Stage Senior 2016 – Livello Basic

Stampato integrale delle lezioni

Autori vari

Indice

Preliminari – Ludovico Pernazza 4
Algebra 1 – Danilo Ciaffi 10
Algebra 2 – Marco Trevisiol 22
Algebra 3 – Marco Trevisiol 42
Combinatoria 1 – Samuele Mongodi 66
Combinatoria 2 – Giovanni Paolini 78
Geometria 1 – Danilo Ciaffi 90
Geometria 2 – Alessandra Caraceni 101
Geometria 3 – Alessandra Caraceni 109
Teoria dei Numeri 1 – Kirill Kuzmin 118
Teoria dei Numeri 2 – Giovanni Paolini 133

Induzione e Pigeonhole (Ludo)

Note Title 9/1/2016

Teorema 0 La proprietà $P(n)$ vale per $n=0$ Dim. ----

Teorema 1 Se $P(0)$ è vera, è vera anche $P(1)$ Dim. ---

Teorema 2 " $P(1)$ " " " " $P(2)$ Dim. ---

Teorema 3 " $P(2)$ " " " " $P(3)$ Dim. ---

Teorema 4 - - Dim

$\vdots$ $\vdots$

6 P_6

5 P_5

4 P_4

3 P_3

Per tutti gli n io so dim. Teorema n con Dim. n.

Allora vale il meta-teorema: $P(n)$ è vera per ogni n naturale.

Ipotesi dell'induzione standard
- $P(n)$ proprietà su $n \in \mathbb{N}$
- 1) $P(0)$ è vera (passo base)
- 2) $\forall n \in \mathbb{N} \setminus \{0\}$, se $P(n-1)$ è vera, è vera anche $P(n)$ (passo induttivo)

$\forall$ = "per ogni" $\Rightarrow$ = "implica" $P(n-1) \Rightarrow P(n)$

$\exists$ = "esiste"

$P(n) = " \sum_{i=0}^{n} i = \frac{n(n+1)}{2} "$ 1) $P(0)$: $\sum_{i=0}^{0} i = \frac{0\cdot(0+1)}{2}$ vera

$\sum_{i=0}^{0} i$ = 0 " 0

2) $P(n-1) \Rightarrow P(n)$

so che $\sum_{i=0}^{n-1} i = \frac{(n-1)(n-1+1)}{2}$ ipotesi induttiva

so da questo dedurre $P(n)$?

$\sum_{i=0}^{n} i \stackrel{?}{=} \frac{n(n+1)}{2}$

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

$= n\left(\frac{n-1}{2} + 1\right) = n\left(\frac{n+1}{2}\right) = \frac{n(n+1)}{2}$ □

$$\sum_{i\geq 0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \qquad \sum_{i\geq 0}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$$

$$P(n) = \sum_{i=1}^{n} \frac{i}{4^i} < \frac{1}{2}$$

L'induzione può partire da $n_0 > 0$. $\tilde{P}(n) = P(n+n_0)$

$n_0 = 1$

$P(1)$: $\sum_{i=1}^{1} \frac{i}{4^i} < \frac{1}{2}$ $\qquad \frac{1}{4} < \frac{1}{2}$ ok. base

$n-1 \to n$ $\qquad \sum_{i=1}^{n-1} \frac{i}{4^i} < \frac{1}{2}$ $P(n-1)$ $\qquad \sum_{i=1}^{n} \frac{i}{4^i} \overset{?}{<} \frac{1}{2}$ $P(n)$

$$\sum_{i=1}^{n} \frac{i}{4^i} = \sum_{i=1}^{n-1} \frac{i}{4^i} + \frac{n}{4^n} < \frac{1}{2}$$

$\sum_{i=1}^{n-1} \frac{i}{4^i}$ $\qquad \frac{1}{2}$

$Q(n)$: $\sum_{i=1}^{n-1} \frac{i}{4^i} \leq \frac{1}{2} - \frac{1}{2^{n+1}}$ $\qquad$ oss.: se $Q(n)$ è vera $\forall n$, anche $P(n)$ lo è

1) $Q(1)$: $\frac{1}{4} \leq \frac{1}{4}$

2) $Q(n-1) \Rightarrow Q(n)$?

$$\sum_{i=1}^{n-1} \frac{i}{4^i} \leq \frac{1}{2} - \frac{1}{2^n}$$

$$\sum_{i=1}^{n} \frac{i}{4^i} = \sum_{i=1}^{n-1} \frac{i}{4^i} + \frac{n}{4^n} \leq$$

$\sum_{i=1}^{n-1} \frac{i}{4^i} \leq \frac{1}{2} - \frac{1}{2^n}$

$$\leq \frac{1}{2} - \frac{1}{2^n} + \frac{n}{4^n} \overset{?}{\leq} \frac{1}{2} - \frac{1}{2^{n+1}}$$

Vera se e solo se

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

$2n \leq \frac{4^n}{2^n} = 2^n$ per ogni $n \geq 1$ (induzione ausiliaria)

Quindi è vera $Q(n)$ per ogni n, e così anche $P(n)$ lo è.

Bernoulli: x reale > -1, $\forall n \in \mathbb{N}$ $1 + nx \leq (1+x)^n$.

$n \geq 4$ $\quad n^2 \leq 2^n$

Induzione "forte" o "estesa".

$P(n)$ proprietà di $n \in \mathbb{N}$

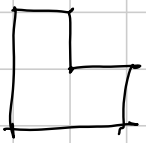
Se (ipotesi dell'induzione forte o estesa)
1) $P(0)$ è vera
2) Se $P(0), P(1), \dots, P(n-1)$ sono vere, anche $P(n)$ è vera, per ogni n.

allora $P(n)$ è vera per ogni n.

$Q(n) =$ "$P(k)$ è vera per $k \leq n$" : le due forme di induzione sono equivalenti.

"Ogni $n \in \mathbb{N}$ $n > 1$ è fattorizzabile in prodotto di un numero finito di fattori primi"

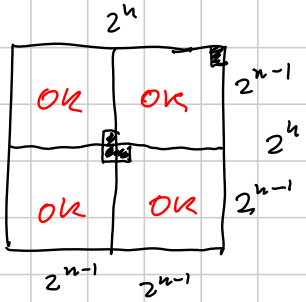
Tutte le scacchiere $2^n \times 2^n$ senza una casella d'angolo si possono tassellare con trimini a L



$n = 0$ diciamo di sì

$n > 1$ ok

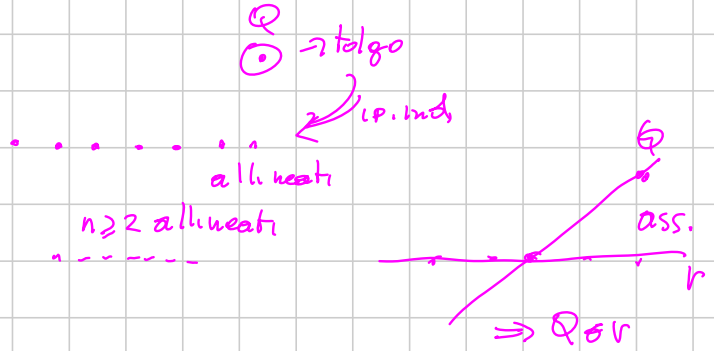
$P(n-1) \Rightarrow P(n)$



Controesempio: $n \geq 3$ punti nel piano sono tali che la retta che passa per (qualunque) due di essi contiene anche (almeno) un terzo punto di essi. Dim. che i punti sono tutti allineati.

$P(3)$: vero

$P(n-1) \Rightarrow P(n)$



Principio dei cassetti (pigeonhole)

Se ho $n+1$ oggetti e li divido in n classi almeno una classe contiene almeno due oggetti

Se ho $kn+1$ oggetti e li divido in n classi almeno una classe contiene almeno $k+1$ oggetti

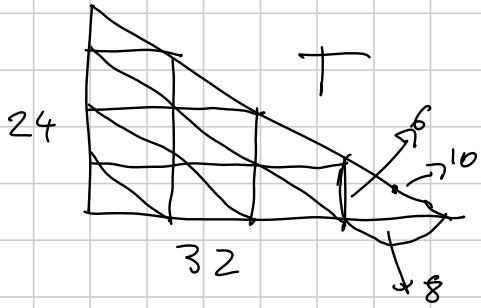
34 quanti almeno con il compleanno nello stesso mese?
4 sul pianeta Zork dove un anno ha 4 mesi

è vero che due persone conoscono lo stesso numero di altre nell'aula?
Classi $= C_0, C_1, \dots, C_{33}$
Oss.: non è possibile che sia C_0 che C_{33} siano non vuote.
C_0 non è vuota ($\Rightarrow C_{33}$ è vuota) $\Rightarrow$ 33 classi, 34 persone. ✓
C_0 è vuota

n+1 interi tra 1 e 2n. Dim. che
a) 2 sono coprimi
b) 2 sono uno mult. dell'altro.

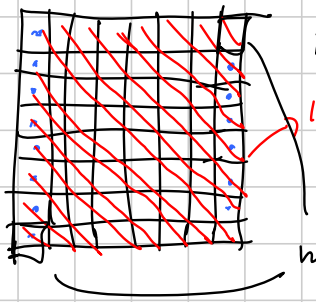
a) 1 2 3 4 5 6 - 2n-1 2n

b) 1 2 4 8 ... 2^k
3 6 12 24 ... $3 \cdot 2^k$
5 10 20 ... $5 \cdot 2^k$
19
} in classi, quante i numeri dispari.



InT ci sono 17 punti
Dim. che esiste un semicerchio di raggio 5 che ne copre 3.

Scacchiera 8×8. Quanti alfieri ci posso mettere al massimo che non si attaccano?



Minimo n per cui tra n interi positivi che hanno fattori primi ≤ 30 ce ne sono sempre 2 il cui prodotto è un quadrato perfetto. 2^{10}

Massimo n numero di targhe di 6 cifre con sempre almeno 2 cifre diverse.

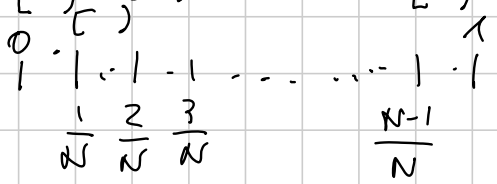
Teorema di Dirichlet sull'approssimazione diofantea:

α numero reale irrazionale. $\forall N$ intero positivo $\exists$ frazione $\frac{p}{q}$ con $q \leq N$ t.c. $\left|\frac{p}{q} - \alpha\right| < \frac{1}{N^2}$ → è q^2

Dim. $\{0\cdot\alpha\}\ \{1\cdot\alpha\}\ \{2\cdot\alpha\}\ \dots\ \{N\cdot\alpha\}$ $\{\ \}$ = parte frazionaria

nessuna è $0, \frac{1}{N}, \frac{2}{N}, \dots \frac{N-1}{N}$ (tranne $0\cdot\alpha$)

$0 < \{i\cdot\alpha\} < 1$ $\forall i = 0, \dots, N$



$\Rightarrow$ $\{i\cdot\alpha\}$ e $\{j\cdot\alpha\}$ sono nello stesso intervallino per certi opportuni indici i e j. Supp. $i > j$

$$0 < \{(i-j)\cdot\alpha\} < \frac{1}{N}$$

$$i\cdot\alpha = K + \{i\cdot\alpha\}$$
$$j\cdot\alpha = H + \{j\cdot\alpha\}$$

$$(i-j)\cdot\alpha = K - H + \{(i-j)\cdot\alpha\}$$

$$\alpha = \frac{K-H}{i-j} + \frac{\{(i-j)\cdot\alpha\}}{i-j}$$

$$\left|\alpha - \frac{K-H}{i-j}\right| = \frac{\{(i-j)\cdot\alpha\}}{i-j} < \frac{\frac{1}{N}}{i-j}$$

A1 Basic

Danilo

Note Title 9/3/2016

Polinomi e numeri complessi

NUMERI COMPLESSI STRIKE BACK

$$\mathbb{C} = \{ a+ib \mid a,b \in \mathbb{R},\ i^2 = -1 \}$$

$$z = \rho(\cos\theta + i\sin\theta) = \rho e^{i\theta}$$

Operazioni

- SOMMA
- PRODOTTO
- CONIUGIO
- MODULO

$$\frac{z}{w} = \frac{a+ib}{c+id} = \frac{a+ib}{c+id}\cdot\frac{c-id}{c-id} = \frac{(a+ib)(c-id)}{c^2+d^2} = \frac{(ac+bd)+i(bc-ad)}{c^2+d^2}$$

Abbiamo scoperto che $\frac{1}{w} = \frac{\bar{w}}{|w|^2}$ $\left(\Rightarrow w\bar{w} = |w|^2\right)$

PROPRIETÀ

- $\overline{wz} = \bar{w}\cdot\bar{z}$
- $\overline{w+z} = \bar{w}+\bar{z}$
- $|w\cdot z| = |w||z|$
- $|z+w| \leq |z|+|w|$

$$\left(\mathbb{R} = \{ a+ib \in \mathbb{C} \mid b=0 \} = \{ z \in \mathbb{C} \mid z = \bar{z} \} \right)$$

Formula di de Moivre

$$z^n = \left[\rho(\cos\theta + i\sin\theta)\right]^n = \rho^n(\cos(n\theta) + i\sin(n\theta))$$

$$z^n = (\rho e^{i\theta})^n = \rho^n e^{in\theta}$$

Perché questi complessi?

$x^2 + 2x + 1 = 0$

$x^2 + 1 = 0$

non ha soluz $x = \pm i$

$x^2 - 1 = 0$

$x^2 + 2x + 3 = 0$

$-1 \pm \sqrt{-2}$

$\sqrt{-2} = 0 + i(\sqrt{2})$

Non è forse che $p(x)$ ha sempre radici in $\mathbb{C}$?

Polinomi

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

n: deg p; a_n: coefficiente direttore; a_1: termine lineare; a_0: termine noto

$a_n = 1$, p è monico

$a_n, a_{n-1}, a_{n-2}, \dots, a_1, a_0 \in \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \square, \dots$

Tra polinomi funziona la divisione con resto! Cioè se ho due polinomi $a(x)$, $b(x)$, esistono altri due polinomi $q(x)$ e $r(x)$ t.c.

$$a(x) = q(x)b(x) + r(x), \quad \deg r < \deg b$$

Def (MCD) Dati $a(x)$, $b(x)$, esiste $d(x)$ t.c.:

- $d(x) \mid a(x)$
- $d(x) \mid b(x)$
- Se $e(x)$ t.c. $e(x) \mid a(x)$ e $e(x) \mid b(x)$ allora $e(x) \mid d(x)$

L'algoritmo di Euclide funziona (in particolare è vero che $(a(x), b(x)) = (b(x), r(x))$)

(Identità di Bézout) $a(x), b(x), d(x) = (a(x), b(x))$, esistono $h(x), k(x)$ t.c.

