Stage Senior 2011 – Livello Medium

Stampato integrale delle lezioni

Autori vari

Indice

SENIOR 2011 – PRELIMINARI (medium)

Titolo nota 04/09/2011

PIGEONHOLE

Esempio 1 (Approssimazione diofantea)
Sia $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Allora esiste una successione di frazioni $\frac{p_n}{q_n} \in \mathbb{Q}$ t.c.

$$\left| \alpha - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n^2}$$

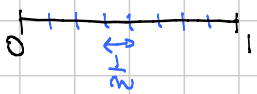
Oss. In certo senso è falso se $\alpha \in \mathbb{Q}$ perché la differenza o è uguale a 0, oppure è dello stesso ordine di $\frac{1}{q_n}$
Se fosse $\alpha = \frac{p}{q}$

$$\left| \frac{p}{q} - \frac{p_n}{q_n} \right| = \left| \frac{p q_n - p_n q}{q\, q_n} \right| \geq \boxed{\frac{1}{q}}^{\text{Fisso}} \frac{1}{q_n}$$

Lemma Dato α e dato n, esiste p/q t.c.

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{nq} \quad \text{e} \quad q \leq n$$

Dim. Consideriamo $\{0 \cdot \alpha\}, \{1 \cdot \alpha\}, \{2 \cdot \alpha\}, \dots, \{n \cdot \alpha\}$
dove $\{x\} = x - \lfloor x \rfloor$ = parte frazionaria.
Ho quindi $(n+1)$ numeri che stanno in $[0,1]$. Quindi o ne sono almeno 2 la cui distanza è $\leq \frac{1}{n}$



Quindi

$$\left| \{k_1 \cdot \alpha\} - \{k_2 \cdot \alpha\} \right| \leq \frac{1}{n}$$

$$= \left| k_1 \alpha - R_1 - (k_2 \alpha - R_2) \right| \leq \frac{1}{n} \iff \left| (k_1 - k_2)\alpha - (R_1 - R_2) \right| \leq \frac{1}{n}$$

Divido per $k_1 - k_2$:

$$\left| \alpha - \underbrace{\boxed{\frac{R_1 - R_2}{k_1 - k_2}}}_{\frac{p}{q}} \right| \leq \underbrace{\boxed{\frac{1}{n \cdot (k_1 - k_2)}}}_{\frac{1}{nq}}$$

Il denominatore $k_1 - k_2$, che WLOG posso supporre > 0, è $\leq n$ perché diff. di 2 numeri $\leq n$.

— o — o —

Dim. di approx. diofantea dato il Lemma.

Fisso $n = 12$

Trovo $\frac{p_1}{q_1}$ t.c. $\left|\alpha - \frac{p_1}{q_1}\right| \leq \frac{1}{12 q_1} \leq \frac{1}{q_1^2}$

↑ perché $12 \geq q_1$

Ora utilizzo nuovamente il lemma con un valore di n t.c.

$$\frac{1}{n} < \left|\alpha - \frac{p_1}{q_1}\right|$$

Trovo $\frac{p_2}{q_2}$ t.c. $\left|\alpha - \frac{p_2}{q_2}\right| \leq \frac{1}{n \cdot q_2} \leq \frac{1}{q_2^2}$ (perché $q_2 \leq n$)

$$\leq \frac{1}{n} < \left|\alpha - \frac{p_1}{q_1}\right|$$

Questo assicura che $\frac{p_2}{q_2} \neq \frac{p_1}{q_1}$

E così via per induzione.

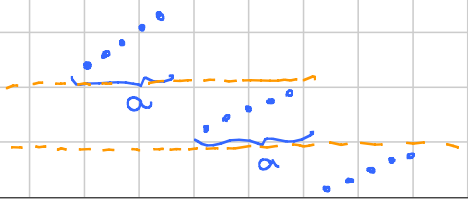
— o — o —

Esempio 2 **Lemma ab+1** Supponiamo di avere una successione di $ab+1$ numeri reali. Allora esistono

- o una sottosucc. di $a+1$ termini debolmente crescente
- o una sottosucc. di $b+1$ termini debolmente decrescente.

Oss. 1 Se gli $ab+1$ numeri sono tutti distinti, allora sono strettamente monotone.

Oss 2 Se i numeri sono solo ab, allora non è detto che esistano



Facciamo b scalini di questo tipo.

Dim 1 Supponiamo che non esistano sottosuccessioni con $b+1$ elementi decrescenti. Voglio trovare una di $a+1$ termini crescente.

Per ogni elemento degli $ab+1$ dati, considero la più lunga s. succ. decrescente di cui fa parte (potrebbe essere fatta da 1 solo elemento, se sono più di una ne scelgo una a caso). Considero la posizione che questo elemento occupa nella sottosuccessione: può essere un intero da 1 a b.

Pigeonhole: ci saranno almeno $a+1$ termini che occupano la stessa posizione. Voglio dimostrare che questi formano una s. succ. crescente.

Supponiamo per assurdo che non sia così. Mettiamo che siano i "tersi" delle rispettive successioni

↑ ora questo ha 3 elementi prima in ordine decrescente, quindi ho "allungato" la succ. di cui faceva parte. Assurdo

Dim. 2 Supponiamo che non esista s. succ. di $b+1$ decrescente.

Prendo un el. qualunque, prendo la max decrescente (o una delle ...) e la elimino. Poi ripeto sui rimanenti, e così via. Ad ogni mossa elimino al max b elementi, quindi faccio almeno $a+1$ mosse.

Hope: i primi elementi delle varie s. succ. considerate ai vari passi siano in ordine crescente.

Se non lo fossero

eliminati insieme

Falso perché ce n'è ancora una prima.

è la più lunga decrescente che contiene un certo suo elemento

Non funziona, perché magari il precedente era già stato eliminato in un passaggio precedente.

—o—o—

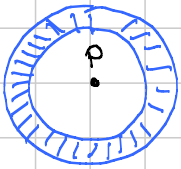
Esempio 3 Dati 28 p.ti in sfera di raggio 2, ne esistono almeno 2 con distanza ≤ 2.

Idea basic: dividere la sfera in 27 parti, tutte di diametro ≤ 2

Idea medium: per ogni p.to prendiamo la sfera con centro in lui e raggio 1. Se la tesi del problema fosse falsa, le sfere sarebbero tutte disgiunte.
Queste sferette possono uscire dalla sfera iniziale, ma comunque stanno nella sfera di raggio 3 e stesso centro di quella iniziale.
Ma 28 sfere di raggio 1 disgiunte non stanno in una sfera di raggio 3.

Esempio 4 Cerchio con $R = 16$ e 196 p.ti dentro.
Allora esiste una corona circolare di raggi 4 e 5 che ne contiene almeno 5.

Idea medium



Se voglio che P stia in una corona, il centro della corona dovrà stare in una corona con centro in P e raggi 4-3.

Conclusione ① per ognuno dei 196 p.ti considero la corona con centro in lui e raggi 4-5.
② ho 196 corone contenute in un cerchio di raggio 21
③ Conto: 196 · area corona $> 21^2 \pi \cdot 4$
④ Pigeonhole: esiste almeno un p.to che sta in 5 corone. La corona centrata in quel p.to contiene almeno 5 p.ti originari.

Fatto generale Se ho k figure $F_1, \dots, F_k$ contenute in G e

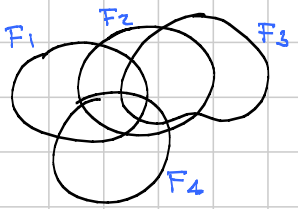
$$\text{Area}(F_1) + \dots + \text{Area}(F_k) > n \cdot \text{Area}(G)$$

Allora almeno un p.to di G è contenuto in almeno $(n+1)$ delle figure F_k.

Specie di double counting.

Suddivido G in "figure elementari": dato un sottoinsieme $A \subseteq \{1, \dots, k\}$, pongo

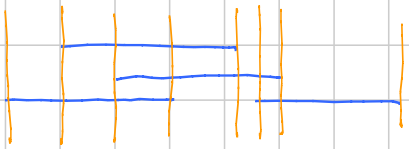
$$F_A = \{ x \in G : x \in F_k \ \forall k \in A, \quad x \notin F_k \ \forall k \notin A \}$$



Somma Aree (F_k) = somma aree elementari figura per figura.
Altro modo di contare: ogni figura elementare conto quante volte viene considerata.

Se ogni p.to del piano sta in al + n figure, allora ogni figura elementare conta al massimo n volte, quindi

$$\text{Somma Aree}(F_k) \leq n \cdot \text{somma Aree}(\underbrace{\text{fig. elem.}}_{\text{sono disgiunte.}}) \leq n \cdot \text{Area } G$$



Esempio 1 Convergenza di serie

$$\frac{1}{1^a} + \frac{1}{2^a} + \frac{1}{3^a} + \dots + \frac{1}{n^a} = S_{a,n}$$

Per quali valori di a esiste una costante M t.c.

$$S_{a,n} \le M \qquad \forall n \in \mathbb{N}.$$

Risposta: se e solo se $a > 1$

Abbastanza facile: per $a = 1$ non è limitata, dunque non lo è nemmeno per $a \le 1$.

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \dots$$

$$\ge 1 + \underbrace{\frac{1}{2}}_{\frac{1}{2}} + \underbrace{\frac{1}{4} + \frac{1}{4}}_{\frac{1}{2}} + \underbrace{\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}}_{\frac{1}{2}} + \underbrace{\frac{1}{16} + \dots}_{\dots}$$

$a = 2$ Dico che $1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2} \le 2$

Per induzione così non funziona. Provo a dim. una cosa più difficile

$$1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2} \le 2 - \frac{1}{n}$$

Provo per induzione: $n = 1$ ok.

P.I.

$$1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2} + \frac{1}{(n+1)^2} \overset{\text{Hp induttiva}}{\le} 2 - \frac{1}{n} + \frac{1}{(n+1)^2} \overset{\text{spero}}{\le} 2 - \frac{1}{n+1}$$

Speranza $\iff \frac{1}{(n+1)^2} + \frac{1}{n+1} \le \frac{1}{n}$

$$\iff \frac{1 + n + 1}{(n+1)^2} \le \frac{1}{n} \iff (n+2)\,n \le (n+1)^2$$

Ok, fortuna!

Cosa succede per $a \in (1,2)$? Provo per induzione a dim. che

$$1 + \frac{1}{2^a} + \frac{1}{3^a} + \dots + \frac{1}{n^a} \leq A - \frac{B}{n^{a-1}}$$

$n=1$ Basta $A - B \geq 1$

P.I. $$1 + \dots + \frac{1}{n^a} + \frac{1}{(n+1)^a} \leq A - \frac{B}{n^{a-1}} + \frac{1}{(n+1)^a} \overset{\text{Hope}}{\leq} A - \frac{B}{(n+1)^{a-1}}$$

Speranza $\iff$ $$B\left(\frac{1}{n^{a-1}} - \frac{1}{(n+1)^{a-1}}\right) \geq \frac{1}{(n+1)^a}$$

$$\iff \left(\frac{(n+1)^{a-1}}{n^{a-1}} - 1\right) \geq \frac{1}{n+1}\,\frac{1}{B}$$

$$\iff \left(\frac{n+1}{n}\right)^{a-1} - 1 \geq \frac{1}{B}\,\frac{1}{n+1} \qquad (1+x)^\alpha \geq 1 + \alpha x$$

$$\left(1 + \frac{1}{n}\right)^{a-1} \geq 1 + \frac{a-1}{n} \geq 1 + \frac{a-1}{n+1}$$

Quindi ok per di prendere $B = \frac{1}{a-1}$ e A di conseguenza.

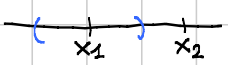
— o — o —

IMO 1991 – 6 Sia $a > 1$. Mostrare che esiste una successione $x_0, x_1, x_2, \dots$ limitata tale che

$$|x_i - x_j| \geq \frac{1}{|i-j|^a} \quad \text{per ogni } i \neq j.$$

Prendo x_1 dove mi pare. Quali vincoli ho?

Gli altri $|x_i - x_1| \geq \frac{1}{|i-1|^a}$



Prendo x_2 fuori dall'intervallo. Quali vincoli ho?

Supponiamo di aver scelto $x_1, \dots, x_k$. Dove non posso prendere x_{k+1}? Non può stare:

* a distanza 1 da x_k
* a distanza $\frac{1}{2^a}$ da x_{k-1}
* a distanza $\frac{1}{3^a}$ da x_{k-2}

⋮

L'unione degli intervalli esclusi ha area

$$2 \cdot \left(1 + \frac{1}{2^a} + \frac{1}{3^a} + \dots + \frac{1}{k^a}\right)$$

Costruzione: prendo un intervallone di area $>$ 2 · somma serie

Ad ogni passaggio, la somma delle aree escluse è minore dell'area dell'intervallo, quindi c'è sempre almeno 1 pto buono

— o — o —

Esempio 3 Frazioni egizie: $\frac{1}{n}$ (numeratore = 1)

Problema classico: ogni razionale >0 è somma di frazioni egizie (in modo non unico) distinte.

Non solo: se ho iniziato una scrittura di un certo $q \in \mathbb{Q}$, e sono ancora sotto, posso completarla.

Idea: mettere ad ogni passaggio la frazione più grande che ci sta. Quello che succede è che ad ogni passaggio il numeratore SCENDE!

Supponiamo che rimanga da fare $\frac{p}{q}$. Voglio usare un certo $\frac{1}{n}$. Chi sarà il resto nuovo?

$$\frac{p}{q} - \frac{1}{n} = \frac{np - q}{nq}$$

Voglio $np - q \geq 0 \quad n \geq \frac{q}{p}$

Voglio $np - q < p \iff (n-1)p < q \iff n < \frac{q}{p} + 1$

Quindi prendo $n = \lceil \frac{q}{p} \rceil$

Devo verificare che questa procedura produce n nuovi di volta in volta.

RMH 2009 - 4

$X \subseteq \mathbb{N}$ t.c. $\sum_{x \in X} \arctan \frac{1}{x} < \frac{\pi}{2}$

$\Rightarrow \exists\, Y \supseteq X,\ Y \subseteq \mathbb{N}$ t.c.

$$\sum_{y \in Y} \arctan \frac{1}{y} = \frac{\pi}{2}$$

$$\frac{3}{2} = \frac{1}{2} + \frac{1}{2} + \frac{1}{2}$$
$$= \frac{1}{2} + \frac{1}{2} + \frac{1}{3} + \frac{1}{6}$$
$$= \frac{1}{2} + \frac{1}{3} + \frac{1}{6} + \frac{1}{3} + \frac{1}{6} + \frac{1}{12} + \dots$$

SENIOR 2011 - A1 MEDIUM

Titolo nota 06/09/2011

① Polinomi
② Poli simmetrici in + variabili
③ Lemma di Gauss, irriduc in $\mathbb{Q}[x]$
④ Polinomi ciclotomici

Polinomio $\sum_{i=0}^{n} a_i x^i$. $a_i \in \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$
$K[x_1, \dots, x_n]$

Principio di identità ⟹ infinito
A anello: f, g polinomi di grado $\leq n$. Sono equivalenti:
① $f = g$ come poli (sono = i coeff)
② $f(x) = g(x)$ per $n+1$ valori di x
③ $f(x) = g(x)$ $\forall x \in A$.

Dim:
① ⟹ ②,③
② ⟹ ① $x_1, \dots, x_{n+1}$ radici
$x - x_1 \mid f(x) - g(x)$.
$f(x) - g(x) = (x - x_1)\, q_1(x)$
$= (x - x_1)(x - x_2) \cdots (x - x_{n+1})\, q_{n+1}(x)$
grado $\leq n$ grado $\geq n+1$ oppure è il poli $\equiv 0$

Attenzione! ③ non è equivalente
$\mathbb{Z}/p\mathbb{Z}$ $x^p - x = 0$ è vero $\forall x \in \mathbb{F}_p$ (piccolo Fermat)
ma non sono uguali come poli!!

Con anello infinito, basta ③ ⟹ ②.

② ⇒ ① $f(x) = \sum_{i=0}^{m} a_i x^i$ t.c

$f(x_i) = g(x_i) \quad \forall i = 0, \dots m+1$

$$\begin{cases} a_0 + a_1 x_1 + \dots + a_m x_1^m = g(x_1) \\ \vdots \\ a_0 + a_1 x_{m+1} + \dots + a_m x_{m+1}^m = g(x_{m+1}) \end{cases}$$

sono $m+1$ condizioni lineari.

Fatto misto 1: un sist lineare (m eq in m incognite) ha esattam una sol ($\Leftrightarrow$) det della matrice dei coeff è $\neq 0$

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^m \\ \vdots & & & & \\ 1 & x_{m+1} & x_{m+1}^2 & \dots & x_{m+1}^m \end{pmatrix}$$

= matrice dei coeff

Fatto misto 2: le matrici di questa forma hanno sempre det $\neq 0$.

Prop: dati $m+1$ punti (x_i, y_i) esiste un unico poli di grado $\leq m$ t.c $p(x_i) = y_i \ \forall i$.

Dim:

1° caso: $y_0 = \dots y_m = 0 \quad p(x) = 0$

$y_0 = 1 \quad y_1 = \dots y_m = 0. \quad (x - x_1) \dots (x - x_m) = q(x)$

$\frac{q(x)}{q(x_0)}$ realizza tutto $= \frac{(x-x_1)\dots(x-x_m)}{(x_0-x_1)\dots(x_0-x_m)} = L_0(x)$

Caso generale:

$P(x) = \sum y_i L_i(x)$ funziona, perchè

$$L_i(x) = \begin{cases} 0 & \text{se } x \neq x_i \\ 1 & \text{se } x = x_i \end{cases}$$

$P(x_k) = y_k$.

Criterio della derivata

$f(x) = \sum_{i=0}^{m} a_i x^i \Rightarrow Df(x) := \sum_{i=1}^{m} a_i\, i\, x^{i-1}$. $a_i \in K$ campo

Proprietà:

$D(f+g) = Df + Dg$

$D(\lambda f) = \lambda Df$ se $\lambda \in K$

$D(fg) = Df \cdot g + Dg \cdot f$ [Ex: verificare]

Ex: ① $x^4 + 3x + 1 \longrightarrow 4x^3 + 3$

② in $\mathbb{F}_p$ $x^p - 1 \longrightarrow \underbrace{p}_{=0} x^{p-1} = 0$

Criterio: K campo, $f \in K[x]$.

f ha radici multiple (in $\overline{K}$) $\iff$

$MCD(f, Df) \neq 1$.

Dim

$\Rightarrow$) $f(x) = (x-x_1)^m \cdot q(x)$ $m > 1$

$MCD\big((x-x_1)^m \cdot q(x),\ (x-x_1)^m Dq(x) + D((x-x_1)^m)\, q(x)\big)$

$D((x-x_1)^m) = m(x-x_1)^{m-1}$ [Ex: per induz su m]

L'MCD è diviso da $(x-x_1)^{m-1} \neq 1$!

$\Leftarrow$) Dobbiamo dimostrare che, se f non ha radici multiple,

$x - x_1 \mid f(x) \overset{?}{\Rightarrow} x - x_1 \nmid Df(x)$.

$f(x) = (x-x_1)\, q(x)$ e $q(x_1) \neq 0$

$Df(x) = q(x) + (x-x_1)\, Dq(x)$

$Df(x_1) = \underbrace{q(x_1)}_{\neq 0} + 0$. ok.

Polinomi in più indeterminate.

$p(a,b,c) = a^3+b^3+c^3-3abc$.

Ex: p simmetrico $\Rightarrow$ se posso scomporlo, i suoi fattori sono simmetrici.

Ex: p è omogeneo $\Rightarrow$ tutti i fattori sono omogenei.

Dim 2:

Idea: $p(x_1,\dots,x_m) = f(x_1,\dots,x_m)\cdot g(x_1,\dots,x_m)$

Consideriamo i monomi di grado più alto in f e g.

Come si fattorizzano?

1° modo: guardiamo c come la variabile principale, a,b fissi. $c=-a-b$ è radice

$a^3+b^3+(-a-b)^3+3ab(a+b)=0$

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

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

$a^3+b^3+c^3-3abc = (a+b+c)\cdot$ cosa?

Posso ottenere "cosa" facendo la divisione

$$\begin{array}{l} c^3 - 3abc + a^3+b^3 \\ -c^3 + ac^2+bc^2 \\ \hline (a+b)c^2 - 3abc + a^3+b^3 \end{array} \quad \Big| \; c+a+b \qquad c^2 \quad \text{etc.}$$

Altro modo per dot "cosa":

Teorema fondamentale dei poli simmetrici

$x_1,\dots,x_n$ indeterminate

$$\begin{cases} \sigma_1 = x_1+\dots+x_n \\ \sigma_2 = x_1x_2+x_1x_3+\dots+x_{n-1}x_n \\ \sigma_k = \prod_{i=1}^{n} x_i \end{cases}$$ sono funz simmetriche.

$F(x_1,\dots,x_n)$ poli simmetrico, allora $\exists\, \tilde{F}$ polinomio

t.c $F(x_1,\dots,x_n) = \tilde{F}(\sigma_1,\dots,\sigma_n)$.

Ex: $x_1^2 + \dots + x_n^2 = F(x_1,\dots,x_n)$

$(\sum x_i)^2 - 2\sum_{i\neq j} x_i x_j$

$\tilde{F}(\sigma_1,\dots,\sigma_n) = \sigma_1^2 - 2\sigma_2$.

$a^3+b^3+c^3-3abc = (a+b+c)\cdot f(a,b,c)$

Sappiamo che $f(a,b,c)$ è simmetrico (ex di prima), è omogeneo di grado 2.

$f(a,b,c) = A\,\underset{(a+b+c)^2}{\sigma_1^2} + B\,\underset{ab+bc+ca}{\sigma_2}$

Devo determinare A e B.

Chi è il coeff di a^3?

In LHS è 1, in RHS è A

$1 = A$

Come det B? L'uguaglianza deve valere con $a=b=c=1$

$0 = 3(3^2 + B\cdot 3)$

$B = -3$

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

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

Es: $\mathbb{Q}(i)$.

K campo $p(x) \in K[x]$.

$\frac{K[x]}{(p(x))}$

Es: $p(x) = x^2 - 5 \qquad x^3 - 3x$ va diviso per $p(x)$ e poi si prende la classe di resto.

Fatto: $\frac{K[x]}{p(x)}$ è un campo se p è irriducibile.

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

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

$\{a+bx : a,b \in \mathbb{R}\}$

$a+bx \longrightarrow a+bi$.

Gli oggetti si sommano e moltiplicano allo stesso modo:

$(a+bx)+(a'+bx) = a+a'+(b+b')x$

$(a+bi)+(a'+b'i) = a+a'+(b+b')i$

Idem per la moltiplicaz

Dim del fatto:

Ogni elemento $\overset{f(x)}{\text{V}}$ ha un inverso?

Teorema di Bezout per polinomi:

$f(x), p(x)$ sono coprimi $\Rightarrow \exists\, a(x), b(x)$ t.c

$1 = a(x)\cdot f(x) + b(x)\cdot p(x)$.

L'inverso di $f(x)$ in $\frac{K[x]}{(p(x))}$ è $a(x)$, perché

$a(x)\cdot f(x) \equiv 1 \quad (p(x))$.

Ex: $\dfrac{\mathbb{F}_p[x]}{(x^2-5)} =$ → se $\exists\, a \in \mathbb{F}_p$ t.c. $a^2 = 5$, poco interess
→ altrimenti il denom è irriducibile,
$\{a+bx : a,b \in \mathbb{F}_5\}$ quindi quello è un campo.
Quanti elementi? 25.

Ex: consideriamo i Fibonacci

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

Guardiamo la succ mod p, p primo.

① La succ è periodica, chiamiamo $\pi(p)$ il periodo.

② Se $p \equiv \pm 1 \ (5)$ allora $\pi(p) \mid p-1$

③ Se $p \equiv \pm 2 \ (5)$ allora $\pi(p) \mid 2(p+1)$

Dim:

① $\{(F_i, F_{i+1}) : i = 1, \dots, p^2+1\}$
Una coppia si ripete. Da lì, si ripete tutta la stringa.

Perchè non ha antiperiodo?

Oss 1: $p \equiv \pm 1 \bmod 5 \iff p$ è un quadrato mod 5
$\iff 5$ è un quadrato mod p
(dalla reciprocità quadratica,
$\left(\frac{p}{5}\right)\cdot\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{5-1}{2}} = 1$.

Oss 2: Possiamo pensare la succ in $\mathbb{F}_p$

Oss 3: $F_n = \dfrac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$.

Vale anche in $\mathbb{F}_p$, se $\exists\, x \in \mathbb{F}_p$ t.c. $x^2 = 5$

Ex: ricavare la formula per i Fibonacci in $\mathbb{F}_p$.

Dim di ②. $\sqrt{5}$ è un elemento di $\mathbb{F}_p$.
mod 11 $\sqrt{5} = 4$

Basta far vedere che

$F_{p-1} = 0$ e $F_p = 1$.

$$F_{p-1} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{p-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{p-1}}{\sqrt{5}} \overset{\text{piccolo teo Fermat}}{=} \frac{1-1}{\sqrt{5}} = 0$$

$$F_p = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{p} - \left(\frac{1-\sqrt{5}}{2}\right)^{p}}{\sqrt{5}} = \frac{\frac{4+\sqrt{5}}{2} - \frac{4-\sqrt{5}}{2}}{\sqrt{5}} = 1 \text{ . ok.}$$

Dim di ③ Im $\frac{\mathbb{F}_p[x]}{(x^2-5)} =: K$ è elemento x è una radice di 5

$x^2 = 5$

$\mathbb{F}_p \ni a \mapsto a + 0 \cdot x$

le piccolo teo di Fermat non vale più!!! (No dim di prima).

Domanda: quanto fa $\left(\frac{1+\sqrt{5}}{2}\right)^p$ in K?

$(a+b)^p = ?$ se $a, b \in K$

$$= \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p$$

Quindi $\left(\frac{1+\sqrt{5}}{2}\right)^p = \frac{(1+\sqrt{5})^p}{2^p} \overset{\text{fatto sopra}}{=} \frac{1+(\sqrt{5})^p}{2}$

Basta capire cosa fa $(\sqrt{5})^p$.

Osserviamo che $(\sqrt{5})^p$ risolve $x^2 - 5 = 0$:

$$(\sqrt{5}^p)^2 - 5 = \sqrt{5}^{2p} - 5 = 5^p - 5 = 0.$$

$x^2 - 5 = 0$ ha due sol: $\sqrt{5}$ e $-\sqrt{5}$

Può essere $(\sqrt{5})^p = \sqrt{5}$? No! Se lo fosse, $\sqrt{5}$ sarebbe una radice di $x^p - x = 0$.

Ma conosciamo tutte quelle radici: $0, 1, \dots p-1$.
Avevamo assunto che $\sqrt{5} \notin \mathbb{F}_p$.

Quindi $(\sqrt{5})^p = -\sqrt{5}$.

Allora $\left(\frac{1+\sqrt{5}}{2}\right)^p = \frac{1+(\sqrt{5})^p}{2} = \frac{1-\sqrt{5}}{2}$ (*)

Similmente $\left(\frac{1-\sqrt{5}}{2}\right)^p = \frac{1-(\sqrt{5})^p}{2} = \frac{1+\sqrt{5}}{2}$ (*)

Per dim la tesi, basta vedere
$F_{2p+2} = 0$ $\quad$ $F_{2p+3} = 1$

$$F_{2p+2} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{2p+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{2p+2}}{\sqrt{5}} \overset{(*)}{=} \frac{\left(\frac{1-\sqrt{5}}{2}\right)^2\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1+\sqrt{5}}{2}\right)^2\left(\frac{1-\sqrt{5}}{2}\right)^2}{\sqrt{5}}$$

$$= 0$$

[$F_{2p+3} = $ ex.]

□.

Ex! (4) mostrare che $\pi(p^k) \leq p^{k-1}\pi(p)$
con $=$ se e solo se $\pi(p) \neq \pi(p^2)$.

Polinomi a coeff interi

Teorema: $f(x) = \sum a_i x^i$ $a_i \in \mathbb{Z}$, p/q radice razionale $(p,q)=1$

Allora

$p \mid a_0$

$q \mid a_m$.

Dimo

$$q^m \cdot 0 = \left(a_0 + a_1 \tfrac{p}{q} + \dots + a_m \tfrac{p^m}{q^m}\right) q^m$$

$$0 = a_0 q^m + a_1 p q^{m-1} + \dots + a_m p^m$$

p divide la somma e il $2^\circ, \dots m^\circ$ monomio

$\Rightarrow p \mid a_0 q^m \qquad (p,q)=1$

$\Rightarrow p \mid a_0$.

L'altra è uguale.

Esempio: x^3+x+1 è riducibile in $\mathbb{Q}[x]$?

No. Se fosse riducibile avrebbe un monomio di grado 1, quindi una radice razionale

Per il teo precedente, il numerat dovrebbe dividere 1 e anche il denom.

Ma 1 e -1 non sono radici

Lemma di Gauss

$p(x) \in \mathbb{Z}[x]$. Se $p(x)$ si spezza in $\mathbb{Q}[x]$ allora si spezza anche in $\mathbb{Z}[x]$.

$p(x) = a(x) \cdot b(x)$ $\quad a, b \in \mathbb{Q}[x] \Rightarrow \exists\, \tilde{a}$ e $\tilde{b} \in \mathbb{Z}[x]$ t.c

$$p(x) = \tilde{a}(x) \cdot \tilde{b}(x).$$

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

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

Def: $p(x) \in \mathbb{Z}[x]$, $p(x) = \sum a_i x^i$. Il CONTENUTO DI p è

$$c(p) = MCD(a_0, \ldots, a_m).$$

Lemma: il contenuto è moltiplicativo,

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

Oss: una divisibilità è ovvia.

Dim lemma:

① Basta farlo con $c(a) = c(b) = 1$.

$a(x) = c(a) \cdot \tilde{a}(x)$ $\qquad b(x) = c(b) \cdot \tilde{b}(x)$

con $c(\tilde{a}) = c(\tilde{b}) = 1$

$a(x) \cdot b(x) = c(a) \cdot c(b) \cdot \tilde{a}(x) \cdot \tilde{b}(x)$

Supponiamo di aver dimostrato la tesi su $\tilde{a}$ e $\tilde{b}$

$c(a(x) \cdot b(x)) = c(a) \cdot c(b) \cdot \underbrace{c(\tilde{a} \cdot \tilde{b})}_{= 1}$

② $c(a) = c(b) = 1$

Dobbiamo dim che $\nexists\, p$ t.c.

$p \mid$ tutti i coeff di $a(x) \cdot b(x)$.

Se esistesse un tale p,

$\bar{a}(x) \cdot \bar{b}(x) = 0$ in $\mathbb{F}_p[x]$,

assurdo (prendiamo $a_k x^k$ monomio di grado max in $\bar{a}(x)$, $b_\ell x^\ell$ monomio di grado max in $\bar{b}(x)$.
$\bar{a}(x)\cdot\bar{b}(x)$ contiene un solo monomio di grado $x^{\ell+k}$, che è $a_k \cdot b_\ell x^{k+\ell}$, che non si annulla).

[Fatto intermedio: se p divide tutti i coeff di $a(x)\cdot b(x)$, allora divide tutti i coeff di a oppure di b.].

Dim lemma di Gauss

① Supponiamo $c(p)=1$

② $p(x)=a(x)\cdot b(x)$ $\quad a(x)=\frac{A(x)}{m}\in\mathbb{Z}[x]$, $m\in\mathbb{N}$ $\quad b(x)=\frac{B(x)}{n}$, $n\in\mathbb{N}$.

$mn\, p(x)=A(x)\cdot B(x)$

$c(mn\, p(x))=mn\, c(p(x))=1$ $= c(A(x)\cdot B(x))$

[Fatto: $c(m\cdot p(x))=m\cdot c(p(x))$] $= c(A(x))\cdot c(B(x))$

(lemma) (*)

$p(x)=a(x)\cdot b(x)=\frac{A(x)}{m}\cdot\frac{B(x)}{n}$ uso (*) $=\frac{A(x)}{c(A(x))}\cdot\frac{B(x)}{c(B(x))}$

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

Oss: se $n=6$ esistono due poli a prodotto nullo in $\mathbb{Z}/6\mathbb{Z}[x]$:

$(2x+2)\cdot 3x \equiv 6x^2+6x = 0$ in $\mathbb{Z}/6\mathbb{Z}[x]$.

Irriducibilità

Come faccio a dire che $f(x)$ (monico) è irriducibile su $\mathbb{Z}[x]$?

(1) Trovare p primo t.c. $\overline{f}(x)$ è irriducibile.

Oss: esistono polinomi riducibili su $\mathbb{F}_p[x]$ $\forall p$ primo, ma irriducibili su $\mathbb{Z}[x]$. Es: x^4+1. [Ex].

Se si riducesse $f(x) = a(x)\cdot b(x)$ su $\mathbb{Z}[x]$

La guardo mod p.

(2) Eisenstein (vedi N1)

(3) $f(x) \in \mathbb{Z}[x]$, con termine noto ≠ 0 primo
e $|a_0| > \sum |a_i|$.
Allora f è irriducibile su $\mathbb{Q}[x]$

Dim!
Se f si riducesse
$f(x) = a(x)\cdot b(x)$ $\quad a, b \in \mathbb{Z}[x]$ (per il lemma di Gauss)
↑ ↑
WLOG il termine noto di $a(x)$ è ± 1 (e altrimenti è $\pm p$)
Allora $a(x)$ ha una radice (complessa) di mod ≤ 1, che chiamo z. (perché il prodotto delle radici è 1)

z è radice anche di f

$$0 = |f(z)| = \left|\sum a_i z^i\right| \geq |a_0| - \sum |a_i| \underbrace{|z|^i}_{\leq 1}$$
$$\geq |a_0| - \sum |a_i|$$
$$> 0$$
↑ per hp.

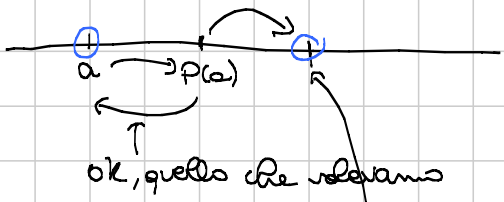
Assurdo.

Ex (IMO 2006 - 5)
$P(x)$ poli a coeff interi, $K \in \mathbb{N}$, $n = \deg P > 1$
Consideriamo il polinomio
$$P^{(k)}(x) = P(\underbrace{\dots}_{k \text{ volte}} P(x)) .$$
Dimostrare che esistono al più n interi t.c.
$$P^{(k)}(x) = x .$$

Dim:
[Fatto gen] $a, b \in \mathbb{Z}$ $\quad a-b \mid P(a)-P(b)$ (*)
Dim 1: fisso b, muovo a. $a=b$ è radice
Dim 2: $P(x) = \sum a_i x^i$
$$P(a) - P(b) = \sum a_i (a^i - b^i)$$
↑ divisibile per $a-b$

Step 1: sia a t.c $P^{(k)}(a) = a$.
$a - P(a) \mid P(a) - P^{(2)}(a) \mid P^{(2)}(a) - P^{(3)}(a) \mid \dots \mid P^{(k)}(a) - P^{(k+1)}(a)$
$= a - P(a)$
(*) con $b = P(a)$

Sono tutte "quasi" uguaglianze:
$$a - P(a) = \pm (P(a) - P^{(2)}(a))$$
Vediamo che $a = P^{(2)}(a)$ per ogni a t.c $a = P^{(k)}(a)$
Wlog $a < P(a)$



Se $P(P(a)) \geq$, $P^{(k)}(a)$ non può mai essere a (perchè si dovrebbe ripassare da $P(a)$ ...)

Ci siamo ridotti al caso $K=2$.

Vogliamo dim che

$p(p(x)) = p^{(2)}(x) = x$

ha al più n sol intere.

