 \equiv a_2 a_3 a_4 \equiv \dots \equiv a_2 a_3 a_4 \dots a_{k-1} a_k \equiv$$

$$\equiv a_2 a_3 a_4 \dots a_{k-1} a_k a_1$$

Quindi avremmo che $a_2 \equiv a_1 \pmod n$. ↯

- Supponete che n sia primo. Poi. $n = pq$. ecc...

Polinomi in $\mathbb{Z}/p\mathbb{Z}$

$\mathbb{Z}/p\mathbb{Z} = \{0, 1, \dots, p-1\}$

~~$\mathbb{Z}_p$~~

① $p(x)$ polinomio di grado d, ha al più d radici. ($a \neq 0,\ b \neq 0 \Rightarrow ab \neq 0$)

② $\exists\ q(x)$ tale che $q(x) \neq 0$ come polinomio ma $q(i) = 0\ \forall\ i$

$q(x) = x^{p-1} - 1$ ⟶ $(0) \equiv -1 \pmod p$, $(1) \equiv 0 \pmod p$, $(2) \equiv 0 \pmod p$, ⋮ ← (LFT, PTF)

$q(x) = x^p - x$

$\Rightarrow q(0) \equiv q(1) \equiv q(2) \equiv \dots \equiv q(p-1)$

Se $r(0) \equiv r(1) \equiv \dots \equiv r(p-1) \equiv 0 \pmod p$

in $\mathbb{Q} \Rightarrow r(x) = x(x-1)(x-2)\cdots(x-(p-1)) \cdot q(x) + r_1(x)$

$r_1(x)$ ha tutti coeff. multipli di p

$r(x) \equiv x(x-1)\cdots(x-(p-1))\, q(x)$

↳ polinomio monico di grado p che ha come radici $\{0, 1, \dots, p-1\}$

$\equiv (x^p - x)\, q(x)$

Sia $q(x)$ un polinomio di grado $\leq p-2$.
Dimostrare che $q(0)+q(1)+\dots+q(p-1)\equiv 0 \pmod p$.

Step I Basta dimostrarlo per $q_m(x)=x^m$:
supponiamo sia vero per essi

$$q(x)=a_d x^d + a_{d-1}x^{d-1} + \dots + a_1 x + a_0$$

$$\sum_{i=0}^{p-1} q(i) \equiv \Big(a_d\cdot 0^d + a_{d-1}\cdot 0^{d-1} + \dots + a_1\cdot 0 + a_0\Big) + \Big(a_d\cdot 1^d + a_{d-1}\cdot 1^{d-1} + \dots + a_1\cdot 1 + a_0\Big) + \Big(a_d\cdot 2^d + a_{d-1}\cdot 2^{d-1} + \dots + a_1\cdot 2 + a_0\Big) + \vdots + \Big(a_d\cdot (p-1)^d + a_{d-1}\cdot (p-1)^{d-1} + \dots + a_1(p-1) + a_0\Big)$$

$$\equiv \underbrace{a_d\cdot 0 + a_{d-1}\cdot 0 + \dots + a_1\cdot 0 + a_0\cdot 0}_{(p-1)\text{ volte}}$$

$$\equiv 0.$$

Step II $0^m + 1^m + 2^m + \dots + (p-1)^m \equiv 0 \pmod p$.

(a) sia g un generatore modulo p $\left(g^{p-1}\equiv 1 \pmod p,\ g^k \not\equiv 1 \pmod p,\ k<p-1\right)$

$$\{g^0, g^1, \dots, g^{p-2}\} = \{1, \dots, p-1\}$$

$$\sum_{i=1}^{p-1} i^m \equiv \sum_{k=0}^{p-2} \left(g^k\right)^m = \sum_{k=0}^{p-2} \left(g^m\right)^k = \frac{\left(g^m\right)^{p-1}-1}{g^m-1} \equiv 0 \pmod p$$

poiché $1 \le m \le p-2$, so che $g^m \not\equiv 1$ (g generatore)

$(g^{p-1})^m \equiv 1$.

(b) $\{1, 2, \dots, p-1\} = \{a, 2a, 3a, \dots, a(p-1)\}$

$(a,p)=1$ so che $a \not\equiv 0$, $2a \not\equiv 0$, $\dots$, $a(p-1) \not\equiv 0$ (mod p); $ia \not\equiv ja$ se $i \not\equiv j$

$S_m = 1^m + 2^m + \dots + (p-1)^m \equiv a^m + (2a)^m + \dots + ((p-1)a)^m$

$S_m \equiv a^m S_m \quad (p) \quad \forall (a,p)=1$

$S_m (a^m - 1) \equiv 0 \quad (p)$

Fatto: se $1 \le m \le p-2$ $\exists\, a$ t.c. $a^m \not\equiv 1 \ (p)$

ad esempio è vero per $a = g$.

Esistenza di un generatore (mod. p) (p primo)

Sia x tale che $x^{24} \equiv 1 \ (61)$.

è vero che $x^{36} \equiv 1 \ (61)$?

$\mathrm{ord}_{61}(x)$?

$$\mathcal{O}_x = \{ k \mid x^k \equiv 1 \pmod 61 \}$$

$0 \in \mathcal{O}_x$ $\qquad$ $60 \in \mathcal{O}_x$ $\Leftarrow$ piccolo teorema di fermat.

$k \in \mathcal{O}_x \Rightarrow 2k \in \mathcal{O}_x,\ 3k \in \mathcal{O}_x \dots$

$k, j \in \mathcal{O}_x \Rightarrow k+j \in \mathcal{O}_x$

$x^k \equiv 1 \quad x^j \equiv 1 \Rightarrow x^{k+j} \equiv 1$

$$\mathcal{O}_x = \{0, m, 2m, 3m, \dots\}$$

$m = ord_{61}(x)$

Sia m il minimo di $\mathcal{O}_x \setminus \{0\}$.