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

Dim $a(x) = b(x)q(x) + r(x)$

$d(x) = (b(x), r(x))$ | Induzione su deg b

Supponiamo che Bézout valga per i polinomi di grado $\leq$ deg a

$$d(x) = b(x)h'(x) + r(x)k'(x)$$

$$r(x) = a(x) - b(x)q(x)$$

$$d(x) = b(x)h'(x) + \left(a(x) - b(x)q(x)\right)k'(x) =$$

$$= b(x)h'(x) + a(x)k'(x) - b(x)q(x)k'(x) =$$

$$= a(x)k'(x) + b(x)\underbrace{\left(h'(x) - q(x)k(x)\right)}_{\text{polinomio}}$$

□

Ruffini (Odi et amo)

$b(x) = x - \alpha$

$a(x) = (x-\alpha)q(x) + r(x)$ ← chi è?

$\deg b \geq \deg r \Rightarrow r$ è un polinomio di grado 0
calcoliamo tutto in $x = \alpha$

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

$$\boxed{a(x) = (x - \alpha)\, q(x) + a(\alpha)}$$

Cor (Ruffini che conoscevate)
se $p(\alpha) = 0 \Rightarrow (x - \alpha) \mid p(x)$

Cor Un polinomio di grado n ha al più n radici

$\deg p = n$
$p(x) = (x - \alpha_1)\, q(x)$ ha $\deg n-1$
↳ ↳ ...

Criterio di identità dei polinomi Se $a(x)$ e $b(x)$ $\deg a, \deg b < n$, se $a(x_i) = b(x_i)$ $i = 1, \dots, n$
$\Rightarrow a(x) = b(x)$.

$p(x) = a(x) - b(x)$
$p(x_i) = a(x_i) - b(x_i) = 0$ per $i = 1, \dots, n$

$\Rightarrow p(x) \equiv 0 \Rightarrow a(x) = b(x)$

Fattorizzazione unica Un polinomio $a(x)$ ammette un'unica scrittura come

$$a(x) = f_1(x)^{\alpha_1} \cdot \dots \cdot f_n(x)^{\alpha_n}$$

dove f_i sono irriducibili (:= "non hanno divisori")

Interpolazione di Lagrange

(x_i, y_i) $i = 1, \dots, n$ voglio trovare un polinomio t.c. $p(x_i) = y_i$ $\forall i = 1, \dots n$. Esiste?
Sì, e lo costruiamo:

$$p_i(x) = \frac{(x-x_1)(x-x_2)\dots(x-x_{i-1})(x-x_{i+1})\dots(x-x_n)}{(x_i-x_1)(x_i-x_2)\dots(x_i-x_{i-1})(x_i-x_{i+1})\dots(x_i-x_n)}$$

$p_i(x_i) = 1$ $\qquad$ $p_i(x_j) = 0$ per $j \neq i$

$$P(x) = \sum_{i=1}^{n} p_i(x)\, y_i$$ funziona!

$P(x)$ ha grado $n-1$

Polinomi a coefficienti interi

Lemma (degli zeri razionali) $p(x) = a_n x^n + \dots + a_1 x + a_0$ a coefficienti interi, $\frac{q}{r}$, $q, r \in \mathbb{Z}$, $(q,r) = 1$.
se $p(\frac{q}{r}) = 0$ allora $q \mid a_0$, $r \mid a_n$

Dim $0 = p\left(\frac{q}{r}\right) = a_n\left(\frac{q}{r}\right)^n + a_{n-1}\left(\frac{q}{r}\right)^{n-1} + \dots + \left(\frac{q}{r}\right)a_1 + a_0 =$

$$= \underbrace{a_n q^n + a_{n-1} q^{n-1} r + \dots + a_1 q r^{n-1}}_{\text{div. per } q} + \underbrace{a_0 r^n}_{\text{div per } r}$$

Siccome $(q,r) = 1$, $\Rightarrow$ a_n deve essere divisibile per r
allo stesso modo a_0 deve essere divisibile per q. D

Lemma $p(x)$ a coefficienti interi, $a, b \in \mathbb{Z}$, $a \neq b$
$\rightarrow$ $a - b \mid p(a) - p(b)$

Dim

$p(x) = (x-a)\,q(x) + \underbrace{r(x)}_{\text{è } p(a)}$ e calcolo in b

$p(b) = (b-a)\,q(x) + p(a) \Rightarrow p(a) - p(b) = (a-b)\,q(b)$ D

Polinomi a coefficienti razionali

Teorema di Gauss $p(x)$ monico a coefficienti razionali.
$p(x)$ è irriducibile su $\mathbb{Q} \iff p(x)$ è irriducibile su $\mathbb{Z}$.

Polinomi a coefficienti complessi

Teorema Ogni polinomio a coefficienti in $\mathbb{C}$ ammette radici in $\mathbb{C}$.

Teorema (fondamentale dell'algebra)
$p(x)$ è un polinomio a coefficienti complessi di grado n e $x_1, \dots x_n$ sono le sue radici posso scrivere

$$p(x) = \alpha (x - x_1)(x - x_2) \dots (x - x_n)$$

Polinomi a coefficienti reali

Teorema (bello) Ogni polinomio a coefficienti reali si spezza in fattori di grado 1 o 2.

Dim Lemma preliminare: se $p(\underbrace{z}_{\in \mathbb{C}}) = 0$ allora $p(\bar{z}) = 0$

$$\begin{aligned} 0 &= a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0 = \\ &= \overline{a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0} = \\ &= a_n \bar{z}^n + a_{n-1} \bar{z}^{n-1} + \dots + a_1 \bar{z} + a_0 = p(\bar{z}) \end{aligned}$$

#

Per induzione sul grado (uso l'induzione forte: il teorema vale per ogni $q(x)$, $\deg q < n$)

- $p(x)$ ha una radice $\alpha \in \mathbb{R}$

allora $p(z) = q(z)(z-\alpha)$ → ha grado $< n$ ✓

- $p(z)$ ha una radice $\alpha \in \mathbb{C}\setminus\mathbb{R}$

$(z-\alpha) \mid p(z) \xrightarrow[\text{lemma}]{} (z-\bar{\alpha}) \mid p(z)$

$(z-\alpha)(z-\bar{\alpha}) \mid p(z)$

$\alpha+\bar{\alpha} = a+ib+(a-ib) = 2a = 2\,\mathrm{Re}\,\alpha$

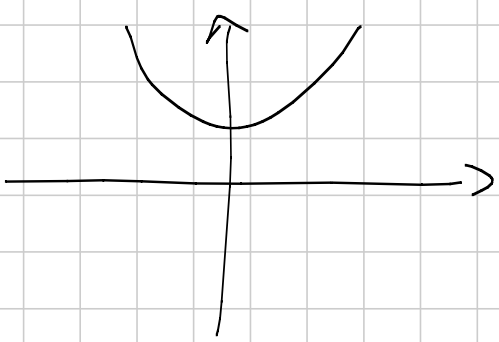
$z^2 - (\alpha+\bar{\alpha})z + \alpha\bar{\alpha} = z^2 - 2\,\mathrm{Re}\,\alpha\, z + |\alpha|^2$

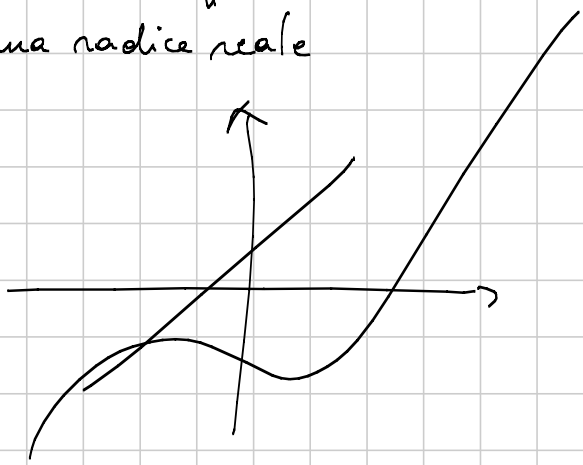
$z^2 - 2\,\mathrm{Re}\,\alpha\, z + |\alpha|^2 \mid p(z)$

significa $p(z) = (z^2 - 2\,\mathrm{Re}\,\alpha\, z + |\alpha|^2)\, q(z)$

$q(z)$ ha grado $n-2$ □

Corollario Ogni polinomio a coefficienti reali di grado dispari ha una radice reale





Formule di Viète

$(x-\lambda_1)(x-\lambda_2) = x^2 - (\lambda_1+\lambda_2)x + \lambda_1\lambda_2$

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

$p(x)$ di grado n e monico

$$p(x) = 1\cdot(x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n) =$$

$$= x^n + \left(-\lambda_1-\lambda_2-\lambda_3,\cdots-\lambda_n\right)x^{n-1} + \left(\lambda_1\lambda_2+\lambda_1\lambda_3+\cdots\right)x^{n-2} +$$

$$\cdots + (-1)^{n-1}\left(\lambda_1\lambda_2\cdots\lambda_{n-1}+\cdots\right)x + (-1)^n\lambda_1\lambda_2\lambda_3\cdots\lambda_n$$

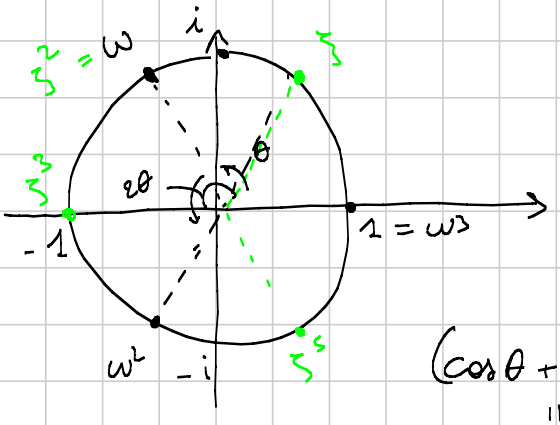
Tutti i coefficienti si scrivono in funzione di somme simmetriche nelle radici

$$S_k = \lambda_1^k + \lambda_2^k + \cdots + \lambda_n^k$$

Tutti i coefficienti si esprimono come somme e prodotti degli S_k.

Radici dell'unità

Sono quei numeri complessi per cui esiste $n\in\mathbb{N}\setminus\{0\}$, t.c. $z^n = 1$



ω è una radice terza

$\omega^3 = 1$

$$\omega = \underbrace{\rho}_{=1}(\cos\theta + i\sin\theta)$$

$$(\cos\theta + i\sin\theta)^3 = 1$$

$$\cos(3\theta) + i\sin(3\theta)$$

Quale angolo θ è t.c. $3\theta = \frac{2\pi}{3}$

$z^n = 1 \Rightarrow z^n - 1 = 0$ sono n radici

ζ radice sesta $\zeta^6 = 1$. In particolare

$(\zeta^2)^3 = 1 \Rightarrow \zeta^2$ è una radice terza.

Una radice n-esima si dice primitiva se non è una radice d-esima per nessun $d|n$.

$\zeta, \zeta^2, \zeta^{(3)}, \dots \zeta^{(n)} = 1$

se divide n

tutti gli esponenti coprimi con n mi danno radici primitive (attenzione: devo essere partito da una radice primitiva)

Domanda: come si fattorizza $x^n - 1$?

Pag 13 69, 70, 72, 75, 77

Pag 23 4, 5, 7, 8, 11.

(72) $p(2) = a \quad p(a) = a + 2$

$a - 2 \mid p(a) - p(2) = a + 2 - a = 2$

$a - 2 = \pm 1, \pm 2$

(75) $p(x) = \frac{(x-a)(x-b)}{(c-a)(c-b)} + \frac{(x-b)(x-c)}{(a-b)(a-c)} + \frac{(x-a)(x-c)}{(b-c)(b-a)} = 1$

$p(x) - 1 = 0$ (deg 2) ha 3 radici (a, b, c).

(7) • Esiste un polinomio t.c. $p(n) = 2^n \ \forall 0 \le n \le k$?
• Ne esiste uno t.c. $p(n) = 2^n \ \forall n \in \mathbb{N}$?

1) Certo: Interpolazione di Lagrange

$(0,1)\ (1,2)\ (2,4), \dots\ (k, 2^k)$ ← $k+1$ valori

Con Lagrange so trovare il polinomio che cerco che avrà grado k.

2) $P(n) = 2^n$, $P(n+1) = 2^{n+1}$ ~~$(g(x) = P(x) - 2^x)$~~

Costruisco $g(x) = P(x+1) - 2P(x)$.

$g(n) = 0 \ \forall n \in \mathbb{N}$, quindi $g \equiv 0$

$$P(x+1) = 2P(x)$$

$$a_n \underbrace{(x+1)^n}_{a_n x^n + (\dots)} + \dots = 2a_n x^n + \dots \Rightarrow a_n = 2a_n \Rightarrow a_n = 0$$

ma non soddisfa le mie richieste.

(8) Polinomio $P(x)$, $P(0)=2$, $P(1)=4$, $P(2)=6$, $P(3)=56$

$p(x) = x\,q(x) + p(0)$ $\quad q(x) = x(x-1)(x-2)(x-3)$

Ho un polinomio di terzo grado (il resto!) di cui conosco 4 valori distinti.

⇒ Uso Lagrange per trovare il polinomio che passa per quei 4 valori.

(11) $p(x)$ di grado 2002

"Prendo" valori $a_1, a_2, \dots a_{2002}$

$$\begin{cases} P_1(x) = x - a_1 \\ P_{n+1}(x) = P_n(x)^2 - a_{n+1} \end{cases}$$

$$p(x) = \alpha (x-\lambda_1)(x-\lambda_2) \dots (x-\lambda_{2002})$$

$P(x) \mid P_{2002}(x)$ significa che $P_{2002}(\lambda_i) = 0$

$$0 = P_{2002}(\lambda_i) = \left[P_{2001}(\lambda_i)\right]^2 - a_{2002}$$

vuol dire che $P_{2001}(\lambda_i)$ deve essere una costante per tutti: λ_i.

Rienunciamo: Voglio riuscire a trovare $a_1, \dots, a_{k+1}$ t.c. $P_k(\lambda_i) = \text{cost}$ per $i = 1, \dots k+1$

Procediamo per induzione:

- $\boxed{k=1}$ deve valere $P_1(x) = x - a_1$

$$(\lambda_1 - a_1)^2 = (\lambda_2 - a_1)^2$$

devono essere uno l'opposto dell'altro

$$a_1 = \frac{\lambda_1 + \lambda_2}{2}$$

- Passo induttivo $\boxed{k \Rightarrow k+1}$

Ho già scelto $a_1 \dots a_k$ che funzionano, cioè tali che $P_k(\lambda_i) = \text{cost}$ per $i = 1, \dots k$.