[Nota: $p^{(2)}(x) = x$ ha n^2 sol in $\mathbb{C}$ (perché n^2 è il grado]

Supponiamo per assurdo che ne abbia $n+1$, e siano $a_1, \dots, a_{n+1}$.

$a-b \mid p(a)-p(b) \mid p(p(a)) - p(p(b))$ (*) $\forall a,b \in \mathbb{Z}$.

Se $a=a_i$, $b=a_j$, otteniamo

$a_i - a_j = \pm(p(a_i)-p(a_j))$ (*)

(perché (*) dice

$a_i-a_j \mid p(a_i)-p(a_j) \mid a_i-a_j$)

ovvero

- $p(a_i)-a_i = p(a_j)-a_j$ (segno + in (*))
- $p(a_i)+a_i = p(a_j)+a_j$

per ogni $i,j \in \mathbb{N}$.

Chiamiamo $R(x) = p(x)-x$

$S(x) = p(x)+x$.

Allora $\forall i,j \in \mathbb{N}$

- $R(a_i) = R(a_j)$
- $S(a_i) = S(a_j)$

È possibile che $R(a_1) = R(a_j)$ $\forall j = 2, \dots, n+1$?

No, perché ~~$R(x)$~~ $R(x)-R(a_1)$ ha grado n e $n+1$ radici

Similmente, non è possibile che $S(a_1) = S(a_j)$ $\forall j = 1, \dots, n+1$

Quindi $\exists a_i, a_j$ t.c

(*) $R(a_i) \neq R(a_i) \Rightarrow S(a_i) = S(a_i)$

$S(a_i) \neq S(a_j) \Rightarrow R(a_i) = R(a_j)$ (*)

Prendiamo la coppia i, j.

$R(a_i) = R(a_j)$ o $S(a_i) = S(a_j)$

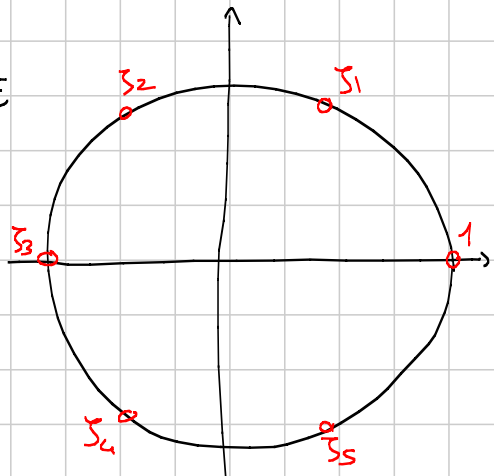
impossibile $R(a_i) = R(a_i)$ da (*), che contraddice (*)

Anche l'altra è assurda.

Radici dell'unità

Def: $\zeta \in \mathbb{C}$ si chiama RADICE n-ESIMA DI 1 se risolve

$$x^n - 1 = 0$$



Calcoliamo

ζ_1 $\zeta_1^2 = \zeta_2$ $\zeta_1^3 = \zeta_3$ ζ_4 ζ_5 1
ζ_2 ζ_4 1
$\zeta_3 = -1$ 1
ζ_4 ζ_2 1
ζ_5 ζ_4 ζ_3 ζ_2 ζ_1 1

ζ_1 ha periodo 6
ζ_2 " " 3
ζ_3 " " 2
ζ_4 " " 3
ζ_5 " " 6

Fattorizziamo

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

1 $\zeta_2\ \zeta_4$ -1 $\zeta_1\ \zeta_5$

periodo 1 — periodo 3 perché sono le radici terze di 1 — periodo 2 — periodo 6

Oss: radici con lo stesso periodo stanno nello stesso fattore

Def: si chiama n-ESIMO POLINOMIO CICLOTOMICO

$$\Phi_n(x) = \prod_{(i,n)=1} (x - \zeta_i)$$

Oss: ζ_i ha ordine $n \iff (i,n) = 1$ [Ex].

Oss: ① $\deg \Phi_n(x) = \varphi(n)$

② $\Phi_p(x)$ con p primo? $\Phi_p(x) = 1 + x + \ldots + x^{p-1} = \dfrac{x^p - 1}{x - 1}$

Fatto 1 $\Phi_m(x)$ ha coeff in $\mathbb{Z}[x]$ e è monico.

Dim

Per induzione su m. (estesa)

$$x^n - 1 = \prod (x - \zeta_i)$$

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

(Ex: pensarci bene)

$$= \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x) \cdot \Phi_n(x)$$

↑

Per ip induttiva $\Phi_d(x) \in \mathbb{Z}[x]$ $\forall d \mid n$ e monici

$\Rightarrow \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x) \in \mathbb{Z}[x]$ ed è monico

Se divido poli a coeff interi per poli monico e coeff interi, ottengo poli a coeff interi.
(pensare a come si fa la divisione)

Quindi: $\Phi_n(x)$ ha coeff interi ed è monico.

Ex: $z = \frac{3+4i}{5}$ può essere una radice di 1 per qualche n?

No!

Oss: $e^{i\theta}$ è radice di 1 se e solo se $\theta = p/q \cdot 2\pi$
(ex: scrivere perché)

Se fosse radice, $\{z^j\}_{j \in \mathbb{N}}$ sarebbe succ periodica.
Ma allora lo sarebbe in particolare $\mathrm{Re}(z^j) = \cos j\theta$
Allora $\{\cos j\theta\}_{j \in \mathbb{N}}$ sarebbe finito

$\cos\theta = \frac{3}{5}$, $\cos 2\theta = 2\cos^2\theta - 1 = 2 \cdot \frac{3^2}{5^2} - 1 = \frac{-7}{5^2}$

$\cos 4\theta = 2\cos^2 2\theta - 1 = 2\frac{7^2}{5^4} - 1 = \frac{2 \cdot 7^2 - 5^4}{5^4}$

Si vede che $\{\cos 2^j\theta\}$ ha potenze di 5 sempre + grandi

al denom.
Quindi la succ non assume un n° finito di valori.

□

Fatto: $\Phi_n(x)$ è irriducibile per ogni n

Dim:
[Ex: per n primo.
Idea: applicare Eisenstein a $\Phi_n(x+1)$]
↑ trucco

$n \in \mathbb{N}$.
Teorema: esistono infiniti primi $p \equiv 1 \ (n)$.

Dim:
Consideriamo $a \in \mathbb{N}$, p primo

$$p \mid \Phi_n(a)$$

$$p \nmid n$$

[Ex: vedere che a e p con queste proprietà esistono e sono ∞]

[Riscritto: dato $f(x)$ polinomio non costante
$\{p : \exists x \in \mathbb{N} \ p \mid f(x)\}$ è infinito
Supponiamo sia finito. $\{p_1, \dots, p_m\}$.
Prendiamo $a_0 p_1 \cdots p_m \cdot 2$

$$f(a_0 p_1 \cdots p_m) = a_0 + a_1 a_0 p_1 \cdots p_m + \cdots + a_m a_0^m p_1^m \cdots p_m^m$$

$$= a_0 \left(1 + \underbrace{a_1 p_1 \cdots p_m + \cdots}_{\text{è divisibile per } p_1 \cdots p_m}\right)$$

$\Rightarrow$ è coprimo con $p_1 \cdots p_m$, quindi ha un altro fattore primo (se non è 1...)]

Teorema: $n \in \mathbb{N}$. esistono infiniti primi $p \equiv 1 \ (n)$.

Dim:

Consideriamo $a \in \mathbb{N}$, p primo

$$p \mid \Phi_n(a)$$

$$p \nmid n .$$

$$a^n - 1 = \Phi_n(a) \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(a) \equiv 0 \quad (p)$$

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

Vediamo che $\boxed{\operatorname{ord}_p a = n}$. Potrebbe essere meno?

Chiamiamo $\operatorname{ord}_p a = k$. Sappiamo $k \mid n$. ok

$a^k - 1 \equiv 0 \ (p)$.

$$p \mid \Phi_n(a) \mid \frac{a^n - 1}{a^{n/k} - 1} = 1 + a^k + a^{2k} + \dots + a^{(n/k-1)k}$$

$$\equiv 1 + 1 + 1 \dots + 1$$

$$\equiv \frac{n}{k} \quad (p)$$

$$\not\equiv 0 \quad (\text{perché } p \nmid n)$$

Siccome $\operatorname{ord}_p a = n$, $n \mid p-1$, che è la tesi.

□

Senior 2011 A2m – Jack

Titolo nota 08/09/2011

$p(x) = a_0 x^n + \dots + a_n \qquad a_i \in A \qquad A = \mathbb{Z}[x]$

ζ è radice di $p(x) \longrightarrow (x-\zeta) \mid p(x)$ (Ruffini)

ζ radice di molt. k se $(x-\zeta)^k \mid p(x)$

$p(\zeta) = 0, \; p'(\zeta) = 0 \dots, \; p^{(k-1)}(\zeta) = 0$

$\frac{d}{dx} x^m = m x^{m-1}$

$\forall p(x) \in \mathbb{C}[x] \quad \exists \zeta \in \mathbb{C} : p(\zeta) = 0$ | Teo fond Alg

Lemma 1. $\forall p(x) \in \mathbb{R}[x], \; \partial p \equiv 1 (2) \quad \exists \zeta \in \mathbb{R} : p(\zeta) = 0$ (per continuità)

Lemma 2. $p(x) \in \mathbb{R}[x] \quad p(\zeta) = 0$, allora $p(\bar{\zeta}) = 0$

$\zeta = a + ib, \quad \bar{\zeta} = a - ib$

$p(\zeta) = 0 \longrightarrow \bar{p}(\zeta) = 0 = p(\bar{\zeta})$

Lemma 3. (Viète) $p(x) \in \mathbb{C}[x] \qquad [x^{\partial p}] p(x) = 1$ monico

∂p radici $\zeta_1, \dots, \zeta_{\partial p}$

$n = \partial p$

$[x^{n-j}] p(x) = (-1)^j \sum_{1 \le i_1 < \dots < i_j \le n} \prod_{n=1}^{j} \zeta_{i_j}$ ← $p(x) = \prod_{i=1}^{n} (x - \zeta_i)$

$f(x_1, \dots, x_n)$ è f. sym. di n var se

$\forall \sigma \in S_n$ si ha $f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$

F. sym elementari di n variabili

$e_1(x_1, \dots, x_n) = x_1 + \dots + x_n$

$e_2(x_1, \dots, x_n) = \sum_{i<j} x_i x_j$

Somme di potenze

$p_1(x_1, \dots, x_n) = x_1 + \dots + x_n$

$p_k(x_1, \dots, x_n) = \sum x_i^k$

Theo Sia $\{e_i\}_{i=0}^{n-1}$ che $\{p_i\}_{i=0}^{n-1}$ sono una base per l'anello delle f. sym in n variabili

Dim Ind sul grado.

Formule di Newton-Girard

$$k \cdot e_k = \sum_{j=1}^{k} (-1)^{j-1} e_{k-j} p_j$$

Dim.
Ind sul grado
+ trucco analitico

$\frac{d}{dx} x^m \to m x^{m-1}$ $\qquad \delta : p(x) \to p(x) - p(x+1)$

forward diff. op.

$$\begin{cases} p \in \mathbb{Z}[x] \to \delta p \in \mathbb{Z}[x] \\ \delta(pq) + p \cdot (\delta q) + q \cdot (\delta p) + (\delta p)(\delta q) = 0 \\ \partial(\delta p) = \partial p - 1 \\ [x^{\partial p - 1}](\delta p) = -\partial p \, [x^{\partial p}] p \\ \delta^{\partial p} p = (-1)^{\partial p} \cdot (\partial p)! \cdot [x^{\partial p}] p \end{cases}$$

5	10	21	32	37
5	11	11	5	pol'n. di grado 2
6	0	−6		polinomio di grado 1
−6	−6	||		costante

metodo delle diff. finite

Disuguaglianze $x^2 \geq 0$.

$f : \mathbb{R}^n \to \mathbb{R}$ è detta convessa se $\forall \lambda_1, \dots, \lambda_n \in [0,1]$, $\sum \lambda_i = 1$ si ha $f(\sum_{i=1}^{n} \lambda_i x_i) \leq \sum_{j=1}^{n} \lambda_j f(x_j)$

Disug. di Jensen

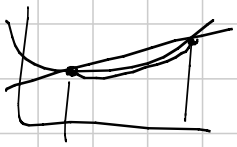
f si dice midpoint-convex se $\forall (c,d) \in [a,b]^2$ si ha

$$f\left(\frac{c+d}{2}\right) \leq \frac{f(c)+f(d)}{2}$$

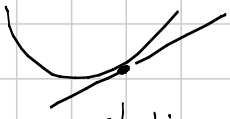
lemma midpoint-convex + continua $\longrightarrow$ convessa.

$f \in C^1([a,b])$, $f'(x)$ è una f. deb cresc $\longrightarrow$ f è convessa

$f \in C^2([a,b])$, $f''(x) \geq 0$ $\longrightarrow$ f è convessa



al di sotto delle secanti



al di sopra delle tangenti

Disug di Karamata (Hardy-Littlewood)

$(a_1, \dots, a_k) \gg (b_1, \dots, b_k)$ di numeri reali ≥ 0 debolmente decrescenti

$$\begin{cases} a_1 \geq b_1 \\ a_1 + a_2 \geq b_1 + b_2 \\ \dots \\ a_1 + \dots + a_{n-1} \geq b_1 + \dots + b_{n-1} \\ a_1 + \dots + a_n = b_1 + \dots + b_n \end{cases}$$

$\forall f$ convessa vale ($f \in C^1$)

$$\sum_{i=1}^{k} f(a_i) \geq \sum_{i=1}^{k} f(b_i)$$

$$\gamma_f(a,b) = \frac{f(b)-f(a)}{b-a} \qquad \gamma_f(a,a) = f'(a) \qquad c_i = \gamma_f(a_i, b_i)$$

$$A_i = \sum_{j=1}^{i} a_j \qquad B_i = \sum_{j=1}^{i} b_i$$

$$\begin{aligned} \sum_{i=1}^{k} (f(a_i) - f(b_i)) &= \sum_{i=1}^{k} c_i (a_i - b_i) \\ &= \sum_{i=1}^{k} c_i (A_i - A_{i-1} - B_i + B_{i-1}) \\ &= \sum_{i=1}^{k-1} \underbrace{(c_i - c_{i+1})}_{\geq 0} \underbrace{(A_i - B_i)}_{\geq 0} \end{aligned}$$

$$c_i = \delta_f(a_i, b_i) \geq \delta_f(b_i, a_{i+1}) \geq \delta_f(b_{i+1}, a_{i+1}) = c_{i+1}$$

Disug di Cauchy - Schwarz

$$\left(\sum_{j=1}^{k} a_j b_j\right)^2 \leq \left(\sum_{j=1}^{k} a_j^2\right)\left(\sum_{j=1}^{k} b_j^2\right)$$

$$p(x) = \sum_{j=1}^{k} (a_j x + b_j)^2 \geq 0 \quad \text{allora} \quad \Delta p \leq 0.$$

$v, w \in \mathbb{R}^k \qquad \|v - w\|^2 \geq 0$

$$\|v\|^2 + \|w\|^2 - 2\langle v, w\rangle \geq 0$$

$$\langle v, w\rangle \leq \frac{1}{2}\left(\|v\|^2 + \|w\|^2\right)$$

Trick: amplificazione o interpolazione

$$\forall \lambda \in \mathbb{R}_0^+ \qquad \langle v, w\rangle \leq \frac{1}{2}\left(\frac{1}{\lambda^2}\|v\|^2 + \lambda^2\|w\|^2\right)$$

$$\lambda^2 = \|v\| / \|w\|$$

$$\langle v, w\rangle \leq \|v\| \cdot \|w\| \qquad \text{C.S.}$$

Disug. di riarrangiamento

$(a_1, \dots, a_k)$ $(b_1, \dots, b_k)$ seq. deb. cresc. di num. real ≥ 0

allora $\forall \sigma \in S_k$ vale $\sum_{j=1}^{k} a_j b_j \geq \sum_{j=1}^{k} a_j b_{\sigma(j)} \geq \sum_{j=1}^{k} a_j b_{k+1-j}$

$=$ $\uparrow$

struttura di S_k + induzione

$\sigma_1 = (n_1\ n_2)\,\sigma_2$ $\square$

Disug di Chebyshev

$(a_1, \dots, a_k)$ $(b_1, \dots, b_k)$ non decrescenti di num. real ≥ 0

Allora $k \cdot \sum_{j=1}^{k} a_k b_k \geq \left(\sum_{j=1}^{k} a_j\right)\left(\sum_{j=1}^{k} b_j\right)$

$\sigma \in S_k$ della forma $\sigma = (1\ 2\ \dots\ k)$, σ^2, $\vdots$, $\sigma^k = Id$ } sommare k dove di riarrangiamento.

$$T[a_1, \dots, a_k] = \sum_{\sigma \in S_k} x_{\sigma(1)}^{a_1} \cdot x_{\sigma(2)}^{a_2} \cdot \dots \cdot x_{\sigma(k)}^{a_k} = \sum_{sym} \prod_{j=1}^{k} x_j^{a_j}$$

Schur

$\forall a, b \in \mathbb{R}^+ \quad T[a+2b, 0, 0] + T[a, b, b] \geq 2 \cdot T[a+b, b, 0]$

Muirhead / Bunching / Riarrang. gen.

$(a_1, \dots, a_k)$ $(b_1, \dots, b_k)$ sono seq. deb decrescenti per cui $a \gg b$

Allora $T[a_1, \dots, a_k] \geq T[b_1, \dots, b_k]$

$$\sum_{sym} b^2 c^2 \geq \sum_{sym} ab c^2$$

$(2,2,0) \gg (2,1,1)$

$(a_1, \dots a_j, a_{j+1}, \dots, a_k)$ vs $(a_1, \dots, a_j - \rho, a_{j+1}, \dots, a_s + \rho, a_{s+1}, \dots, a_k)$

$\gg$

$x_1, \dots, x_k \geq 0$ allora $\frac{1}{k} \sum_{j=1}^{k} x_j \geq \left(\prod_{j=1}^{k} x_j \right)^{1/k}$

AM – GM

Hint: $\log x$ è concavo per $x \geq 0$ } applico Jensen e ottengo:

$\frac{d}{dx} \log x = \frac{1}{x} \quad \frac{d^2}{dx^2} \log x = -\frac{1}{x^2} \leq 0$

$$\log\left(\frac{1}{k}\sum_{j=1}^{k} x_j\right) \geq \frac{1}{k}\sum_{j=1}^{k}\log(x_j)$$

$$\frac{1}{k}\sum_{j=1}^{k} x_j \geq e^{\frac{1}{k}\sum_{j=1}^{k}\log(x_j)} = \left(\prod_{j=1}^{k} x_j\right)^{1/k}$$

Se $m_1 > m_2$

$$\left(\frac{1}{k}\sum_{j=1}^{k} x_j^{m_1}\right)^{1/m_1} \geq \left(\frac{1}{k}\sum_{j=1}^{k} x_j^{m_2}\right)^{1/m_2}$$

$y_j = x_j^{1/m_2}$

$$\forall t > 1 \quad \left(\frac{1}{k}\sum_{j=1}^{k} y_j^t\right)^{1/t} \geq \frac{1}{k}\sum_{j=1}^{k} y_j$$

per omogeneità, non è restrittivo supporre

$$\sum_{j=1}^{k} x_j = k$$

$z_i = y_i - 1$

$$\sum_{j=1}^{k} (1+z_j)^t \geq k$$

V/ Bernoulli

$$\sum_{j=1}^{k}(1 + t z_j)$$

$$\lim_{t\to 0}\left(\sum_{j=1}^{k} a_j^t\right)^{1/t} = \left(\prod_{j=1}^{k} a_j\right)^{1/k}.$$

$(x_1, \dots, x_n)$ n-uple di num. reali ≥ 0

$$a_k = \binom{n}{k}^{-1} [t^{n-k}] \prod_{j=1}^{n}(t + x_j)$$

$$a_2 = \frac{x_1x_2 + x_1x_3 + x_2x_3}{3}$$

Disug. Newton-McLaurin

Valgono (1) $a_{k-1}\, a_{k+1} \leq a_k^2$

2) $a_k^{1/k} \geq a_{k+1}^{1/(k+1)}$

$$P(x,y) = \prod_{j=1}^{n} (x + y \cdot x_j)$$

i valori di $\frac{x}{y}$ per cui P si annulla sono tutti reali positivi

$$\Delta\left(\frac{\partial^{n-2}}{(\partial x)^{n-2}} P(x)\right) \geq 0.$$

$a_0 = 1$ $\quad (a_0 a_2)(a_1 a_3)^2 \cdot \ldots \cdot (a_{k-1} a_{k+1})^k$

$\leq \quad a_1^2 \cdot a_2^4 \cdot \ldots \cdot a_k^{2k}$

$a_{k+1}^k \leq a_k^{k+1} \quad \Rightarrow$ 2).

Disug di Young $\quad p > 1 \quad \frac{1}{p} + \frac{1}{q} = 1$

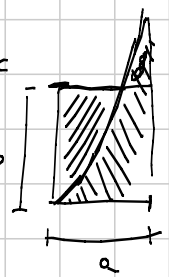
q è detto esponente coniugato di p

$$|ab| \leq \frac{|a|^p}{p} + \frac{|b|^q}{q}.$$

$f(x) = x^{p-1} \qquad g(x) = x^{\frac{1}{p-1}} = x^{q-1}$

f, g sono funz cresc

$$\int_0^{|a|} x^{p-1}\, dx + \int_0^{|b|} x^{q-1}\, dx \geq |ab|$$



Hölder $\quad p > 1 \quad \frac{1}{p} + \frac{1}{q} = 1$

$$\sum_{j=1}^{k} |x_j y_j| \leq \left(\sum_{j=1}^{k} |x_j|^p\right)^{1/p} \cdot \left(\sum_{j=1}^{k} |x_j|^q\right)^{1/q}$$

$$\|x\|_p = \left(\sum_{j=1}^{k} |x_j|^p\right)^{1/p}$$

$$\frac{\sum_k |x_k||y_k|}{\|x\|_p \, \|y\|_q} \leq \frac{1}{p} \underbrace{\sum_k \frac{|x_k|^p}{\|x\|_p^p}}_{=1} + \frac{1}{q} \underbrace{\sum_k \frac{|y_k|^q}{\|y\|_q^q}}_{=1} = \frac{1}{p} + \frac{1}{q} = 1$$

Minkowski

$$\left(\sum_{j=1}^{k} |x_j + y_j|^p\right)^{1/p} \leq \left(\sum_{j=1}^{k} |x_j|^p\right)^{1/p} + \left(\sum_{j=1}^{k} |y_j|^p\right)^{1/p}$$

$$\|A + B\| \leq \|A\| + \|B\|$$

$$\|x+y\|_p^p \leq \sum_{j=1}^{k} |x_j| \cdot |x_j + y_j|^{p-1} + \sum_{j=1}^{k} |y_j| \cdot |x_j + y_j|^{p-1}$$

Hölder

$$\leq \left(\|x\|_p + \|y\|_p\right)\left(\|x+y\|_p^{p-1}\right)$$

---

1) $(a,b,c) \geq 0 \implies \frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} \geq \frac{3}{2}$ (Nesbitt)

2) $\prod_{j=1}^{n} (|x_j| + |y_j|)^{1/n} \geq \prod_{j=1}^{n} |x_j|^{1/n} + \prod_{j=1}^{n} |y_j|^{1/n}$ (Mehler)

3) $(a,b,c) \geq 0 \quad a+b+c=3$

Allora $\sum_{cyc} \frac{1}{a^2} \geq \sum_{cyc} a^2$

4) $x_0 > 0$
$x_{k+1} = x_k^2 + x_k \qquad \forall n \in \mathbb{N} \quad \sum_{j=1}^{n} \frac{1}{x_j + 1} \leq \frac{1}{x_1}.$

1) $A = b+c$, $B = a+c$, $C = a+b$, $a = \frac{1}{2}(B+C-A)$

$$\sum_{cyc} \frac{a}{b+c} = \sum_{cyc} \frac{1}{2} \frac{B+C-A}{A} = -\frac{3}{2} + \sum_{cyc} \frac{B+C}{2A} \geq \frac{3}{2}.$$

$x \geq 0$, $x + \frac{1}{x} \geq 2$, $\frac{A}{B} + \frac{B}{A} \geq 2$, $\sum_{cyc} \frac{B+C}{2A} \geq 3$

2) AM-GM

$$\prod_{k=1}^{n} \left(\frac{|x_k|}{|x_k|+|y_k|} \right)^{1/n} \leq \frac{1}{n} \sum_{k=1}^{n} \frac{|x_k|}{|x_k|+|y_k|}$$

$$\prod_{k=1}^{n} \left(\frac{|y_k|}{|x_k|+|y_k|} \right)^{1/n} \leq \frac{1}{n} \sum_{k=1}^{n} \frac{|y_k|}{|x_k|+|y_k|}$$

$$\frac{1}{n} \sum_{k=1}^{n} \frac{|x_k|+|y_k|}{|x_k|+|y_k|} = 1$$

4) $x_0 > 0$, $x_k > 0 \ \forall k$

Dec. in fratti semplici (Dec. di Hurwitz)

$$x_{k+1} = x_k^2 + x_k \qquad \frac{1}{x_{k+1}} = \frac{1}{x_k^2 + x_k} = \frac{1}{x_k(x_k+1)} = \frac{1}{x_k} - \frac{1}{x_k+1}$$

$$\frac{1}{x_k+1} = \frac{1}{x_k} - \frac{1}{x_{k+1}}$$

$$\sum_{k=1}^{n} \frac{1}{x_k+1} = \sum_{k=1}^{n} \frac{1}{x_k} - \sum_{k=1}^{n} \frac{1}{x_{k+1}}$$

$x_{n+1} \geq 0$

$$\sum_{k=1}^{n} \frac{1}{x_k} - \sum_{k=2}^{n+1} \frac{1}{x_k} = \frac{1}{x_1} - \frac{1}{x_{n+1}} \leq \frac{1}{x_1}.$$

3) $a+b+c = 3$, $a, b, c \geq 0$

$$\sum_{cyc} \frac{1}{a^2} \geq \sum_{cyc} a^2$$

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

$$0 = f\left(\frac{a+b+c}{3}\right) \leq \frac{f(a)+f(b)+f(c)}{3}$$

$f''(x) = \frac{6}{x^4} - 2$ $\quad f$ è convessa su $(0, 3^{1/4})$

$$\sum_{cyc}\left(\frac{1}{a^2} - a^2\right) = \sum_{cyc} \frac{(1-a)(1+a)(1+a^2)}{a^2} \geq 0$$

$$\sum_{cyc} \frac{(1+a)(1+a^2)}{a^2} \geq \sum_{cyc} \frac{(1+a)(1+a^2)}{a}$$

$$\sum_{cyc} (1+a)(1+a^2)b^2c^2 \geq \sum_{cyc} (1+a)(1+a^2)ab^2c^2$$

$$(a+b+c)\sum_{cyc} (1+a)(1+a^2)b^2c^2 \geq 3\sum_{cyc} (1+a)(1+a^4)ab^2c^2$$

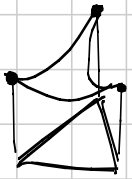
$(-)\ b^3c^2 + b^2c^3 \qquad (-)\ 2\,ab^2c^4$

$(3\,2\,0) >> (2\,2\,1)$

per bunching, fine.

Remark 1. Studiare i casi in cui vale $=$ per tutte le disug. esposte finora

Remark 2. f convessa su un chiuso ammette massimo al bordo



Remark 3. Se i punti critici di una disug sono molteplici e giacciono nella parte interna del dominio di definizione, le tecniche qui mostrate, da sole, sono insufficienti.

SENIOR 2011 – A3 MEDIUM

Titolo nota 09/09/2011

Successioni, eq. funzionali

Ricorrenze lineari: (comogenea)

$$a_{n+1} = c \cdot a_n \Rightarrow a_n = c^n \cdot a_0$$

$$a_{n+1} = c \cdot a_n + d \quad \text{(succ. perturbata)}$$

$$b_n = a_n + \beta$$

$$b_{n+1} = a_{n+1} + \beta \overset{a_{n+1} = c\cdot a_n + d}{=} c \cdot a_n + d + \beta = c \cdot b_n \underbrace{- c\beta + d + \beta}_{=0}$$

$$b_{n+1} = c \cdot b_n \qquad a_n = b_n - \beta$$

$$-c\cdot\beta + d + \beta = 0 \rightsquigarrow \beta = \frac{d}{c-1}$$

Ora sappiamo che $b_n = c^n \cdot b_0$, ma allora

$$a_n = b_n - \beta = c^n \cdot b_0 - \frac{d}{c-1}$$

Per sapere chi è b_0, utilizziamo la condizione iniziale

Metodo alternativo:

$$a_{n+1} = c \cdot a_n + d$$

$$a_1 = c \cdot a_0 + d$$

$$a_2 = c \cdot a_1 + d = c^2 \cdot a_0 + c \cdot d + d$$

$$a_3 = c \cdot a_2 + d = c^3 \cdot a_0 + c^2 \cdot d + c \cdot d + d$$

$$\vdots$$

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

Ovviamente la formula è da dimostrare per induzione →

$$a_n = c^n \cdot a_0 + d \frac{c^n - 1}{c - 1} .$$

$$\boxed{a_{n+1} = c \cdot a_n} .$$

Prendiamo la classe di tutte le soluzioni di questa successione per ricorrenza.

1) Se a_n è soluzione e b_n è soluzione, anche $a_n + b_n$ è soluzione;

2) Se a_n è soluzione, anche $\lambda \cdot a_n$ è soluzione $(\lambda \in \mathbb{R})$.

o —— o —— o —— o

$$a_{n+1} = c \cdot a_n + \text{Mostro}(n)$$

Che proprietà sono verificate dall'insieme delle soluzioni di questa?

Se a_n è sol. e b_n anche, cosa posso dire di $a_n + b_n$?

$$a_{n+1} = c \cdot a_n + \text{Mostro}(n)$$
$$b_{n+1} = c \cdot b_n + \text{Mostro}(n)$$
$$a_{n+1} + b_{n+1} = c \cdot (a_n + b_n) + 2 \cdot \text{Mostro}(n)$$

Non va bene ...

E per la differenza?

$$(a_{n+1} - b_{n+1}) = c \cdot (a_n - b_n)$$

Soluzione generale con Mostro = Sol. generale dell'omogenea + Sol. speciale con Mostro

$$a_{n+1} = c \cdot a_n + d$$

Vogliamo trovare tutte le soluzioni di questa. L'omogenea la sappiamo risolvere, ci basta trovare UNA soluzione particolare.
Proviamo a cercarla $a_n \equiv \alpha$. Cosa deve valere?

$$\alpha = c \cdot \alpha + d$$

$$\rightsquigarrow \quad \alpha = -\frac{d}{c-1}$$

Quindi la soluzione generale è:

$$a_n = -\frac{d}{c-1} + c^n \cdot k$$

dove k si deve trovare con le condizioni iniziali.

Proviamo a risolvere $a_{n+1} = 3a_n + n$

$a_n = \alpha n + \beta$

$\alpha(n+1) + \beta = 3(\alpha \cdot n + \beta) + n$

$\alpha n + \alpha + \beta = 3\alpha n + 3\beta + n$

$(2\alpha + 1)n + 2\beta - \alpha = 0$

$\downarrow$

$2\alpha + 1 = 0 \qquad 2\beta = \alpha \quad \Rightarrow \quad \alpha = -\frac{1}{2}, \ \beta = -\frac{1}{4}$

$$a_n = -\frac{1}{2}n - \frac{1}{4} + 3^n \cdot l$$

Esempio 3. $a_{n+1} = 5a_n - 6a_{n-1} + \boxed{3n^2}$ Monico (n)

$a_n = \alpha n^2 + \beta n + \gamma$

$-3n^2 + \alpha(n+1)^2 + \beta(n+1) + \gamma = 5(\alpha n^2 + \beta n + \gamma) - 6(\alpha(n-1)^2 + \beta(n-1) + \gamma)$

Facciamo i conti e troviamo α, β, γ

$$a_n = \alpha n^2 + \beta n + \gamma + l_1 \cdot 2^n + l_2 \cdot 3^n$$

$x^2 - 5x + 6 = (x-2)(x-3)$

Piccola digressione: Consideriamo l'insieme delle successioni che verificano

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

è chiuso per somma e moltiplicazione per numeri $\alpha \in \mathbb{R}$, quindi se abbiamo a_n che soddisfa e b_n che soddisfa, allora

$$c_n = \alpha \cdot a_n + \beta \cdot b_n$$

Supponiamo di voler risolvere

$$\begin{cases} a_{n+2} = 5a_{n+1} - 6a_n \\ a_0 = 0 = \alpha \cdot a_0 + \beta \cdot b_0 \\ a_1 = 1 = \alpha \cdot a_1 + \beta \cdot b_1 \end{cases} \rightsquigarrow$$

ha sol. ! $a_0 \cdot b_1 - b_0 \cdot a_1 \neq 0$

Sapendo questo cerchiamo succ. della forma $a_n = \rho^n$

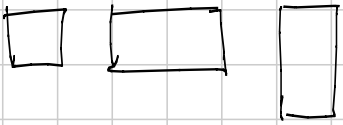
$$x^2 = 5x - 6$$

nel caso l'equazione avesse radici doppie, consideriamo $a_n = \rho^n$, $b_n = n\rho^n$.

Ovviamente tutto questo vale anche per le ricorrenze con K termini.

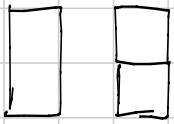
Esempio K.

rettangolo $2 \times n$, da tassellare con mattonelle 1×1 o 2×1

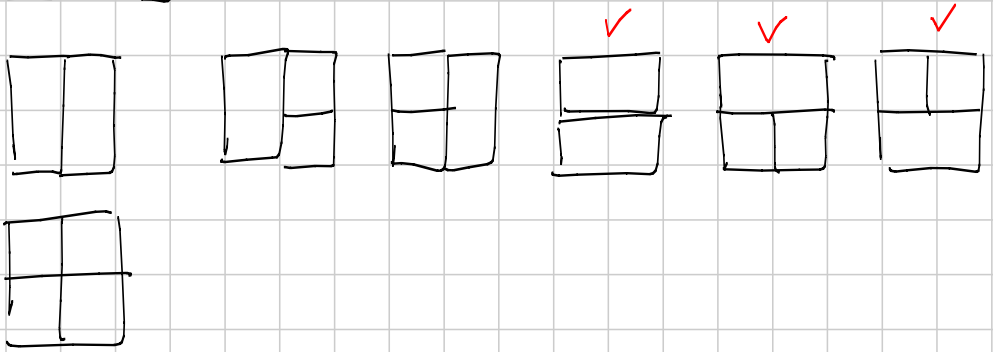


a_n

$n = 1$



$n = 2$



$(a_0 = 1)$

$a_1 = 2$ $\quad a_2 = 7$

Come posso fare $2 \times n$. Guardo cosa succede a destra. Cerco il punto più vicino dove non taglio nessuna mattonella.