$\mathcal{O}_x$, dato $n \in \mathcal{O}_x$ $\qquad$ $n = qm + r$

$$1 \equiv x^n \equiv x^{qm+r} \equiv x^{qm} \cdot x^r = (x^m)^q \cdot x^r$$

$$\equiv x^r \pmod 61 \qquad r \in \mathcal{O}_x$$

$0 \le r < m \Rightarrow r = 0. \Rightarrow m \mid n.$

$x^k \equiv 1 \pmod 61 \Rightarrow ord_{61}(x) \mid k$

$x^{60} \equiv 1 \pmod 61 \qquad ord_{61}(x) \mid 60$

$x^{24} \equiv 1 \quad (61) \qquad ord_{61}(x) \mid 24$

$\star\ x^{12} \equiv 1 \quad (61) \qquad ord_{61}(x) \mid 60 \qquad \Rightarrow ord_{61}(x) \mid (24,60) = 12$

$x^{36} \equiv 1 \quad (61)$? Sì perché $(x^{12})^3 \equiv 1^3 \equiv 1$.

$31 \mid x^{19} - y^{19} \Rightarrow 31 \mid x^9 - y^9 \qquad \mid 30$

$\left(\frac{x}{y}\right)^{19} \equiv 1 \quad (31) \Rightarrow ord_{31}\left(\frac{x}{y}\right) \mid 19 = 1$.

$ord_p(a) = k \qquad ord_p(b) = j$

$ord_p(ab) \overset{?}{=} mcm$

$\boxed{b = a^{-1}}$

$ord_p(a) = k \qquad ord_p(a^{-1}) = k \qquad ord_p(\underbrace{a \cdot a^{-1}}_{1}) = 1$

$(ab)^{mcm(k,j)} \equiv a^{mcm(k,j)} \cdot b^{mcm(k,j)} \equiv 1 \cdot 1 \equiv 1 \quad (p)$

$m = ord_p(ab) \mid mcm(ord_p(a), ord_p(b))$

$(ab)^{mj} \equiv 1^j = 1^j \qquad ord_p(a) \mid mj$

$a^{mj} \cdot b^{mj} \equiv a^{mj} \cdot (b^j)^m \equiv a^{mj}$

$k \mid m$, $j \mid m$ $\quad$ $\mathrm{mcm}(k,j) \mid m$ $\quad$ $\mathrm{MCD}(k,j)$

$k^2 \mid mjk$, $j^2 \mid mjk$ $\Rightarrow$ $\mathrm{mcm}(k^2, j^2) \mid mjk$

$\mathrm{mcm}(k,j)^2 \mid mjk$

$jk = \mathrm{mcm}(j,k)\,\mathrm{MCD}(j,k)$ $\quad$ $\mathrm{mcm}^2 \mid m \cdot \mathrm{mcm} \cdot \mathrm{MCD}$

$\left(p^a \cdot p^b = p^{\max\{a,b\}} \cdot p^{\min\{a,b\}} \right)$ $\quad$ $\frac{\mathrm{mcm}}{\mathrm{MCD}} \mid m$

Th. $\quad \frac{\mathrm{mcm}}{\mathrm{MCD}} \mid \mathrm{ord}_p(ab) \mid \mathrm{mcm}$

Corollario

in particolare se $\mathrm{MCD}\left(\mathrm{ord}_p(a), \mathrm{ord}_p(b)\right) = 1$

allora $\mathrm{ord}_p(ab) = \mathrm{mcm} = \mathrm{ord}_p(a) \cdot \mathrm{ord}_p(b)$.

Esercizio $\quad a, b$ coprimi con p, mostrare che $\exists\ c$ coprimo con p tale che

$\mathrm{ord}_p(c) = \mathrm{mcm}\left(\mathrm{ord}_p(a), \mathrm{ord}_p(b)\right)$.

Caso facile $\quad \left(\mathrm{ord}_p(a), \mathrm{ord}_p(b)\right) = 1$ so che

$c = ab$ risolve per il Cor. precedente.

$c = a^i b^h$ $\quad \to \left(\mathrm{ord}_p(a^i), \mathrm{ord}(b^h)\right) = 1$

$\to$ ok $\mathrm{ord}_p(a^i) \cdot \mathrm{ord}(b^h) = \mathrm{mcm}(k,j)$

$$\frac{\mathrm{ord}_p(a)}{(\mathrm{ord}_p(a), i)} = \mathrm{ord}_p(a^i) \begin{cases} \mathrm{ord}_p(a) & (i, \mathrm{ord}_p(a)) = 1 \\ \frac{\mathrm{ord}_p(a)}{i} & (i \mid \mathrm{ord}_p(a)) \end{cases}$$

$$m = \mathrm{ord}_p(a^i) = \min\{ n : (a^i)^n \equiv 1 \ (p) \}$$

$$= \min\{ n : a^{in} \equiv 1 \ (p) \}$$

$$\min\{ n : \mathrm{ord}_p(a) \mid in \}$$

$$m = \frac{\mathrm{ord}_p(a)}{(\mathrm{ord}_p(a), i)}.$$

$M = \{$ il più grande intero che sia ordine moltiplicativo per qualche $x \bmod p \}$

$$= \max\{ \mathrm{ord}_p(x) : x \in 1, \dots, p-1 \} = \mathrm{ord}_p(g)$$

Cor. $x^M \equiv 1 \ (p) \quad \forall \ x \in 1, \dots, p-1.$

supp. per assurdo che $\exists\ y$ t.c.

$y^M \not\equiv 1 \ (p)$ $\quad \mathrm{ord}_p(g) \nmid M$

$\mathrm{mcm}(\mathrm{ord}_p(g), \mathrm{ord}_p(g)) > M$

$\mathrm{ord}_p(c)$ $\quad \mathrm{ord}_p(c) > M$ assurdo.