Devo controllare il $k+1$-esimo

$$P_{k+1}(\lambda_i) = P_k(\lambda_i)^2 - a_{k+1}$$

per $i = 1, \dots, k$ $P_k(\lambda_i) = \text{cost}$.

$$P_{k+1}(\lambda_{k+2})^2 = P_{k+1}(\lambda_1)^2$$

$$\left(P_k(\lambda_{k+2})^2 - a_{k+1}\right)^2 \stackrel{?}{=} \left(P_k(\lambda_1)^2 - a_{k+1}\right)^2$$

Di nuovo devono essere opposti:

$$P_k(\lambda_{k+2})^2 - a_{k+1} = a_{k+1} - P_k(\lambda_1)^2$$

$$\boxed{a_{k+1} = \frac{P_k(\lambda_{k+2})^2 + P_k(\lambda_1)^2}{2}}$$

□

A2 - Basic Tess

Note Title 9/4/2016

Disuguaglianze

Es: ① mostrare che $\forall\, a,b,c \in \mathbb{R}$ si ha

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

② mostrare che $\forall\, a,b,c>0$ si ha [Nesbitt]

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

③ $\forall\, a,b,c>0$ si ha [IMO 2001-2]

$$\frac{a}{\sqrt{a^2+8bc}}+\frac{b}{\sqrt{b^2+8ca}}+\frac{c}{\sqrt{c^2+8ab}} \geq 1$$

④ $\forall\, a,b,c>0$ t.c. $abc=1$ si ha

$$\frac{1}{a+b+1}+\frac{1}{b+c+1}+\frac{1}{c+a+1} \leq 1$$

[Canada 1997]

Notazione: somme cicliche e simmetriche

es: $\sum_{cyc} \frac{1}{a+b+1} = \frac{1}{a+b+1}+\frac{1}{b+c+1}+\frac{1}{c+a+1}$

↳ sottintendo su a,b,c

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

↳ sottintendo su a, b, c

$$\sum_{sym} ab = ab + bc + ca + ac + ba + cb = 2\sum_{cyc} ab$$

es: (1) $\sum_{c} a^2 \geq \sum_{c} ab$

Bernoulli $(1+x)^n \geq 1+nx \quad \forall\, x > -1 \quad \forall\, n \in \mathbb{N}$

$(1+x)^n \geq 1 + nx + \binom{n}{2}x^2 \quad \forall\, x \geq 0 \quad \forall\, n \in \mathbb{N}$

(invece $\leq$ se $x \in (-1, 0)$)

$(1+x)^r \geq 1 + rx \quad \forall\, x > -1, \forall\, r \geq 1$

(invece $\leq$ se $r \in (0, 1)$)

Molte disuguaglianze discendono da

$$\forall x \in \mathbb{R} \qquad x^2 \geq 0$$

di conseguenza $x^2 + y^2 \geq 0$

$$\sum_{i=0}^{n} x_i^2 \geq 0 \quad \text{[S.O.S.]}$$

(1) prendete $x = a-b$ $y = b-c$ $z = c-a$

$$\sum_{c} (a-b)^2 \geq 0$$

$$\sum_{c} a^2 - 2ab + b^2 \geq 0$$

$$\sum_{c} 2a^2 - 2ab \geq 0$$

$$\sum_{c} a^2 \geq \sum_{c} ab$$

C'è un caso di uguaglianza:

quando $x_0 = x_1 = \dots = x_n = 0$

$a^2 + b^2 \geq 2ab$ ($x_0 = a-b$, vera)

non ha senso prendere $x_0 = a-2b$

$x_1 = \dots$

$\vdots$

→ infatti non torna l'uguaglianza

Serve l'= se $a=b$

se volete usare $(a-2b)^2 \geq 0$
non può funzionare perché
$a=b \Rightarrow (a-2b)^2 \geq 0$

AM-GM $\quad \forall a,b>0$ si ha $\frac{a+b}{2} \geq \sqrt{ab}$

vera per $(\sqrt{a}-\sqrt{b})^2 \geq 0$

in generale $a_1, \dots, a_n > 0$

$AM = \frac{\sum_{i=1}^{n} a_i}{n}$ $\qquad$ vale $AM \geq GM$

$GM = \sqrt[n]{\prod_{i=1}^{n} a_i}$ $\qquad$ $\frac{\sum a_i}{n} \geq \sqrt[n]{\prod a_i}$

Si dimostra per induzione su n

P.B. $n=2$

P.I. i) $n \Rightarrow 2n$
ii) $n+1 \Rightarrow n$

i) $\sum_{i=1}^{n} \frac{a_i}{n} \geq \sqrt[n]{\prod_{i=1}^{n} a_i}$ (la so)

$\sum_{i=1}^{2n} \frac{a_i}{2n} \geq \sqrt[2n]{\prod_{i=1}^{2n} a_i}$ (vorrei mostrare)

$A = \frac{\frac{\sum_{i=1}^{n} a_i}{n} + \frac{\sum_{i=n+1}^{2n} a_i}{n}}{2} = B$

$$\sqrt{\sqrt[n]{\prod_{i=1}^{n} a_i}\ \sqrt[n]{\prod_{i=n+1}^{2n} a_i}}$$

$C \leq D$

voglio mostrare che $\frac{A+B}{2} \geq \sqrt{CD}$

$\frac{A+B}{2} \geq \sqrt{AB}$ (P. B.) $\qquad A \geq C$ (ip. ind.) $\qquad B \geq D$ (ip. ind.)

ii) $n+1 \Rightarrow n$

ipotesi $\frac{\sum_{i=1}^{n+1} a_i}{n+1} \geq \sqrt[n+1]{\prod_{i=1}^{n+1} a_i}$

pongo $a_{n+1} = \sqrt[n]{\prod_{i=1}^{n} a_i} =: G$

$\frac{\sum_{i=1}^{n} a_i}{n} =: A \qquad \sqrt[n]{\prod_{i=1}^{n} a_i} =: P$

$\frac{nA+G}{n+1} \geq \sqrt[n+1]{P^n G}$ ma $P = G$

$\frac{nA+G}{n+1} \geq G$

$A \geq G$

$$a^3+b^3 \geq a^2b+b^2a$$

$$\frac{a^3+a^3+b^3}{3} \geq \sqrt[3]{a^6b^3} = a^2b$$

vale anche l'altra, sommando ho la tesi.

$$(1+x)^n \geq \frac{n^n}{(n-1)^{(n-1)}}x \qquad \forall\, x>0$$

$$1+x \geq n\sqrt[n]{\frac{x}{(n-1)^{n-1}}}$$

$$\frac{1+x}{n} \geq \sqrt[n]{\frac{x}{(n-1)^{n-1}}}$$

vale per AM-GM su $\left(\underbrace{\frac{1}{n-1},\frac{1}{n-1},\dots,\frac{1}{n-1}}_{n-1 \text{ volte}},x\right)$

Test iniziale n° 1

$$\begin{cases} x^4yz=1 \\ x(x+2y)(x+3z)=a \end{cases}$$

quando ho unica sol. con $x,y,z>0$?

Sol: svolgendo il prodotto ottengo

$$x^3 + 2x^2y + 3x^2z + 6xyz = 2$$

$$\frac{x^3 + 6xyz}{2} \geq \sqrt{x^4yz \cdot 6} = \sqrt{6}$$

$$\frac{2x^2y + 3x^2z}{2} \geq \sqrt{x^4yz6} = \sqrt{6}$$

$\Rightarrow 2 \geq 2\sqrt{6}$, l'= solo con $x^3 = 6xyz$
$2x^2y = 3x^2z$
$\Rightarrow \exists!$ terna

Bunching se $a, b, c \geq 0$

e $n_1 \geq m_1 \geq r_1$ sono interi tali che
$n_2 \geq m_2 \geq r_2$,,

$n_1 \geq n_2$
$n_1 + m_1 \geq n_2 + m_2$
$n_1 + m_1 + r_1 = n_2 + m_2 + r_2$

e.s. $2 \geq 0 \geq 0$
$1 \geq 1 \geq 0$

allora $\sum_{sym} a^{n_1} b^{m_1} c^{r_1} \geq \sum_{sym} a^{n_2} b^{m_2} c^{r_2}$

① $\sum_{sym} a^2 \geq \sum_{sym} 2b$

Bunching in n variabili

supponete di avere reali $t_1 \geq t_2 \geq \dots \geq t_n$
$s_1 \geq s_2 \geq \dots \geq s_n$

tali che $t_1 \geq s_1$
$t_1 + t_2 \geq s_1 + s_2$
$\vdots$
$t_1 + \dots + t_{n-1} \geq s_1 + \dots + s_{n-1}$
$t_1 + \dots + t_n = s_1 + \dots + s_n$

Allora $\sum_{sym} x_1^{t_1} \cdot \dots \cdot x_n^{t_n} \geq \sum_{sym} x_1^{s_1} \cdot \dots \cdot x_n^{s_n}$

$\forall\, x_1, \dots, x_n > 0$

Es: $\sum_{c} a^4 b \geq \sum_{c} a^2 b^2 c \quad \forall\, a, b, c > 0$

L'uguaglianza del Bunching si ha solo quando $x_1 = \dots = x_n$ (se gli esponenti sono diversi)

Un termine in a,b,c si dice omogeneo di grado $\alpha \in \mathbb{R}$ se $f(\lambda a, \lambda b, \lambda c) = \lambda^\alpha f(a,b,c)$

$(\forall \lambda > 0)$

Es: ① i termini sono omogenei di grado 2

②, ③ sono omogenei di grado 0

Es: Test Iniziale 2 disug. 2:

$a \le x$ era omog. di grado 4
a Dx " 6

se ponete $x = y = z$

$a \le x$ $\quad C_1 x^4 \le C \cdot C_2 x^6$

→ non può essere vera per ogni $x > 0$
se scegliete $x \ll 1$ non può essere vera

④ non c'è l'omogeneità

$$\sum_{cyc} \frac{1}{a+b+1} \le 1 \qquad \text{con } abc = 1$$

per renderla omogenea sostituite $\square$ $\sqrt[3]{abc}$

$$\sum_{cyc} \frac{1}{a+b+\sqrt[3]{abc}} \leq 1 \Rightarrow \frac{1}{\sqrt[3]{abc}}$$

volendo sostituite $x = \sqrt[3]{a}$ e cyc

$$\Rightarrow \sum_{cyc} \frac{1}{x^3+y^3+xyz} \leq \frac{1}{xyz}$$

Si risolve con Bunching, dopo aver tolto i denominatori

Cauchy-Schwarz per gli amici C-S

Se $x_1, \dots, x_n$; $y_1, \dots, y_n$ sono reali

allora $\left(\sum_i x_i^2\right)\left(\sum_i y_i^2\right) \geq \left(\sum_i x_i y_i\right)^2$

(volendo $\sqrt{\sum x_i^2}\sqrt{\sum y_i^2} \geq \sum_i x_i y_i$)

sia $t \in \mathbb{R} \Rightarrow$

$$(x_1 + t y_1)^2 \geq 0 \ , \ \dots \ (x_i + t y_i)^2 \geq 0$$

$$\sum_i (x_i + t y_i)^2 \geq 0$$ è polinomio di grado 2

$\Rightarrow \Delta \leq 0$

$$\Delta = \left(2\sum_i x_i y_i\right)^2 - 4\left(\sum_i x_i^2\right)\left(\sum_i y_i^2\right)$$

① $x_1 = a$, $x_2 = b$, $x_3 = c$

$y_1 = b$, $y_2 = c$, $y_3 = a$

C-S: $\left(\sum_c a^2\right)^2 \geq \left(\sum_c ab\right)^2$

Scegliendo $y_i = 1 \ \forall i$

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

$$\sqrt{\frac{\sum_i x_i^2}{n}} \geq \frac{\sum_i x_i}{n}$$

QM AM QM-AM

① $x_1 = a$, $x_2 = b$, $x_3 = c$ $\qquad \sqrt{\frac{\sum a^2}{3}} \geq \frac{\sum a}{3}$

$$3\sum_{cyc} a^2 \geq \left(\sum_{cyc} a\right)^2$$

$$= \sum_{cyc} a^2 + 2\sum_{cyc} ab$$

Lemma di Titu: se $x_1, \dots, x_n > 0$
$y_1, \dots, y_n > 0$

allora $$\sum_{i=1}^{n} \frac{x_i^2}{y_i} \geq \frac{\left(\sum_{i=1}^{n} x_i\right)^2}{\sum_{i=1}^{n} y_i}$$

Dim: $$\left(\sum_i \frac{x_i^2}{y_i}\right)\left(\sum_i y_i\right) \geq \left(\sum_i x_i\right)^2$$

vera per C-S su $\left(\frac{x_1}{\sqrt{y_1}}, \dots, \frac{x_n}{\sqrt{y_n}}\right)$

e su $\left(\sqrt{y_1}, \dots, \sqrt{y_n}\right)$

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

titu su $\sqrt{a}$ e cyc

e $b+c$

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

hope!

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

$$\Updownarrow$$

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

$$\Updownarrow$$

$$\sum_{cyc} \sqrt{2b} \geq \sum_{cyc} a$$ È la (1) al contrario!

$x = \sqrt{a}$ etc. $\Leftrightarrow$

$$\sum_{c} xy \geq \sum_{c} x^2$$ falso!

Il problema si fa così:

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

titu $\geq \dfrac{\left(\sum_c a\right)^2}{\sum_c ab+ac} \geq \dfrac{3}{2}$ hope!

$$\left(\sum_c a\right)^2 \geq 3\sum_c ab$$

$$\sum_c a^2 \geq \sum_c ab$$ è vera! ☺

③ $\sum_c \frac{a}{\sqrt{a^2+8bc}} \geq 1 \qquad (a,b,c>0$

$\sum_c \frac{a}{\sqrt{a^2+8bc}} = \sum_c \frac{a^2}{a\sqrt{a^2+8bc}}$

titu $\geq \frac{(\sum_c a)^2}{\sum_c a\sqrt{a^2+8bc}} \geq 1$ hope!

mi rimane

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

C-S $\leq \sqrt{\sum a^2}\cdot\sqrt{\sum a^2+8bc}$

$(a,b,c)\ (\sqrt{\ },\sqrt{\ },\sqrt{\ })$

C-S 2°

$(\sqrt{a},\sqrt{b},\sqrt{c})\ (\sqrt{a}\sqrt{\ },\sqrt{b}\sqrt{\ },\sqrt{c}\sqrt{\ })$

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

basta che $\left(\sum_c a\right)^{\frac{3}{2}} \geq \sqrt{\sum_c a^3+8abc}$

l'ultima speranza

elevando al quadrato

$$\left(\sum_c a\right)^3 \geq \sum_c a^3 + 24abc$$

$$\sum_c a^3 + 3\sum_s a^2b + 6abc \geq \sum_c a^3 + 24abc$$

AM-GM su a^2b, e sym

$$\frac{\sum_s a^2b}{6} \geq \sqrt[6]{a^6b^6c^6} = abc$$

Esercizi 85, 88, ④

- $\sum_{i=1}^n x_i = 1 \; ; \; x_i > 0 \Rightarrow \sum_{i=1}^n \frac{1}{x_i} \geq n^2$ [hint: AM-GM pesata saggiamente]
- $a,b,c>0 \; ; \; \sum_{cyc} \frac{a+b}{c} \geq 6$
- $\sum_c a^4b \geq \sum_c a^2b^2c$
- $x_i>0$, $x_2 \cdot \ldots \cdot x_n = 1 \Rightarrow (1+x_2)^2 \cdot \ldots \cdot (1+x_n)^n > n^n$ [IMO 2012 2]

[hint: usare fatto visto a lezione]

- $\forall r \geq 0, \forall x,y,z \quad \sum_c x^r(x-y)(x-z) \geq 0$ [Schur]
- $\sum_{sym} a^3 + \sum_{sym} abc \geq 2\sum_{sym} a^2b$ [Schur]

Altri!

[hint: usare l'esercizio prec.]

– $\sum_c (x+y)\sqrt{(y+z)(z+x)} \geq 4\sum_c xy$ [BMO2012-2]

[hint: usare la sostituzione $a=y+z$ e cyc
e l'esercizio prec.