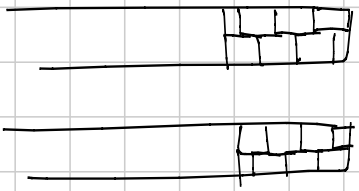
$$a_n = 2 \cdot a_{n-1} + 3 \cdot a_{n-2} + 2 \cdot a_{n-3} + 2 \cdot a_{n-4} + \dots 2 a_1$$

$2 \cdot a_{n-1}$: se posso tagliare alla prima colonna

$3 \cdot a_{n-2}$: se posso tagliare alla 2ª colonna

posi. a destra nel caso taglio alla 1ª colonna: 3

Da 3ª colonna in poi l'unica è:



Quindi 2 possibilità per la parte a dx

$$a_n = 2a_{n-1} + 3a_{n-2} + 2a_{n-3} + \dots + 2\cdot a_1 + 2\cdot a_0$$

$$a_{n-1} = 2\cdot a_{n-2} + 3a_{n-3} + 2a_{n-4} + \dots + 2a_0$$

Sottraggo:

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

$$a_n = 3a_{n-1} + a_{n-2} - a_{n-3}. \quad \text{Ok bene!}$$

$$A_n = a_0 + a_1 + \dots + a_n$$

$$\begin{cases} a_{n+1} = 2\cdot A_n + a_{n-1} \\ A_{n+1} = a_{n+1} + A_n \end{cases} \qquad A_n = \frac{a_{n+1} - a_{n-1}}{2}$$

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

- $a_{n+1} = a_n + \underbrace{a_{n-1} + \dots + a_0}_{= a_n}$.
- $a_{n+1} = n a_n + \underbrace{(n-1) a_{n-1} + \dots + 2a_2 + a_1}_{= a_n}$.
- $a_{n+1} = a_n + 2 \cdot a_{n-1} + \dots + (n-1)a_2 + n a_1$
- $a_{n+1} = a_n + a_n = 2 \cdot a_n = 2^n \cdot \alpha$

- $a_{n+1} = (n+1)\, a_n = (n+1)! \cdot \alpha$

— o — o — o —

$a_{n+1} = a_n + a_{n-1} + \text{Mostro}(n)$

Mostro = polinomio [ok] sol. particolare: polinomio dello stesso grado

= esponenziale [ok] esponenziale con la stessa base, con un coeff. davanti

$7^n \rightsquigarrow \alpha \cdot 7^n$ ⚠*

= polinomio + esp. [ok] pol. + esp.

= pol. · esp. [ok] pol. · esp.

= log(n)

* Attenzione, se 7 è rad. del polinomio caratteristico allora provare $\alpha \cdot n \cdot 7^n$ come sol. part.

$\alpha \cdot 7^{n+2} = \alpha \cdot 7^{n+1} + \alpha \cdot 7^n + 7^n$

$\alpha 7^2 = \alpha 7 + \alpha + 1$

$$a_{n+1} = c \cdot a_n + \log(n)$$

$$a_n = \log(n) + c\log(n-1) + c^2\log(n-2)$$

$$= \log\left(n \cdot (n-1)^c (n-2)^{c^2} \cdots \cdot 2^{c^{n-1}}\right)$$

logaritmi, purtroppo, no!

$$\text{Mostro}(n) = \sin(n\theta) = \frac{e^{in\theta} - e^{-in\theta}}{i} = \frac{\rho_1^n - \rho_2^n}{i}$$

$$\rho_1 = e^{i\theta} = \cos\theta + i\sin\theta$$

$$\rho_2 = e^{-i\theta} = \cos\theta - i\sin\theta$$

Funzioni trigonometriche sì, se della forma

$$\sin(n\theta + \varphi), \cos(n\theta + \xi)$$

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

— $a_{n+1} = 2a_n^2 - 1$ ← mi ricorda la formula di duplicazione del coseno

$$a_0 = \cos\theta$$

$$\Rightarrow a_1 = \cos(2\theta), \quad a_2 = \cos(4\theta)$$

$$\cdots \quad a_n = \cos(2^n\theta)$$

$a_0 = 2$

$a_0 = 2\cos\theta$

$a_1 = 2(2\cos\theta)^2 - 1 = 8\cos^2\theta - 1 =$

$a_0 = \dfrac{e^{i\theta} + e^{-i\theta}}{2} = \dfrac{x + \frac{1}{x}}{2}$, dove $x = e^{i\theta}$

$a_1 = 2\left(\dfrac{x+\frac{1}{x}}{2}\right)^2 - 1 = 2\dfrac{x^2+2+\frac{1}{x^2}}{4\,2} - 1 =$

$= \dfrac{x^2+\frac{1}{x^2}}{2}$

$a_1 = \dfrac{x^2+\frac{1}{x^2}}{2}$ $\quad a_2 = \dfrac{x^4+\frac{1}{x^4}}{2}$ $\quad a_3 = \dfrac{x^8+\frac{1}{x^8}}{2}$

$a_n = \dfrac{x^{2^n}+\frac{1}{x^{2^n}}}{2}$

$x \in \mathbb{R}$ $\quad a_0 = \dfrac{x+\frac{1}{x}}{2}$ che valori potrà assumere?

$\dfrac{x+\frac{1}{x}}{2} \geq \sqrt{x\cdot\frac{1}{x}} = 1$ se $x = 1$

Con rag. di cont. dico che riesco a prendere tutti i num. reali ≥ 1, e anche quelli ≤ -1.

$$a_n = \left\lfloor (\sqrt{5}+2)^n \right\rfloor$$

$$\underbrace{(\sqrt{5}+2)^n}_{A\sqrt{5}+B} + \underbrace{(2-\sqrt{5})^n}_{-A\sqrt{5}+B} = 2B \in 2\mathbb{N}$$

$$-1 < 2-\sqrt{5} < 0 \qquad |2-\sqrt{5}| < 1$$

$$b_n = (\sqrt{5}+2)^n + (2-\sqrt{5})^n = \begin{cases} a_n & \text{se } n \text{ è dispari} \\ a_n+1 & \text{se } n \text{ è pari} \end{cases}$$

$$b_n = (\sqrt{5}+2)^n - \varepsilon = \left\lfloor (\sqrt{5}+2)^n \right\rfloor \qquad (n \text{ dispari})$$

$$b_n = (\sqrt{5}+2)^n + \varepsilon = \left\lfloor (\sqrt{5}+2)^n \right\rfloor + 1 \qquad (n \text{ pari})$$

$$x^2 - 4x - 1$$

$$\begin{cases} b_{n+1} = 4b_n + b_{n-1} \\ b_0 = 2 \\ b_1 = 4 \end{cases}$$

$$(\sqrt{2}+1)^n = a_n + \sqrt{2}\,b_n$$

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

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

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

eq. funzionali

$f : S \longrightarrow S$

$$f(x+y) = f(x) + f(y) \qquad \forall x \in S,\ \forall y \in S$$

$S = \mathbb{Q} \Rightarrow f(x) = \lambda \cdot x$ per qualche $\lambda \in \mathbb{Q}$

- $f(0) = 0$
- $f(n) = n \cdot f(1)$ (induzione) $f(x) = \lambda x$ su $\mathbb{N}$
- $f(x) = \lambda x$ su $\mathbb{Z}$
- $f(x) = \lambda x$ su $\mathbb{Q}$ (induzione e $f(mx) = m f(x)$; $x = \frac{p}{m}$)

Non possiamo andare oltre $S = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

$$f(a + \sqrt{2} b) = \begin{cases} b + \sqrt{2}\, a \\ a \\ b \\ a + b \end{cases} \qquad \forall\ a, b \in \mathbb{Q}$$

f lineare $\Rightarrow$ $f(a + \sqrt{2} b) = \lambda a + \lambda \sqrt{2} b \quad \forall a, b \in \mathbb{Q}$

$$f(a + \sqrt{2} b) = a f(1) + b f(\sqrt{2}).$$

Quindi ci sono sol. dell'eq. di Cauchy brutte quanto voglio, in particolare il grafico è denso in $\mathbb{R}^2$, cioè preso un qualunque cerchietto in $\mathbb{R}^2$, esso conterrà almeno 1 punto del grafico.

Vorrei fare un esempio di $f:\mathbb{R}\to\mathbb{R}$ che soddisfi l'eq. di Cauchy ma non sia lineare.

BASI DI HAMEL Un sottoinsieme $B \subseteq \mathbb{R}$ è detto base di Hamel se soddisfa le seguenti 2 proprietà:

① per ogni $r\in\mathbb{R}$, esistono un num. finito di $b_1, b_2, \dots, b_k \in B$ e $q_1, q_2, \dots, q_k \in \mathbb{Q}$ t.c.

$$r = q_1 b_1 + q_2 b_2 + \dots + q_k b_k$$

② se ho $\{b_1, \dots, b_k\} \subseteq B$ $q_1, q_2 \dots, q_k \in \mathbb{Q}$ t.c.

$$q_1 b_1 + q_2 b_2 + \dots + q_k b_k = 0$$

$$\Rightarrow \quad q_1 = q_2 = \dots = q_k = 0$$

Sappiamo subito dalla ②+① che ogni numero reale ha una e una sola rappr. con la base di Hamel.

Avendo una base di Hamel possiamo costruire un controesempio alla Cauchy

$$f(r) = f(q_1 b_1 + q_2 b_2 + \dots + q_k b_k) =$$
$$= q_1 f(b_1) + q_2 f(b_2) + \dots + q_k f(b_k)$$

Per costruire una f che soddisfi Cauchy, mi basta fissare i valori sulla base di Hamel.

$f(b_1) = b_2$, $f(b_2) = b_1$ e $f(b_i) = b_i$ $\forall i \geq 3$

$f(\alpha_1 b_1 + \alpha_2 b_2 + \text{roba}) = \alpha_1 b_2 + \alpha_2 b_1 + \text{roba}$

- $f(x + 3f(y)) = ay + f(x)$

[$a = 0$ $f \neq 0$, esiste?]

1. $x = 0$ $\quad f(3f(y)) = ay + f(0)$ $\quad a \neq 0$ $\quad f$ iniettiva e surgettiva
2. x_0 t.c. $f(x_0) = 0$ $\quad y = x_0$ in $\uparrow$

$$f(0) = a x_0 + f(0) \qquad x_0 = 0$$

3. back to 1 : $\quad f(3f(y)) = ay$
4. poiché f è surjettiva anche $3f$ lo è e quindi $\forall z$ posso trovare y t.c. $3f(y) = z$

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

$\rightsquigarrow$ $f(x) = \lambda x$ per $x \in \mathbb{Q}$

Sostituendo trovo $\lambda^2 \cdot 3 = a$ $\rightsquigarrow$ $a \geq 0$

per a negativi non ci sono soluzioni

$f(x) = \lambda x$ per $x \in \alpha\mathbb{Q}$

fisso la base di Hamel:

so che $f(b_i) = \pm \lambda_0 b_i$ $\quad \lambda_0^2 \cdot 3 = a$

$$f(x + 3f(y)) = ay + f(x)$$

Se $\frac{a}{3} \in \mathbb{Q}^2$, ho soluzioni non banali, altrimenti

boh!

5 $a = 0$ $\quad f(x + 3f(y)) = f(x)$

base di Hamel $= b_1, b_2, \ldots$

$f(b_i) = b_1$ per ogni $i > 1$

$f(b_1) = 0$

$k \in \mathbb{Q}$

$$f(x + 3f(y)) = f(x + 3\underset{\downarrow}{k} \cdot b_1) = f(x) + 3kf(b_1) = f(x)$$

– 1 sugli interi e 0 altrove, funziona anche

– $f(x) = \begin{cases} 1 & \text{se } \lfloor x \rfloor \equiv 1 \quad (3) \\ 2 & \equiv 2 \quad (3) \\ 0 & \equiv 0 \quad (3) \end{cases}$

———— o ————

con $a > 0$

$1 \quad \lambda_0 \quad \lambda_0^2 \quad \lambda_0^3 \quad \cdots \quad \lambda_0^n \quad \cdots$

$\alpha \quad \lambda_0\alpha \quad \lambda_0^2\alpha \quad \cdots \quad \cdots$

Se fosse stato $\lambda_0 = \sqrt{2}$, allora prendo la base di Hamel di $\mathbb{R}$ su $\mathbb{Q}(\sqrt{2})$ $= \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$.

Quando possiamo affermare che $f: \mathbb{R} \to \mathbb{R}$ che sodd. Cauchy è lineare?

- monotonia;
- locale limitatezza;
- continuità in un punto;
- un qualsiasi cerchietto in $\mathbb{R}^2$ è privo di punti del grafico di f.

→ breve sketch di dimostrazione: loc. lim. in 0

wlog che $f(1)=0 \quad f(x) - xf(1) = g(x)$

$g(1) = g(0) = 0 \rightsquigarrow g(\mathbb{Q}) = 0$

prendiamo un η t.c. $g(\eta) > 0$.

Supponiamo per assurdo che $|g(x)| \leq M \quad \forall\, |x| \leq \varepsilon$

Prendo n t.c. $g(n\eta) = n\, g(\eta) > M$

Ora so che $\exists\, q \in \mathbb{Q}$ t.c. $|n\eta - q| \leq \varepsilon$

$\rightsquigarrow g(n\eta - q) = g(n\eta) - g(q) > M$

contraddicendo l'ipotesi ($|nq - q| < \varepsilon$).

IMO 1992 – 2

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

① $x = 0$ $\quad f(f(y)) = y + f(0)^2$ $\quad$ f in. e su.

② $y = x_0$ $\quad f(0) = x_0 + f(0)^2$

$f(x_0) = 0$

$x = x_0 \quad f(x_0^2 + f(y)) = y$

$x = -x_0 \quad f(x_0^2 + f(y)) = y + [f(-x_0)]^2$

$\rightsquigarrow f(-x_0) = 0$

$-x_0 = x_0 \Rightarrow x_0 = 0$

③ back to ① $\quad f(f(y)) = y \quad \forall \ y \in \mathbb{R}$

④ $y = 0 \quad f(x^2) = f(x)^2$

⑤ $y = f(z) \quad f(x^2 + f(f(z))) = f(z) + f(x)^2$

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

Questa è Cauchy, chiamando $x^2 = y$

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

$\rightsquigarrow f(x) = \lambda x$ per $\lambda \in \mathbb{Q}$

ci dice $\lambda = \pm 1$

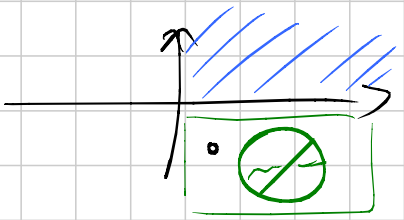
⑥ $f(x^2+z) = f(z) + f(x)^2$

$f(z + \text{qualcosa di positivo}) = f(z) + \text{qualcosa di positivo}$

$w \geq z \qquad x = \sqrt{w-z}$

$f(w) = f(z) + f(\sqrt{w-z})^2 \geq f(z)$

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



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

① $x=0 \quad f(f(y)) = y + f(0)^2 \qquad f$ in surg.

② $x=x_0 \quad f(f(y)) = y + 0^2 \qquad f(0)=0$

③ $f(f(y)) = y$

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

$x = f(z) \qquad f(f(z)f(f(z))) = [f(f(z))]^2 = z^2$

$f(z \overset{\parallel}{f}(z)) = [f(z)]^2$

$f(z)^2 = z^2 \qquad \forall z \in \mathbb{R}$

$f(x) = \pm x \qquad \forall x \in \mathbb{R}$

Dobbiamo controllare il MISTONE.

$f(a) = a \qquad f(b) = -b \qquad a, b \neq 0$

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

$a^2 - b$ $\quad$ $b - a^2$

$b = 0$ $\quad$ $a = 0$

Non va bene, il mistone non ha colpito!

Bmo '07 - 2 $\quad f(f(x) + y) = f(f(x) - y) + 4f(x) \cdot y$

$y = f(x)$

$f(2 \cdot f(x)) = f(0) + 4f(x)^2 \qquad z = 2f(x)$

$f(z) = f(0) + z^2 \qquad z \in 2\,\mathrm{Im}(f)$

$y = f(x) - 2f(z)$ ← è per fare in modo da

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

e quindi io la posso calcolare

$f(2(f(x) - f(z))) = f(0) + 4f(z)^2 + 4f(x)(f(x) - 2f(z))$

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

$f(z) = f(0) + z^2 \qquad z \in 2(\mathrm{Im}f - \mathrm{Im}f)$

$f(\text{qualcosa}) = f(\text{qualcos'altro}) + 4f(x)\cdot z$

$f(\quad) - f(\quad) = 4f(x)\cdot z$

fisso $f(x) \neq 0$, ottengo che in effetti ($f \equiv 0$ soluzione?) $\mathrm{Im}f - \mathrm{Im}f = \mathbb{R}$

$\mathrm{Im}f - \mathrm{Im}f = \mathbb{R}$ vuol dire che, preso un qualsiasi $c \in \mathbb{R}$, so trovare $\alpha, \beta \in \mathbb{R}$ t.c. $f(\alpha) - f(\beta) = c$.

$f(x) \neq 0$

$\forall\ c$ scelgo z t.c. $4f(x)\cdot z = c$

$\Rightarrow \quad z = \dfrac{c}{4f(x)}$

$f\left(x + f(z)\right) - f\left(x - f(z)\right) = 4zf(x)$

$f\left(x + f\left(\frac{c}{4f(x)}\right)\right) - f\left(x - f\left(\frac{c}{4f(x)}\right)\right) = c$

$\alpha = x + f\left(\frac{c}{4f(x)}\right) \qquad \beta = x - f\left(\frac{c}{4f(x)}\right)$

$f(\alpha) - f(\beta) = c.$

C1 Medium - dario2994 (generatrici)

Titolo nota 06/09/2011

$a_0, a_1, a_2, \dots \in \mathbb{C}$

$a_0 + a_1 x + a_2 x^2 + \dots = \sum_{i=0}^{\infty} a_i x^i = \text{ogf}(a_i)$

$\text{ogf}(a_i) \quad \text{ogf}(b_i)$

$\text{ogf}(a_i) + \text{ogf}(b_i) := \text{ogf}(a_i + b_i)$

$\text{ogf}(1) = 1 + x + x^2 + \dots$

$\text{ogf}(i) = 0 + x + 2x^2 + 3x^3 + \dots$

$\text{ogf}(i+1) = 1 + 2x + 3x^2 + 4x^3 + \dots$

$\text{ogf}(a_i) \cdot \text{ogf}(b_i) := \text{ogf}\left(\sum_{j=0}^{i} a_j b_{i-j}\right)$

$(1 + 2x + 3x^2 + 4x^3)(3 + 2x + x^2 + 2x^3) = \dots x^2(1+1+4+\dots)$

$\text{ogf}(1) \cdot \text{ogf}(1) = (1 + x + x^2 + \dots)(1 + x + x^2 + \dots) = \dots x^4(1+1+1+1+\dots)$

$\text{ogf}\left(\sum_{j=0}^{i} 1 \cdot 1\right) = \text{ogf}(i+1)$

$\text{ogf}(a_i) = \text{ogf}(b_i) \iff \forall i \in \mathbb{N} \quad a_i = b_i$

$A, B, C \quad \text{ogf}(a_i, b_i, c_i)$

$A + (B + C) = (A + B) + C$

$A + B = B + A$

$AB = BA$

$A \cdot (BC) = (A \cdot B) C$

$A(B + C) = (A \cdot B) + (A \cdot C)$

$AB = 0 = \text{ogf}(0) \longrightarrow A = 0 \vee B = 0$

Data $ogf(a_i)$ $\quad \frac{1}{ogf(a_i)} = ogf(b_i) \iff ogf(a_1)ogf(b_i) = 1$

$[x^k] \sum_{i=0}^{\infty} a_i x^i = a_k$

L'inverso di $ogf(a_i)$ esiste ed è unico $\iff a_0 \neq 0$

Dim.

Caso I: $a_0 = 0 \quad ogf(b_i) \cdot ogf(a_i) = 1$

$b_0 \cdot a_0 = [x^0]\, ogf(b_1) \cdot ogf(a_1) = 1$

$b_0 = 0$

Caso II: $a_0 \neq 0$

$a_0 \cdot b_0 = 1 \to b_0 = \frac{1}{a_0}$

$b_0, b_1, \dots, b_n$ già scelti

$[x^{n+1}]\, ogf(a_i) \cdot ogf(b_i) = [x^{n+1}]\, 1 = 0$

$\sum_{j=0}^{n+1} a_j b_{n+1-j} = 0$

$-a_0 \cdot b_{n+1} = \sum_{j=1}^{n+1} a_j b_{n+1-j}$

b_{n+1} ha un valore già scelto

$b_{n+1} = -\frac{\sum_{j=1}^{n+1} a_j b_{n+1-j}}{a_0}$

$ogf(a_i) = \frac{1}{P(x)}$

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

Vale come uguaglianza tra reali per $|x| < 1$

$ogf(1)$ è una generatrice

$ogf(1)\cdot(1-x) = 1$

ho solo 0

$[x^0] = 1\cdot 1 = 1$

$[x^n](1\cdot 1) + (1\cdot(-1)) + 0 = 0$

$ogf(1) = \frac{1}{1-x}$ $\quad a_{-1} = 0$

$ogf(a_i)\cdot(1-x) = ogf(a_i - a_{i-1})$

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

$\frac{ogf(a_i)}{1-x} = ogf(a_0 + a_1 + \dots + a_i)$

$ogf(a_{i+1}) \stackrel{?}{=} a_1 + a_2 x + a_3 x^2 + \dots$

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

x

$ogf(a_{i+1}) = \frac{ogf(a_i) - a_0}{x}$

$ogf(a_{i-1}) = a_0 x + a_1 x^2 + \dots = x\, ogf(a_i)$

0

$ogf(F_i) = F(x)$.

$F_{n+2} = F_{n+1} + F_n$ $\quad F_0 = 0$, $F_1 = 1$

ci fermiamo qui un attimo.

$$\text{ogf}(F_{i+2}) = \text{ogf}(F_{i+1} + F_i) = \text{ogf}(F_{i+1}) + \text{ogf}(F_i)$$

$$\frac{F(x) - F_0 - F_1 x}{x^2} \qquad \frac{F(x) - F_0}{x} \qquad F(x)$$

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

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

$D\ \text{ogf}(a_i) := \text{ogf}((i+1)a_{i+1})$

$D\ a_0 + a_1 x + a_2 x^2 + \cdots = a_1 + 2a_2 x + 3a_3 x^2 + \cdots$

$\int \text{ogf}(a_i) := \text{ogf}\left(\frac{a_{i-1}}{i}\right)$ per $i = 0$ 0

$\int D\ \text{ogf}(a_i) = \text{ogf}(a_i)$ (a meno di $[x^0]$)

$D \int \text{ogf}(a_i) = \text{ogf}(a_i)$

$$\text{ogf}(a_i) \circ \text{ogf}(b_i) = \text{ogf}\left(\sum_{j=0}^{\infty} [x^i]\left(a_j (\text{ogf}(b_i))^j\right)\right)$$

$B(x)$

$$a_0 + a_1 B(x) + a_2 (B(x))^2 + a_3 (B(x))^3 + \cdots$$

$$\text{ogf}(k^i) = 1 + kx + k^2x^2 + k^3x^3 + \cdots = 1 + (kx) + (kx)^2 + \cdots$$

$$= \text{ogf}(1) \circ (kx) = \frac{1}{1 - kx}$$

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

α, β le radici di $1 - x - x^2$

$$F(x) = -x\left(\frac{1}{(x-\alpha)(x-\beta)}\right) = \frac{-x}{\alpha - \beta}\left(\frac{1}{x-\alpha} - \frac{1}{x-\beta}\right) =$$

$$\frac{x}{\alpha - \beta}\left(\frac{\frac{1}{\alpha}}{1 - \frac{x}{\alpha}} - \frac{\frac{1}{\beta}}{1 - \frac{x}{\beta}}\right)$$

$F_k = [x^k] F(x) = [x^{k-1}] \frac{F(x)}{x} = \frac{1}{\alpha-\beta}\left(\left(\frac{1}{\alpha}\right)\left(\frac{1}{\alpha}\right)^{k-1} - \left(\frac{1}{\beta}\right)\left(\frac{1}{\beta}\right)^{k-1}\right)$

$= \frac{\left(\frac{1}{\alpha}\right)^k - \left(\frac{1}{\beta}\right)^k}{\alpha-\beta} = \frac{\beta^k - \alpha^k}{\alpha-\beta}$

$ogf\left(\binom{n}{i}\right) = \binom{n}{0} + \binom{n}{1}x + \cdots + \binom{n}{n}x^n + 0 - - -$

$= (X+1)^n$

$1, n+1, \ldots$

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

$(1+x+x^2+\cdots)(1+x+x^2+\cdots)\cdots(1+x+x^2+\cdots)$ ($n+1$)

$\binom{k+n}{n}$ il hope

$[x^k]$ = modi di scegliere $n+1$ naturali a somme k.

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

Dato $n \in \mathbb{N}\setminus 0$ chiamo $A(n)$ il numero di $2n$-uple $(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots y_n) \in (0,1)$ t.c.:

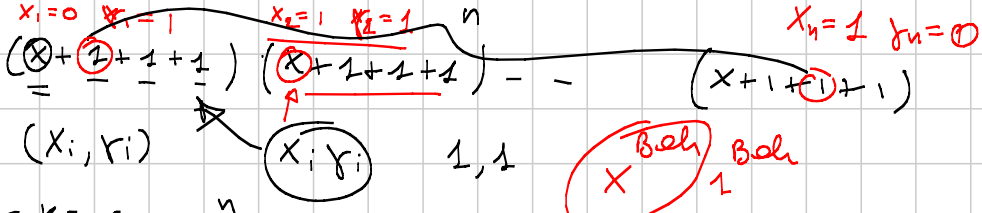
$\sum_{i=1}^{n} x_i y_i$ è pari

e $B(n)$ è dispari.

Quanto vale $\frac{A(n)}{B(n)}$?

a_k è il numero di $2n$-uple t.c. fa k.

$[x^k](x+3)^n = a_k$



$[x^k]\,(x+3)^n = a_k$

$[x^k]\,(x+3)^n = a_k$

$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$

$A(n) = a_0 + a_2 + \cdots + a_n, a_{n-1}$

$$\frac{(x+3)^n + (-x+3)^n}{2} = a_0 + a_2 x^2 + a_4 x^4 + \cdots + a_n x^n.$$

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

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

Sia $a_0, a_1, a_2 \cdots$ definita da una ricorrenza infinita:

a_0 ha il valore che vuole

$$a_{n+1} = a_0 \cdot b_n + a_1 \cdot b_{n-1} + \cdots + a_n b_0 = \sum_{j=0}^{n} a_j\, b_{n-j}.$$

$\operatorname{ogf}(a_i) = A(x)$ $\operatorname{ogf}(b_i) = B(x)$ ←

$$\operatorname{ogf}(a_{n+1}) = \operatorname{ogf}\left(\sum_{j=0}^{n} a_j\, b_{n-j}\right)$$

$$\frac{A(x) - a_0}{x} = A(x) \cdot B(x)$$

$$A(x) = \frac{a_0}{1 - xB}.$$

$a_0 = 100$

$a_{n+1} = a_0 + a_1 + \cdots + a_n$

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

$$A(x) = \frac{100}{1-\frac{x}{1-x}} = \frac{100}{\frac{1-x-x}{1-x}} = \frac{100(1-x)}{1-2x} = 100\left[\frac{1-x}{1-2x}\right]$$

$100(1-x)\,\mathrm{ogf}(2^i) = 100\cdot \mathrm{ogf}(2^i - 2^{i-1}) = \mathrm{ogf}(100(2^{i-1}))$.

$a_0, a_1, a_2, \dots, a_n$ e caso

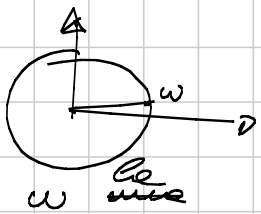
$a_{n+k+1} = b_0 a_{n+k} + b_1 a_{n+k-1} + \dots - b_k a_n \qquad \mathrm{ogf}(a_i)$

$\mathrm{ogf}(a_{n+k+1}) =$

Roots of unity filter

Sia $A(x) = \mathrm{ogf}(a_i)$. e sia p un numero primo.

$$b_i := \begin{cases} a_i & \text{se } p \mid i \\ 0 & \text{se } p \nmid i \end{cases}$$



sia ω una radice primitiva dell'unità p-esima.

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

$a_0 + a_p x^p + a_{2p} x^{2p} + \dots$

$$B(x) = \frac{\sum_{j=0}^{p-1} A(\omega^j x)}{p}$$

---

o

$$b_k \text{ uguale a } [x^k]\frac{\sum_{j=0}^{p-1} A(\omega^j x)}{p} = \frac{1}{p}\sum_{j=0}^{p-1} a_k(\omega^j)^k = a_k\left(\frac{\sum_{j=0}^{p-1}(\omega^j)^k}{p}\right)$$

Caso I: $p \mid k$ In questo caso vorre

$$\frac{\sum_{j=0}^{p-1}(\omega^j)^k}{p} = 1$$

$$\frac{1}{p}\sum_{j=0}^{p-1}(\omega^k)^j = \frac{1}{p}\sum_{j=0}^{p-1} 1 = \text{(I)}$$

Caso II: $p \nmid k$

$$\frac{\sum_{s=0}^{p-1} (\omega^s)^k}{p} = 0 \iff \sum_{s=0}^{p-1} (\omega^k)^s = 0$$

ω^k se $p \nmid k$ è una radice primitiva p-esima dell'unità.

$$(\omega^k - 1)\left(\sum_{s=0}^{p-1} (\omega^k)^s\right) = (\omega^k)^p - 1 = 0$$

non si annulla $\Rightarrow$ la somma $= 0$

Quanti sono i numeri di n cifre che sono divisibili per 3 e contengono solo cifre $\{2, 3, 7, 9\}$?

La somma delle cifre deve essere divisibile per 3.

Devo scegliere n numeri da $\{2, 3, 7, 9\}$ con somma $\equiv 0 \pmod 3$

$$\underbrace{(x^2 + x^3 + x^7 + x^9)(x^2 + x^3 + x^7 + x^9) \cdots (x^2 + x^3 + x^7 + x^9)}_{n}$$

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

$$\frac{P(x) + P(\omega x) + P(\omega^2 x)}{3}$$

Il risultato è $\dfrac{P(1) + P(\omega) + P(\omega^2)}{3}$

$P(1)$? 4^n

$P(\omega)$? $(\omega^2 + 1 + \omega + 1)^n = (1 + (\omega^2 + \omega + 1))^n = 1$

$P(\omega^2)$? $= 1$

$$\boxed{\frac{4^n + 2}{3}}$$

Romania 2003.

exponential generating function

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

$Egf(a_i) + Egf(b_i) = Egf(a_i + b_i)$

$Egf(a_{i+1}) \overset{?}{=} D\,Egf(a_i)$

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

$$= ogf\left(\sum_{j=0}^{i} \frac{a_j\, b_{i-j}}{j!(i-j)!}\right) = Egf\left(\sum_{j=0}^{i}\binom{i}{j} a_j\, b_{i-j}\right)$$

$$Egf(1) \overset{?}{=} 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \cdots = e^x$$

IMO 2008.

$k \geq n > 0$; $k \equiv n \pmod 2$

$2n$ lampadine numerate.

Sequenze di mosse = cambiare da ON → OFF alcune delle 2 lampadine

Sia $A(k)$ il numero di sequenze di k mosse t.c. alla fine le prime n sono accese, le seconde n sono spente.

Sia $B(k)$ " " " " " " , le seconde n non sono spente.

Calcolare $\frac{A(k)}{B(k)}$.

2^{k-n}.

Mosse di tipo B = spegnere ad ognuna delle prime n lampadine un numero di volte e poi accenderle in tutti i modi possibili

a_1 a_2 a_3 $\cdots$ a_n

$$\binom{a_1+a_2+\cdots+a_n}{a_1, a_2, \ldots, a_n} = \binom{k}{a_1, a_2, \ldots, a_n}$$

3 caramelle A, B, C

1 mora nelle prime 3 nelle seconde 5 nelle 3°.

⇕

numero di modi di ordinare 9 palline di cui 1 rosa, 3 blu, 5 verdi. $\frac{9!}{1!\,3!\,5!} = \binom{9}{1,3,5}$

$[x^k]\, F(x) = \frac{\mathcal{B}(k)}{k!} =$

$F(x) = \left(x + \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots\right)^n = \mathrm{egf}(\mathcal{B}(i))$.

gli esponenti in numero $\to [x^k]$ mi arriva k nome proprio. $\frac{1}{a_1!} \cdot \frac{1}{a_2!} \cdots \cdots \frac{1}{a_n!} = \frac{\binom{k}{a_1, a_2 \cdots a_n}}{k!}$

$\mathcal{B}(k) = k! \cdot [x^k] F(x)$.

---

o

$A(k)$?

$A(k) = k! \cdot [x^k]\left(x + \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots\right)^n \left(1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots\right)^n$

$F(x)$ lo so scrivere bene. e^x senza i coefficienti pari! $\frac{e^x - e^{-x}}{2}$

$\frac{e^x + e^{-x}}{2}$

$A(k) = k![x^k]\left(\frac{e^x - e^{-x}}{2}\right)^n \left(\frac{e^x + e^{-x}}{2}\right)^n = k![x^k]\left(\frac{e^{2x} - e^{-2x}}{4}\right)^n$

$B(k) = k![x^k]\left(\frac{e^x - e^{-x}}{2}\right)^n$ $\qquad \left(\frac{e^{2x} - e^{-2x}}{2}\right)^n$

2^n

$$\rightarrow \frac{A(x)}{B(x)} = \frac{[x^k]\left(\frac{e^{2x}-e^{-2x}}{2}\right)^n}{[x^k]\left(\frac{e^x-e^{-x}}{2}\right)^n} \cdot \frac{1}{2^n}$$

$$\frac{[x^k]\, g(2x)}{[x^n]\, g(x)} = \frac{z \cdot 2^k}{z} = 2^k$$

$$2^k / 2^n = 2^{k-n}.$$

$a_0, a_1, \ldots$ e $b_0, b_1, \ldots$ sono uguali

$$\Leftrightarrow \quad \mathrm{ogf}(a_i) = \mathrm{ogf}(b_i).$$

Snake oil method

$$a_n = \sum_{j=0}^{n} z_{j,n} \cdot r^n \qquad z_{j,n} = \binom{n}{j}\binom{n+100}{j}\binom{(n+100)\cdot 30^n}{n-j}$$

$z_{m,n}$ con $n<m$ è 0

$$\mathrm{ogf}(a_i) = \sum_{j=0}^{\infty} \mathrm{ogf}(z_{j,i}).$$

$$z_{3,0} + z_{3,1}x + z_{3,2}x^2 + \ldots$$

$$\mathrm{ogf}(a_i) = \sum_{i=0}^{\infty} x^i (a_i) = \sum_{i=0}^{\infty} x^i \left(\sum_{j=0}^{i} z_{j,i}\right) =$$

$[x^0]\ z_{0,0}$

$[x^1]\ z_{0,1}\quad z_{1,1}$

$[x^2]\ z_{0,2}\quad z_{1,2}\quad z_{2,2}$

$$\sum_{s=0}^{\infty}\left(z_{s,0}+z_{s,1}x+z_{s,2}x^2+\dots\right)=\sum_{s=0}^{\infty}\text{ogf}(z_{s,i})$$

Iran NMO 2008

Dimostrare che

$$\sum_{i=1}^{n}\binom{n+i-1}{2i-1}=F_{2n}$$

$\text{ogf}(F_{2i})=?\ F(x)$

$F_{2(n+1)}-F_{2n}$

$F_{2(n+2)}=F_{2n+3}+F_{2(n+1)}=F_{2(n+1)}+F_{2n+1}+F_{2(n+1)}$

$=3F_{2(n+1)}-F_{2n}$

$\text{ogf}(F_{2(i+2)})=3\cdot\text{ogf}(F_{2(i+1)})-\text{ogf}(F_{2i})$

$F_{2(i+2)}=F_{2i+3}+F_{2(i+1)}$

$\frac{F(x)-F_0-xF_2}{x^2}=3\frac{F(x)-F_0}{x}-F(x)$

$\frac{F(x)-x}{x^2}\qquad 3\frac{F(x)}{x}$

$F(x)-x=3xF(x)-x^2F(x)$

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

$\text{ogf}(\text{somma sotto})=\sum_{n=0}^{\infty}x^n\left(\sum_{i=1}^{n}\binom{n+i-1}{2i-1}\right)=$

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

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

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

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

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

qualcosa di MacLaurin

$$\frac{\Delta^k ogf(a_i)\big|_0}{k!} = a_k \qquad \Delta^2 ogf(a_i) = \Delta\left(\Delta\, ogf(a_i)\right)$$

Si dimostra per induzione! Facile!

