Stage Senior 2010 – Livello Medium

Stampato integrale delle lezioni

Autori vari

Indice

SENIOR 2010 – M. – PRELIMINARI

Titolo nota 05/09/2010

INDUZIONE CLASSICA $P(n) \Rightarrow P(n+1)$

INDUZIONE ESTESA $P(0), P(1), \dots, P(n) \Rightarrow P(n+1)$

PRINCIPIO MINIMO INTERO: $A \subseteq \mathbb{N}$, $A \neq \emptyset \Rightarrow \exists \min A$

Esempio 1 Esistenza della fattorizzazione (non unicità)

$n+1 \to$ o è primo

$\searrow$ o $n+1 = a \cdot b$ (più piccoli)

Idem sui polinomi.

Esempio 2 BEZOUT: Dati a, b e posto $d = (a,b)$

$\exists\, x, y$ t.c. $ax + by = d$

Dim.: induzione sul numero di divisioni euclidee.

Supponiamo wlog $a > b$. Allora

$a = qb + r$ Fatto generale: $0 \le r < b$

$d = (a,b) = (b,r)$

La coppia (b,r) produce d con una divisione in meno

$\bar{x}b + \bar{y}r = d$ per Hp induttiva

$$\bar{x}b + \bar{y}(a - qb) = d \qquad \underbrace{(\bar{x} - q\bar{y})}_{y} b + \bar{y} a = d$$

($\bar{y}$: x)

Se $a = b$, it's easy!

—o— o —

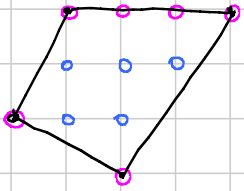
Esempio 3 Teorema di PICK.

Dato un poligono nel piano con vertici a coord. intere (anche non convesso), allora

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

I = p.ti coord. intere int.

B = " " " bordo



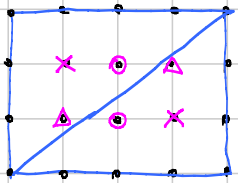
$I = 5 \qquad B = 6$

$\text{Area} = 5 + 3 - 1 = 7$

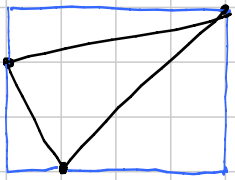
Idea della dim.

Caso Facilissimo: rettangoli (esercizio)

Caso Semifacile: triangoli rettangoli
Cercare di capire come i p.ti cambiano di categoria dal rettangolo al triangolo

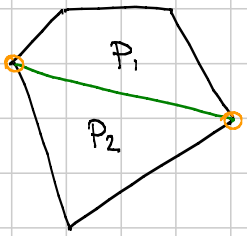


Caso un po' meno facile: triangoli qualunque
Idea: ogni triangolo è differenza di un rettangolo, meno un po' di triangoli rettangoli.
Ci sono un po' di casi ...



Induzione: un poligono qualunque lo divido in 2 tracciando una diagonale
(ovvio per i convessi, ma non ovvio per i non convessi)

I 2 sottopoligoni hanno meno lati.
Per ipotesi induttiva



$P = P_1 \cup P_2$

$$\text{Area}(P_1) = I_1 + \frac{1}{2} B_1 - 1$$

$$\text{Area}(P_2) = I_2 + \frac{1}{2} B_2 - 1$$

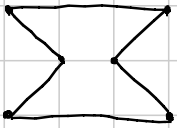
I due estremi della diagonale "uccidono un -1"

I_1, I_2: interni a P_1, P_2 ma non tutti

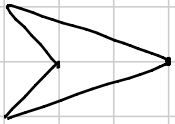
B_1, B_2: quelli sulla diagonale diventano interni con peso 1, quelli sul resto del bordo vanno con peso $\frac{1}{2}$ nel bordo di P

Come suddividere un non convesso in 2 sotto poligoni ?

Domanda 1 : è vero che da ogni vertice esce una diagonale buona ?

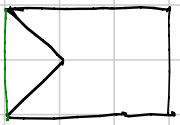


NO!



Domanda 2 : come trovo una diagonale interna ?

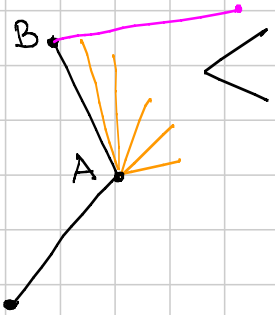
Idea alternativa : invece di dividere, convessifico e poi ragiono sulla differenza.



$P = P_1 \setminus P_2$

P_1 e P_2 hanno meno lati e ragiono come prima.

Partiamo da un vertice con angolo $> 180°$



Idea : usciamo con i p.ti del lato rosa
→ o arriviamo all'altro estremo del lato rosa
→ o nel frattempo abbiamo incontrato un altro vertice

N.B. il rosa non è detto che sia quello che esce da B...

— o — o —

Esempio 4 Giochi finiti.
→ 2 giocatori
→ regole
→ $\exists M$: la partita si conclude dopo $\leq M$ mosse con un vinc.

Teorema: in ogni gioco finito esiste una strategia vincente per uno dei 2 giocatori

Dim. Induzione su M.

$M = 1$ banale ($M=0$ ancora meglio!)

$M \Rightarrow M+1$ Idea: fatta una mossa ottengo un gioco con al + M mosse.

Quindi ci sono 2 casi

→ Alberto può muovere in modo che il gioco nuovo sia vincente per il secondo: muove così e vince

→ tutti i nuovi giochi sono vincenti per il primo: Alberto si arrende

—o—

Esempio 5 Stupido $(1+x)^n \geq \frac{n(n-1)}{2}x^2$ $n \in \mathbb{N}$

Provo per induzione ...

$$(1+x)^{n+1} = (1+x)(1+x)^n \overset{\text{serve } x \geq -1}{\underset{\text{Hp ind.}}{\geq}} (1+x)\frac{n(n-1)}{2}x^2$$

$$= \frac{n(n-1)}{2}x^2 + \frac{n(n-1)}{2}x^3 \overset{?}{\geq} \frac{n(n+1)}{2}x^2$$

Spero che $\frac{n(n-1)}{2}x^2 + \frac{n(n-1)}{2}x^3 \overset{?}{\geq} \frac{n(n+1)}{2}x^2$

$(n-1)(1+x) \overset{?}{\geq} n+1$ Se $x \sim 0$ NON VA !!!

PIÙ FORTE $(1+x)^n \geq 1 + nx + \frac{n(n-1)}{2}x^2$

Questo viene banalmente per induzione !!!

Esempio 6 $\quad 1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\dots+\frac{1}{n^2} \le 2$

Per induzione non viene ... così!

Più forte: $\quad 1+\frac{1}{4}+\dots+\frac{1}{n^2} \le 2-\frac{1}{n}$

Proviamo ... $n=1$: ok

$P_n \Rightarrow P_{n+1}$ $\quad 1+\dots+\frac{1}{n^2}+\frac{1}{(n+1)^2} \le 2-\frac{1}{n}+\frac{1}{(n+1)^2}$

$\overset{?}{\le} 2-\frac{1}{n+1}$

Quindi spero che $\quad \frac{1}{n+1} \overset{?}{\le} \frac{1}{n}-\frac{1}{(n+1)^2}$

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

Resta $\quad n^2+n \le n^2+n+1$ $\quad$ Ok!!!

Esercizio per casa Provare con $\quad \frac{1}{1^a}+\frac{1}{2^a}+\dots+\frac{1}{n^a} = f_a(n)$

Dimostrare che è limitata se $a>1$.

Idea 1: $\quad f_a(n) \le 100-\frac{1}{n}$ $\quad$ Non può funzionare!

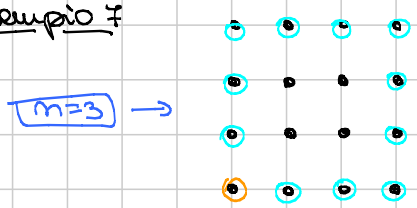
Idea 2: $\quad f_a(n) \le M_a-\frac{1}{n}$ $\quad$ con M_a opportuno

(Non dovrebbe funzionare...)

Idea 3: $\quad f_a(n) \le M_a-\frac{N_a}{n^{a-1}}$: si tratta di scegliere bene M_a ed N_a

Ci sta sotto $\quad \int_1^n \frac{1}{x^a}\,dx = \left[\frac{1}{1-a}\,\frac{1}{x^{a-1}}\right]_1^n = \frac{1}{a-1}\left(1-\frac{1}{n^{a-1}}\right)$

Esempio 7



IMO 2007 – 6 Facilitato
Reticolo $(m+1)\times(m+1)$ Trovare minimo numero di rette che coprono i p.ti del reticolo – Basso sx.

Risposta : $2m$. P.ti del bordo : $4m-1$
Ogni retta ne tocca al + 2 $\Rightarrow$ almeno $\frac{4m-1}{2} = 2m-\frac{1}{2}$ rette, quindi almeno $2m$ rette.
Ovviamente è falso per colpa delle rette non diagonali

Enunciato + forte : dato rettangolo $(m+1)\times(m+1)$ servono almeno $m+m$ rette
Dim : stessa (p.ti del bordo) e se ho una retta verticale scendo di 1 in una dimensione (induzione su $m+n$)

Achtung! I passi base sono gli $1\times m$ e $n\times 1$ (volendo anche questi si riducono allo stesso modo)

Soluzione "ufficiale" che si generalizza in 3 variabili

Fatto generale : $P(x,y)$ polinomio che si annulla sui p.ti del reticolo meno p.to base
$\Rightarrow$ grado $P \geq m+n$
Basta poi prendere $P(x,y)$ = prodotto equazioni rette

Induzione su $m\times n$, o meglio principio del minimo intero.
Supponiamo che per $m_0\times n_0$ abbia polinomio di grado + piccolo $P(x,y)$. Come trovo polinomio per $(m_0-1)\times n_0$?

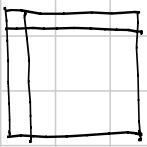
$$Q(x,y) = P(x+1,y) - P(x,y)$$

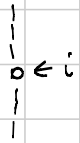
Tutte le proprietà e grado + basso

Esercizio Matrice $n \times n$ di interi simmetrica $a_{ij} = a_{ji}$
Tutti Dispari sulla diagonale
$\Rightarrow$ esistono un po' di colonne che sommate danno una colonna di tutti Dispari

Tradotto: matrice in $\mathbb{Z}_2$ simmetrica con tutti 1 sulla diagonale.
Esiste un vettore in $\mathbb{Z}_2$ che moltiplicato per la matrice dà tutti 1.

Variante: grafo con lampadine. Ad ogni mossa cambio stato una lampadina e tutte le sue collegate.

Induzione:  se va male ottengo 

Analogo: killando i-esima riga e i-esima colonna 

Idea: se posso ottenere 2 colonne, posso ottenere la somma
Posso ottenere 2 uni dove voglio e resto zeri
$\Rightarrow$ se n è pari ho finito.

Nel caso dispari basterebbe riuscire ad ottenere un # dispari di uni, ma per questo basta sommare tutte le colonne
(N.B. funziona solo se n è dispari)

Achtung! L'ipotesi l'ho però usata anche per n pari per avercela sull'$n-1$ dispari precedente!

A1 MEDIUM Pol

Titolo nota 07/09/2010

$\sum_{n=0}^{d} a_n X^n$

$R \subset \mathbb{Z}\ (\mathbb{N})\ \mathbb{Z}/n\mathbb{Z}$

p primo $\qquad f(x) = x^p$

$\Updownarrow$

$g(x) = x$

Principio di identità dei polinomi

f, g polinomi di grado $\leq n$

Se $f(x) = g(x)$ per $n+1$ valori di x,

allora $f = g$ (come polinomi)

X^2+1

$[f-g](x) = (x-x_0)(x-x_1)\cdots(x-x_n)\,q(x)$

$\uparrow$ n — grado $n+1$

x_i

---

a_0, a_1, a_2, a_3, a_4 $\quad p(1)=5$ $\quad p(2)=7$

$$\begin{cases} a_0+a_1+a_2+a_3+a_4 = 5 \\ a_0 + a_1\cdot 2 + a_2\cdot 2^2 + \dots = 7 \end{cases}$$

$a+bi$ $\qquad$ $r\cdot e^{i\vartheta}$

↑ facili somme $\qquad$ ↑ facile prodotti

Es $\quad p(2)=p(4)=5 \quad p(3)=7$

$$p(x)-5 = (x-2)(x-4)q(x)$$

$$p(0)-5 = (-2)\cdot(-4)\cdot \underbrace{q(x)}_{\text{intero}}$$

$$\Rightarrow p(0) \equiv 5 \pmod 8$$

Interpolazione

Trovare un polinomio dati i suoi valori

$p(1)=5$

$\begin{cases} p(2)=6 \\ p(3)=9 \end{cases}$ Dati $n+1$ punti, $\exists!$ polinomio di grado $\leq n$ che ci passa $(x_0,y_0),\dots(x_n,y_n)$

dim

1) Mi basta fare il caso $y_i=0$ per tutti gli i tranne uno:

Sia $\boxed{L_j(x)} = \begin{cases} 0 & \text{in } x_i \ i\neq j \\ 1 & \text{in } x_j \end{cases}$

$$p(x)=\sum_{j=0}^{n} L_j(x)\, y_j$$

$$L_j = \frac{\prod_{i\neq j}(x-x_i)}{\prod_{i\neq j}(x_i-x_j)}$$

$$p(x_1)=\sum L_j(x_1)\, y_j = L_1(x_1)\, y_1 = y_1$$

ESISTENZA

UNICITÀ: grado $\leq n$, coincidono su $n+1$ punti $\Rightarrow$ uguali

Quelli di grado più alto sono

$$p(x)+(x-x_0)(x-x_1)\cdots(x-x_n)q(x)$$

$$\begin{cases} a_0+a_1x_1+a_2x_1^2+\dots+a_nx_1^n=y_1 \\ \vdots \\ a_0+a_1 \end{cases}$$

$$V = \begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^n \\ \vdots & & & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{bmatrix}$$

Vandermonde

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

Fatto

Chi è V^{-1}

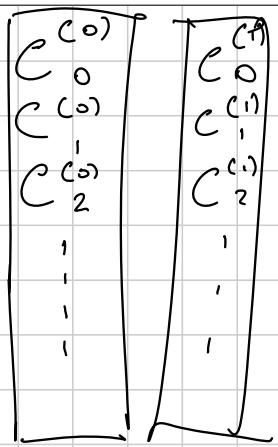
$$V \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{bmatrix}$$

$$V^{-1} \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{bmatrix}$$

$$p(x) = \sum_{j=0}^{n} L_j(x)\, y_j \qquad a_0 = L_j(0)\, y_j$$

coefficienti di L_j

$L_j = \sum_i c_i^{(j)} x^i$



parallelismo tra interi e polinomi:

MCD $\longleftrightarrow$ MCD

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

$|r| < |b|$ $\qquad$ $\deg(r) < \deg(b)$

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

$b(x) = x - \alpha$

pongo $x = \alpha$, $a(\alpha) = r$

Bézout: a, b

Thm: dati a, b polinomi con m.c.d 1 esistono p, q polinomi t.c.

$$a \cdot p + b \cdot q = 1$$

In più, $\deg p < \deg b$

$\deg q < \deg a$

Esiste una e una sola scelta di p, q tali che

Fatto: altre soluzioni: [tutte]

$$\begin{cases} p + r(x) b \\ q - r(x) a \end{cases}$$

Teorema cinese $\Leftrightarrow$ interpolazione

$$\begin{cases} x \equiv y_0 \ (x_0) \\ \vdots \\ x \equiv y_n \ (x_n) \end{cases}$$

$$\begin{cases} p(x) \equiv y_0 & x - x_0 \\ \vdots \\ p(x) \equiv y_n & x - x_n \end{cases}$$

$$p(x) = y_n + (x - x_n) \cdot q(x)$$

congruenze tra polinomi

$p(x) \equiv r(x) \mod q(x)$

$p(x) - r(x)$ multiplo di $q(x)$

$\mathbb{Z}/n\mathbb{Z}$

$x^5 + x^4 - x + 1 \mod x^3 + 1$

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

$-(x^4 + x)$

$-x^2 - 2x + 1$

Fatto

Se il poly. rispetto al quale fate congruenza è irriducibile, lo spazio quoziente è un campo

$$\frac{\mathbb{R}[x]}{(x^3+1)}$$

$x \pm a \mid x^n \pm a^n$

Faccio congruenze mod $x-a$

$x \equiv a$

$x^n \equiv a^n$ $\qquad x^n - a^n \equiv 0$

$x-a \mid x^n - a^n$

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

$ax+b$ +

$cx+d$

$(a+c)x+(b+d)$

$(ax+b)(cx+d) =$

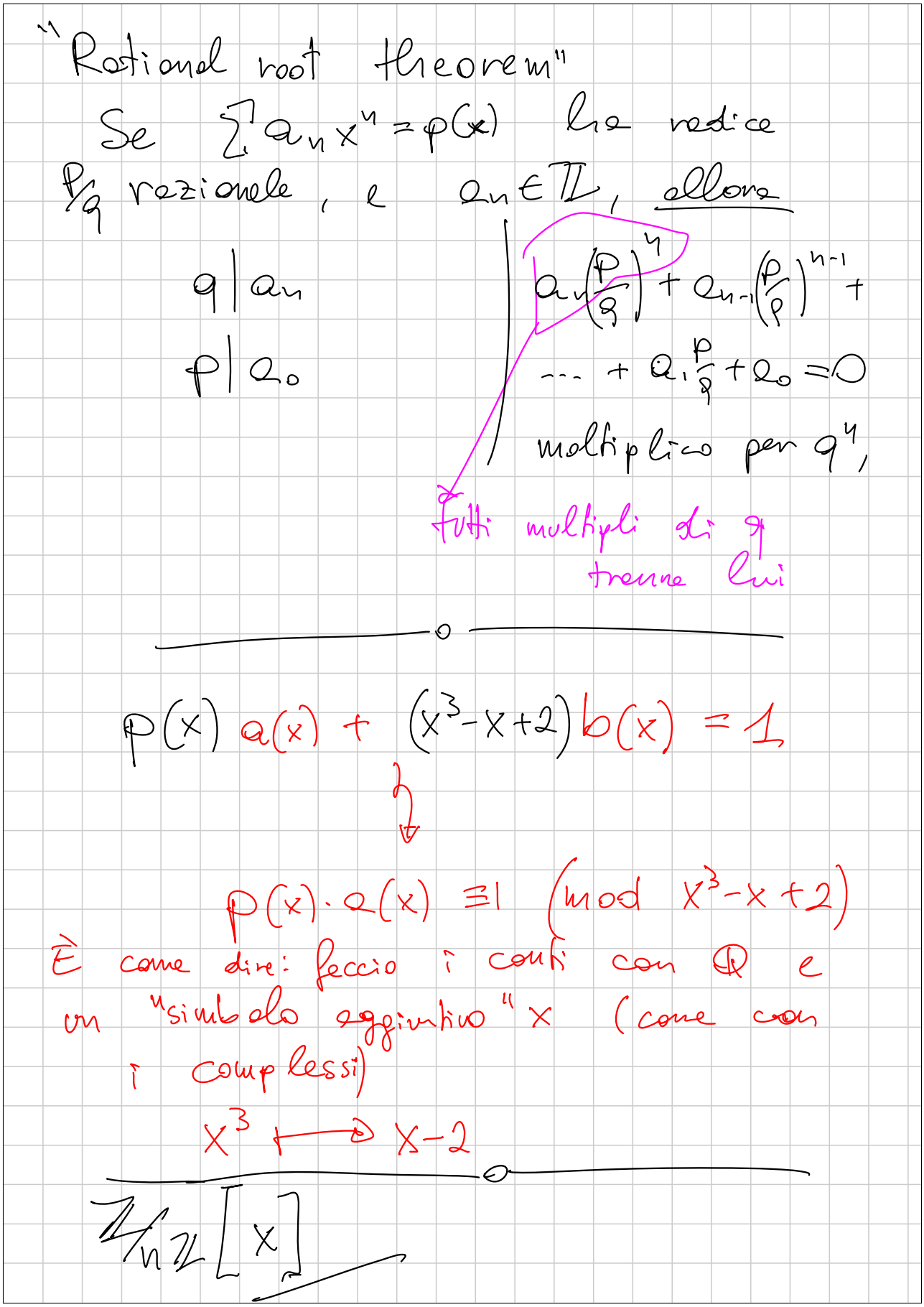
$= acx^2 + bcx + adx + bd \equiv$

$\equiv (-ac+bd)$

$x^2 \equiv -1$

$(x-\alpha)(x-\bar{\alpha})_1 \, (x-\beta)(x-\bar{\beta})_2 \cdots (x-\lambda)(x-\mu)$

$$\frac{\mathbb{Q}[x]}{(x^3-x+2)}$$


"Rational root theorem"
Se $\sum a_n x^n = p(x)$ ha radice p/q razionale, e $a_n \in \mathbb{Z}$, allora
$q \mid a_n$
$p \mid a_0$
$a_n \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \dots + a_1 \frac{p}{q} + a_0 = 0$
moltiplico per q^n,
tutti multipli di q tranne lui
$p(x)\,a(x) + (x^3 - x + 2)\,b(x) = 1$
$p(x) \cdot a(x) \equiv 1 \pmod{x^3 - x + 2}$
È come dire: faccio i conti con $\mathbb{Q}$ e un "simbolo aggiuntivo" x (come con i complessi)
$x^3 \longmapsto x - 2$
$\mathbb{Z}/n\mathbb{Z}[x]$

$\frac{}{(p(x))}$

(E) $\frac{\mathbb{Z}/5\mathbb{Z}}{(x^3-x+2)}$ è un campo

ax^2+bx+c $\in \mathbb{Z}/5\mathbb{Z}$ $\in \mathbb{Z}/5\mathbb{Z}$ $\in \mathbb{Z}/5\mathbb{Z}$

Fatto: $\forall p, \forall n, \exists$ un polinomio irriducibile mod p di grado n

$\Downarrow$

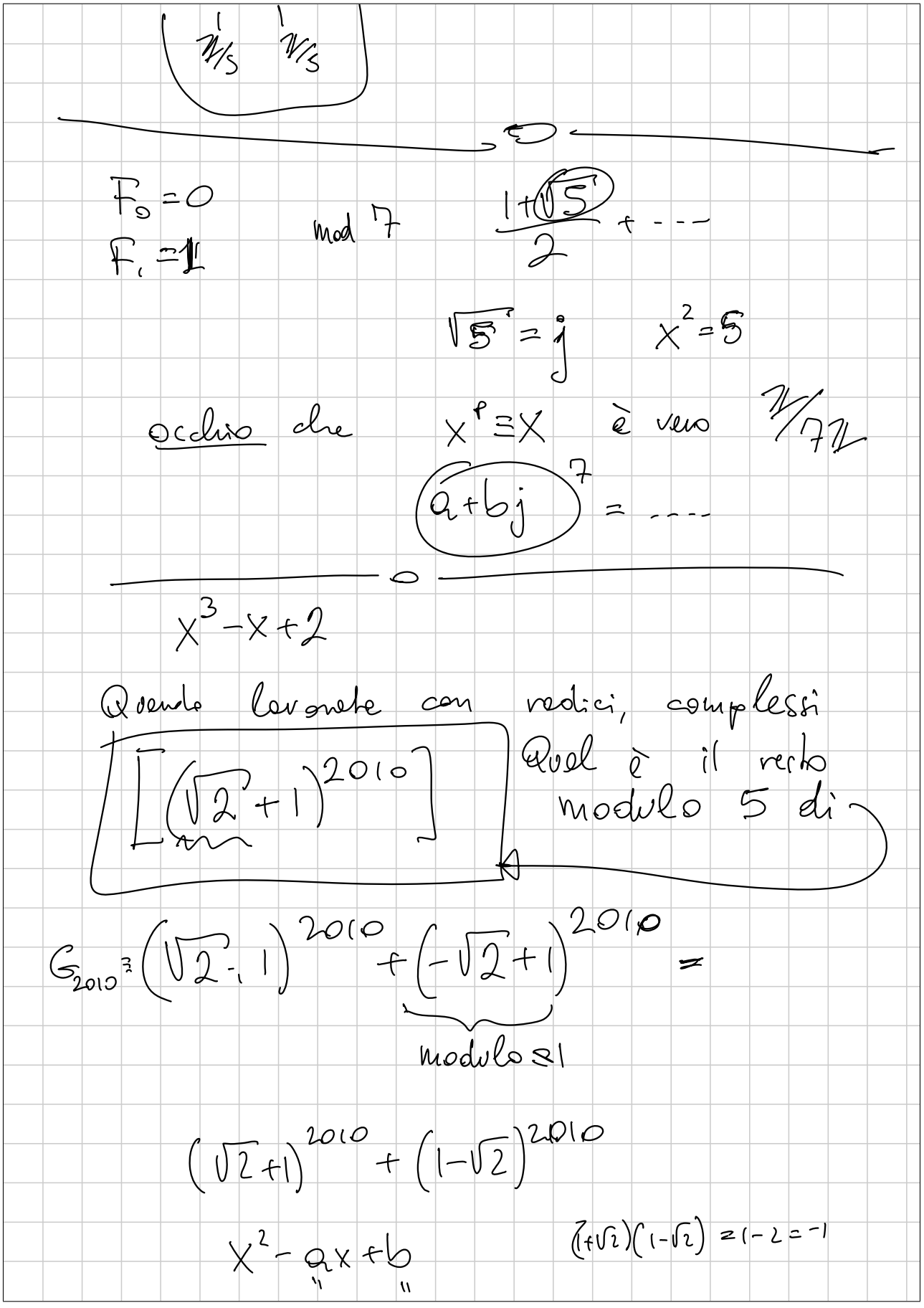
$\forall p, \forall n \exists$ un campo con p^n elementi $\frac{\mathbb{Z}/p\mathbb{Z}[x]}{(p(x))}$

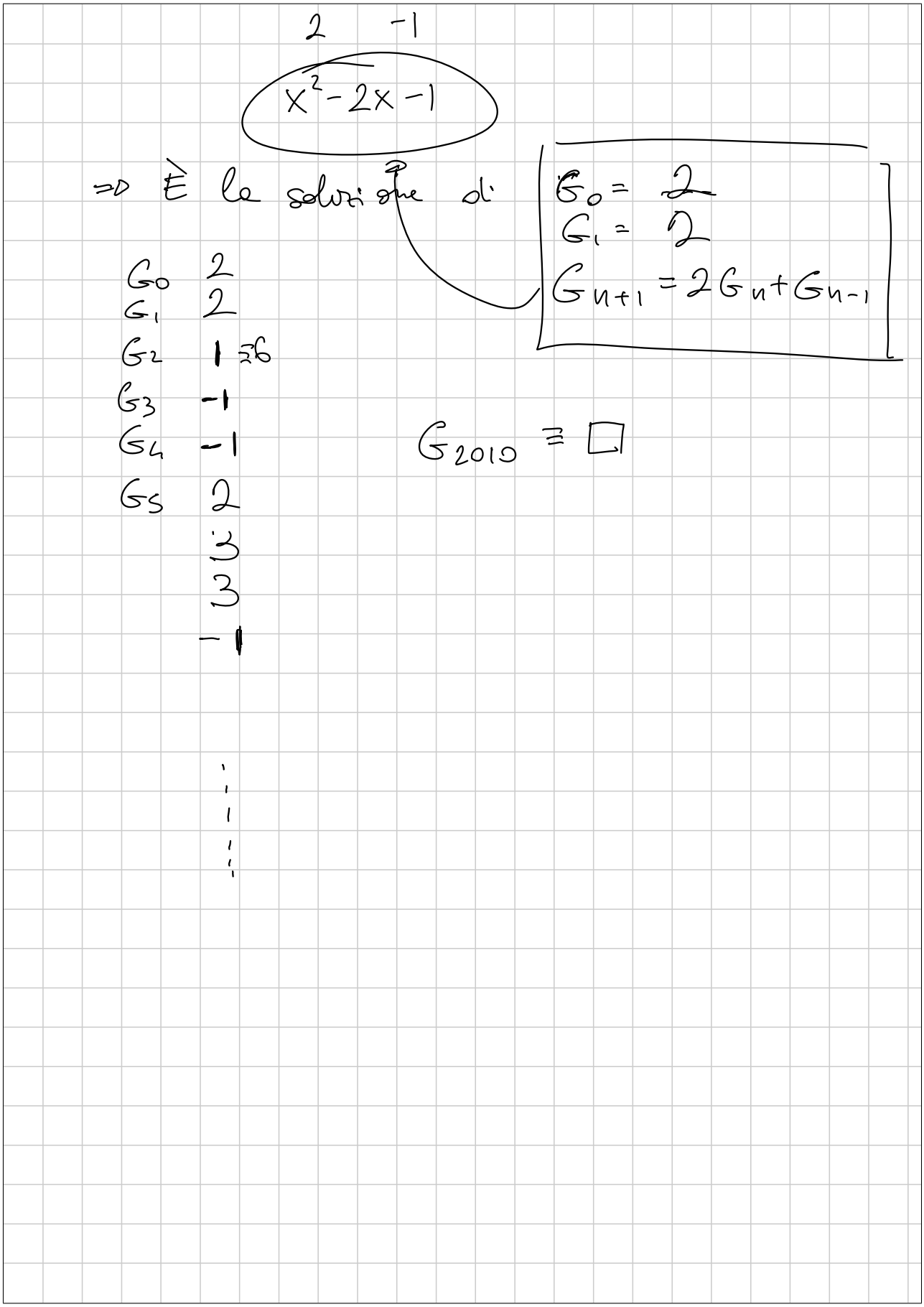
Fatto: questi sono **tutti** i campi finiti

$\mathbb{Z}/5\mathbb{Z}$ x^2-2

chiamo j una soluzione

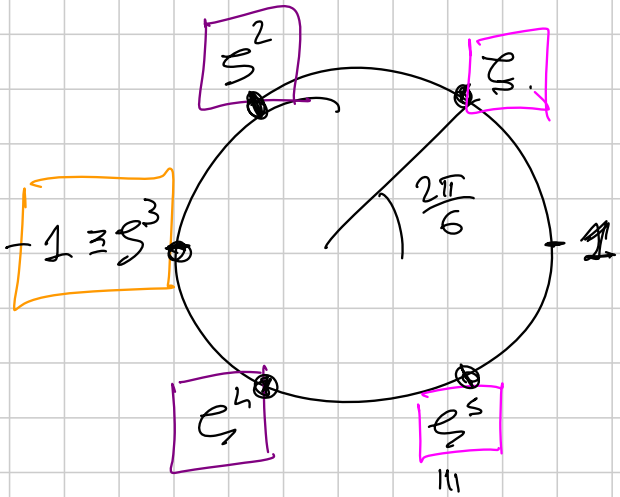
$a+bj$ $j^2 \to 2$


1/5 1/5
$F_0 = 0$
$F_1 = 1$
mod 7
$\frac{1+\sqrt{5}}{2}$ + ---
$\sqrt{5} = j$ $x^2 = 5$
occhio che $x^p \equiv x$ è vero 7/7
$(a+bj)^7$ = ...
$x^3 - x + 2$
Quando lavorate con radici complessi
$[(\sqrt{2}+1)^{2010}]$
Qual è il resto modulo 5 di
$G_{2010} = (\sqrt{2}+1)^{2010} + (-\sqrt{2}+1)^{2010} =$
modulo ≤ 1
$(\sqrt{2}+1)^{2010} + (1-\sqrt{2})^{2010}$
$X^2 - aX + b$
$(1+\sqrt{2})(1-\sqrt{2}) = 1-2 = -1$


2 -1
x^2-2x-1
$\Rightarrow$ È la soluzione di
$G_0 = 2$
$G_1 = 2$
$G_{n+1} = 2G_n + G_{n-1}$
G_0 2
G_1 2
G_2 6
G_3 -1
G_4 -1
G_5 2
3
3
-1
$G_{2010} \equiv \square$

A1 MEDIUM PARTE 2

Titolo nota 07/09/2010



potenze

#						
→	ζ_1	ζ_2	ζ_3	ζ_4	ζ_5	1
→	ζ_2	ζ_4	1	ζ_2	ζ_4	1
$-1 \equiv$	ζ_3	1	-1	1	-1	
→	ζ_4	ζ_2	1	ζ_4	ζ_2	1
	ζ_5					

Radici primitive = generatori

$$(X-\zeta_1)(X-\zeta_2)(X-\zeta_3)(X-\zeta_4)(X-\zeta_5)(X-1)$$

$$= X^6 - 1$$

$$\frac{X^6-1}{X-1} = X^5 + X^4 + X^3 + X^2 + X + 1$$

$$X^3 - 1 = (X - \zeta_2)(X - \zeta_4)(X - 1)$$

$$\Rightarrow (X - \zeta_2)(X - \zeta_4) = \frac{X^3 - 1}{X - 1} = X^2 + X + 1$$

$X^{18} - 1$ radici 18-esime di 1

1 ζ^9 periodo 2

2 ζ^6, ζ^{12} periodo 3

2 $\zeta^3 \cdot \zeta^{15}$ periodo 6

9

In $\mathbb{Z}_{18}$, quante classi di resto sono tali che

$6x \equiv 0$

$3x \not\equiv 0$

$2x \not\equiv 0$

$3 \mid x$

$6 \nmid x$

$9 \nmid x$

$0 \dots 17$

3 15

$0 \dots 18$

multipli di 3

$3 \times (0 \dots 5)$

mioni di 6 e primi con 6

$\varphi(6)$

Radici n-esime dell'unità di periodo $d \mid n$

$$\begin{cases} x^d = 1 \\ x^n = 1. \end{cases} \qquad x^{\mathrm{mcd}(d,n)} = x^{a\cdot d + b\cdot n} = (x^d)^a \cdot (x^n)^b = 1$$

$x^d = 1 \qquad k = 1, 2, 3 \dots n$

- $\zeta^{k\cdot d} = 1 \qquad n \mid k\cdot d$
- il periodo è davvero d, non qualcosa di più piccolo, cioè, per ogni $b \mid d$ $\zeta^{k\cdot b} \neq 1 \qquad n \nmid k\cdot b$

d divisore di n

$k\cdot d \equiv 0 \pmod{n}$

$k \equiv 0 \pmod{\frac{n}{d}}$

$K = [0, \dots, n]$

d

$\forall\ b \mid d$

$n \nmid k \cdot b \qquad k \cdot b \neq 0 \ (n)$

$\zeta^{(n/d)\cdot k} \qquad \zeta^{k \cdot n/d}$

$k \in 0, \dots d$

Se k non ha fattori comuni con d, $(d \mid n)$

$\left(k \cdot \frac{n}{d}\right)$ → periodo d

Se k ha fattori comuni con d,

$\mathrm{mcd}\left(k \cdot \left[\frac{n}{d}\right], n\right)$

$\mathrm{mcd}\left(q \cdot k' \cdot \frac{n}{q \cdot d'}, n\right)$

Questo dovrebbe provare che le radici n-esime dell'unità di periodo d sono:

- $\phi(d)$ se $d \mid n$
- 0 altrimenti

$$(X-\zeta^0)(X-\zeta^1)\cdots(X-\zeta^{n-1})$$

$n=18$

- $\Phi_1 = (X-1)$ periodo 1
- $\Phi_2 = (X+1)$ periodo 2 $\varphi(2)$
- $\Phi_3 = (X-\zeta^6)(X-\zeta^{12})$ periodo 3 $\varphi(3)$
- $(X-\zeta^3)(X-\zeta^{15})$ Φ_6 periodo 6 $\varphi(6)$
- $(X-\zeta^2)(X-\zeta^4)(X-\zeta^8)$ Φ_9 periodo 9 $\varphi(9)$

  $10 \quad 14 \quad 16$

tutte le altre Φ_{18} $\varphi(18)$

$$\Phi_N = \prod_{\substack{z \text{ di} \\ \text{periodo } N \\ z \in \mathbb{C}}} (X-z)$$

[o anche $z \in$ radici dell'unità]

Dim che hanno coeff. razionali: INDUZIONE

Φ_{18} è a coeff. razionali:

$$\frac{X^{18}-1}{\Phi_1(x)\,\Phi_2(x)\,\Phi_3(x)\,\Phi_6(x)\,\Phi_9(x)} =$$

$$= \Phi_{18}(x)$$

→ è un polinomio

→ ha coefficienti interi, perché lo ottengo da fatte divisioni fra polinomi, e i divisori sono monici

MENO BANALE: $\Phi(x)$ irriducibili

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

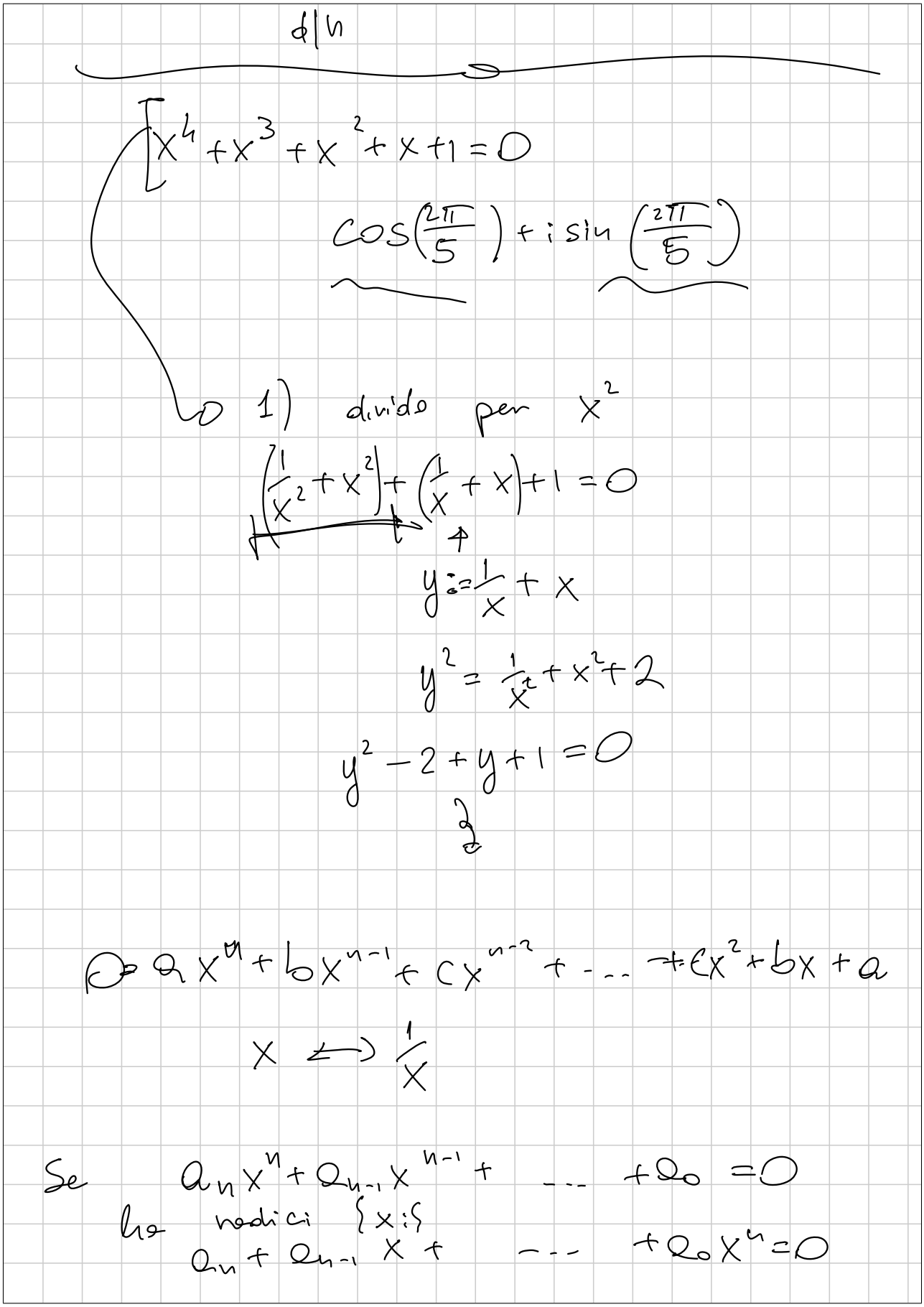
$\zeta \longmapsto \zeta^p$ p primo con n

dim: non fatta

Corollario

$$\phi(18)+\phi(9)+\phi(6)+\phi(3)+\phi(2)+\phi(1)=18$$

$$n = \sum_{+} \phi(d)$$


d|n
$x^4+x^3+x^2+x+1=0$
$\cos\left(\frac{2\pi}{5}\right)+i\sin\left(\frac{2\pi}{5}\right)$
1) divido per x^2
$\left(\frac{1}{x^2}+x^2\right)+\left(\frac{1}{x}+x\right)+1=0$
$y:=\frac{1}{x}+x$
$y^2=\frac{1}{x^2}+x^2+2$
$y^2-2+y+1=0$
$a_nx^n+b_nx^{n-1}+cx^{n-2}+\dots+ex^2+bx+a$
$x\longleftrightarrow\frac{1}{x}$
Se $a_nx^n+a_{n-1}x^{n-1}+\dots+a_0=0$
ha radici $\{x_i\}$
$a_n+a_{n-1}x+\dots+a_0x^n=0$

ha radici $\left\{\frac{1}{x_i}\right\}$ $\qquad aX^2 + a = 0$

$\frac{1}{x_1} \longleftrightarrow x_1$

$\frac{1}{x_2} \longleftrightarrow x_2$

Lemma di Gauss

$a(x) = \sum_n a_n x^n$

Contenuto di $a(x)$ è M.C.D(coefficienti)

Lemma

$$c(a \cdot b) = c(a)\, c(b)$$

dim: mi basta farlo quando $c(a) = c(b) = 1$

$$\left(\sum p_n x^n\right) = \left(\sum a_n x^n\right)\left(\sum b_n x^n\right)$$

$$(\quad) = \boxed{\not{a}}\left(\sum a_n x^n\right)(\quad)$$

Devo dimostrare che $\nexists\, p$ t.c.
$p \mid$ tutti i coefficienti di $a(x)b(x)$
con a, b di contenuto 1

Vedo tutto mod p:
Se esistesse tale p,

$$0 = (\quad)(\quad)$$

cose che non sono zero

$$a(x) = \sum a_n x^n$$

prendo il coeff' di grado più alto k di a t.c. $p \nmid a_k$

e quello di grado più alto h di b t.c. $p \nmid b_h$

$$a_k x^k \cdot b_h x^h$$

che non si annulla con niente

Allora contenuto è moltiplicativo ☐

Se un polinomio $p(x) \in \mathbb{Z}[x]$

$p(x) = a(x)\,b(x)$

con $a(x), b(x) \in \mathbb{Q}[x]$,

allora si spezza anche a coeff' interi

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

ES

$$p(x) = \left(\frac{x+2}{3}\right) \cdot (3x+6) = x^2+4x+4$$

$(x+2)\ (x+2) = \checkmark$

dim:

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

$p(x) = \frac{\bar{a}(x)}{m} \cdot \frac{\bar{b}(x)}{n}$

↑ supponiamo inoltre $c[p] = 1$

$m \cdot n \cdot p(x) = \bar{a}(x)\,\bar{b}(x)$

$c(\ ) = m \cdot n \qquad m \cdot n = c(\bar{a}) \cdot c(\bar{b})$

↑ qui uso moltiplicatività

$p(x) = \frac{\bar{a}(x)\,\bar{b}(x)}{mn} = \frac{\bar{a}(x)}{c(a)} \frac{\bar{b}(x)}{c(b)}$

$\tilde{a}(x) \quad \tilde{b}(x)$ sono a coeff' interi. □

Idee buone

1) proiettare i coefficienti modulo n

(IE) se un polinomio è irriducibile in $\mathbb{Z}/p\mathbb{Z}[x]$

2) prendere i pezzi di grado massimo

$(xy^2 + x^3 + 37y^3 + 2x^2y) =$

no: $(xy + y + x)(y^2 + \ldots x \ldots)$

polinomi omogenei hanno fattori omogenei

polinomi simmetrici hanno fattori simmetrici

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

$*$ $a^3+b^3+x^3-3abx$ è un multiplo di $a+b+x$?

cioè:

è $\equiv 0 \mod (a+b+x)$

$x \equiv -a-b$

$* \equiv a^3+b^3+(-a^3-b^3-3ab(a+b))-3abx \equiv$ ($x \to -a-b$)

$\equiv 0$

$\frac{a^3+b^3+x^3-3abx}{a+b+x}$ è un polinomio in x

$\frac{1}{a+b}x + \ldots$

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

omogeneo
simmetrico

$$\alpha(a^2+b^2+c^2)$$
$$\beta(ab+bc+ca)$$

guarda i coefficienti di a^3: $\alpha = 1$

$$a^3+b^3+c^3-3abc = (a+b+c)(a^2+b^2+c^2-ab-bc-ca)$$

Teo ogni polinomio simmetrico è un polinomio nelle funzioni simm. elementari

---

$$S_k = \sum_{i=1}^{n} x_i^k$$

x_i radici di $\sum_{i=0}^{n} a_k x^k$

$$\sum a_k S_{k+k} = 0$$

$$x_i^t\left(a_0 + a_1 x_i^1 + \dots + a_n x_i^n\right) = 0$$

$$D\left[\sum a_n x^n\right] := \sum a_n \cdot n x^{n-1}$$

Es $D\left[3x^3 + 2x + 37\right] = 3 \cdot 3x^2 + 2$

Proprietà

1) $D[f+g] = Df + Dg$
2) $D[af] = aDf$ (a costante)
3) $D[fg] = D[f] \cdot g + f \cdot D[g]$

$f_1, f_2 \longrightarrow f_1 + f_2$

$$D[(f_1+f_2)g] = D[f_1 g + f_2 g] =$$
$$D[f_1 g] + D[f_2 g] = D[f_1]\, g + f_1 \cdot Dg +$$
$$+ D[f_2]\, g + f_2 \cdot Dg =$$
$$= D[f_1 + f_2]\, g + (f_1 + f_2)\, Dg$$

Mi riconduco a f, g monomi con questo trucco

$$D[ax^m \cdot bx^n] \stackrel{?}{=} D[ax^m]bx^n + ax^m D[bx^n]$$

$$ab(m+n)x^{m+n-1} \stackrel{\checkmark}{=} abmx^{m-1}x^n + abx^m nx^{n-1}$$

CRITERIO DELLA DERIVATA

Un polinomio $f(x)$ ha radici multiple se e solo se

$$\mathrm{mcd}\left(f(x), Df(x)\right) \neq 1$$

dim: $\Rightarrow$

$$\mathrm{mcd}\left((X-a)^m q(x),\ m(x-a)^{m-1}q(x) + (x-a)^m q(x)\right)$$

entrambi i fattori contengono $(x-a)^{m-1}$

$\Leftarrow$)

controllo tutti i fattori di $f(x)$

$(x-a)$: devo verificare che

$$x-a \nmid Df[x]$$

$$f(x) = (x-a)\boxed{q(x)} \Rightarrow q(a) \neq 0$$

$$D[f] = (x-a)q'(x) + 1 \cdot q(x)$$

Valuto in a e vedo se fa 0:

$$D[f](a) = q(a) \neq 0$$

Fattorizzazione unica dei polinomi:

Se l'anello A è a fatt. unica,

$A[x]$ è a fatt. unica

IN PRATICA: SEMPRE

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

$$x^2-5 \qquad \mathbb{Z}/7\mathbb{Z}$$

$$(x^2-5)^2$$

se "chiamo" j una radice del polinomio $aj+b$

$$(x^3-x+2)^2, \quad (x^3-x+2)(18x+37)$$

"tutte le radici coniugate vanno insieme"

Se $p(x),\ q(x) \in \mathbb{Q}[x]$

$p(\sqrt{2}) = q(\sqrt{2}) = 0 \qquad (x-\sqrt{2})$

$p(-\sqrt{2}) = q(-\sqrt{2}) = 0 \qquad (x+\sqrt{2})$

$$\begin{cases} x+y+z+t = 1 \\ x^2+y^2+z^2+t^2 = 2 \\ x^3+y^3+z^3+t^3 = 3 \\ x^4+y^4+z^4+t^4 = 4 \end{cases}$$

$x^2+y^2+z^2+t^2 = (x+y+z+t)^2 - 2(xy+\dots)$

$S = x+y+z+t$

$P = xyzt$

$Q = xy+yz+\dots$

$\lambda^4 - \lambda^3 - \frac{1}{2}\lambda^2 + \square\lambda + \square 1$

$S_3 + A_3 S_2 + A_2 S_1 + 3A_1 = 0$

$a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x = -a_0$

$a_4 x^3 + a_3 x^2 + a_2 x + a_1 = -\frac{a_0}{x}$

$$a_4 \sum x^3 + a_3 \sum x^2 + a_2 \sum x + n a_1 = -\frac{a_0}{x}$$

$$+ a_0 \cdot \frac{a_1}{a_0}$$

$$a_4 x^2 + a_3 x + a_2 + \boxed{\frac{a_1}{x} + \frac{a_0}{x^2}} = 2a_2$$

SENIOR 2010 – A3 MEDIUM

Titolo nota 10/09/2010

Successioni
Funzioni

Ricorrenze lineari $a_{n+1} = ca_n \Rightarrow a_n = c^n \cdot a_0$ (induzione)

$a_{n+1} = ca_n + d$

Pongo $b_n = a_n - l$ cerco l in modo che b_n risolva una ricorrenza senza termine noto:

$$b_{n+1} = a_{n+1} - l = ca_n + d - l = c(b_n + l) + d - l$$

(uso ricorr. per a_n; ricavo a_n)

$$= cb_n + \boxed{cl + d - l}$$

impongo $=0$

$l(c-1) + d = 0 \qquad l = -\frac{d}{c-1}$. Per questa scelta diventa $b_{n+1} = cb_n$, quindi

$$b_n = b_0 \cdot c^n$$

da cui si finisce (con ovvia modifica quando $c=1$)

Alternativa bovina a_0 dato $a_1 = ca_0 + d =$

$a_2 = ca_1 + d = c^2 a_0 + cd + d$

$a_3 = ca_2 + d = c^3 a_0 + c^2 d + cd + d$

$$\vdots$$

$$a_n = c^n \cdot a_0 + d(1 + c + c^2 + \dots + c^{n-1}) = c^n a_0 + d\,\frac{c^n - 1}{c-1}$$

(Induzione ...)

Consideriamo l'insieme delle successioni tali che $a_{n+1} = ca_n$.
Ha 2 proprietà fondamentali
→ è chiuso rispetto alla somma (cioè se a_n e b_n sodd., anche $a_n + b_n$ soddisfa)

→ è chiuso rispetto al prodotto per un numero C (cioè se $a_{n+1} = C a_n \ \forall n \in \mathbb{N}$, allora anche la succ. $b_n = \lambda a_n$ ha la stessa proprietà)

Stessa cosa con termini lontani. Insieme delle succ. am t.c.

$$a_{n+1} = C a_n + \text{Mostro}(n) \qquad (\star)$$

Le 2 proprietà precedenti non valgono più, MA

→ date 2 successioni che verificano, la loro differenza verifica la ricorrenza senza Mostro(n).

Sia quindi $\bar{a}_n$ una qualunque soluzione della $(\star)$. Allora ogni altra soluzione a_n sarà del tipo

$$a_n = \underbrace{a_n - \bar{a}_n}_{= C^n \cdot \alpha} + \bar{a}_n = C^n \cdot \alpha + \bar{a}_n$$

SOLUZIONE GENERALE CON MOSTRO	=	SOLUZIONE GEN. SENZA MOSTRO	+	SOLUZIONE SPECIALE CON MOSTRO

Se conosco una soluzione, allora le conosco tutte.
Torniamo a

$$a_{n+1} = C a_n + d$$

Voglio trovare UNA soluzione. La cerco del tipo costante $a_n \equiv \beta$

$$\beta = C\beta + d \quad \Rightarrow \quad \beta = -\frac{d}{C-1} = \text{il del primo approccio}$$

$$a_n = \alpha \cdot C^n - \frac{d}{C-1} \qquad \text{con} \quad a_0 = \alpha - \frac{d}{C-1}$$

Esempio 2 $a_{n+1} = 6a_n + 5n$

Cerco una soluzione speciale del tipo $a_n = \alpha n + \beta$

$\alpha(n+1) + \beta = 6\alpha n + 6\beta + 5n$ (a_{n+1} a sinistra, $6a_n$ a destra)

$\alpha n + \alpha + \beta = 6\alpha n + 6\beta + 5n$

$5\alpha = -5$ coeff. di n

$\alpha = 5\beta$ termine noto

$\Rightarrow \alpha = -1 \quad \beta = -\frac{1}{5}$

$a_n = -n - \frac{1}{5} + 6^n \cdot c$

c: parametro libero fissato dal dato iniziale

Esempio 3 $a_{n+2} = 4a_{n+1} - 3a_n + n^2$

Voglio formula generale (con 2 parametri).

Cerco una soluzione speciale del tipo

$a_n = an^2 + bn + c$

$a(n+2)^2 + b(n+2) + c = 4[a(n+1)^2 + b(n+1) + c] - 3(an^2 + bn + c) + n^2$

Sviluppo... e impongo che si annullino i coeff. di $n^2, n, 1$: ottengo 3 equazioni lineari in 3 incognite: di solito funziona.

La soluzione generale sarà del tipo

$a_n = \underbrace{an^2 + bn + c}_{\text{a,b,c trovati risolvendo il sistema}} + \underbrace{\alpha \cdot 1^n + \beta \cdot 3^n}_{\text{soluzione generale senza nostro}}$

Sol. generale senza nostro: $x^2 - 4x + 3 = 0$ Radici: $x = 1$ e $x = 3$

Reinterpretazione del basic Successioni che soddisfano la ricorrenza lineare senza nostro hanno queste proprietà

* chiuse rispetto alla somma
* " " al prodotto per un numero

Conseguenza: se x_n va bene e y_n va bene, allora va bene anche

$$a_n = \underbrace{c_1 x_n + c_2 y_n}_{\text{comb. lineare}}$$

Se la ricorrenza è di ordine 2 (dipendenza dai 2 termini prec.) allora la succ. è univoc. determinata conoscendo a_0 e a_1. Quindi se x_n e y_n sono scelte bene, posso trovare c_1 e c_2 in modo da soddisfare a_0 e a_1. La condizione è che

$$\begin{cases} c_1 x_0 + c_2 y_0 = a_0 \\ c_1 x_1 + c_2 y_1 = a_1 \end{cases}$$

ha soluzione $\Leftrightarrow$ $x_0 y_1 - x_1 y_0 \neq 0$ (unica) per ogni a_0, a_1

Tutta la teoria del basic serve a produrre 2 soluzioni speciali x_n e y_n (di solito di tipo esponenziale).

La teoria vale per successioni a valori reali, ma anche a valori complessi

$$a_{n+2} = 4a_{n+1} - 13a_n$$

Polinomio: $x^2 - 4x + 13 = 0$ $\quad x_{1,2} = 2 \pm \sqrt{4-13} = 2 \pm 3i$

Tutte le soluzioni (complesse) sono del tipo

$$a_n = c_1 \cdot (2+3i)^n + c_2 (2-3i)^n$$

Se voglio una formula senza complessi $\quad 2+3i = \rho e^{i\theta}$ $\quad 2-3i = \rho e^{-i\theta}$

$$a_n = c_1 \cdot \rho^n e^{in\theta} + c_2 \rho^n e^{-in\theta}$$

$$\rho^n e^{in\theta} = \rho^n (\cos(n\theta) + i \sin(n\theta)) = x_n$$
$$\rho^n e^{-in\theta} = \rho^n (\cos(n\theta) - i \sin(n\theta)) = y_n$$

Se x_n e y_n vanno bene, allora vanno bene anche

$\frac{1}{2}(x_n + y_n) = \rho^n \cos(n\theta)$ $\qquad$ $\frac{1}{2i}(x_n - y_n) = \rho^n \sin(n\theta)$

Ogni combinazione lineare di x_n e y_n si può scrivere (cambiando i coefficienti) come comb. lin. di

$\rho^n \cos(n\theta)$ $\qquad$ $\rho^n \sin(n\theta)$

Se Mostro(n) = polinomio di grado n cerco $\bar{a}_n$ = polinomio dello stesso grado

Se Mostro(n) = k^n, allora cerco $\bar{a}_n = \lambda \cdot k^n$ con stesso k e λ da trovare.

Esempio (n+1) $\qquad a_{n+2} = 5a_{n+1} - 6a_n + 4^n$

Cerco soluzione $a_n = \lambda \cdot 6^n$:

$$\lambda \cdot 4^{n+2} = 5\lambda 4^{n+1} - 6\lambda 4^n + 4^n$$

$$16\lambda = 20\lambda - 6\lambda + 1 \qquad 2\lambda = 1 \qquad \lambda = \frac{1}{2}$$

Sol. generale $\qquad a_n = \frac{1}{2} \cdot 6^n + c_1 2^n + c_2 \cdot 3^n$

$x^2 - 5x + 6 = 0 \qquad x = 2,\ x = 3$

Esempio $(n + \frac{3}{2})$ $\qquad a_{n+2} = 5a_{n+1} - 6a_n + 3^n$. Cerco $\bar{a}_n = \lambda 3^n$

$$\lambda 3^{n+2} = 5\lambda 3^{n+1} - 6\lambda 3^n + 3^n$$

$$9\lambda = 15\lambda - 6\lambda + 1$$

Bella scoperta: 3^n era soluzione della ricorrenza senza Mostro!

Basta aggiungere una n: tentativo $\bar{a}_n = \lambda n \cdot 3^n$

$\lambda(n+2)3^{n+2} = 5\lambda(n+1)3^{n+1} - 6\lambda n 3^n + 3^n$; $18\lambda = 15\lambda + 1$ ok.

In generale si sa risolve con Horner (n) = somma di esponenziali + polinomio in n

E se ci fosse $n^2 4^n$ tanto $(an^2+bn+c)4^n$

$n^2 3^n$ " $(an^2+bn+c)\cdot n4^n$

—o—o—

$a_{n+1} = 2a_n^2 - 1$ NON È LINEARE

Idea: se fosse $a_n = \cos\theta$, sarebbe $a_{n+1} = 2\cos^2\theta - 1 = \cos(2\theta)$

da cui per induzione $a_n = \cos(2^n\theta_0)$ dove $a_0 = \cos\theta_0$

E se fosse $a_0 = 2010$? Esiste θ_0 t.c. $\cos\theta_0 = 2010$??

Sì, ma nei complessi

$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2} \qquad \cos z = \frac{e^{iz} + e^{-iz}}{2}$$

ha senso per z complesso! $[e^{a+ib} = e^a \cdot e^{ib} = e^a(\cos b + i\sin b)]$

La funzione $z \to \cos z$ vista $\mathbb{C} \to \mathbb{C}$ è iniettiva? NO!

È suriettiva? SÌ

$\cos z = w \qquad e^{iz} + e^{-iz} = 2w \qquad e^{iz} = y$

$y + \frac{1}{y} = 2w \rightsquigarrow$ trovo $y \neq 0 \rightsquigarrow$ devo risolvere $e^{iz} = y$

—o—o—

EQUAZIONI FUNZIONALI

$$f: S \to S$$

Cauchy: $f(x+y) = f(x) + f(y) \qquad \forall x \in S \quad \forall y \in S$

$S = \mathbb{Q}$. Allora $\exists\, \lambda \in \mathbb{Q}$ t.c. $f(x) = \lambda x \quad \forall x \in \mathbb{Q}$ $(\lambda = f(1))$

Passi fondamentali:

- $f(0) = 0$
- conquista di $\mathbb{N}$ (induzione su $\mathbb{N}$)
- conquista di $\mathbb{Z}$ (dopo aver osservato che f è dispari)
- conquista di $\mathbb{Q}$ (si dimostra per induzione che $f(nx) = n f(x)$ $\forall x \in \mathbb{Q}$, poi si pone $x = \frac{p}{q}$ e $n = q$ ...)

Andare oltre $\mathbb{Q}$ non è possibile

$$S = \{a + b\sqrt{2} \,:\, a \in \mathbb{Q},\, b \in \mathbb{Q}\}$$

Se pongo $f(a+b\sqrt{2}) = b + a\sqrt{2}$, questa risolve la Cauchy senza essere lineare (cioè del tipo λx)

BASI DI HAMEL

Un sottoinsieme $B \subseteq \mathbb{R}$ è una base di Hamel se ha 2 proprietà.

① Per ogni $x \in \mathbb{R}$, esistono $n \geq 1$ intero, esistono $b_1, \dots, b_n \in B$ (diversi), esistono $q_1, \dots, q_n \in \mathbb{Q}$ tali che

$$x = q_1 b_1 + q_2 b_2 + \dots + q_n b_n$$

② Se $b_1, \dots, b_n$ sono elementi diversi di B, e $q_1, \dots, q_n \in \mathbb{Q}$, e

$$q_1 b_1 + \dots + q_n b_n = 0$$

allora $q_1 = \dots = q_n = 0$.

Corollario La scrittura di cui al punto ① è unica

Sostanzialmente ogni reale x si può scrivere in modo unico come comb. lineare finita di elementi di B.

Per dimostrare l'esistenza di una base di Hamel serve il lemma di Zorn (dim. difficile)

Base di Hamel permette di costruire una soluzione della Cauchy non lineare (esattamente come con $a+b\sqrt{2}$)
Scelgo 2 elementi b_1 e b_2 della base di Hamel e li "scambio" Tutti gli altri li lascio fissi

$x = q_1 b_1 + q_2 b_2 + \text{altro}$
$f(x) = q_1 b_2 + q_2 b_1 + \text{altro}$ si vede che risolve la Cauchy.

Esempio $f: \mathbb{R} \to \mathbb{R}$ t.c. $f(x + f(y)) = y + f(x) \quad \forall x, y \in \mathbb{R}$

① $x = 0 \Rightarrow f(f(y)) = y + f(0) \Rightarrow f$ iniettiva e surgettiva.
Per la surgettività esiste $x_0 \in \mathbb{R}$ t.c. $f(x_0) = 0$

② $x = y = x_0 \Rightarrow f(x_0 + 0) = x_0 + f(x_0)$
$0 = x_0 \Rightarrow f(0) = 0$

③ Back to ① $f(f(y)) = y \quad \forall y \in \mathbb{R}$
Pongo $y = f(z)$
$f(x + f(f(z))) = f(z) + f(x)$
$f(x + z) = f(x) + f(z) \quad \forall x \in \mathbb{R} \ \forall z \in \mathbb{R}$
Cauchy!!! $\Rightarrow f(x) = \lambda x \quad \forall x \in \mathbb{Q}$

④ Posso fare conquista di $\mathbb{R}$? NO!!
L'esempio è lo stesso di prima (f scambia b_1 e b_2 e lascia gli altri invariati)

Da $\mathbb{Q} \to \mathbb{Q}$ ok $f(x) = \lambda x$ e poi si trova $\lambda = \pm 1$
Da $\mathbb{R} \to \mathbb{R}$ non si va avanti (ci sono infinite soluzioni)

Cosa aggiungere alla Cauchy per andare in $\mathbb{R}$?
Una cosa a scelta tra
* monotonia
* continuità
* limitatezza inferiore / superiore in un qualunque intervallo
* un qualsiasi cerchietto nel piano in cui non entra il grafico

<u>Idee della dim</u> ① wlog $f(1)=0$, quindi $f(\mathbb{Q})=0$
(basta considerare $g(x) = f(x) - f(1)\,x$)
② per assurdo $\exists\, r \in \mathbb{R} \setminus \mathbb{Q}$ t.c. $g(r) > 0$
Allora esistono punti del tipo ($q_1, q_2 \in \mathbb{Q}$)
$q_1 + q_2 r > 0$ e vicini a zero quanto voglio con q_2 grande quanto voglio.
Ma $g(q_1 + q_2 r) = \underbrace{g(q_1)}_{0} + \underbrace{q_2\, g(r)}_{\text{enorme}}$

—o—o—

IMO 1992 – 2 $\quad f(x^2 + f(y)) = y + [f(x)]^2 \qquad f: \mathbb{R} \to \mathbb{R}$

① $x=0 \Rightarrow f(f(y)) = y + [f(0)]^2 \Rightarrow f$ iniettiva e surgettiva

② Sarebbe bello $f(0)=0$. Facciamo finta di averlo fatto
Back to ① $\quad f(f(y)) = y \quad \forall y \in \mathbb{R}$

③ $y=0 \Rightarrow f(x^2) = [f(x)]^2 \quad \forall x \in \mathbb{R}$

④ $y = f(z)$: $\quad f(x^2 + f(f(z))) = f(z) + [f(x)]^2$

$\qquad\qquad \updownarrow ② \qquad\qquad\qquad \updownarrow ③$

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

Pongo $x^2 = y$ e ottengo

$$f(y+z) = f(y) + f(z) \qquad \forall z \in \mathbb{R} \quad \boxed{\forall y \geq 0}$$

Variante della Cauchy, che ha le stesse conclusioni
$\Rightarrow$ conquista di $\mathbb{Q}$

⑤ Cerco monotonia. La ④ la posso riscrivere come

$$f(z+x^2) = f(z) + [f(x)]^2 \quad \Rightarrow \text{monotonia crescente}$$

va fatto formale, ma

$$f(z + \text{roba positiva}) = f(z) + \text{altra roba positiva}$$

$\Rightarrow f(x) = \lambda x \quad \forall x \in \mathbb{R}$. Sostituendo si trova λ.

Come dimostrare che $f(0)=0$. $\quad f(2)=a \quad f(\sqrt{2})=0$

$y=0 \Rightarrow f(x^2+a) = [f(x)]^2 \qquad (\star\star)$
$x=0 \Rightarrow f(f(y)) = y+a^2 \qquad (\star)$
$x=y=0 \Rightarrow f(a) = a^2$
$y=a \Rightarrow f(x^2+a^2) = a + [f(x)]^2$
Applico f:

$$f(f(x^2+a^2)) = f\left(a+[f(x)]^2\right)$$
$$\updownarrow(\star) \qquad\qquad \updownarrow(\star\star)$$
$$x^2+2a^2 = [f(f(x))]^2 = [x+a^2]^2$$

svolgendo si vede che l'unica possibilità è $a=0$.

—o—o—

BMO 1997-4 $\quad f(xf(x)+f(y)) = [f(x)]^2+y \qquad f:\mathbb{R}\to\mathbb{R}$

①
$x=0 \Rightarrow$ iniettiva e suriettiva $\quad f(f(y)) = a^2+y$
$\exists x_0 \in \mathbb{R}$ t.c. $f(x_0)=0$

② $x=x_0 \Rightarrow f(f(y)) = y$. Confrontando con il punto ① otteniamo $a=0$ (quindi $f(0)=0$) e $x_0=0$

③ $y=0 \Rightarrow f(xf(x)) = [f(x)]^2$

④ Idea nuova: $x = f(z)$:

$$f(f(z)\cdot f(f(z))) = [f(f(z))]^2$$

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

e confrontando con ③ ottengo $[f(x)]^2 = x^2$, da cui

$$f(x) = \pm x.$$

ACHTUNG !!! OCCHIO AL MISTONE $f(x) = x$ per certi x e $f(x) = -x$ per altri x.

⑤ Supponiamo $f(a) = a$ e $f(b) = -b$ $(a \neq 0,\ b \neq 0)$

Pongo $x = +b$ e $y = a$

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

$-b^2+a = b^2+a \rightsquigarrow b=0$ NO

$b^2-a = b^2+a \rightsquigarrow a=0$ NO

⑥ Verifica...

—o—o—

BMO 2007-2 $f(f(x)+y) = f(f(x)-y) + 4f(x)\cdot y$ $f: \mathbb{R}\to\mathbb{R}$

$y = f(x)$ $f(2f(x)) = f(0) + 4f^2(x)$

$= f(0) + [2f(x)]^2$

Quindi $f(z) = f(0) + z^2$ e queste verificano

NO!!! SI! Ma solo $\forall z \in 2\,\mathrm{Im}(f)$

Uno sa che iniettività e suriettività NON ci sono.

Come sfruttare la y fuori

Provo con $y = f(x) - 2f(z)$

$$f(2(f(x)-f(z))) = f(2f(z)) + 4f(x)(f(x)-2f(z))$$

↓ so

$$f(2(f(x)-f(z))) = f(0) + 4[f(z)]^2 + 4[f(x)]^2 - 8f(x)\cdot f(z)$$

$$= f(0) + [2(f(x)-f(z))]^2$$

Quindi $f(x) = f(0) + x^2$ su tutti gli x che sono $2(\mathrm{Im} - \mathrm{Im})$ e spero che questo sia tutto $\mathbb{R}$

$$f(\text{Mostro}) - f(\text{Mostro}) = 4y f(x)$$

Se $f(x) \equiv 0$ c'è poco da fare
Se $\exists x_0 \in \mathbb{R}$ t.c. $f(x_0) \neq 0$, allora il RHS è tutto $\mathbb{R}$
Quindi

$$f(\mathbb{R}) - f(\mathbb{R}) = \mathbb{R} \quad \text{e anche}$$
$$2(f(\mathbb{R}) - f(\mathbb{R})) = \mathbb{R}.$$

—o—o—→

IMO 1999 – 6 $\quad f(x - f(y)) = f(f(y)) + x f(y) + f(x) - 1$

① $x = 2f(y) \Rightarrow f(f(y)) = f(f(y)) + 2f^2(y) + f(2f(y)) - 1$

$$f(2f(y)) = 1 - 2[f(y)]^2 = 1 - \frac{1}{2}[2f(y)]^2$$

$$\Rightarrow \quad f(x) = 1 - \frac{x^2}{2} \qquad \forall x \in 2\,\mathrm{Im}(f)$$

② $\boxed{x = f(y)}$ $\quad \underbrace{f(0)}_{a} = 2f(f(y)) + [f(y)]^2 - 1$

$$f(f(y)) = \frac{a+1}{2} - \frac{1}{2}[f(y)]^2$$

③ $x = f(z)$ $\qquad f(f(z)-f(y)) = f(f(y)) + f(z)\cdot f(y) + f(f(z)) - 1$

so fare $\qquad$ so fare

$$= -\frac{1}{2}\left[f(z)-f(y)\right]^2 + \text{costante}$$

$\Rightarrow \quad f(x) = \text{costante} - \frac{x^2}{2} \qquad$ per ogni $x \in \mathrm{Im}(f) - \mathrm{Im}(f)$

④ Resta da dim che $\mathrm{Im} - \mathrm{Im} = \mathbb{R}$

$$f(x-f(y)) - f(x) = f(f(y)) + x f(y) - 1$$

Se $f \equiv 0$ non funziona

altrimenti $\exists\, y_0 \in \mathbb{R}$ t.c. $f(y_0) \neq 0$. Il RHS percorre tutto $\mathbb{R}$.