Correzione

85: 3° $\left(\sum_c a\right)\left(\sum_c a^2-ab\right) =$

$\left(\sum_c a\right)\left(\sum_c a^2\right) - \left(\sum_c a\right)\left(\sum_c ab\right) =$

$a+b+c$

check:
grado
#termini
= sostituire 1

$\sum_c a^2(a+b+c) - \sum_c ab(a+b+c) =$

$\sum_c a^3 + \sum_s a^2b - \sum_s a^2b - 3abc =$

$\sum_c a^3 - 3abc = \frac{1}{2}\sum_s a^3 - \frac{1}{2}\sum_s abc$

volendo avete $a^3+b^3+c^3 \geq 3abc$
dimostrato che

6° $\left(\sum_c a^2b\right)\left(\sum_c a^2c\right) =$

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

$\sum_c a^4bc + \sum_c a^2b^2c^2 + \sum_c a^3c^3 =$

$$\frac{1}{2}\sum_{S}\left(a^4bc + a^2b^2c^2 + a^3c^3\right)$$

8 8 $\quad \min\left\{x+2y+3z : x^3y^2z=1\right\}$

$$x+2y+3z \geq C\left(x^3y^2z\right)^{\alpha}$$

← l'esponente lo trovo per omogeneità

$\rightarrow \alpha = \frac{1}{6}$

AM-GM $\quad \dfrac{\frac{x}{3}+\frac{x}{3}+\frac{x}{3}+y+y+3z}{6} \geq \sqrt[6]{\dfrac{x^3y^2z}{9}}$

$C = \dfrac{6}{\sqrt[6]{9}}$, $\quad \frac{x}{3} = y = 3z = r$ mi dà $r =$

r è t.c. $r^3 \cdot 27 \cdot r^2 \cdot \frac{r}{3} = 1$

$r = \sqrt[6]{9^{-1}} = 3^{-\frac{1}{3}}$

- se $\sum x_i = 1 \Rightarrow \sum \frac{1}{x_i} \geq n^2$

C-S $\quad \left(\sqrt{x_i}\right), \left(\frac{1}{\sqrt{x_i}}\right)$

$$\left(\sum x_i\right)\left(\sum \frac{1}{x_i}\right) \geq \left(\sum 1\right)^2 = n^2$$

AM-GM $\quad \dfrac{\sum x_i}{n} \geq G = \sqrt[n]{\prod x_i}$

$$\frac{\sum \frac{1}{x_i}}{n} \geq \frac{1}{G}$$

da cui, moltiplicando membro a membro ho l'=

per casa usare C-S per mostrare $AM \geq HM$

$\left(HM = \left(\frac{\sum \frac{1}{x_i}}{n} \right)^{-1} = \left(\frac{\sum x_i^{-1}}{n} \right)^{-1} \right)$

usare AM-GM per mostrare

$AM \geq GM \geq HM$

$$\sum_c \frac{a+b}{c} \geq 6$$

$$\frac{a}{c} + \frac{b}{c} + \frac{c}{b} + \frac{a}{b} + \frac{b}{a} + \frac{c}{a} \geq 6$$

AM-GM (volendo su 3 coppie)

volendo $\sum_s a^2 b \geq 6abc$ (se moltiplicate i denominatori)

per fare la (2) potevate sostituire

$a+b=z$ e cyc da cui

$$\sum_c \frac{a}{b+c} = \sum_c \frac{\frac{y+z-x}{2}}{x} = \frac{1}{2} \sum_c \frac{y+z}{x} - \frac{3}{2}$$

da cui $\sum_c \frac{a}{b+c} \geq \frac{3}{2} \rightarrow \sum_c \frac{y+z}{x} \geq 6$

$$\sum_{cyc} a^4 b \geq \sum_{cyc} a^2 b^2 c$$

$$a^4 b + b^4 c + c^4 a \geq a^2 b^2 c + \_ \_$$

$$\frac{A\,\frac{a^4 b}{A} + B\,\frac{b^4 c}{B} + C\,\frac{c^4 a}{C}}{A+B+C} \geq \sqrt[A+B+C]{\frac{a^{4A+C}\, b^{4B+A}\, c^{4C+B}}{A^A\, B^B\, C^C}}$$

AM-GM

per la a: $\frac{4A+C}{A+B+C} = 2$, $4A+C = 2A+2B+2C$

b: $4B+A = 2A+2B+2C$

c: $4C+A = 0A+B+C$

$\rightarrow$ si arriva a $A=6$, $B=5$, $C=2$

IMO 2012 - 2

$$(1+x)^n \geq \frac{n^n}{(n-1)^{n-1}} x \quad \leftarrow \text{visto a lezione}$$

$$(1+x_2)^2 \geq \frac{2^2}{1} x_2 \quad \leftarrow x = x_2,\ n = 2$$

(4) $\vdots$

$$(1+x_n)^n \geq \frac{n^n}{(n-1)^{n-1}} x_n \quad \leftarrow x = x_n,\ n = n$$

$$(1+x_2)^2 \cdot \ldots \cdot (1+x_n)^n \geq \frac{2^2}{1} \cdot \frac{3^3}{2^2} \cdot \ldots \cdot \frac{n^n}{(n-1)^{(n-1)}} \, x_2 \cdot \ldots \cdot x_n$$

$= 1$

il $>$ stretto si ottiene mostrando che le $\circledast$ non possono avere l'$=$ tutte insieme

A3 Basic Tess

Note Title 9/5/2016

Successioni (per ricorrenza)

Equazioni funzionali

Def: una funzione è una legge tra A e B tale che

(A, B: insiemi)

$\forall\, a \in A$ associo 1 solo elemento di B

Esempi: $f: A \to B$

$a \mapsto b$ con b fissato, $\forall\, a \in A$

$Id: A \to A$

$a \mapsto a$

Una trasformazione geometrica del piano è una funzione dal piano al piano ($A = B =$ piano)

Una terna, una n-upla è una funzione

↳ di reali è $f: \{1,2,3\} \to \mathbb{R}$

n-upla: $f: \{1, \dots, n\} \to \mathbb{R}$

$f : \mathbb{R} \to \mathbb{R}$ ci sono esempi che non si scrivono e non si disegnano.

Successioni

una **successione** è una funzione

$$a : \mathbb{N} \to B$$

$$a(0) ; a(1) ; \dots$$

$$\updownarrow \quad \updownarrow \quad \updownarrow$$

$$a_0 ; a_1 ; a_2 \dots$$

Una successione di reali è $a : \mathbb{N} \to \mathbb{R}$

Posso definire una successione "ricorsivamente"

Es $\begin{cases} a_0 = 1 \\ a_{n+1} = 2a_n + 1 \end{cases} \quad \forall n \in \mathbb{N}$

Es $\begin{cases} a_0 = 0 ; a_1 = 1 \\ a_{n+2} = a_{n+1} + a_n \end{cases} \quad \forall n \in \mathbb{N}$

Esempi $a_{n+k} = 5a_{n+k-1} + \dots + 8a_n$

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

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

Se $f: \mathbb{R} \to \mathbb{R}$, $a_{n+1} = f(a_n)$

Se $f: \mathbb{R}^k \to \mathbb{R}$, $a_{n+k} = f(a_{n+k-1}, \dots, a_n)$

$f: \mathbb{R}^k \times \mathbb{N} \to \mathbb{R}$ $a_{n+k} = f(a_{n+k-1}, \dots, a_n, n)$

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

↳ $a_{n+1} = a_n + n$

Se f non dipende da n

si dice che è lineare se

$$\begin{cases} f(x+y) = f(x)+f(y) \\ f(\lambda x) = \lambda f(x) \end{cases} \quad \forall \lambda \in \mathbb{R} \quad \forall x, y \in \mathbb{R}$$

↳ ho solo $f(x) = k \cdot x$

$$\begin{cases} f(x_1+y_1, \dots, x_n+y_n) = f(x_1, \dots, x_n) + f(y_1, \dots, y_n) \\ f(\lambda x_1, \dots, \lambda x_n) = \lambda f(x_1, \dots, x_n) \end{cases}$$

$\forall \lambda, x_1, \dots, x_n, y_1, \dots, y_n \in \mathbb{R}$

↳ ho solo $f(x_1, \dots, x_n) = k_1 x_1 + \dots + k_n x_n$

per $k_1, \dots, k_n$ fissate e costanti

$f(x) = kx$ (k costante, es $k=2$)

$= 2x$

$\begin{cases} a_0 = \dots \\ a_{n+1} = 2a_n \end{cases} \longrightarrow a_n = 2^n a_0 = 2^n \dots$

$f(x) = 2x+1$

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

Suppongo di avere $a_0, a_1, \dots$
$b_0, b_1, \dots$

successioni che soddisfano $x_{n+1} = 2x_n + 1$

sia $c_n = a_n - b_n \quad \forall n$

$$c_{n+1} = a_{n+1} - b_{n+1} = 2(a_n - b_n) + 1 - 1$$
$$= 2c_n$$

quindi: c_n soddisfa una ricorrenza lineare

$\Rightarrow c_n = 2^n c_0$

$\circledast \quad a_n = 2^n c_0 + b_n$

Oss: se so calcolare la a_n per un solo termine iniziale, allora lo so fare per tutti infatti:

se so b_0 ($\to$ ottengo b_n)

e voglio calcolarla per a_0

(*) $a_0 = c_0 + b_0$ $\to$ se sapete a_0, b_0
sapete c_0
$\to$ sapete $a_n = 2^n c_0 + b_n$

Cerco una soluzione costante, c

$c = 2c + 1 \quad \Rightarrow \quad c = -1$

$\Rightarrow$ tutte le successioni che soddisfano f

sono della forma $a_n = 2^n \cdot k - 1$

se so a_0, pongo $n=0$ $\quad a_0 = k - 1 \Rightarrow k = a_0 + 1$

Un altro modo:

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

$c_n := a_n + c$

che successione soddisfa la c_n?

$\to \quad c_{n+1} - c = 2c_n - 2c + 1$

$c_{n+1} = 2c_n - c + 1$

se scelgo $C=1$, $c_{n+1}=2c_n$

——— o ———

$f(x,n)=2x+n$

$a_{n+1}=2a_n+n$ ⊛

se (a_n) e (b_n) soddisfano ⊛

allora a_n-b_n soddisfa $f(x)=2x$

Una costante non torna:

$C=2C+n \quad \forall n$ impossibile

Scelgo $Cn+D$

$C(n+1)+D=2Cn+2D+n$

$(-1-C)n+(C-D)=0$

$\Rightarrow C=D, \quad C=-1$

scegliendo $-n-1$

la generica ricorsione sarà $a_n=\overbrace{2^n\cdot K}^{\text{differenza}}\underbrace{-n-1}_{\text{una sol. particolare}}$

Lo stesso trucco funziona con

$$f(x, n) = Cx + g(n)$$

$$\text{con } \frac{1}{1+\sqrt{n^2+1}}$$

se a_n e b_n soddisfano $f(x, n)$

allora $a_n - b_n$ soddisfa $x_{n+1} = Cx_n$

$$a_{n+1} = Ca_n + g(n)$$

$$b_{n+1} = Cb_n + g(n)$$

$$a_{n+1} - b_{n+1} = C(a_n - b_n)$$

In generale la soluzione sarà $a_n = C^n \cdot k + b_n$

con b_n che conosco

Proviamo con 2 termini:

$$x_{n+2} = 4x_{n+1} - 3x_n$$

Oss: se (a_n) e (b_n) soddisfano

anche $(a_n + b_n)$ soddisfa

anche (λa_n) soddisfa

Cerchiamo soluzioni del tipo $x_n = c^n$

come deve essere c?

$$c^{n+2} = 4c^{n+1} - 3c^n \quad , \quad c = 0 \text{ oppure}$$

$$c^2 = 4c - 3 \quad \Rightarrow \quad c = 1 \quad c = 3$$

Tutte le successioni $a_n = \lambda \cdot 1^n + \mu \cdot 3^n$

$(\forall\, \lambda, \mu \in \mathbb{R})$ soddisfano la ricorsione

λ e μ li trovo impostando l'uguaglianza per $n = 0, 1$

devono essere noti $\begin{cases} a_0 = \lambda + \mu \\ a_1 = \lambda + 3\mu \end{cases}$

Es: Fibonacci

$$x_{n+2} = x_{n+1} + x_n$$

le soluzione particolari soddisfano

$$c^2 = c + 1 \qquad c^2 - c - 1 = 0$$

[il polinomio $t^2 - t - 1$ è il "polinomio caratteristico della ricorrenza"]

$$c = \frac{1 \pm \sqrt{5}}{2}$$

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

dove λ e μ soddisfano

$$0 = F_0 = \lambda + \mu$$
$$1 = F_1 = \lambda \left(\frac{1+\sqrt{5}}{2}\right) + \mu \left(\frac{1-\sqrt{5}}{2}\right)$$

Es: $X_0 = 0$
$X_1 = 1$
$X_{n+2} = X_{n+1} - X_n$

Equazioni funzionali

trovare tutte le

1. $f(x+y) = f(x)+f(y) \quad \forall x,y \in \mathbb{Q}$ — $f: \mathbb{Q} \to \mathbb{Q}$
2. $f(x+f(y)) = f(x)+y \quad \forall x,y \in \mathbb{Q}$ — $f: \mathbb{Q} \to \mathbb{Q}$
3. $f(f(x)^2 y) = x^3 f(xy) \quad \forall x,y \in \mathbb{Q}^+$ — $f: \mathbb{Q}^+ \to \mathbb{Q}^+$
4. $f(xf(x)+f(y)) = f(x)^2 + y \quad \forall x,y \in \mathbb{R}$ — $f: \mathbb{R} \to \mathbb{R}$

(2) $x = 0$, $y = 0$

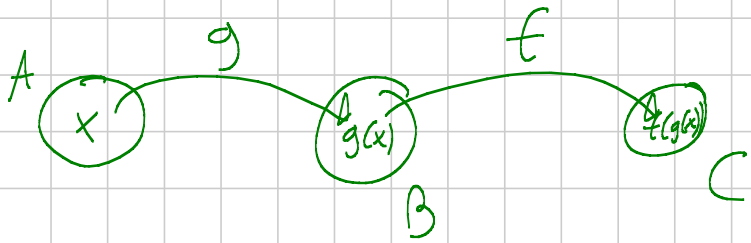
$f(f(0)) = f(0)$, quindi se $c = f(0)$, $f(c) = c$

$x = 0$

$f(f(y)) = c + y \quad \forall y \in \mathbb{Q}$

Oss. generale: se $f(g(x))$ è suriettiva

$\Rightarrow$ f è suriettiva



se $f(g(x))$ è iniettiva, g lo è

$\Rightarrow$ f è iniettiva e suriettiva

per la suriettività $\exists\ x_0 \mapsto 0$ t.c. $f(x_0) = 0$

$y = x_0 \Rightarrow$

$\forall x \quad f(x) = f(x) + x_0 \Rightarrow x_0 = 0$

$\forall x \quad f(f(x)) = x$ (perché $c = 0$)

sostituisco $y = f(z)$ in (2)

ottengo $f(x + f(f(z))) = f(x) + f(z)$

$\Rightarrow f(x+z) = f(x) + f(z)$

$\Rightarrow$ (1) allora voglio risolverla

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

$x = 0, y = 0 \quad \Rightarrow \quad f(0) = 2f(0) \Rightarrow f(0) = 0$

$x = 1, y = 1 \qquad f(2) = 2f(1)$

$x = 2, y = 1 \qquad f(3) = f(2) + f(1) = 3f(1)$

per induzione voglio vedere se $f(n) = nf(1) \;\forall n \in \mathbb{N}$

$x = n-1, y = 1 \quad \Rightarrow f(n) = f(n-1) + f(1)$ ← testo

$= (n-1)f(1) + f(1)$ ← ip. induttiva

$= nf(1)$

$y = -x \quad \Rightarrow \quad f(0) = 0 = f(x) + f(-x) \quad \forall\, x \in \mathbb{Q}$

$\Rightarrow \quad f(-x) = -f(x)$

$\frac{1}{n} + \dots + \frac{1}{n} = 1$

Mostro per induzione che

$$f(nx) = n f(x) \quad \forall\ n \in \mathbb{N}$$

P.B. $n = 1$ è ovvio

P.I. $y = (n-1)x \Rightarrow$

$$f(nx) = f((n-1)x) + f(x) \quad \leftarrow \text{testo}$$
$$= n f(x) \quad \leftarrow \text{ip. induttiva}$$

Ponendo $x = \frac{m}{n} \Rightarrow f(m) = n f\left(\frac{m}{n}\right)$

$$\Rightarrow f\left(\frac{m}{n}\right) = \frac{m f(1)}{n}$$

$$\Rightarrow f(x) = x f(1) \quad \forall\ x \in \mathbb{Q}$$

se f soddisfa è della forma $f(x) = \lambda x$ $\lambda \in \mathbb{Q}$

Sostituendo nel testo ottengo

$$\lambda(x+y) = \lambda x + \lambda y \quad \text{che è vera } \forall\ \lambda, x, y \in \mathbb{Q}$$

La (1) si chiama Equazione di Cauchy

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

f soddisfi la (1) è vero che $f(x) = \lambda x$

funziona $\forall\ \lambda \in \mathbb{R}$ ma non sono

le uniche!