$q(x) = x^M - 1$ ha per radici $1, 2, 3, \dots, p-1$

$\Rightarrow \quad M \geq p-1 \qquad M \leq p-1$ (piccolo Th. di Fermat)

$\Rightarrow \quad M = p-1 \rightsquigarrow \operatorname{ord}_p(g) = p-1$ (generatore)

$\{1, g, g^2, \dots, g^{p-2}\} = \{1, 2, \dots, p-1\}$

piccolo th. di fermat: $x^{p-1} \equiv 1 \ (p) \quad \forall \ x = 1, \dots, p-1$

$\operatorname{ord}_p(x) \mid p-1$

$\leq p-1.$

$n < p \leq \frac{4n+3}{3} \Rightarrow p \mid \sum_{i=0}^{n} \binom{n}{i}^4$

$n = p-1 \qquad \binom{p-1}{i} = \frac{(p-1)\cdot(p-2)\cdot(p-3)\cdots(p-i)}{1 \cdot 2 \cdot 3 \cdots i} \equiv$

$\equiv \frac{(-1)}{1} \cdot \frac{(-2)}{2} \cdot \frac{(-3)}{3} \cdots \frac{(-i)}{i} = (-1)^i \ (p)$

$\sum_{i=0}^{p-1} \left((-1)^i\right)^4 = p \equiv 0 \quad (p) \quad . \quad \text{ok.}$

$n = p-2 \qquad \binom{p-2}{i} = \frac{(p-2)(p-3)\cdots(p-i-1)}{1 \cdot 2 \cdot 3 \cdots i} = (-1)^i (i+1)$

$$\sum_{i=0}^{p-2} \binom{p-2}{i}^4 = \sum_{i=0}^{p-2} (\quad (i+1)\quad)^4 = \sum_{i=0}^{p-1} q(i) \equiv 0 \ (p)$$

$\deg q \leq p-2$ se ≤ 5

$$p \leq \frac{4(p-2)+2}{3} \Rightarrow 3p \leq 4p - 6$$

$6 \leq p$

$n = p - r$

$$\binom{p-n}{i} = \frac{(p-r)(p-r-1)\cdots(p-r-i+1)}{1 \cdot 2 \cdot 3 \cdots r-1 \cdot \cdots i} \equiv$$

$$\equiv (-1)^i \frac{(p-i-1)(p-i-2)\cdots(p-i-(r-1))}{1 \cdot 2 \cdot 3 \cdots (r-1)} \equiv (-1)^i q_r(i)$$

$$\sum_{i=0}^{p-r} \binom{p-r}{i}^4 \equiv \sum_{i=0}^{p-r} q_r(i)^4 = \sum_{i=0}^{p-1} q_r(i)^4 \overset{?}{\equiv} 0$$

$\deg q_r^4 = 4(r-1)$

$$4(r-1) \overset{?}{\leq} p-2$$

$$p \leq \frac{4n+2}{3} \qquad p \leq \frac{4(p-r)+2}{3}$$

$$3p \leq 4p - 4r + 2$$

$4(r-1) \leq p-2$ ok.

Lifting the exponent lemma.

Lemma (LTE) Sia p un primo dispari e siano a, b numeri interi coprimi con p. Allora se $p \mid a-b$ allora

$$v_p(a^{p^k} - b^{p^k}) = v_p(a-b) + k$$

altrimenti $v_p(a^{p^k} - b^{p^k}) = 0$.

Def. (valutazione p-adica) Dato un primo p e un intero a, si definisce $k = v_p(a)$ il massimo numero naturale tale che $p^k \mid a$

Esempi:

$v_2(10) = 1$ $\quad$ $v_3(1001) = 0$

$v_5(100) = 2$ $\quad$ $v_3(1010102) = 1$

$v_7(49^3) = 6$

nei razionali $\quad v_2\left(\frac{1}{10}\right) = -1 \quad v_2\left(\frac{1}{1000}\right) = -3$

$v_5\left(\frac{17}{9}\right) = 0$

Proprietà di v_p: • $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$

• $v_p(a \cdot b) = v_p(a) + v_p(b)$

Dim. $(a^{p^k} - b^{p^k}) = (a-b)(\text{Mostriciattolo})$

chiaramente $v_p(a^{p^k} - b^{p^k}) \geq v_p(a-b)$

$k=1$ $\quad a^p - b^p = (a-b)(a^{p-1} + a^{p-2}\cdot b + \cdots + b^{p-2}\cdot a + b^{p-1})$

So che $a \equiv b \ (p)$ $\quad a^{p-1} + a^{p-1} + \cdots + a^{p-1} =$

$= p \cdot a^{p-1} \equiv 0 \ (p)$

Ah! Ma allora $v_p(a^p - b^p) \geq v_p(a-b) + 1$

$a = b + kp^s$ $\quad$ (dove $(k,p) = 1$)

$a - b = k \cdot p^s$ $\quad s = v_p(a-b)$

$$a^p - b^p = (b + kp^s)^p - b^p =$$

$$= p \cdot (kp^s) \cdot b^{p-1} + \underbrace{\binom{p}{2} (kp^s)^2 \cdot b^{p-2} + \cdots}_{\text{multiplo di } p^{s+2}}$$

$\frac{p(p-1)}{2} \cdot p^{2s} \cdot k^2 \cdot b^{p-2}$

$p^{s+1} \cdot p^s$

$$= p^{s+1} \cdot k' + p^{s+2} \cdot k'' =$$

$$= p^{s+1}(k' + p \cdot k'')$$

sicuramente NON ha fattori p.

$$v_p(a^p - b^p) = v_p(a-b) + 1$$

Per induzione: $v_p(a^{p^k} - b^{p^k}) = v_p(a-b) + k$

(a, b sono coprimi con p e $p \mid a-b$)

[$p=2$] $v_p(a^{2^k} - b^{2^k}) = v_p(a^2 - b^2) + k - 1$

$= v_p(a-b) + v_p(a+b) + k - 1$

Teo Sia g generatore modulo p tale che $p^2 \nmid g^{p-1} - 1$. Allora g è generatore modulo p^k $\forall k$.