Funzioni generatrici

Titolo nota 07/09/2010

$a_0, a_1, \dots$ $\quad a_0 + a_1 x + a_2 x^2 + \dots$

$\binom{n}{0} + \binom{n}{1} x + \binom{n}{2} x^2 + \dots \qquad \binom{n}{n} x^n = (1+x)^n$

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

$a_0 = 0$

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

$S(x) = a_0 + a_1 x + a_2 x^2 + \dots$ ($a_0 = 0$)

$a_1 + a_2 x + a_3 x^2 + \dots = 2a_0 + 1 + (2a_1 + 1)x + (2a_2 + 1)x^2 + \dots$

$\frac{S(x)}{x}$

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

$S(x) = 2xS(x) + \frac{x}{1-x}$

$S(x) = \left| \frac{x}{(1-x)(1-2x)} \right| = \frac{A}{1-x} + \frac{B}{1-2x}$ ($A = -1$, $B = 1$)

$S(x) = \frac{1}{1-2x} - \frac{1}{1-x}$

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

$a_n = 2^n - 1$ $\qquad a_2$

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

$a_0, a_1, a_2, \dots$ $\quad ogf(a_i)$

$[x^n]\, \delta(x) =$ coef. di x^n.

$ogf(a_i) = ogf(b_i) \iff a_i = b_i \ \forall i$

$ogf(a_i) + ogf(b_i) = ogf(a_i + b_i)$

$ogf(a_i) \cdot ogf(b_i) = ogf\left(\sum_{s=0}^{i} a_s \cdot b_{i-s}\right)$

$ogf(a_i) = ogf(b_i)$ se $a_k = b_k = 0$

$\frac{ogf(a_i)}{ogf(b_i)}$ se $b_w = 0$

$[x^0]\, \delta(x) \neq 0 \to G(x)$ se $[x^0]\, \delta(x) = 0$

$\frac{G(x)}{\delta(x)} = G(x) \cdot \left[\frac{1}{\delta(x)}\right]$ $\qquad A(x) = \frac{G(x)}{\delta(x)}$

$A(x) \cdot \delta(x) = G(x)$

$x^n \left[A(x) \cdot \frac{\delta(x)}{x^n} \right] =$ col termine noto. ($x^n V(x)$)

$\frac{A(x)}{B(x)} = A(x) \cdot \frac{1}{B(x)}$

$C(x) = \frac{1}{B(x)} \iff C(x) \cdot B(x) = 1$

$ogf(a_i) \cdot ogf(b_i) = 1$ $\qquad a_0 \cdot b_0$ $\quad a_0 = \frac{1}{b_0}$

$ogf\left(\sum_{s=0}^{i} a_s \cdot b_{i-s}\right)$

$\sum_{s=0}^{n} a_s b_{n-s} = 0 \quad a_n \quad \Longrightarrow \quad a_n = \frac{\text{quelcosa}}{b_0}$

$A(x) = \text{ogf}(a_i)$ $\quad A(B(x)) =$

$B(x) = \text{ogf}(b_i)$

$a_0 + a_1 \text{ogf}(b_i) + a_2 \underbrace{\text{ogf}(b_i)^2} + \dots$

$A(x) = \frac{1}{1-x}$
$B(x) = \frac{1}{1-x}$
$\Big\}$ $1 + (1 + x + x^2 + \dots) + (1 + x + x^2 + \dots)^2 + \dots$

$\log(f(x)) = g(x)$ $\quad \dots \; e^{g(x)} = f(x)$

$a_0 + a_1 x + a_2 x^2 + \dots = \delta(x)$

$a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \dots$

$\exists R \in \mathbb{R} : \forall |r| < R \;\; \delta(r)$ converge; $\forall |r| > R$ si comporta male.

Per $r = R$ o $-R$.

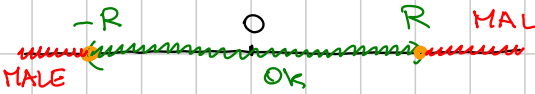
$a_0 + a_1 x + \dots = \delta(x)$

Se converge per K positivo $(\delta(K)) \Rightarrow$ converge anche per i positivi minori.

$B_n(x) = \sum_{i=0}^{n} a_i x^i$

SERIE DI POTENZE

$\sum_{n=0}^{\infty} a_n x^n$ Domanda: per quali $x \in \mathbb{R}$ la serie converge



può anche essere $+\infty$

$R = [0, +\infty]$

SERIE DI NUMERI $\sum_{n=0}^{\infty} b_n$

FATTO 1 $\sum_{n=0}^{\infty} b_n$ converge $\Rightarrow b_n \to 0$

Dim. $S_n = b_0 + b_1 + \dots + b_n$ $\quad b_n = S_n - S_{n-1}$

$\ell - \ell = 0$

Viceversa Se $b_n \not\to 0$, allora di sicuro $\sum b_n$ NON converge

Nella zona rossa $a_n x^n$ NON tende a zero

Esempio $\sum_{n=0}^{\infty} x^n$

$x \geq 1$ DIVERGE A $+\infty$

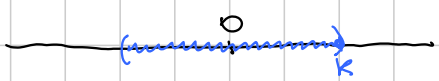
$x < -1$ INDETERMINATA

$x = -1$ $+1-1+1-1+1-1$

FATTO 2 $\sum_{n=0}^{\infty} |b_n|$ converge $\Rightarrow \sum_{n=0}^{\infty} b_n$ converge

FATTO 2 $\Rightarrow$ Teorema sul raggio di convergenza

Se in k converge, allora converge per gli x con $|x| < k$



Prendo k e prendo $|x| < k$. Dico che in x si ha

$$\sum_{n\geq 0}^{\infty} |a_n x^n| \quad \text{converge}$$

$$= \sum_{n\geq 0}^{\infty} |a_n| \frac{|x|^n}{k^n} k^n = \sum_{n\geq 0}^{\infty} |a_n| k^n \left|\frac{x}{k}\right|^n = (\star)$$

Sapendo che $\sum a_n k^n$ converge, FATTO 1 $\Rightarrow a_n k^n \to 0$

$\Rightarrow \exists M$ t.c. $|a_n| \cdot k^n \leq M \quad \forall n \in \mathbb{N}$

$(\star) \leq M \underbrace{\sum_{n\geq 0}^{\infty} \left|\frac{x}{k}\right|^n}_{\text{converge}}$ (Serie del tipo $\sum_{n\geq 0}^{\infty} a^n$ con a fisso <1)

FATTO 3 $\sum_{n\geq 0}^{\infty} a^n$ converge $\Leftrightarrow |a| < 1$ e la somma è $\frac{1}{1-a}$

$\mathcal{D}\,\text{ogf}(e_1) = \text{ogf}((n+1)e_{n+1})$

$$\mathcal{D}\sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} \mathcal{D}(a_n x^n) = \sum_{n=0}^{\infty} n a_n x^{n-1}$$

$f(x)$

$$\mathcal{D}\frac{e^x}{1-x} = \text{serie di potenze}$$

$$\int \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} \frac{a_n}{n+1} x^{n+1}$$

$\delta(x) = \text{ogf}(a_i)$

$A(x) = \text{ogf}(a_{i+k})$

$a_0 + a_1 x + \cdots + a_k x^k + a_{k+1} x^{k+1} + \cdots$

$a_k + a_{k+1} x + a_{k+2} x^2 + \cdots$

$$\frac{\delta(x) - (a_0 + a_1 x + \cdots + a_{k-1} x^{k-1})}{x^k} = A(x)$$

$B(x) = ogf(a_{i-k})$

$\underbrace{0+0+\dots}_{k} a_0 x^k + a_1 x^{k+1} + a_2 x^{k+2} + \dots$

$B(x) = S(x) \cdot x^k$

$ogf(n \cdot a_n) = x \cdot D\, ogf(a_n)$

$ogf\left(\frac{a_n}{n}\right) = \int \frac{ogf(a_n) - a_0}{x}$

Moltiplicare o dividere per $1-x$

$ogf(a_i) = A(x)$ → n-esimo

Quanto fa $A(x) \cdot (1-x)$? $= B(x)$

$B(x) = ogf\left(\sum_{j=0}^{k} a_0 \cdot 0 + a_1 \cdot 0 + \dots - a_{n-1} + a_n\right) = ogf(a_n - a_{n-1})$

Dividere per $1-x$ = moltiplicare per $\frac{1}{1-x}$ =

$ogf(1) \qquad A(x) \cdot \frac{1}{1-x} = ogf\left(\sum_{j=0}^{n} a_j\right)$

$Egf(a_i) = ogf\left(\frac{a_i}{i!}\right)$

$Egf(a_i) \cdot Egf(b_i) = ogf\left(\frac{a_i}{i!}\right) \cdot ogf\left(\frac{b_i}{i!}\right) = ogf\left(\sum_{j=0}^{n} a_j \cdot b_{n-j} \cdot \frac{1}{j!(n-j)!}\right) = Egf\left(\sum_{j=0}^{n} \binom{n}{j} \cdot a_j \cdot b_{n-j}\right)$

$Egf(a_{i+k}) = D^k\, egf(a_i)$

$Egf(a_{i-k}) = \int^k egf(a_i)$

Mac Laurin

$A(x) = ogf(a_i)$ $\qquad [x^k]\, ogf(a_i)$

$[\ ]\, \Delta^k ogf(a_n) = a_k \cdot k!$

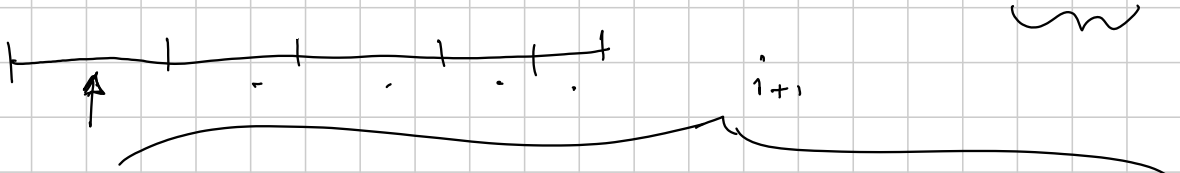
$$[x^k]\, ogf(a_i) = \frac{[\Delta^k ogf(a_i)]_0}{k!}$$

$$ogf(a^n) = \frac{1}{1-ax}$$

$$ogf\left(\binom{k}{i}\right) = (x+1)^k$$

$$ogf\left(\binom{i+k}{k}\right) = \binom{k}{k} + \binom{k+1}{k}x + \binom{k+2}{k}x^2 + \cdots$$

Partizionare n in $i+1$ parti si può fare in $\binom{n+i}{i}$.



$$(\ x^k\ )(\ x^n\ )(\ x^3\ )\cdots(\ x^k\ )$$

$$[x^n](1 + x + x^2 + x^3 + \cdots)(1 + x + x^2 + x^3 + \cdots)\cdots(1 + x + x^2 + x^3 + \cdots)$$

CORRETTO DOPO VIDEO

$$\left|\frac{1}{(1-x)^{k+1}}\right| \qquad \left|\binom{n+i}{i}\right|$$

$$(1 + x + x^2 + \cdots)^{k+1} = ogf\left(\binom{n+k}{k}\right)$$

$$\lim_{k\to\infty} \sum_{i=0}^{\infty} \frac{\binom{i+k}{k}}{(k+2)^i}$$

$\frac{1}{k+2}$ nella formula di $\operatorname{ogf}\left(\binom{n+k}{k}\right)$

$$\lim_{n\to\infty} \frac{1}{\left(1-\frac{1}{k+2}\right)^{k+1}} = \left(\frac{1}{\frac{k+2-1}{k+2}}\right)^{k+1} = \left(\frac{k+2}{k+1}\right)^{k+1} = \left(1+\frac{1}{k+1}\right)^{k+1}$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots$$

$$a_{n+k} = 80\, a_n + 57\, a_{n+1} - \cdots + 29\, a_{n+k-1}$$

$$a_{n+1} = \sum_{i=0}^{n} a_i \cdot b_{n-i} \qquad A(x) = \operatorname{ogf}(a_n)$$

$$\operatorname{ogf}(a_{n+1}) = \operatorname{ogf}(a_n) \cdot \operatorname{ogf}(b_n)$$

$$\frac{\operatorname{ogf}(a_n) - a_0}{x}$$

$$\frac{A(x)-a_0}{x} = A(x)\,B(x) \Rightarrow A(x) = \frac{a_0}{1-xB(x)}$$

Catalan

Il numero di modi in cui ordinare n parentesi aperte e n chiuse in modo valido.

$((\,)(\,)(\,))$ $\quad C_5$

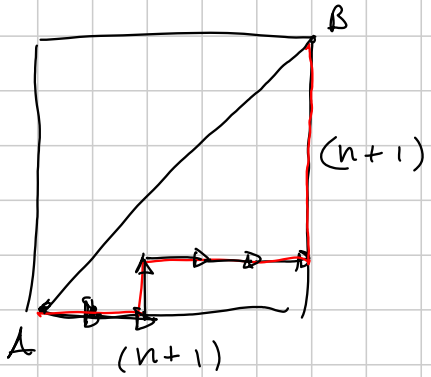
$2n$

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

$(\,(\,-\text{MINIMA}\,|\,)\,)$

c'è una $2k$-stringa buona

$C_n = \sum_{i=1}^{n} C_{i-1} \cdot C_{n-i}$



$\rightarrow$ $\uparrow$ C_n

$\rightarrow = (\quad \uparrow =)$.

$C(x) = \text{ogf}(C_n)$

$C_{n+1} = \sum_{i=0}^{n} C_i \cdot C_{n-i} \Rightarrow C(x) = \frac{C_0}{1 - x\,C(x)}$

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

$\frac{(1-\sqrt{1-4x})(1+\sqrt{1-4x})}{2x\,(1+\sqrt{1-4x})} = \frac{1-(1-4x)}{2x\,(\text{ROBA senza } x)} = \frac{2}{1+\sqrt{1-4x}}$

Snake oil method

$a_i = \sum \text{BRUTTO}$ $\quad i \mapsto n$

$b_n = \sum_{\delta=0}^{n} \binom{2\delta}{\delta}$ $\qquad B(x) = \sum_{n=0}^{\infty} x^n \sum_{\delta=0}^{n} \binom{2\delta}{\delta}$

$B(x) = \sum_{\delta=0}^{\infty} \sum_{n=\delta}^{\infty} x^n \binom{2\delta}{\delta} = \sum_{\delta=0}^{\infty} \binom{2\delta}{\delta} \cdot \sum_{n=\delta}^{\infty} x^n$

b_0 $\boxed{j=0}$

b_1 $\boxed{j=0}$ $\boxed{j=1}$

b_2 $\boxed{j=0}$ $\boxed{j=1}$ $\boxed{j=2}$

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

Figo.

$$\forall n \in \mathbb{N} \quad \sum_{i=1}^{n} \binom{n+i-1}{2i-1} = F_{2n}$$

$$\sum_{n=0}^{\infty} x^n \sum_{i=1}^{n} \binom{n+i-1}{2i-1} = \sum_{i=1}^{\infty} \sum_{n=i}^{\infty} x^n \binom{n+i-1}{2i-1}$$

$\operatorname{ogf}\left(\binom{n+k}{k}\right)$ $\quad \binom{(n+i)+i-1}{2i-1}$ $\quad x^i \sum_{n=0}^{\infty} x^{n-i} \binom{(n-i)+2i-1}{2i-1}$

$\boxed{2i-1}$

$\operatorname{ogf}\binom{n+2i-1}{2i-1}$ Shiftata di $\boxed{-i}$

$$x^i \sum_{n=0}^{\infty} x^n \binom{n+2i-1}{2i-1} = x^i \frac{1}{(1-x)^{2i}} = \left[\frac{x}{(1-x)^2}\right]^i$$

$$\sum_{i=0}^{\infty} \left(\frac{x}{(1-x)^2}\right)^i = \frac{1}{1-\left(\frac{x}{(1-x)^2}\right)} - 1$$

$F_{2n} =$ $\quad F_{2n+4} = 3F_{2n+2} - F_{2n}$

Roots of unity filter

$A(x) = ogf(a_i)$ $\quad ogf(a_{pi})$ con $p \in \mathbb{P}$

$\omega \Rightarrow 1 + \omega + \omega^2 + \dots + \omega^{p-1} = 0$

$$\frac{\sum_{i=0}^{p-1} A(\omega^i x)}{p} = a_0 + a_p x^p + a_{2p} x^{2p} + \dots$$

$$\sum_{i=0}^{p-1} a_n x^n \omega^{ni} = \begin{cases} p \nmid n \\ p \mid n \end{cases}$$

$$a_n x^n \sum_{i=0}^{p-1} \omega^{in} = \begin{cases} p \mid n = a_n x^n (1+1+\dots+1) = p\, a_n x^n \\ p \nmid n \Rightarrow a_n x^n \cdot 0 \end{cases}$$

Somma di una permutazione delle radici

$n \in \mathbb{N}$

$A(n)$ è il numero di $2n$-uple $(x_1, x_2, \dots, x_n, r_1, r_2, \dots, r_n)$ t.c. $\sum_{i=1}^{n} x_i r_i \equiv 0 \pmod 2$

$B(n)$ le altre

Calcolare $\frac{A(n)}{B(n)}$

$(x_i, r_i) \in \{(0,1), (1,0), (\omega, 0)\}$

$(1,1)$ $\quad (x_1, r_1)$

$$[x^n](x+1+1+1)^n = [x^n](x+3)^n = \quad S(x)$$

$$\frac{S(x)+S(-x)}{2} \qquad A(n) = \frac{(1+3)^n + (-1+3)^n}{2}$$

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

$$\frac{4^n+2^n}{4^n-2^n} = \boxed{\frac{2^n+1}{2^n-1}}$$

Quanti sono i numeri $\equiv 0 \ (3)$ con n cifre tra queste:

$$\{2,3,7,9\}.$$

$$[x^n](x^2+x^3+x^7+x^9)^n = P(x)$$

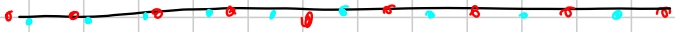
$$N = \frac{P(1)+P(\omega)+P(\omega^2)}{3}$$

$$\frac{4^n + \overbrace{(\omega^2+1+\omega+1)}^{0}{}^n + \overbrace{(\omega+1+\omega^2+1)}^{0}{}^n}{3} = \frac{4^n+2}{3}$$

Exact covering System

$(a_1, b_1); (a_2, b_2); \dots; (a_k, b_k)$ di interi con $b_i > 1 \ \forall i$.

$a_i + n b_i$



$(1,2)\ (2,4)\ (0,4)$.

$$\sum_{m=1}^{k} \frac{1}{b_m} = 1$$

$\exists\, i,j : b_i = b_j$ (Errato)

$\exists\, i : 2 \mid b_i \quad \forall i,j \ b_i = b_j$

$a_i + n b_i$ come la scrivo con generatrici??

$$\sum_{i=1}^{k} X^{a_i} + X^{a_i+b_i} + X^{a_i+2b_i} + X^{a_i+3b_i} + \dots = 1 + x + x^2 + \dots$$

$$X^{a_i} \sum_{j=0}^{\infty} (X^{b_i})^j = \frac{X^{a_i}}{1 - X^{b_i}}$$

$$(*) \quad \sum_{i=1}^{k} \frac{X^{a_i}}{1 - X^{b_i}} = \frac{1}{1-X} \Longrightarrow \sum_{i=1}^{k} \frac{X^{a_i}}{1 + X + X^2 + \dots + X^{b_i - 1}} = 1$$

$$\sum_{i=1}^{k} \frac{1}{b_i} = 1$$

Considerare il b_i massimo e porre X una sua radice

dell'unità primitiva. b_5

$\frac{x^{a_5}}{1-x^{b_5}}$ un mese.

A, B partizione di $\mathbb{N}$ (con 0)

$\forall n \quad \left| \{ x, y \mid (x,y) \in A^2 ; \; x \neq y ; \; x+y=n \} \right| =$ ↑ B

$A(x) = x^7 + x^9 + x^{51} + \dots$

$B(x) =$ gli altri

$$\begin{cases} A(x) + B(x) = \frac{1}{1-x} \\ A(x)^2 - A(x^2) = B(x)^2 - B(x^2) \end{cases}$$

$B(x) = \frac{1}{1-x} - A(x)$

$$A(x)^2 - A(x^2) = \left(\frac{1}{1-x}\right)^2 + A(x)^2 - \frac{2}{1-x} A(x) - \frac{1}{1-x^2} + A(x^2)$$

$$2A(x^2) - \frac{2}{1-x} A(x) = \frac{1}{1-x^2} - \frac{1}{(1-x)^2}$$

$[x^k] \; 2A(x^2) - \frac{2}{1-x} A(x) =$ Definito.

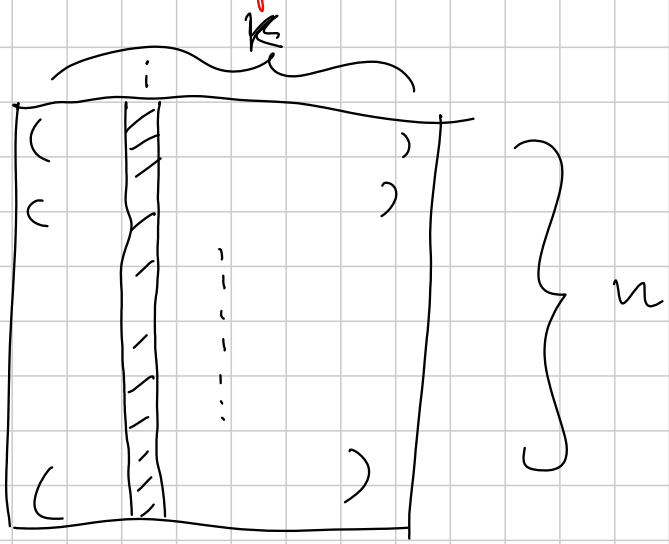
A, B

A, B partizionano in base alla parità del numero di 1 nella rappresentazione binaria.

Una scheduine è un insieme non ordinato di k-uple ordinate.

Exponential formula

n - scheduine



Scheduine vuote: solo 0

Giocare una scheduine: rimpiazzare gli 0 con numeri interi.

L'unione di una m-scheduine con una n - scheduine è una m+n - scheduine senza colore.

Le scheduine hanno un colore

Una (a,b)-scommessa è un insieme di b scheduine con nome dei costi a t.c. ogni colonna dell'unione è tra l'insieme $\{1, 2, 3, \dots, a\}$.

Assumo che esistano d_n colori per le n-scheduine.

Definisco $D(x) = \frac{d_0}{0!^k} + \frac{d_1}{1!^k} x + \frac{d_2}{2!^k} x^2 + \dots$

Assumo che di ognuno ne ho infinite vuote. Questo lo chiamo negozio di $D(x)$.

Chiamo $\int^{D(x)}(a,b)$ numero di (a,b) scommesse diverse creabili con le scheduine del negozio giocabile.

Definisco $H^{D(x)}(x,y)$ t.c. $[x^a y^b] H^{D(x)}(x,y) = a!^k \cdot \delta^{D(x)}(a,b)$

$$H^{\sqrt{D(x)}}(x,y) = e^{y D(x)}$$

enumerare

Ponendo $k=1$

Lemma 1: Se un negozio ha solo una seledina $\Leftrightarrow$ un tipo di
la formula vale. $G(x)$

$$G(x) = \frac{x^n}{(n!)^k}$$

Lemma 2: Se 2 negozi A,B hanno associate $A(x), B(x)$.
Chiamo C il negozio che ha associato $A(x) + B(x) = C(x)$

$$H^{C(x)}(x,y) = H^{A(x)}(x,y) \cdot H^{B(x)}(x,y)$$

Lemma 3: $[x^n] e^{y f(x)}$ = se taglio $f(x)$ al coef n-esimo

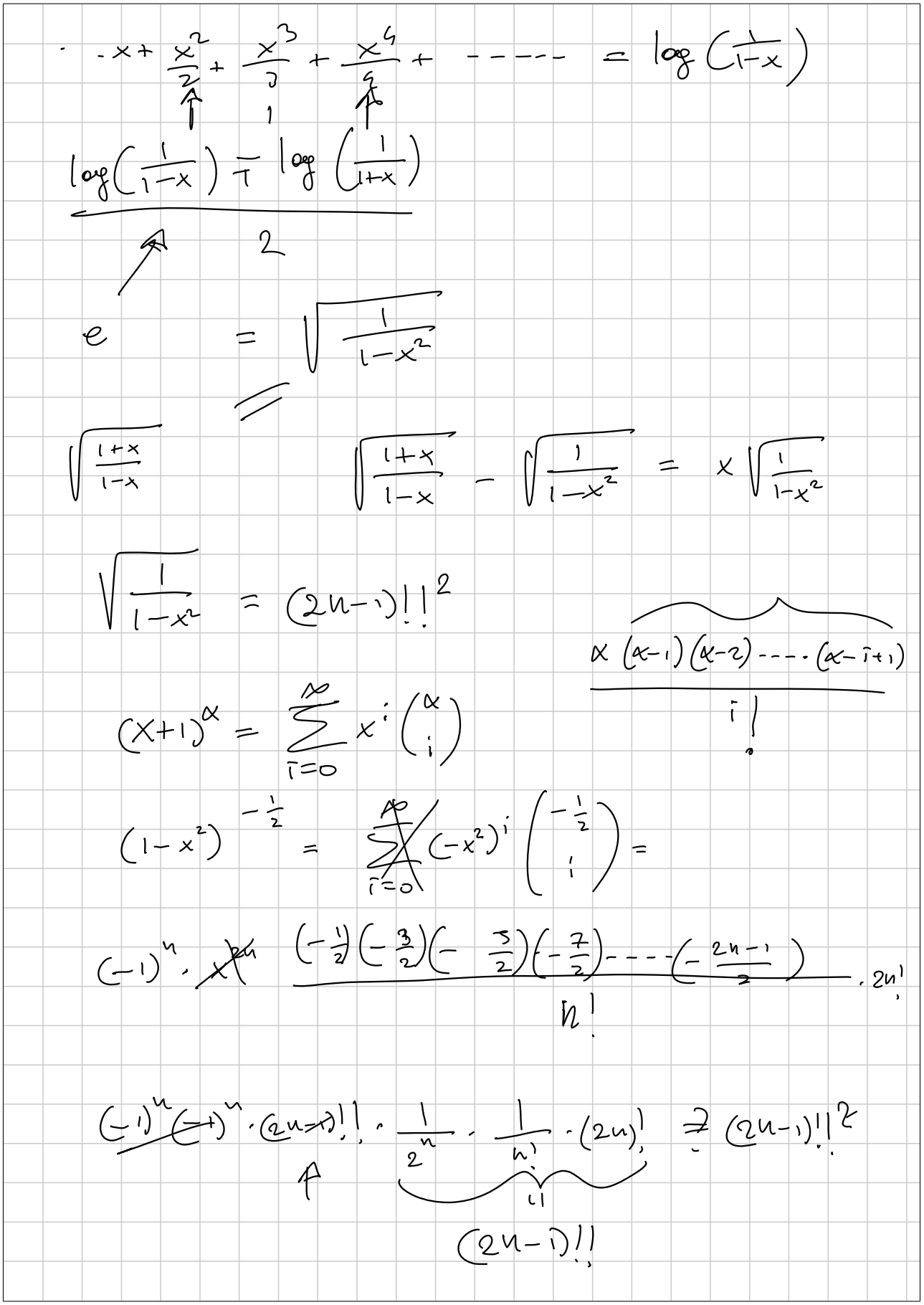
---

$\sigma : (1,2,\dots,2n) \to (1,2,\dots 2n)$

Le ~~sole~~ $2k$- seledine sono $[(2k-1)!]$
Le $2k+1$ - " sono 0

$$B(x) = 0 + \frac{x^2 \cdot (2-1)!}{2!} + \frac{x^4 (4-1)!}{4!} + \dots = \frac{x^2}{2} + \frac{x^4}{4} + \frac{x^6}{6} + \dots$$

$$e^{*B(x)} \rightsquigarrow e^{D(x)} =$$


$-x+\frac{x^2}{2}+\frac{x^3}{3}+\frac{x^4}{4}+\cdots = \log\left(\frac{1}{1-x}\right)$
$\log\left(\frac{1}{1-x}\right) - \log\left(\frac{1}{1+x}\right)$
2
$e = \sqrt{\frac{1}{1-x^2}}$
$\sqrt{\frac{1+x}{1-x}}$
$\sqrt{\frac{1+x}{1-x}} - \sqrt{\frac{1}{1-x^2}} = x\sqrt{\frac{1}{1-x^2}}$
$\sqrt{\frac{1}{1-x^2}} = (2n-1)!!^2$
$\frac{\alpha(\alpha-1)(\alpha-2)\cdots(\alpha-i+1)}{i!}$
$(X+1)^\alpha = \sum_{i=0}^{\infty} x^i \binom{\alpha}{i}$
$(1-x^2)^{-\frac{1}{2}} = \sum_{i=0}^{\infty} (-x^2)^i \binom{-\frac{1}{2}}{i} =$
$(-1)^n \cdot x^{2n} \frac{\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)\left(-\frac{5}{2}\right)\left(-\frac{7}{2}\right)\cdots\left(-\frac{2n-1}{2}\right)}{n!} \cdot 2n!$
$(-1)^n(-1)^n \cdot (2n-1)!! \cdot \frac{1}{2^n} \cdot \frac{1}{n!} \cdot (2n)! = (2n-1)!!^2$
$(2n-1)!!$

$$\frac{1}{\sqrt{1-4x}} = \text{ogf}\left(\binom{2n}{n}\right).$$

In quanti modi posso mettere in pedana un cuneo scacchiera $n \times n$ in modo che ce ne sia 1 per riga e per colonna.

Una funzione generatrice è una corda a cui appendere una successione per metterla in mostra

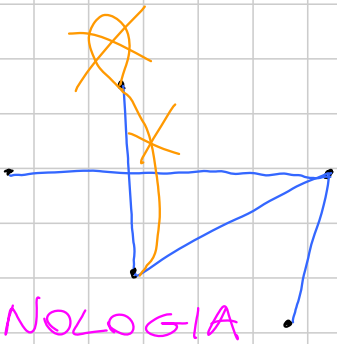
Mr Herbert Wilf

COMBINATORIA 2 (medium)

Titolo nota 10/09/2010

TEORIA DEI GRAFI

(A, E)



vertici A (nodi)

archi $E \subseteq \{\{a,b\} \mid a \neq b \in A\}$

TERMINOLOGIA

CONNESSO, CICLO, ALBERO (connesso aciclico), COMPLETO K^n

BIPARTITO

TEORIA DI RAMSEY

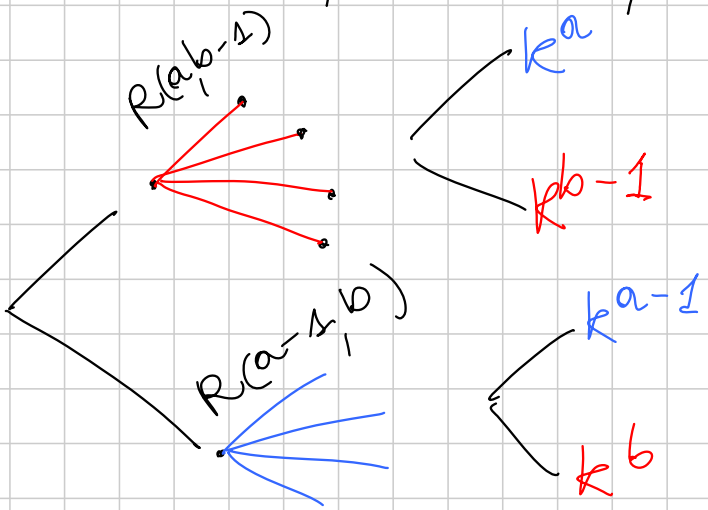
6 persone; $\exists$ 3 persone che si conoscono / $\exists$ 3 persone 2 a 2 sconosciute

K^6 contiene, comunque 2-colorato K^3 o K^3

(RAMSEY) a, b $\exists$ $R(a,b)$ t.c. se 2-coloro $K^{R(a,b)}$ in m e m ho un K^a o un K^b

dim (induzione su $a+b$)

$$R(a,b) \leq R(a,b-1) + R(a-1,b)$$



(IMO 1964, 4) 17 studiosi intrattengono corrispondenza (2 a 2) su 3 argomenti. $\exists$ 3 studiosi che corrispondono sullo stesso argomento.

$R(3,3,3) = ?$

$$R(a,b,c) \leq R(a-1,b,c) + R(a,b-1,c) + R(a,b,c-1) - 1$$

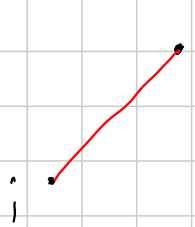
$$\Rightarrow R(3,3,3) \leq 3R(2,3,3) - 1$$

$$\| \quad 6$$

(IMO 1978.6) $\{1 \dots 1978\}$
6-colorato

$\exists$? una terna monocromatica (x, y, z) con $x + y = z$

[Schur]



se $|i-j|$ è

$R(3,3,3,3,3,3) \Rightarrow$ c'è

un triangolo monocromatico (wlog)

$\rightsquigarrow$ $|i-j|, |j-k|, |k-i|$ sono

$\rightsquigarrow$ $i - j + j - k = i - k$

$i \geq j \geq k$

$R(3 \dots 3) \leq 1978$

- $R(3 \dots 3) - 1 \leq r(R(3 \dots 3) - 1) + 1$

(r volte; $r-1$)

$S_r \leq$

$S_r < r\, S_{r-1}$

5

$R(3,3,3,3,3,3) - 1 < 6 \cdot 5 \cdot 4 \cdot 3\, S_2$

$R(3,3,3,3,3,3) \leq 1800$

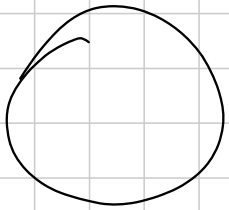
ES $R(3 \overset{r}{\dots} 3) \leq \lfloor e r! \rfloor + 1$ ↑ parte intera

Se chiedevo $x + y = 2z$

↳ $x - z = z - y$

[Van der Waerden] dati r, k esiste $W(r,k)$ tc. se r-colora i numeri $\{1 \dots W(r,k)\}$ trovo una prog. arit. monocromatica lunga k.

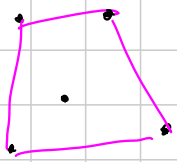
ES



colorata con r colori allora esistono infiniti (più che numerabili) triangoli isosceli monocromatici.

HAPPY END THEOREM

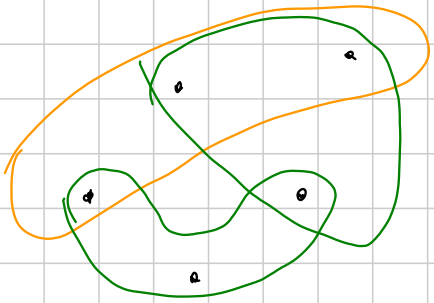
Dati 5 pti nel piano (in posizione generale) ce ne sono 4 che formano un quadrilatero convesso.