Teorema binomiale esteso!

Def. $\binom{\alpha}{n} = \frac{\alpha(\alpha-1)\cdots(\alpha-(n-1))}{n!}$ con $\alpha \in \mathbb{R}$, $n \in \mathbb{N}$

Allora $ogf\left(\binom{\alpha}{n}\right) = (x+1)^\alpha$

Il Th. bin. esteso si mostra con MacLaurin

Per induzione vale:

$$\Delta^k (x+1)^\alpha = \alpha(\alpha-1)\cdots(\alpha-(k-1))(x+1)^{\alpha-k}.$$

$$[x^k](x+1)^\alpha = \frac{\Delta^k (x+1)^\alpha\big|_0}{k!} = \frac{\alpha(\alpha-1)\cdots(\alpha-(k-1))}{k!} = \binom{\alpha}{k}$$

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

$$[x^k]\ \frac{1}{\sqrt{1-4x}} = [x^k]\ (1-4x)^{-\frac{1}{2}} = (-4)^k \binom{-\frac{1}{2}}{k} =$$

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

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

Dim. che esiste un unico modo di partizionare $\mathbb{N}$ in A, B in modo che $\forall n \in \mathbb{N}$ il # di modi di esprimerlo come somma di el. distinti di A = # di B.

$$A(x) = \sum_{a \in A} x^a \qquad B(x) = \sum_{b \in B} x^b.$$

$$a(i) := \begin{cases} i \in A \to 1 \\ i \notin A \to 0 \end{cases} \qquad \text{stesso come per } b(i)$$

$A(x) = \text{agf}(a(i))$ e $B(x) = \text{agf}(b(i))$.

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

$[x^k]\ A(x)^2 \neq 2\,(\#$ modi di esprimere k come somma di 2 el. distinti $)$

$(\#$ modi di esprimerlo come somma di 2 elementi uguali$)$

$k = m+n \qquad x^m \cdot x^n \qquad x^n \cdot x^m$

$k = m+m \qquad x^m \cdot x^m$

$$A(x)^2 - A(x^2) = 2 \cdot \#\text{ modi di ottenere } k$$

$$B(x)^2 - B(x^2) = A(x)^2 - A(x^2)$$

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

$$(x-1)A(x^2)+A(x)=\frac{x}{1-x^2}=x\left(1+x^2+(x^2)^2+(x^2)^3+\dots\right)=$$

$$x+x^3+x^5+\dots$$

Posso ottenere WLOG $a(0)=1$ o in A

$$[x^{2k}](x-1)A(x^2)+A(x)=0$$

$$[x^{2k-1}]A(x^2)-[x^{2k}]A(x^2)+[x^{2k}]A(x)=0$$

$$0 \quad -[x^k]A(x)+[x^{2k}]A(x)=0 \to -a(k)+a(2k)=0$$

Con lo stesso metodo ma prendendo $[x^{2k+1}]$ otengo

$$a(2k+1)+a(2k)=1$$

$$\begin{cases} a_0=1 \\ a(2k)=a(k) \\ a(2k+1)=-a(2k)+1 \end{cases} \to \text{Sequenza è univocamente determinata}$$

Provate che $a(i)\in\{0,1\}\ \forall i$ e trovate quanto vale $a(100000)$

$a(i)=1 \iff$ il numero di 1 nella rappresentazione binaria di i è pari $\leftarrow a_0=1$

$a_0+a_1x+a_2x^2+\dots$ ci posso sostituire un valore $x\in\mathbb{C}$ e vedere quanto viene.

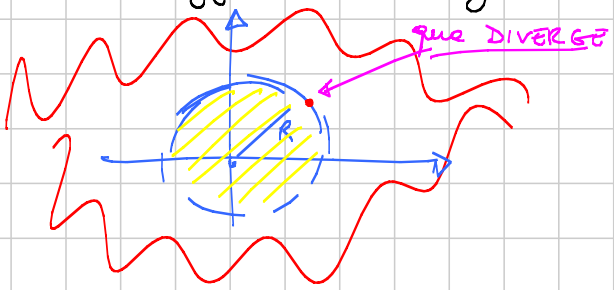
$a_0,a_1,\dots\in\mathbb{C}$

Voglio mostrare che $\sum_{i=0}^{\infty} a_i x^i$

$\exists R\geq 0, R\in\mathbb{R}$ t.c.

- Converge se $|x| < R$
- Non converge se $|x| > R$
- Non so cosa fa per $|x| = R$

R si chiama raggio di convergenza della serie



$$R = \liminf_{n\to\infty} \frac{1}{\sqrt[n]{a_n}}$$

Se $|x| > R \to a_n x^n$ non è infinitesimo per $n \to \infty$

Se per $x > 0 \in \mathbb{R}$ $\sum_{i=0}^{\infty} |a_i x^i|$ converge $\to \sum_{i=0}^{\infty} a_i y^i$ converge sempre per $y \in \mathbb{C}$ con $|y| < x$

E perché $\sum_{i=0}^{\infty} |a_i x^i|$ per $x \in \mathbb{R}$ con $x < R$ converge?

Perché è minorata da una geometrica $a_i x^i$

Quanto vale $\sum_{n=0}^{\infty} \frac{F_n}{2^n}$? (USA 2003 qualcosa)

Quanto vale $\sum_{n=0}^{\infty} \frac{2^n}{3^n} F_n$? si può comportare male solo divergendo

$$\text{ogf}(F_i) = \frac{x}{1-x-x^2} \qquad \text{ogf}\left(\frac{F_i}{2^i}\right) = \text{ogf}(F_i) \circ \frac{x}{2} =$$

$$\text{ogf}\left(\frac{F_i}{2^i}\right) = \frac{\frac{x}{2}}{1-\frac{x}{2}-\frac{x^2}{4}}$$ } ne questo non diverge mai per $|x| < 1 \to$ Ho vinto

$$\sum_{i=0}^{\infty} \frac{F_i}{2^i} = \frac{\frac{1}{2}}{1-\frac{1}{2}-\frac{1}{4}} = \boxed{2}$$

non posso mettere 1 perché una radice è < 1

$$\frac{\frac{2}{3}x}{1-\frac{2}{3}x-\frac{4}{9}x^2}$$

$$\sum_{i=0}^{\infty} F_i \frac{2^i}{3^i} = \Delta$$

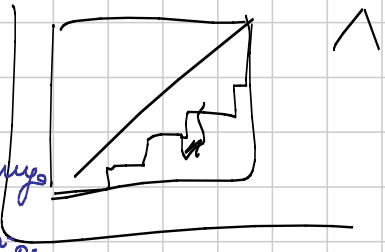
o

Catalan!

I numeri di Catalan $C_0, C_1, C_2, \dots$.

C_n è il numero di disposizioni ordinate di n parentesi (e n parentesi).

)((~~no~~ ()() sì



A ogni disposizione associo la sottostringa iniziale che è una buona disposizione.

((()())) (())

(()) (())

((()))

$$C_{n+1} = \sum_{i=0}^{n} C_i \cdot C_{n-i}$$

Prendo le disposizioni che hanno come sottostringa iniziale buona lunga $(i+1)$

$C_0 = 1$.

$$ogf(C_{in}) = \frac{C_0}{1 - x\, ogf(C_i)} \qquad ogf(C_i) = C(x)$$

$$C(x) = \frac{1}{1 - xC(x)} \longrightarrow xC(x)^2 - C(x) + 1 = 0$$

$$C(x) = \frac{1 \pm \sqrt{1-4x}}{2x} \qquad 1 \pm \sqrt{1} = 0$$

si deve semplificare!

$$C(x) = \frac{1 - \sqrt{1-4x}}{2x} \qquad ogf\left(\binom{2i}{i}\right) = \frac{1}{\sqrt{1-4x}}$$

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

$$ogf\left((i+1)\, C_i\right) \overset{\text{hope}}{=} ogf\left(\binom{2i}{i}\right) = \frac{1}{\sqrt{1-4x}}$$

$D\left(x \cdot C(x)\right)$ e applicando le regole di derivazione trovo l'identità!

Sono dati n pesi $2^0, 2^1, \dots, 2^{n-1}$ e una bilancia a 2 bracci.

modi di piazzare i pesi (contando l'ordine) in modo che nel piatto di destra ci sia sempre un peso maggiore che nel piatto di sinistra? $= a_n$

Fatto I: Non cambia nulla se scelgo n potenze di 2 distinte a caso. Motivazione: Somma di potenze di 2 < delle successive.

Prendo 2^{n-1} e lo piazzo per k^{esimo}. In quanti modi posso farlo?

2^{n-1} → prodotto di destra.

I k precedenti pesi già presenti li posso scegliere in $\binom{n-1}{k}$ modi. E li posso piazzare in a_k modi!

I successivi in quanti modi posso piazzarli? $(n-1-k)!\ 2^{n-1-k}$

$$\binom{n-1}{k}\, a_k \cdot (n-1-k)! \cdot 2^{n-1-k}$$

$$a_n = \sum_{k=0}^{n-1} \binom{n-1}{k} a_k\, (n-1-k)!\ 2^{n-1-k}$$

$$b_n = \frac{a_n}{n!}$$

$$n\, b_n = \sum_{k=0}^{n-1} b_k \cdot 2^{n-1-k}$$ ← Prodotto

$$f(x) = \mathrm{ogf}(b_i)$$ $\qquad f' = \frac{f}{1-2x}$

$$g(x) = \mathrm{ogf}\left((i+1)\, b_{i+1}\right).$$ $\qquad 2^0 + 2^1 x + 2^2 x^2 + \dots = \frac{1}{1-2x}$

$$(n+1)\, b_{n+1} = \sum_{k=0}^{n} b_k\, 2^{n-k}$$

$$g(x) = \mathrm{ogf}\left((i+1)\, b_{i+1}\right) = \mathrm{ogf}\left(\sum_{k=0}^{i} b_k\, 2^{i-k}\right) =$$

$$\mathrm{ogf}(b_i) \cdot \mathrm{ogf}(2^i) = \frac{f(x)}{1-2x}$$

$$(1-2x)\, g(x) = f(x) \qquad [x^n]$$

$$[x^{n+1}]\, g(x) - 2[x^n]\, g(x) = [x^{n+1}]\, f(x)$$

$$(n+1)\, b_{n+1} - 2n\, b_n = b_n \;\to\; b_{n+1} = \frac{2n+1}{n+1} - b_n$$

Per induzione è facile accorgersi che: $b_n = \frac{(2n-1)!!}{n!}$

$a_n = n!$ $b_n = (2n-1)!!$

COMBINATORIA 2 - (soprattutto) GRAFI

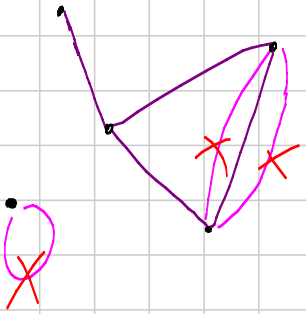
Titolo nota 09/09/2011

$G = (V(G), E(G))$ GRAFO

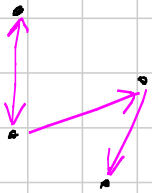
(V, E)

$\| \quad \|$

$V(2)$



GRAFO diretto

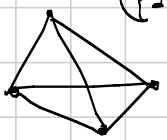


TEORIA DI RAMSEY

6 persone → ci sono 3 amici
o 3 sconosciuti

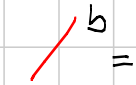
grafo "completo" K_6

[notazione: K_n $(\{1,\dots,n\}, \{1,\dots,n\}^{(2)})$

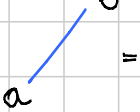


]

2-colora gli archi



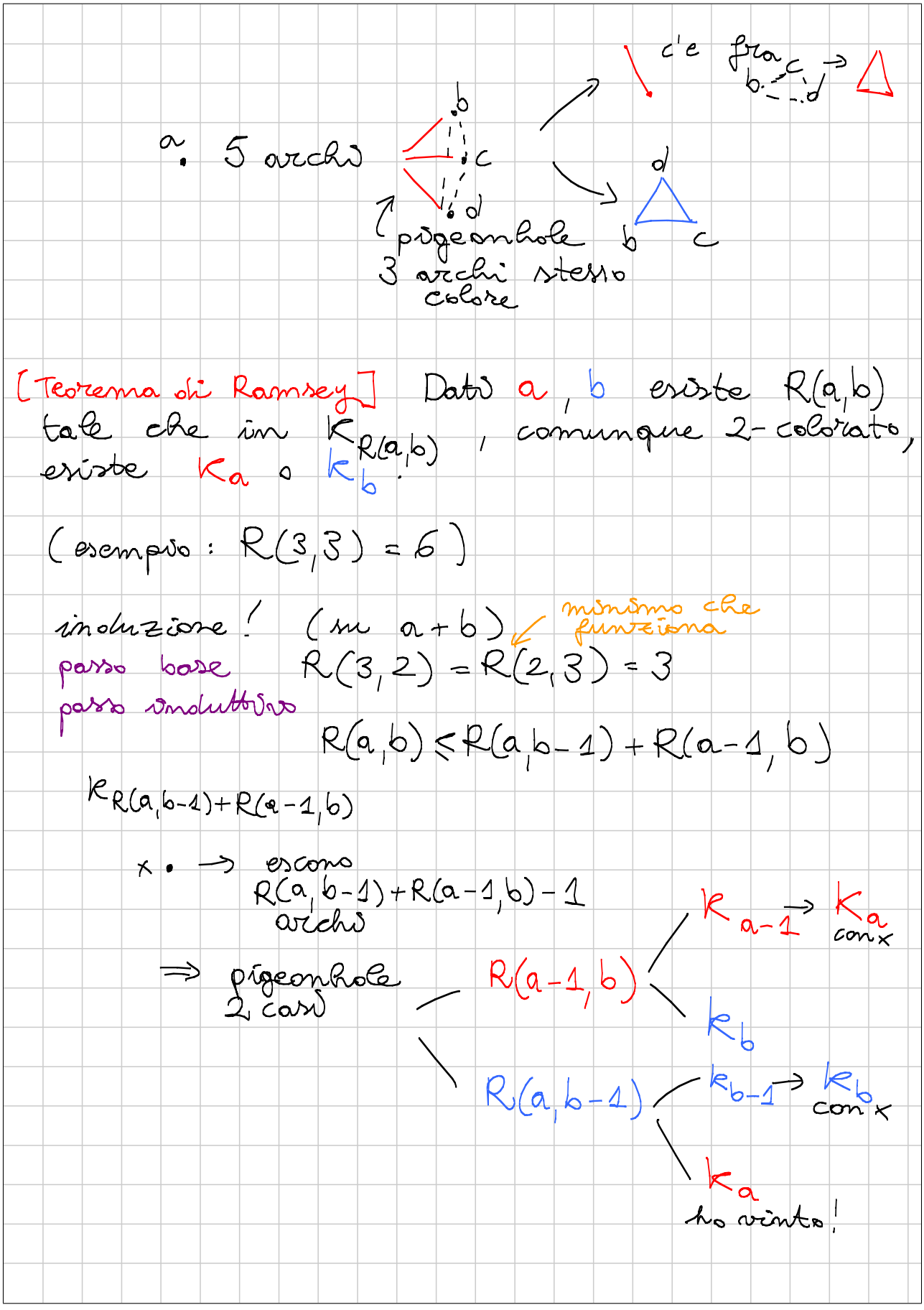
a b = a e b sono amici



a b = a e b sconosciuti

TESI: $\exists$ △ o △

pigeonhole!



[Teorema di Ramsey] Dati a, b esiste $R(a,b)$ tale che in $K_{R(a,b)}$, comunque 2-colorato, esiste K_a o K_b.

(esempio: $R(3,3) = 6$)

induzione! (su $a+b$) ← minimo che funziona

passo base $R(3,2) = R(2,3) = 3$

passo induttivo

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

$K_{R(a,b-1)+R(a-1,b)}$

x → escono $R(a,b-1)+R(a-1,b)-1$ archi

⇒ pigeonhole 2 casi

$R(a-1,b)$ — $K_{a-1} \to K_a$ con x

$R(a-1,b)$ — K_b

$R(a,b-1)$ — $K_{b-1} \to K_b$ con x

$R(a,b-1)$ — K_a ho vinto!

STIMA: $R(a,b) \leq \binom{a+b-2}{b-1}$

base $R(2,3) = R(3,2) = 3 = \binom{3}{1}$

passo induttivo

$$R(a,b) \leq \binom{a+b-3}{b-2} + \binom{a+b-3}{b-1} =$$

$$= \binom{a+b-2}{b-1} \qquad \square$$

Problema: ROM TST 2008

Un insieme di persone è n-bilanciato se:
- $\forall$ sottoinsieme da 3 ci sono 2 amici
- $\forall$ sottoinsieme da n ci sono 2 sconosciuti

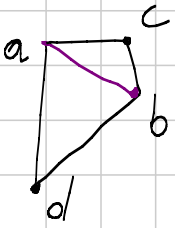
mostrare che un insieme n-bilanciato ha $\leq \frac{(n-1)(n+2)}{2}$ persone.

K_N due-colorato | ogni K_3 ha —→ No K_3
ogni K_n ha —→ No K_n

$$N \leq R(n,3) - 1 \leq \binom{n+1}{2} - 1 = \frac{n^2+n-2}{2} =$$

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

Problema 6 punti nel piano: formano segmenti di lunghezze tutte $\neq$.
Allora $\exists$ segmento che è lato + lungo di un triangolo e lato + corto di un altro.



Ho un K_6.
Guardo ciascun triangolo; colora ——— il suo lato + corto.

Ramsey $\Rightarrow \exists$ △ o △

△: unico caso: prendo il suo lato + lungo

△: NON può esistere

TEORIA DEI GRAFI ESTREMALE

Ho un grafo su n vertici; quanti archi ha al max se NON contiene un K_3?
$ex(n, K_3) = \left\lfloor \frac{n^2}{4} \right\rfloor$ ([Teorema di Mantel])

- induzione
- CS

dimostrazione: ($G = (V(G), E(G))$ con $|V(G)| = n$ NO △.

[Notazione: **independent set** insieme di nodi non collegati da archi; K_n invisibile]

insieme dei nodi

prendo $A \subseteq V$ independent set massimale.
$B = V \setminus A$
↑ covering

[notazione: B è **covering** se ogni arco ha un vertice in B]

[x nodo $d(x)$ = grado di x = # archi che escono da x]

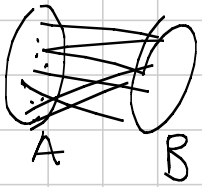
$$|E(G)| \le \sum_{x \in B} d(x) \le |B|\,|A| \le \left(\frac{|A|+|B|}{2}\right)^2$$

(AM-GM)

$d(x) \le |A|$ perché {vicini di x} è un independent set

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

caso di uguaglianza $|A| = |B|$ (n pari)



grafo bipartito completo $K_{\frac{n}{2},\frac{n}{2}}$

caso n dispari $K_{\lceil \frac{n}{2} \rceil, \lfloor \frac{n}{2} \rfloor}$

$ex(n, K_r)$ = # max archi di un grafo su n nodi SENZA K_r.

$n \ge r$

[Teorema di Turán] $ex(n, K_r) \le \left(1 - \frac{1}{r-1}\right)\frac{n^2}{2}$

dimostrazione. induzione (estesa) su n.

passo base $n = 0 \dots r$

passo induttivo G con $ex(n, K_{r+1})$ archi, n nodi, SENZA K_{r+1}.

G contiene come sottografo K_r. ($A \subseteq V(G)$)

$\subseteq B$

$x \in V(G) \setminus A \quad d_A(x) \leq r-1$

$|A| = r$

$|B| = n-r$

$$|E(G)| \leq (n-r)(r-1) + ex(n-r, K_{r+1}) + \binom{r}{2} =$$

(dentro B; da B in A)

$\leq \left(1-\frac{1}{r}\right)\frac{(n-r)^2}{2}$

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

$(2n-r)$

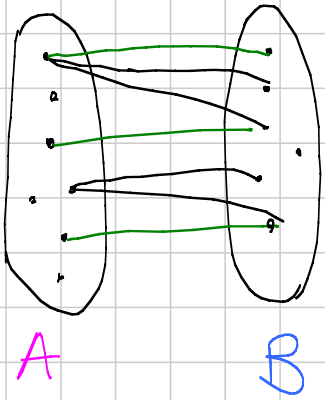
$$= \frac{r(2n-r)}{2} - \frac{r(2n-r)}{r\,2}$$

$$= \left(1-\frac{1}{r}\right)\left(\frac{2nr-r^2}{2}\right)$$

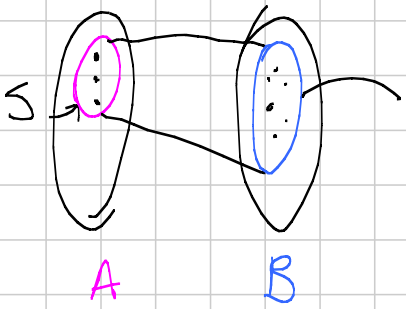
$$= \left(1-\frac{1}{r}\right)\frac{n^2 - \cancel{2nr} + \cancel{r^2} + \cancel{2nr} - \cancel{r^2}}{2} =$$

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

MATCHING in grafi bipartiti



q perfect matching ($|A| = |B|$)
un matching su tutti gli elementi di A



$N(S)$ = uomini che piacciono almeno a una tipa di S

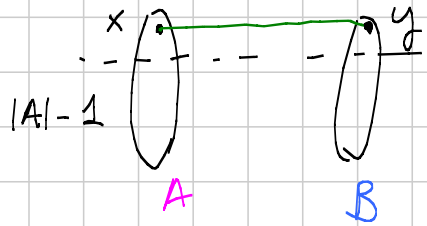
se $\exists$ perfect matching $|N(S)| \geq |S|$

[Teorema di Hall / Lemma dei matrimoni]

Dato grafo bipartito con $V = A \cup B$ ($|A| \leq |B|$) esiste un matching di A in $B \iff \forall S \subseteq A \quad |N(S)| \geq |S|$. (*)

($\Rightarrow$) ovvio. ($\Leftarrow$) dimostriamo! Per induzione (estesa) su $|A|$.

- $\forall S \neq A \quad |N(S)| > |S|$



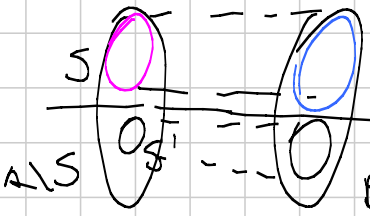
scelgo $x, y \in N(x)$ e li sposo.
È vera (*) per $A \setminus \{x\}$, $B \setminus \{y\}$?

per assurdo $S' \subseteq A \setminus \{x\}$
$|N(S') \setminus \{y\}| < |S'|$: avrei

$|N(S')| \leq |S'| \rightarrow$ NO $(|N(S')| \geq |S'|)$ per ipotesi

- $\exists S \subsetneq A \quad |N(S)| = |S|$

usare ipotesi induttiva!



grafo indotto da S, $N(S)$ ($|S| < |A|$) soddisfa (*) → per hp induttiva posso sposare S con $N(S)$.

Riesco a dimostrare (*) per $A \setminus S$, $B \setminus N(S)$?

S':

$S' \subseteq A \setminus S$ per assurdo $|N(S') \cap (B \setminus N(S))| < |S'|$;

$$|N(S' \cup S)| < |S'| + |N(S)| = |S'| + |S| = |S' \cup S|$$

non può essere! (contraddice (*))

VIETNAM TST 2010

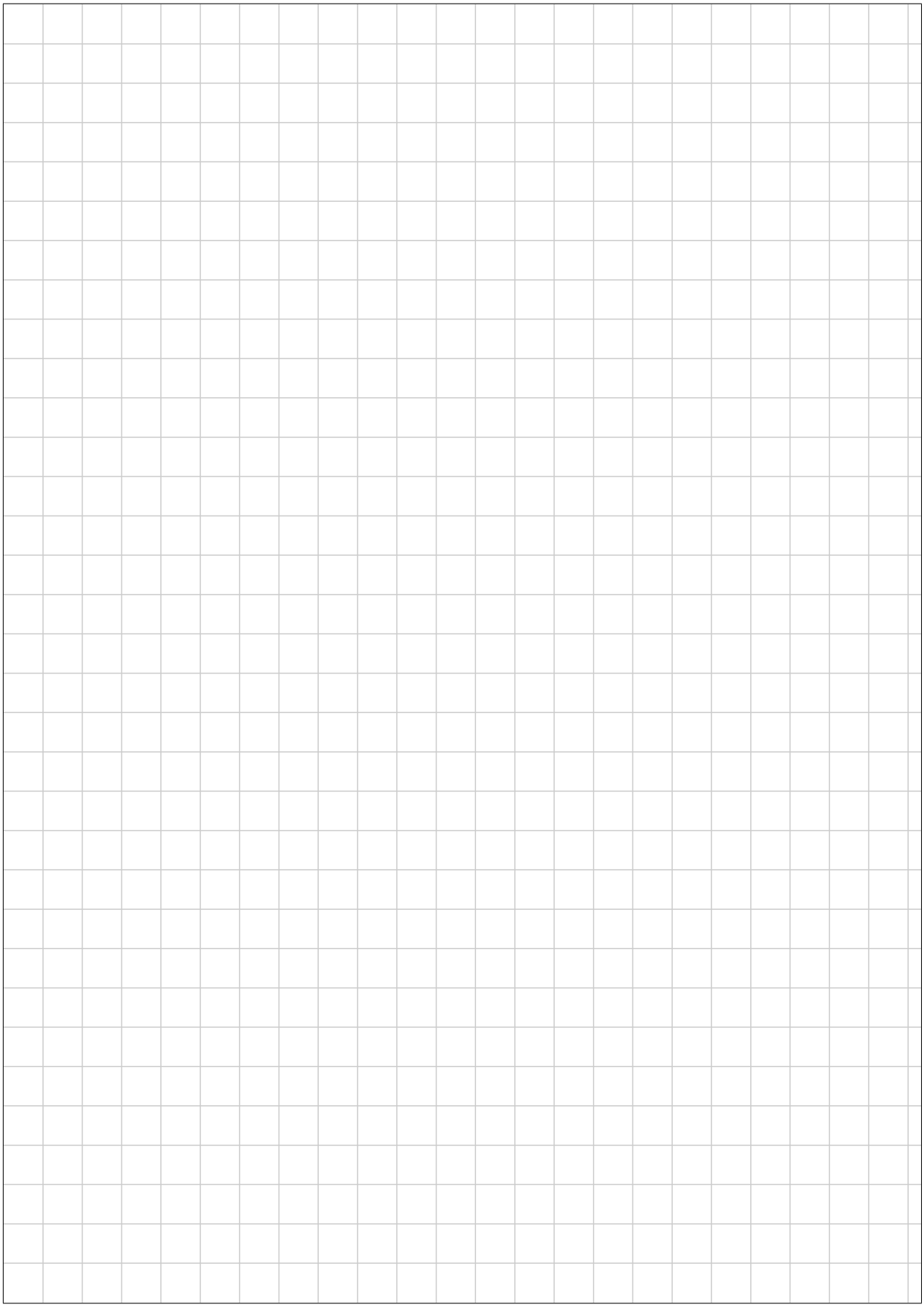
$1 < m < n$ nm bambini, n nazioni

m bambini per nazione;

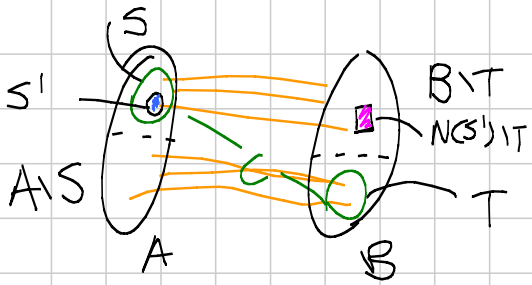
n classi, in ogni classe m bambini,

bambini della stessa nazionalità NON nella stessa classe.

Voglio scegliere n bambini senza che ci siano 2 della stessa classe né della stessa nazionalità.



Combinatoria 2 (Medium) – Alessandra Caraceni



dimostro che $\exists$ matching di S in $B \setminus T$ e T in $A \setminus S$

Devo verificare (*).

Prendo $S' \subseteq S$ $\quad |N(S') \cap (B \setminus T)| < |S'|$ per assurdo.

sostituisco $N(S') \setminus T$ a S' in C, ottengo C'

È ancora un cover!

$|C'| < |C| = \beta$: assurdo!

POSETS

"poset" = partially ordered set

$(X, \leq)$ ← rel d'ordine parziale

↑ insieme

- $x \leq x$
- $x \leq y, y \leq x \Rightarrow x = y$
- $x \leq y, y \leq z \Rightarrow x \leq z$

ESEMPI $\quad (\mathbb{N}, \leq)$, $(\mathbb{Z}^2, \leq)$, $(\mathcal{P}(X), \subseteq)$

$x \leq y$

(X = partizioni di $\{1, \dots, n\}$, "finezza")

catena $\quad x_1 < x_2 < \dots < x_m$

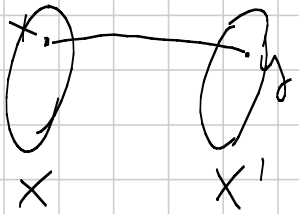
antocatena $\quad$ insieme di elementi 2 a 2 NON confrontabili

(poset finiti) ← "larghezza" del poset

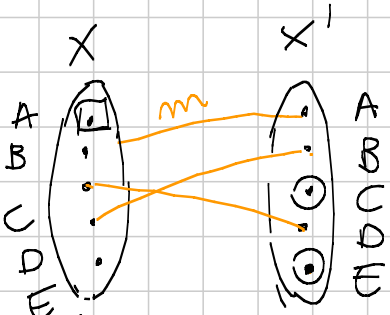
[Teorema di Dilworth] # max anticatena = # minimo ricoprimento del poset come unione di catene.

dimostrazione!

interpreto poset come grafo bipartito



arco se $x \leq y$



di m archi

matching ⟷ copertura in catene

↺ n−m catene

$C < D < B < A$

E

> 2 catene

ho un m-matching

⇒ ho copertura in catene da $n-m$

ho un covering C' minimale di m elementi;

ho $\geq n-m$ elementi di X che non hanno copie in C.

Sono un'anticatena.

Quindi min # cop in anticatene $\leq$ # max anticatena $\geq$ ovvio (ogni el dell'anticatena deve stare in catena diversa).

insieme $X \subseteq \mathbb{N}$

ROM TST 2005 n^2+1 naturali positivi | $\forall$ sottinsieme da $n+1$ ha 2 el - $a, b \in S$ tc. $a \mid b$.

Allora $\exists\ x_1, x_2, \dots, x_{n+1} \in S$ tc $x_1 \mid x_2 \mid x_3 \mid \dots \mid x_{n+1}$

$(X, \mid)$ è un poset!

max anticatena $\leq n$

$\Rightarrow \exists$ un ricoprimento di X in n catene $\Rightarrow$ per pigeonhole $\exists$ catena lunga $n+1$. □

[Duale di Dilworth] #max catena = # min ric in anticatene.

$\leq$ è ovvio.

$f(x) =$ # più lunga catena di cui x è l'elemento massimo.

$f(X) \subseteq \{1 \dots n\}$ ← # max catena

$f^{-1}(i)$ è un'anticatena!

$x < y \Rightarrow f(y) \geq f(x) + 1$

$X = \bigcup_{i=1}^{n} f^{-1}(i)$ ricoprimento in anticatene.

[Erdös-Szekeres] successione di $ab+1$ reali $\Rightarrow$
$\exists$ sottosucc. di $a+1$ ↗ o di $b+1$ ↘.

POSET: $\{x_1 \dots x_{ab+1}\}$ $\leq$?
$x_i \leq x_j \iff i \leq j,\ x_i \leq x_j$

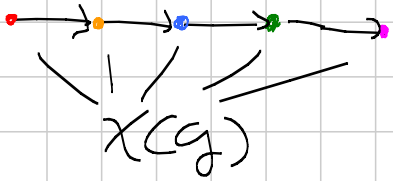
CATENE = sotto-successioni crescenti
ANTICATENE = successioni decrescenti

se non c'è catena di lungh. $a+1$
posso coprire con a anticatene $\Rightarrow$
(pigeonhole) ho un'anticatena di # $\geq b+1$.

[Lemma di Sperner] in $\mathcal{P}(\{1 \dots n\})$ la max anticatena ha #
$\binom{n}{\lfloor n/2 \rfloor}$.

problema partita. $\forall G$ $\chi(G)$- esiste un "cammino arcobaleno" cioè

[notazione: $\chi(G)$ = min n° di colori con cui posso colorare nodi in modo che non ci sia]



$1 < 2 < \dots$ rendiamo G un grafo diretto

dico che $x < y$ se $\exists$ cammino orientato da x a y.
C'è una catena lunga $\chi(G)$?
Hope: la colorazione è una partizione in anticatene ...? VERO!
NON ci può essere una partizione in meno di $\chi(G)$ anticatene

$\chi(G) - 1$ anticatene

G1 medium, Senior 2011

elianto84 (Jack)

Titolo nota 05/09/2011

$\cos(a+b) = \cos a \cdot \cos b - \sin a \sin b$

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

$\cos(3a) = \cos(a+2a) = \cos a \cos 2a - \sin a \sin 2a$

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

(P.t. $\sin^2 a = 1 - \cos^2 a$) $= 2\cos^3 a - \cos a - 2\sin^2 a \cos a$

$= 2\cos^3 a - \cos a - 2(1-\cos^2 a)\cos a$

$= 4\cos^3 a - 3\cos a.$

Claim: $\forall n \in \mathbb{N}$ $\cos(nx)$ è un poly di grado n in $\cos x$.

Def. $T_n(x) = \cos(n \arccos x)$

⊙ $T_{n+2}(x) = 2x\,T_{n+1}(x) - T_n(x)$ (rel. ricorr.)

$x = \cos y$

$\cos((n+2)y) = 2\cos y \cos((n+1)y) - \cos(ny)$

$\cos((n+2)y) + \cos(ny) = 2\cos y \cos((n+1)y)$

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

$\begin{cases} T_0(x) = 1 \\ T_1(x) = x \\ T_2(x) = 2x^2 - 1 \end{cases}$ Poly di Chebyshev del 1° tipo.

Claim. $T_n(x) = \dfrac{(x - \sqrt{x^2-1})^n + (x + \sqrt{x^2-1})^n}{2}$ $\Big]$ $F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{-1+\sqrt{5}}{2}\right)^n\right)$

$= \widetilde{T}_n(x)$

$\widetilde{T}_0(x) = 1 \quad \widetilde{T}_1(x) = x$

Per induzione su n $\widetilde{T}_{n+2}(x) = 2x\,\widetilde{T}_{n+1}(x) - \widetilde{T}_n(x).$

$$\left(x - \sqrt{x^2-1}\right)^n = \sum_{j=0}^{n} \binom{n}{j} x^j (-1)^{n-j} (x^2-1)^{\frac{n-j}{2}}$$

$$= \sum_{j=0}^{n} \binom{n}{j} x^{n-j} (-1)^j (x^2-1)^{j/2} \quad \|$$

$$\left(x + \sqrt{x^2-1}\right)^n + \left(x - \sqrt{x^2-1}\right)^n = 2 \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j} x^{n-2j} (x^2-1)^j \quad |$$

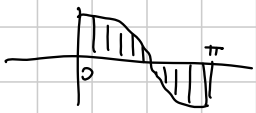
Quali sono le radici del polinomio $T_n(x)$?