Esempio 2 mod 5

$25 \nmid 2^4 - 1 = 15$

$2_2 = 2$
$2^2 = -1$
$2^3 = 3$
$2^4 = 1$

(anche 3 è generatore)

$\rightsquigarrow$ 2 e' generatore modulo 5^k per ogni k.

Dim. Voglio stabilire $\text{ord}_{5^k}(2)$. So che $\text{ord}_{5^k}(2) \mid \varphi(5^k)$ (teo eulero)

$$x^{\varphi(n)} \equiv 1 \pmod{n} \qquad \forall \quad (x,n) = 1$$

$$\Rightarrow \quad \mathrm{ord}_n(x) \mid \varphi(n)$$

$$\mathrm{ord}_{5^k}(2) \mid 5^{k-1} \cdot 4$$

$$\mathrm{ord}_5(2) \mid \mathrm{ord}_{5^k}(2) = m_k \qquad 2^{m_k} \equiv 1 \pmod{5^k}$$

$$2^{m_k} \equiv 1 \pmod{5}$$

$$4 \mid \mathrm{ord}_{5^k}(2) \mid 5^{k-1} \cdot 4 \qquad \Rightarrow \mathrm{ord}_5(2) \mid m_k$$

$$\mathrm{ord}_{5^k}(2) = 5^s \cdot 4 \qquad s \text{ lo dobbiamo trovare}$$

$$s \le k-1$$

$$v_5\left(2^{5^s \cdot 4} - 1\right) = v_5\left(\left(2^4\right)^{5^s} - (1)^{5^s}\right) =$$

$$\overset{\text{LTE}}{=} v_5\left(2^4 - 1\right) + s = s+1$$

$$2^{5^s \cdot 4} \equiv 1 \pmod{5^k}$$

$$5^k \mid 2^{5^s \cdot 4} - 1 \qquad v_5\left(5^k\right) \le v_5\left(2^{5^s \cdot 4} - 1\right)$$

$$s \ge k-1 \quad \Leftarrow \quad k \le s+1$$

$$s = k-1 \quad \Rightarrow \quad \mathrm{ord}_{5^k}(2) = 5^{k-1} \cdot 4 = \varphi\left(5^k\right)$$

$\Rightarrow$ 2 è generatore.

Cor. Esistenza di un generatore modulo p^2.

g generatore mod p t.c. $p^2 \mid g^{p-1} - 1$

Ese. $(g+p)$ è generatore mod p

e $(g+p)^{p-1} \not\equiv 1 \quad (p^2)$.

$4p^k$ NON può avere generatori

perché $\operatorname{ord}_{nm}(x) = \operatorname{mcm}(\operatorname{ord}_n(x), \operatorname{ord}_m(x))$

quando n, m sono coprimi

in particolare $\operatorname{ord}_{4p^k}(x) \mid \varphi(p^k) \neq \varphi(4p^k)$

$= 2\varphi(p^k)$

p q dispari $\operatorname{ord}_{pq}(x) \mid \dfrac{(p-1)(q-1)}{2}$.

Residui modulo p:

residui quadratici

quanti sono? (esclusi lo 0, $\frac{p-1}{2}$) $\frac{p+1}{2}$

0^2 1^2 2^2 3^2 4^2 - - - $(p-2)^2$ $(p-1)^2$

$a^2 \equiv b^2 \ (p) \iff p \mid (a-b)(a+b)$? $a \equiv b \ (p)$ oppure $a \equiv -b \ (p)$

i residui quadratici sono $\frac{p+1}{2}$ e sono esattamente

$0 \quad (\pm 1)^2 \quad (\pm 2)^2 \quad \dots \quad \left(\pm \frac{p-1}{2}\right)^2$

Come faccio a sapere se a è un residuo quadratico?
- criterio di Eulero
- simbolo di Jacobi

Se $a \equiv b^2 \ (p)$ a residuo quadratico

$a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \ (p) \Rightarrow a^{\frac{p-1}{2}} \equiv 1 \ (p)$

(I) a non è un residuo quadratico, allora $a = g^k$ k per forza dispari

$a^{\frac{p-1}{2}} \equiv g^{\frac{k(p-1)}{2}} \not\equiv 1$ $\quad p-1 \nmid \frac{k(p-1)}{2}$

$\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 \Rightarrow a^{\frac{p-1}{2}} \equiv -1 \ (p)$

(II) $X^{\frac{p-1}{2}} - 1 = q(x)$ ha al più $\frac{p-1}{2}$ radici.

So che i residui quadratici sono radici ma allora non ce ne sono altre e quindi se a non

a è residuo $a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$ $\left(\equiv -1\right)$.