[Erdős - Szekeres] $\forall n \; \exists N$ tc dati N pti nel piano i.p.g. esistono n

che formano un n-agono convesso.

IPERGRAFO



Vale Ramsey!

Dati r colori e $a_1, a_2 \dots a_r$ esiste

$$R_k(a_1, a_2, \dots a_r)$$

- Un n-agono è convesso $\iff$ lo sono tutti i suoi quadrilateri.
- $R_4(5, n)$ va bene!

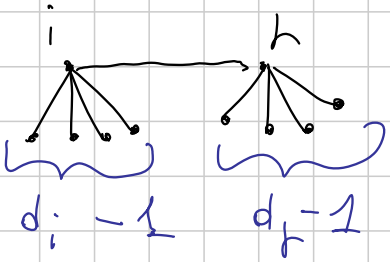
EXTREMAL GRAPH THEORY

Quanti archi minimo metto su n vertici per assicurare un K_3?

$$\left\lfloor \frac{n^2}{4} \right\rfloor + 1$$

Dimostriamo! G è un grafo senza triangoli "estremale" su n vertici.

$|E|$ archi



$$d_i - 1 + d_j - 1 \leq n-2$$
$$d_i + d_j \leq n$$

$$n|E| \geq \sum_{ij \text{ arco}} d_i + d_j = \sum_i d_i^2$$

$$\sum d_i^2 \cdot \underbrace{\sum_i 1^2}_{n} \geq \left(\sum d_i\right)^2$$

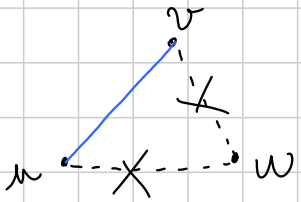
$$n^2|E| \geq 4|E|^2 \rightsquigarrow |E| \leq \frac{n^2}{4}$$

[Turàn] Un grafo su n vertici senza k-sottografi completi ha al più $\left\lfloor \frac{(k-2)n^2}{2(k-1)} \right\rfloor$

$$\left[\left[n = (k-1)h \right.\right.$$
$$\left.\left. \binom{k-1}{2} h^2 = \frac{(k-1)(k-2)n^2}{2(k-1)(k-1)} \right]\right]$$

G grafo senza k^k estremale.
dimostro che è $k-1$-partito completo.

CLAIM



NON può succedere

dimostro.

CASO 1 $d(w) < d(u)$

Cancello w e "raddoppio" u

→ gli archi diventano
$$|E| - d(w) + d(u) > |E|$$

→ può contenere un k^k ?
- senza $\tilde{u}$? NO
- con u e $\tilde{u}$? NO
- con $\tilde{u}$ e senza u ? NO

CASO 2 $d(w) \geq \begin{matrix} d(u) \\ d(v) \end{matrix}$ Cancello u e v e "triplico" w

→ $|E| - d(u) - d(v) + 1 + 2d(w) > |E|$

→ può contenere un k^k ?
- con più di una dei w fratelli? NO
- con (al più) uno dei w? NO

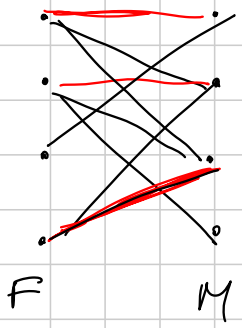
ES $5n$ punti $10n^2 + 1$ archi; comunque lo colora con 2 colori ha un triangolo monocromatico.

$$\frac{(k-2)(5n)^2}{(k-1)2} \qquad \frac{4 \cdot 25n^2}{10} = 10n^2$$

6

→ il mio grafo ha un K^6 → RAMSEY...

MATCHING



donne

$|A|$

$|B|$

uomini

ogni donna ha un po' di uomini che piacciono.

Posso sposare le tutte donne a partner graditi?

uomini graditi alle tizie di S

$S \subseteq A \quad |\Gamma(S)| \geq |S|$

CONDIZIONE NECESSARIA

[Hall] $\forall S \subseteq A \quad |\Gamma(S)| \geq |S| \iff$ esiste un "perfect matching"

$\Leftarrow$ già fatta

dimostriamo! induzione su $|A| = |B|$

$\forall S \quad |\Gamma(S)| \geq |S|$

- $|\Gamma(S)| = |S|$, $S \neq A$
  - S ha un perfect matching con $\Gamma(S)$
  - $A \setminus S$ ha un perfect matching con $B \setminus \Gamma(S)$
    - $S' \subseteq A \setminus S \quad |\Gamma(S') \cap (B \setminus \Gamma(S))| \geq |S'|$

per assurdo ho $<$

$\Gamma(S' \cup S) < |\Gamma(S') \cap (B \setminus \Gamma(S))| + |\Gamma(S)| < |S' \cup S|$

$\Downarrow$

$|S|$

$\exists\, |\Gamma(S)| > |S| \quad \forall S \subsetneq A$

prendo x e un suo vicino y.

se grafo $A \setminus \{x\} \cup B \setminus \{y\}$ soddisfa la condizione:

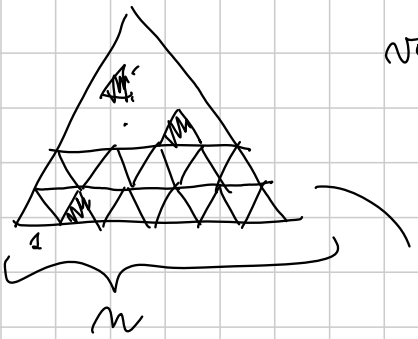
per ass. $S' \subseteq A \setminus \{x\}$ $|\Gamma(S')| > |S'|$

└ c'è y ma $|\Gamma(S') \setminus \{y\}| \geq |S'|$

se non c'è ancora meglio

□

ES (ISL 2006. C6)



voglio tassellarlo ◇

n buchi ▲

∀ sottotriangolo da k  ha almeno k buchi ▲

k

TEOREMA DI DILWORTH

$(X, \leq)$ poset

ORDINE PARZIALE
$\leq$ è una RELAZIONE su X
- riflessiva $(x \leq x)$
- antisimmetrica $(x \leq y, y \leq x \Rightarrow x = y)$
- transitiva $(x \leq y, y \leq z \Rightarrow x \leq z)$

$(\mathbb{R}, \geq)$, $(\mathbb{R}^2, \geq)$, $(\mathbb{N}, |)$, $(\mathcal{P}(X), \subseteq)$

$(a,b) \geq (c,d) \iff a \geq c, b \geq d$

[Dilworth] La cardinalità della massima anticatena è uguale al minimo numero di catene la cui unione è tutto.

$(X, \leq)$ poset $x_1 < x_2 < \dots < x_n$ è una CATENA (di lunghezza n)

Un insieme $A \subseteq X$ con elementi 2 a 2 NON CONFRONTABILI è un' ANTICATENA.

[Dilworth duale] Sostituisci "catena" con "anticatena" e viceversa.

[ROM TST '05] n^2+1 interi tc $\forall$ sott da $n+1$ c'è una coppia di el. $(a,b) \mid a \mid b$, allora posso trovare

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

la massima anticatena ha # $\leq n$.

$\rightsquigarrow$ riesco a coprire tutto con al + n catene

Quanto possono essere lunghe?
Almeno una è lunga (almeno) $n+1$.

[Erdős – Szekeres] Successione di $ab+1$ reali distinti
Allora ha una sottosuccessione crescente da $a+1$, o una decrescente da $b+1$.

$x_1 \dots x_{ab+1}$ $\quad x_i < x_j$ se $i < j$, $x_i < x_j$

max anticatena $\leq b$

$\rightsquigarrow$ ricopro con b catene (succ crescenti)

$\rightsquigarrow \exists$ una catena lunga $a+1$

alessandra.caraceni@sns.it

G 1 - Medium - TRIGO

Titolo nota 06/09/2010

$z = a + ib \qquad e^z = e^a(\cos b + i \operatorname{sen} b)$

$e^z e^w = e^{z+w} = e^{a+c}(\cos(b+d) + i \operatorname{sen}(b+d))$

$z = a + ib$

$w = c + id$

$(x + iy)(s + it) =$

$= (xs - yt) + i(xt + ys)$

$a = c = 0$

$(\cos b + i \operatorname{sen} b)(\cos d + i \operatorname{sen} d) =$

$= \cos(b+d) + i \operatorname{sen}(b+d)$

$\Rightarrow \cos(b+d) = \cos b \cos d - \operatorname{sen} b \operatorname{sen} d$

$\operatorname{sen}(b+d) = \cos b \operatorname{sen} d + \operatorname{sen} b \cos d$

$$\sum_{n=1}^{2010} \operatorname{sen}(n\theta) = \sum_{n=1}^{2010} \operatorname{Im}\left(e^{in\theta}\right) =$$

$$= \operatorname{Im}\left(\sum_{n=1}^{2010} e^{in\theta}\right) = \operatorname{Im}\left(\sum_{n=1}^{2010} (e^{i\theta})^n\right) =$$

$$= \operatorname{Im}\left(\frac{e^{i2011\theta} - 1}{e^{i\theta} - 1} - 1\right) = \operatorname{Im}\left(\frac{e^{i\theta \cdot 2011} - 1}{e^{i\theta} - 1}\right) =$$

$$= \operatorname{Im}\left(\frac{\cos(2011\theta) - 1 + i \operatorname{sen} 2011\theta}{\cos\theta - 1 + i \operatorname{sen}\theta}\right) =$$

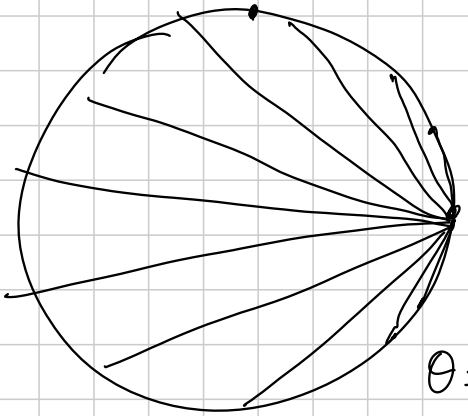
$$= \mathrm{Im}\left[\frac{\left[\cos(2011\theta)-1+i\sin(2011\theta)\right](\cos\theta-1-i\sin\theta)}{(\cos\theta-1)^2+\sin^2\theta}\right] =$$

$$= \frac{\sin(2011\theta)(\cos\theta-1)-\sin\theta\left[\cos(2011\theta)-1\right]}{\cos^2\theta-2\cos\theta+1+\sin^2\theta} =$$

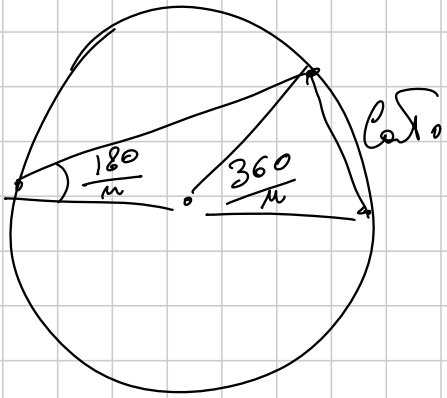
$$= \frac{\sin(2010\cdot\theta)-\sin(2011\cdot\theta)+\sin\theta}{2(1-\cos\theta)}$$

Es: n-agono regolare inscritto nella cf. unitaria.

Quanto vale il prodotto di tutti i lati e tutte le diagonali?



$\theta = \frac{180}{n}$



Teo del seno: $\text{lato} = 2R\sin\theta = 2\sin\theta$

ℓ - diagonale $= 2\sin 2\theta$

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

$$??= \prod_{k=1}^{n-1} 2\cdot\sin(k\theta) =$$

$$= 2^{n-1} \prod_{k=1}^{n-1} \sin(k\theta) = 2^{n-1} \prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right)$$

$$\prod_{k=1}^{n-1} \left|1 - e^{i\frac{2k\pi}{n}}\right| = \left| \prod_{k=1}^{n-1} (1 - \xi_k) \right| = |p(1)| = n$$

$$\prod_{k=1}^{n-1} (x - \xi_k) = \frac{x^n - 1}{x - 1} = \sum_{k=0}^{n-1} x^k = p(x)$$

$$\prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right) = \frac{n}{2^{n-1}}$$

Es: $x_{n+1} = \dfrac{1 + x_n}{1 - x_n}$ $\quad x_0 = 2010$ $\quad x_{2012} = ?$

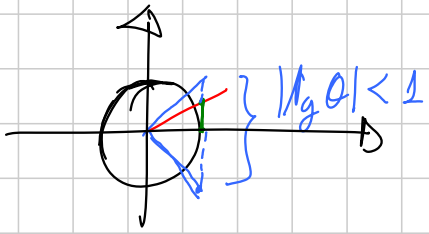
$x_n = \operatorname{tg} \alpha_n \qquad \alpha_{n+1} = \dfrac{1 + \operatorname{tg}\alpha_n}{1 - \operatorname{tg}\alpha_n} = \operatorname{tg}\left(\alpha_n + \frac{\pi}{4}\right)$

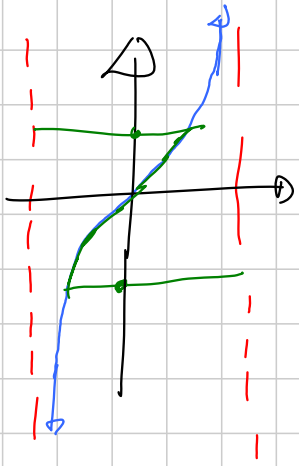
$\operatorname{tan}(\theta + \varphi) = \dfrac{\operatorname{Tan}\theta + \operatorname{Tan}\varphi}{1 - \operatorname{Tan}\theta \operatorname{Tan}\varphi} \qquad \alpha_{n+1} = \alpha_n + \frac{\pi}{4} \mod 2\pi$

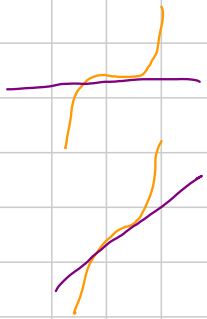
Es: Dati 5 numeri reali $\neq 1, -1$, Tra di essi ve ne sono 2, a e b tali che
$|ab + 1| > |a - b|$

$\left|\dfrac{a-b}{ab+1}\right| < 1 \qquad a = \operatorname{tg}\alpha$
$b = \operatorname{tg}\beta$

$|\operatorname{tg}(\alpha - \beta)| < 1 \qquad |\alpha - \beta| < \frac{\pi}{4}$







OSS: $\tg : \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \to \mathbb{R}$ è biiettiva

$\Downarrow$

Dati 5 numeri reali $\neq -1, 1$ x_i $\exists$ 5 angoli θ_i t.c. $x_i = \tg\theta_i$ $-\frac{\pi}{2} < \theta_i < \frac{\pi}{2}$

ABC Triangolo A, B, C gli angoli: $A+B+C = \pi$

•) $\tan\frac{A}{2}\tan\frac{B}{2} + \tan\frac{B}{2}\tan\frac{C}{2} + \tan\frac{C}{2}\tan\frac{A}{2} = 1$

$C = \pi - A - B \qquad \frac{C}{2} = \frac{\pi}{2} - \left(\frac{A}{2} + \frac{B}{2}\right)$

$$\tan\frac{C}{2} = \cot\left(\frac{A}{2}+\frac{B}{2}\right) = \frac{1}{\tg\left(\frac{A}{2}+\frac{B}{2}\right)}$$

$$\tan\frac{A}{2}\cdot\tan\frac{B}{2} + \tan\frac{B}{2}\cdot\frac{1}{\tg\left(\frac{A}{2}+\frac{B}{2}\right)} + \tg\frac{A}{2}\,\frac{1}{\tg\left(\frac{A}{2}+\frac{B}{2}\right)} =$$

$$\tg\left(\frac{A}{2}+\frac{B}{2}\right) = \frac{\tg\frac{A}{2}+\tg\frac{B}{2}}{1-\tg\frac{A}{2}\tg\frac{B}{2}}$$

$$= \tg\frac{A}{2}\cdot\tg\frac{B}{2} + \tg\frac{B}{2}\left(1-\tg\frac{A}{2}\tg\frac{B}{2}\right) + \tg\frac{A}{2}\left(1-\tg\frac{A}{2}\tg\frac{B}{2}\right) =$$

$$\tg\frac{A}{2}+\tg\frac{B}{2} \qquad\qquad \tg\frac{A}{2}+\tg\frac{B}{2}$$

$$= \tan\frac{A}{2}\cdot\tan\frac{B}{2} + \left(1 - \tan\frac{A}{2}\tan\frac{B}{2}\right) = 1.$$

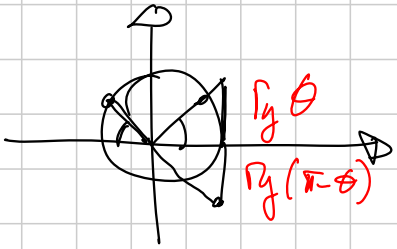
Cor: $\tan\frac{A}{2}\tan\frac{B}{2}\tan\frac{C}{2} \le \frac{\sqrt{3}}{9} = \frac{1}{3\sqrt{3}}$

$$1 = \tan\frac{A}{2}\tan\frac{B}{2} + \tan\frac{B}{2}\tan\frac{C}{2} + \tan\frac{C}{2}\tan\frac{A}{2} \ge 3\sqrt[3]{\left(\tan\frac{A}{2}\tan\frac{B}{2}\tan\frac{C}{2}\right)^2}$$

Cor: $\cot\frac{A}{2} + \cot\frac{B}{2} + \cot\frac{C}{2} = \cot\frac{A}{2}\cot\frac{B}{2}\cot\frac{C}{2}$

- $\tan A + \tan B + \tan C = \tan A \tan B \tan C$

$C = \pi - (A+B) \qquad \tan C = -\tan(A+B) = -\dfrac{\tan A + \tan B}{1 - \tan A \tan B}$



$$\frac{(\tan A + \tan B)(1 - \tan A\tan B) - \tan A - \tan B}{1 - \tan A\tan B} = -\frac{\tan A\tan B(\tan A + \tan B)}{1 - \tan A\tan B}$$

$$\tan A + \tan B - \tan A\tan B(\tan A + \tan B) - \tan A - \tan B$$

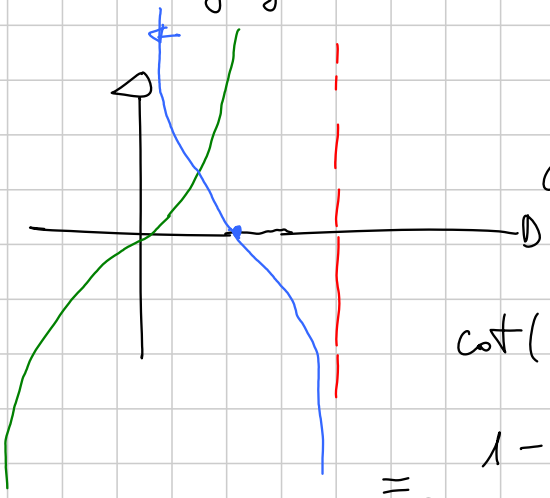
Cor: $\tan A \tan B \tan C \ge 3\sqrt{3}$

$\sum \tan A \ge 3\sqrt[3]{\prod \tan A} \qquad \prod \tan A \ge 3\sqrt{3}$

$\prod \tan A$

• $\cot A \cot B + \cot B \cot C + \cot C \cot A = 1$

e se $xy+yz+zx=1 \Rightarrow \exists A,B,C$ angoli di un Triangolo tali che $x=\cot A$ etc...



$\cot$ biiettiva da $(0,\pi) \to \mathbb{R}$

$$\cot(\alpha+\beta) = \frac{1}{\tan(\alpha+\beta)} = \frac{1-\tan\alpha\tan\beta}{\tan\alpha+\tan\beta} = \frac{\cot\alpha\cot\beta-1}{\cot\alpha+\cot\beta}$$

$$z = \frac{1-xy}{x+y} = -\cot(A+B)$$

•) $\sin^2\frac{A}{2}+\sin^2\frac{B}{2}+\sin^2\frac{C}{2}+2\sin\frac{A}{2}\sin\frac{B}{2}\sin\frac{C}{2}=1$

$x^2+y^2+z^2+2xyz=1, \quad x,y,z>0$

$\frac{C}{2} = \frac{\pi}{2} - \left(\frac{A}{2}+\frac{B}{2}\right)$ $\quad \sin^2\frac{C}{2} = \cos^2\left(\frac{A}{2}+\frac{B}{2}\right) = 1-\sin^2\left(\frac{A}{2}+\frac{B}{2}\right) =$

$= 1 - \sin^2\frac{A}{2}\cos^2\frac{B}{2} - \sin^2\frac{B}{2}\cos^2\frac{A}{2}$

$- 2\sin\frac{A}{2}\cos\frac{A}{2}\sin\frac{B}{2}\cos\frac{B}{2}$

$2\sin\frac{A}{2}\sin\frac{B}{2}\sin\frac{C}{2} = 2\sin\frac{A}{2}\sin\frac{B}{2}\cos\left(\frac{A}{2}+\frac{B}{2}\right) =$

$= 2\sin\frac{A}{2}\sin\frac{B}{2}\cos\frac{A}{2}\cos\frac{B}{2} - 2\sin^2\frac{A}{2}\sin^2\frac{B}{2}$

$$-\sin^2\frac{A}{2}\cos^2\frac{B}{2}-\sin^2\frac{B}{2}\cos^2\frac{A}{2}-2\sin\frac{A}{2}\sin\frac{B}{2}\cos\frac{A}{2}\cos\frac{B}{2}+$$

$$+2\sin\frac{A}{2}\sin\frac{B}{2}\cos\frac{A}{2}\cos\frac{B}{2}-2\sin^2\frac{A}{2}\sin^2\frac{B}{2}=$$

$$-\sin^2\frac{A}{2}-\sin^2\frac{B}{2}$$

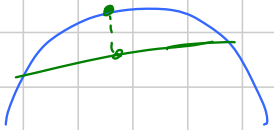
$$-\sin^2\frac{A}{2}\left(\cos^2\frac{B}{2}+\sin^2\frac{B}{2}\right)-\sin^2\frac{B}{2}\left(\sin^2\frac{A}{2}+\cos^2\frac{A}{2}\right)=$$

$$=-\sin^2\frac{A}{2}-\sin^2\frac{B}{2}.$$

$$x=-yz+\sqrt{(1-y^2)(1-z^2)}$$

Es: •) $\sin\frac{A}{2}\sin\frac{B}{2}\sin\frac{C}{2}\le\frac{1}{8}$

•) $\sin^2\frac{A}{2}+\sin^2\frac{B}{2}+\sin^2\frac{C}{2}\ge\frac{3}{4}$



•) $\cos^2\frac{A}{2}+\cos^2\frac{B}{2}+\cos^2\frac{C}{2}\le\frac{9}{4}$

•) $\cos\frac{A}{2}\cos\frac{B}{2}\cos\frac{C}{2}\le\frac{3\sqrt{3}}{8}$

•) $\csc\frac{A}{2}+\csc\frac{B}{2}+\csc\frac{C}{2}\ge 6$

Es: •) $\sum\sin 2A=4\prod\sin A$

•) $\sum\cos 2A=-1-4\prod\cos A$

•) $\sum\sin^2 A=2+2\prod\cos A$

•) $\sum\cos^2 A+2\prod\cos A=1$

$$\begin{cases} -x + y\cos B + z\cos C = 0 \\ x\cos B - y + z\cos A = 0 \\ x\cos C + y\cos A - z = 0 \end{cases} \qquad (\sin A, \sin C, \sin B)$$

$$\sum \cos^2 A + 2\prod \cos A - 1 = 0.$$

•) $4R = \dfrac{abc}{[ABC]} = \dfrac{abc}{S}$

$$R = \frac{a}{2\sin A} = \frac{abc}{2\sin A\, bc} = \frac{abc}{4S}$$

$$S = \frac{1}{2} bc \sin A$$

•) $2R^2 \sin A \sin B \sin C = S \iff \sin A \sin B \sin C = \dfrac{S}{2R^2}$

$a = 2R\sin A$
$b = 2R\sin B$
$c = 2R\sin C$

$S = \dfrac{abc}{4R}$ ⇓ $4R\sin A\sin B\sin C = \dfrac{abc}{2R^2}$

•) $2R\sin A\sin B\sin C = r(\sin A + \sin B + \sin C)$

•) $a\cos A + b\cos B + c\cos C = \dfrac{abc}{2R^2}$

$a\cos A = 2R\sin A\cos A = R\sin 2A$

$R(\sin 2A + \sin 2B + \sin 2C) = 4R\sin A\sin B\sin C$ QR.

•) $r = 4R\sin\frac{A}{2}\sin\frac{B}{2}\sin\frac{C}{2}$

BTW: $r = 4R\cdots \le \frac{1}{8}4R = \frac{R}{2}$

$r \le \frac{R}{2}$ Dis. di Eulero.

$IO^2 = R^2 - 2Rr = R(R-2r) > 0$

$$\sin^2\frac{A}{2} = \frac{1-\cos A}{2} = \frac{1}{2}\left(1 - \frac{b^2+c^2-a^2}{2bc}\right) =$$

bisezione Carnot

$$= \frac{1}{2}\left(\frac{a^2-(b-c)^2}{2bc}\right) = \frac{(a-b+c)(a+b-c)}{4bc} =$$

$$= \frac{(s-b)(s-c)}{bc} \qquad s = \frac{a+b+c}{2}$$

$$\sin\frac{A}{2} = \sqrt{\frac{(s-b)(s-c)}{bc}}$$

$$\sin\frac{A}{2}\sin\frac{B}{2}\sin\frac{C}{2} = \frac{(s-a)(s-b)(s-c)}{abc} =$$

$$= \frac{s(s-a)(s-b)(s-c)}{s\,abc} = \frac{[ABC]^2}{s\,abc} = \frac{[ABC]}{s}\cdot\frac{[ABC]}{abc} =$$

$$= r\cdot\frac{1}{4R}$$

a) $4R\cos\frac{A}{2}\cos\frac{B}{2}\cos\frac{C}{2} = s$

$$\frac{1}{2}\frac{R\sin A\sin B\sin C}{\sin\frac{A}{2}\sin\frac{B}{2}\sin\frac{C}{2}} = \frac{1}{2}\,\frac{\frac{[ABC]}{2R}}{\frac{r}{4R}} = \frac{[ABC]}{r} = s$$

$$\Rightarrow\quad s \le \frac{3\sqrt{3}}{2}R$$

b) $\cos A+\cos B+\cos C = 1+4\sin\frac{A}{2}\sin\frac{B}{2}\sin\frac{C}{2} = 1+\frac{r}{R}$

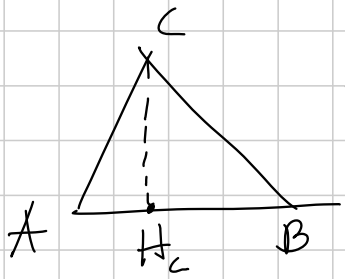
$$\cos A+\cos B = 2\cos\left(\frac{A+B}{2}\right)\cos\left(\frac{A-B}{2}\right) = 2\sin\frac{C}{2}\cos\left(\frac{A-B}{2}\right)$$

$$1-\cos C = 2\sin^2\frac{C}{2} = 2\sin\frac{C}{2}\cos\left(\frac{A+B}{2}\right)$$

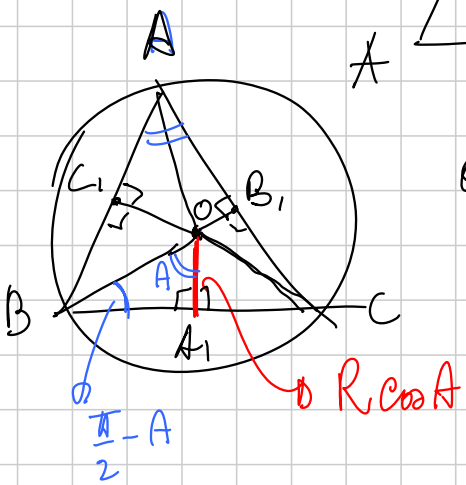
$$2\sin\frac{C}{2}\cos\left(\frac{A-B}{2}\right) = 2\sin\frac{C}{2}\cos\left(\frac{A+B}{2}\right) + 2\sin\frac{A}{2}\sin\frac{B}{2}\cdot 2\sin\frac{C}{2}$$

$$\cos\left(\frac{A-B}{2}\right) - \cos\left(\frac{A+B}{2}\right) = 2\sin\frac{A}{2}\sin\frac{B}{2}$$

Oss: $\cos A$



$AH_C = b\cos A$



$OA_1 + OB_1 + OC_1 = R + r$ T. di Tolomeo.

$OA \cdot C_1B_1 = AC_1 \cdot OB_1 + OC_1 \cdot AB_1$

$R\frac{a}{2} = \frac{c}{2}OB_1 + \frac{b}{2}OC_1$

$$R\left(\frac{a+b+c}{2}\right) = OA_1\cdot\left(\frac{c+b}{2}\right) + OB_1\left(\frac{c+a}{2}\right) + OC_1\left(\frac{a+b}{2}\right) =$$

$$= OA_1\left(1-\frac{a}{2}\right) + OB_1\left(1-\frac{b}{2}\right) + OC_1\left(1-\frac{c}{2}\right) =$$

$$= s\left(OA_1 + OB_1 + OC_1\right) - \frac{[ABC]}{s}$$

$OA_1 + OB_1 + OC_1 = R + r$

Es: ABC triangolo r, R i soliti, r_0 = raggio del cerchio inscritto nel triangolo degli excentri.

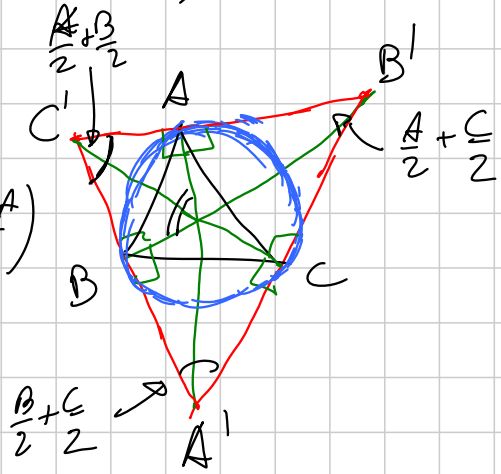
$\Rightarrow$ $r_0 \geq 2r$ $\qquad R \geq r_0 \geq 2r$

$$\frac{r}{4R} = \sin\frac{A}{2}\sin\frac{B}{2}\sin\frac{C}{2}$$

$$\frac{r_0}{4R_0} = \sin\left(\frac{A+B}{4}\right)\sin\left(\frac{B+C}{4}\right)\sin\left(\frac{C+A}{4}\right)$$

$\| \; 8R$

$$\frac{r_0}{4R} = 2\frac{r}{4R_0}$$



$$\prod \sin\left(\frac{A+B}{4}\right) \geq \prod \sin\frac{A}{2} \qquad \sin^4\left(\frac{A+B}{4}\right) \geq \sin\frac{A}{2}\sin\frac{B}{2}$$

$1 - 2\sin^2\frac{A+B}{4} = \cos\left(\frac{A+B}{2}\right)$

$$\sin^2\frac{A+B}{4} = \frac{1-\cos\left(\frac{A+B}{2}\right)}{2} = \frac{1-\sin\frac{C}{2}}{2}$$

$$\| \; \frac{1}{2}\left(1 - \cos\frac{A}{2}\cos\frac{B}{2} + \sin\frac{A}{2}\sin\frac{B}{2}\right)$$

$$1 - \cos\frac{A}{2}\cos\frac{B}{2} - \sin\frac{A}{2}\sin\frac{B}{2} \geq 0$$

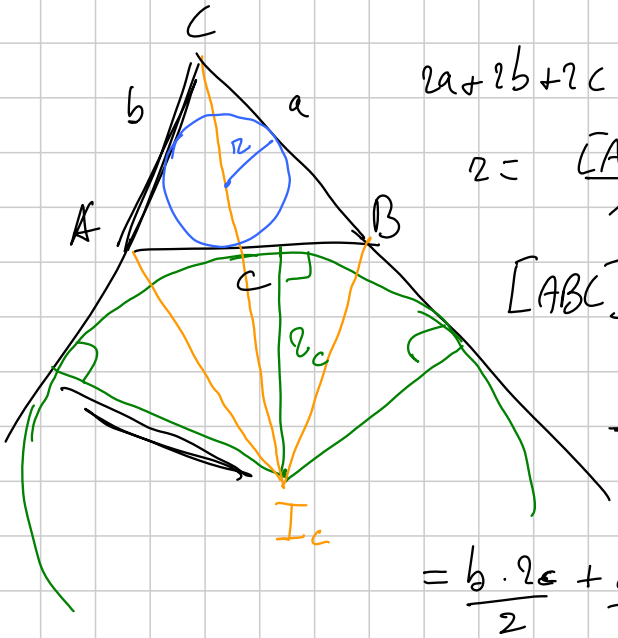
$1 \geq \cos\left(\frac{A-B}{2}\right)$ è vera.