④ $x=0$ $\quad f(f(y)) = f(0)^2 + y \quad \forall y \in \mathbb{R}$ ⊛

surj + inj

$\Rightarrow$ surj inj

sia x_0 : $f(x_0)=0$

pongo $x = x_0$ e ottengo $f(f(y)) = y \quad \forall y \in \mathbb{R}$ ✱

che insieme a ⊛ $f(0)=0 \Rightarrow x_0 = 0$ per inj

pongo $x = f(z)$ ← uso una nuova variabile

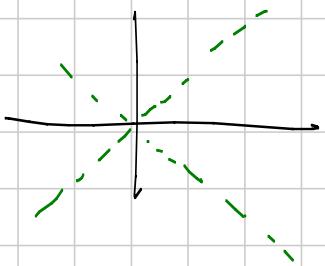
$f(f(z)f(f(z)) + f(y)) = f(f(z))^2 + y \quad \forall z, y$

✱ $\Rightarrow$ $f(f(z)z + f(y)) = z^2 + y \quad \forall z, y$

④ $\Rightarrow$ $f(z)^2 + y = z^2 + y \quad \forall y, z$

$\Rightarrow$ $f(z) = \pm z \quad \forall z \in \mathbb{R}$

Attenti al mistone!



sia $a \neq 0$ t.c. $f(a)=a$ e $b \neq 0$ t.c. $f(b)=-b$

sost. $x=b$, $y=a$

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

1 $-b^2+a$ 2 b^2-a

$1 \Rightarrow b^2=0$

$2 \Rightarrow a=0$

Manca solo la verifica!

(3) $f(f(x)^2 y) = x^3 f(xy)$ $*$ $\forall x,y \in \mathbb{Q}^+$

$y=1 \Rightarrow f(f(x)^2) = x^3 f(x)$ $*$

$$\frac{f(f(x)^2)}{f(x)} = x^3$$

x^3 ← inj

$g(f(x))$

Sia $g(y) = \frac{f(y^2)}{y}$

$g(f(x)) = x^3 \Rightarrow f$ iniettiva

$* + *$ Ottengo $f(f(yz)^2) = y^3 z^3 f(yz)$

ponendo $x = yz$

ma ora $y^3z^3f(yz) = y^3 f(f(z)^2 y) =$

testo con y, z

testo con $f(z)^2, y$

$= f(f(y)^2 f(z)^2)$

$\Rightarrow f(f(y)^2 f(z)^2) = f(f(yz)^2)$

/ per l'inj

$f(y)f(z) = f(yz)$

Esercizi

Ricorrenze: quello di prima; 92, 95 alcuni

Trovare formula esplicita per $a_{n+2} = 6a_{n+1} - 9a_n$ con $a_0 = 0, a_1 = 3$

IMO 2014 - 1

[hint: mostrare che una successione decresce]

Funzionali: 89, 90 alcuni, 91 il primo

Test iniziale 3: (c)

Trovare tutte le $f: \mathbb{R} \to \mathbb{R}$ t.c. [imo 92-2]

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

[hint: supponete dapprima $f(0) = 0$]

Ricorrenze

quello di prima $\quad p(t) = t^2 - t + 1$

$\to$ le radici: ξ, ξ^{-1} sono radici dell'unità, sesta $\xi^6 = 1$

$$a_n = \lambda \xi^n + \mu \xi^{-n}$$

$$\Rightarrow a_{n+6} = \lambda \xi^{n+6} + \mu \xi^{-n-6} = \lambda \xi^n + \mu \xi^{-n} = a_n$$

92 $\sum_{n=0}^{k} 4^n = a_k$

$a_{k+1} = a_k + 4^{k+1}$

$= 4a_k + 1$

$\underbrace{1+4+\dots+4^{k+1}}_{a_{k+1}} = 1+4\underbrace{(1+4+\dots+4^k)}_{a_k}$

$a_{n+2} = 6a_{n+1} - 9a_n \Rightarrow (t-3)^2 = 0$

$\Rightarrow$ soluzioni del tipo c^n c'è solo quella con

$c = 3$

nc^n ← la stessa c

le soluzioni particolari sono c^n, nc^n

$3^n, n3^n$

Oss. generale: se una radice r del polinomio caratteristico ha molteplicità h, allora $p(n)r^n$ è soluzione $\forall$ $p(x)$ polinomio di grado $< h$

Accenno alla dim: nel caso in cui $r=1$

il polinomio caratt. è $q(t)(t-1)^h$

è vero che $p(n)$ soddisfa $(t-1)^h$

se $h=1$ $\quad p(n+1)=p(n)$

$p(n+1)-p(n)$

se $h=2$ $\quad [p(n+2)-p(n+1)]-[p(n+1)-p(n)]=0$

ecc. per $h>2$

se $p(x)$ è un polinomio di grado h

$\Rightarrow$ $p(x+1)-p(x)$ " $h-1$

(basta guardare il termine di grado h)

Rivediamo il 92

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

→ polinomio di grado 2 in n

→ $\frac{n(n-1)}{2}$

$$a_{k+1}=a_k+\binom{k+1}{2}$$

sia $b_k=a_k-a_{k-1}$ (*)

$$b_k+a_k=a_k+\binom{k}{2}$$

$b_k=\binom{k}{2}$ è polinomio di grado 2

$c_k=b_k-b_{k-1}$ = polinomio di grado 1

$d_k = c_k - c_{k-1}$ → polinomio costante

→ a_k è un polinomio di grado 3

Ora avete $a_k = \alpha k^3 + \beta k^2 + \gamma k + \delta$

(*) $a_k - a_{k-1} = \frac{1}{2}k^2 - \frac{1}{2}k$

95 l'ultimo $a_n = \frac{1}{2}a_{n-1} + \frac{1}{n}$

→ $b_n =$ da trovare per casa ...

IMO 2014-1 $a_0 < a_1 < \dots$ interi

dim che $\exists!\, n$ t.c. $a_n \leq \frac{a_0 + \dots + a_n}{n} \leq a_{n+1}$

In pochi passaggi ottengo che

$\square \iff \left(\sum_{i=0}^{n} a_i\right) - n a_n > 0$

$\square \iff \left(\sum_{i=0}^{n} a_i\right) - n a_{n+1} \leq 0$

$b_n = \left(\sum_{i=0}^{n} a_i\right) - n a_n$

$= \sum_{i=0}^{n-1} a_i - (n-1) a_n$

$\square \iff b_n > 0$

$\square \iff b_{n+1} \leq 0$

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

$$= n(a_n - a_{n+1}) < 0$$

$b_{n+1} < b_n$ sono interi $\Rightarrow b_{n+1} \leq b_n - 1$

Funzionali

89 $\sim$ (2)

Con lo stesso procedimento della (1) + (2)

ottengo $f(x) = \lambda x \quad \forall x \in \mathbb{Q}$

guardando $f(f(x)) = x \Rightarrow \lambda = \pm 1$

$f(100)$ può essere solo ± 100

90 $f(x+y) + f(x-y) = 2f(x) + 2f(y)$

né iniettiva, né surgettiva perché ~~dovrebbe~~ esiste

~~esistere~~ esiste $f(x) = C = 0$

$f(xy) = xf(y)$

quasi ... se non fosse per $f(x)=0$

se $\exists\, y_0 \neq 0$ t.c. $f(y_0) \neq 0$ allora sostituisco

e ottengo $f(xy_0) = x f(y_0)$

$f(z) = \frac{z}{y_0} f(y_0)$

$f(x^2) = x^2$ ← non so nulla! per $x<0$ della $f(x)$

Se avessi avuto $f: \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ allora sì sarà a inj che a surj

Test. iniziale: 3

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

$y=0 \Rightarrow f(x) = f(f(x)) + c$ $\forall x \in \mathbb{Q}$ $(c = f(f(0)))$

$\Rightarrow$ sostituisco nel testo e ottengo

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

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

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

chiamo $g(x) = f(x)+k$

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

$\Rightarrow g(x) = \lambda x \Rightarrow f(x) = \lambda x + \mu$

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

$x = z+k$

$f(z+y+k) = f(z+k) + f(y+k)$

$g(x) := f(x+k)$

IMO 92 - 2

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

ponendo $x=0 \rightarrow f(f(y)) = f(0)^2 + y$

$\rightarrow$ inj + surj

se avessi $f(0) = 0$, avrei $f(f(y)) = y$

pongo $y = f(z)$

$f(x^2 + z) = f(x)^2 + f(z) \quad \forall x, z$

$z=0 \Rightarrow f(x^2)=f(x)^2 \quad \forall z$

$f(x^2+z)=f(x^2)+f(z) \quad \forall x,z$

$f(w+z)=f(w)+f(z) \quad \forall w>0, z$

mancano 2 cose: 1 la conquista di $\mathbb{R}$

2 $f(0)=0$

1 MEDIUM

2 ponendo $y=0$ nel testo

$f(x^2+c)=f(x)^2 \quad (c=f(0))$

ponendo $y=f(z)$

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

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

volevo dire che per la surgettività

$\exists\, z_0$ t.c. $f(z_0)=0$

$f(x^2+c)=f(x^2+z_0+c^2)$

iniett.

$\Rightarrow \quad c=z_0+c^2$

In realtà bastava $x=z_0$ nel testo

$f(z_0^2+c^2+z)=0+f(z)$

$\Rightarrow \quad z_0^2 + c^2 + z = z$

$\Rightarrow z_0^2 + c^2 = 0 \Rightarrow z_0 = 0 \text{ e } c = 0$

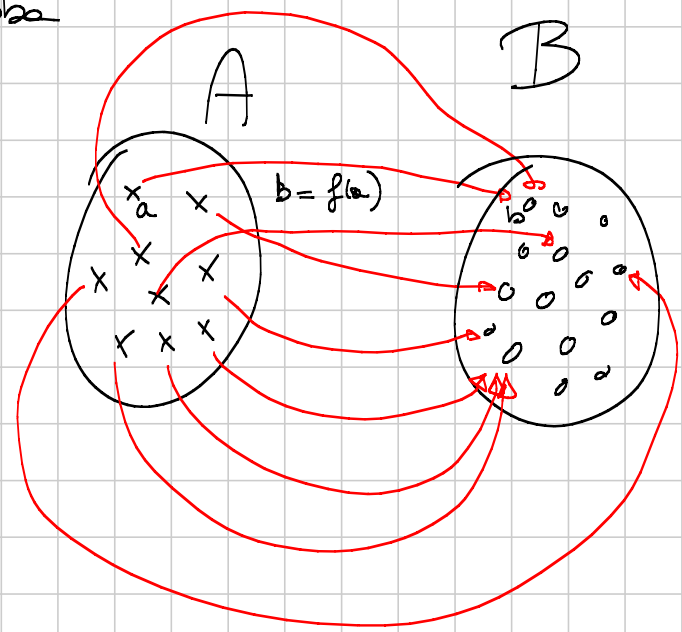
C1B - Sam

Note Title 9/2/2016

Conteggi = contare roba

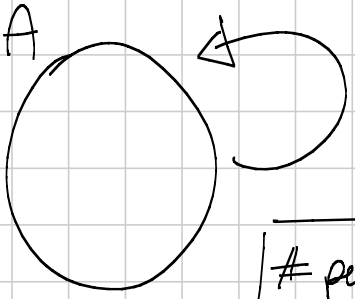
·) $f: A \to B$

f SURGETTIVA (SURIETTIVA)
$B = f(A)$



f INIETTIVA
se $a \neq a'$
allora $f(a) \neq f(a')$

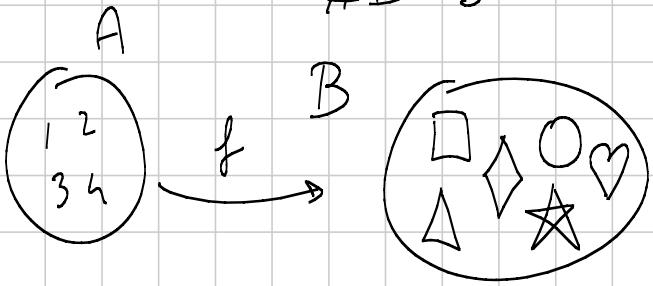
f BIGETTIVA se è INIETTIVA e SURGETTIVA



f bigettiva
è una permutazione

 # permutazioni = n!

- $f: A \to B$ $\#A$ = cardinalità di A = n° di el di A $= a$
$\#B = b$



1 → ? 6
2 → ? 6
3 → ? 6
4 → ? 6

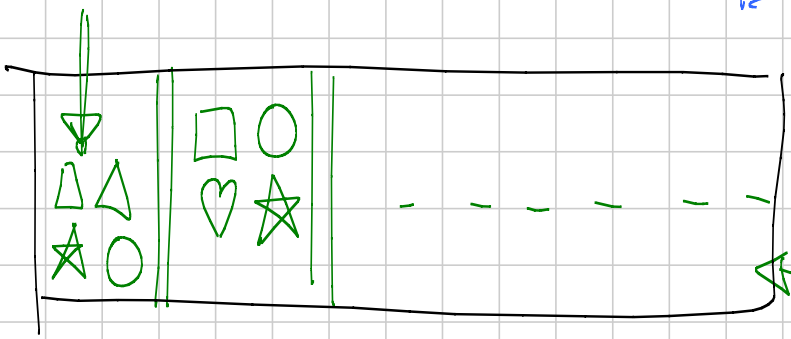
6^4 funzioni $\longrightarrow$ $\boxed{b^a}$ n° funzioni