Per quali valori di x si ha

$$\cos(n \arccos x) = 0 \quad ?$$

$$n \arccos x \in \left\{(2k+1)\frac{\pi}{2}\right\} \qquad \arccos x \in \left\{(2k+1)\frac{\pi}{2n}\right\}$$

$$x \in \left\{\cos\left((2k+1)\frac{\pi}{2n}\right)\right\} =: E_n$$



$$|E_n| = n.$$

Tutte le radici di $T_n(x)$ sono reali.

Def. $$U_n(x) = \frac{\sin((n+1)\arccos x)}{\sin(\arccos x)}$$

$$U_{n+2}(x) = 2x\, U_{n+1}(x) - U_n(x) \qquad \begin{cases} U_0(x) = 1 \\ U_1(x) = 2x \end{cases}$$

$$U_2(x) = 4x^2 - 1$$

Le radici di $U_n(x)$ sono

$$\cos\left(\frac{\pi k}{n+1}\right) \quad \text{per } k = 1, \dots, n$$

T_n, U_n soddisfano rel. ric.

conosciamo le radici
conosciamo i coefficienti
} Viète $\triangleright$ $$\sum_{k=1}^{n} \cos^3\left(\frac{\pi k}{n+1}\right)$$

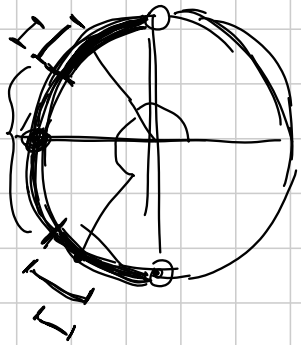
(1) Determinare tutti i $\theta \in [0, 2\pi)$ tali per cui

$\forall n \in \mathbb{N}$ si ha $\cos(2^n \theta) \leq 0$. (*)

$n=0$ $\cos\theta \leq 0$; $\theta \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ NO

$n=1$ $\cos 2\theta < 0$

$n=2$ $\cos 4\theta < 0$



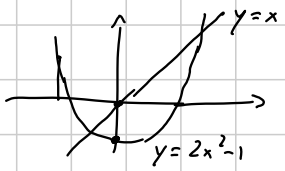
Claim: gli unici θ per cui vale (*) sono $\theta = \frac{2\pi}{3}$, $\theta = \frac{4\pi}{3}$.

$2\pi\left(\frac{1}{2} - \frac{1}{4} + \frac{1}{8} - \frac{1}{16} + \frac{1}{32} - \dots\right)$ $\quad 4\pi\left(\frac{1}{2} - \frac{1}{4} + \dots\right)$

$\theta \in (\pi/2, 3\pi/2)$ $n=0$ ha verificato $\cos\theta \overset{t}{<} 0$

$f: t \mapsto 2t^2 - 1$ Quali punti di $[-1, 0)$ sono tali per

$\forall n \geq 1$ $f^{(n)}(t) < 0$



Disuguaglianze geometriche

Claim A, B, C angoli di un triangolo $A, B, C \geq 0$, $A+B+C = \pi$

allora $\left| \prod_{cyc} \sin\frac{A}{2} \right| \leq \frac{1}{8}$.

$\sin\frac{A}{2} \sin\frac{B}{2} \sin\frac{C}{2}$

Jensen (convessità)

$\log(\sin t)$ concava per $t \leq \frac{\pi}{2}$

Briggs' $\Rightarrow \left| \sum_{cyc} \cos A \leq \frac{3}{2} \right|$ $\overset{\text{Carnot}}{\underset{\text{coseno}}{\Rightarrow}}$ $\sum_{cyc} \frac{b^2+c^2-a^2}{2bc} \leq \frac{3}{2}$

$$2\sum_{sym} ab^2 \leq \sum_{sym} (a^3 + abc)$$

$p(a,b,c)$

Disuguaglianza di Schur.

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

WLOG $a \geq b \geq c$

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

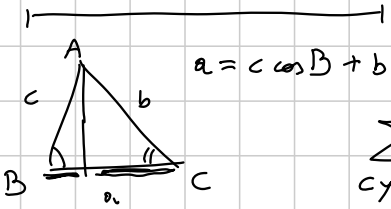
Schur – Vornicu

$a,b,c,x,y,z \in \mathbb{R}$ $a \geq b \geq c$ e $x \geq y \geq z$ oppure $x \leq y \leq z$

$k > 0$ $f(z)$ funzione monotona o convessa

$$f(x)(a-b)^k(a-c)^k + f(y)(b-a)^k(b-c)^k + f(z)(c-a)^k(c-b)^k \geq 0$$

(+ potente delle disug di "bunching").



$a = c\cos B + b\cos C$

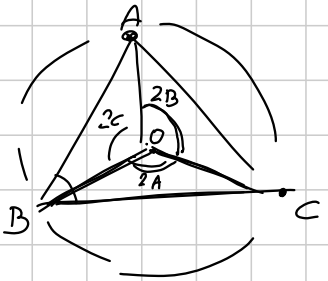
$$\sum_{cyc} a\cos A \leq \frac{a+b+c}{2} = p$$

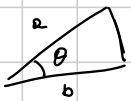
$$R\sum_{cyc} \sin(2A) \leq \frac{\Delta}{r}$$

$$\sum_{cyc} R^2 \sin(2A) \leq \frac{\Delta R}{r}$$

$$2\Delta \leq \frac{\Delta R}{r}$$

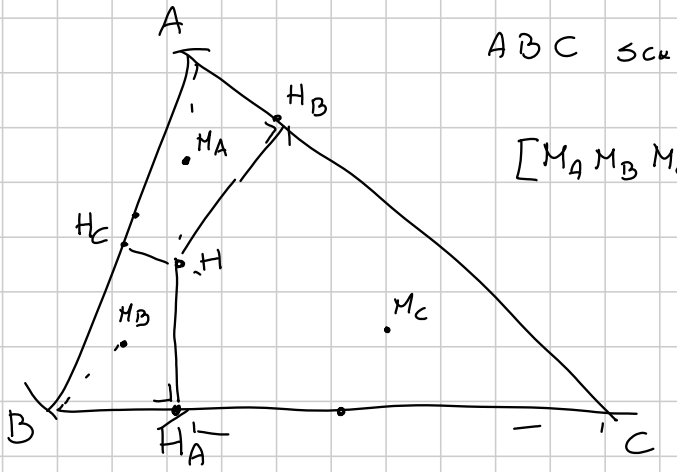
(Eulero). $R \geq 2r$





$\frac{1}{2}ab\sin\theta$

$[OBC]$ $\frac{1}{2}R^2\sin(2A)$



ABC scaleno e acutangolo

$[M_A M_B M_C] \geq [H_A H_B H_C]$.

$\updownarrow$

$H \not\equiv O$.

$CH_A H_B$ è simile al triangolo $CAB \Rightarrow H_A H_B = c \cdot \cos C$

$R(H_A H_B H_C) = \frac{1}{2} R(ABC)$.

$$\prod_{cyc} \cos A \leq \frac{1}{8}$$

$$\sum_{cyc} \sin^2 A \leq \frac{9}{4}$$

$$9R^2 \geq (a^2 + b^2 + c^2)$$

O, H, G sono allineati per il T. di Eulero

$\uparrow$ $H = A + B + C$ in un sistema centrato nel circocentro O

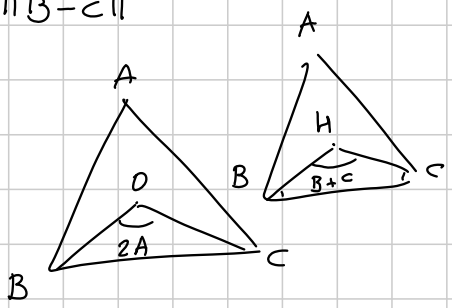
$$\|H\|^2 = \|A+B+C\|^2 = \sum_{cyc} \|A\|^2 + \sum_{cyc} 2(A \circ B) \quad \text{(teo. coseno)}$$

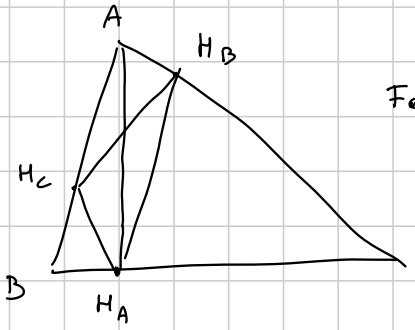
$$= 3R^2 - \sum_{cyc} (\|B-C\|^2 - \|B\|^2 - \|C\|^2)$$

$$= 9R^2 - \sum_{cyc} \|B-C\|^2$$

- $OH^2 = 9R^2 - (a^2 + b^2 + c^2)$.

$\begin{cases} 2A = B+C \\ \text{e cyc} \end{cases} \Rightarrow A = B = C = \frac{\pi}{3}$.





Fatto noto: $\widehat{H_C H_A A} = \widehat{A H_A H_B}$

A, B, C sono excentri di $H_A H_B H_C$

$\begin{cases} \text{t. portenza} \\ \text{t. ortico} \end{cases} \longrightarrow \begin{cases} \text{t. portenza} \\ \text{t. degli excentri} \end{cases}$

$$[I_A I_B I_C] = \frac{ab\cos(C/2)}{2\sin(A/2)\sin(B/2)} = 8R^2 \prod_{cyc} \cos\frac{A}{2}$$

$$= 2R^2 \sum_{cyc} \sin A \quad \text{(Brigs)}$$

$$= 2p\,R$$

$R \geq 2r$ (Eulero).

---

a, b, c lati di un triangolo.

$a^2 + b^2 + c^2 = 8R^2 \longrightarrow$ ABC è rettangolo.

α, β sono angoli acuti $\in (0, \frac{\pi}{2})$

Se $\sin^2\alpha + \sin^2\beta = \sin(\alpha+\beta)$

allora $\sin^2\alpha + \sin^2\beta = 1$.

---

r_a il raggio delle circ. ex-inscritte ad ABC relative al vertice A

allora $4R + r = \sum_{cyc} r_a$.

A_n poligono regolare di n lati di lunghezza unitaria.

Quanto vale il prodotto delle lunghezze di tutte le diagonali di A_n?

$|OH|^2 = 9R^2 - (a^2+b^2+c^2)$ Se $a^2+b^2+c^2 = 8R^2$

$|OH|^2 = R^2$

$H \in \Gamma(ABC)$

I simmetrici di H rispetto ai lati appartengono a $\Gamma(ABC)$

$H \in$ lati almeno 2 lati sono anche altezze

ABC è rettangolo.

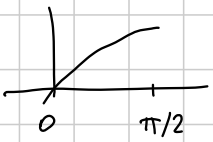
$$a^2+b^2+c^2 = 8R^2$$

$$\sum_{cyc} \sin^2 A = 2 \qquad \sum_{cyc} \cos 2A = -1 \qquad \text{Briggs} \qquad \prod_{cyc} \cos A = 0$$

almeno 1 tra A, B e C è pari a $\pi/2$.

$$\sin^2\alpha + \sin^2\beta = \sin\alpha\cos\beta + \sin\beta\cos\alpha$$

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



$\alpha+\beta=\pi/2$

$\alpha+\beta > \frac{\pi}{2}$ $\begin{cases} \alpha > \frac{\pi}{2}-\beta \\ \beta > \frac{\pi}{2}-\alpha \end{cases}$

$$\sin\alpha > \sin\left(\frac{\pi}{2}-\beta\right)$$
$$\sin\beta > \sin\left(\frac{\pi}{2}-\alpha\right)$$

$\alpha+\beta < \frac{\pi}{2}$

$$r_a = p\tan\frac{A}{2} = p\,\frac{2bc\sin A}{2bc(1+\cos A)} = \frac{4p\Delta}{(b+c-a)(b+c+a)} = \frac{\Delta}{p-a}$$

moltiplichiamo LHS e RHS per Δ ed applichiamo Erone

$$abc + (p-a)(p-b)(p-c) = \sum_{cyc} p(p-b)(p-c) \overset{\text{Erone}}{=} \Delta^2 = p(p-a)(p-b)(p-c)$$

$$V(a_1,\dots,a_n) = \begin{pmatrix} 1 & a_1 & \dots & a_1^{n-1} \\ \vdots & & & \\ 1 & a_n & \dots & a_n^{n-1} \end{pmatrix}$$

$$\det V(a_1,\dots,a_n) = \prod_{1\le i<j\le n} (a_j - a_i)$$

$\zeta = e^{2\pi i/n} = e(1/n)$ $\quad e(\alpha) = e^{2\pi i \alpha}$

$\zeta^k \quad k = 0, 1, \dots, n-1$ $\quad \prod_{1 \le i < j \le n} (\zeta^j - \zeta^i)$

$\det \begin{pmatrix} 1 & \zeta & \zeta^2 & \dots & \zeta^{n-1} \\ 1 & \zeta^2 & \zeta^4 & \dots & \zeta^{2n-2} \\ \vdots & & & & \\ 1 & \dots & & & \end{pmatrix}$ $\quad \cdot \zeta^n = 1$

$\det A = \det A^T$

$\det(A \cdot A^T)$

$$\det A = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \prod_{i=1}^{n} A_{i,\sigma(i)}$$

$A \cdot A^T = \begin{pmatrix} n & & 0 \\ & n & \\ 0 & & \ddots\ n \end{pmatrix}$ $\quad \det(A \cdot A^T) = n^n$

$\det A = n^{n/2}$

$\forall z \in \mathbb{C} \setminus \{0\}$ $\quad \frac{\sin z}{z} = \prod_{n=1}^{+\infty} \left(1 - \frac{z^2}{\pi^2 n^2}\right)$

$$\cos z = \prod_{m=0}^{+\infty} \left(1 - \frac{4z^2}{\pi^2 (2m+1)^2}\right)$$

Prodotti di Weierstress

$$\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

$\mathbb{Z}/p\mathbb{Z} \overset{*}{=} \mathbb{F}_p^*$ è un gruppo $\quad$ i quadrati vengono detti residui quadratici

$\langle g \rangle \quad |\mathbb{Z}/p\mathbb{Z}^*| = p-1$ $\quad |\text{residui quadratici } \mathbb{F}_p| = \frac{p-1}{2}$

a è un residuo quadratico sse $a^{\frac{p-1}{2}} \equiv 1 \pmod p$

$a^{\frac{p-1}{2}} = \begin{matrix} +1 \\ -1 \end{matrix} > \left(\frac{a}{p}\right)$ simbolo di Legendre

$$G(a,p) = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right) e(ax/p) \qquad e(a) = e^{2\pi i a}$$

$$\left(\frac{0}{p}\right) = 0$$

$$\left(\frac{a}{p}\right) G(a,p) = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{ax}{p}\right) e(ax/p) \qquad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \checkmark$$

$$= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right) e(x/p)$$

$$= G(1,p)$$

$$\zeta = e^{2\pi i/p}$$

$$\sum_{a=0}^{p-1} G(a,p)G(-a,p) = \sum_{a=0}^{p-1}\sum_{j=0}^{p-1}\sum_{k=0}^{p-1} \left(\frac{j}{p}\right)\left(\frac{k}{p}\right) \zeta^{a(k-j)}$$

$$= \sum_{j=0}^{p-1}\sum_{k=0}^{p-1} \left(\frac{j}{p}\right)\left(\frac{k}{p}\right) p\, \delta(j,k)$$

$$= \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)^2 p = p(p-1).$$

$$= (p-1)\left(\frac{-1}{p}\right) G(1,p)^2$$

$$G(a,p) = \left(\frac{a}{p}\right) G(1,p)$$

$$\begin{cases} G(1,p) = \left(\frac{-1}{p}\right)\sqrt{p} \\ G(a,p) = \left(\frac{-a}{p}\right)\sqrt{p} \end{cases}$$

$$\sin\frac{2\pi}{7} + \sin\frac{4\pi}{7} + \sin\frac{8\pi}{7} = \frac{1}{2}\sqrt{7}$$

$$\sin z = \frac{e^{iz} - e^{-iz}}{2i}$$

$q \in \mathbb{R}$ Si dice algebrico su $\mathbb{Q}$ se $\exists\, p(x) \in \mathbb{Q}[x]$ per cui $p(q) = 0$

Se $q \in \mathbb{Q}$
$\cos(2\pi \cdot q)$

Quel è il minimo grado di un polinomio $p \in \mathbb{Q}[x]$ tale per cui $p(q) = 0$.

$\begin{cases} p(q) = 0 \\ q(q) = 0 \end{cases}$ $\partial p > \partial q$ $\exists r : r(q) = 0,\ \partial r < \partial p$

$\cos\frac{2\pi}{7}$ $T_7(x) = x \cdot Q(x)$ $\partial Q = 6$

$\cos\frac{2\pi}{7} = \frac{(e^{2\pi i/7} + e^{-2\pi i/7})}{2}$

$\left(\frac{x^7 - 1}{x - 1}\right) = \prod_{j=1}^{6} \left(x - e^{\frac{2\pi i}{7} \cdot j}\right)$

$= x^6 + x^5 + \dots + 1$

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

Claim
$x^k + \frac{1}{x^k}$ è un polinomio di grado k in $\left(x + \frac{1}{x}\right)$

$\left(x^3 + \frac{1}{x^3}\right) - \left(x + \frac{1}{x}\right)^3$

$\frac{x^7 - 1}{x - 1} = x^3 \cdot Q\left(x + \frac{1}{x}\right)$ $\partial Q = 3$

$A, B, C > 0$ $\quad f(A,B,C) = C(A+B+C) + \left(\frac{A-B}{2}\right)^2$

$$\sqrt{f(A,B,C)} + \sqrt{f(B,C,A)} + \sqrt{f(C,A,B)} \geq 2 \max\left(\sqrt{f(A,B,C)}, \sqrt{f(B,C,A)}, \sqrt{f(C,A,B)}\right).$$

Provare che $\forall \varepsilon > 0 \quad \exists A_\varepsilon \subseteq \mathbb{N}$ per cui

$$\left| 1 - \sum_{a \in A_\varepsilon} \frac{\sin(a^2)}{a} \right| \leq \varepsilon.$$

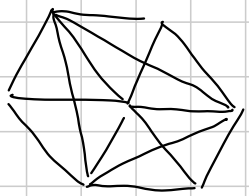
Scherzone!!!

$$\sum \frac{\sin n^2}{n}$$

$a = B + C \quad b = A + C \quad c = A + B$

Stewart $\quad m_a^2 = \frac{1}{2}b^2 + \frac{1}{2}c^2 - \frac{1}{4}a^2$

Le mediane di un t. formano un triangolo:



□.

$\{a_n\}_{n \in \mathbb{N}} \quad \left(\sum_{n \in \mathbb{N}} a_n\right)$ convergente se $\exists \lim_{N \to +\infty} \left(\sum_{n=1}^{N} a_n\right)$

assolutamente convergente $\exists \lim_{N \to +\infty} \left(\sum_{n=1}^{N} |a_n|\right)$

Teoremeccio. Se una serie è convergente
ma non assolutamente convergente
se ne può riarrangiare l'ordine di somma
in modo che la nuova serie
converga ad una qualunque costante.

$$\left|\sum_{n=1}^{N} a_n b_n\right| = \left|A_N b_N\right| - \left|\sum_{n=1}^{N-1} A_n (b_{n+1} - b_n)\right| \qquad \text{Sommazione per parti}$$

$$A_n \doteq \sum_{j=1}^{n} a_j$$

$a_n = e^{in^2}$ $\quad b_n = \frac{1}{n}$

$(|A_N| = o(n).)$

$b_{n+1} - b_n \sim \frac{1}{n^2}.$

Disuguaglianza di Weyl

$$\left|\sum_{n=M+1}^{M+N} \chi(n)\right| \ll \sqrt{N} \cdot \log N$$

GEOMETRIA 2 - Medium

Titolo nota 07/09/2011

(Metodi Algebrici)

1) Coordinate cartesiane

- $$\begin{cases} x^2+y^2+\alpha x+\beta y+\gamma=0 \\ x^2+y^2+\alpha' x+\beta' y+\gamma'=0 \end{cases}$$

$$\begin{cases} x^2+y^2+\alpha x+\beta y+\gamma=0 \\ (\alpha'-\alpha)x+(\beta'-\beta)y+\gamma'-\gamma=0 \end{cases}$$

asse radicale

— · —

- Se $\mathcal{C}$ e $\mathcal{C}'$ sono due parabole congruenti ottenute l'una dall'altra per una rotazione di $\frac{\pi}{2}$, allora $\mathcal{C}\cap\mathcal{C}'$ è fatto di punti concicli.

$$\begin{cases} y=x^2+ax+b \\ x=y^2+cy+d \end{cases}$$

$y=p(x)$ $\deg p(x)=2$

$$\begin{cases} y=kx^2+ax+b \quad (\circ) \\ x=ky^2+cy+d \quad (\circ\circ) \end{cases}$$

$$\begin{cases} y=kx^2+ax+b \\ kx^2+ky^2+(a-1)x+(c-1)y+b+d=0 \end{cases}$$

- Classificazione delle coniche

$$3x^2 + 4y^2 - 28xy + 2x - 3y + 1 = 0$$

$$3\left(x - \frac{14}{3}y\right)^2 - \frac{184}{3}y^2 + 2x - 3y + 1 = 0$$

$$\frac{196}{9}y^2$$

$$3\left(x - \frac{14}{3}y + \frac{1}{3}\right)^2 - \frac{184}{3}y^2 + \frac{19}{3}y + \frac{2}{3} \Longrightarrow \begin{cases} x' = ax + by + c \\ y' = dx + ey + f \end{cases}$$

$$-\frac{28}{3}y$$

$$3\square - \frac{184}{3}\square = k$$

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

$$x^2 - y^2 = 1$$

$$x + y^2 = 1$$

$$\alpha x^2 + 2\beta xy + \gamma y^2 + \dots$$

$$\left(\sqrt{\alpha}x + \frac{\beta}{\sqrt{\alpha}}y + \dots\right)^2 + y^2\left(\gamma - \frac{\beta^2}{\alpha}\right) + \dots$$

$$\gamma - \frac{\beta^2}{\alpha} = \frac{\alpha\gamma - \beta^2}{\alpha} = \frac{4\alpha\gamma - (2\beta)^2}{4\alpha}$$

>0 ellisse

$=0$ parabola

<0 iperbole

2) Vettori

- Baricentro di $ABC = \dfrac{\vec{A} + \vec{B} + \vec{C}}{3}$ Vale per ogni origine

- Ortocentro di $ABC = \vec{OA} + \vec{OB} + \vec{OC} = \vec{A} + \vec{B} + \vec{C}$ con origine in O = circocentro

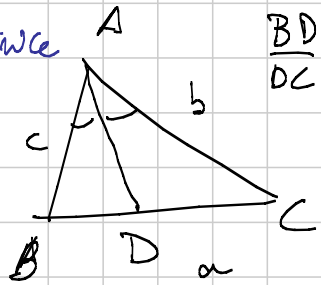
• Centro della c.p. di Feuerbach $= \frac{\vec{O}+\vec{H}}{2} = \frac{\vec{A}+\vec{B}+\vec{C}}{2}$

vero sempre

con origine in O.

• Incentro di $ABC = \frac{a\vec{A}+b\vec{B}+c\vec{C}}{a+b+c}$ vale per ogni scelta dell'origine

Perché? 1) Bisettrice



$\vec{D} = \frac{b\vec{B}+c\vec{C}}{b+c}$

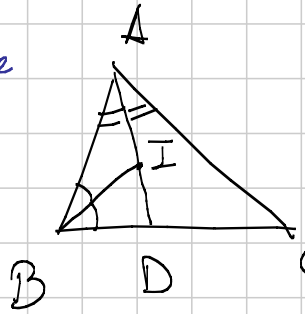
$\frac{BD}{DC} = \frac{AB}{AC} = \frac{c}{b}$

$\frac{DC}{BD} + 1 = \frac{b}{c} + 1$

$\frac{BC}{BD} = \frac{b+c}{c}$

$BD = \frac{ca}{b+c}$

2) Un'altra bisettrice



$\frac{AI}{ID} = \frac{AB}{BD}$

$= \frac{c}{ca}(b+c)$

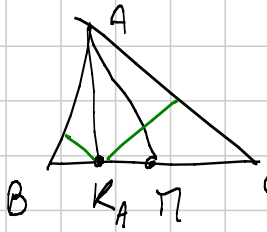
$\frac{AI}{ID} = \frac{b+c}{a}$

$\vec{I} = \frac{a\vec{A}+(b+c)\vec{D}}{a+b+c} = \frac{a\vec{A}+b\vec{B}+c\vec{C}}{a+b+c}$

• Punto di Lemoine di ABC = ?

SCARPA GIOACCHINO

1) Simmediana



AK_A simm. $\frac{d(K_A,AB)}{d(K_A,AC)} = \frac{d(M,AC)}{d(M,AB)} = \frac{2\cdot[ABC]/AC}{2[ABC]/AB} = \frac{AB}{AC} = \frac{c}{b}$

$\frac{BK_A}{K_AC}$ //

$$\frac{[ABK_A]}{[ACK_A]} = \frac{AB \cdot d(K_A, AB)}{AC \cdot d(K_A, AC)} = \frac{c}{b} \cdot \frac{c}{b} = \frac{c^2}{b^2}$$

2) Come per l'incentro $\Rightarrow \vec{K} = \dfrac{a^2\vec{A} + b^2\vec{B} + c^2\vec{C}}{a^2 + b^2 + c^2}$

Prodotto scalare: $\langle \vec{A}, \vec{B} \rangle \quad (\vec{A}, \vec{B}) \quad \vec{A} \cdot \vec{B}$

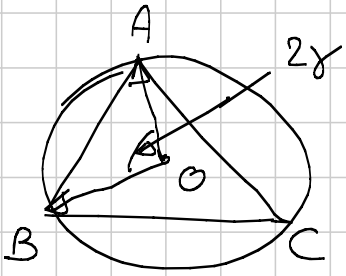
$$OH^2 = \vec{OH} \cdot \vec{OH} = (\vec{A}+\vec{B}+\vec{C}) \cdot (\vec{A}+\vec{B}+\vec{C}) =$$

con origine in O

$$= \underbrace{\vec{A}\cdot\vec{A} + \vec{B}\cdot\vec{B} + \vec{C}\cdot\vec{C}}_{3R^2} + 2(\vec{A}\cdot\vec{B} + \vec{B}\cdot\vec{C} + \vec{C}\cdot\vec{A})$$

1. def. di prod. scalare

$$X \cdot Y = \|X\| \cdot \|Y\| \cdot \cos X\hat{O}Y$$



$$\cos A\hat{O}B = \cos 2\gamma = \frac{2R^2 - c^2}{2R^2}$$

$$A \cdot B = R^2 \cdot \frac{2R^2 - c^2}{2R^2} = R^2 - \frac{c^2}{2}$$

2. proprietà del prodotto scalare

$$c^2 = (A-B)\cdot(A-B) = A\cdot A + B\cdot B - 2A\cdot B = 2(R^2 - A\cdot B)$$

$$A \cdot B = R^2 - \frac{c^2}{2}$$

$$\Rightarrow OH^2 = 3R^2 + 2(A\cdot B + B\cdot C + C\cdot A) = 3R^2 + 2\left(3R^2 - \frac{a^2+b^2+c^2}{2}\right) =$$

$$= 9R^2 - a^2 - b^2 - c^2.$$

• $OI^2 = (O-I)\cdot(O-I) = I\cdot I = \frac{1}{p^2}(aA+bB+cC)\cdot(aA+bB+cC) =$

(origine in O)

$= \frac{1}{p^2}\left((a^2+b^2+c^2)R^2 + (2ab+2bc+2ca)R^2 - abc(a+b+c)\right) =$

$R^2(a+b+c)^2$

$= \frac{1}{p^2}\left(R^2p^2 - abc\cdot p\right) = R^2 - \frac{abc}{p} = R^2 - \frac{abc}{4S}\cdot 2\cdot\frac{2S}{p} =$

$\underbrace{\quad}_{R} \qquad \underbrace{\quad}_{r}$

$= R^2 - 2Rr \qquad OI = \sqrt{R(R-2r)}$

Formula di Eulero

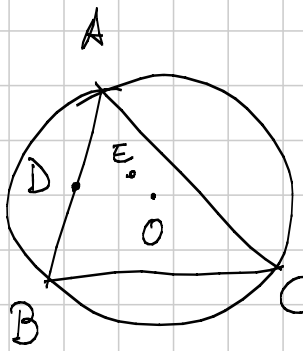
$r < \frac{R}{2}$

$OH = \sqrt{9R^2 - a^2 + b^2 - c^2}$

$4R^2\left(\frac{9}{4} - \sum \sin^2\alpha\right)$

$\frac{9}{4} \geq \sum \sin^2\alpha$

Ed:



E = baricentro di ΔACD

D = pt medio di AB

$CD \perp OE \iff AB = AC$

Sol (forse): Origine in O. La Tesi diventa

$(C-D)\cdot E = 0 \iff \|A-B\| = \|A-C\|$

$(A-B)\cdot(A-B) = (A-C)\cdot(A-C)$

$A\cdot A + B\cdot B - 2A\cdot B = A\cdot A + C\cdot C - 2A\cdot C$

origine in O

$A\cdot(B-C) = 0.$

(i) $D = \frac{A+B}{2}$

(ii) $E = \frac{A+C+D}{3} = \frac{A+C+\frac{A+B}{2}}{3} =$

$= \frac{3A+2C+B}{6}$

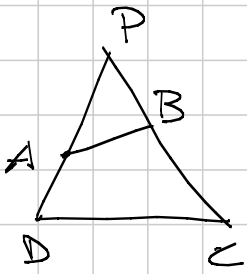
$$(C-D)\cdot E = \underbrace{\left(C-\frac{A+B}{2}\right)}_{\frac{2C-A-B}{2}}\cdot\left(\frac{3A+2C+B}{6}\right) =$$

$$= \frac{1}{12}\left(6C\cdot A + 4C\cdot C + 2C\cdot B - 3A\cdot A - 2A\cdot C - A\cdot B - 3A\cdot B - 2B\cdot C - B\cdot B\right) =$$

$$= \frac{1}{12}\left(A\cdot(6C-2C-B-3B)\right) = \frac{1}{12}A\cdot(4C-4B) =$$

$$= \frac{1}{3}A\cdot(C-B)$$

$$\frac{1}{3}A\cdot(C-B)=0 \iff A\cdot(B-C)=0 \qquad \square$$



E_1 (perp. da mediane) per cose:

O_1, H_1 circo-ortho-centre di PAB

O_2, H_2 circo/ortho-centre di PDC

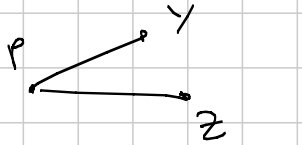
Le perp. da E_1 a CD
la perp da E_2 a AB $\Longleftarrow$
H_1H_2
concorrono.

E_i pr. med. di O_iH_i $i=1,2$

Inizio: P = origine $\qquad X_1 = (\text{perp da } E_1 \text{ a } CD)\cap H_1H_2$

$X_2 = (\text{perp. da } E_2 \text{ a } AB)\cap H_1H_2$

Se trovo che $X_1\cdot Y = X_2\cdot Y$, $X_1\cdot Z = X_2\cdot Z$ } Y, Z non allineati

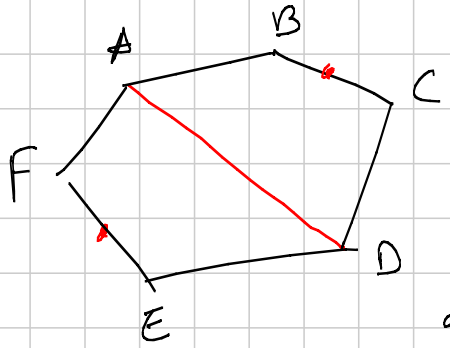


$X_1\cdot Y = \alpha$
$X_1\cdot Z = \beta$

$X_1 = \lambda Y + \mu Z$
λ, μ unici!

$X_1 = X_2$

Es:



$AD = BC + EF$
$BE = CD + FA \Rightarrow \frac{AB}{DE} = \frac{EF}{BC} = \frac{CD}{FA}$
$CF = AB + DE$

disug. triangolare

$$\|A-D\| = \|B-C\| + \|F-E\| \geq \|B-C+F-E\|$$
$$\|B-E\| = \|C-D\| + \|F-A\| \geq \|C-D+A-F\|$$
$$\|C-F\| = \|A-B\| + \|D-E\| \geq \|A-B-D+E\|$$

$X = A-D$
$Y = B-E$
$Z = C-F$

$\|X\| \geq \|Y-Z\|$
$\|Y\| \geq \|Z-X\|$
$\|Z\| \geq \|X-Y\|$

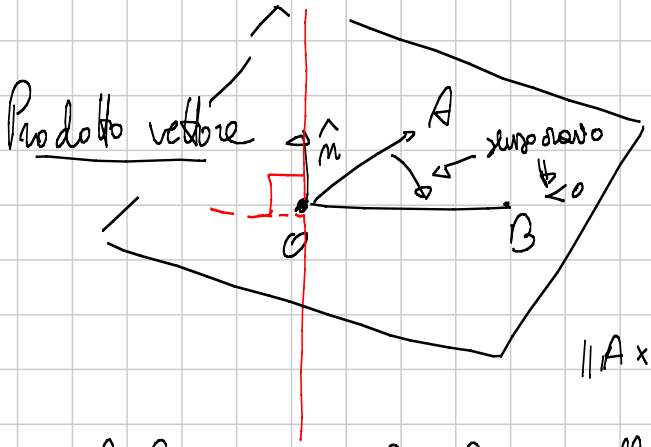
$L = \frac{Y+Z-X}{2}$
$M = \frac{X+Z-Y}{2}$
$N = \frac{X+Y-Z}{2}$

$Y - Z = L+N-(L+M) = N-M$

$\|M+N\| \geq \|M-N\|$
$\|L+N\| \geq \|L-N\|$
$\|L+M\| \geq \|L-M\|$

To be continued

Prodotto vettore



$A \times B = \|OA\| \cdot \|OB\| \cdot \sin \hat{AOB} \cdot \hat{n}$
$= OA \times OB$

angolo orientato

$\|A \times B\| = 2 \cdot [OAB]$

$A \times B = 0 \iff A, O, B$ sono allineati.