-1 è res. quadratico $\iff (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{se } 4 \mid p-1 \\ -1 & \text{altrimenti} \end{cases}$

p primo dispari $(a,p)=1$ (simbolo di Jacobi)

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \text{ è res. quadratico} \\ -1 & \text{se } a \text{ NON è res. quad.} \end{cases}$$

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Almeno uno tra 2, 3 e 6 è residuo quadratico modulo p.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

rec. quadratica $(p,q$ primi$)$ $\qquad \left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

$$\left(\frac{1787}{61}\right) = \left(\frac{-43}{61}\right) = \left(\frac{18}{61}\right) = \cancel{\left(\frac{3}{61}\right)\left(\frac{3}{61}\right)}\left(\frac{2}{61}\right) = (-1)^{\frac{61^2-1}{8}} = -1$$

$$\left(\frac{3}{61}\right) = \left(\frac{61}{3}\right) \cdot = \left(\frac{1}{3}\right) = 1.$$

$$2 \cdot 4 \cdot 6 \cdot 8 \cdot \cdots \frac{p-1}{2} \cdot \frac{p+3}{2} \cdots p-1 =$$

$$P = 2 \cdot 4 \cdot 6 \cdot 8 \cdot \cdots (p-1) =$$

$$= 2^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)$$

$$= 2 \cdot 4 \cdot \cdots \frac{p-1}{2} \cdot \left(\frac{p+3}{2} \cdots 1\right) \cdot (-1)^{\left\lfloor \frac{p-1}{4} \right\rfloor}$$

$$= \left(\frac{p-1}{2}\right)!$$

$$2^{\frac{p-1}{2}} \equiv (-1)^{\left\lfloor \frac{p-3}{4} \right\rfloor} \cdot$$

$\frac{p^2-1}{8}$ pari se $p \equiv \pm 1 \ (8)$

dispari se $p \equiv \pm 3 \ (8)$

TdN 2 : (10) $D = \{ n \in \mathbb{N} : n \mid 2^n + 1 \}$

a) determinare tutti i primi p che stanno in D.

$p+f \qquad x^p \equiv x \ (p)$

$p \mid 2^p + 1 \equiv 2 + 1 = 3 \qquad p \mid 3$

$p = 3$ va bene $\qquad 3 \mid 9$

(b) Determ potenze di primi che sono in D

$$p^k \mid 2^{p^k}+1 \qquad 2^p+1 \mid 2^{p^k}+1$$

$$0 \equiv 2^{p^k}+1 \equiv \left(2^{p^{k-1}}\right)^p+1 \equiv 2^{p^{k-1}}+1 \dots \equiv 2+1 \ (p)$$

$p=3$

$$\left(x^{p^2}=\left(x^p\right)^p \equiv x^p \equiv x\right)$$

$$3^k \mid 2^{3^k}+1 = 2^{3^k}-(-1)^{3^k}$$

vogliono i k t.c. $k \le v_3\left(2^{3^k}-(-1)^{3^k}\right) =$

$$= v_3(2-(-1))+k = k+1$$

$\forall k$. $\quad D \supseteq \{3, 3^2, 3^3, \dots\}$.

(c) $n = pq$

$$pq \mid 2^{pq}+1$$

$$2^{pq} \equiv -1 \ (p) \qquad 2^{pq} \equiv -1 \ (q)$$

$$(2^p)^q \equiv 2^q \equiv -1 \ (p) \qquad 2^p \equiv -1 \ (q)$$

$2^{2q} \equiv 1 \ (p)$ $\qquad$ $2^{2p} \equiv 1 \ (q)$

$\text{ord}_p(2) \mid 2q$ $\qquad$ $\text{ord}_q(2) \mid 2p$

$\text{ord}_p(2) \nmid q$ $\qquad$ $p \leq q$

$\text{ord}_p(2) \mid p-1$ $\qquad$ $\text{ord}_p(2) \mid (2q, p-1)$

$(2, p-1) = 2$

$\text{ord}_p(2) = 2$

$2^2 - 1 \equiv 0 \ (p)$

$3 \equiv 0 \ (p)$

$3 = p$

$3 \mid 2^q + 1$ $\qquad$ $q \mid 2^3 + 1 = 9$ $\qquad$ $q = 3$

(c): unico è q

(d):

$n = p^s \cdot A$ $\qquad$ p è il più piccolo primo che divide n

$p^s A \mid 2^{p^s A} + 1$ $\qquad$ $2^{p^s A} \equiv -1 \ (p)$

$\text{ord}_p(2) \mid (2p^s A, p-1) \iff$ $\qquad$ $2^{2p^s A} \equiv 1 \ (p)$

2

$2^2 - 1 \equiv 0 \ (p) \Rightarrow p = 3$

(e) $n = p^2 q$

$p=3 \rightarrow n = 9q$

$q=3 \rightarrow n = 3p^2$

$9q \mid 2^{9q}+1$ $\quad 27 \cdot 19$

$q \mid 2^{9q}+1 \equiv 2^9+1$ $\quad 11$

$q = 19$

[e si verifica che funziona]

$3p^2 \mid 2^{3p^2}+1$

$p \mid 2^{3p^2}+1 \equiv 2^3+1 = 9$ $\quad p=3$ ☺.

Senior 2013 - N2 medium

Titolo nota 06/09/2013

"Lemma del guadagno di un primo" LGP

$$x^p - 1 = (x-1)\left(1 + x + x^2 + \cdots + x^{p-1}\right) = (x-1)f(x)$$

$f(n)$ $\qquad n^p \equiv 1 \pmod q$

$\Downarrow !$

$q \mid f(n)(n-1)$

$f(x) = 1 + x + \cdots + x^{p-1}$

$f(n)$ ha come divisori primi solo $\begin{cases} p \\ q \equiv 1 \pmod p. \end{cases}$

$f(1) = p$ può capitare

$q \mid f(n) \Rightarrow q \mid n^p - 1 \Rightarrow n^p \equiv 1 \pmod q$

$\operatorname{ord}_q n \begin{cases} 1 \to n \equiv 1 \bmod q \to f(1) = p \text{ e simili,} \\ p \qquad p = q \end{cases}$

ma $\operatorname{ord}_q n \mid \varphi(q) = q-1$

$\Rightarrow p \mid q-1 \Rightarrow q \equiv 1 \pmod p$

e $q^2 \mid f(n)$? $\qquad q = p$ no

$n \equiv 1 \pmod p \qquad n = kp+1$

$$1 + (kp+1) + (kp+1)^2 + \cdots + (kp+1)^{p-1} =$$

$$= \overbrace{(1+1+\cdots+1)}^{p} + k(1+2+3+\cdots+p-1)p + Np^2 =$$

$$= p + kp \cdot p\frac{p-1}{2} + Np^2 = p + \left(k\frac{p-1}{2} + N\right)p^2 \equiv$$

se $p>2$

$$\equiv p \pmod{p^2}.$$

$q \equiv 1 \pmod p$? Era necessario prima, quindi anche adesso.