– funzioni iniettive da A a B $\quad \#A = a \quad (a \le b)$

$\#B = b$

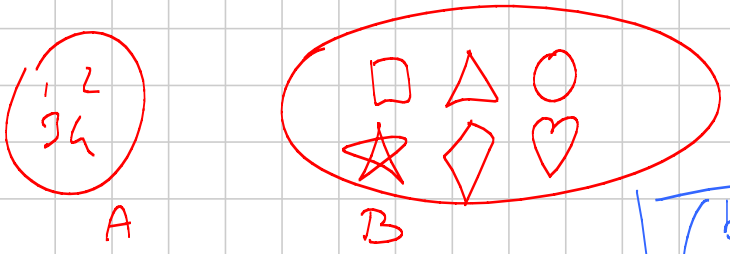
1° 2° 3° - - a°

$b(b-1)(b-2) \cdot \cdots \cdot (b-a+1) = \boxed{\dfrac{b!}{(b-a)!}}$ n° f. iniettive



f. iniett.

ho diviso le f. iniettive in $\binom{b}{a}$ sottoinsiemi



$\boxed{\binom{b}{a} a!}$ n° di f. iniettive

– $f: A \to B$ suriettive $\quad \left(\begin{matrix}\#B \le \#A \\ b \le a\end{matrix}\right)$

$\{x_1, \dots, x_b\} = B$

$\#\{f: A \to B \text{ che non hanno } x_1 \text{ nell'immagine}\} = (b-1)^a$

$\#\{- \cdots - \quad - \cdots x_3 \cdots - \cdots -\} = (b-1)^a$

$X_j = \{ f: A \to B \text{ che non hanno } x_j \text{ nell'immagine} \}$

$X_1 \cup X_2 \cup \dots \cup X_b = \{ f: A \to B \text{ non suriettive} \}$

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

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

$$\#(X_1 \cup \dots \cup X_b) = \sum_{j=1}^{b} \#X_j - \sum_{i<j} \#(X_i \cap X_j) + \sum_{i<j<k} \#(X_i \cap X_j \cap X_k) - \dots - (-1)^b \#(X_1 \cap \dots \cap X_b)$$

PIE
Principio Inclusione Esclusione

$$\#(X_1 \cap X_5) = (b-2)^a$$

$$b(b-1)^a - \binom{b}{2}(b-2)^a + \binom{b}{3}(b-3)^a - \dots - (-1)^{b-1}\binom{b}{b-1}(1)^a$$

$$\binom{b}{0}b^a - \binom{b}{1}(b-1)^a + \binom{b}{2}(b-2)^a - \binom{b}{3}(b-3)^a + \dots + (-1)^{b-1}\binom{b}{b-1}(1)^a$$

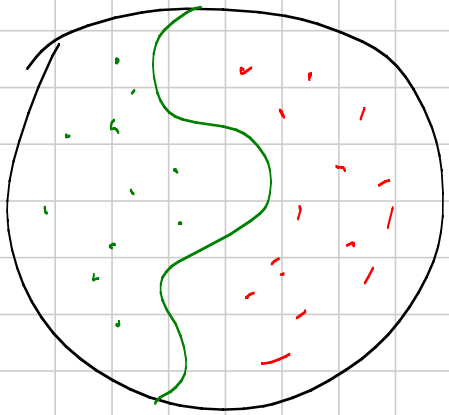
n° f. suriettive

TI 2016 - 6 $X = \{1, 2, \ldots, 200\}$

$S \subseteq X \qquad f(S) = (\Sigma \text{ el. di } S) \cdot (\Sigma \text{ el di } X - S)$

Si può dim che il valor medio di $f(S)$ quando S varia tra i sottoins. con 100 elementi è un numero intero n.

Quanto è n? $\sum_{\substack{S \subseteq X \\ \#S = 100}} f(S) \Big/ \binom{200}{100}$



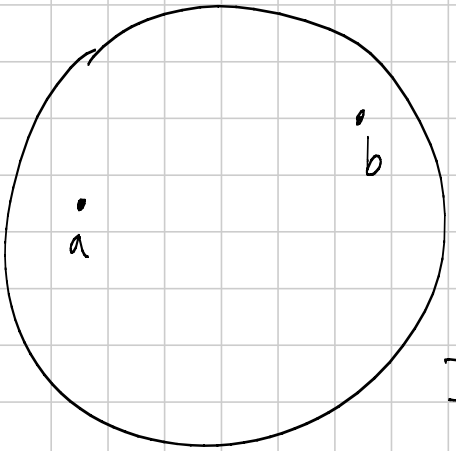
$\{a_1 a_2 a_3\} = S$

$\{b_1 b_2 b_3\} = X - S$

$f(S) = (a_1 + a_2 + a_3) \cdot (b_1 + b_2 + b_3) =$

$= a_1 b_1 + a_1 b_2 + a_1 b_3 + a_2 b_1 + a_2 b_2 + a_2 b_3$

$+ a_3 b_1 + a_3 b_2 + a_3 b_3$



Per quante scelte di $S \subseteq X$, $\#S = 100$ si ha che $a \in S$, $b \notin S$?

$\binom{198}{99}$

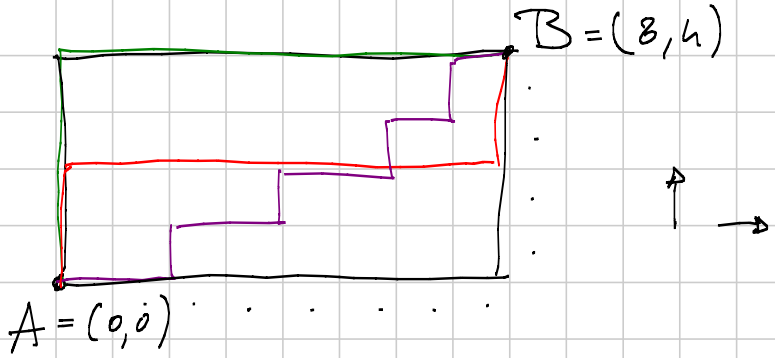
Il prodotto $a \cdot b$ compare $2 \cdot \binom{198}{99}$ volte.

$$\frac{\sum_{\substack{S\subseteq X\\ \#S=100}} f(S)}{\binom{200}{100}} = 2\cdot\frac{\binom{198}{99}}{\binom{200}{100}}\cdot\boxed{\sum_{1=i<j}^{200} i\cdot j}_{P} =$$

$$= 2\cdot\frac{198!\,100!\,100!}{99!\,99!\,200!\cdot 199}P =$$

$$= \frac{100}{199}\cdot P \qquad P = \frac{(1+2+\dots+200)^2 - 1^2 - 2^2 - \dots - 200^2}{2}$$

Es:

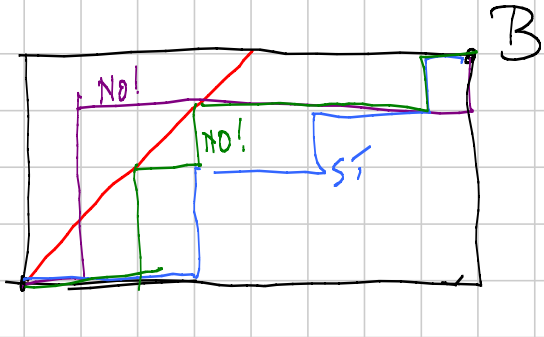


1) Anagrammi di ↑↑↑↑→→→→→→→→→→→→

2) Ho 12 mosse, scelgo le 8 che sono a dx

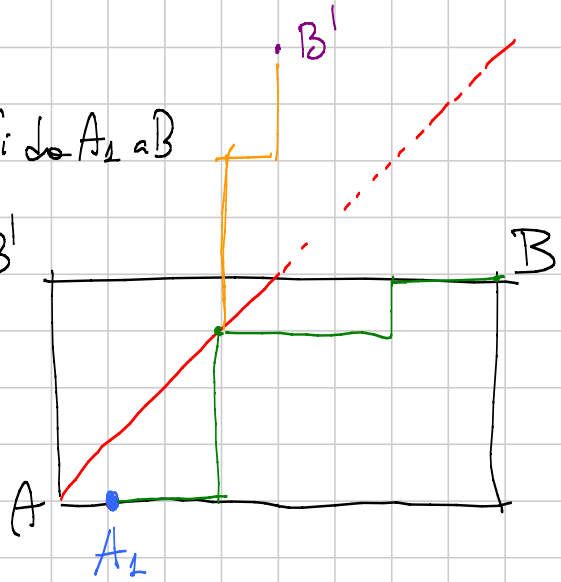
$$\binom{12}{8} = \frac{12!}{8!\,4!} = \binom{12}{4}$$

Es+:



percorsi da A a B monotoni che non toccano le rette rosse

Tutti i percorsi − # percorsi sbagliati



percorsi sbagliati da A_1 a B

$=$ # percorsi da A_1 a B'

$= \binom{11}{3}$

percorsi da A a B che non tocca la retta rossa di nuovo $=$

percorsi da A_1 a B che non tocca mai la retta rossa $=$

$=$ # percorsi da A_1 a B $-$ # percorsi sbagliati da A_1 a B $=$

$= \binom{11}{4} - \binom{11}{3} = \dots$

Es: Quante sono le stringhe di A e B lunghe n che non contengono due A consecutive?

n	1	2	3	4
	A	AB	ABA, ABB	ABAB, ABBA, ABBB
	B	BA	BAB	BABA, BABB
		BB	BBA, BBB	BBAB, BBBA, BBBB

A_n = n° di stringhe lunghe n senza due A consecutive che finiscono per A

B_n = $\dots$ che finiscono per B

$A_{n+1} = B_n$

$B_{n+1} = A_n + B_n$

$S_n = A_n + B_n$

$S_{n+1} = A_{n+1} + B_{n+1} =$

$= B_n + A_n + B_n =$

$= S_n + B_n = S_n + A_{n-1} + B_{n-1} =$

$= S_n + S_{n-1}$

TI 2016 – 5 I_n, Π_n, O_n

$I_n = \Pi_{n-1}$

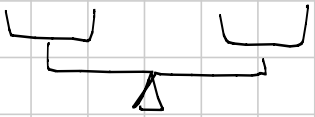
$O_n = \Pi_{n-1}$

$S_n = I_n + \Pi_n + O_n =$

$= 2\Pi_{n-1} + S_{n-1} = S_{n-1} + 2S_{n-2}$

$\Pi_n = I_{n-1} + O_{n-1} + \Pi_{n-1} = S_{n-1}$

IMO 2011 – 4:



n pesi

$2^0, 2^1, \dots, 2^{n-1}$

Volete posizionarli sui due piatti di modo che a SX ci sia sempre più peso che a dx.

In quanti modi si può fare?

$\uparrow D_n$

Se non è la prima mossa, il peso 2^0 non conta niente.

Avete $(n-1)$ pesi $\Rightarrow D_{n-1}$

$\left(1 + 2(n-1)\right) D_{n-1} = D_n$

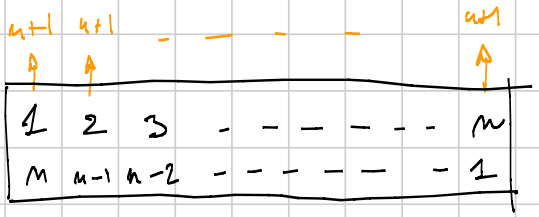
$D_n = (2n+1)\, D_{n-1}$

$D_1 = 1$ $\qquad$ D_n = prodotto dei dispari da 1 a $2n+1$.

$= (2n+1)!!$

Double counting

$\sum_{i=1}^{n} i$



Σ per righe $= 2 \cdot \sum_{i=1}^{n} i$

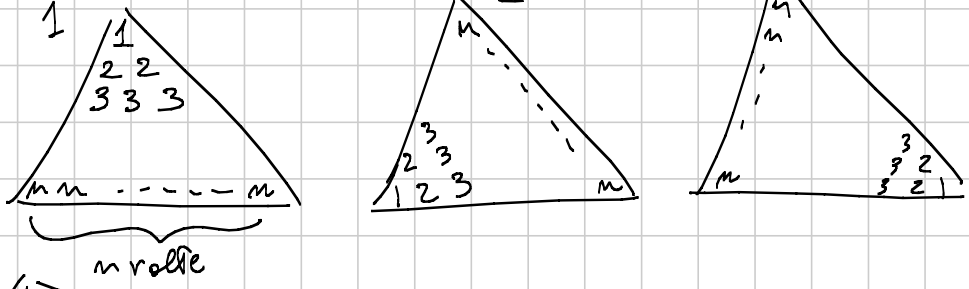
Σ per colonne $= (n+1) \cdot n$ $\leftarrow$ #colonne

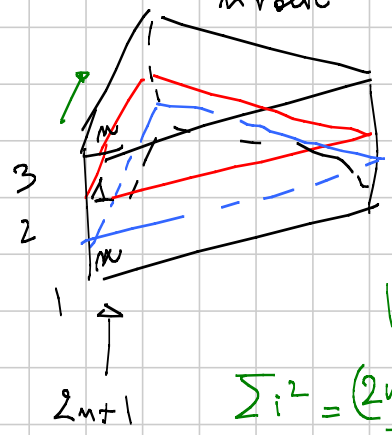
$\uparrow$

Σ di ogni colonna

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

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





Σ per piani $= 3 \cdot \Sigma i^2$

Σ colonne $= (2n+1) \cdot \frac{n(n+1)}{2}$

$\uparrow$

Σ di ogni colonna

$\Downarrow$

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

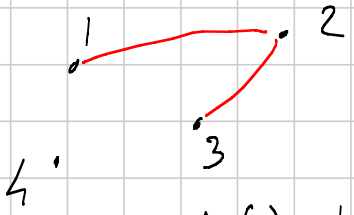
Grafi: (V, E) (Edges)

V: vertici

E: lati, archi, spigoli

$E \subseteq V \times V$ simmetrico: $(a,b) \in E \Rightarrow (b,a) \in E$

$V = \{1, 2, 3, 4\}$ $E = \{(1,2), (2,1), (3,2), (2,3)\}$



$v \in V$

$\deg(v) = \#$ archi che lo hanno come estremo

$\deg(1) = 1$
$\deg(2) = 2$
$\deg(3) = 1$
$\deg(4) = 0$

$$2 \#\text{archi} = \sum_{v \in V} \deg(v) \Rightarrow \#\text{vertici con } \deg(v) \equiv 1 \ (2) \text{ è pari.}$$

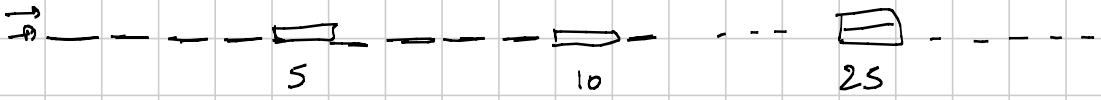
Esercizi: 97, 98, 99, 100, 108, 112, 114

Problemi: C1-10, C1-3, ITA 2015-1

Correzione di es. scelti

100) # zeri finali in 2013!