- proprietà: $(A+B)\times C = A\times C + B\times C$

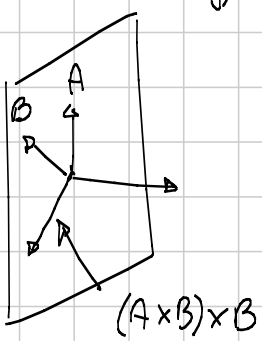
$A\times B = -B\times A$

$(\lambda A)\times B = \lambda(A\times B)$

$A\times A = 0$

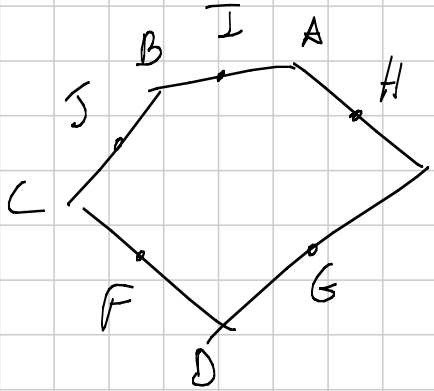
$A\times B\times C \qquad (A\times B)\times C \qquad A\times(B\times C)$

$B = C$ ⟶ $\| \; 0$



$A\times(B\times B) = 0.$

Es:



F, G, H, I, J pt. medi dei lati

AF, BG, CH, DI concorrono in P

⇓

anche EJ passa per P

$(A-P)\times(F-P) = 0$

$(B-P)\times(G-P) = 0$ ⟹ $(E-P)\times(J-P) = 0$

$(C-P)\times(H-P) = 0$

$(D-P)\times(I-P) = 0$

$$0=(A-P)\times\left(\frac{C+D}{2}-P\right)=\frac{A\times C}{2}+\frac{A\times D}{2}-A\times P-\frac{P\times C}{2}-\frac{P\times D}{2}+$$

$$0=\frac{B\times D}{2}+\frac{B\times E}{2}-B\times P-\frac{P\times D}{2}-\frac{P\times E}{2}+$$

$$0=\frac{C\times B}{2}+\frac{C\times A}{2}-C\times P-\frac{P\times E}{2}-\frac{P\times A}{2}+$$

$$0=\frac{D\times A}{2}+\frac{D\times B}{2}-D\times P-\frac{P\times A}{2}-\frac{P\times B}{2}+$$

$$0=0+0+0+\frac{C\times E}{2}+\frac{B\times E}{2}+0+0-\frac{C\times P}{2}-\frac{B\times P}{2}-P\times E=$$

$$\Downarrow$$

$$0=\frac{E\times B}{2}+\frac{E\times C}{2}-E\times P-\frac{P\times B}{2}-\frac{P\times C}{2}$$ ok

---

Fissato un triangolo ABC, per ogni P del piano esiste un'unica terna (α,β,γ) di numeri reali t.c. $\alpha+\beta+\gamma=1$ e $P=\alpha A+\beta B+\gamma C$

Dim: $P=\alpha A+\beta B+\gamma C \qquad \alpha+\beta+\gamma=1$

$$2\cdot[PAB]=\|(B-P)\times(A-P)\|=\|(-\alpha A+(1-\beta)B-\gamma C)\times((1-\gamma)A-\beta B-\gamma C)\|=$$

$$=\|\alpha\beta\, A\times B+\alpha\gamma\, A\times C+\underbrace{(1-\alpha)(1-\beta)}_{1-\alpha-\beta+\alpha\beta}B\times A-\beta(1-\beta)B\times C-\gamma(1-\alpha)C\times A+\gamma\beta\, C\times B\|=$$

$$=\|A\times B\underbrace{(\alpha\beta-\alpha\beta-(1-\alpha-\beta))}_{-\gamma}+B\times C\underbrace{(-\gamma+\gamma\beta-\gamma\beta)}_{-\gamma}+$$

$$+CxA\left(-\alpha\gamma - \gamma + \alpha\gamma\right)\| = |\gamma|\,\|A\times B + B\times C + C\times A\| =$$

$$= |\gamma|\,\|(C-B)\times(A-B)\| = |\gamma|\cdot 2\,[ABC]$$

$$\frac{[PAB]}{[ABC]} = |\gamma|$$

se usiamo le aree orientate $\Rightarrow \dfrac{[PAB]}{[ABC]} = \gamma$

$[ABC] > 0$
se A, B, C sono in senso antiorario

$=0$ dati α, β, γ P è sempre univocamente determinato dato P, ho $\alpha = \dfrac{[PBC]}{[ABC]}$, ...

Teorema: A, B, C D, E, F misti

$$\frac{BD}{DC} = \frac{\lambda_2}{\lambda_1} \qquad \frac{CE}{EA} = \frac{\mu_2}{\mu_1} \qquad \frac{AF}{FB} = \frac{\nu_2}{\nu_1}$$

$$\lambda_1 + \lambda_2 = 1$$
$$\mu_1 + \mu_2 = 1$$
$$\nu_1 + \nu_2 = 1$$

$$\lambda_2\mu_2\nu_2 = -\lambda_2\mu_1\nu_1$$

$\Updownarrow$

D, E, F allineati.

$$D = \lambda_1 B + \lambda_2 C$$
$$E = \mu_1 C + \mu_2 A$$
$$F = \nu_1 A + \nu_2 B$$

Vogliamo $F = \alpha D + \beta E \qquad \alpha + \beta = 1$

$\Updownarrow$

$$\alpha\lambda_1 B + \alpha\lambda_2 C + \beta\mu_1 C + \beta\mu_2 A = \nu_1 A + \nu_2 B$$

$$(\alpha\lambda_1 - \nu_2)B + (\alpha\lambda_2 + \beta\mu_1)C + (\beta\mu_2 - \nu_1)A = 0$$

Oss: $(\alpha\lambda_1 - \nu_1) + (\alpha\lambda_2 + \beta\mu_1) + (\beta\mu_2 - \nu_2) =$

$= \alpha(\lambda_1 + \lambda_2) + \beta(\mu_1 + \mu_2) - (\nu_1 + \nu_2) =$

$= \alpha + \beta - 1 = 0.$

Oss 2: Se ogni coeff. è 0

$$\begin{cases} \alpha\lambda_1 = \nu_1 & \beta = \dfrac{\nu_2\lambda_2}{\mu_1\lambda_1} \\ \beta\mu_2 = \nu_2 & \beta = \dfrac{\nu_1}{\mu_2} \\ \alpha\lambda_2 + \beta\mu_1 = 0 & \alpha = -\beta\dfrac{\mu_1}{\lambda_2} \end{cases} \qquad \frac{\mu_2\nu_2\lambda_2}{\mu_1\nu_2\lambda_1} = -1 \iff \exists\, \alpha, \beta$$

Oss 3: Sa che $\exists\, x, y, z$ t.c. $x+y+z=1$

$0 = xA + yB + zC.$

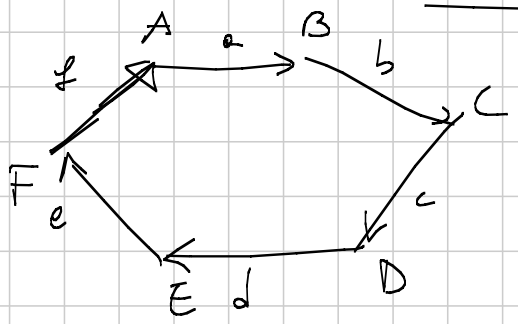
Se $\exists\, u, v, w$ t.c. $u+v+w=0$

$0 = uA + vB + wC$

$r + s + t = \overset{(x+y+z)}{+} \underset{(u+v+w)}{} = 0 + 1 = 1$ $\quad 0 = (x+u)A + (y+v)B + (z+w)C$

$r = x+u$, $s = y+v$, $t = z+w$

$\Rightarrow r = x$, $s = y$, $t = z$ $\Rightarrow u = v = w = 0.$



$B - A = a$ $\quad A - F = f$

$C - B = b$

$D - C = c$ $\quad a+b+c+d+e+f = 0$

$E - D = d$

$F - E = e$

$$AD = a+b+c = -d-e-f = \frac{1}{2}(a+b+c-d-e-f)$$

$B-A$ $\qquad$ $\dfrac{x-y+z}{2}$

$x = a-d$

$y = e-b$

$z = c-f$

$AD = BC + EF$

$$\left|\frac{x-y+z}{2}\right| = |b|+|e| \geq |b-e| = |y|$$

$$\left|\frac{y+z-x}{2}\right| \geq |x|$$

$$\left|\frac{x+y-z}{2}\right| \geq |z|$$

$$\frac{x-y+z}{2} = \ell$$

$$\frac{y+z-x}{2} = m$$

$$\frac{x+y-z}{2} = n$$

$$|\ell| \geq |m+n|$$

$$|m| \geq |n+\ell|$$

$$|n| \geq |\ell+m|$$

$$\ell+m+n = \frac{1}{2}(x+y+z)$$

$$|\ell+m+n|^2 = |\ell|^2+|m|^2+|n|^2+2(\ell m+n\ell+mn)$$

$$|\ell|^2 \geq |m+n|^2 = |m|^2+|n|^2+2\,m\cdot n$$

$$|m|^2 \geq |n|^2+|\ell|^2+2\ell n$$

$$|n|^2 \geq |m|^2+|\ell|^2+2\ell m$$

$$|\ell|^2+|m|^2+|n|^2 \geq 2(|\ell|^2+|m|^2+|n|^2)+2(\ell m+\ell n+mn)$$

$$0 \geq \|\ell+m+n\|^2 \Longrightarrow \ell+m+n=0$$

$$\Rightarrow x+y+z=0$$

$\Rightarrow$ parallelismo $\Rightarrow$ ..., $\square$

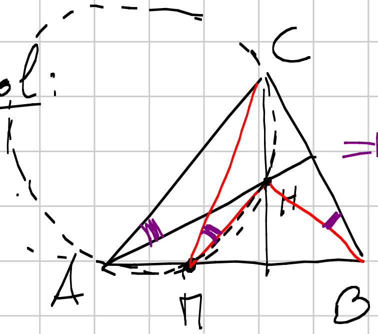
———— • ———— APMO – 2010

ABC Triangolo acutangolo, $AB > BC$, $AC > BC$.

O, H. Circonf. circo a AHC interseca AB in M $\neq A$.
Circonf. circo a AHB interseca AC in N $\neq A$.

$\Rightarrow$ Circocentro di MNH sta su OH

Sol:



$\Rightarrow$ M simm. di B risp. ad HC.
N simm. di C risp. ad HB
O = origine, cf. circo ad AB è unitaria
$h = a+b+c$

$$x \to x - c \to (x-c)\frac{\bar h - \bar c}{|\bar h - \bar c|} \to (\bar x - \bar c)\frac{h-c}{|h-c|} \to (\bar x - \bar c)\Big[\ \Big] \to +c$$

$$m = a + c - \frac{ab}{c}$$

$$n = a + b - \frac{ac}{b}$$

Oss: Circocentro di O, x, y $= z$

$$\begin{cases} \dfrac{z - \frac{x}{2}}{x/2} = -\dfrac{\bar z - \frac{\bar x}{2}}{\bar x/2} \\[2ex] \dfrac{z - \frac{y}{2}}{y/2} = -\dfrac{\bar z - \frac{\bar y}{2}}{\bar y/2} \end{cases} \qquad \begin{cases} \dfrac{2z}{x} - 1 = 1 - \dfrac{2\bar z}{\bar x} \\[2ex] \dfrac{2z}{y} - 1 = 1 - \dfrac{2\bar z}{\bar y} \end{cases}$$

$$z\left(\frac{\bar{x}}{x}-\frac{\bar{y}}{y}\right)=\bar{x}-\bar{y}$$

$$z=\frac{xy(\bar{x}-\bar{y})}{\bar{x}y-x\bar{y}}$$

Oss: $h\to 0$ $\quad m\to m-h$ $\quad n\to n-h$

$m-h=-\frac{ab}{c}-b$ $\qquad$ $n-h=-\frac{ac}{b}-c$

$-\frac{b}{c}(a+c)$ $\qquad$ $-\frac{c}{b}(a+b)$

$$w=\frac{-(a+c)(a+b)\left(\frac{c}{b}\left(\frac{1}{a}+\frac{1}{c}\right)-\frac{b}{c}\left(\frac{1}{a}+\frac{1}{b}\right)\right)}{\frac{c}{b}\frac{c}{b}\left(\frac{1}{a}+\frac{1}{c}\right)(a+b)-\frac{b}{c}\frac{b}{c}(a+c)\left(\frac{1}{a}+\frac{1}{b}\right)}=$$

$$=-(a+c)(a+b)\left(\frac{c}{ba}+\frac{1}{b}-\frac{b}{ca}-\frac{1}{c}\right)=\frac{c^2+ac-b^2-ab}{abc}$$

$(c+b)(c-b)+a(c-b)$

$(c-b)(a+b+c)$

$$\frac{c^2}{b^2a}(a+b)+\frac{c}{b^2}(a+b)-\frac{b^2}{c^2a}(a+c)-\frac{b}{c^2}(a+c)$$

$$\frac{c^2}{b^2}+\frac{c^2}{ab}+\frac{ac}{b^2}+\frac{c}{b}-\frac{b^2}{c^2}-\frac{b^2}{ac}-\frac{ab}{c^2}-\frac{b}{c}=$$

$$=\frac{ac^4+c^4b+a^2c^3+abc^3-ab^4-b^4c-a^2b^3-ab^3c}{ab^2c^2}=$$

$$=\frac{c^4(a+b)+a^2(c^3-b^3)-b^4(a+c)+abc(c^2-b^2)}{ab^2c^2}=$$

$$=\frac{a(c^4-b^4)+cb(c^3-b^3)+a^2(c^3-b^3)+abc(c^2-b^2)}{ab^2c^2}$$

$$-\frac{(a+c)(a+b)(c+b)(a+b+c)\frac{1}{abc}}{(c+b)\left[(c^2+b^2)(c+b)a+(cb+a^2)(a^2+bc+b^2)+abc(c+b)\right]}$$

ab^2c^2 $\quad c^3a+c^2ba+b^2ca+b^3a+abc^2+ab^2c$

$ca(c^2+cb+b^2)+ab(b^2+c^2+bc)$

$$= \frac{-(a+c)(a+b)(a+b+c)bc}{(a^2+ab+ac+cb)(c^2+bc+b^2)} = -\frac{bc}{c^2+bc+b^2}(a+b+c) = u$$

$$\frac{u}{u} = \frac{\overline{u}}{\overline{u}} \qquad s=0 \ u, u, 0 \text{ allineati}$$

$$\frac{u}{u} = \frac{\overline{u}}{\overline{u}} \qquad \frac{u}{u} = \frac{-bc}{c^2+bc+b^2}$$

$$\frac{\overline{u}}{\overline{u}} = \frac{-\frac{1}{bc}}{\frac{1}{c^2}+\frac{1}{bc}+\frac{1}{b^2}} = \frac{-\frac{1}{bc}bc}{\frac{b^2+bc+c^2}{b^2c^2}} = -\frac{bc}{c^2+bc+b^2}$$

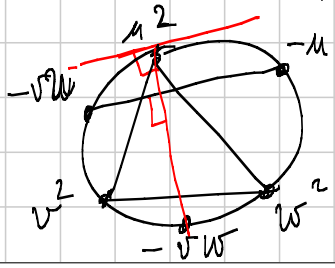
1) distanza tra I e il centro della cp. dei 9 punti

O = origine

Claim: $\exists\, u, v, w$ numeri complessi sulla cp. unitaria

t.c. $A=u^2 \quad B=v^2 \quad C=w^2$

e $-uv, -vw, -uw$ sono le altezze rispettivamente di AI, BI, CI con la cp. unitaria



$A'=-vw \quad B'=-uw \quad C'=-uv$

$\Rightarrow I =$ ortocentro di $A'B'C'$

$I = -uv - vw - uw \qquad F = \frac{u^2+v^2+w^2}{2}$

$|IF| = |F - I| = \left| \frac{u^2+v^2+w^2+2uv+2vw+2uw}{2} \right| =$

$= \left| \frac{(u+v+w)^2}{2} \right| \qquad |OI| = |I| = |-uv-vw-uw| =$

$= |uvw| \cdot \left| \frac{1}{w} + \frac{1}{v} + \frac{1}{u} \right| = |uvw| \left| \bar{w} + \bar{v} + \bar{u} \right| =$

$= |uvw| \left| \overline{u+v+w} \right| = \underbrace{|uvw|}_{1} |u+v+w|$

$R = 1$

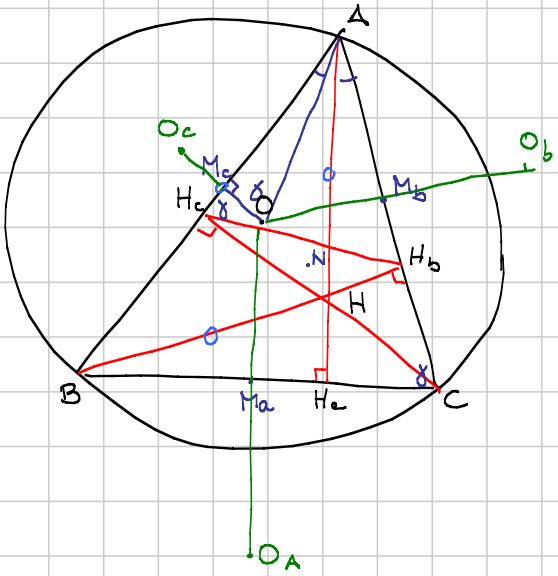
$IF = \frac{10^2}{2} = \frac{R^2 - 2Rr}{2} = \frac{1-2r}{2} = \frac{1}{2} - r$

raggio della circ. di Feuerbach

SENIOR 2011 - G3 MEDIUM

Titolo nota 08/09/2011

Circocentro e ortocentro



① AH_bH_aB è ciclico.

② AH_bHH_c è ciclico.

③ $B\hat{A}O = H\hat{A}C$

(sono entrambi $90-\gamma$)

④ $A\hat{B}C$ è simile a $A\hat{H}_cH_b$

(da ①)

⑤ O è ortocentro di $M_aM_bM_c$

($M_aO \perp BC \parallel M_bM_c$)

⑥ H è incentro di $H_aH_bH_c$

(angoli)

⑦ $OA \perp H_bH_c$

($H_c\hat{A}O = 90-\gamma$, $AH_c\hat{H}_b = \gamma$ ...)

(2° modo: omotetia di centro A + simm rispetto alla bisettr manda $ABC \to AH_bH_c$, manda $AH_a \to AO$, che quindi è altezza del nuovo triangolo AH_bH_c).

⑧ A, B, C, H è sistema ortocentrico

⑨ $H_aH_bH_c$ e $M_aM_bM_c$ hanno la stessa circonf circoscr, il centro è il pto medio di OH.

⑩ Circonf circoscr a ABC, HBC, HAB, HAC sono congruenti.

(il simmetrico di H rispetto a AB sta su Γ_{ABC}.
$\Rightarrow \Gamma_{ABH}$ è la simmetrica di Γ_{ABC} rispetto ad AB)

⑪ I loro circocentri formano un sist ortocentrico congruente al primo.

(O_A, O_B, O_C, O si ottengono da ABCH facendo un'omot di centro G e rapporto $\frac{1}{2}$ e poi un'omot di centro O e rapporto 2).

(2° modo $AB \parallel M_aM_b \parallel O_aO_b$. $AB = 2M_aM_b = O_aO_b$)

(12) AO_a, BO_b, CO_c concorrono nel centro della circ di Feuerbach di ABC

(A,B,C,H si ottiene da $O_A O_B O_C O$ mediante una simm centrale, perchè la composiz di omotetie è ancora un'omotetia di rapporto il prodotto dei precedenti. H deve andare in O quindi il centro è il pto medio di OH)

(13) H è centro radicale per ogni terna di circonferenze che hanno ciascuna un'altezza di ABC come corda.

(dobbiamo dimostrare

$AH \cdot HH_a = BH \cdot HH_b = CH \cdot HH_c$.

(*) segue dalla ciclicità di AH_aH_bB)

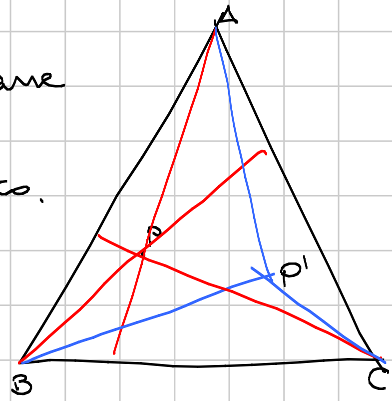
(2ª dim di (12): la circonf di Feuerbach di ABH è la stessa di ABC.

O_c, N, C sono circoc, centro di Feuerbach, ortoc di HAB. Quindi sono allineati e si bisecano.

Quindi O_c si ottiene da C mediante simm centr di centro N)

Coniugato isogonale

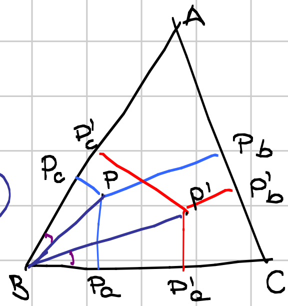
Dato P in ABC, simmetrizzo le ceviane rispetto alle bisettrici.
Concorrono in P' per Ceva Trigonometrica.
P' è detto coniugato isogonale di P.



Teorema: P' coniug isog di P ⟹ le proiez sui lati di P e P' sono concicliche.

Esempi di coniug isog: ① Circoc - ortoc
② Incentro resta in sè
③ Baric e pto di incontro delle simmed.

Dim
Mostriamo intanto che sono conciclici a 4 a 4: lo vediamo su $P_aP'_aP_cP'_c$.
E' suff dimostrare che (ciclicità "metrica")
$BP_c \cdot BP'_c = BP_a \cdot BP'_a$. (Ex: dimostrare e' equivalenza)



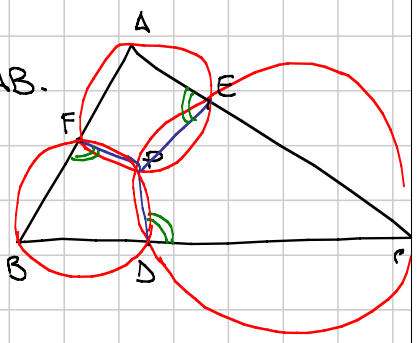
Calcoliamo
$BP_c = BP \cdot \cos A\hat{B}P$
$BP'_c = BP' \cdot \cos A\hat{B}P'$
$BP_a = BP \cdot \cos C\hat{B}P$
$BP'_a = BP' \cdot \cos C\hat{B}P'$.
Quindi
$BP_c \cdot BP'_c = BP \cdot BP' \cdot \cos A\hat{B}P \cdot \cos A\hat{B}P' = BP_a \cdot BP'_a$.
$A\hat{B}P = P'\hat{B}C \qquad A\hat{B}P' = P\hat{B}C$

Oss: il centro della circo è il pto medio di PP' (incontro degli assi di $P_aP'_a$ e $P_cP'_c$)

Se due circonf coincidono, ok.
Se fossero tutte diverse, l'asse radicale di una coppia di queste circo sarebbe un lato del triangolo.
Ma gli assi radicali devono concorrere!!!

Teorema di Miquel

ABC triangolo, D, E, F su. lati BC, CA, AB.
$\Rightarrow$ le circonf circoscr a BDF, CDE, AEF concorrono.

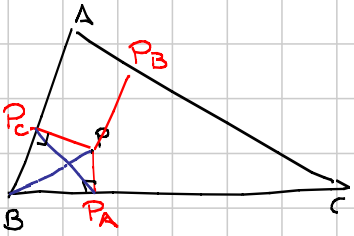


Dim!
$P = \Gamma_{BDF} \cap \Gamma_{CDE}$
Dobbiamo dim AFPE è ciclico.
$B\hat{F}P = P\hat{D}C = P\hat{E}A$.
↑ BDFP ciclico ↖ DCEP ciclico

Def: se $\hat{C}$ è retto, il triangolo DEF si dice PEDALE

Teorema (Simson Wine)

ABC triangolo, P_a, P_b, P_c proiez di P sui lati. Allora
P_A, P_B, P_C sono allineati. $\Leftrightarrow P \in \Gamma_{ABC}$.



Dim!
Calcoliamo la lungh dei lati del triangolo pedale
$P_A P_C = 2R_{\Gamma_{BP_AP_CP}} \cdot \sin\hat{B}$
↑ teo dei seni su BP_AP_C
$= BP \cdot \sin\hat{B}$
↑ BP è diametro
$= BP \ \frac{b}{2R}$

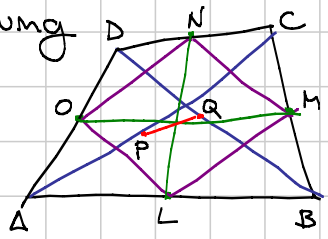
$P_A P_B P_C$ sono allineati: $\Leftrightarrow$
$P_AP_B \pm P_AP_C \pm P_BP_C = 0$
$\Leftrightarrow CP \cdot c \pm BP \cdot b \pm AP \cdot a = 0$
Weag + −.
Per il teo di Tolomeo vale $\geq$ sempre, con $=$
↳ applicato a ABPC

se e solo se P, A, B, C conciclici.

Quadrilateri

Fatto 1: ABCD quadrilatero. I segmenti: congiung. punti med. di lati opposti e pti med. di diag concorrono e si bisecano.

Dim 1: vettori.



Fatto 2: come in figura, OLMN è un parallelogrammo.

Dim del fatto 2: Talete!

$LB = \frac{1}{2} AB$ $\quad BM = \frac{1}{2} BC$ $\Rightarrow$ per Talete $LM \parallel AC$ e $LM = \frac{1}{2} AC$

Similm, per Talete $ON \parallel AC$ e $ON = \frac{1}{2} AC$.

Dim fatto 1 dato il 2:

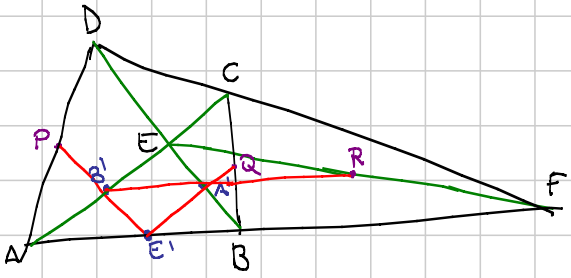
OM e LN si bisecano

Oss: il fatto 2 vale con quadrilateri intrecciati!

Quindi lo applichiamo a ACBD

PQ e OM si bisecano
Allora il pto medio di OM è anche pto medio di LN e di PQ. □

Teorema (linea di Gauss)
ABCD quadrilatero, $E = AC \cap BD$
$F = AB \cap CD$,
P pto medio di AD
Q " " " BC
R " " " EF.
Allora P, Q, R sono allineati.



Dim 1: geometria analitica (magari dopo un'affinità)
Dim 2: chiamiamo
A' pto medio di EB
E' " " " AB
B' " " " AE
Abbiamo P, B', E' allineati etc.
Usiamo Menelao per mostrare allineamento (triangolo $\hat{A'B'E'}$, "retta" PQR)
Basta quindi dimostrare

$$\frac{EQ}{QA'} \cdot \frac{A'R}{RB'} \cdot \frac{B'P}{PE'} \stackrel{?}{=} -1$$

LHS

$$LHS = \frac{AC}{CE} \cdot \frac{BF}{FA} \cdot \frac{ED}{DB} = -1$$

Talete $ABC \sim AE'Q$... ; Menelao su $\hat{AEB}$, retta CFD.

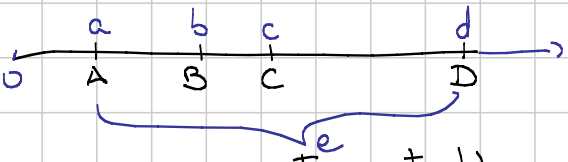
Dim 3 Consideriamo il luogo dei pti Z t.c.

$$[ABZ] + [CDZ] = [ACZ] + [BDZ]$$

Si vede che $Z = P, Q, R$ verificano. [Ex].
La funzione $Z \to [ABZ]$ è lineare.
Allora $Z \to [ABZ] + [CDZ] - [ACZ] - [BDZ]$ è somma di funz lineari $\Rightarrow$ lineare.
Il luogo di zeri può essere un pto, una retta, il piano
$\Rightarrow$ il luogo è una retta per P, Q, R. (uno ci sono P,Q,R no A non c'è)

Birapporto

$$(A,B;C,D) = \frac{AC \cdot BD}{AD \cdot BC}$$



Si considerano segmenti con segno; un punto potrebbe essere ∞.

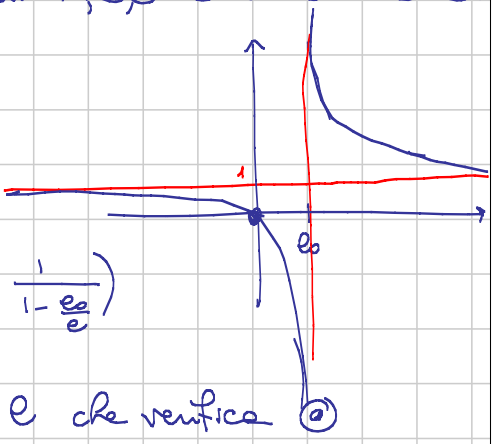
Oss: quando $(A,B;C,D) = 1$? Se e solo se $C=D$ o $A=B$.

Dim:

(a) $\frac{AC}{BC} = \frac{AD}{BD}$. Pensiamo fissati A,B,C. Dove deve stare D?

Se $D=C$ ok.

(b) equivale a $\frac{AC}{BC} = \frac{e}{e-AB}$. $\odot$



Disegnamo la funz $e \to \frac{e}{e-e_0}$

È monotona (facendo la deriv $\frac{1}{1-\frac{e_0}{e}}$)

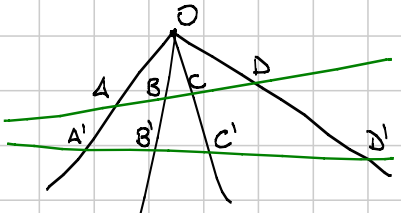
in $(e_0,+\infty)$ e $(-\infty,e_0)$

Per $\frac{AC}{BC} \neq 1$, c'è esattam un e che verifica $\odot$

Per $\frac{AC}{BC} = 1$, abbiamo $A=B$.

Prop: come in figura. Si ha che

$$(A,B;C,D) = (A',B';C',D')$$



Dim:

Scriviamo $(A,B;C,D)$ in funz degli angoli in O.

$$(A,B;C,D) = \frac{AC \cdot BD}{AD \cdot BC}$$

Per il Teo dei seni su ACO

$$\frac{AC}{\sin A\hat{O}C} = \frac{AO}{\sin O\hat{C}A}$$

In modo simile

$$\frac{BD}{\sin B\hat{O}D} = \frac{OB}{\sin O\hat{D}B} \qquad \frac{AD}{\sin A\hat{O}D} = \frac{AO}{\sin O\hat{D}A} \qquad \frac{BC}{\sin B\hat{O}C} = \frac{OB}{\sin O\hat{C}A}$$

$$(A,B;C,D) = \frac{\sin A\hat{O}C \cdot AO}{\sin O\hat{C}A} \cdot \frac{\sin B\hat{O}D \cdot OB}{\sin O\hat{D}B} \cdot \frac{\sin O\hat{D}A}{\sin A\hat{O}D} \cdot \frac{1}{OA} \cdot \frac{\sin O\hat{C}A}{\sin B\hat{O}C} \cdot \frac{1}{OB}$$

È indipendente dalla retta trasversale.

Conseguenza: posso def il birapp tra 4 rette concorrenti (interseco con una secante a caso e calcolo il birapp delle intersezioni. Per la prop non dipende dalla secante)

Oss: cosa succede al birapp permutando i punti?

$\lambda = (A,B;C,D) \Rightarrow (B,A;C,D) = ? = \frac{BC\cdot AD}{AC\cdot BD} = \frac{1}{\lambda}$

Permutando A,B,C,D i birapporti che posso ottenere sono 6:

$$\left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, 1-\frac{1}{\lambda}, \frac{\lambda}{\lambda-1}\right\}$$

Esempio: $(A,B;C,D)+(A,C;B,D) = 1$

$$\frac{(c-a)(d-b)}{(d-a)(c-b)} + \frac{(b-a)(d-c)}{(d-a)(b-c)} \stackrel{?}{=} 1$$

Li guardo come polinomi in a,b,c,d. Riscrivo

$(c-a)(d-b) - (b-a)(d-c) \stackrel{?}{=} (d-a)(c-b)$

$d-a \mid LHS$ (metto $a=d$, si annulla)

$c-b \mid LHS$ (" $c=b$, " ")

LHS è di 2° grado, quindi LHS e RHS differiscono al più di un fattore numerico.

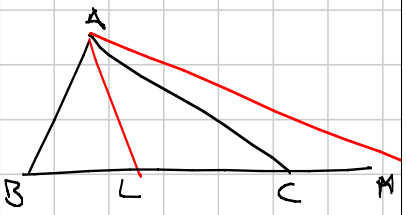
Ma il coeff di cd è 1. (Oppure $a=5$ $b=2$ $c=1$ $d=0$)

Def: A,B,C,D allineati. Se $(A,B;C,D) = -1$ allora si chiama quaterna armonica.

Esempio 1: vertici e piedi delle bisettrici

$(B,C;L,M) = -1$

(usare il teo della bis due volte)

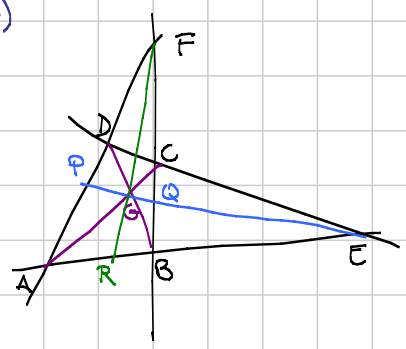


Esempio 2: ABCD quadrilatero

$E = AB\cap CD$, $F = AD\cap BC$

$G = AC\cap BD$

Allora $(E,G,P,Q) = -1$.



Corollario: $(E,R;A,B) = -1$

Dim coroll: proiettiamo da F la retta PGQE sulla retta ARBE, usiamo la prop.

Dim esempio 2:

$(E,G;P,Q) = (D,A;P,F)$

↑ proiett con centro C sulla retta FD

$= (G,E;P,Q)$

↑ proietto da B su EQ

Da ⊙, $= (E,G;P,Q)^{-1}$

Quindi

$(E,G;P,Q) = \begin{cases} 1 \\ \text{oppure} \\ -1 \end{cases}$ ⇝ no perché i pti sono distinti.

Altra dim:

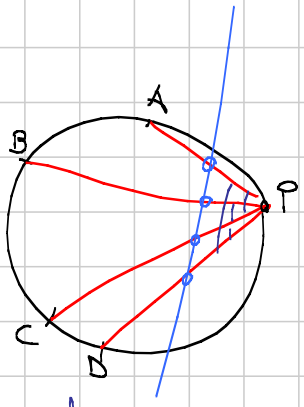
Menelao su ABF con retta QDE + Ceva.

[Ex].

Binapporti e circonferenze (coniche)

Def: dati 4 pti A,B,C,D su Γ circonf, $P \in \Gamma$

$(A,B;C,D)_P$ = binapporto tra PA, PB, PC, PD.



Oss: non dipende da P

Dim: abbiamo scritto il binapp in funzione dei soli angoli.

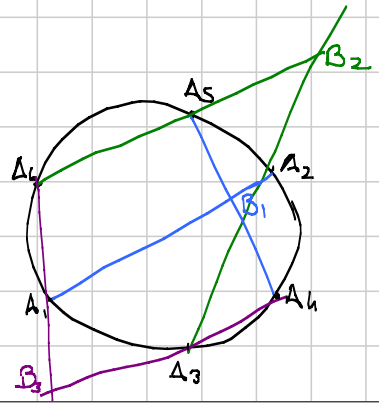
Teorema di Pascal

$A_1, \dots, A_6$ su una (conica) circonf

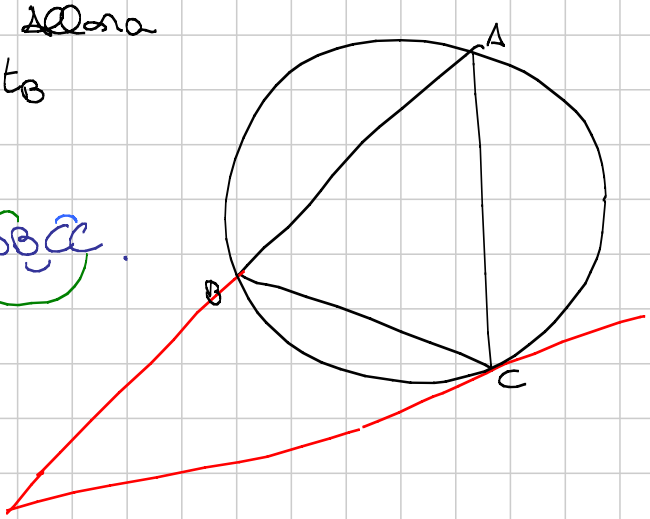
$B_i = A_iA_{i+1} \cap A_{i+3}A_{i+4}$ con $i = 1,\dots,3$

Allora B_1, B_2, B_3 sono allineati.

Dim: (coi binapporti)



Esempio: ABC Triangolo. Allora $AB \cap t_C$, $BC \cap t_A$, $AC \cap t_B$ sono allineati.



Dim: Pascal su $AABBCC$.