Jensen su $\log\sin(x)$

$f' = \frac{\cos x}{\sin x}$

$f'' = \frac{-\sin^2 x - \cos^2 x}{\sin^2 x} = -\frac{1}{\sin^2 x}$

*) $\sum \frac{a^2}{r_a} = 4(R+r)$ $\qquad r_a$ = raggio cf. ex inscritta



$$2a+2b+2c = 2[ABC]$$

$$r = \frac{[ABC]}{s}$$

$$[ABC] = [ACI_c] + [I_cCB] - [BAI_c] =$$

$$= \frac{b \cdot r_c}{2} + \frac{a r_c}{2} - \frac{c r_c}{2}$$

$$r_c = \frac{[ABC]}{\left(\frac{b+a-c}{2}\right)}$$

$$r_a = \frac{[ABC]}{\frac{b+c-a}{2}}$$

$$r_b = \frac{[ABC]}{\frac{a+c-b}{2}}$$

a) $$r r_a r_b r_c = \frac{s^4}{s(s-a)(s-b)(s-c)} = \frac{s^4}{s^2} = s^2$$

a) $$\frac{1}{r_a} + \frac{1}{r_b} + \frac{1}{r_c} = \frac{1}{[ABC]} \cdot \left(\frac{[ABC]}{r_a} + \frac{[ABC]}{r_b} + \frac{[ABC]}{r_c}\right) =$$

$$= \frac{1}{[ABC]}\left(s-a+s-b+s-c\right) = \frac{s}{[ABC]} = \frac{1}{r}$$

$$\sum \frac{a^2}{r_a} = 4(R+r)$$

$$\sum \frac{a^2}{[ABC]}(s-a) = \frac{abc}{[ABC]} + 4\frac{[ABC]}{s}$$

$$s\left(a^2+b^2+c^2\right) - \sum a^3 = abc + 4(s-a)(s-b)(s-c)$$

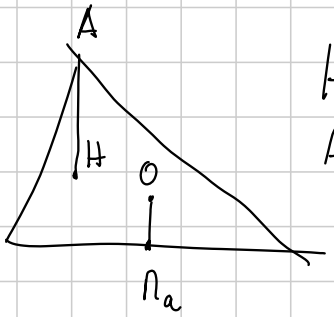
$$\left(\frac{a+b+c}{2}\right)(a^2+b^2+c^2) - \sum a^3 = abc + \frac{1}{8}(c+b-a)(a+c-b)(a+b-c)$$

$$\left[c^2-(b-a)^2\right](a+b-c)$$

$$\frac{a^3+b^3+c^3}{2} + \frac{ab^2}{2} + \frac{ac^2}{2} + \frac{ba^2}{2} + \frac{bc^2}{2} + \frac{ca^2}{2} + \frac{cb^2}{2}$$

$$\frac{1}{2}\left(c^2(a+b) - c^3 - b^2a - b^3 - a^3 - a^2b + a^2b + ab^2 + b^2c + a^2c + 2a^2b + 2ab^2 - 2abc\right)$$

$$II_a + II_b + II_c = 4R + 2r_0$$

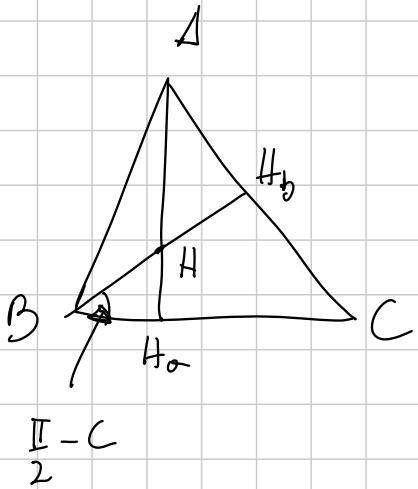


$H \to O$ omot. di centro G e rapp. $-\frac{1}{2}$

$A \to H_a$

$$HA = 2OH_a$$

$$\sum HA = 2\sum OH_a = 2(R+r)$$



$$AH_a = c\cdot\sin B$$

$$BH_a = c\cos B$$

$$HH_a = BH_a\cdot \operatorname{tg}\left(\frac{\pi}{2}-C\right) = c\cdot\cos B\cdot\frac{\cos C}{\sin C}$$

$$AH = c\left(\sin B - \frac{\cos B\cos C}{\sin C}\right) =$$

$$= 2R\left(\sin B\sin C - \cos B\cos C\right) = -2R\cos(B+C) =$$

$= 2R\cos A.$

$II_a + II_b + II_c = 4R + 2r_0 \qquad r_0 \geq 2r$

$II_a + II_b + II_c \geq 4(R+r)$

$\sum \sin^2 A \qquad 4R^2 \sum \sin^2 A = \sum a^2$

$|\vec{A}+\vec{B}+\vec{C}|^2 = |\vec{A}|^2 + |\vec{B}|^2 + |\vec{C}|^2 + 2\langle \vec{A}, \vec{B}\rangle + \dots = (*)$

$3R^2$

$\vec{H}$

Origine = circocentro

$\langle \vec{A}-\vec{B}, \vec{A}-\vec{B}\rangle = c^2$

$\|A\|^2 + \|B\|^2 - 2\langle \vec{A}, \vec{B}\rangle$

$2R^2$

$2\langle A, B\rangle = 2R^2 - c^2$

$(*) = 9R^2 - a^2 - b^2 - c^2 = 9R^2 - \sum a^2 = OH^2$

$9R^2 - \sum a^2 \geq 0 \qquad \sum a^2 \leq 9R^2$

$\sum \sin^2 A \leq \frac{9}{4}$

•) $IH^2 = 4R^2 + 4R_2 + 3r^2 - s^2 \qquad \frac{a\vec{A}+b\vec{B}+c\vec{C}}{a+b+c} = \vec{I}$

$IH^2 \geq 0$

$s^2 \leq 4R^2 + 4Rr + 3r^2$

$s^2 + r^2 \leq 4(R^2 + Rr + r^2)$

$$ab+bc+ca = s^2 + r^2 + 4Rr$$

$$\parallel$$

$$\frac{1}{4}(a+b+c)^2 + \frac{[ABC]^2}{s^2} + \frac{abc}{[ABC]}\cdot\frac{[ABC]}{s}$$

$$s^2(ab+bc+ca) = s^4 + [ABC]^2 + abcs$$

$$[ABC]^2 = s(s-a)(s-b)(s-c) = s\big(s^3 - (a+b+c)s^2 + (ab+bc+ca)s - abc\big) =$$

$$= -s^4 + s^2(ab+bc+ca) - sabc$$

Teo di Tolomeo: $AC\cdot BD = AB\cdot BC + AD\cdot BC$

$\Leftrightarrow$ A, B, C, D conciclici.

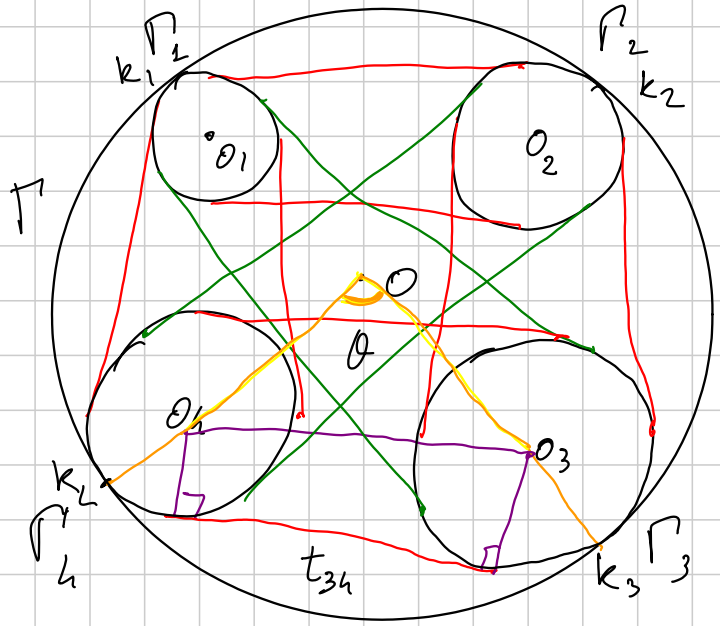
$\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4$ $\quad t_{ij}$ = lungh. della tg est. comune di Γ_i e Γ_j

Teo di Casey (o Tol. generalizzato)

$$t_{13}t_{24} \pm t_{12}t_{34} \mp t_{14}t_{23} = 0$$

$\Updownarrow$

$\exists\, \Gamma$ che tange $\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4$



$$k_3k_4^2 = Ok_3^2 + Ok_4^2 - 2Ok_3 \cdot Ok_4 \cos\theta$$
$$= 2R^2(1-\cos\theta)$$
$$\cos\theta = 1 - \frac{k_3k_4^2}{2R^2}$$

$$t_{34}^2 = O_4O_3^2 - (R_3-R_4)^2 =$$
$$= OO_4^2 + OO_3^2 - 2OO_3 \cdot OO_4 \cos(O_3OO_4) - (R_3-R_4)^2$$
$$\cos(R_3OR_4)$$
$$\cos(2^{\text{II}}k_3Ck_4) \quad C \in \Gamma$$
$$= (R-R_4)^2 + (R-R_3)^2 - 2(R-R_3)(R-R_4)\left(1 - \frac{k_3k_4^2}{2R^2}\right) -$$
$$-(R_3-R_4)^2 =$$

$$= \left[(R-R_4) - (R-R_3)\right]^2$$
$$(R_3-R_4)^2 + \frac{k_3k_4^2}{R^2}(R-R_3)(R-R_4) - (R_3-R_4)^2 =$$
$$= k_3k_4^2\,\frac{(R-R_3)(R-R_4)}{R^2}$$

$$t_{34} = \frac{K_3 K_4}{R}\sqrt{(R-R_3)(R-R_4)}$$

$$t_{12}t_{34} = \frac{K_1K_2 \cdot K_3K_4}{R^2}\sqrt{(R-R_1)(R-R_2)(R-R_3)(R-R_4)}$$

$$\sqrt{\quad} = D$$

$$t_{13}t_{24} = K_1K_3 \cdot K_2K_4 \cdot D$$

$$t_{14}t_{23} = K_1K_4 \cdot K_2K_3 \cdot D$$

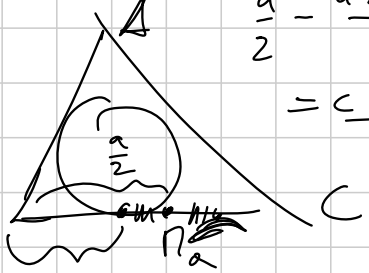
$$t_{12}t_{34} \pm t_{13}t_{24} \mp t_{14}t_{23} = D\left(K_1K_2 \cdot K_3K_4 \pm K_1K_3 \cdot K_2K_4 \mp \right.$$
$$\left. \mp K_1K_4 \cdot K_2K_3\right)$$

Cor: Feuerbach stanga le ex-inscritte

$\Pi_a, \Pi_b, \Pi_c, \omega$

$\frac{a}{2}$ $\frac{b}{2}$ $\frac{c}{2}$ $\frac{c-b}{2}$ $\frac{b-a}{2}$ $\frac{a-c}{2}$

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

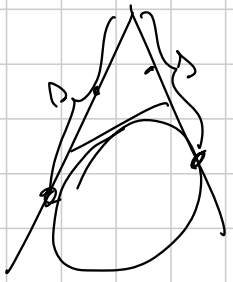


$\frac{a+c-b}{2}$

$\Pi_b \Pi_c$ $\Pi_a \omega$

$$\frac{a}{2}\left(\frac{c-b}{2}\right) \pm \frac{b}{2}\left(\frac{a-c}{2}\right) \pm \frac{c}{2}\left(\frac{a-b}{2}\right)$$

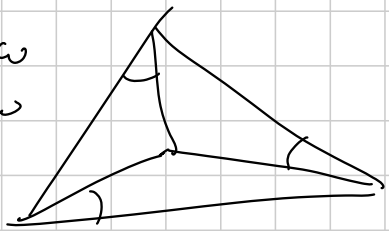
$$a(c-b) + b(a-c) - c(a-b) = 0.$$

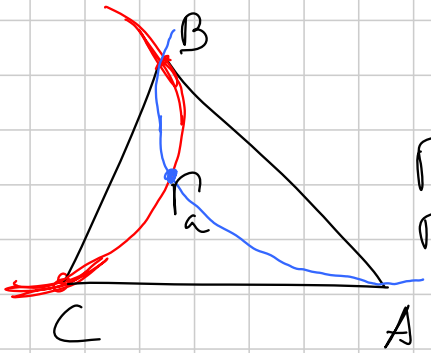


Punto di Brocard

1. $\exists$ due punti Ω e Ω' tali che

$$\Omega\hat{A}B = \Omega\hat{B}C = \Omega\hat{C}A = \omega$$
$$\Omega'\hat{A}B = \Omega'\hat{B}C = \Omega'\hat{C}A = \omega$$





Γ_a per B, C tang. a AC.
Γ_b per AB tg a CB
A Γ_c per A, C tg a AB.

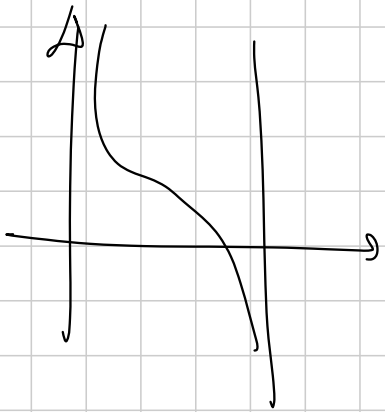
2) il Pri pedale di Ω è simile ad ABC

3) Ω e Ω' sono coniug. isogonali

4) $\cot\omega = \cot A + \cot B + \cot C$

$$\left[\cot A + \cot B + \cot C \geq \underbrace{\sqrt{3}}_{\cot 30^\circ}\right]$$

$$\omega \leq 30^\circ$$



5) $A\Omega$, $B\Omega$, $C\Omega$ incontrano Γ in A', B', C'

$\Rightarrow \triangle A'B'C' \equiv ABC$ $\quad AOA' = 2\omega$

6) $O\Omega = O\Omega'$ e $\Omega\hat{O}\Omega' = 2\omega$

7) La cf. $= \Gamma_\omega$ per O, Ω, Ω' passa per K = coniug. isog. di G (pt di Lemoine) e OK è diametro,

8) Γ_ω è l'inverso in Γ dell'asse = asse di Lemoine per i centri delle cf. di Apollonio (= diam LL', L = piede della bisett. int. L' = " " " est.)

9) O, K, I_1, I_2 sono all. e $\perp$ all'asse di Lemoine.

pt. comuni delle 3 cf. di Apoll

10) $$\cot\omega = \frac{a^2+b^2+c^2}{4[ABC]}$$

G2 - Metodi Algebrici - Medium

Titolo nota 09/09/2010

1. Coord. cartesiane (più di calcolo)
2. Complessi (geometria della cfr ed del tri)
3. Vettori (comb. lineari convesse)
   prodotti vettori

[Coord. baricentriche]

Coniche: $p(x,y) = ax^2 + 2bxy + cy^2 + 2dx + 2ey + f$

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

$(x^2 + y^2 + 1 = 0$ è FINTA$)$

$a > 0$

$$\left(\sqrt{a}\cdot x + \frac{b}{\sqrt{a}}y + \frac{d}{\sqrt{a}}\right)^2 = ax^2 + \frac{b^2}{a}y^2 + \frac{d^2}{a} + 2bxy + 2dx + 2\frac{bd}{a}y$$

$$y^2\left(c - \frac{b^2}{a}\right) + 2y\left(e - \frac{bd}{a}\right) + f - \frac{d^2}{a} =$$

$$= \pm\square + k \qquad c - \frac{b^2}{a} \gtrless 0$$

$$ac - b^2 \gtrless 0$$

$\alpha t^2 + \beta t + \gamma = \pm\square^2$

$+$ = quale radice
$-$ = 2 radici $\Leftarrow k = 0$ 1 radice

$a^2 - b^2 = 0$ ok

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

$a(x) = b(x) = 0$

x^2+1 $\Delta<0$
x^2-1 $\Delta>0$
x^2 $\Delta=0$

$p(x,y) = ax^2 + 2bxy + cy^2 + \dots$

$\Delta < 0$ ellisse
$\Delta = 0$ parabola
$\Delta > 0$ iperbole

Cartesiana: RETTA $ax+by+c=0$

Parametriche: $\begin{cases} x = pt+q \\ y = rt+s \end{cases}$ $t \in \mathbb{R}$

CIRCONFERENZA

$\begin{cases} x = \cos\theta \\ y = \sin\theta \end{cases}$ $\begin{cases} x = \frac{1-t^2}{1+t^2} \\ y = \frac{2t}{1+t^2} \end{cases}$ $t = \tan\frac{\theta}{2}$

$\cos^2\frac{\theta}{2} =$

$x = \tan\alpha$ $x^2 = \frac{\sin^2\alpha}{\cos^2\alpha}$

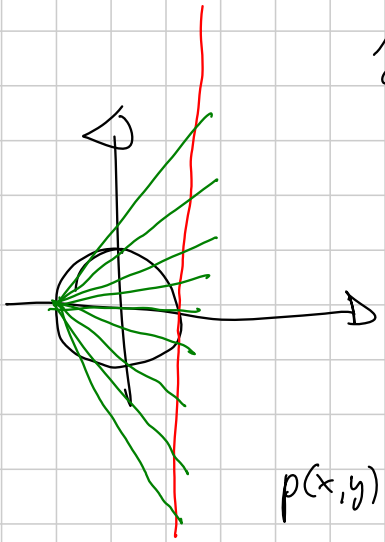
$\cos^2\alpha = \frac{1}{x^2+1}$ $x^2+1 = \frac{\cos^2\alpha+\sin^2\alpha}{\cos^2\alpha} = \frac{1}{\cos^2\alpha}$

$\cos 2\alpha = 2\cos^2\alpha - 1 = \frac{2}{x^2+1} - 1 = \frac{2-x^2-1}{x^2+1} = \frac{1-x^2}{1+x^2}$

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

$t = \frac{m}{n}$ $x = \frac{1-\frac{m^2}{n^2}}{1+\frac{m^2}{n^2}}$ $(n^2-m^2,\ 2mn,\ n^2+m^2)$

$y = \frac{2\frac{m}{n}}{1+\frac{m^2}{n^2}}$



Fascio di rette: $y = m(x+1)$

$\begin{cases} y = m(x+1) \\ x^2+y^2-1 = 0 \end{cases}$

$p(x,y) =$ di grado 2 $\quad a(x) =$ lineare (1° grado)

$p(x, a(x)) =$ grado 2

$p(x,y)=0$ Conica $\quad (x_0,y_0)\in$ Conica

$$\begin{cases} y-y_0=m(x-x_0) \\ p(x,y)=0. \end{cases}$$

Se $p(x,y)\in\mathbb{Q}[x,y]$ ($\circ\ \mathbb{Z}[x,y]$), $x_0,y_0\in\mathbb{Q}\circ\mathbb{Z}$

$m\in\mathbb{Q},\mathbb{Z} \Rightarrow$ altro punto $\in\mathbb{Q},\mathbb{Z}$

$\frac{y_0-y_1}{x_0-x_1}\in\mathbb{Q}\ (\mathbb{Z})$

$\mathbb{Q}\ (\circ\mathbb{Z})$

$$\begin{cases} x=\frac{r_2(t)}{r_1(t)} \\ y=\frac{s_2(t)}{s_1(t)} \end{cases} \qquad r_i,s_i\in\mathbb{Z}[t]$$

3° grado = 3 soluzioni

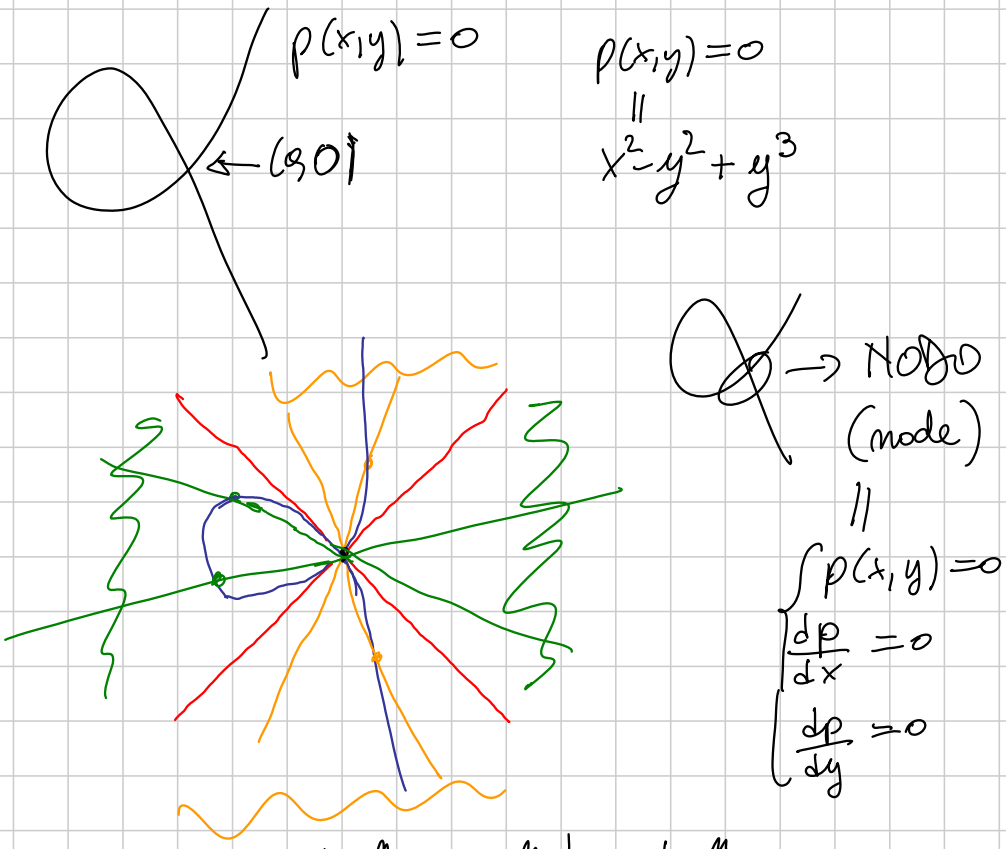
non esiste ($\nexists$) $q(x)\in\mathbb{Q}[x]$ t.c. $q(\zeta_1)=0 \quad q(\zeta_2)\neq 0$.

$p(x)\in\mathbb{Q}[x]$ irriducibile su $\mathbb{Q}[x]$ che ridà ζ_1,ζ_2,ζ_3

Il metodo delle corde funziona se:

1) il 3° grado è fisso $\left((x+y)(x^2+y^2-1)=0\right)$

2) la curva $p(x,y)=0$ è fatta così:



$$\frac{d\,x^n}{dx} = n x^{n-1} \qquad \frac{d\,y^n}{dx} = 0$$

$$\frac{d\,y^n}{dy} = n y^{n-1} \qquad \frac{d\,c^n}{dx} = 0$$

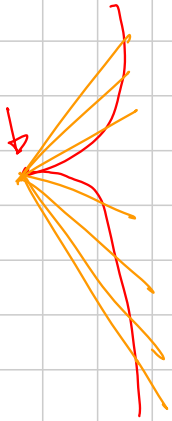
$$\frac{d\,a\cdot f(x,y)}{d\square} = a\cdot\frac{d f(x,y)}{d\square}$$

$$\frac{d\,f(x,y)\cdot g(x,y)}{d\square} = \frac{df}{d\square}\cdot g + f\cdot\frac{dg}{d\square}$$

$$\frac{d\,p(x,y)}{dx} = \frac{d\,x^2-y^2+y^3}{dx} = 2x$$

$$\frac{dp}{dy} = -2y + 3y^2$$

$x^2 = y^3$



CUSPIDE

Es: $x^2 + y^2 = 2z^2$

— ✻ —

Determinante:

$$\begin{cases} ax+by=0 \\ cx+dy=0 \end{cases}$$

esiste $sol \neq (0,0) \iff a = \lambda c$

$b = \lambda d$

$\frac{a}{c} = \frac{b}{d}$

$ad - bc = 0$

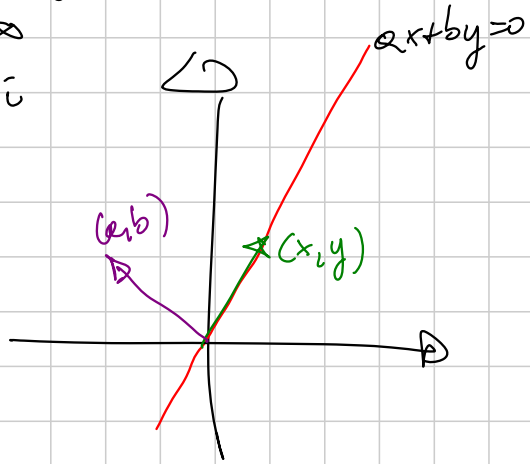
determinante del sistema

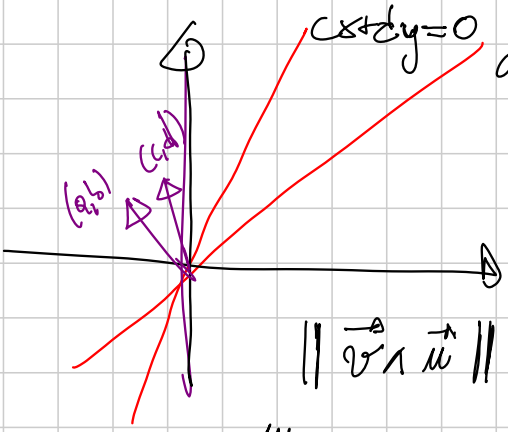
$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$

$0 = ax + by = \langle (a,b), (x,y) \rangle$

vettori

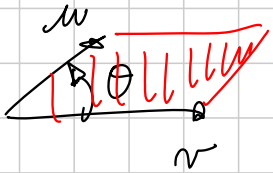
$\iff (a,b)$ perp. a (x,y)



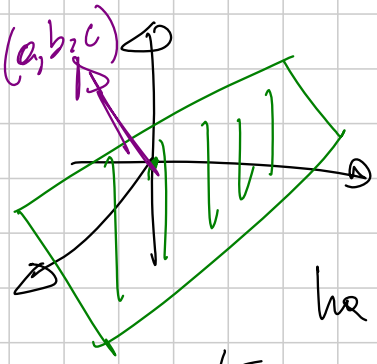


$$(a,b,0) \wedge (c,d,0) = 0$$

$$\| \vec{v} \wedge \vec{w} \| = \|\vec{v}\| \cdot \|\vec{w}\| \cdot \sin \hat{\theta}$$



In 3d: $(a,b,c) \cdot (x,y,z) = 0$



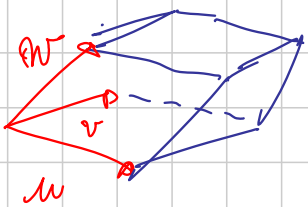
Se $\begin{cases} ax+by+cz=0 \\ dx+ey+fz=0 \\ gx+hy+jz=0 \end{cases}$

ha altre sol ($\neq (0,0,0)$)

c'è una retta in comune (r)

(a,b,c), (d,e,f), (g,h,j) sono $\perp$ a r

$\Leftrightarrow$ Vol $= 0$



base $= \vec{u} \wedge \vec{v}$ $\quad \pm \text{Vol} = (\vec{u} \wedge \vec{v}) \cdot \vec{w}$

C'è una sola area nulla $\iff [(a,b,c) \wedge (d,e,f)] \cdot (g,h,i)$

$(a,b,c) \wedge (d,e,f) = (bf-ec,\ dc-af,\ ae-bd)$

$\pm \text{Vol} = (gbf + hdc + iae - gec - hef - ibd)$

$= \det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$

$\det \begin{pmatrix} \vec{v} \\ \vec{u} \\ \lambda\vec{v}+\mu\vec{u} \end{pmatrix} = 0$

$\begin{cases} ax+by=c \\ dx+ey=f \end{cases}$

$D = \det \begin{vmatrix} a & b \\ d & e \end{vmatrix}$

$D_x = \det \begin{vmatrix} c & b \\ f & e \end{vmatrix}$

$D_y = \det \begin{vmatrix} a & c \\ d & f \end{vmatrix}$

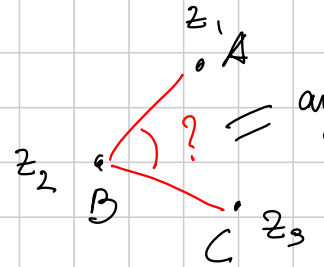
$x = \frac{D_x}{D} \qquad y = \frac{D_y}{D}$

Oss:
$\begin{cases} ax+by+cz=0 & \leftarrow \text{piano} \perp (a,b,c) \\ dx+ey+fz=0 & \leftarrow \text{piano} \perp (d,e,f) \end{cases}$

la retta che risolve il sistema è

$\lambda \cdot (a,b,c) \wedge (d,e,f) \qquad \lambda \in \mathbb{R}$

$\lambda \cdot (bf-ec,\ dc-af,\ ae-bd)$



$= \arg\left(\frac{z_1 - z_2}{z_3 - z_2}\right)$

traslare z_2 in 0 + ruotare la retta tra z_2 e z_3 sull'asse reale.

$$\left|\frac{z_1 - z_2}{z_3 - z_2}\right| = \frac{AB}{BC}$$

$$\frac{w_1 - w_2}{w_3 - w_2} = \frac{z_1 - z_2}{z_3 - z_2} \iff$$

dirett.

i $\triangle$ sono simili

(con i coniugati: inv. simile)

$$\det\begin{pmatrix} z_3 - z_2 & z_1 - z_2 \\ w_3 - w_2 & w_1 - w_2 \end{pmatrix} = 0$$

$$\det\begin{pmatrix} 1 & 1 & 1 \\ z_1 & z_2 & z_3 \\ w_1 & w_2 & w_3 \end{pmatrix} = 0$$

$\triangle$ equilatero $\iff$ $\begin{Vmatrix} 1 & 1 & 1 \\ z_1 & z_2 & z_3 \\ \zeta_3 & \zeta_3^2 & 1 \end{Vmatrix} = 0$

$\zeta_3 =$ rad. 3^a di 1 $\qquad \zeta_3^2 = \overline{\zeta_3}$

$$z_1 + \zeta_3 z_2 + \zeta_3^2 z_3 = 0$$

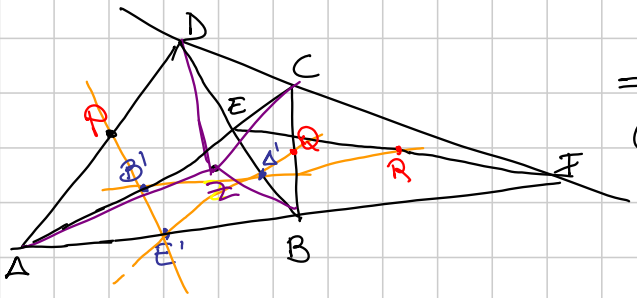
$\triangle$ equilatero $\iff$ $ABC \sim BCA$

$(ABC \sim BAC$ non $\dots$

G3 MEDIUM -Maria-

Titolo nota 08/09/2010

- Linea di Gauss e quadrilateri
- Geo proiettiva: - birapporti
  - polarità
- Ex/Incerchi
- Simmediane ...
- ⋮



P, Q, R pti medi
⇒ P, Q, R allineati
(LINEA DI GAUSS)

Dim 1: geo analitica (+ affinità) es.

Dim 2: Menelao sul triangolo $A'E'B'$.

$$\frac{E'P}{PB'} \cdot \frac{B'R}{RA'} \cdot \frac{A'Q}{QE'} = -1$$

Omotetia manda $AE'P$ in ABD

$$\frac{E'P}{PB'} = \frac{BD}{DE} \qquad \frac{B'R}{RA'} = \frac{AF}{FB} \qquad \frac{A'Q}{QE'} = \frac{EC}{CA}$$

$$\frac{BD}{DE} \cdot \frac{AF}{FB} \cdot \frac{EC}{CA} = -1$$

Menelao su BEA, retta DFC

Dim 3: luogo di Z t.c.

$$(ABZ) + (CDZ) = (ACZ) + (BDZ)$$

$(ABR) + (CDR) = (ACR) + (BDR)$

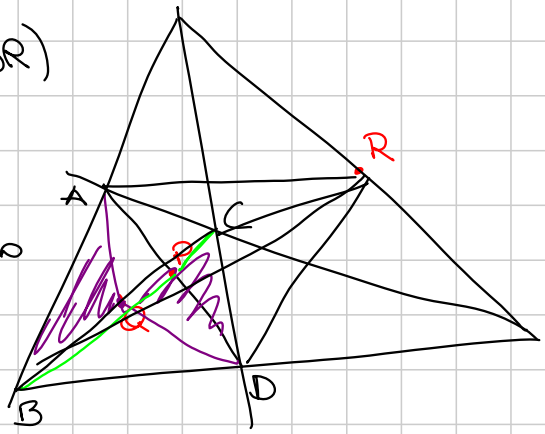
(esercizio)

$\mathbb{R}^2 \longrightarrow \mathbb{R}$

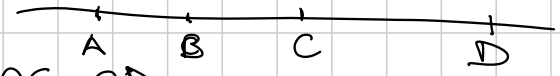
$z \longrightarrow (ABz)$ è un piano

- Contiene P, Q, R
- Non contiene i vertici (a meno di casi da verif a mano)

$\Rightarrow$ è una retta.

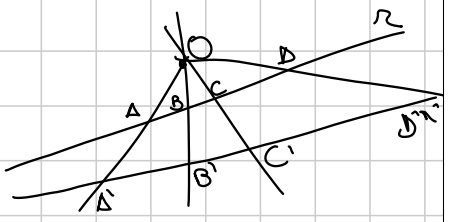


BIRAPPORTI



$$(A,B,C,D) = \frac{AC \cdot BD}{BC \cdot AD}$$

(possono essere ∞)



Prop:

$(A,B,C,D) = (A',B',C',D')$

Dim:

$$\frac{AC}{\sin A\hat{O}C} = \frac{AO}{\sin \hat{C}} \qquad \frac{BC}{\sin B\hat{O}C} = \frac{OC}{\sin \hat{B}} = \frac{BO}{\sin \hat{C}}$$

$$\frac{BD}{\sin B\hat{O}D} = \frac{DO}{\sin \hat{B}} = \frac{BO}{\sin \hat{D}} \qquad \frac{AD}{\sin A\hat{O}D} = \frac{AO}{\sin D}$$

$$\frac{AC \cdot BD}{BC \cdot AD} = \frac{\sin A\hat{O}C \cdot \sin B\hat{O}D}{\sin B\hat{O}C \cdot \sin A\hat{O}D}$$

Posso definire il bir di 4 rette concorrenti

$(ABCD) = \lambda$ $\qquad (BACD) \overset{?}{=} \dfrac{BC \cdot AD}{AC \cdot BD} = \dfrac{1}{\lambda}$

$(ABDC) = ?$

I possibili birapporti $\left\{ \lambda, \dfrac{1}{\lambda}, 1-\lambda, 1-\dfrac{1}{\lambda}, \dfrac{1}{1-\lambda}, 1-\dfrac{1}{1-\lambda} \right\}$

(esercizio)

$(ABCD) + (ACBD) = 1$

$\dfrac{(C-A)(D-B)}{(C-B)(D-A)} + \dfrac{(B-A)(D-C)}{(B-C)(D-A)} \overset{?}{=} 1$

$(C-A)(D-B) - (B-A)(D-C) \overset{?}{=} (C-B)(D-A)$.

Se $B=C$ si annulla il 1° membro

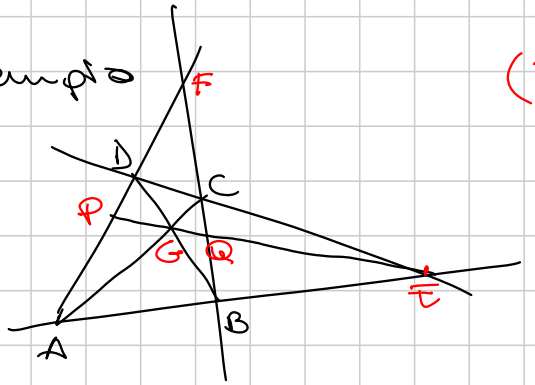
$(B-C) \mid$ 1° membro

BD

Def: $(A,B,C,D) = -1$

$\rightsquigarrow$ QUATERNA ARMONICA

Esempio



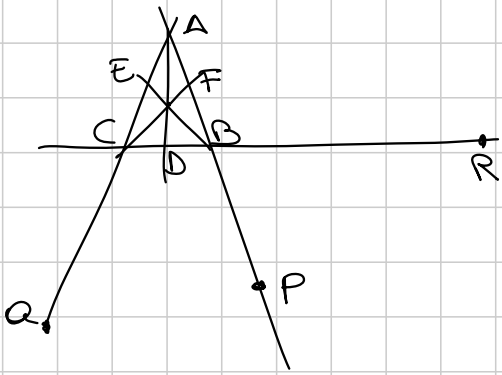
$(E,G,P,Q) = -1$

$(E,G,P,Q) \overset{\uparrow}{=} (D,A,P,F)$ centro C retta FD

$= (G,E,P,Q) = \dfrac{1}{(EGPQ)}$ centro B retta EG

$(EG,P,Q) = \begin{cases} 1 & \text{NO} \\ -1 & \text{SI} \end{cases}$

Esercizio



$(ABFP) = -1$

$(ACEQ) = -1$

$(CBDR) = -1$

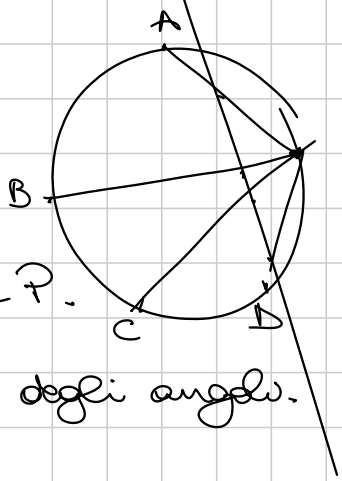
$\Rightarrow$ P, Q, R all.