$1 \cdot 2 \cdot 3 \cdot 4 \cdot \boxed{5} \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot \boxed{10} \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot \boxed{15} \cdot 16 \cdot 17 \cdot 18 \cdot 19$
$\cdot \boxed{20} \cdot 21 \cdot 22 \cdot 23 \cdot 24 \cdot \boxed{25} \cdot 26 \cdot 27 \cdot 28 \cdot 29 \cdot \boxed{30} \cdot 31 \cdot \ldots$



$$\left\lfloor \frac{2013}{5} \right\rfloor + \left\lfloor \frac{2013}{25} \right\rfloor + \left\lfloor \frac{2013}{125} \right\rfloor + \left\lfloor \frac{2013}{625} \right\rfloor = \dots$$

108 $n = a_1 + \dots + a_k$ $\quad a_i \geq 0$ $\quad n=4 \quad k=3 \quad a,b,c \geq 0$

$4 = a+b+c$

$0+0+4$

$4+0+0$

$4 = n$

$2 = k-1$

$0+2+2$

$$\binom{4+2}{2} \rightsquigarrow \binom{n+k-1}{k-1}$$

112: A_n = gli anagrammi che sporcano ogni lettera al più di 1

$A_{n+1} \rightsquigarrow A_n$

B_n = gli anagrammi … con la prima lettera fissa

$A_n = B_n + C_n$

C_n = … con la 1ª lettera al secondo posto

$B_n = A_{n-1}$

$C_n = A_{n-2}$ $\qquad A_n = A_{n-1} + A_{n-2}$

114: $(A,B) \in Y^2$ $\quad A \cap B = \emptyset$.

$\#A = a$ $\quad \#B = b$ $\quad a+b \leq n$

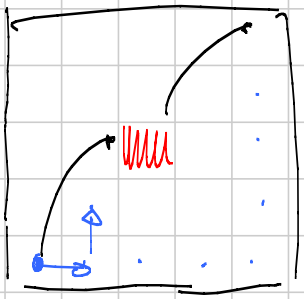
$$\sum_{a,b} \binom{n}{a}\binom{n-a}{b} \qquad f : \{1,\dots,n\} \longrightarrow \{A, B, \emptyset\}$$

3^n

C1-3

percorsi − # percorsi che passano dal centro

$$\binom{8}{4} - \binom{4}{2}\binom{4}{2}$$



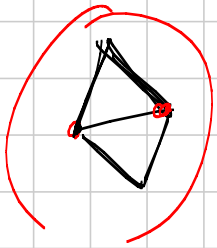
ITO 2015-1

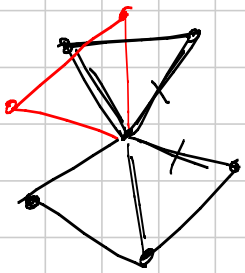
(a) equilibrato

$n=3$ tri equilatero

n dispari $\Rightarrow$ poligono regolare

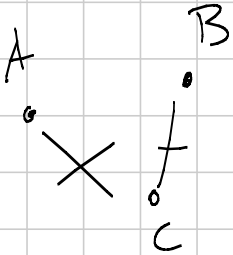
$n=4$





6

(b)



C buono per AeB

$\binom{n}{2}$ coppie. $\frac{n(n-1)}{2}$

al max C è buono per $\frac{n-2}{2}$ coppie se non è ecc

$\Downarrow$

non è equilibrato.

$\Downarrow$

n. $\frac{n-2}{2} < \frac{n(n-1)}{2}$

C1 - 10

$V, E \qquad \#V = 12k$

$v \in V \quad \deg(v) = 3k+6$

$\forall\, v, w \in V \quad \exists!$ esatt. N vertici collegati a entrambi

A = n° di cose così nel grafo

$$\binom{12k}{2} \cdot N = 12k \cdot \binom{3k+6}{2}$$

$$N = \frac{12k\binom{3k+6}{2}}{\binom{12k}{2}} = \boxed{\quad k \quad} + \frac{P(k)}{Q(k)}$$

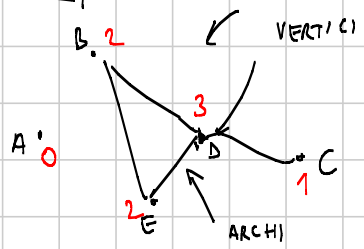
$k = 3$

Ora c'è da fare l'esempio.

SENIOR 2016 – C2 BASIC

Note Title 9/6/2016

GRAFI

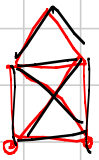


Σ gradi = 2 #archi

Grafi Euleriani

Cammino / ciclo euleriano.

si passa esattamente una volta su ogni arco



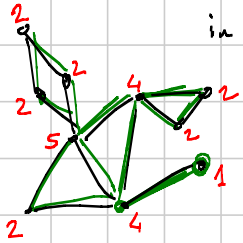
Sì, ma non con un ciclo

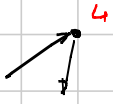
Teorema Un grafo ammette un ciclo euleriano $\iff$ è connesso e tutti i vertici hanno grado pari.

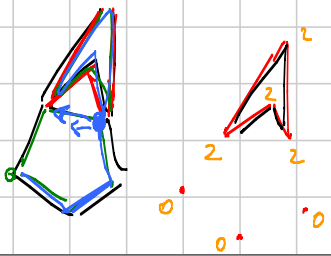
cammino euleriano $\iff$ connesso e al più 2 vertici hanno grado dispari.

($\Leftarrow$ per esercizio)

$\Rightarrow$ in ogni vertice, quando si entra bisogna anche uscire $\Rightarrow$ serve che il grado sia pari, tranne se voglio iniziare/finire il cammino in due vertici diversi.

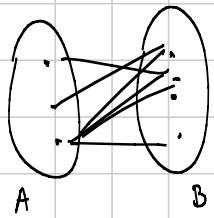






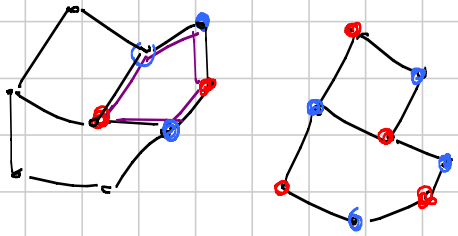
Oss: non ci può essere un unico vertice di grado dispari, quindi la condizione "al più due vertici di grado dispari" ci consente di scegliere tra ciclo (0 vertici di grado dispari) e cammino (2 v....)

GRAFI BIPARTITI



"2-colorazione" di un grafo

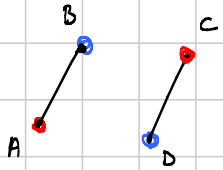
K-colorazione: assegnazione di un colore per ogni vertice, usando $\leq K$ colori distinti e in modo che ogni arco congiunga vertici di colori diversi.



Quante sono le 2-colorazioni di un grafo?

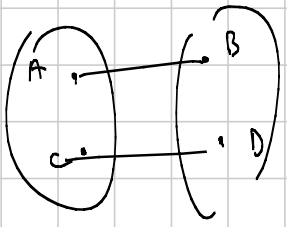
. supponiamo che ce ne sia almeno una.

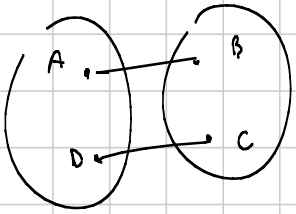
2



componenti connesse

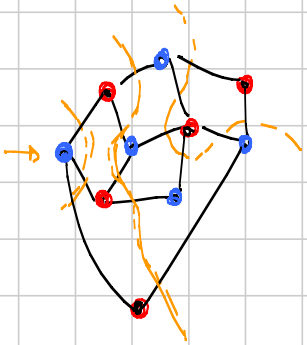
2

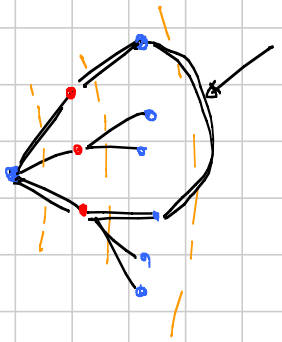




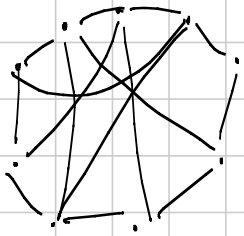
Quando un grafo è 2-colorabile?

Condizione necessaria: non ci devono essere cicli dispari.
È anche sufficiente!

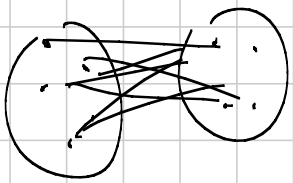




Es Quanti archi ha al massimo un grafo di 9 vertici senza triangoli?



$$9 + \frac{2 \cdot 9}{2} = 18$$

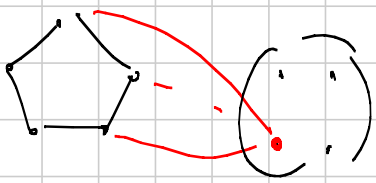


$5 \cdot 4 = 20$

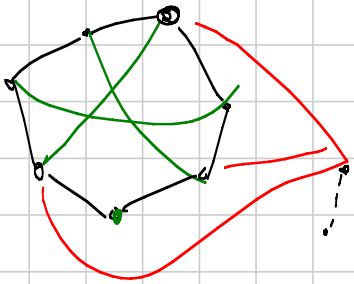
È bipartito $\Rightarrow$ non contiene cicli dispari

$\Rightarrow$ no triangoli.

grafi con cicli dispari di lunghezza ≥ 5



$\leq 5 + 2 \cdot 4 + 4 = 17$

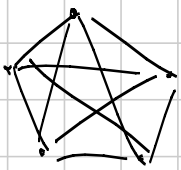


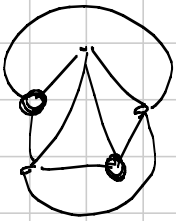
$\leq 7 + \underbrace{\frac{1 \cdot 7}{2}}_{\leq 3} + 3 \cdot 2 + 1 = 17$

GRAFI PLANARI

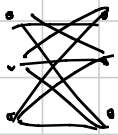
Grafi che potete disegnare su un foglio senza far intersecare gli archi.

K_5



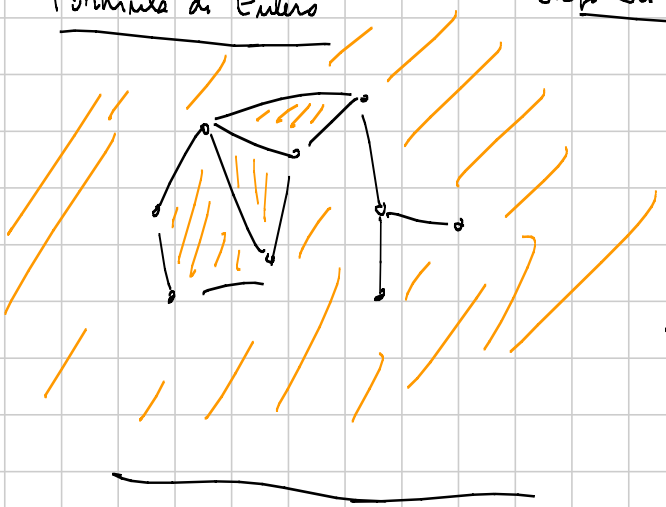


$K_{3,3}$



Formula di Eulero

Grafo convesso



4 facce
9 vertici
11 archi

$$F - A + V = 2$$

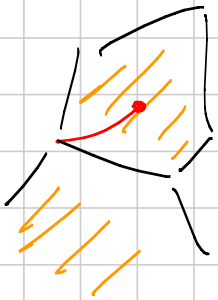
$4 - 11 + 9 = 2$

"Passo base"

$F = 1$
$A = 0$
$V = 1$

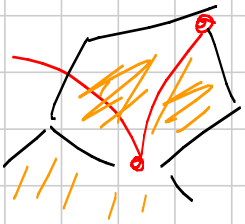
"Passo induttivo"

$-$ $+1$ vertice con un suo arco



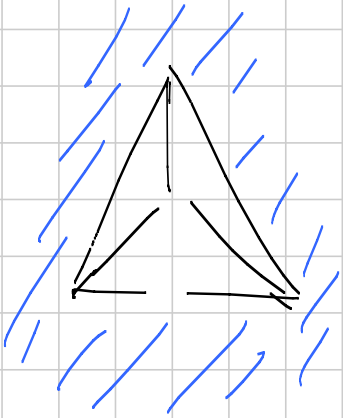
$\Delta V = 1$
$\Delta A = 1$
$\Delta F = 0$

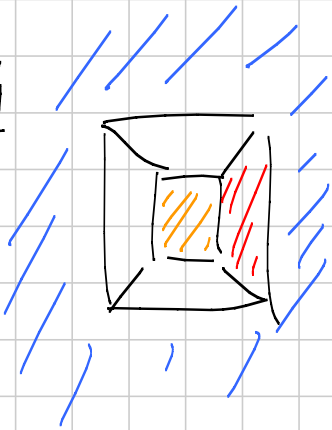
- + 1 arco tra vertici che esistono già



$\Delta F = 1$
$\Delta A = 1$
$\Delta V = 0$

Es: ci sono solo 5 solidi platonici (tetraedro, cubo, ottaedro, icosaedro, dodecaedro)





$F - A + V = 2$

Solido platonico: solido formato da facce → poligoni regolari di n lati in cui in ogni vertice arrivano d facce/spigoli.

→ F

A → $\frac{F \cdot n}{2}$

V → $\frac{F \cdot n}{d}$

$F - A + V = 2$

$F - \frac{F \cdot n}{2} + \frac{F \cdot n}{d} = 2$

$F\left(-\frac{n}{2} + \frac{n}{d} + 1\right) = 2$

$d = 3 \qquad F\left(\underbrace{-\frac{n}{6} + 1}\right) = 2$

$n \leq 5$

$n = 3,\ n = 4,\ n = 5$

↓ tetraedro ↓ cubo ↓ dodecaedro

$d = 4 \qquad F\left(-\frac{n}{4} + 1\right) = 2$

$n \leq 3$

$n = 3 \rightarrow$ ottaedro

$d = 5 \qquad F\left(\frac{n}{5} - \frac{n}{2} + 1\right) = F\left(-\frac{3}{10}n + 1\right)$

$n \leq 3$

$n = 3 \rightarrow$ icosaedro

$d = 6 \qquad F\left(\frac{n}{6} - \frac{n}{2} + 1\right)$

$= F\left(-\frac{n}{3} + 1\right)$

$n \leq 2$

$d \geq 6$

INVARIANTI

Es 

Posso finire con un 4 ?

Invariante: somma dei numeri modulo 2 all'inizio è dispari, e 4 è pari.

Invariante: qualcosa che non varia effettuando le mosse consentite dal problema.