$\exists$ el. di ordine $p \pmod q$ $\left[q \equiv 1 \pmod p\right]$?

prendo g generatore mod q

$g^{q-1} \equiv 1 \pmod q$ $\quad g^k \not\equiv 1 \pmod q$ con $0<k<p-1$

$p \mid q-1$ $\quad g^{\frac{q-1}{p}} \not\equiv 1$ $\quad \frac{q-1}{p} < q-1$

a

$a^p \equiv g^{q-1} \equiv 1$ quanti sono questi elementi

x che mod q fanno $x^p \equiv 1 \pmod q$?

$g^{\frac{q-1}{p}} = a_1$ $\quad (p>2)$ $\left[g^{\left(\frac{q-1}{p}\right)}\right]^2 \equiv g^{2\frac{q-1}{p}} \equiv a^2$

$(a_1^2)^p \equiv (a_1^p)^2 \equiv 1 \pmod q$ $\quad a_1^i$ $\quad i=1,\ldots,p-1$

Come risolvendo $\quad p \cdot x \equiv 0 \pmod{q-1}$

$(g^x)^p \equiv g^{xp} \equiv g^{(q-1)k'} \equiv 1$ $\quad x = k\frac{q-1}{p}$ $\quad k = \overset{No}{0},\ldots,p-1$

E se volessi a_2 t.c. $a_2^p - 1 \equiv 0 \pmod{q^2}$?

$(\mathbb{Z}/q^2\mathbb{Z})^*$ ha un generatore ($\to$ un sistema di generatori fatto da 1 solo elemento)

g_2 sia il generatore. $(g_2^x)^p \equiv 1 \pmod{q^2}$

$g_2^{\frac{q(q-1)}{p}} \equiv a_2 \not\equiv 1 \quad a_2^p \equiv 1 \pmod{q^2}$

$g_2^k \not\equiv 1 \quad k < q(q-1) = \varphi(q^2)$.

Così per trovare a_k t.c. $a_k^p \equiv 1 \pmod{q^k}$

LGP

x intero

$x^p - 1 = (x-1) f(x)$ Allora $\exists$ un divisore primo di $f(x)$ che non divide $x-1$ a meno che non sia $3^2 - 1 = (3-1)(3+1)$.

Dim. $q \mid f(x)$ e $q \mid x-1$ $\quad q \equiv 1 \bmod p$ o $q = p$

$x \equiv 1 \pmod q$

$q \mid f(x) \equiv 1 + (1+kq) + \dots \quad (1+kq)^{p-1} \equiv p$

$q = p \qquad (x-1) \nmid f(x) \qquad (x-1) = p^a$

$f(x) = p^b$

$p \mid f(x) \Rightarrow f(x) \equiv p \pmod{p^2} \Rightarrow f(x) = p \quad b = 1$

$(x-1) = p^a$ $f(x) = p$ $\quad p=2 \to (3-1)(3+1)$

$p \neq 2 \quad a = 0$ ass.

Conclusione: da $x-1$ a x^p-1 si "guadagna" almeno un nuovo divisore primo.

Polinomi a coeff. interi visti in $\mathbb{Z}/p\mathbb{Z}$.

① $f(x)$ non può assumere solo valori primi.

$f(0)=0$ no $\quad f(0) = p \quad f(p) = p \cdot g(p)$ composto $g \neq 1$

② $S = \{ p_i \text{ primi} \mid \exists n \; p_i \mid f(n) \}$ deve essere infinito

$f(0)=0 \quad f(x) = x \cdot g(x) \quad x = p_i$

$f(0) = 1$ Se $\overline{p} = \max S \quad f(\overline{p}!) = N \cdot \prod_{p_i \in S} p_i + 1$

$\Rightarrow p_i \nmid f(\overline{p}!)$ per nessun i

$f(0) = a \quad f(ax) = c_n a^n x^n + c_{n-1} a^{n-1} x^{n-1} + \cdots + c_1 ax + a =$

$= a \cdot g(x) \quad g(0) = 1$ e mi riduco al caso precedente

③ $\forall f(x)$ polinomio $\exists$ infiniti p primi t.c.

$f(x)$ in $\mathbb{Z}/p\mathbb{Z}$ ha una radice.

$\exists \infty \, p$ t.c. $\exists n \; p \mid f(n) \iff f(\overline{n}) \equiv 0 \pmod p$

Oss. pol. ciclotomico di grado n $= \Phi_n(x)$ = pol. che ha come radici tutte le radici primitive n-esime dell'unità $\quad \lambda^h = 1 \quad \lambda^k \neq 1 \quad k < n$

$\Phi_n(x)$ ha coeff. interi (non sempre 0 e 1)

$$x^p - 1 = (x-1)\,\Phi_p(x)$$

$$x^h - 1 = \Phi_n(x) \cdot \Phi_{d_1}(x)\,\Phi_{d_2}(x) \cdots \Phi_1(x) = \prod_{d \mid n} \Phi_d(x) \qquad (x-1 = \Phi_1(x))$$

Equazioni diofantee di secondo grado in due variabili

- 1 var.: $ax^2 + bx + c \equiv 0 \pmod p$
  - $x^2 \equiv a$ / a res. quadr. risolubile / a non lo è, no.
  - Δ / è res. quadr. risolubile / non lo è, no.

$$ax^2 + bxy + cy^2 + dx + ey + f$$

$$x^2 + ay^2 = f$$

- $a > 0$ — # fin. di soluzioni se ci sono
- $a = -b^2$ $\quad (x - by)(x + by) = f$

  Fattorizzo $f = f_1 \cdot f_2$ e faccio molti conti facili
- $a < 0$ — $-a$ non quadrato ?