BIRAPPORTI E CONICHE

Γ (conica) circ

$(A,B,C,D)_P =$

birapporto di PA PB PC PD



Prop: non dipende da P.

Dim:

Era scritto in funzione degli angoli.

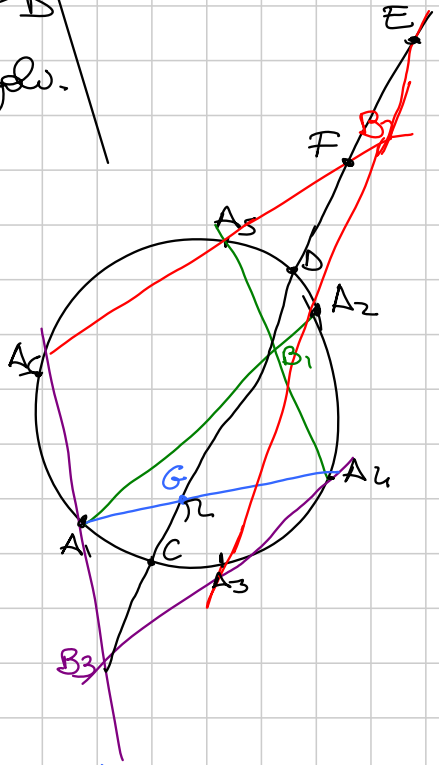
Teo di Pascal:

$A_1, \dots, A_6$ su (conica) circ.

$A_i A_{i+1} \cap A_{i+3} A_{i+4} = B_i$

$i = 1, \dots, 3$

B_i sono allineati.



Dim:

$(C B_3 F D) \overset{\text{centro } A_6,\ \Gamma}{=} (C A_1 A_5 D)$

$= (C G B_1 D)$ centro A_4 sulla retta CD

$(C B_3 E D) \overset{\text{centro } A_3,\ \Gamma}{=} (C A_4 A_2 D) \overset{\text{centro } A_1}{=} (C G B_1 D)$

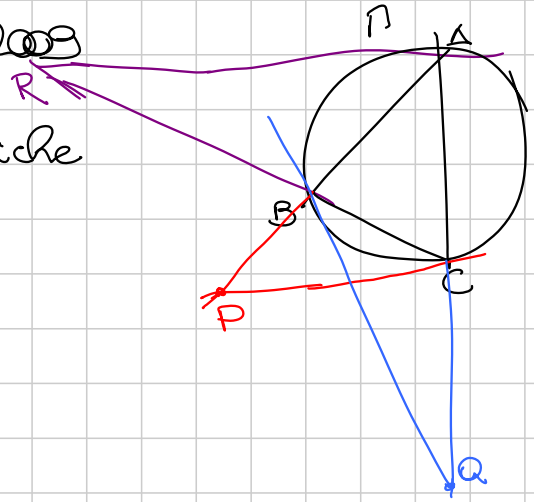
$\Rightarrow F = E$.

Conseguenza 5 2009

Esempio

$AB \cap t_C$, t_C ciclica

sono allineati



Pascal su

AABBCC

Esempio 2:

A', B', C' punti medi degli archi

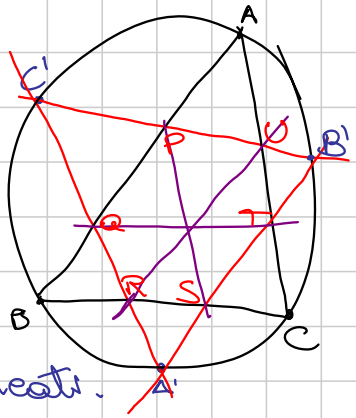
Tesi: PS, QT, UR concorrono.

NELL'INCENTRO.

Pascal

$\hat{A}A'C'\hat{B}BC$

$AA' \cap BB' = I$, R, U sono allineati.



POLARITÀ

Γ (conica) circo

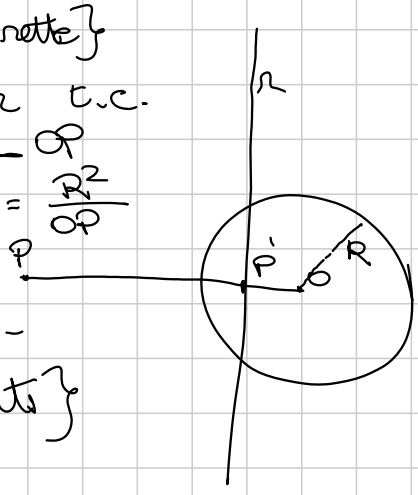
MAPPA DI DUALITÀ

{punti del piano} $\longrightarrow$ {rette}

$P \longrightarrow r$ t.c.

$r \perp OP$

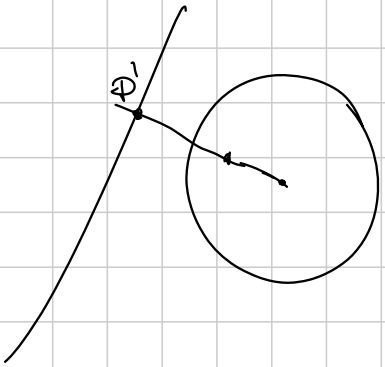
$OP' = \frac{R^2}{OP}$



Questa mappa è invertibile.

{rette} $\longrightarrow$ {punti}

$r \longrightarrow P$

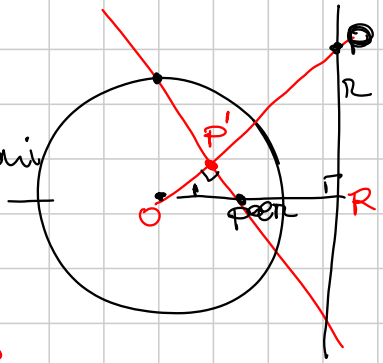


Proprietà

① $P \in C \iff P \in pol_C P$

② (Mantiene) Rovescia le inclusioni

$P \in r \iff pol P \ni pol r$



$OP' \cdot OP = R^2$

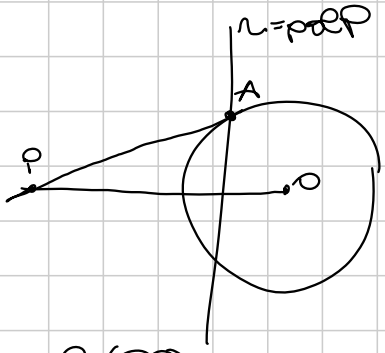
E' suff vedere $O\,pol_R\,P' \sim ORP$

$\overline{O\,pol_R}\ \overline{OR} = R^2$

③ $pol_C(P) \cap C = \{A, B\}$

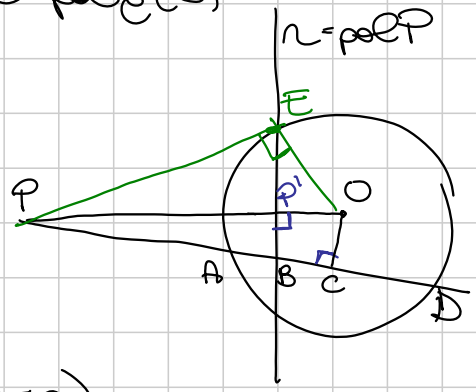
PA, PB sono tangenti

$A \in pol\, r \qquad pol A \ni P$



④ $pol_C(P) \cap pol_C(Q) = pol_C(PQ)$

⑤ retta per $pol_C(r)$ e $pol_C(s)$ $= pol(r \cap s)$



Esercizio

① C = pto medio AD

$PA \cdot PD = PB \cdot PC$

② $(AD\,PB) = -1$ (x casa)

$PA \cdot PD = pot_\Gamma(P)$

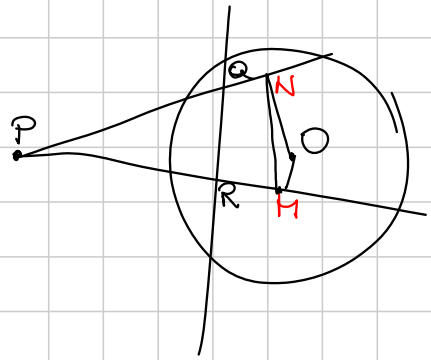
$PB \cdot PC = PP' \cdot PO = OP^2 - R^2$

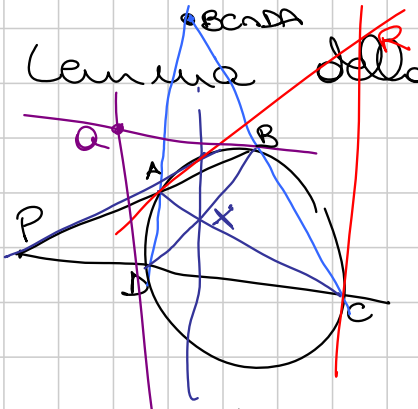
Euclide su OPE $\quad PE^2 = PP' \cdot PO$

RMNQ è ciclico

$PQ \cdot PN = Pow_\Gamma P$

$= PR \cdot PM$





Lemma della polare!

$X \in pol\, P$

Dim ① con i Birapporti sulle rette PB e PC.

Dim ② Pascal su $AABCCD$

$AA \cap CC = R \quad AB \cap CD = P \quad BC \cap DA$

Pascal su $BBADDC$

$BB \cap DD = Q \quad P \quad BC \cap AD$

$\Rightarrow$ P, Q, R, $BC \cap AD$ sono allineati

pol BD, pol (AC)

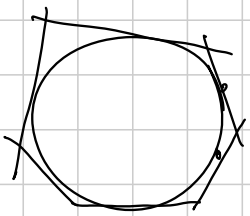
$P \in$ retta per pol BD e pol AC

$\Leftrightarrow AC \cap BD \in pol\, P$

Teo di Br.

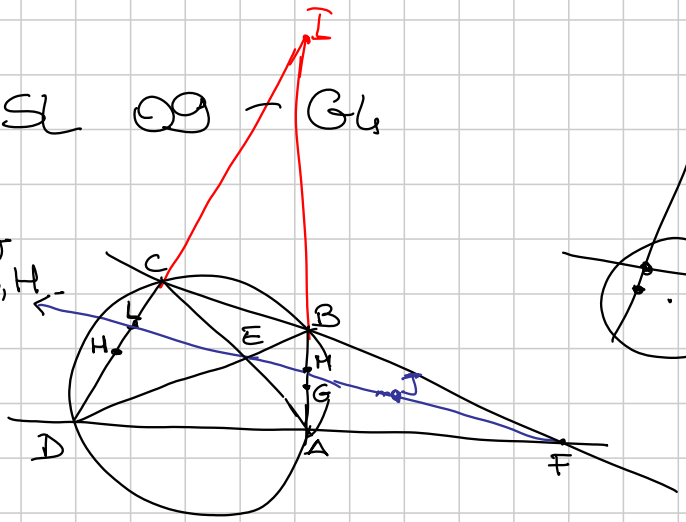
$C_1, \dots - C_6$ esagono circoscr a una conica

$\Rightarrow C_i C_{i+3}$ concorrono —



Esempio IMOSL 09 - G4

Tesi: EF è tang al cerchio per E, G, H.



Sol 1 simm risp alla bis + omotetia.

Sol 2: J pto medio di EF

$\Rightarrow$ H, G, J all. (retta Gauss).

Tesi: $JE^2 = JG \cdot JH$.

$(F, E, M, L) = -1$

$FM \cdot EL = (-EM) \cdot FL$ $\quad \| ME$

$EJ = JF$.

$(EJ + JM)(JL - EJ) = (EJ - JM)(EJ + JL)$

$EJ \cdot JL - EJ^2 + JM \cdot JL - JM \cdot EJ =$

$= EJ^2 - JM \cdot JL - JM \cdot EJ + EJ \cdot JL$

$EJ^2 = JM \cdot JL$.

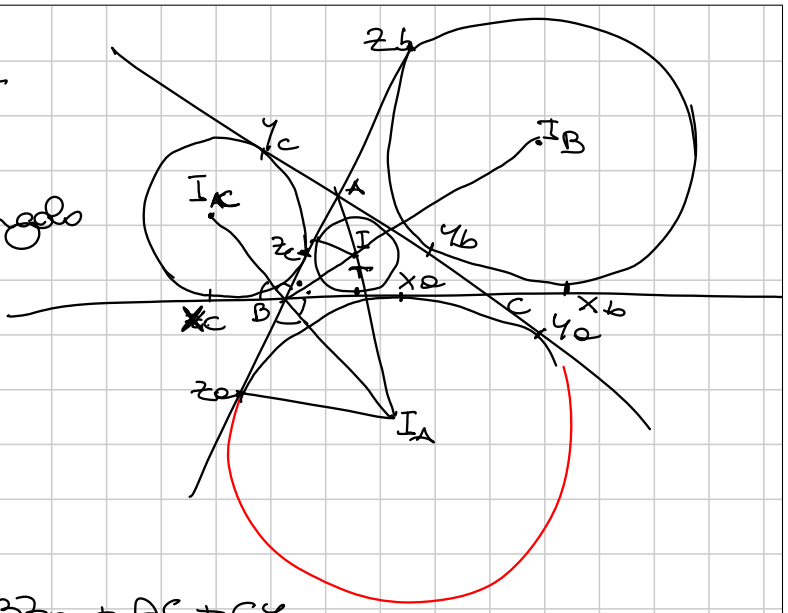
Resta da dim: $JG \cdot JH = JM \cdot JL$

$\Leftarrow$ $HLGM$ ciclico

$\Leftarrow$ $IL \cdot IH = IM \cdot IG$

ok per esercizio di prima.

IN / EX-CERCHI.



① $I_A B I_C$ all. $\Rightarrow$ ABC è il triangolo ortico di $I_A I_B I_C$

$BI_B \perp I_A I_C$

② $AZ_a = \frac{a+b+c}{2}$

$AZ_a = AY_a$

$AZ_a + AY_a = AB + BZ_a + AC + CY_a$

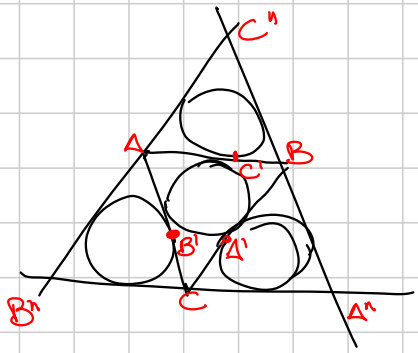
$= c + BX_a + b + CX_a = a+b+c$

③ $BX_a = CT$

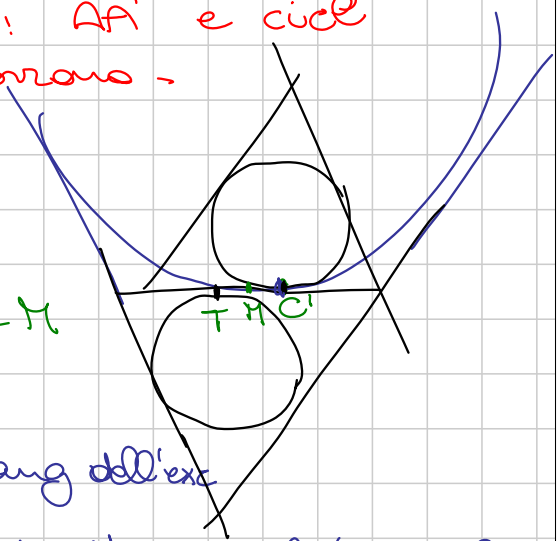
$\|$

$BZ_a - c = \frac{a+b-c}{2}$

④ AX_a, BY_b, CZ_c concorrono. (per Ceva + ③) PUNTO DI NAGEL.



Fatto: AA' e cicl concorrono.



simm rispetto a M

$TM = TC'$ per

$\Rightarrow$ C' è il pto di tang dell'exc

$\Rightarrow$ concorrono nel pto di Nagel del triangolo mediale.

(5) $\frac{1}{r_a} + \frac{1}{r_b} + \frac{1}{r_c} = \frac{1}{r}$

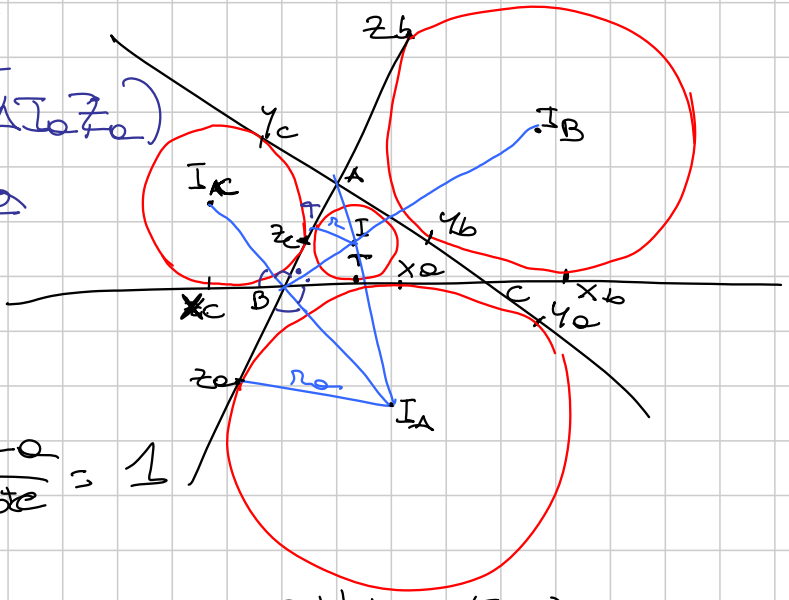
$\frac{r}{r_a} = \frac{AT}{AZ_a}$

(sim $\triangle IT$, AI_aZ_a)

$= \frac{2 \cdot \frac{b+c-a}{2}}{a+b+c}$

$= \frac{b+c-a}{a+b+c}$

$\sum_{cyc} \frac{r}{r_a} = \sum_{cyc} \frac{b+c-a}{a+b+c} = 1$

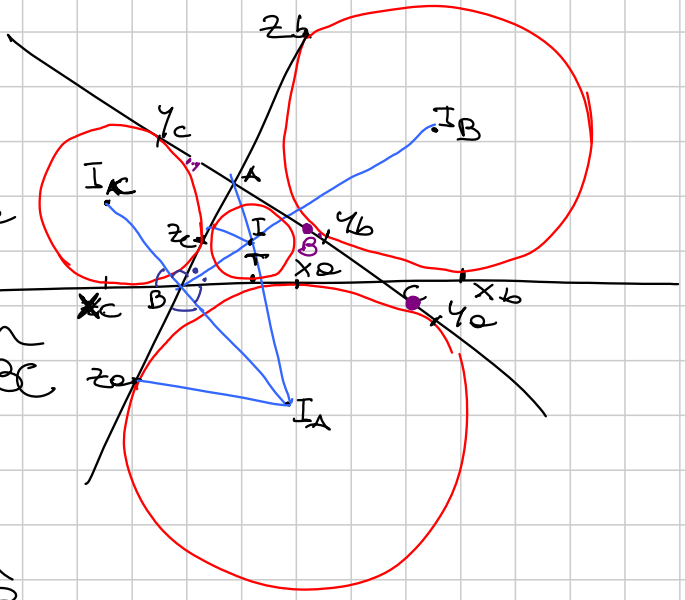


$r_a = I_aZ_a = \frac{a+b+c}{2} \operatorname{tg} \frac{\hat{A}}{2}$

(6) centro radicale dei 3 excerchi?

= incentro del triangolo mediale di ABC

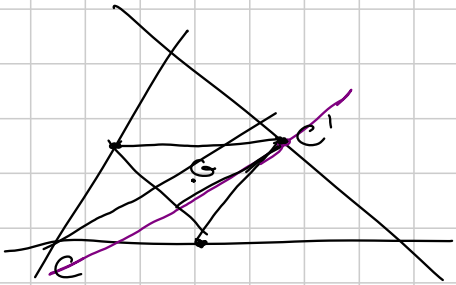
= S = p.ic di Spieker di ABC



Asse rad I_AI_C // Bisettr di $\hat{B}$

Basta dim che
l'asse rad di $I_B I_C$
passa per B'

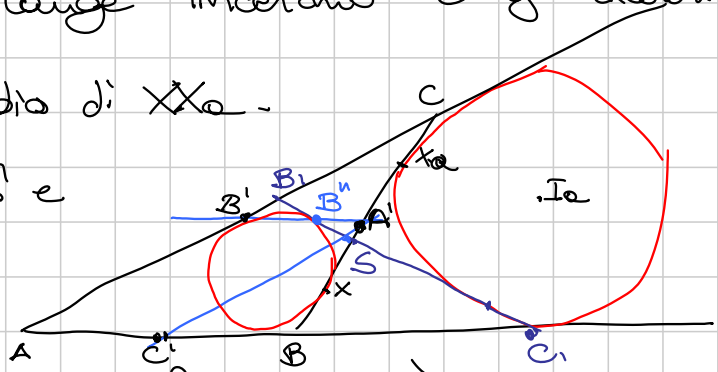
Ritorno!
$B'Y_c^2 = B'Y_a^2$



Teo di Feuerbach
Circonf di F. Tange incerchio e gli excerchi.

Oss A' è pto medio di XX_a.

Inversione di centro A' e raggio $A'X = A'X_a$



incerchio → sè excerchio → sè

T_1 → sè Feuerbach → ? B_1C_1

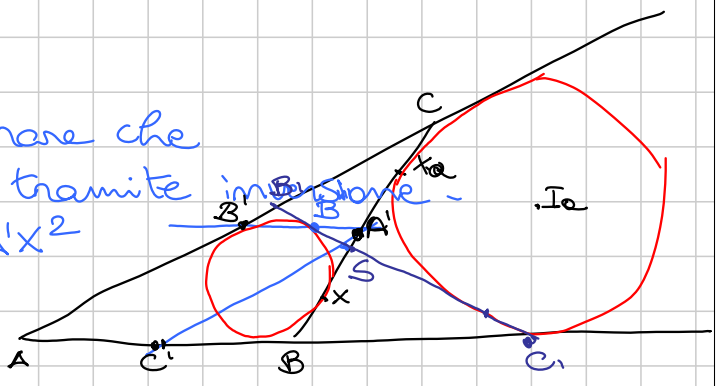
Definiamo B_1C_1 la retta tang a in e ex corr.

B_1C_1 è simm rispetto alla bis di $\hat{A}$ di BC.

S = ? Piede della bisettrice

~~A posteriori~~ S è l'unico del piede dell'altezza da A

$B'' = A'B' \cap B_1C_1$
Dobbiamo mostrare che
B' va in B'' tramite inversione.
$A'B' \cdot A'B'' = A'X^2$



$A'X = CX - CA' = \frac{a+b-c}{2} - \frac{a}{2} = \frac{b-c}{2}$

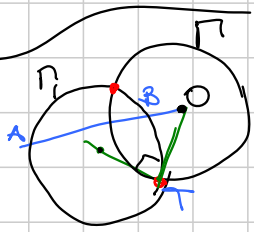
$A'B' = \frac{c}{2}$

Resta da dim $A'B'' \stackrel{?}{=} \frac{(b-c)^2}{2c}$

A e B si scambiano?

$AO \cdot BO = r_1^2$

$\overline{OT}^2$

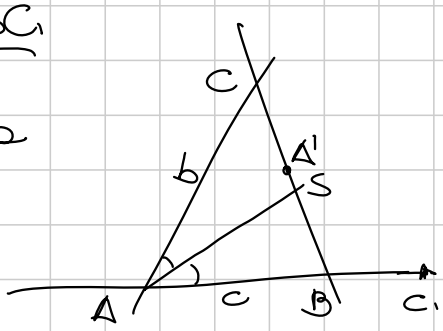


Similitudine $A'B''S$ e BC_1S

$\frac{A'B''}{A'S} = \frac{BC_1}{BS} \Rightarrow A'B'' = \frac{A'S \cdot BC_1}{BS}$

$BS = \frac{c}{b+c} \cdot a$ $\quad CS = \frac{b}{b+c} \cdot a$

$\begin{cases} \frac{BS}{CS} = \frac{c}{b} \\ BS+CS = a \end{cases}$



$A'S = CS - CA' = \frac{ab}{b+c} - \frac{a}{2}$

$BC_1 = b - c$

$$\frac{\frac{2ab-ab-ac}{2(b+c)} \cdot (b-c)}{\frac{ca}{b+c}} = \frac{a(b-c)^2}{2ac}$$

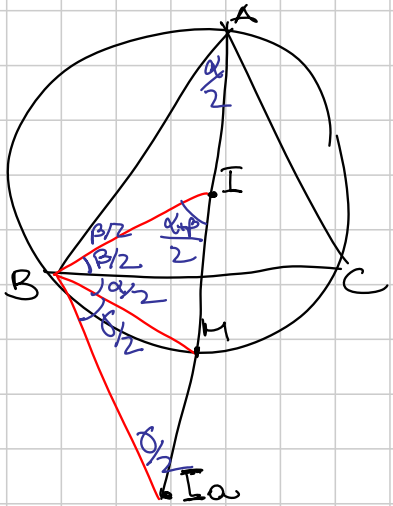
Lemma

$BICI_a$ è ciclico con centro M.

$I_a\hat{B}I = 90°$

BIM è isoscele

$IM = MB = MI_a$ OK

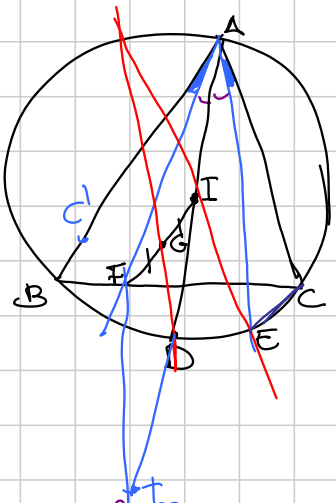


IMO 2010 – 2.

Tesi: $DG \cap IE \in$ circonf circoscr.

$\Leftrightarrow$ Dpto AE è ciclico

$\Leftrightarrow G\hat{D}I \stackrel{?}{=} I\hat{E}A$



$FI_0 // GD$

Tesi: $F\hat{I}_0I \stackrel{?}{=} I\hat{E}A$

$\Leftrightarrow AFI_0$ e AIE sono simili

$\frac{AF}{AI_0} \stackrel{?}{=} \frac{AI}{AE}$

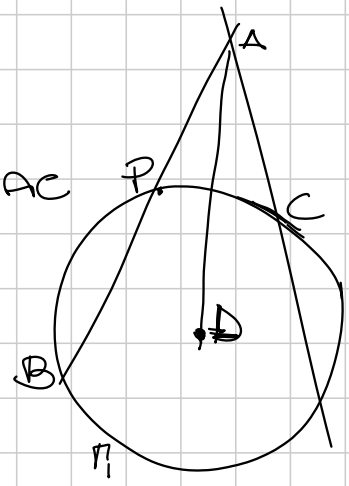
ABF e AEC sono simili $\Rightarrow \frac{AB}{AF} = \frac{AE}{AC}$

$AE \cdot AF = AB \cdot AC$

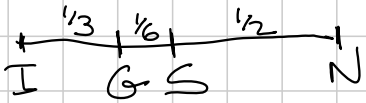
Tesi: $AI \cdot AI_0 = AB \cdot AC$.

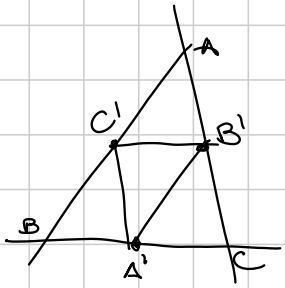
$AP = AC$

$pot_{\Gamma_1} A = AP \cdot AB = AB \cdot AC$



Teorema:





I = incentro di ΔABC

S = incentro di $A'B'C'$

N = punto di Nagel di ΔABC

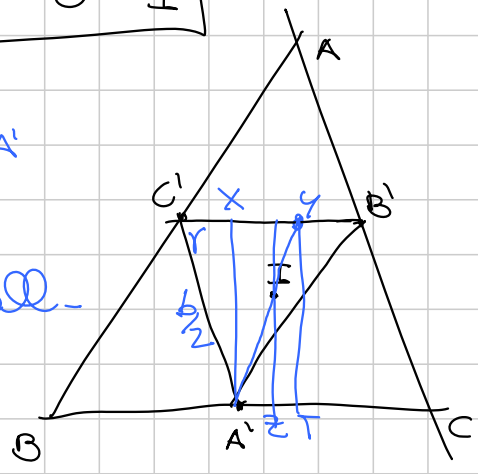
G = baric di ΔABC

$\Rightarrow$ sono all–

Idea: omotetia centro G rapporto $-1/2$

G fisso $I \to S$

Pto di Nagel di $A'B'C'$ è I



Y pto di tang dell'exc $\Gamma_{A'}$

$C'Y = \frac{a+c-b}{2}$

Voglio dim A', I, Y sono all–

$\Leftrightarrow$ Tolte su $A'IZ$ e $A'YT$

ovvero $\frac{IZ}{A'Z} = \frac{YT}{A'T}$

$IZ = r$

$A'Z = BZ - BA' = \frac{a+c-b}{2} - \frac{a}{2} = \frac{c-b}{2}$

$YT = \frac{1}{2} h_a = \frac{1}{2} b \sin\gamma$

$A'T = XY = CY - CX = \frac{a+c-b}{2} - \frac{b}{2}\cos\gamma$

$$\frac{2r}{c-b} = \frac{\frac{1}{2} b \sin\gamma \cdot 4}{a+c-b-2b\cos\gamma}$$

$$r \cdot \frac{a+b+c}{2} = \text{area} = \frac{1}{2} ab\sin\gamma$$

$$\Rightarrow r = \frac{ab\sin\gamma}{a+b+c}$$

$$\frac{a}{(c-b)(a+b+c)} \stackrel{?}{=} \frac{1}{a+c-b-2b\cos\gamma}$$

$$a^2 + ac - ab - 2ab\cos\gamma \stackrel{?}{=} ac - ab + c^2 - b^2$$

OK

TEORIA DEI NUMERI 1

Titolo nota 06/09/2010

a INTERO $\quad n > 1$ INTERO

$(a,n) = 1 \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$

$\mathrm{ord}_n(a) := \min k > 0$ t.c. $a^k \equiv 1 \pmod{n}$

$\langle a \rangle = \{ a^i \mid i \in \mathbb{Z} \} \subseteq \mathbb{Z}_n$

$o(\langle a \rangle) = \mathrm{ord}_n(a)$

$a^m \equiv 1 \pmod{n} \iff \mathrm{ord}_n(a) \mid m$

$m = k\,\mathrm{ord}(a) + r \quad a^m \equiv a^r$

$\mathrm{ord}_n(a) \mid \phi(n)$

$a, b \quad (a,n) = 1 \quad (b,n) = 1$

$\mathrm{ord}(ab)$?

$J = \mathrm{ord}_n(a)$

$K = \mathrm{ord}_n(b)$

$a^m b^m \equiv 1 \pmod{n}$

$a^{mJ} b^{mJ} \equiv 1 \pmod{n}$

$b^{mJ} \equiv 1 \Rightarrow K \mid mJ$

$\frac{K}{(K,J)} \mid m \cdot \frac{J}{(K,J)}$ $\qquad \left(\frac{K}{(K,J)}, \frac{J}{(K,J)}\right) = 1$

$\Downarrow$

$\frac{K}{(K,J)} \mid m$ $\qquad \frac{J}{(K,J)} \mid m$

$\frac{KJ}{(K,J)^2} \mid m$ $\qquad \frac{KJ}{(K,J)^2} = \frac{mcm}{MCD} \mid ord(ab)$

$ord(ab) \mid mcm(ord(a), ord(b))$

$m = mcm \quad J \mid m \quad K \mid m$

$a^m b^m \equiv 1 \cdot 1 \equiv 1$

$\frac{mcm(ord(a), ord(b))}{MCD(ord(a), ord(b))} \mid ord(ab) \mid mcm$ sì

$(ord(a), ord(b)) = 1 \Rightarrow ord(ab) = ord(a)\,ord(b)$

$a, b \in \mathbb{Z}_n^*$ $\exists c$: $ord(c) = mcm(ord\,a, ord\,b)$

$\mathbb{Z}_n^*$ è ciclico di ord. massimo

$a \in \mathbb{Z}_n^*$ $\exists\, L$ $ord\,c = mcm(ord(a), ord(b))$

$\mathrm{ord}(a) \mid \mathrm{ord}(g)$ $\quad \mathrm{ord}(g) = k$

$\forall a,\ \mathrm{ord}(a) \nmid k \iff a^k \equiv 1 \pmod n$

$\mathbb{Z}_p^*$ ciclico

$P(X)$ $\quad P(a) = 0$ $\quad a \in \mathbb{K}$ $\quad P(X) = (X-a)\,q(X)$

$\deg P = d$ $\quad$ **$P(X) = (X-a_1)\cdot\ldots\cdot(X-a_d)$**

$P(X)$ ha al + d radici

$P(X) - \prod (X-a_i)$ d rad grado $\le d-1$

[vero in $\mathbb{Z}_p$ $\quad a \neq 0$ $b \neq 0 \Rightarrow ab \neq 0$

$\mathbb{Z}_8$ $\quad x^2 - 1 \equiv 0 \pmod 8$

$\mathbb{Z}_p$ $\quad g$ ord max $\quad \mathrm{ord}_p(g) = k$

$\forall x \in \mathbb{Z}_p^*$ $\quad x^k \equiv 1 \pmod p$

$p-1$ radici $\quad k \ge p-1$ $\quad \mathrm{ord}(g) \ge p-1$

$=$

$\Rightarrow$ g è generatore

$a = g^m$ $\quad \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$

$$\sum_{i=0}^{p-1} i^n \pmod p \qquad n < p-1$$

$$\sum_{i=1}^{p-1} i^n = \sum_{j=1}^{p-1} (g^j)^n = \sum_{j=1}^{p-1} (g^n)^j \frac{(1-g^{np})}{1-g^n} =$$

$$= \frac{g^n - g^{np}}{1-g^n} = 0$$

$p-1 \nmid n \qquad \sum_{i=0}^{p-1} i^n = 0$ ALTRIMENTI $\sum_{i=0}^{p-1} i^{k(p-1)} = -1 \pmod p$

$$f : \mathbb{Z}_p \to \mathbb{Z}_p \qquad i \to a \cdot i \qquad a \neq 0$$

$$\sum_{i=0}^{p-1} i^n = \sum_{i=0}^{p-1} (a i)^n = a^n \cdot \sum_{i=0}^{p-1} i^n$$

$n < p-1$ $\quad X^n - 1$ al più n radici

$\exists\, a \in \mathbb{Z}_p^* : a^n \neq 1$

$$(a^n - 1) \sum_{i=0}^{p-1} i^n = 0 \iff \sum_{i=0}^{p-1} i^n = 0$$

ESERCIZIO!