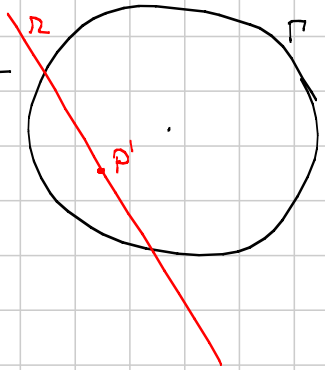
Polarità

Γ circonferenza.

Definiamo la mappa di Dualità

$$\{\text{punti del piano}\} \longrightarrow \{\text{rette del piano}\}$$

$$P \longrightarrow r \text{ t.c. } r \perp OP,\ \operatorname{dist}(r,O) = \frac{R_\Gamma^2}{OP}$$

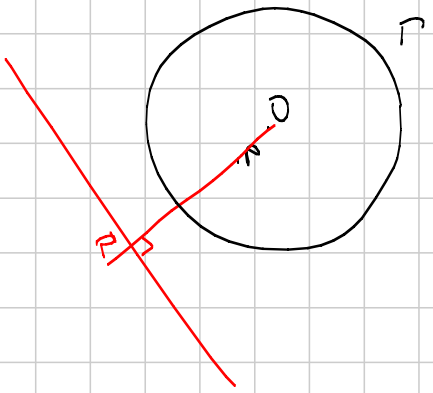


r si indica con $\operatorname{pol}_\Gamma(P)$

Questa mappa è invertibile

$$\{\text{rette}\} \longrightarrow \{\text{pti}\}$$

$$r \longrightarrow P,\quad \operatorname{pol}_\Gamma^{-1}(r)$$



Proprietà

① $P \in \Gamma \iff P \in \text{pol}_\Gamma P$

② La polarità rovescia le inclusioni:

$P \in r \iff \text{pol}\, P \ni \text{pol}\, r$

(chiamo $P' = \text{pol}\, P \cap OP$

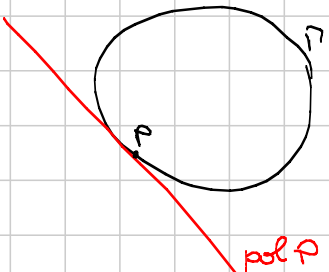
$Q = \text{pol}\, P \cap OR$

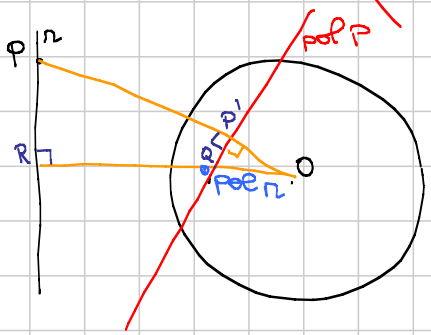
È sufficiente dimostrare che

$OQ \cdot OR \overset{?}{=} r_\Gamma^2$

$OQ \cdot OR = OP' \cdot OP = r_\Gamma^2$

↑ $PRQP'$ è ciclico





③ $\text{pol}(P) \cap \text{pol}(Q) = \text{pol}(PQ)$

(usiamo ②. $P \in PQ \Rightarrow \text{pol}\, PQ \in \text{pol}\, P$

$Q \in PQ \Rightarrow \text{pol}\, PQ \in \text{pol}\, Q$

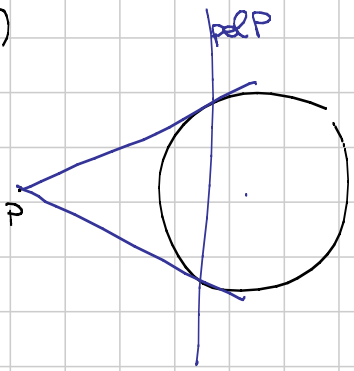
$\Rightarrow$ sta su $\text{pol}\, P \cap \text{pol}\, Q$)

④ $\text{pol}(r \cap s)$ = retta per $\text{pol}(r)$ e $\text{pol}(s)$

(ex)

⑤ La polare di P è la congiungente delle due tangenti a Γ

(ex)

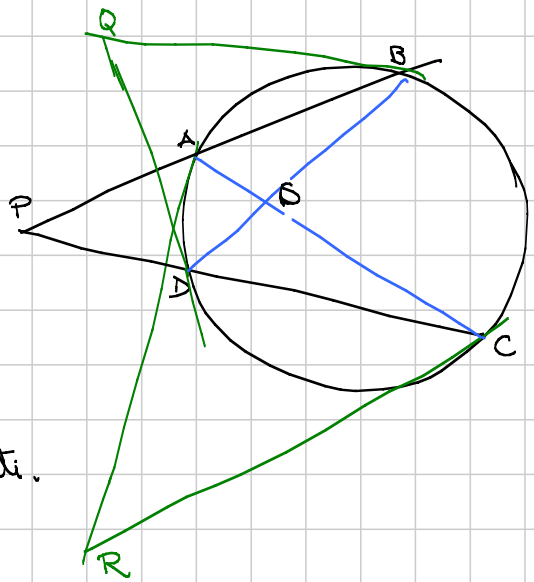


Lemma della polare I

$ABCD$ ciclico, $P = AB \cap CD$.

$S = AC \cap BD$.

Allora $S \in \text{pol}\, P$



Dim:

Pascal su $\triangle ABCCD$

R P $BC \cap DA$ sono allineati.

Pascal su $BBADDC$

Q P $BC \cap DA$ sono all.

In verità R, P, Q, $BC \cap DA$ sono allineati.
$\parallel$ pol AC $\parallel$ pol BD

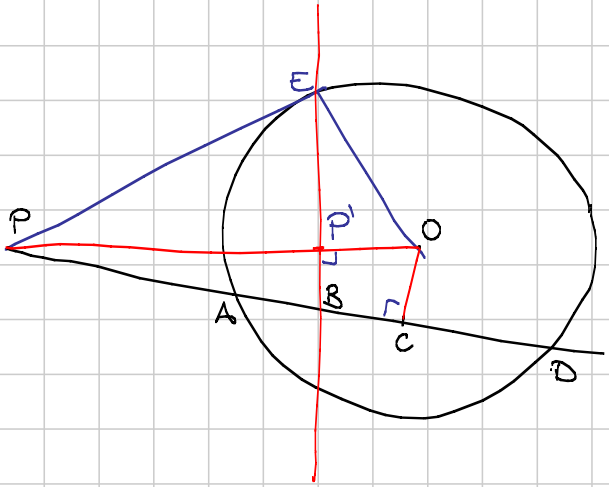
$P \in$ retta per pol AC e pol BD $=$ pol $AC \cap BD$ = pol S
(uso ⑤)

Poi uso ②.

Lemma della polare 2

C = pto medio di AD

$B = PA \cap$ pol P

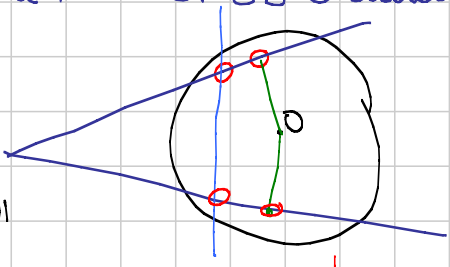


Allora si ha che
① $PA \cdot PD = PB \cdot PC$
② $(A, D; P, B) = -1$

Dim

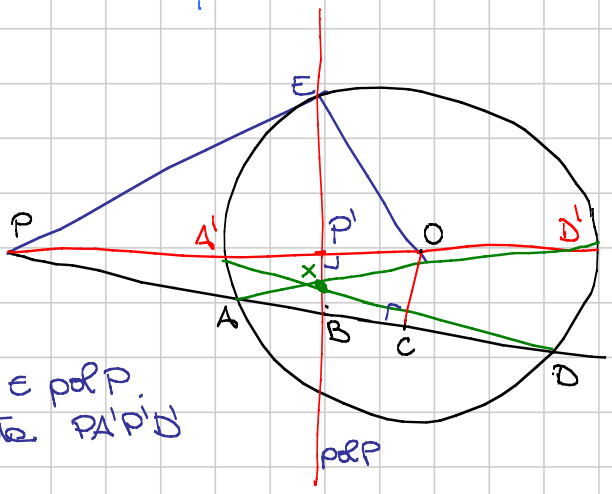
① Chiamo E, P'. ← teorema di Euclide
$PA \cdot PD = PE^2 = PP' \cdot PO = PB \cdot PC$
↑ potenza di P rispetto a Γ ↑ $OP'CB$ è ciclico

Corollario:
i pti rossi sono conciclici
Date due rette passanti per P, P le intersec con pol P e i pti medi delle corde sono conciclici



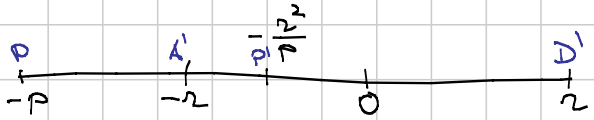
Dim: "ciclicità metrica"

② Basta mostrarlo quando AD è un diametro.
Infatti
$(A, D; P, B) = (D, A'; P, P')$
↑ per l'altro lemma $AD' \cap A'D \in$ pol P. X_4
proiettando da X sulla retta $PA'P'D$



Ora devo mostrarlo per pti sul diametro

$$\frac{D'P \cdot A'P'}{D'P' \cdot A'P} = \frac{(r+p)\left(r-\frac{r^2}{p}\right)}{\left(r+\frac{r^2}{p}\right)\cdot(p-r)} = -1.$$



Esempio:

ABC triangolo, I incentro, D,E,F punti di tangenza. $S = EF \cap BA$

Allora $SI \perp CD$.

Mostriamo che $CD \stackrel{?}{=} pol\, S$.

$S \in pol\, C = EF$

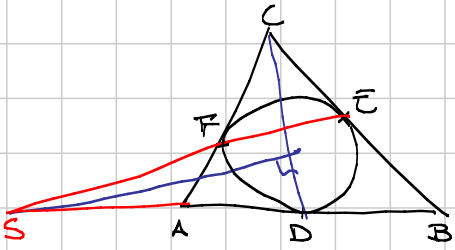
$S \in pol\, D = AB$

La polarità rovescia le inclusioni

$C \in pol\, S$

$D \in pol\, S$

Allora $pol\, S = CD$.



Teorema di Brianchon

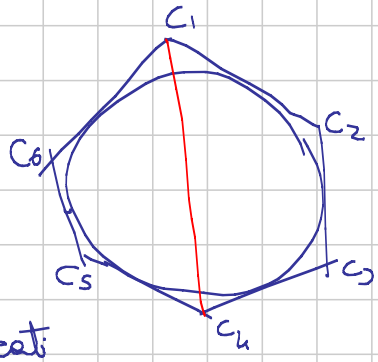
$C_1, \dots, C_6$ esagono circoscritto a una circonferenza.

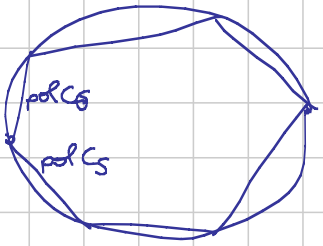
Allora C_1C_4, C_2C_5, C_3C_6 concorrono

Dim:

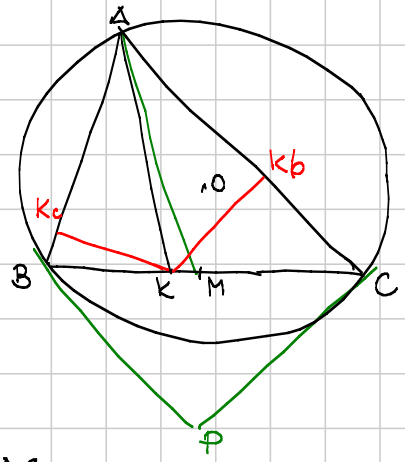
E' il duale di Pascal.

Tesi duale: $pol\, C_1 \cap pol\, C_4$, $pol\, C_2 \cap pol\, C_5$, $pol\, C_3 \cap pol\, C_6$ sono allineati





Lemma della simmediana



ABC triangolo, AK ceviana,
$P = BB \cap CC$, M pto medio di BC

Sono equivalenti

① $B\hat{A}K = M\hat{A}C$

② $\frac{BK}{KC} = \frac{AB^2}{AC^2}$

③ A, K, P allineati

④ Dette K_C, K_b le proiez di K su AB e AC

$$\frac{K_cK}{KK_b} = \frac{AB}{AC}$$

Se AK verifica una delle proprietà sopra, si chiama SIMMEDIANA.

Dim:

Tutti individuano esattamente un pto, quindi per dimm ① ⇔ ② basta dim ① ⇒ ②.

① ⇒ ② Per il teo dei seni su ABK

$$\frac{BK}{\sin B\hat{A}K} = \frac{AB}{\sin B\hat{K}A}$$

$$\frac{KC}{\sin K\hat{A}C} = \frac{BC}{\sin A\hat{K}C}$$

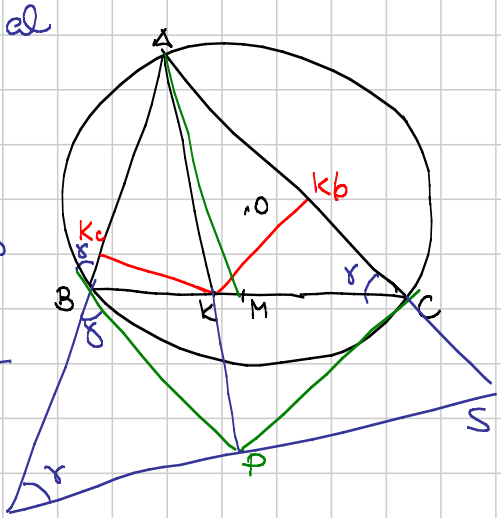
Quindi

$$\frac{BK}{KC} = \frac{\sin B\hat{A}K}{\sin K\hat{A}C} \cdot \frac{AB}{AC} \overset{\text{uso ①}}{=} \frac{\sin M\hat{A}C}{\sin M\hat{A}B} \cdot \frac{AB}{AC}$$

$$= \frac{AB^2}{AC^2}$$

↑ teo seni su BAM e MAC

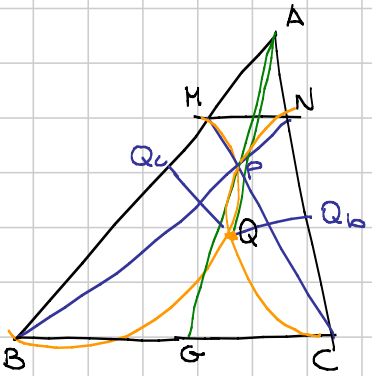
③ ⇒ ① Traccio l'antiparallela al lato BC che passa per P ovvero t.c $B\hat{R}P = \gamma$.



Basta dim che P è pto medio di RS (poi con omotetia di centro A + simm rispetto alla bisettrice di $\hat{A}$ mando $R \to C$ $S \to B$ $P \to M$ e quindi $R\hat{A}P \to C\hat{A}M$, ok)
$R\hat{P}B$ è isoscele $\Rightarrow RP = BP = PC = PS$
↑ stesso ragionamento su PCS

② ⇒ ④ $\dfrac{KcK}{KKb} = \dfrac{BK \cdot \sin\hat{B}}{KC \cdot \sin\hat{C}} = \dfrac{AB^2}{AC^2} \cdot \dfrac{AC}{AB}$
↑ uso ② e teo seni su ABC.

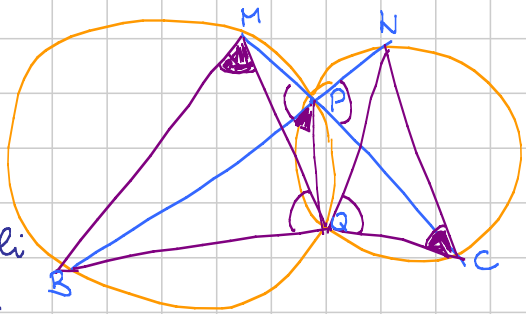
Esercizio: BMO 09 – 2
ABC triangolo, $MN \parallel BC$. $P = MC \cap BN$
I circocerchi di BMP e CNP si incontrano in P e Q
Dim che
$B\hat{A}Q = C\hat{A}P$.



Oss 1: $AP \cap BC$ è il pto medio di BC
(Ceva su ABC con punto P
$\dfrac{BG}{GC} \cdot \dfrac{CN}{NA} \cdot \dfrac{AM}{MB} = 1$
" 1 per Talete.

Resta da dimostrare che AQ è la simmediana.
Basta dim $\dfrac{QcQ}{QQb} \overset{?}{=} \dfrac{AB}{AC}$.

Q è centro di una omotetia + rotazione che manda $Q \to Q$ $B \to N$ $M \to C$.



Basta dim che
$B\hat{Q}M = N\hat{Q}C$
e $B\hat{M}Q = N\hat{C}Q$
(poi sono i due triangoli viola sono simili con centro Q)

$$\frac{QcQ}{QQ_b} = \frac{BM}{NC} = \frac{AB}{AC}.$$

$\frac{QcQ}{QQ_b}$: per rotoomotetia. $\frac{BM}{NC} = \frac{AB}{AC}$: per Talete.

□

Teoria dei Numeri 1 (Medium)

Titolo nota 05/09/2011

$q(x)$ ha grado $n \Rightarrow q$ non ha più di n radici

α è radice di $q \iff q(\alpha) = 0$

$\iff x - \alpha \mid q(x)$ $\quad q(x) = (x-\alpha) r(x)$

- $q(x) = r(x) \quad \forall x \in \mathbb{Z}_p \not\Rightarrow q = r$ come polinomi

$$x^p - x = 0 \quad \forall x \in \mathbb{Z}_p$$

- $f(a) = 1 \quad f(x) = 0 \quad x \neq 0 \pmod p$

$1 - x^{p-1} \qquad 1 - (x-a)^{p-1}$

- $\operatorname{ord}_p(a) = \min\{k > 0 : a^k \equiv 1 \pmod p\}$

$\operatorname{ord} \mid \varphi(p) = p - 1$

$\operatorname{ord}(ab) \qquad \operatorname{ord}(a) \quad \operatorname{ord}(b)$

$b = a = (-1)$

$$(ab)^k \equiv 1 \pmod p$$

$$a^{k \cdot \operatorname{ord}(b)} \cdot b^{k \operatorname{ord}(b)} \equiv 1 \pmod p$$

$$\mathrm{ord}_p(a) \mid k \cdot \mathrm{ord}(b)$$

$$\frac{o(a)}{(o(a), o(b))} \mid k \qquad \frac{o(b)}{(o(a), o(b))} \mid k$$

$$\left[\frac{o(a)}{(o(a), o(b))}, \frac{o(b)}{(\ ,\ )}\right] \mid k$$

$$\frac{1}{(o(a), o(b))} \overset{!!}{[o(a), o(b)]} \mid o(ab) \mid [o(a), o(b)]$$

$$(ab)^{[o(a), o(b)]} \equiv 1 \quad (p)$$

- Modulo p esiste un generatore

$\exists\, g$ t.c. $\mathrm{ord}_p(g) = p-1$

$$\{g^0, g^1, \dots, g^{p-2}\} = \{1, 2, \dots, p-1\}$$

$$\{m \mid \exists x : \mathrm{ord}_p(x) = m\}$$

m_1 m_2 $\qquad m_1 = 9 \cdot 2$

x_1 x_2 $\qquad m_2 = 3 \cdot 4$

x_1^2 ha ordine 9

x_2^3 ha ordine 4

$\Big\}$ $x_1^2 x_2^3$ ha ordine 36

M = massimo degli ordini mod p.

$q(X) = x^M - 1$. Che radici ha?

$a \in \mathbb{Z}_p^*$ $\quad ord_p(a) \nmid M$ (per assurdo)

$M < [o(a), M] \in$ insieme ordini

$a^M \equiv 1 \pmod p \Rightarrow q(a) = 0$

$M = \deg q(x) \geq p-1$

Esiste g : $ord_p(g) = M = p-1$

Oss $\quad ord(g^k)$ se $(k, p-1) = 1$?

$g^{km} \equiv 1 \ (p) \iff p-1 \mid km$

$\iff p-1 \mid m$

$ord(g^k) = p-1$ Ci sono $\varphi(p-1)$ gener.

- $q(x)$ polinomio di grado $\leq p-2$

Allora $\sum_{i=0}^{p-1} q(i) \equiv 0 \pmod p$.

$q(X) = X^m$ (basta per questi)

$i = 0$ non contribuisce (se $m > 0$)

$$\sum_{i=1}^{p-1} q(i) \equiv \sum_{j=0}^{p-2} q(g^j) \equiv$$

$$\equiv \sum_{j=0}^{p-2} g^{mj} \equiv \frac{g^{m(p-1)} - 1}{g^m - 1} \pmod p$$

$$\not\equiv 0$$

Se $m < p-1$, $g^m - 1 \not\equiv 0 \pmod p$

Dim. altern. $f : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$

$i \longmapsto a \cdot i \qquad a \not\equiv 0 \ (p)$

$$\underbrace{\sum_{i=0}^{p-1} i^m}_{S} \equiv \sum_{i=0}^{p-1} (ai)^m \equiv a^m \sum_{i=0}^{p-1} i^m$$

$$S \equiv a^m \cdot S \pmod p$$

$$a^m \not\equiv 1 \Rightarrow S \cdot (a^m - 1) \equiv 0 \pmod p$$

$$\Downarrow$$

$$S \equiv 0 \pmod p$$

a = generatore

$a^m - 1$ non può essere sempre 0, perché altrimenti $x^m - 1$ avrebbe troppe radici

- Frazioni mod p: funzionano

$$a/b \equiv ab^{-1}$$

$$a/b + c/d \equiv \frac{ad+bc}{bd} \pmod p$$

IMO qualcosa (2005/4) Trovare tutti gli n che sono coprimi con tutti i numeri della forma $2^n+3^n+6^n-1$

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

$$p \mid \frac{1}{2}+\frac{1}{3}+\frac{1}{6}-1$$

$$x^{p-1} = 1 \Rightarrow x^{p-2} \equiv 1/x \pmod p$$

$$n = p-2$$

$$2^{p-2}+3^{p-2}+6^{p-2}-1 \equiv \frac{1}{2}+\frac{1}{3}+\frac{1}{6}-1 \equiv 0 \pmod p$$

$\boxed{n=1}$

Attenzione: non dividere per 0 vuol dire non dividere per multipli di p ($\Rightarrow p=2,3$ a mano!)

"SOLLEVAMENTO" DI HENSEL

$q(x) \in \mathbb{Z}[x]$ polinomio a coeff. interi

Mod p ha certe radici $x_1, \dots, x_r$.

Se $q'(x_i) \not\equiv 0 \pmod p$, allora il numero di soluzioni mod p^n non dipende da n

$$q(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 x^0$$

$$q'(x) = n \cdot a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1 x^0 + 0$$

$$q(x_i) \equiv 0 \pmod{p^n}$$

Cerchiamo le radici mod p^{n+1}.

$$q(\alpha) \equiv 0 \pmod{p^{n+1}} \Rightarrow q(\alpha) \equiv 0 \pmod{p^n}$$

$$\alpha \equiv x_i \pmod{p^n} \qquad \alpha \equiv x_i + k \cdot p^n \pmod{p^{n+1}}$$

$$q(x_i + k \cdot p^n) \equiv$$

$$(x_i + k \cdot p^n)^m \equiv x_i^m + x_i^{m-1} \cdot m \cdot k \cdot p^n + p^{2n}(\dots) \equiv$$

$$\equiv x_i^m + (m x_i^{m-1})(k \cdot p^n) \pmod{p^{n+1}}$$

$$0 \equiv q(x_i + k\cdot p^n) \equiv \underset{\downarrow}{q}(x_i) + \underset{\downarrow}{q'}(x_i)\cdot k\cdot p^n \pmod{p^{n+1}}$$

$$q(x_i) = a\cdot p^n$$

$$\Rightarrow \quad -a\cdot p^n \equiv q'(x_i)\cdot k\cdot p^n \quad (p^{n+1})$$

$$\Leftrightarrow \quad -a \equiv q'(x_i)\cdot k \quad (p)$$

$$\Rightarrow \quad k \equiv -a\cdot (q'(x_i))^{-1} \pmod{p}$$

$$x^2 \equiv a \pmod{p^n}$$

$$q(x) = x^2 - a \qquad q'(x) = 2x \qquad q'(x) \neq 0 \quad (\text{se } p \neq 2)$$

$$X^2 \equiv 1 \pmod 8$$

ESERCIZI

$n \nmid 2^n - 1 \qquad n \neq 1$. Per assurdo $n \ldots$

$p \mid n \qquad 2^n \equiv 1 \pmod p$

$\operatorname{ord}_p(2) \mid n$

$\mid \varphi(p) = p-1$

$\mid (n, p-1) = 1$

p = PIU' PICCOLO PRIMO DI n

$\operatorname{ord}_p(2) = 1 \qquad 2^1 \equiv 1 \pmod p$ ASSURDO

$a > b > 0$ interi coprimi $\Rightarrow n \mid \varphi(\overbrace{a^n - b^n}^{M})$

Se sapessimo costruire x t.c. $\operatorname{ord}_M(x) = n$ avremmo vinto.

$b = 1. \qquad \mod a^n - 1$

$a^m \equiv 1 \pmod{a^n - 1}$

$a^n - 1 \mid a^m - 1 \Rightarrow a^m - 1 \geq a^n - 1$

$\Rightarrow m \geq n$

$a^n \equiv 1 \pmod{a^n - 1}$

$a^n \equiv b^n \pmod{a^n - b^n}$

$(a/b)^n \equiv 1 \pmod{a^n - b^n}$

$(a^n - b^n, b) = (a^n, b) = 1$

$(a/b)^k \equiv 1 \quad (a^n - b^n)$

$a^k - b^k \equiv 0 \quad (a^n - b^n)$

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

$a^k - b^k$ è crescente al variare di k

$\Rightarrow k \geq n$ e fine.

$n < p \leq \frac{4n+2}{3}$, p primo

Allora $p \mid \sum_{i=0}^{n} \binom{n}{i}^4$

$n = p-1$ $\quad \binom{p-1}{i} \equiv \frac{(p-1)(p-2)\cdots(p-i)}{i!}$

$\equiv (-1)^i \frac{i!}{i!} \equiv (-1)^i \pmod p$

$n = p-2$ $\quad \binom{p-2}{i} \equiv \frac{(p-2)(p-3)\cdots(p-1-i)}{i!}$

$\equiv (-1)^i \frac{2 \cdot 3 \cdot \ldots \cdot (i+1)}{1 \cdot 2 \cdot \ldots \cdot i}$

$n = p-3$ $\quad (-1)^i \frac{3 \cdot 4 \cdot \ldots \cdot (i+2)}{1 \cdot 2 \cdot 3 \cdot \ldots \cdot i} \equiv (-1)^i \frac{(i+1)(i+2)}{2}$

$n = p-k$ $\quad \binom{p-k}{i} \equiv (-1)^i \frac{(i+k-1)(i+k-2)\cdots(k)}{i!}$

$\equiv (-1)^i \binom{i+k-1}{i} \equiv (-1)^i \binom{i+k-1}{k-1}$

$\binom{n}{i}^4 \equiv q(i)$ con q polin di grado $4(p-n-1)$

$\sum_{j=0}^{p-1} q(j) \equiv 0 \pmod p$ $\qquad i \geq p-k+1 = n+1$

$\sum_{j=0}^{m} q(j)$ $\qquad 4(p-n-1) < p-1$

$3p < 4n+3$

$p < \frac{4n+3}{3}$

VALUTAZIONI P-ADICHE

$p \mid n$ $\quad p^k \| n$ $\quad p^k \mid n$ ma p^{k+1} no

$k = v_p(n)$ $\qquad v_p(a \cdot b) = v_p(a) + v_p(b)$

$v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$

ed è $=$ se $v_p(a) \neq v_p(b)$

$v_p(a) > v_p(b)$ $\qquad b = p^{v_p(b)} \cdot r$

$a = p^{v_p(b)} \cdot p^{v_p(a) - v_p(b)} \cdot q$

$$a + b = p^{v_p(b)} \cdot \underbrace{\left(r + q \cdot p^{v_p(a) - v_p(b)}\right)}_{\not\equiv 0 \ (p)}$$

p primo dispari, $p \mid x-y$, $p \nmid x$ ✓ Allora

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

Per induzione sul numero di fattori primi di n.

$n = q$ $\qquad x - y = kp$

$$x^q - y^q = (y+kp)^q - y^q =$$

$q \neq p$ $\qquad = y^q + y^{q-1} \cdot kpq + (kp)^2(\cdots) - y^q$

$$v_p(y^{q-1} kpq) < v_p(\text{il resto})$$

$$v_p(x^q - y^q) = v_p(kp) = v_p(x-y)$$

$q = p$ $\qquad = y^p + kp^2 y^{p-1} + (kp)^2 p(\cdots) + (kp)^p - y^p$

$$v_p(k^2p^3) > v_p(kp^2)$$

$$v_p((kp)^p) > v_p(kp^2)$$

$$v_p(x^p - y^p) = v_p(kp^2) =$$

$$= v_p(kp) + 1$$

$$= v_p(x-y) + v_p(p)$$

$$v_p(x^{nq} - y^{nq}) = v_p((x^n)^q - (y^n)^q) =$$

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

$$= v_p(x-y) + \underbrace{v_p(n) + v_p(q)}$$

$v_p(nq)$

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

E se $p = 2$?

Se $4 \mid x-y$ $(2 \nmid x)$ va tutto bene

Se $2 \mid x-y$ ma n è pari, $n = 2^k \cdot d$

$$v_2(x^n - y^n) = v_2(x^{2^k} - y^{2^k})$$
$$= v_2\left((x^2)^{2^{k-1}} - (y^2)^{2^{k-1}}\right) =$$
$$= v_2(x^2 - y^2) + k - 1$$
$$= v_2(x^2 - y^2) + v_2(n) - 1$$

$\mathbb{Z}_p^*$ è ciclico.

$\mathbb{Z}_n^*$ è ciclico: per quali n?

$|\mathbb{Z}_n^*| = \varphi(n)$

$g \in \mathbb{Z}_n^*$ t.c. $\operatorname{ord}_n(g) = \varphi(n)$

$x \in \mathbb{Z}_n^*$ $\quad x^m \equiv 1 \pmod n$

$$\Uparrow\!\!\!\!\!\!\Uparrow$$

$$(*) \begin{cases} x^m \equiv 1 \pmod{p_1^{a_1}} \\ \vdots \\ x^m \equiv 1 \pmod{p_k^{a_k}} \end{cases}$$

m è divisibile per l'ordine di x mod $p_i^{a_i}$ $\forall i$

Se prendo $m = \operatorname{mcm}\left(\varphi(p_1^{a_1}), \dots, \varphi(p_k^{a_k})\right)$

ricavamente ho $(*)$

Cercavamo $m = \varphi(n)$. Abbiamo trovato

$$\varphi(n) \mid \left[\varphi(p_1^{a_1}), \dots, \varphi(p_k^{a_k})\right]$$

$$\varphi(n) \quad \varphi(p_1^{a_1}) \cdots \varphi(p_k^{a_k})$$

Ma la φ è "sempre" pari ($\varphi(1), \varphi(2)$)

Caso 1) c'è un solo primo nella fatt. di n

Caso 2) c'è un 2 ed un p^k

Attenzione: $\varphi(2^q)$ è pari anche lui ($q \geq 2$)

$\mathbb{Z}_n^*$ ciclici $\Rightarrow$ $n = p^k$, $2p^k$

$\mathbb{Z}_{2^k}^*$: è ciclico? Solo $\mathbb{Z}_2$, $\mathbb{Z}_4$

g genera $\mathbb{Z}_{2^k}^*$. $g^2 \equiv 1 \pmod 8$

$$v_2\left(g^{2^t} - 1\right) = v_2\left(g^2 - 1\right) + t - 1$$

Essere un generatore vuol dire $g^{2^{k-2}} \not\equiv 1 \pmod{2^k}$

$t = k-2$ dà $v_2\left(g^{2^{k-2}} - 1\right) \geq k - 3 + 3 = k$

$$g^{2^{k-2}} \equiv 1 \pmod{2^k}$$

Massimo degli ordini? È 2^{k-2}, realizzato da 5

$5^{2^{k-3}} \not\equiv 1 \pmod{2^k}$ ma $5^{2^{k-2}} \equiv 1$

Induz. su k. $k = 3$ ok

$$5^{2^{k-2}} = A \cdot 2^k + 1 \quad \text{con } A \text{ dispari}$$

$$5^{2^{k-1}} = \left(A \cdot 2^k + 1\right)^2 = A^2 \cdot 2^{2k} + A \cdot 2^{k+1} + 1$$

$$= 2^{k+1}(A + \text{pari}) + 1$$

$\{5^m\}$ sono metà degli elementi di $\mathbb{Z}_{2^k}^*$

Ogni elemento di $\mathbb{Z}_{2^k}^*$ si scrive come $\pm 5^m$.

Se invece p è un primo dispari $\mathbb{Z}_{p^k}^*$ è cic.

g genera $\mathbb{Z}_p^*$

$$\operatorname{ord}_{p^2}(g) = ?$$

$$g^m \equiv 1 \pmod{p^2} \Rightarrow g^m \equiv 1 \ (p)$$

$$\Rightarrow (p-1) \mid m \mid \varphi(p^2) = p(p-1)$$

Cosa accade se l'ordine è $p-1$?

$$p^2 \mid g^{p-1} - 1$$

$$(g+p)^{p-1} - 1 \equiv \left(g^{p-1} - 1\right) + g^{p-2} \cdot p \ (p^2)$$

$$\equiv p \cdot g^{p-2} \not\equiv 0 \pmod{p^2}$$

Induzione su n (esponente di p)

Sia g un generatore modulo p^2

$$n \leq v_p\left(g^{(p-1)p^t} - 1\right) = v_p\left((g^{p-1})^{p^t} - 1\right)$$

$$= v_p\left(g^{p-1} - 1\right) + v_p\left(p^t\right)$$

$$= 1 + t$$

$$t \geq n-1 \Rightarrow (p-1) \cdot p^t \geq (p-1) \cdot p^{n-1} = \varphi(p^n)$$

$n^2 \mid 2^n + 1$ $\qquad n = 1,\ n = 3$

p = P.P.P. di n. $\qquad p \mid n^2 \mid 2^n + 1 \Rightarrow 2^n \equiv -1 \pmod p$

$\Rightarrow 2^{2n} \equiv 1 \pmod p$

$2^{p-1} \equiv 1 \pmod p$ $\Rightarrow \operatorname{ord}_p(2) \mid (2n, p-1) = 2$

$\operatorname{ord}_p(2) = 2 \Rightarrow 2^2 \equiv 1 \pmod p \Rightarrow p = 3$

$n = 3m$. $\qquad 9m^2 \mid 8^m + 1$

q = P.P.P di m. $\qquad 8^{2m} \equiv 1 \pmod q$

$\operatorname{ord}_q(8) \mid (2m, q-1) = 2$

$q \mid 8^2 - 1 = 63 \qquad q = 3, 7$

Può essere $q = 7$? NO $\qquad 7 \mid 8^m + 1$

Quindi $q = 3$.