$x^2 - 2y^2 = 1$ è antica $\quad x^2 - ay^2 = b$

① $b = 1 \qquad \lambda \in \mathbb{C}$ t.c. $\lambda^2 = -a$

$x^2 + \lambda^2 y^2 = b \qquad x^2 + \lambda^2 y^2 = \|(x, \lambda y)\|^2$.

$\mathbb{Z}[\sqrt{-a}] = \mathbb{Z}[\lambda]$

Caso paradigmatico $\lambda = i$

$x^2 - y^2 = b \qquad x^2 + y^2 = b$

$\| \quad (x+iy)(x-iy) = b$

$\mathbb{Z}[i]$ = interi di Gauss. Ma come funziona la fattorizzazione negli interi di Gauss?

(Devo fattorizzare anche b in $\mathbb{Z}[i]$)

$2 = (1+i)(1-i)$

2 non è irriducibile $\Leftrightarrow$ non si può scrivere come $a \cdot b$ a meno che a o b non siano invertibili (in $\mathbb{Z}$, ± 1)

Invertibili in $\mathbb{Z}[i]$?

2 non è primo $\Leftrightarrow 2 \mid a \cdot b \Rightarrow 2 \mid a$ o $2 \mid b$

primo $\Rightarrow$ irriducibile:

WLOG

$p = a \cdot b \Rightarrow p \mid a \cdot b \Rightarrow p \mid a \Rightarrow a = k \cdot p \Rightarrow p = k \cdot p \cdot b$

$\Rightarrow k \cdot b = 1 \Rightarrow b$ invertibile

~~$\leq$~~ non sempre vero

Fatt. in $\mathbb{Z}$ 1) dividendo, numero diminuisce

2) unicità a meno dell'ordine

$N(a+ib) = a^2+b^2 \in \mathbb{Z}_+$ $N((a+ib)(c+id)) = N(a+ib)\,N(c+id)$

Se $a+ib$ è invertibile? Sia $c+id$ l'inverso.

$N(a+ib)\,N(c+id) = N(1) = 1 \Rightarrow N(a+ib) = 1.$

Invertibili: $1, -1, i, -i$

$N(a+ib) = p$ e fattorizzassi $(a+ib) = z_1 \cdot z_2$

$p = N(z_1)\cdot N(z_2)$

$\Rightarrow$ o $N(z_1)=1$ o $N(z_2)=1 \Rightarrow$ o z_1 o z_2 è invert.

$\Rightarrow a+ib$ irriducibile. (= primo in $\mathbb{Z}[i]$)

$a+ib \in \mathbb{Z}$ $b=0$ a non primo $\rightarrow$ niente

$a=2 \rightarrow$ non primo $-i(1+i) = (1-i)$

$a=p$? Se $p = z_1 \cdot z_2$

$N(p) = N(z_1)\cdot N(z_2)$

$p^2 = N(z_1)\cdot N(z_2)$ $\begin{cases} N(z_1)=1 \\ N(z_2)=1 \end{cases}$ $p \rightarrow$ NON È FATTORIZ.

$N(z_1)=p$ $N(z_2)=p$ p

$N(z_1)=p$ $p = a^2+b^2$ $(a+ib)(a-ib)$

$a^2 \equiv -b^2 \pmod p$ $\left(\frac{a}{b}\right)^2 \equiv -1 \pmod p$

$\Leftrightarrow \left(\frac{-1}{p}\right) = 1$ Ma $\mathbb{Z}/p\mathbb{Z}^*$ ha $p-1$ elem. e un gen. g

$g^k \equiv -1 \Leftrightarrow g^{2k} \equiv 1 \quad g^k \not\equiv 1$

Voglio k pari $\Leftrightarrow 4 \mid p-1 \Rightarrow p \equiv 1 \pmod 4$

Se ora $\exists\ a \quad a^2 \equiv -1 \pmod p \qquad a^2+1 \equiv 0 \pmod p$

$(ka)^2 + k^2 \equiv 0 \pmod p \quad \forall k$

Tutti i $p \equiv 1 \pmod 4$ sono somme di due quadrati $\Rightarrow$ non sono primi in $\mathbb{Z}[i]$. Viceversa, $p \equiv 3 \pmod 4$ sono ancora primi. (Così, sono primi $1+i$ e $1-i$).

Fattorizzando, la norma diminuisce $\Rightarrow$ # finito di fattori.

2) Unicità? $\mathbb{Z}[\sqrt{-5}]$

$6 = 2 \cdot 3 = (1-\sqrt{-5})(1+\sqrt{-5})$

$e_{3,2} \neq (1-\sqrt{-5}) \cdot$ invertibile

Ma in $\mathbb{Z}[i]$ la fattorizzazione è unica

$\mathbb{Z}[\sqrt{-1}]$ (anche $\sqrt{-2}, \sqrt{-3}, \dots \sqrt{-163}$ 9 casi

$x^2+y^2=b \qquad b = 2^a \cdot \underbrace{p_1^{k_1} \dots p_e^{k_e}}_{\equiv 1 \pmod 4} \cdot \underbrace{q_1^{h_1} \dots q_n^{h_n}}_{\equiv 3 \pmod 4}$

$(x+iy)(x-iy) = (-i)^a (1+i)^{2a} \prod (c_j+id_j)^{k_j} (c_j-id_j)^{k_j} \cdot \prod q_j^{h_j} =$

$= (A+iB)(C+iD)$

in tutti i modi possibili (inclusi gli invertibili)

e con MOLTI conti e sistemi
trovo tutte le soluzioni

$x^2 - dy^2 = b \quad d>0 \qquad \mathbb{Z}[\sqrt{-d}]$

$\sqrt{-d} = \lambda \qquad x^2 + x^2 y^2$

$a + \sqrt{-d}\, b \qquad a^2 + d b^2 \qquad a^2 - d b^2$?