$\forall\, p$: $\quad p \mid z^{n^3+1} - z^{n^2+1} + z^{n+1}$ almeno n.

$p \neq 2, 3, 5 \qquad z^{p-1} = z^{p(p-1)} z^{p-1} = 1 \pmod p$

$D = \{ p \mid \exists n : p \mid 2^{n^3+1} - 3^{n^2+1} + 5^{n+1} \}$

$P = \prod_{p \in D} (p-1)$

$n = 4kP$

$p \neq 2,3,5 \quad p \in P$

$2^{n^3+1} - 3^{n^2+1} + 5^{n+1} \equiv 2 - 3 + 5 \equiv 6 \not\equiv 0$

$2^{n^3+1} - 3^{n^2+1} + 5^{n+1} = 2^a 3^b 5^c \qquad a \leq 1$

$b = 0$

$c = 0$

mod 4 | | |

$0 - 3 + 5 \equiv 2 \mod 4$

mod 3

$\equiv 2 + 5 \equiv 7 \not\equiv 0$

$2 - 3 \equiv -1 \not\equiv 0$

$\left| 2^{(4kP)^3+1} - 3^{(4kP)^2+1} + 5^{4kP+1} \right| \leq 2$

$n \nmid 2^n - 1 \qquad n > 1$

$\mathrm{ord}_n(2) \mid n$

$\exists n \quad n \mid 2^n - 1$

$\mathrm{ord}_n(2) \mid n$

$\mathrm{ord}_n(2) \mid \phi(n)$

p più piccolo primo t.c. $p \mid n$

$p \mid n \mid 2^n - 1 \qquad p \mid 2^n - 1$

$\operatorname{ord}_p(2) \mid n \quad \Rightarrow \quad \operatorname{ord}_p(2) \mid (n, p-1) = 1$

$\operatorname{ord}_p(2) \mid p-1$

$p \mid 2 - 1$ assurdo

$a > b > 0$ interi $(a, b) = 1$

$n \mid \phi(a^n - b^n)$

$a \in \mathbb{Z}_m \qquad m = a^n - b^n$

$n \mid \operatorname{ord}(a) \Rightarrow n \mid \phi(m)$

$x = \frac{a}{b} \mod m \qquad a, b$ coprimi

$\exists s, k \quad sa + kb = 1$

$(b, m) = 1 \quad \exists s, k : sb + km = 1 \quad sb \equiv 1 \pmod m$

$\frac{a}{b} + \frac{p}{q} = \frac{aq + bp}{bq}$

$\left(\frac{a}{b}\right)^k = 1 \; ? \qquad a^k \equiv b^k \qquad m \mid a^k - b^k$

$0 < k < n \qquad 0 < a^k - b^k < m \qquad m = a^n - b^n$

$\mathrm{ord}_p\left(\frac{a}{b}\right) = n \qquad n \mid \phi(a^n - b^n)$

$n^{exp} \mid \phi(a^n - b^n)$

$n < p \leq 4n+2 \qquad p \mid \sum_{i=0}^{n} \binom{n}{i}^4$

$p \mid \sum_{i=0}^{p-1} i^n \qquad n < p-1 \qquad q(x) \quad \deg(q) < p-1$

$\mid \sum_{i=0}^{p-1} q(i)$

BINOMIALE $\in$ POL. IN i

$\binom{p-1}{k} \equiv (-1)^k \pmod p$

$\frac{(p-1)\cdot\ldots\cdot(p-k)}{k!} \equiv \frac{(-1)}{1}\cdot\frac{(-2)}{2}\cdot\ldots\cdot\frac{(-k)}{k} \equiv (-1)^k$

$\frac{\binom{n}{i}}{\binom{p-1}{n}} \equiv \frac{\frac{n!}{i!(n-i)!}}{\frac{(p-1)!}{i!(p-1-i)!}} = \frac{n!}{(p-1)!}\cdot\frac{(p-1-i)!}{(n-i)!}$

$n = p-2$

$\frac{n!}{(p-1)!}\,(p-i-1)\cdot(p-i-2)\cdot\ldots\cdot(p-i-n+1)$

$$\sum_{i=0}^{n} \binom{n}{i}^4 = \sum_{i=0}^{n} \frac{\binom{n}{i}^4}{\binom{p-1}{i}^4} \qquad \binom{p-1}{n}^4 \equiv 1 \mod p$$

$$\sum_{i=0}^{n} \left\{ \frac{n!}{(p-1)!} \left[(p-i-1)(p-i-2)\cdots(p-i-n) \right] \right\}^4$$

$n < i \leq p-i$ $\qquad$ III $\sum_{i=0}^{p-1}$

$\deg(\varphi(X)) < p-1$

$4(n-1) < p-1$ $\qquad$ $n = p-n$

$4(p-n-1) < p-1$ $\qquad$ Hp: $p \leq \frac{4n+2}{3}$

$\boxed{3p < 4n+3}$

CVD

~~////~~

VALUTAZIONE p-ADICA

$a \neq 0$ $\qquad$ p PRIMO

$k \in \mathbb{N}$

$p^k \mid a$ $\qquad$ $k = v_p(a)$

$p^k \| a$

$p^{k+1} \nmid a$

$$v_p(ab) = v_p(a) + v_p(b)$$

$v_p(a+b) \geq \min(v_p(a), v_p(b))$

$v_p(a) \neq v_p(b) \qquad v_p(a+b) = \min$

$a \equiv 1 \mod p \qquad a = kp^{\alpha} + 1$

$v_p(a^n - 1) \qquad (k, p) = 1$

$\alpha = v_p(a-1)$

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

$\dots$

$1 + 1 \dots + 1 = n \not\equiv 0 \pmod{p}$

$(n, p) = 1$

ALLORA $v_p(a^n - 1) = v_p(a-1)$

p PRIMO DISP.

$v_p(a^p - 1)$?

$a = k \cdot p^{\alpha} + 1$

$a^p - 1 = (kp^{\alpha} + 1)^p - 1 = \sum_{i=1}^{p} k^i p^{\alpha i} \binom{p}{i}$

$= kp^{\alpha} \cdot p + kp^{2\alpha} \cdot \binom{p}{2} + n \cdot p^{3\alpha} =$

$p \neq 2$

$k p^{\alpha+1} \pmod{p^{\alpha+2}}$ $\qquad p^{\alpha+1} \mid\mid a^p - 1$

$v_p(a^p - 1) = v_p(a-1) + 1$

ES: $4 \mid a-1$ $\qquad v_p(a^2-1) = v_p(a-1) + 1$

$v_p(a^n - 1) = v_p(a-1) + v_p(n)$ $\qquad a \equiv 1 \pmod{p^\alpha}$, $p \nmid \alpha$, $\text{spp. } p=2 \Rightarrow 4 \mid a-1$

LEMMA $\qquad$ PRIMO DISP.

g GEN IN $\mathbb{Z}_p^*$

ITOPE: g GEN $\mathbb{Z}_{p^k}^*$

g GEN IN $\mathbb{Z}_{p^k}^*$ $k \geq 2 \iff$ g GEN $\mathbb{Z}_p^*$, $v_p(g^{p-1} - 1) = 1$

$p^k \mid g^n - 1 \Rightarrow p \mid g^n - 1$ $\qquad p-1 \mid n$

$n = m(p-1)$ $\qquad g^{p-1} \equiv a$ $\qquad v_p(a-1) = 1$

$p^k \mid [g^{p-1}]^m - 1$ $\qquad p^k \mid a^m - 1$

$p^k \mid a^m - 1 \iff v_p(a^m - 1) \geq k$

$v_p(a-1) + v_p(n) \geq k$

$v_p(n) \geq k-1 \qquad (p-1)p^{k-1} \mid n(p-1) = \mathrm{ord}(g)$

$\mathrm{ord}(g) = n(p-1)$ $\quad g$ GENERA!

$\Longrightarrow$

g GEN IN $\mathbb{Z}_{p^k}^*$ $\qquad$ g GEN IN $\mathbb{Z}_p^*$

$v_p(g^{p-1}-1) = 1$

$\forall (a,p)=1$ fn: $g^{\varphi(n)} \equiv a \pmod{p^k}$

$\forall (a,p)=1$ fn $g^n \equiv a \pmod{p}$

$v_p(g^{p-1}-1) \geq 2$

$p^k \mid g^{(p-1)p^{k-2}} - 1 \qquad \mathrm{ord}(g) < (p-1)p^{k-1}$

~~~~~~

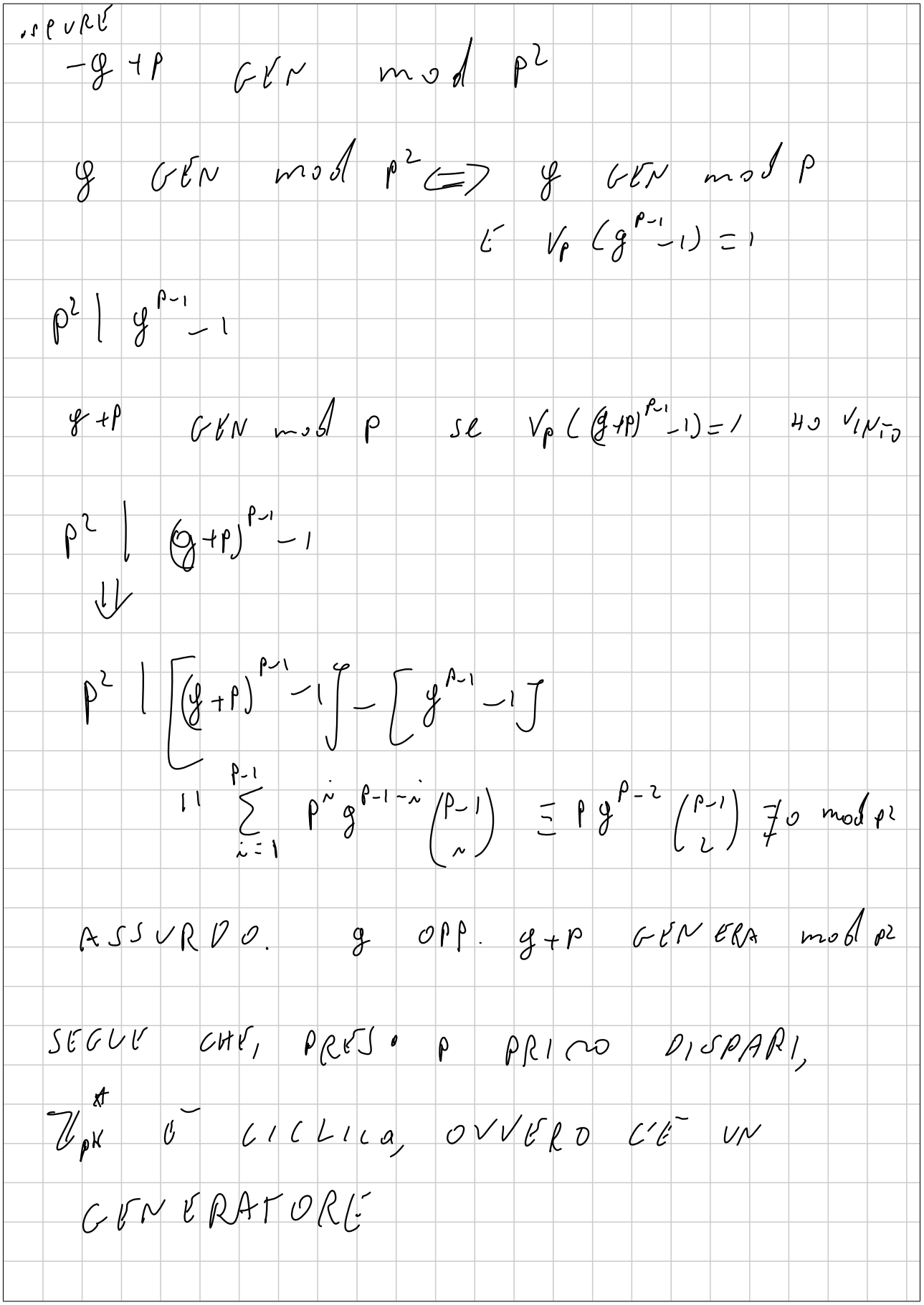
1) g GEN mod p^2

$\Downarrow$

g GEN mod p^k $\forall k$

2) g GEN mod p

$-g$ GEN mod p^2
~~~~~~


ASSURDO
$g+p$ GEN mod p^2
g GEN mod $p^2 \Rightarrow g$ GEN mod p
è $v_p(g^{p-1}-1)=1$
$p^2 \mid g^{p-1}-1$
$g+p$ GEN mod p se $v_p((g+p)^{p-1}-1)=1$ HO v_{INF}
$p^2 \mid (g+p)^{p-1}-1$
$p^2 \mid [(g+p)^{p-1}-1] - [g^{p-1}-1]$
$\| \sum_{i=1}^{p-1} p^i g^{p-1-i} \binom{p-1}{i} \equiv p g^{p-2} \binom{p-1}{1} \not\equiv 0 \bmod p^2$
ASSURDO. g OPP. $g+p$ GENERA mod p^2
SEGUE CHE, PRESO p PRIMO DISPARI,
$\mathbb{Z}_{p^k}^*$ è CICLICA, OVVERO C'È UN
GENERATORE

$\mathbb{Z}_{2^k}^*$

$4 \mid a-1$ $\qquad \boxed{v_2(a^n-1) = v_2(a-1) + v_2(n)}$

$n \geq 3$ $\qquad \mathrm{ord}_{2^n}(5)$???

$\min k$ t.c. $v_2(5^k-1) \geq n$

$5 \equiv 1 \pmod 4$ $\qquad 5 \equiv 1 \pmod 4$

$v_2(5-1) = 2$

$v_2(5^k-1) = v_2(k) + v_2(5-1) = v_2(k) + 2$

$v_2(k) + 2 \geq n$

PIÙ PICCOLO $k > 0$ PER CUI SUCCEDE ??

$2^{n-2} \mid k$ $\qquad k = 2^{n-2}$

$\mathrm{ord}_{2^n}(5) = 2^{n-2}$

$|\mathbb{Z}_{2^n}^*| = 2^{n-1}$ $\qquad k \in \{1, \dots, 2^{n-2}\}$

$\langle \pm 5^k \rangle$ $\qquad 5^k \equiv \pm 5^j \pmod{2^n}$

ALLORA $k = j$ $\qquad$ E' UN PIÙ

$5^k \equiv 5^j \Rightarrow 5^{k-j} \equiv 1 \quad |k-j| < \mathrm{ord}(5)$

$k-j = 0$

$5^k \equiv -5^j \pmod{2^n}$

$\Downarrow$

$5^k \equiv -5^j \pmod 8$

$5^{k-j} \equiv -1 \pmod 8$

$5 \quad 1 \quad 5 \quad 1$

$\pm 5^k \quad 2^{n-1}$ numeri tutti diversi

Preso $a \in \mathbb{Z}_{2^n}^*$ $\exists k$ t.c. $a \equiv 5^k \vee a \equiv -5^k$

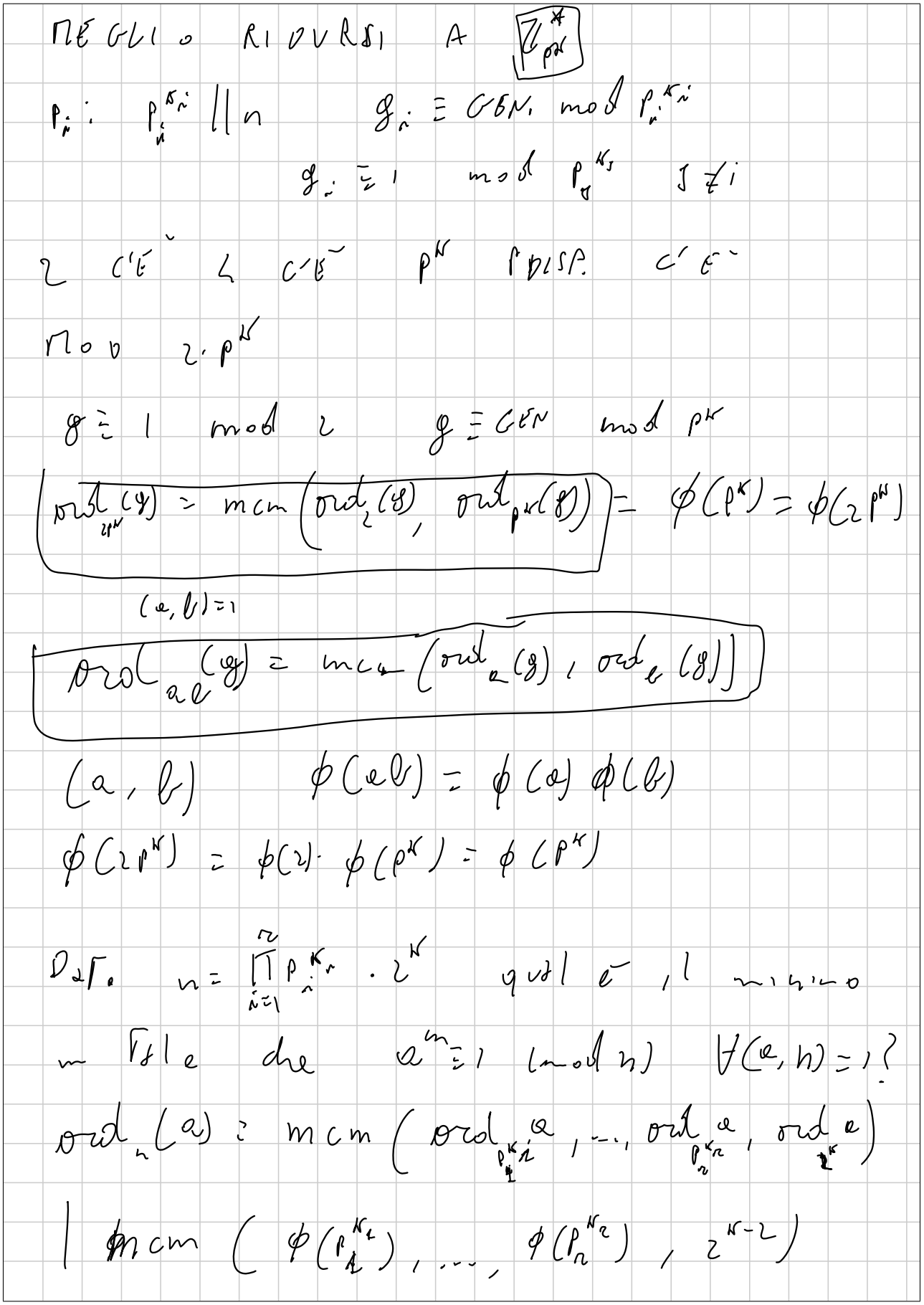
ORDINE massimo: c'è sempre ed è ord massimo

in $\mathbb{Z}_{2^n}^*$ l'ordine è almeno 2^{n-2}

$\mathrm{ord}(5) \geq 2^{n-2}$

$\mathrm{ord}_{2^n}(g) = 2^{n-1} \qquad g = \boxed{\pm 5^k}$

$g^{2^{n-2}} \equiv (\pm 5^k)^{2^{n-2}} \equiv 5^{k \cdot 2^{n-2}} \equiv 1 \mod 2^n$



Teoria dei Numeri 1 (Medium) – Pietro Vertechi

se $8 \mid n$ oppure se $\exists p \neq q$ primi dispari

$pq \nmid n$ allora vale $\operatorname{mcm} < \phi(n)$

$$\phi(n) = \prod \phi(p_i^{k_i}) \cdot 2^{k-1}$$

$$\operatorname{mcm}(\phi(p_1^{k_1}), \dots, 2^{k-2}) \leq \prod \phi(p_i^{k_i}) \cdot 2^{k-2}$$

$$< \prod \phi(p_n^{k_i}) \cdot 2^{k-1}$$

se $8 \mid n \Rightarrow$ no CBN (mod 8 no CBN)

$\exists p \neq q$ disp prim. $pq \mid n$

$\forall p \quad a^{p-1} \equiv 1 \pmod{p}$

$\equiv 1 \pmod{n}$

$a^{\operatorname{mcm}(p-1, q-1)} \equiv 1$

$\operatorname{mcm}(p-1, q-1) < (p-1)(q-1)$

- Dato k trovare una tale che 2^n ha un blocco di esatt. k ter. consecutivi in base 10

$2^n = 1572500000006$

3^n 3 è un generatore modulo 5^N

k $n = 2^{k+1} \cdot 5^k$

$3^n \equiv 1 \pmod{5^{k+1}}$

$3^n \equiv 1 \pmod{2^{k+1}}$

$3^n = m \cdot 2^{k+1} + 1$

$1\,5\,4 \ldots 0\,0\,0\,0\,0\,1$

k zeri

$5^{k+1} \nmid n$

$3^n \not\equiv 1 \pmod{5^{k+2}}$

$n^2 \mid 2^n + 1$ $n = 3$ risolve

$3^2 \mid 2^3 + 1$

p più piccolo primo che divide n

$p^2 \mid 2^n + 1 \mid 2^{2n} - 1$

$\text{ord}_p(2) \mid 2n \qquad \text{ord}_p(2) \mid p-1$

$(p-1, 2n) = 2 \qquad (p-1, n) = 1$

$\text{ord}_p(2) \mid 2$

$p \mid 2^2 - 1 \qquad p = 3$

$n = 3^k m \qquad (m, 3) = 1$

$3^{2k} \cdot m^2 \mid 2^{3^k \cdot m} + 1 \Rightarrow 3^{2k} \mid 2^{3^k \cdot 2m} - 1$

$(m, 3)$ COPRIMI

$3^{2k} \mid 4^{3^k \cdot m} - 1 \qquad v_3(4^{3^k m} - 1) =$

$= v_3(4-1) + v_3(3^k m) =$

$2k \leq 1 + k \qquad 1 + k$

$k \leq 1$

$n = 3m \qquad (3, m) = 1$

$9 m^2 \mid 2^{3m} + 1 = 8^m + 1$

p PIÙ PICCOLO PRIMO

$p^2 \mid 8^m + 1 \mid 8^{2m} - 1 = 64^m - 1$

$\text{ord}_p 64 \mid m \qquad \text{ord}_p(64) \mid p-1$

$(m, p-1) = 1 \qquad \mathrm{ord}_p(6^k) = 1$

$p \mid 6 \} \qquad p = 3 \quad \text{NO!}$

$p = 7$

$p^2 \mid 6^m + 1 \qquad p = 7 \quad \text{NO!}$

$6^m + 1 \equiv (-1)^m + 1 \equiv 2 \not\equiv 0 \mod 7$

$k = 3$ È L'UNICA SOLUZIONE.

DATO UN INTERO $n > 1$ E a INTERO

a È RESIDUO QUADRATICO $\mod n$

SE $\exists\, m \in \mathbb{Z} : \; n \mid m^2 - a$

SIMBOLO DI LEGENDRE:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & \text{se } p \nmid a \text{ e } a \text{ È RESIDUO Q.} \\ -1 & \text{se } p \nmid a \text{ e } a \text{ NON È RESIDUO Q.} \end{cases}$$

$a \equiv g^k \pmod p$

$k = 2n \qquad a \equiv g^{2n} \equiv (g^n)^2 \pmod p$

$a \equiv g^{2n+1} \qquad a \equiv x^2 \pmod p$

$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1$

$g^{2n+1} \overset{?}{\equiv} (g^{2n})^{\frac{p-1}{2}} \cdot (g)^{\frac{p-1}{2}} \equiv (g^{p-1})^n \, g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod p$

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

$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

$R \cdot R = R \qquad NR \cdot NR = R \qquad R \cdot NR = NR$

o R. Q. $\quad g^k$ res $\iff k$ è PARI

$\frac{p-1}{2}$ RESIDUI PRIMI CON p $(\neq 0)$

p PRIMO DISP.

a RES. MOD p $\qquad a \equiv g^m \pmod{p^k}$

$\Downarrow$ a RES MOD p^N $\qquad a \equiv g^n \pmod p$

g GEN MOD p^N $\qquad n \Downarrow$ PARI $\quad n = 2m$

$a \equiv (g^m)^2 \bmod p^N$

$n \geq 3$ QUALI RESIDUI (DISPARI) CI SONO mod 2^n

$a^2 \equiv 1 \pmod 8$ AL PIÙ 2^{n-3}

5 ha ord 2^{n-2}

$5^2, 5^4, \ldots, 5^{2^{n-2}}$ TUTTI RESIDUI DISPARI

SONO 2^{n-3}

a R.Q. mod 2^n $(n \geq 3) \iff a \equiv 1 \pmod 8$

$n = \prod p_i^{k_i} \cdot 2^k$ $\qquad (a, n) = 1$

a R.Q. $\iff \forall i \left(\frac{a}{p_i}\right) = 1$ se $k = 2$ $a \equiv 1 \pmod 4$

se $k \geq 3$ $a \equiv 1 \pmod 8$

$n \mid x^2 - a$ e $m \mid n \Rightarrow m \mid x^2 - a$

QUANDO -1 È R.Q mod p?

$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \cdot \begin{cases} = 1 & \text{se } 4 \mid p-1 \\ = -1 & \text{se } p \equiv 3 \pmod 4 \end{cases}$

LEMMA DI GAUSS

p PRIMO DISPARI (a, p) INTERO

$A = \left\{ a_i \mid 1 \leq i \leq \frac{p-1}{2} \right\} \subseteq \mathbb{Z}_p^*$

PRESO a_i $\exists!$ $1 \leq b_i \leq \frac{p-1}{2}$ $\qquad a_i \equiv \pm b_i \pmod p$

$\left\{ -\frac{p-1}{2}, \ldots, -1, 1, \ldots, \frac{p-1}{2} \right\}$ $\qquad f : \left\{1, \ldots, \frac{p-1}{2}\right\} \to \{-1, 1\}$

$a_i \equiv f(i)\, b_i \pmod p$

$\left(\frac{a}{p}\right) = (-1)^n \qquad n = \#\{ i \mid f(i) = -1 \}$

$i \neq j \quad b_i \neq b_j \quad b_i = b_j \quad ai \equiv \pm aj \pmod p$

$a(i \pm j) \equiv 0 \pmod p$ $\quad \frac{p-1}{2}$ int. div.

$i \pm j \equiv 0 \Rightarrow i = j$ $\quad 1 \leq b_i \leq \frac{p-1}{2}$

$\prod_{i=1}^{\frac{p-1}{2}} ai \equiv \prod_{i=1}^{\frac{p-1}{2}} b_i \, f(i) = \prod f(i) \cdot \prod b_i \equiv (-1)^n \cdot \left(\frac{p-1}{2}\right)! \pmod p$

$\prod_{i=1}^{\frac{p-1}{2}} ai \equiv \prod a \cdot \prod i \equiv a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \pmod p$

$a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^n \cdot \left(\frac{p-1}{2}\right)! \pmod p$

$a^{\frac{p-1}{2}} \equiv (-1)^n \pmod p$

$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p \qquad \left(\frac{a}{p}\right) = (-1)^n$

2 $\quad$ p

$\{2, 4, \dots, p-1\}$ $\qquad \{1, \dots, \frac{p-1}{2}\}$

$\{\frac{p+1}{2}, \dots, p-1\}$

$p \equiv 1 \pmod 8$

$\{2, 4, \dots, \frac{p-1}{2}\}$ $\qquad \{\frac{p-1}{2} + 2, \dots, p-1\}$

$\frac{\left(\frac{p-1}{2} - \frac{p-1}{2}\right)}{2} \equiv \frac{p-1}{4}$ PARI $\Leftrightarrow$ R.Q

2 è R.S $\Leftrightarrow$ $p \equiv \pm 1 \pmod 8$

RECIPROCITÀ QUADRATICA

p e q PRIMI DISPARI

VALE

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

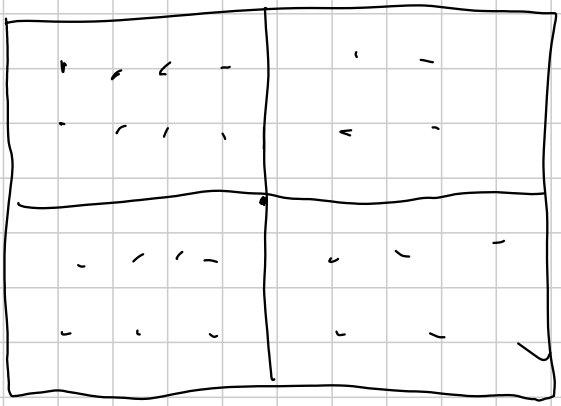
modulo quali primi 5 è R.Q.?

$\left(\frac{5}{q}\right)\left(\frac{q}{5}\right) = (-1)^{2 \cdot \frac{q-1}{2}} = 1$

5 è res. mod q sse q è res mod 5, cioè $q \equiv \pm 1 \bmod 5$

$p = 2a+1$

$q = 2b+1$



$$S = [-a, a] \times [-b, b] \cap \mathbb{N}^2$$

$$S = \{ (x,y) \mid x,y \in \mathbb{Z},\ |x| \le a,\ |y| \le b \}$$

$$\left(\frac{p}{q}\right) = \#\left\{ 1 \le i \le \frac{p-1}{2} \mid pi \in \left\{ -\frac{q-1}{2}, -\frac{q-1}{2}+1, \dots, -1 \right\} \text{ in } \mathbb{Z}_q \right\}$$

$$f : \left\{ 1, \dots, \frac{pq-1}{2} \right\} \longrightarrow S$$

$$f(n) = (x,y) \qquad n \equiv x \bmod p, \quad n \equiv y \bmod q$$

$$P = \left\{ 1, \dots, \frac{pq-1}{2} \right\}$$

$$v = \#\{ (x,0) \mid x < 0, (x,0) \in P \}$$

$$\left(\frac{q}{p}\right) = (-1)^v$$

$$\frac{p-1}{2} \cdot q \le \frac{pq-1}{2} < \frac{p+1}{2} \cdot q$$

$$-\frac{p}{2} \le -\frac{1}{2}$$

$$\frac{p}{2} \ge \frac{1}{2}$$

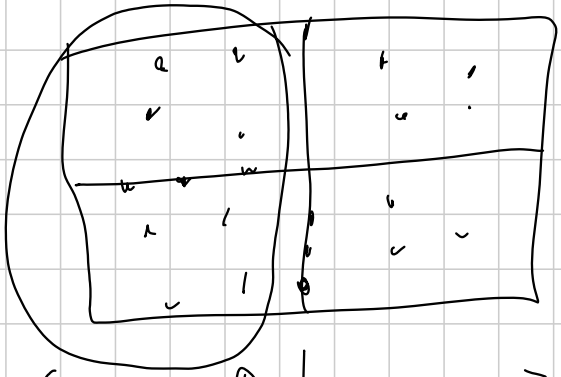
$$s \equiv x \bmod p \qquad s = kq$$

$$kq \qquad \boxed{q, 2q, \dots, \frac{p-1}{2} \cdot q}$$

$$x \in \left\{ -\frac{p-1}{2}, \dots, -1 \right\}$$

$$V = \#\{ (0,y) \mid y < 0, (0,y) \in P \}$$

$$\left(\frac{p}{q}\right) = (-1)^V$$



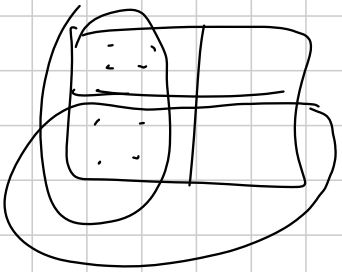
$A = \{(x,y) \in P \mid x < 0\}$

I NUMERI TRA 1 E $\frac{pq-1}{2} = p\cdot\frac{q-1}{2} + \frac{p-1}{2}$

TALI CHE $i \in \{-\frac{p-1}{2}, \dots, -1\}$ in $\mathbb{Z}_p$

$|A| = \frac{p-1}{2}\cdot\frac{q-1}{2} = ab$

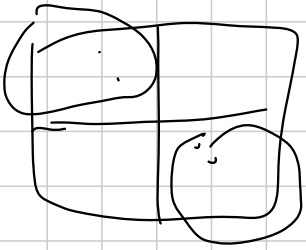
$B = \{(x,y) \in P \mid y < 0\}$



$|B| = ab$

$C = \{(x,y) \in P \mid (x>0 \text{ e } y<0) \text{ opp. } (x<0 \text{ e } y>0)\}$

$(x,y) \in Imm(f) \iff (-x,-y) \notin Imm f$



$f : \{-\frac{pq-1}{2}, \dots, \frac{pq-1}{2}\} \xrightarrow{\text{SURG}} S$

$f^{-1}(x,y) > 0$

$f^{-1}(x,y) = -f^{-1}(-x,-y)$

$C = \{(x,y) \in P \mid xy < 0\}$

$D = \{(x,y) \in S \mid xy < 0\}$

$\{(x,y), (-x,-y)\} \to$ COPPIE DI QUESTO TIPO PARTIZIONANO D,

UNO SOLO DI QUESTI CE L'E' IN C

$|C| = \frac{|D|}{2}$

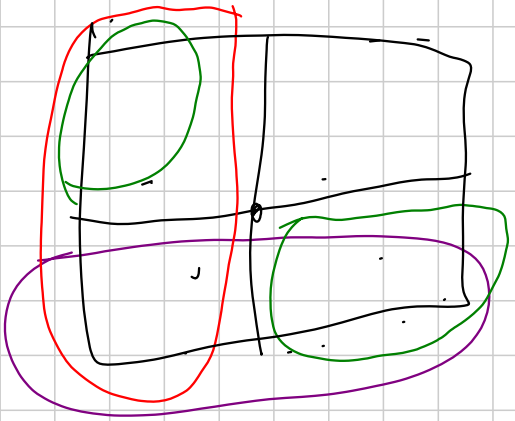
$\{1, \dots, a\} \times \{-b, \dots, -1\} \cup \{-a, \dots, -1\} \times \{1, \dots, b\}$

$|D| = 2 \cdot ab \qquad |C| = ab$

$|A| = |B| = |C|$

$|A| + |B| + |C| =$

$= |A \cap B| + 2|B \cap C| + 2|A \cap C| + U + V$



$3ab = 2|A\cap B| + 2|B\cap C| + 2|A\cap C| + u + v$

$ab \equiv u + v \pmod 2$

$(-1)^{ab} = (-1)^u \cdot (-1)^v = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)$

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

ESERCIZI:

- $x^2 = y^3 + 7 \qquad x, y \in \mathbb{N}$

mod 4 $\qquad x^2 \equiv 0, 1 \pmod 4$

$x^2 \equiv 0 \qquad y^3 + 7 \equiv 0 \pmod 4 \qquad y^3 \equiv +1 \pmod 4 \qquad y \equiv 1 \pmod 4$

$x^2 \equiv 1 \qquad y^3 \equiv 2 \pmod 4$

$y \equiv 1 \pmod 4$

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ $\qquad p \mid x^2 + y^2 \qquad (x, y) = 1$

$x^2 \equiv -y^2 \qquad \left(\frac{x}{y}\right)^2 \equiv -1 \pmod p$

$v_p \equiv 1 \pmod 4$

$x^2 + 1 = y^3 + 8$

$(y+2) \mid y^3 + 8 \Rightarrow y + 2 \mid x^2 + 1$

$p \mid y + 2 \Rightarrow p \equiv 1 \pmod 4$

$y + 2 = \prod p_i^{k_i} \equiv \prod 1^{k_i} \equiv 1 \pmod 4$

Sia n intero positivo dispari.