$v_3(n^2) \le v_3(8^m + 1)$

$\| \qquad\qquad \|$

$2v_3(n) \qquad\quad = v_3(8^m - (-1)^m)$

$2[v_3(m) + 1] \qquad = v_3(8+1) + v_3(m)$

$2v_3(m) \le v_3(m) \qquad v_3(m) \le 0$

ASSURDO se $m \neq 1$

IMO 2000) Dire se esiste n : $n \mid 2^n+1$ e n ha esattamente 2000 fattori primi distinti

$$n \mid 2^n+1 \mid 2^{nd}+1$$

$(n, d) = 1$ con $d \mid 2^n+1$

$$\Rightarrow \quad nd \mid 2^n+1 \mid 2^{nd}+1$$

Saremmo contenti di avere $n = 3^k$

$$3^k \mid \underbrace{2^{3^k}+1}_{a_k} \qquad v_3\left(2^{3^k}+1\right) =$$

$$= v_3(2+1) + v_3\left(3^k\right) = k+1$$

$$v_3\left(2^{3^{k+1}}+1\right) = v_3\left(2^{3^k}+1\right) + 1$$

Passando da 3^k a 3^{k+1}, $a_{k+1} \sim a_k^{\,3}$ ed ha solo un fattore 3 in più.

$$v_p\left(2^{3^{k+1}}+1\right) = v_p\left(\left(2^{3^k}\right)^3+1\right) =$$

$$= v_p\left(2^{3^k}+1\right) + \underbrace{v_p(3)}_{0, \text{ per } p \neq 3}$$

$$2^{3^k}+1 \mid 2^{3^{k+1}}+1$$ (i fattori primi di a_k si trovano tutti anche in a_{k+1})

Trovare (a,b) con $a>1$, $b>1$ t.c.

$$b^a \mid a^b - 1$$

p = P.P.P che divide b.

$$a^b \equiv 1 \pmod{p}$$

$$\operatorname{ord}_p(a) \mid (b, p-1) = 1 \Rightarrow a \equiv 1 \pmod{p}$$

Se p è dispari vale

$$a v_p(b) = v_p(b^a) \leq v_p(a^b - 1) =$$

$$= v_p(a-1) + v_p(b)$$

$$v_p(b) \cdot (a-1) \leq v_p(a-1)$$

$$\| \quad a-1$$

ASSURDO ($\Rightarrow p$ non era dispari)

$$a\, v_2(b) \leq v_2(a^2-1) + v_2(b) - 1$$

$$(a-1) v_2(b) \leq v_2(a+1) + v_2(a-1) - 1$$

$$\| \quad a-1$$

$$a \leq v_2(a^2-1)$$

$$2^a \leq a^2 - 1 \Rightarrow a \leq 3$$

$a = 3$. $\quad b^3 \mid 3^b - 1 \quad b = 2c$

$$8c^3 \mid 9^c - 1$$

q = p.p.p che divide c

$$g^c \equiv 1 \pmod q$$

$$\mathrm{ord}_q(g) \mid (c, q-1) = 1$$

$\Rightarrow$ $q \mid g-1 = 8$, cioè c è pari NO

RESIDUI QUADRATICI E NON

$a \in \mathbb{Z}_p^*$ t.c. $x^2 \equiv a \pmod p$ si risolva

Def. $\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{se } a \text{ è un res. q. mod } p \\ 0, & \text{se } p \mid a \\ -1, & \text{se } a \text{ non è un residuo} \end{cases}$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

"Criterio di Eulero" $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

Se a è un quadrato, $a \equiv x^2$, $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \ (p)$

$q(x) = x^{\frac{p-1}{2}} - 1 \qquad f : x \longmapsto x^2$

$$f(x) = f(y) \iff x \equiv \pm y \ (p)$$

$$x^2 - y^2 \equiv 0 \ (p) \iff (x+y)(x-y) \equiv 0 \ (p)$$

Quadrati = RADICI DI $q(x)$

$$\left(x^{\frac{p-1}{2}}\right)^2 \equiv x^{p-1} \equiv 1 \pmod p$$

$$x^{\frac{p-1}{2}} = +1, -1$$

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

$$\left(g^k\right)^{\frac{p-1}{2}} \equiv 1 \pmod p \iff p-1 \mid k\left(\frac{p-1}{2}\right)$$

$$\iff k \text{ è pari}$$

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, quindi -1 è R.Q. $\Leftrightarrow p \equiv 1 \ (4)$

ed in tal caso $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p$

$(p-1)! \equiv -1 \pmod p$

- Se $p \equiv 3 \pmod 4$ e $\left(\frac{a}{p}\right) = 1$, allora

(una) radice di a è $a^{\frac{p+1}{4}}$

$$\left(a^{\frac{p+1}{4}}\right)^2 \overset{?}{\equiv} a$$

$$\left(a^{\frac{p+1}{4}}\right)^4 \overset{?}{\equiv} a^2$$

$$\Downarrow \qquad \text{ok}$$

$$a^{p+1} \equiv a^2$$

Quindi $\left(a^{\frac{p+1}{4}}\right)^2 \equiv \pm a$.

Siccome $p \equiv 3 \ (4)$, $\left(\frac{-1}{p}\right) = -1$, cioè esattamente uno tra a e $-a$ è un quadrato, e perciò era proprio $+a$ (perché LHS è un quadrato).

Reciprocità quadratica

p, q primi dispari distinti.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Se almeno uno tra p, q è $\equiv 1 \pmod 4$, allora p è residuo mod q $\Leftrightarrow$ q residuo mod p

Viceversa, se $p \equiv q \equiv 3 \pmod 4$, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$.

Lemma (Gauss) Sia $n \not\equiv 0 \pmod p$, $p \neq 2$

$$A = \left\{ [kn]_p < p/2 \;\middle|\; k = 1, \dots, \frac{p-1}{2} \right\}$$

$$B = \left\{ [kn]_p > p/2 \;\middle|\; k = 1, \dots, \frac{p-1}{2} \right\}$$

$m = |B|$ $\qquad \left(\frac{n}{p}\right) = (-1)^m$

$b \in B \qquad p - b \overset{?}{=} a \iff a + b = p$

$n(k_1 + k_2) \neq p$

$$|(p - B) \cup A| = \frac{p-1}{2}$$

$$\| \quad \left\{1, \dots, \frac{p-1}{2}\right\}$$

$$\prod_{i=1}^{\frac{p-1}{2}} i \equiv \left(\prod_{a \in A} a\right)\left(\prod_{b \in B} (p-b)\right) \pmod p$$

$$\equiv \left(\prod_{a \in A} a\right) (-1)^{|B|} \cdot \left(\prod_{b \in B} b\right)$$

$$\equiv \left(\prod_{i=1}^{\frac{p-1}{2}} (in)\right) (-1)^{|B|}$$

$$\equiv n^{\frac{p-1}{2}} \cdot \prod_{i=1}^{\frac{p-1}{2}} i \cdot (-1)^m \pmod p$$

$$1 \equiv n^{\frac{p-1}{2}} \cdot (-1)^m \pmod p$$

$$(-1)^m \equiv \left(\frac{n}{p}\right) \pmod p$$

$\left(\frac{2}{p}\right)$

$\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1$

Considera $\left\{ [2k]_p > p/2 \;\middle|\; k = 1, \dots, \frac{p-1}{2} \right\}$

$= \left\{ 2k > p/2 \;\middle|\; k = \quad \right\}$

Risultato: $\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}}$

Sia $i = \sqrt{-1} \mod p$. $\quad 2 = \frac{(1+i)^2}{i} = \frac{1-1+2i}{i} = 2$

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv \left[\frac{(1+i)^2}{i}\right]^{\frac{p-1}{2}} \equiv \frac{(1+i)^{p-1}}{i^{\frac{p-1}{2}}} \equiv \frac{(1+i)^p}{(1+i)\left(i^{\frac{p-1}{2}}\right)}$$

$$\equiv \frac{1+i^p}{(1+i)\, i^{\frac{p-1}{2}}} \pmod p$$

---

a = somma elementi A, $b = \dots$ di B

$$1 + 2 + \dots + \frac{p-1}{2} = a + mp - b$$

a: somma elementi A; b: somma elem $p - B$

$$n + 2n + 3n + \dots + \left(\frac{p-1}{2}\right)n = a + b + \sum_{k=1}^{\frac{p-1}{2}} p\left\lfloor \frac{kn}{p} \right\rfloor$$

$$(n-1)\left(1 + \dots + \frac{p-1}{2}\right) = 2b - mp + \sum_{k=1}^{\frac{p-1}{2}} p\left\lfloor \frac{kn}{p} \right\rfloor$$

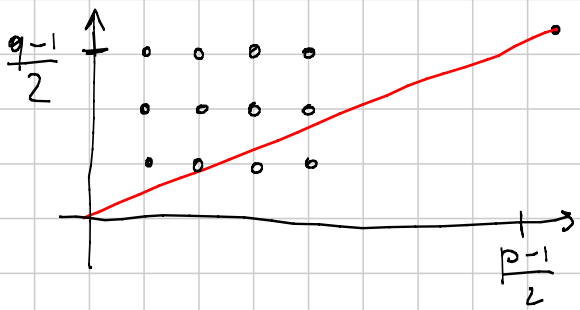
n disp.

$$\Rightarrow \qquad mp \equiv \sum_{k=1}^{\frac{p-1}{2}} p\left\lfloor \frac{kn}{p} \right\rfloor \pmod 2$$

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kn}{p} \right\rfloor \qquad (2)$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{m_1}(-1)^{m_2} = (-1)^{\sum_k \left\lfloor \frac{kq}{p} \right\rfloor + \sum \left\lfloor \frac{kp}{q} \right\rfloor}$$

$$(-1)^{\frac{(p-1)(q-1)}{4}}$$



Simbolo di Jacobi $n = p_1^{a_1} \cdots p_k^{a_k}$

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)^{a_1} \cdots \left(\frac{m}{p_k}\right)^{a_k}$$

Vale ancora la recipr. quadr.

$\left(\frac{m}{n}\right) = -1$ $\Rightarrow$ m non è quadr. mod n

Es $a \equiv b \pmod 2$. $2^a - 1 \mid 3^b - 1$

$(a \neq 1)$

a è pari $3 \mid 2^a - 1 \mid 3^b - 1$ ASSURDO

a è dispari. $3^b - 1 \equiv 0 \quad (2^a - 1)$

$$\Rightarrow 3^{b+1} \equiv 3 \quad (2^a - 1)$$

$$1 = \left(\frac{3}{2^a - 1}\right) = (-1)^{2(2^a-2)/4} \left(\frac{2^a - 1}{3}\right)$$

$$= -\left(\frac{2^a - 1}{3}\right) = -\left(\frac{(-1)^a - 1}{3}\right)$$

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

ASSURDO

$\left(\frac{n}{p}\right) = 1 \quad \forall p \Rightarrow n$ è un quadrato

$n = p_1 \cdots p_k$

$$1 = \left(\frac{n}{p}\right) = \left(\frac{p}{n}\right) = \left(\frac{p}{p_1}\right)\left(\frac{p}{p_2}\right) \cdots \left(\frac{p}{p_k}\right) = -1$$

$p \equiv 1 \ (4)$ $\quad -1 \quad 1 \quad \cdots \quad 1$

Scegliamo q un non-residuo mod p_1 e vediamo

$$\begin{cases} p \equiv q \pmod{p_1} \\ p \equiv 1 \pmod{p_2} \\ \vdots \\ p \equiv 1 \pmod{p_k} \\ p \equiv 1 \pmod{4} \end{cases}$$

Modo 1: c'è un teorema (Dirichlet) che dice che p esiste.

$a \cdot n + b$ con $(a, b) = 1$

Modo 2: simboli di Jacobi + pensateci

(idea: scegli p soluzione del sistema anche se non è primo)

Residui d-esimi, $d \mid p-1$

a : $x^d \equiv a$ ha soluz.

$x^d \equiv y^d \pmod p \Rightarrow \left(\frac{x}{y}\right)^d \equiv 1 \pmod p$

$x^d - 1 \mid x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1))$

Quindi $x^d - 1$ ha esattamente d soluz.

$f(x) = x^d : \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^*$

La cardinalità dell'img è $\frac{p-1}{d}$

$\Rightarrow$ i residui d-esimi sono $\frac{p-1}{d}$

In generale sono $\frac{p-1}{(d, p-1)}$; in particolare,

se $(d, p-1) = 1$, f è surgettiva (e quindi iniettiva)

TEORIA DEI NUMERI 2 (MEDIUM)

Titolo nota 07/09/2011

"VIETA - JUMPING"

Per ogni $m>0$ esistono infinite coppie (x,y) tali che $x \cdot y \mid x^2+y^2+m$

$(x,y) = (1,1) \qquad (m+1, 1)$

$x \mid y^2+m, \quad y \mid x^2+m$

$$\frac{x^2+y^2+m}{xy} = m+2$$

$$x^2+y^2+m-(m+2)xy = 0$$

$$X^2 - X((m+2)y) + (y^2+m) = 0$$

Per $y=1$ l'equazione ha la sol $x=1$

somma radici $= (m+2)y$ $\quad (x=m+1,\ y=1)$

$(1, m+1)$

$$x^2 - x((m+2)(m+1)) + ((m+1)^2+m) = 0$$

Soluz. $x=1$ che conosciamo

altra $= (m+2)(m+1) - 1$

$(m^2+3m+1,\ m+1)$

Idea: se ho una relaz. di 2° grado e conosco una soluzione ne ho subito un'altra

$\frac{a^2+b^2}{1+ab} = k \Rightarrow k$ è un quadrato perfetto $(a, b > 0)$

Fissiamo k e supponiamo che (a, b) sia una soluzione. $\quad a^2+b^2-k-kab=0$

$a \geq b \qquad (\bar{a}, b)$ con $a \cdot \bar{a} = b^2 - k$

$a + \bar{a} = kb$

$$\bar{a} = \frac{b^2-k}{a} \leq \frac{a^2-k}{a} < \frac{a^2}{a} = a$$

Può capitare che $\bar{a} \leq 0$?

Se $\bar{a} < 0 \longrightarrow k = \frac{\bar{a}^2+b^2}{1+\bar{a}b} \Rightarrow k < 0$ NO

Se $\bar{a} = 0 \Rightarrow \frac{b^2-k}{a} = 0 \Rightarrow \boxed{k = b^2}$

Supponiamo che k si scriva $\frac{a^2+b^2}{1+ab}$.

Esiste una soluzione minima (a, b)

Ma anche $\left(\frac{b^2-k}{a}, b\right)$ è soluzione e $\frac{b^2-k}{a} < a$. Se $b^2 - k \neq 0$ ho costruito una soluzione + piccola della minima, assurdo.

$4ab-1 \mid (4a^2-1)^2 \Rightarrow a=b$

$(4a^2-1)^2 \equiv 0 \pmod{4ab-1}$

$(b, 4ab-1)=1$

$b^2(4a^2-1)^2 \equiv 0 \pmod{4ab-1}$

$\|\|$

$(4a^2b-b)^2$

$0 \equiv (4a^2b^2-b^2)^2$ boh!

$4a \equiv 1/b \pmod{4ab-1}$

$0 \equiv (4a^2-1)^2 \equiv \left(\frac{a}{b}-1\right)^2 \pmod{4ab-1}$

(*) $0 \equiv (a-b)^2 \pmod{4ab-1}$

$\frac{(a-b)^2}{4ab-1} = k$ intero (Tesi: $k=0$)

Domanda: da (*) non segue $a \equiv b \ (4ab-1)$?

$4 \mid 6^2$ $\quad$ $4 \nmid 6$

$$(a-b)^2 - k(4ab-1) = 0$$

$$a^2 - a(2b+4kb) + b^2 + k = 0$$

Prendo (a,b) soluz. minima

$(\bar{a}, b)$ $\quad 0 < \bar{a} = \dfrac{b^2+k}{a} \;\overset{?}{\neq}\; a$

$$b^2 + k \leq a^2$$

$$\frac{(a-b)^2}{4ab-1} = k \leq a^2 - b^2 \iff (a-b)^2 \leq (a-b)(a+b)(4ab-1)$$

Se $a = b$ vale l'uguale

Se $a \neq b$ $\quad (a-b > 0)$ $\quad a-b < (a+b)(4ab-1)$

VERA

La soluz. minima fissato k deve avere $a = b$

$$\Rightarrow \quad k = 0 = \frac{(a-b)^2}{---}$$

$$\frac{x^2+y^2+z^2}{xyz} = k \Rightarrow k = 1 \text{ o } 3$$

$x = y = z \rightsquigarrow \frac{3x^2}{x^3} = \frac{3}{x}$ che dà 1, 3

$$x^2 + y^2 + z^2 = 2xyz$$

Modulo la potenza giusta di 2

$$x^2 + y^2 + z^2 \equiv 0 \pmod 2$$

$x \equiv y \equiv z \equiv 0$, esattamente 2 dispari

$\Rightarrow$ c'è un pari

$$x^2 + y^2 + z^2 \equiv 0 \pmod 4$$

$\Rightarrow$ sono tutti pari

$x = 2a$, $y = 2b$, $z = 2c$

$$4(a^2+b^2+c^2) = 16\,abc$$

DISCESA INFINITA! • $x^2+y^2+z^2 = 2^k xyz$

• Controllare le valutaz. 2-adiche

$x^2+y^2+z^2-kxyz=0$ (simmetrica)

$x \geq y \geq z$

Prendo (x,y,z) soluz.

$(\bar{x},y,z)$ $\qquad x\bar{x}=y^2+z^2>0$

$$\bar{x}=\frac{y^2+z^2}{x}\leq\frac{2x^2}{x}=2x$$

$$x+\bar{x}=kyz$$

$$x,\bar{x}=\frac{1}{2}\left[kyz\pm\sqrt{(kyz)^2-4(y^2+z^2)}\right]$$

Le cose ci vanno male se x era la soluz. piccola, cioè se

$$y\leq x=\frac{1}{2}\left[kyz-\sqrt{}\right]$$

$$2y+\sqrt{(kyz)^2-4(y^2+z^2)}\leq kyz-2y$$

$$(kyz)^2-4(y^2+z^2)\leq(kyz)^2+4y^2-4ky^2z$$

$$ky^2z-z^2\leq 2y^2$$

$$y^2(kz-2)\leq z^2$$

$$kz-2\leq\left(\frac{z}{y}\right)^2\leq 1$$

$$\Rightarrow kz\leq 3 \Rightarrow \boxed{k\leq 3}$$

$$\frac{x^2+y^2+1}{xy} = 3$$

$$\frac{a^2+b^2+c^2+d^2}{1+abcd} = n \qquad (a,b,c,d>0)$$

$n=2$

$$a^2+b^2+c^2+d^2-n-nabcd=0$$

Gli n che si rappr. sono (ammesso che esistano) tra quelli che fanno andare male VJ

$(\overline{a}, b, c, d)$ $\qquad a\cdot\overline{a} = b^2+c^2+d^2-n$

$\overline{a} < a$?

$b^2+c^2+d^2-n < a^2$ (ok)

Altrimenti $b^2+c^2+d^2 \geq a^2+n$

b, c, d sono "non troppo piccoli" rispetto ad a

$bcd \geq a$ $\qquad n = \dfrac{a^2+b^2+c^2+d^2}{1+abcd} \leq \dfrac{4a^2}{1+a^2} < 4$

$a^2 = b^2+c^2+d^2-k, \quad k \geq 2$

$$bcd \geq \sqrt{b^2+c^2+d^2-2} \geq \sqrt{b^2+c^2+d^2-k}$$

$\|$

a

Γ $b^2c^2d^2 \geq b^2+c^2+d^2-2$

$b^2(c^2d^2-1) \geq c^2+d^2-2$

Se $c \cdot d \geq 2$ $\quad c^2d^2-1 \geq 3$

$3b^2+2 \geq c^2+d^2$

$\lrcorner$ Se $c=d=1$ $\quad 0 \geq 0$ vera

$0 < \bar{a} < a$ $\qquad \bar{a} = \dfrac{b^2+c^2+d^2-n}{a}$

$0 < \dfrac{a^2+b^2+c^2+d^2}{1+abcd} = n$ $\qquad 0 < \dfrac{\bar{a}^2+b^2+c^2+d^2}{1+\bar{a}bcd}$

$\bar{a} \geq 0$ $\qquad \bar{a}=0$ (succede per $n = b^2+c^2+d^2$)

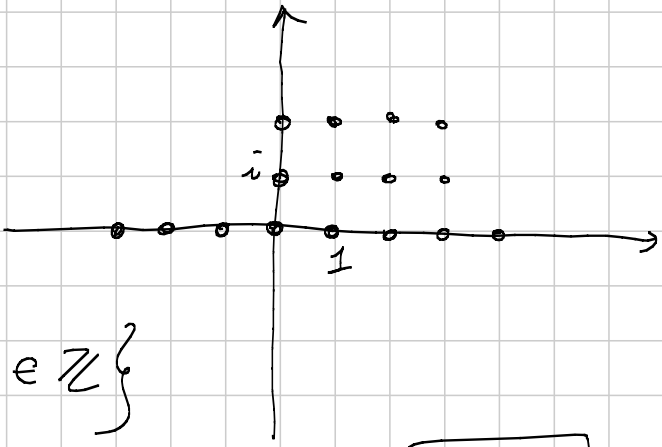
Male: $\cdot\ n < 4$

$\cdot\ n = b^2+c^2+d^2$ $\quad (b,c,d>0)$

Questi si fanno!

Interi di Gauss

$i^2 = -1$



$\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$

Norma complessa: $N(a+bi) = \sqrt{a^2+b^2}$

Si lavora con la norma quadra

$$N(z_1 \cdot z_2) = N(z_1)\,N(z_2)$$

$$x^2+y^2 = (x+iy)(x-iy)$$

In $\mathbb{Z}[i]$ valgono
- la divisione euclidea
- la fattoriz. unica

Dati a e $b \neq 0$ $\exists\, q, r$ con $a = bq+r$

con $N(r) < N(b)$ (o $r = 0$)

Primi: $p = ab \Rightarrow a = p,\ b = 1$ o viceversa

(in realtà è la def. di irriducibile)

Vera def. $p \mid ab \Rightarrow p \mid a$ oppure $p \mid b$

(e $p \neq \pm 1$)

$15 = (-3)(-5)$

$$2 = (1+i)\cdot(1-i) = 1^2 + 1^2$$

$$-i\,(1+i)^2$$

Invertibili di $\mathbb{Z} = \{1, -1\}$

Invertibili di $\mathbb{Z}[i] = \{1, -1, i, -i\}$

$$(1+i)\,i = (i-1)$$

Sia z un invertibile. Esiste w con $zw = 1$

$$\Rightarrow \quad N(zw) = 1$$

$$N(z)\cdot N(w) \qquad \Rightarrow \quad N(z) = 1$$

$$z = x+iy \quad \Rightarrow \quad x^2 + y^2 = 1$$

$$5 = (2+i)(2-i)$$

Fatto: i primi di Gauss sono: $(p = x+iy)$

$\longrightarrow$ i primi $p \in \mathbb{Z}$ con $p \equiv 3 \pmod 4$

$\longrightarrow$ x^2+y^2 è un numero primo (di $\mathbb{Z}$)

IRRIDUC = PRIMI

$\boxed{\Leftarrow}$ Sia p un primo. per assurdo $p = a\cdot b$

$\Rightarrow p \mid a$ oppure $p \mid b$, $a = kp$

$$p = kp\cdot b \Rightarrow 1 = k\cdot b$$

$$p = 1\cdot p = (-1)(-p) = (i)(-ip) = (-i)(ip)$$

$\boxed{\Rightarrow}$ Sia p un irriducibile, $p \mid a \cdot b$

Se $p \nmid a$ e $p \nmid b$, $(p, a) = 1$

$(p, b) = 1$

$1 = mp + ha$, $1 = np + kb$ (Bézout)

$1 = 1 \cdot 1 = (mp + ha)(np + kb)$

$= mnp^2 + hanp + mbkp + hkab$

$\Rightarrow p \mid 1$ ASSURDO

Prendiamo $p \equiv 3 \pmod 4$ $(p \in \mathbb{N})$

$$0i + p = (a+bi)(c+di)$$

$$(0^2+p^2) = (a^2+b^2)(c^2+d^2)$$

1	p^2	• fatt. falsa
p	p	non esiste
p^2	1	• fatt. falsa

$p = a^2+b^2$ (No! Assurdo mod 4)

$p \equiv 1 \pmod 4$ non sono primi di Gauss

$\left(\frac{-1}{p}\right) = 1$, esiste $x \in \mathbb{N}$ con $x^2 \equiv -1 \ (p)$

$\Rightarrow \quad p \mid x^2 + 1 = (x+i)(x-i)$

(3i è primo = primo vero · unità-)

Se p è primo di Gauss, $p \mid x+i$ (o $x-i$)

$p(a+bi) = x+i$ $\qquad pb = 1$ NO

$\rightsquigarrow$ p non è irriducibile $\Rightarrow p = (a+bi)(c+di)$

$$p^2 = (a^2+b^2)(c^2+d^2)$$

$1, p, p^2$

$$\Rightarrow \boxed{p = a^2+b^2} \qquad p = (a+bi)(a-bi)$$

Prendiamo un generico $z = x+iy$ con $x^2+y^2 =$ primo (di $\mathbb{Z}$)

z è un primo di Gauss

$$z = z_1 \cdot z_2 \Rightarrow N(z) = N(z_1) \cdot N(z_2)$$

p

$\Rightarrow N(z_1) = 1$, cioè z_1 è un'unità e la fatt. è falsa.

(Dimostra che $1+i$ è un primo)

Sia $p = x+iy$ primo nel senso di Gauss.

$$p \mid x^2+y^2 = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$$

(p: primo di Gauss; $p_1, \ldots, p_k$: primi di $\mathbb{Z}$)

(Fattorizziamo $3+i$. $3^2+1^2 = 10$

$$10 = (3+i)(3-i) = 2 \cdot 5 = (2+i)(2-i)(1+i)(1-i)$$

$1+i$ divide $3+i$? $3+i = 2 + (1+i)$

$= (1+i)(1-i) + (1+i)$

$= (1+i)(2-i)$)

$$p \mid p_1^{\alpha_1} \cdots p_k^{\alpha_k} \Rightarrow p \mid p_1^{\alpha_1} \Rightarrow p \mid p_1$$

$$p_1 = p \cdot z$$

norme

$$p_1^2 = N(p) \cdot N(z)$$

$$p_1, p_1^2$$

p è primo con norma prima

$p = p_1 \in \mathbb{Z}$ (a meno di unità)

$p \equiv 1 \ (4) \Rightarrow p = a^2 + b^2$

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

$(a+bi)(c+di) = (ac-bd) + i(ad+bc)$

Se $n = 2^a p_1^{a_1} \cdots p_k^{a_k}$ con $p_i \equiv 1 \pmod 4$ si rappresenta.

$p^2 + 0^2$. Anche $n = 2^a \underbrace{p_1^{a_1} \cdots p_k^{a_k}}_{\equiv 1 \ (4)} \underbrace{q_1^{2b_1} \cdots q_k^{2b_k}}_{\equiv 3 \ (4)}$

Supponiamo $n = a^2 + b^2$ e sia $p \mid n$, $p \equiv 3 \ (4)$

$a^2 + b^2 \equiv 0 \pmod p$ $\rightarrow$ $p \mid a$, $p \mid b$

$\rightarrow \left(\frac{a}{b}\right)^2 \equiv -1 \pmod p$

$\text{ord}_p\left(\frac{a}{b}\right) = 4 \mid p-1$

ASSURDO

$a = pa_1$, $b = pb_1$ $\qquad \left(\frac{n}{p^2}\right) = a_1^2 + b_1^2$

$x^2 + y^2 = z^2$

$(x+iy)(x-iy)$ $\qquad \gcd(x+iy, x-iy)$

$\gcd(2x, x+iy) = 1$

Se $p \mid 2x$ e $p \mid x+iy$ $\quad p \mid 2$

$p \mid x \Rightarrow p \mid y$

$x = p(a+bi) \Rightarrow x = \overline{x} = \overline{p}\ \overline{(a+bi)}$

$\overline{a+bi} = a-bi$

Otteniamo $\overline{p} \mid x$ $\qquad p\overline{p} \mid x,\ p\overline{p} \mid y$ $\quad (p\overline{p} \in \mathbb{Z})$

$1+i \mid x+iy \Rightarrow 1+i \mid (x+iy) - y(1+i) = x-y$

$1+i \mid x-y \Rightarrow 1-i \mid x-y \Leftrightarrow 2 \mid x-y$

ATTENZIONE

x, y entrambi dispari (assurdo mod 4)

$x+iy = (m+in)^2 = (m^2-n^2) + i(2mn)$

$x = m^2-n^2, \quad y = 2mn, \quad z = m^2+n^2$

Abbiamo perso $x+iy = (m+in)^2 \cdot$ le unità non banali

$\begin{cases} y^3 - 11^x = 4 \\ x \text{ pari} \end{cases}$ mod 5 $y^3 - 1 \equiv 4 \ (5)$

$\Rightarrow y^3 \equiv 0 \ (5) \Rightarrow 5 \mid y$

$5^3 - 4 = 121$ $(x = 2, \ y = 5)$

Mod 25? $-11^x \equiv 4 \pmod{25}$

$11^x \equiv 11^2 \pmod{25}$

$11^{x-2} \equiv 1 \pmod{25}$

$11, \ 11^2 \equiv -4, \ 11^3 \equiv -44 \equiv 6, \ 11^4 \equiv 16 \quad 11^5 \equiv 1 \pmod{25}$

$y^3 - 11^{2z} = 4$

$y^3 = 11^{2z} + 4 = (11^z + 2i)(11^z - 2i)$

$\text{mcd}(11^z + 2i, \ 11^z - 2i) = \text{mcd}(2 \cdot 11^z, \ 11^z + 2i)$

$= \text{mcd}((1+i)(1-i)11^z, \ 11^z + 2i)$

$= \text{mcd}((1+i)(1-i), \ 11^z + 2i) =$

$= \text{mcd}(2, \ 11^z) = 1$

$(11^z + 2i) = (a + bi)^3 \Rightarrow \quad 2i = 3a^2bi - b^3i$

$2 = b(3a^2 - b^2) \qquad b \mid 2$

$i = (-i)^3, \quad (-1) = (-1)^3, \quad (-i) = i^3$

"Stime"

$\frac{p(n)}{q(n)} \in \mathbb{Z}$ per infiniti valori di n

$\Rightarrow$ $q(x) \mid p(x)$ come polinomi

$p(x) = q(x)\, r(x) + s(x)$, $\deg s(x) < \deg q(x)$ oppure $s(x) = 0$

$r(x),\ s(x) \in \mathbb{Z}[x]$

$\frac{p(n)}{q(n)} = \underset{\in \mathbb{Z}}{r(n)} + \frac{s(n)}{q(n)} \in \mathbb{Z}$ infinite volte

Per n molto grande $\left|\frac{s(n)}{q(n)}\right| < 1$

$s(x) = x^k + \dots$ $\quad q(x) = x^h + \dots$ $\quad h > k$

$$\frac{s(n)}{q(n)} = \frac{x^k + \dots}{x^{h-k}\left(x^k + \dots\right)}$$ limitata

va a $+\infty$

Perciò $s(n)/q(n) = 0$ infinite volte $\Rightarrow s \equiv 0$

$p(n)$ è divisibile per infiniti primi

$$p(X) = a_n X^n + \dots + a_1 X + a_0$$

Caso facile: $a_0 = 1$, supponiamo solo finiti primi $q_1, \dots, q_k$

$$p(h\, q_1 \cdots q_k) \equiv 1 \ (q_i)$$

Può capitare sia proprio $= 1$, ma al variare di h non sarà sempre $= 1$.

Caso a_0 generico $\quad p(a_0 X) =$

$$= a_0 \left(a_0^{n-1} X^n \cdot a_n + \dots + a_1 X + 1 \right)$$

$q_1, \dots, q_k$. Fissiamo M.

Tra i numeri $\le M$ quanti si fattorizzano solo con i q_j?

$$q_1^{a_1} \cdots q_k^{a_k} \le M$$

$$a_1 \le \log_{q_1} M \le \log_2 M$$

Sono al più $(1+\log_2 M)^k$

Quanti sono i valori assunti dal polin. e $\le M$?

$P(x) = a_n x^n + \dots$

$x = 0, \dots, \ell \qquad a_n \ell^n < M \qquad \ell \sim \sqrt[n]{M/a_n}$

$\ell \gtrsim c \cdot M^{1/n}$

$$c \cdot M^{1/n} < (1+\log_2 M)^k \quad \forall M$$

$M = 2^{t \cdot n} \qquad c \cdot 2^t < (1+nt)^k$ NO

(CONFRONTARE AMMISSIONE SNS)

Dato m,
Esistono m interi consecutivi non della forma

$$a^5 + b^7 + c^{11}$$

Fisso M. I numeri $\le M$ quanti sono?

$a \le M^{1/5} \qquad b \le M^{1/7} \qquad c \le M^{1/11}$

Non sono di più di $M^{1/5} \cdot M^{1/7} \cdot M^{1/11}$.

$\underbrace{1\ 2\ 3}_{m}\ \underbrace{\quad}_{m}\ \dots\ \underbrace{\quad M \quad}_{m}$

Cassetti $= M/m$

$M^{\frac{1}{5}+\frac{1}{7}+\frac{1}{11}} \geq \frac{M}{m} \quad \forall M$ $\qquad \alpha < 1$

$m \geq M^{1-\alpha} \quad \forall M$ per M grande è falsa!

Esistono m interi cons. non potenze perfette

Fissiamo M. Le potenze perfette quante sono?

$$\leq \sqrt{M} + M^{1/3} + \dots + M^{1/k}$$

$2^k > M \qquad k = \log_2 M$

$$\leq \underbrace{(\log_2 M)}_{\text{n° termini}} \cdot \underbrace{M^{1/2}}_{\text{ogni termine}}$$

Se la tesi fosse falsa, $M/m \leq M^{1/2} \log_2 M$, che però diventa falsa DEFINITIVAMENTE

$n \equiv p \pmod{p^2}$ $\qquad p_1, \dots, p_m$

$$\begin{cases} n \equiv p_1 \pmod{p_1^2} \\ 1+n \equiv p_2 \pmod{p_2^2} \\ \vdots \\ n+m-1 \equiv p_m \pmod{p_m^2} \end{cases}$$

TCR $\Rightarrow \exists\, n$ soluz

Sia $f: \mathbb{N} \longrightarrow \mathbb{N}$ t.c. per ogni coppia a, b di interi $af(a) + 2ab + bf(b)$ è un quadr. perf. $\Rightarrow f(n) = n \quad \forall n$

- $a = p$ primo, $b = 0$ $\quad pf(p) = \square$

  $f(p) = p \cdot g(p)^2 \qquad p \mid f(p)$

- $pf(p) + 2p + f(1) = m^2$

  $pf(p) + 4p + 2f(2) = n^2$

Supponiamo $f(p) \neq p \Rightarrow f(p) \geq 2p \Rightarrow m, n \geq \sqrt{2}\, p$

$$2p + (2f(2) - f(1)) = n^2 - m^2 \geq (m+1)^2 - m^2 = 2m+1 \geq 2\sqrt{2}\, p + 1$$

Questo è falso per p abbast. grande.

$\Rightarrow f(p) = p$ per tutti i p grandi

- Per ogni a, $p \gg 1$ $\quad a^2 + 2ap + p^2 = \square$

  $af(a) + 2ap + p^2 = \square$

  ($p \cdot f(p)$)

  $a(a - f(a)) =$ differenza di $\square$

  (a: costante risp. p)

Da qui assurdo per $p \to \infty$, perché

$\square - \square$ va a $+\infty$, ma è costante.

Esiste una potenza di 2 che, in base 10,

contiene le cifre 1372546 (per dire)

$$2^n = 137\ldots = 1{,}37\ldots \cdot 10^m$$

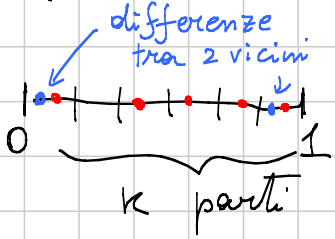
$$n \log_{10} 2 = m + \log_{10}(1{,}37\ldots)$$

m: intero; $\log_{10}(1{,}37\ldots)$: $0 < \bullet < 1$

Ci interessa $\{n \cdot \log_{10} 2\} =$ quasi uguale $\log_{10}(1{,}37\ldots)$

Con la successione $\{n \cdot \log_{10} 2\}$ approssimo bene

ogni numero reale.



$\{n \log_{10} 2\}$ per $k+1$ valori distinti di n

Diciamo che n_0 fa sì che $\{n_0 \log 2\} < 1/k$

$\{2n_0 \log 2\}$, $\{3n_0 \log 2\}$