$x^2 - dy^2 = 1 \qquad N(z_1 \cdot z_2) = N(z_1) N(z_2)$

$(a+\sqrt{-d}\, b)(m + \sqrt{-d}\, n) =$

$(am - dbn) + \sqrt{-d}(an + bm)$

$a^2m^2 - 2dabmn + d^2b^2n^2 \pm = (am - dbn)^2 \pm d(an+bm)^2 \stackrel{?}{=}$

$(da^2n^2 + 2dabmn + db^2m^2) \pm \stackrel{?}{=} (a^2 \pm db^2)(m^2 \pm dn^2)$

$a^2m^2 \pm a^2dn^2 \pm db^2m^2 + d^2b^2n^2$

$x^2 - dy^2 = 1 \qquad x^4 - 2dy^2x^2 + d^2y^4 = 1$

$m^2 - dn^2 = 1$

$x^2m^2 + d^2n^2y^2 - dm^2y^2 - dn^2x^2 = 1$

$a^2 - db^2$?

$(x^2m^2 \pm 2dxymn + d^2n^2y^2) - d(m^2y^2 \mp 2xymn + n^2x^2)$

$(xm \pm dny)^2 - d(my \mp nx)^2$

sol.

$(x,y) \to (x+\sqrt{-d}\, y)(m + \sqrt{-d}\, n)$

$x \pm \sqrt{-d}\, y$

$(x,y) \to (x+\sqrt{-d}\, y)^k \to (x', y')$ che è ancora soluz.

$x^2 - dy^2 = a$
$m^2 - dn^2 = b$ $\longrightarrow (xm \pm dny)^2 - d(my \mp nx)^2 = ab.$

$(x, y, a)\ (m, n, 1) \longmapsto (x', y', a)$

Trovo così ∞ soluzioni, (tante quante quelle con 1) ma ATTENZIONE ci possono essere più famiglie infinite.

$x^2 - dy^2 = 1$ $\qquad a^2 - db^2 = k \qquad (m, 1, m^2 - d)$

$am + db,\ a + bm,\ k(m^2 - d)$

Se $am + db$ e $a + bm$ sono multipli di k,

$$\left(\frac{am + db}{k}, \frac{a + bm}{k}, \frac{m^2 - d}{k} \right)$$

Cerco m $\begin{cases} am + db \equiv a + bm \equiv 0 \pmod{k} \\ \dfrac{m^2 - d}{k} \text{ "piccolo"} \end{cases}$

Se $\dfrac{m^2 - d}{k} \neq 1$, lo rifaccio: Teo arrivo sempre.

Minimizzando la $N(z)$, le soluzioni di

$x^2 - dy^2 = 1$ sono potenze di una fondamentale.

Dopo ne trovo una particolare di

$x^2 - dy^2 = b$ e moltiplico.

Spesso è utile "stringere tra due quadrati"

Se $f:\mathbb{N}\to\mathbb{N}$ e $\forall n,m$ $nf(n)+2nm+mf(m)$ è un quadrato

Allora $f(n)=n$.

Dim [$f(n)=n$ va bene ovv.]

$a=p$ (primo) $b=0$ $\quad pf(p)$ è quadrato

$\Rightarrow p\mid f(p)$ $\quad f(p)=p\cdot g^2(p)$

$p,1$ $\quad pf(p)+2p+f(1)=a^2$

$p,2$ $\quad pf(p)+4p+2f(2)=b^2$ $\quad a\neq b$

$2p+2f(2)-f(1)=b^2-a^2\geq 2a+1>2\sqrt{2}p+1$

se $f(p)\neq p$ $\quad f(p)\geq 2p$ $\quad a,b\geq\sqrt{2}\cdot p$

per infiniti p!

$p>100^{100}$ $\quad \frac{2f(2)-f(1)}{\sqrt{2}}$ assurdo.

$2p+K>2\sqrt{2}p+1$

"Più piccolo primo"

$n=p_1^{a_1}\cdots p_k^{a_k}$

prendo il p_i più piccolo.

IMO 1990/3

Quando $\frac{2^n+1}{n^2}$ è intero?

n dispari

$2^n \equiv -1 \pmod n$ $\quad 2^{2n} \equiv 1 \mod n$

$\operatorname{ord}_n(2) \mid 2n$ $\quad n$ primo $= p$

$\operatorname{ord}_p(2) \mid (2p, p-1) \Rightarrow \begin{cases} 1 \\ 2 \end{cases}$

$p = 3$ $\quad \frac{2^3+1}{3^2} = 1$ $\quad \frac{2^1+1}{1} = 3$

$n = 3^k \cdot m$ $\quad 2^{3^k m} \equiv -1 \pmod{3^{2k} m^2}$

quando $3^a \parallel 2^{3^k m} + 1 ? = (2^{3^{k-1} m} + 1)\underbrace{(2^{2 \cdot 3^{k-1} m} - 2^{3^{k-1} m} + 1)}_{1 \text{ solo } 3}$

$a = k+1$ per induzione

$\Rightarrow$ le uniche sol. sono $k = 0, 1$

Tra gli altri, prendo il minimo primo p_i a parte 3

$\operatorname{ord}_{p_i}(2) \mid (2p_i, p_i - 1)$

$\Rightarrow$ solo poche scelte: 2^1-1 2^2-1 2^3-1 2^6-1
1 3 7 63
$7 \cdot 9$

ma modulo 7 non funziona

$\Rightarrow$ solo 3.

Teorema di Chevalley
"Vieta jumping" IMO 1988/6 $\frac{a^2+b^2}{1+ab}$ se è intero è quadr.