Se n è r.q modulo ogni primo $\Rightarrow$ è un quad.

$n = \prod p_i^{a_i}$ SE n NON È UN QUADRATO

WLOG a_i DISPARI

q PRIMO $\equiv 1 \pmod 4$ $\equiv a \pmod{p_1}$

SIA a UN N.R. mod p_1 $\forall n \neq 1$ $\equiv 1 \pmod{p_i}$

$q \equiv m \pmod{4\prod p_i}$ $(m, 4\prod p_i) = 1$

m P $(m, P) = 1$ $\exists \infty\, q : q \equiv m \pmod P$

$q \equiv m \pmod{4 \prod p_i}$

$q = \prod p_i^{a_i}$

$\prod \left(\frac{n}{p_i}\right)^{a_i} = -1$ $\exists i$ T.C. $\left(\frac{n}{p_i}\right) = -1$

$\left(\frac{m}{n}\right) = \prod \left(\frac{m}{p_i}\right)^{a_i}$ n non PRIMO

$\left(\frac{m}{n}\right) = 1 \iff m$ è RQ mod n

m è res. $\Rightarrow \left(\frac{m}{n}\right) = 1$

m, n int. disp. coprimi

$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}$

$q \equiv m \pmod{4\prod p_i}$

$\Downarrow \left(\frac{n}{q}\right) = -1 \quad \exists p \mid q \text{ t.c. } \left(\frac{n}{p}\right) = -1$

n è N.R per almeno primo

RESIDUI d-esimi

a è res. d-esimo mod p

se $a \equiv x^d \pmod p$ ha soluzioni

$a \equiv g^k \pmod p \quad (d, p-1) \mid k$

$g^1, \dots, g^{p-1} \quad (d, p-1)$

$\frac{p-1}{(d, p-1)}$ è il num di res. d-esimi.

$X^{p-1} - 1$ CONOSCIAMO $p-1$ RADICI

$X^{p-1} - 1 \equiv \prod_{i=1}^{p-1} (X - i) \pmod p$

$-1 \equiv \prod_{i=1}^{p-1} (-i) \equiv (p-1)! \pmod p$

$\prod_{i<j} ij \equiv 0 \pmod p$

$d \mid p-1$

$x^d - 1 \mid x^{p-1} - 1$

$x^d - 1 = \prod_{i=1}^{d} (x - a_i)$

$d \mid p-1$, ci sono esattamente d radici d-esime dell'unità

$\sum_{d \mid n} \phi(d) = n$

$f(d) = \#\{ x \in \mathbb{Z}_p^* \mid \mathrm{ord}_p(x) = d \}$

$f(d) = \phi(d) \quad \forall d \mid p-1$

Vuoto) $d = 1$ ✓

$n \mid p-1$

$\sum_{d \mid n} f(d) = n$

$x^n - 1$

RAGGRUPPA PER VALORI

QUANTI DI HA

$\sum_{d \mid n} f(d) = \left[\sum_{\substack{d \mid n \\ d < n}} f(d) \right] + f(n) = \sum_{\substack{d \mid n \\ d < n}} \phi(d) + f(n)$

$\left[\sum_{\substack{d \mid n \\ d < n}} \phi(d) \right] + f(n) = n = \sum_{d \mid n} \phi(d)$

$f(n) = \phi(n) \quad \forall n \mid p-1$

$n = p-1 \qquad f(p-1) = \phi(p-1) > 0$

x^d funz. $\mathbb{Z}_p^* \to \mathbb{Z}_p^*$

ESATTAMENTE d el vanno in 1.

a Rés. d-esimo

$a = g^{sd}$

$x = gy$

$x: x^d = a$ $\qquad g^d y^d = a \iff y^d = 1$

$p-1$ el d. $\mathbb{Z}_p^*$

$\frac{p-1}{d}$ BLOCCHETTI da d el.

1 R d-esimi

d el vanno in 1

IV
~~X~~ res. $\frac{p-1}{d}$-esimo $\Rightarrow x^d = 1$ $\qquad x = y^{\frac{p-1}{d}}$

sono $\checkmark$ $\qquad x^d = y^{p-1} = 1$

d

$x^d = 1 \iff x$ res $\frac{p-1}{d}$-esimo

$n = \frac{p-1}{d}$ $\qquad x^{\frac{p-1}{n}} \equiv 1 \pmod p \iff x$ res n-esimo $(n \mid p-1)$

$n = 2$ $\quad x$ R.Q. sse $x^{\frac{p-1}{2}} \equiv 1 \pmod p$

ESERCIZI

$x^2 + 4 = y^5$ ASSURDO mod p PER QUALCHE PRIMO

$\frac{p-1}{(d, p-1)}$ CONVIENE CHE $d \mid p-1$

$(5, p-1) = 1$

$p \equiv 1 \pmod 2$

$\equiv 1 \pmod 5$

$p \equiv 11$ $\quad y^5 \in \{-1, 0, +1\}$ $\quad (p-a)^2 \equiv a^2 \pmod p$

$x^2 \equiv y^5 + 7$ $\quad 6 \to 7$ $\quad 0, 1, 4, 9, 5, 1$

$\to 8$

ASSURDO $\pmod{11}$

Preso p PRIMO, $\exists q$ TALE CHE

p NON È UN RES. p-esimo mod q.

$p \mid q-1$ ALTRIMENTI TUTTI SONO RES p-esimi

$p \mid \mathrm{ord}_q(p)$

$p^{\frac{q-1}{p}} \not\equiv 1 \mod q$

q: $\mathrm{ord}_q(p) = p$

$q \mid p^p - 1$ $\quad q \nmid p-1$ $\quad q \mid \frac{p^p - 1}{p-1}$

$q \mid \frac{p^p-1}{p-1}$ $\quad p^p \equiv 1$ $\quad p \equiv 1 \pmod q$?

$\left(\frac{a^p-1}{a-1}, a-1\right) \mid p$ $\quad \left(\frac{p^p-1}{p-1}, p-1\right) = 1$

$\text{ord}_q(p) = p$

$p^{\frac{q-1}{p}} \not\equiv 1 \pmod q$ $\quad p \nmid \frac{q-1}{p}$ cioè $p^2 \nmid q-1$

$\exists\, q : q \mid \frac{p^p-1}{p-1}$ $\quad q \not\equiv 1 \pmod{p^2}$

$q \mid \frac{p^p-1}{p-1}$ SIANO $\equiv 1 \pmod{p^2}$

$$\frac{p^p-1}{p-1} = \prod_{i=1}^{k} q_i^{a_i} \equiv \prod_{i=1}^{k} 1^{a_i} \equiv 1 \pmod{p^2}$$

$$\frac{p^p-1}{p-1} \equiv 1 \pmod{p^2}$$

$p^2 \nmid \frac{p^p-1}{p-1} - 1$

$p^2 \mid \frac{p^p-p}{p-1} = p \cdot \boxed{\frac{p^{p-1}-1}{p-1}}$

$\exists\, q : p \,\|\, q-1$

$\text{ord}_q(p) = p$ $\quad p$ NON res. p-ESIMO

TEORIA DEI NUMERI 2

Titolo nota 08/09/2010

EQ DIOFANTEE.

$\frac{1}{m} + \frac{1}{n} = \frac{1}{p}$ p PRIMO in $\mathbb{N}^+$

$np + mp = mn$ $\quad mn - nf - mp + p^2 = p^2$

$(m-p)(n-p) = p^2$

DISCESA

$f(x_1, \dots, x_n) = 0$

SUPPORRE $a_1, \dots, a_n$ SOL + PICCOLA

TROVARNE UNA MINORE

VIETA - JUMPING

$f(x, y) = 0$ $\quad f$ COEFF. INTERI
POL DI 2° GRADO SIMM.

$a, b \quad a \geq b$

$f(x, b) = 0$ $\quad$ CONOSCIAMO UNA SOL. $x = a$

$\exists$ UN'ALTRA SOL. a'

SE $a > a' \Rightarrow$ ASSURDO

ESERCIZIO:

$(4ab-1) \mid (4a^2-1)^2 \Rightarrow a = b$

$(\alpha, \beta$ + PICCOLA SOL. $\alpha > \beta)$

MOD $4ab-1$ $\quad 4a \equiv \frac{1}{b} \pmod{4ab-1}$

$(4ab-1) \mid (4a^2-1)^2 \iff \left(a \cdot \frac{1}{b} - 1\right)^2 \equiv 0 \pmod{4ab-1}$

$(b, 4ab-1) = 1$ $\quad \Downarrow$

$(a-b)^2 \equiv 0 \pmod{4ab-1}$

$(a-b)^2 - K(4ab-1) = 0 \qquad K \in \mathbb{Z}$ RISOLVO

α, β LA + PICCOLA SOLUZIONE $\alpha > \beta$

$x^2 - 2x\beta + \beta^2 - 4K\beta x + K = 0 \qquad \alpha, \gamma \qquad \alpha > \gamma$

$\alpha > \frac{\text{SOMMA RADICI}}{2}$

$\alpha > \sqrt{\text{PROD RADICI}}$

$\alpha\gamma = K + \beta^2$

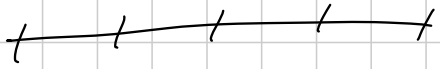
$\alpha^2 \geq K + \beta^2$ $\qquad (\alpha - \beta)^2 \geq K(4\alpha\beta - 1)$

$\alpha \geq (\beta + c)$ $\qquad c^2 \geq K(4(\beta+c)\beta - 1)$

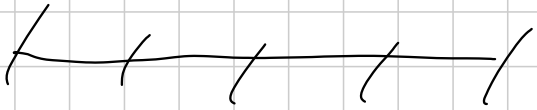
$\beta^2 + 2\beta c + c^2 > K + \beta^2$

$c^2 = K(4\alpha\beta - 1) > K$

$c > 0$



$x^4 + y^4 = z^4$ $\qquad (x, y, z) \in \mathbb{N}^3$



RIDURRE MOD. p

$f(x_1, \dots, x_n) = 0$ $\qquad x_n \in \mathbb{N}$

$\equiv 0 \pmod p$

$x^2 - 3y^2 = 17$ $\qquad x, y$ INTERI

HA SOL MOD p $\forall p \neq 3$

È POSS. CHE UNA CERTA EQ HA SOL MODULO p, MA DIAGARI NON MOD p^4

$x^3 + 2x + 1 = 2^n \quad x \equiv 5 \pmod 8$

$\forall n \ \exists x : \ 2^n \mid x^3 + 2x + 1$?

LEMMA DI HENSEL:

$f(x)$ POL HA RAD mod $p^n \ \forall n$?

SIA f UN POL. COEFF. INTERI.

SE' $\exists \ x_1 \in \mathbb{Z}$:

- $f(x_1) \equiv 0 \pmod p$
- $f'(x_1) \not\equiv 0 \pmod p$

$f(x) = \sum a_n x^n$

$f'(x) = \sum a_n n x^{n-1}$

ALLORA $\exists$ SUCC. x_n :

- $p^n \mid f(x_n)$
- $x_{n+1} \equiv x_n \pmod{p^n}$

PASSO BASE: SI'

INDUZIONE:

$f(x_n) = p^n \cdot k \qquad x_n \equiv x \pmod p$

$f'(x_1) \not\equiv 0 \pmod p$

SCRIVIAMO GENERICO

$x_n + m \cdot p^n$

$f(x_n + m \cdot p^n) \equiv f(x_n) + m \cdot p^n f'(x_n) \pmod{p^{n+1}}$

IN CASO

$\varphi(x)$ $\deg \varphi = d$

$$\varphi(x) = \sum_{i=0}^{d} \frac{f^{(i)}(x_0)}{i!} (x - x_0)^i$$

$$\varphi(x_0 + m \cdot n) = \sum_{i=0}^{d} \frac{f^{(i)}(x_0)}{i!} (mn)^i \equiv \sum_{i=0}^{r} \frac{f^{(i)}(x_0)}{i!} (mn)^i \pmod{p^r}$$

$$f(x + m \cdot p^n) = \sum_{i=0}^{d} a_i (x + m \cdot p^n)^i \equiv \sum a_i x^i + \left(\sum a_i x^{i-1} \cdot i \right) m p^n$$

$$f(x) + f'(x) \cdot m p^n \equiv$$

$f(x_n + m \cdot p^n) \equiv f(x_n) + m \cdot p^n \cdot f'(x_n) \pmod{p^{n+1}}$

$f(x_n) = k \cdot p^n$

$0 \equiv k \cdot p^n + m p^n \cdot f'(x_n) \quad (p^{n+1})$

$p \mid k + m f'(x_n)$

$f'(x_n) \not\equiv 0 \quad (p)$

$m \equiv -\frac{k}{f'(x_n)} \pmod{p}$

$x_{n+1} \equiv x_n + m \cdot p^n$

- $p \mid f(x_1)$
- $p \nmid f'(x_1)$

LEMMA PIÙ GENERALE:

$\boxed{v_p(f(x_1)) > 2 v_p(f'(x_1))}$

POI IN PIÙ VARIABILI:

LE FISSO TUTTE TRANNE 1

APPLICO IL LEMMA IN 1 VARIABILE

$n \geq 3$ QUALI RK. Q. mod 2^n

$\Downarrow$

$Q \equiv 1 \pmod 8$

$x^2 \equiv a \pmod 8$ $\quad x = 1$

$x^2 - a \xrightarrow{\text{deriv}} 2x$

$v_2(x^2-a) \geq 2\, v_2(2x)$, ?

3 ≥ 2

$x^3 + 2x + 1 = 2^n$ $\quad x = 0$

$n = p_{n+1}$

$x = 1$

$1 + 2 + 1 = 2^2$

$m = 2^k$ È L'UNICA SPERANZA!

$\forall\, n \geq k$

$x^3 + 2x + 1 \equiv 0 \pmod{2^k}$

$k = 1$

$x^3 + 2x + 1 \equiv 0 \pmod 2$

$x = 1$

$3x^2 + 2$ $\quad x = 1$

$\to 5$

$\Rightarrow$ C'È SOL mod 2^n

POLINOMI

TEST DELLA DERIVATA:

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

x^2+1 $\qquad f(x) = \prod q_i^{\alpha_i}(x)$

q_i IRR.

TH FATTORIZZAZIONE UNICA A MENO DI UNITÀ

q IRR. $\quad q(x) \mid a(x)\,b(x)$

$\Rightarrow q(x) \mid a(x) \vee q(x) \mid b(x)$

$q(x) = (q(x), a(x)) \cdot (q(x), b(x))$

DIVISIONE EUCLIDEE VI DEFINISCE MCD

BÉZOUT:

DATI $p(x), q(x)$ $\exists\ a(x), b(x) \in \mathbb{Q}[x]$

$a(x)p(x) + b(x)q(x) = MCD(p(x), q(x))$

TEST DELLA DERIVATA:

$f(x)$ HA FATTORI DOPPI

$\Downarrow$

$(f(x), f'(x)) \neq 1$

VALE ANCHE IN $\mathbb{Z}_p[x]$

(COEFF. mod p)

α RAD. DOPPIA $f'(\alpha) \equiv 0 \pmod p$

ESERCIZIO:

$f(x) \in \mathbb{Z}[x]$ IRRIDUCIBILE

$\exists$ INF. $n \in \mathbb{N}$:

$f(n)$ NON È UN QUAD. PERFETTO

$\deg f' < \deg f \qquad (f(x), f'(x)) = 1$

$a, b \in \mathbb{R}[x]$

$a(x) f(x) + b(x) f'(x) = 1$

$m, n \in \mathbb{R}[x]$

$m(x) f(x) + n(x) f'(x) = c \neq 0$

$p \nmid c \Rightarrow p \mid f(x) \Rightarrow p \nmid f'(x)$

$\exists \infty\ p : \exists n \in \mathbb{N} : p \mid f(n)$

$\exists p : \exists n : p \mid f(n)$ ma $p \nmid c \Rightarrow p \nmid f'(n)$

$p^2 \mid f(n)$

$f(n+p) \equiv f(n) + p \cdot f'(n) \pmod{p^2}$

$p \mid f(n+p) \Rightarrow$ ASSURDO

$p^2 \nmid f(n+p)$

Sia $f(x)$ in $\mathbb{R}$. $\exists \infty\ p : \exists n : p \nmid f(n)$

TECNICA DI STRINGERE TRA 2 QUAD.

$a \in \mathbb{N}$

$a^2 < b < (a+1)^2 \Rightarrow b$ NON È UN QUADRATO.

$f(X) = X^{2n} + a_1 X^{2n-1} + \dots + a_{2n}$

$\exists\, q(X) \in \mathbb{Q}(X) \quad \deg(q) = n$

$\deg(f(X) - q^2(X)) < n$

$q = X^n + \frac{a_1}{2} X^{n-1} + \dots$

$\exists\, m > 0 : \; m\, q(X) \in \mathbb{Z}[X]$

$\deg(m^2 f(X) - m^2 q^2(X)) < n \qquad \deg(q) = n$

$(m\,q(X) - 1)^2 < m^2 f(X) < (m\,q(X) + 1)^2$

$(m^2 q^2(X) - m^2 f(X)) - 2m\,q(X) + 1 < 0$

$m^2 f(X) = [m\,q(X)]^2 \qquad f(X) = q^2(X) \quad \forall X > N$

$\Rightarrow f(X) = q^2(X)$ CONTRADDIZIONE

$p(x), q(x) \ \forall x \in \mathbb{R} \quad p(x) = q(x) \Rightarrow$ LO STESSO POLINOMIO

$X^p \quad X \quad \mathbb{Z}_p$

COMBINATORIAL NULLSTELLENSATZ

$f(x_1, \dots, x_n)$

$\deg(f) = d$

$\exists$ monomio $x_1^{d_1} \cdot \dots \cdot x_n^{d_n}$ $\sum d_i = d$

coefficiente $\neq 0$

$\Rightarrow$ se io posso scegliere la variabile x_i in $d_i + 1$ modi, per ogni, riesco a trovare n-upla in cui $f(x_1, \dots, x_n) \neq 0$

$S_i : \quad |S_i| = d_{i+1}$

$f(x_1, \dots, x_n) \in S_1 \times \dots \times S_n : f(x_1, \dots, x_n) \neq 0$

DIMOSTRAZIONE:

SUPP. $\exists\, S_i$: A si annulla, $S_1 \times \dots \times S_n$

X_1 $\qquad f(X_1, \dots, X_n) = P_{x_2, x_3, \dots, x_n}(X)$

$\{a_0, a_1, a_2, \dots, a_d\} = S_1$

$(X - a_0)(X - a_1) \dots (X - a_d) = 0 \quad \forall X \in S_1$

$g_{x_2, \dots, x_n}(X) \equiv f(X_1, \dots, X_n) \quad (\text{non } P_{x_2, \dots, x_n}(X))$

$\deg(g) < d+1 \Rightarrow \deg(g) \le d$

$X y^2 + x^2 y \qquad S_x = \{1, 2\}$

$(X-1)(X-2) \qquad x^2 = 3x = 2 \qquad \forall X \in S_x$ IL VALORE DEL POL NON CAMBIA

$\Leftrightarrow \prod (X - a_i) = 0$

$\deg_X(g) \le d$

$g(X_1, \dots, X_n) \equiv f(X_1, \dots, X_n) \quad \forall x_i \in S_i$

$X_1^{d_1} \cdots X_n^{d_n}$ ha sempre coeff $\neq 0$

$X_2^{d_2} \cdots X_n^{d_n}$ in $g_{x_1}(x_2, \dots, x_n)$

$p(x_1) : X_2^{d_2} \cdots X_n^{d_n}$

$\deg(p) = d_1$ $\quad |S| = S_1 + 1$

$\exists\, a \in S_1 : p(a) \neq 0$

$g(a, x_2, \dots, x_n) \in \mathbb{K}[x_2, \dots, x_n]$

non solo $\deg(x_i) \leq d_1$

ma per ogni x_i allo stesso modo,

così ora semplice da

$g = f \quad \forall x_1, \dots, x_n \in S_1 \times \cdots \times S_n$

$\deg(x_i) \leq d_i$:

$X_2^{d_2} \cdots X_n^{d_n}$ ha grado ≥ 1

$\exists\, a_2, \dots, a_n : g(a, a_2, \dots, a_n) \neq 0$

$a_i \in S_i \Rightarrow f(a, a_2, \dots, a_n) = g(a, \dots a_n) \neq 0$

COROLLARIO:

Th Chevalley – Warning:

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \dots \\ f_k(x_1, \dots, x_n) = 0 \end{cases} \qquad \sum_{i=1}^{k} \deg(f_i) < n$$

$\Downarrow$

se c'è una soluzione allora ce n'è un'altra (in $\mathbb{Z}_p$) $\quad S_i = \mathbb{Z}_p$

sec. pezzo $= 0$ se $\exists i \; x_i \neq a_i$

se $x_i = a_i \; \forall i$ vuol dire 1 ✓

$$\prod_j \frac{(x_j - 1)(x_j - 2) \cdots (x_j - (a_j - 1)) \cdot (x_j - (a_j + 1)) \cdots (x_j - p)}{(a_j - 1) \cdots \qquad (a_j - p)}$$

$$\prod_{i=1}^{n} (1 - f_i^{p-1}(x_1, \dots, x_n)) - \prod_{j=1}^{n} \left(\prod_{\substack{a \in \mathbb{Z}_p \\ a \neq a_j}} \frac{x_j - a}{a_j - a} \right)$$

Γ

$(p-1) \sum \deg(f_i) < (p-1)n$

$x_1^{p-1} \cdots x_n^{p-1}$

$\exists\, a_1, \dots, a_n : \varphi(a_1, \dots, a_n) \neq 0$

$\Rightarrow$ È UN'ALTRA SOLUZIONE!!

COROLLARIO:

TH CAUCHY-DAVENPORT

$A \subseteq \mathbb{Z}_p \qquad B \subseteq \mathbb{Z}_p$

$A = \{1, p+1, \dots, np+1\} \qquad |A| = 1$

$A + B = \{a + b \mid a \in A, b \in B\} \subseteq \mathbb{Z}_p$

$A = \{ x^2 \mid x \in \mathbb{Z}_p \}$ $\quad |A| = \frac{p-1}{2} + 1$

$A = B$

$A + B = \{ x^2 + y^2 \mid x, y \in \mathbb{Z}_p \}$

$|A + B| \geq |A| + |B| - 1$

OPPURE $\quad A + B = \mathbb{Z}_p$

LAVORO $\quad |A| + |B| - 1 \geq \mathbb{Z}_p \Rightarrow A + B = \mathbb{Z}_p$

se $\quad |A| + |B| - 1 < \mathbb{Z}_p \Rightarrow |A+B| \geq |A| + |B| - 1$

$\exists\, C : \quad |C| = |A| + |B| - 2$ $\qquad |A| = m$

$A + B \subseteq C$ $\qquad |B| = n$

$\Phi(X, Y) = \prod_{c \in C} (X + Y - c)$ $\qquad$ grado $m + n - 2$

$X^{m-1} Y^{n-1}$ $\qquad (m-1) + (n-1)$ $\qquad x \in A \; y \notin B$

$\therefore x + y \notin C$

$p \nmid \binom{n+m-2}{m-1} \geq \frac{(n+m-2) \cdots (n)}{(m-1) \cdots 1}$

$n, m < p \qquad n+m < 2p$

$n+m-1 \leq p$

$p \nmid \binom{n+m-2}{m-1}$ ABBIAMO UN 0!

$|A+B| \geq n+m-1$

$n+m-1 > p$

$\emptyset \subsetneq A, \quad E \subsetneq B : |D|+|E|-1 = p$

$|D+E| \geq p \Rightarrow \mathbb{Z}_p \subseteq D+E \subseteq A+B$

$A+B = \mathbb{Z}_p$

$|A_1 + A_2 + \dots + A_n| \geq |A_1| + \dots + |A_n| - n + 1$

opp. $\mathbb{Z}_p = A_1 + \dots + A_n$

$|A_1 + \dots + A_n| \geq |A_1 + \dots + A_{n-1}| + |A_n| - 1$

$\geq |A_1| + \dots + |A_{n-1}| - (n-1) + 1 + |A_n| - 1 =$

$|A_1| + \dots + |A_n| - n + 1$

ESERCIZIO:

$\sum_{i=1}^{n} a_i x_i^{d_i} = c \qquad a_i \in \mathbb{Z}$

$p \nmid a_i \quad \forall i \qquad \sum \frac{1}{d_i} \geq 1$

ALLORA C'È SOL. MOD p!

$A_i = \{ a_i x_i^{d_i} \mid x_i \in \mathbb{Z}_p \}$

$|A_i| \geq \frac{p-1}{d_i} + 1$

$c \in A_1 + A_2 + \dots + A_n$

$|A_1 + \dots + A_n| \geq \sum |A_i| - n + 1 \geq$

$\geq \sum \left(\frac{p-1}{d_i} + 1 \right) - n + 1 = \sum \frac{p-1}{d_i} + \cancel{\sum 1} - n + 1 =$

$= (p-1) \sum \frac{1}{d_i} + 1 \geq p - 1 + 1 = p$

$\mathbb{Z}_p = A_1 + \dots + A_n$

$x^2 - 3y^2 = 1 \quad ?$ $\qquad p = 3$

$x_1^d + \dots + x_d^d \equiv 0 \pmod p$

HA SEMPRE SOLUZIONE!

$a_1, \dots, a_{2p+1} \in \mathbb{Z}$

NE ESISTONO p LA CUI SOMMA È MULTIPLA DI p.

POLINOMI CICLOTOMICI

$\Phi_n(x) = \prod_{(k,n)=1} (x - \omega^k) \qquad \omega = e^{\frac{2\pi i}{n}}$

$\deg \Phi_n = \phi(n)$

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

$\Phi_n(x) \in \mathbb{Z}[x]$

CONSIDERARLI MODULO p!

AD ESEMPIO, $p \nmid n \quad \Phi_n : nm \equiv 1$

$f(X) = X^n - 1 \qquad (nX^{n-1})Xm - (X^n - 1) \equiv 1 \pmod p$

$\Phi_n(a) \qquad p \mid \Phi_n(a) \qquad p \nmid n$

$X^n - 1 \qquad p \nmid \Phi_d(a) \quad \forall\, d \mid n,\ d < n$

$(f(x), f'(x)) = 1 \Rightarrow f(x)$ no [illegible]

$f(X) = P(X) \cdot P_1(X) \Leftarrow$ NO!

$(X-a) \cdot P_1(X) \qquad (X-a)^2 \mid f(X)$

$\Phi_n(X) \cdot \Phi_d(X) \mid X^n - 1$

$(X-a) \mid \Phi_n(X) \Leftrightarrow \Phi_n(a) = 0$

$(X-a) \nmid \Phi_d(X) \Leftrightarrow \Phi_n(a) \neq 0$

$\forall\, d < n,\ d \mid n \qquad \Phi_d(a) \not\equiv 0 \pmod p$

$m < n,\ m \mid n \qquad \boxed{X^m - 1 = \prod_{d \mid m} \Phi_d(X)}$

$a^m - 1 = \prod_{d \mid m} \Phi_d(a) \not\equiv 0 \pmod p$

$m \mid n,\ m < n \qquad a^m \not\equiv 1 \pmod p$

$\Phi_n(X) \mid X^n - 1$

$p \mid \Phi_n(a) \Rightarrow p \mid a^n - 1$

$p \mid \Phi_n(a) \mid a^n - 1$

$p \nmid n$ e $p \mid \Phi_n(a) \Rightarrow \mathrm{ord}_p(a) = n$

$\mathrm{ord}_p(a) = n$

$p \mid \Phi_d(a) \therefore d \mid n$

$p \mid a^n - 1$

SUPP. $d < n$ $p \mid \Phi_d(a) \mid a^d - 1$ NO!

$p \mid \Phi_n(a)$

$(p, n) = 1$ ALLORA $p \mid \Phi_n(a) \iff \mathrm{ord}_p(a) = n$

$n = p - 1$

$X^{p-1} - 1 \equiv \prod_{i=1}^{p-1} (X - i) \pmod p$

$\Phi_{p-1}(X) \mid X^{p-1} - 1$

SI FATT. IN FATT. LINEARI

ESISTONO $\phi(p-1)$ RADICI DI QST POL.

VISTO CHE $p \nmid p-1$

a SIA UNA RADICE $\iff \mathrm{ord}_p(a) = p-1$

$\iff a$ È UN GENERATORE

$p \mid n \qquad n = mp$

$p \mid \Phi_{mp}(a)$

$m \mid n \qquad X^m - 1 \mid X^n - 1$

$$\frac{X^n-1}{X^m-1} = \frac{\prod_{d \mid n} \Phi_d(X)}{\prod_{d \mid m} \Phi_d(X)} = \prod_{\substack{d \mid n \\ d \nmid m}} \Phi_d(X)$$

$\Phi_n(X) \mid \dfrac{X^n-1}{X^m-1}$

$\Phi_n(a) \mid \dfrac{a^{mp}-1}{a^m-1}$

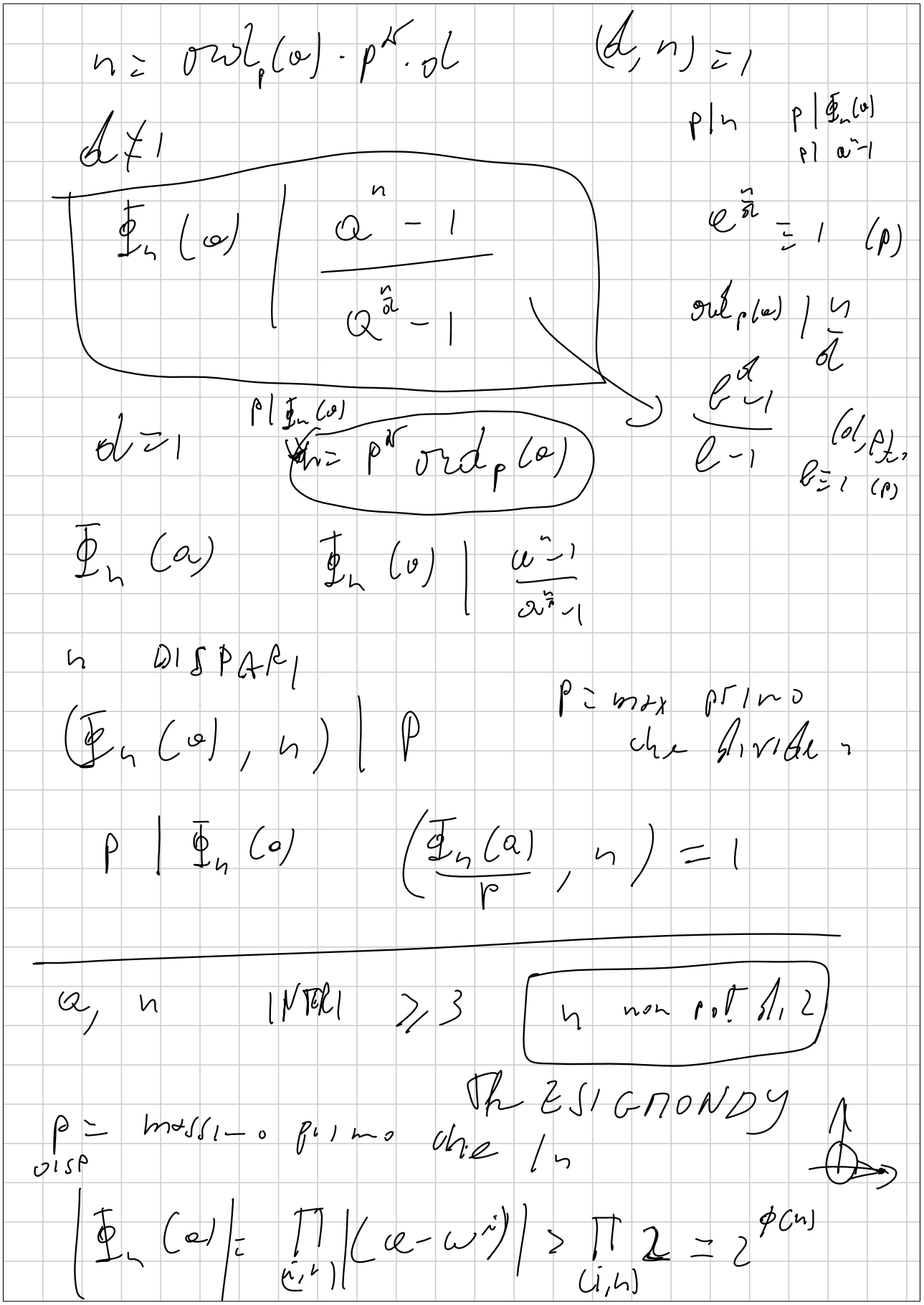
$a^p - b^p$ HA FATTORE PRIMO NUOVO RISP A $a-b$

$p \mid (a^m)^p - 1 \qquad (a^m)^p \equiv a^m \Rightarrow p \mid a^m - 1$

$v_p(a^{mp}-1) = 1 + v_p(a^m-1)$ p DIFF.

$v_2(a^{m2}-1) = v_p(a^m-1) + v_p(a^m+1)$ $p=2$

$p \mid \Phi_n(a) \quad \therefore p \mid a^n - 1$


n = ord_p(a) · p^α · d
(d, n) = 1
d ≠ 1
p | n
p | Φ_n(a)
p | a^n − 1
Φ_n(a) | (a^n − 1)/(a^{n/d} − 1)
e^{n/d} ≡ 1 (p)
ord_p(a) | n/d
(a^α − 1)/(a − 1)
d = 1
p | Φ_n(a)
n = p^α ord_p(a)
(d, p, e, e ≡ 1 (p))
Φ_n(a)
Φ_n(a) | (a^n − 1)/(a^{n/r} − 1)
n DISPARI
(Φ_n(a), n) | p
p = max primo che divide n
p | Φ_n(a)
(Φ_n(a)/p, n) = 1
a, n INTERI ≥ 3
n non può stare 2
Th ZSIGMONDY
p = massimo primo che divide n
DISP
|Φ_n(a)| = ∏_{(i,n)=1} |(a − ω^i)| > ∏_{(i,n)} 2 = 2^{φ(n)}

$p \nmid \Phi_n(a)$ $\quad q \nmid n$ $\quad \operatorname{ord}_q(a) = n$

$q \mid \Phi_n(a)$

$p \mid \Phi_n(a)$ $\quad \left(\frac{\Phi_n(a)}{p}, n\right) = 1$

$|\Phi_n(a)| > 2^{\varphi(n)} \geq n$

$\left|\frac{\Phi_n(a)}{p}\right| \geq 1 \Rightarrow \exists q : q \mid \frac{\Phi_n(a)}{p}$

$\Rightarrow q \nmid n$

$\operatorname{ord}_q(a) = n$

$a, n \geq 3$ $\quad n \neq 2^N$

$\exists q$ PRIMO T.C. $\operatorname{ord}_q(a) = n$

$\forall n \in \mathbb{N}^+ \exists$ infiniti primi $\equiv 1 \pmod{n}$

$n \mid m$ T.C. $m \geq 3$ m non è potenza di 2

$m = 3n$

$$P = \prod_{\substack{p \equiv 1 \pmod{m} \\ p \text{ PRIMO}}} p$$

$\exists q : \operatorname{ord}_q(P) = m$

$m \mid q-1 \Rightarrow q \equiv 1 \pmod m \qquad q \mid P$

ASSURDO !

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