Es 17 blu, 17 rossi, 17 gialli

B → G
R → G

R → B
G → B

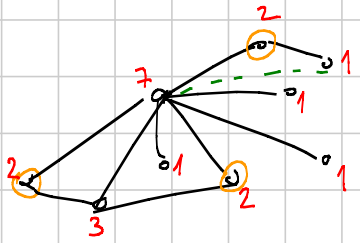
B → R
G → R

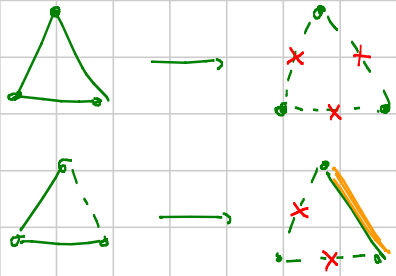
Si può arrivare ad avere 21 blu, 8 rossi, 22 gialli ?

Un invariante è la somma dei numeri di camaleonti !

B	R	G	
17	17	17	
12	12	27	sono tutti congrui mod 3 !
20	8	23	
18	12	21	
24	9	18	
23	8	20	

Es (C2-8)

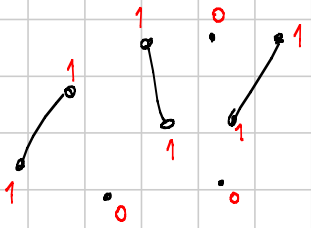




Perde chi non può muovere.
Dimostrare che l'esito della partita non dipende dalle scelte dei giocatori.

0) Il numero di archi diminuisce strettamente ad ogni mossa
⇒ il gioco finisce.

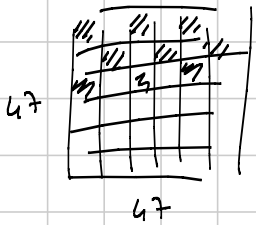
1) Quali sono le configurazioni "finali"?



2) La parità dei gradi è un invariante!

3) $\sum$ gradi mod 4 (varia di 2) è un invariante che varia
archi mod 2 (varia di 1) è un invariante che varia

Es

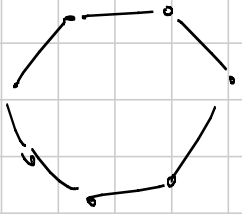


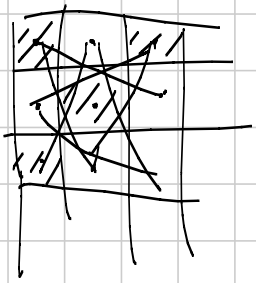
È possibile, con un cavallo percorrere la scacchiera con un ciclo che passi esattamente una volta per ogni casella?

- Ogni mossa ci fa cambiare colore della casella
- $\frac{47^2+1}{2}$ nere, $\frac{47^2-1}{2}$ bianche

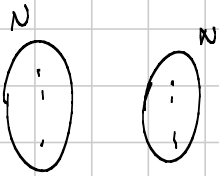
nere = # bianche + 1

47^2 è dispari!





Il grafo è bipartito
(caselle nere / caselle bianche)

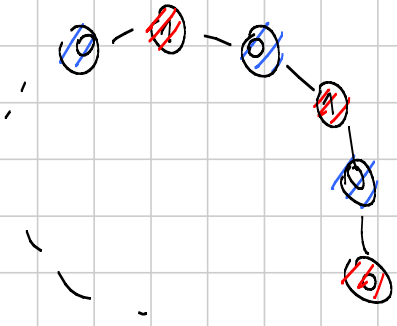


Staremmo cercando un ciclo dispari, che però non può esistere.

Esercizi "base": 116, 117, 119, 120, 123.
Esercizi C2: 2, 3, 5, 13.

(117) 2014 – agono

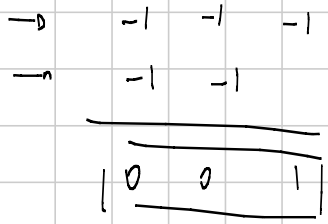
$\sum$ dispari $-$ $\sum$ pari si conserva

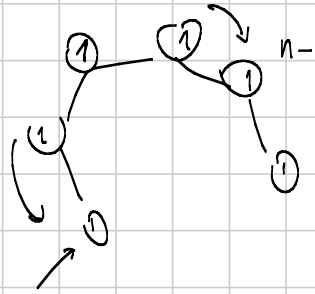


(119) 7 B 9 G 15 R

~~$3B + 4G - R \mod 8$~~

$aB + bG + cR \mod m$



(120)  n-agono

n dispari sì

n pari

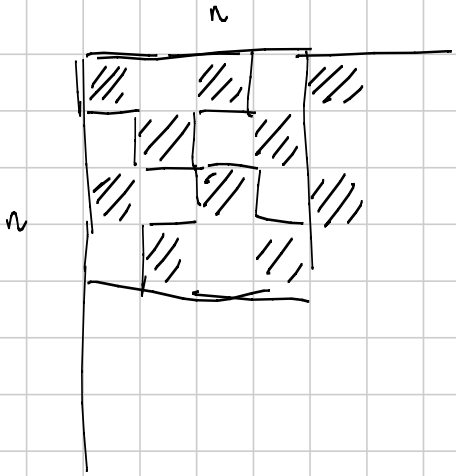
mod n: somma delle distanze "orientate" dall'origine

$\sum_{i=0}^{n-1} i \cdot (\#\text{pedine sul vertice } i) \mod n$

inizio: $\frac{(n-1)n}{2} \leftarrow \equiv \frac{n}{2} \ (n)$

per n pari

fine: 0

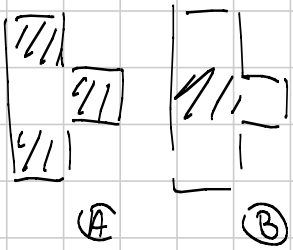
② 

$n \equiv 0 \ (4)$

n dispari $\Rightarrow 4 \nmid n^2$

non è possibile

$n \equiv 2 \ (4)$



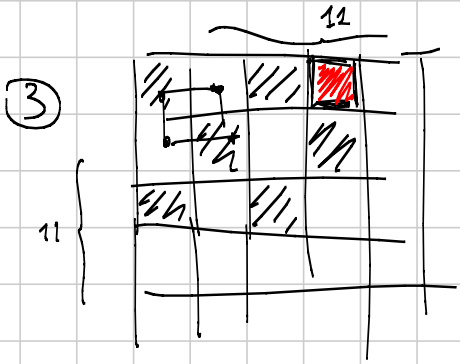
$n^2/2$ nere, $n^2/2$ bianche

$4 \nmid n^2/2$

tasselli $\equiv 1 \ (2)$

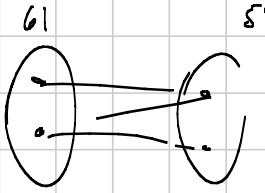
$\Rightarrow$ # tasselli A $\neq$ # tasselli B

$\Rightarrow$ c'è uno scompenso tra caselle nere e bianche, assurdo.

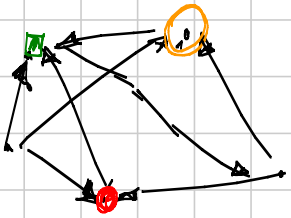
③ 

61 nere

60 bianche $\longrightarrow$ 59 bianche



⑤



"GRAFO ORIENTATO"

Per assurdo, supponiamo che ∄ una città da cui si raggiungono tutte le altre.

Consideriamo la città che massimizza il numero di città raggiungibili da lei.

Esiste una città non raggiungibile da

Deve esistere un percorso

Assumo, perché la è strettamente migliore della .

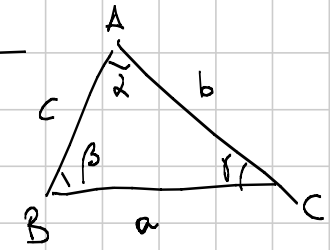
G1 Basic

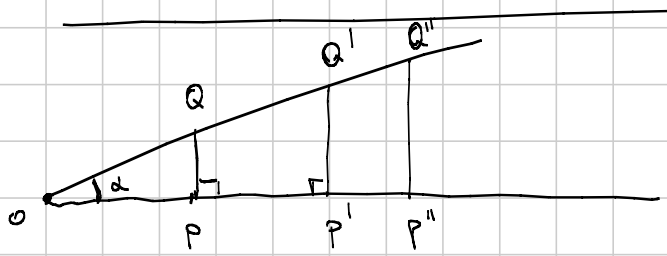
Danilo

Note Title 9/2/2016

G1 - Trigonometria
G2 - Metodi analitica
G3 - Sintetica

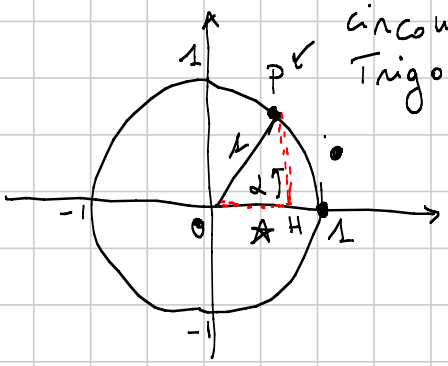
Notazione





$$\frac{OP}{OQ} = \frac{OP'}{OQ'} = \bigstar$$

$$\frac{QP}{OQ} = \frac{Q'P'}{OQ'} = \bullet$$



circonferenza Trigonometrica

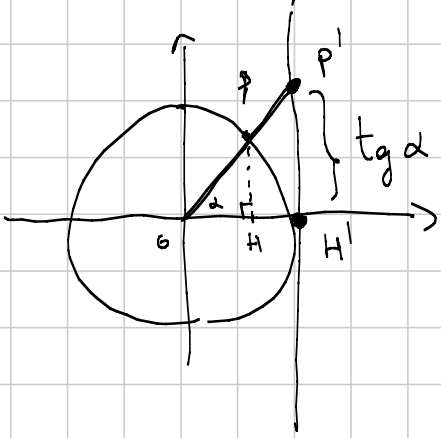
$\bigstar = \cos\alpha$

$\bullet = \sin\alpha$

$$\overline{OP}^2 = 1^2 = \overline{OH}^2 + \overline{PH}^2 = \cos^2\alpha + \sin^2\alpha$$

$$1 = \cos^2\alpha + \sin^2\alpha$$

$\sin\alpha, \cos\alpha \in [-1, 1]$



$$tg\alpha = \frac{\overline{P'H'}}{\overline{OH'}} = \frac{\overline{PH}}{\overline{OH}} = \frac{\sin\alpha}{\cos\alpha}$$

Chiamiamo: "α che?"

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

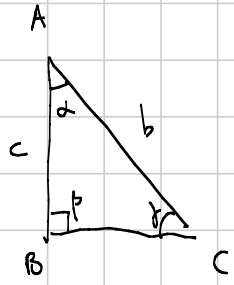
$2\pi \longleftrightarrow 360$

$\pi \longleftrightarrow 180$

$\frac{\pi}{2} \longleftrightarrow 90$

$\frac{\pi}{3} \longleftrightarrow 60$

$\dots$



$\beta = 90^\circ = \frac{\pi}{2}$

$c = b\cos\alpha$

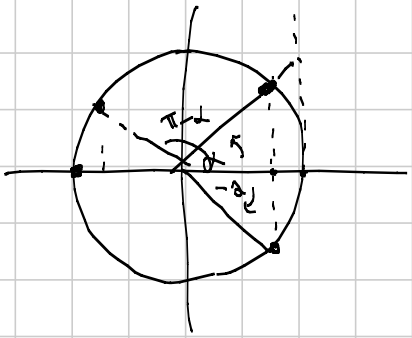
$a = b\sin\alpha = b\cos\gamma$

ma $\beta = 90^\circ \Rightarrow \gamma = 90 - \alpha$

$b\sin\alpha = b\cos\gamma = b\cos(90-\alpha)$

$\Rightarrow \sin\alpha = \cos(90-\alpha)$

"A volte ritornano"



$\sin(2\pi+\alpha) = \sin(\alpha)$

$\cos(2\pi+\alpha) = \cos(\alpha)$

$\sin(\alpha) = \cos(90-\alpha)$

$\beta = \alpha + 90 \hookrightarrow \beta - 90 = \alpha$

$\sin(\beta - 90) = \cos(\beta)$

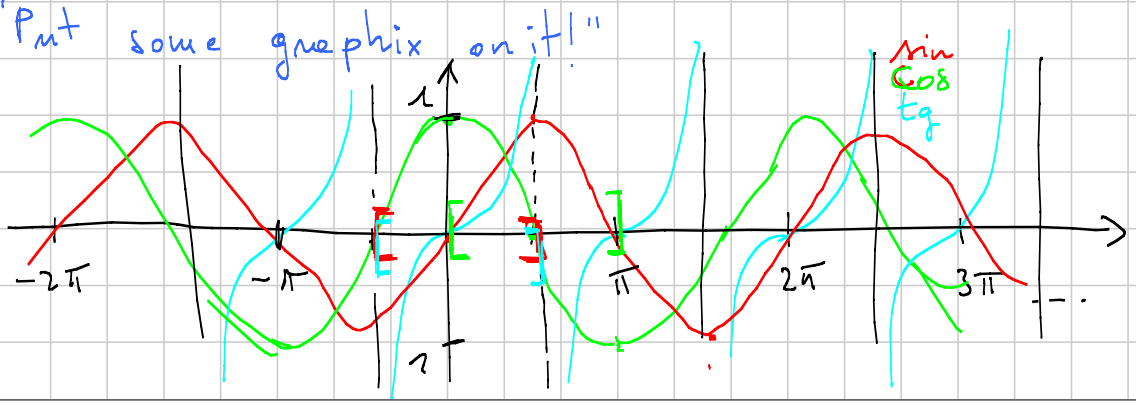
$\sin(-\alpha) = -\sin\alpha$ ← funzioni dispari

$\cos(-\alpha) = \cos\alpha$ ← funzioni pari

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

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

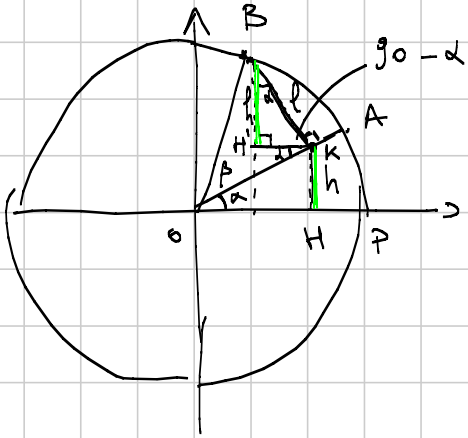
"Put some graphix on it!"



Cerchiamo quando sono iniettive, cioè dove vale "$f(x)=f(y) \iff x=y$".

sin	in	$\left[-\frac{\pi}{2},\frac{\pi}{2}\right]$	$\rightsquigarrow$	$\arcsin : [-1,1] \to \left[-\frac{\pi}{2},\frac{\pi}{2}\right]$
cos	in	$[0,\pi]$	$\rightsquigarrow$	$\arccos : [-1,1] \to [0,\pi]$
tg	in	$\left(-\frac{\pi}{2},\frac{\pi}{2}\right)$	$\rightsquigarrow$	$\arctg : \mathbb{R} \to \left(-\frac{\pi}{2},\frac{\pi}{2}\right)$

"Abracadabra"



~~$\sin(\alpha+\beta) = \sin\alpha + \sin\beta$~~ ||| 😱 |||

$\sin(\alpha+\beta) = h + h'$.

$l = \overbrace{OB}^{1} \sin\beta$

$h' = l\cos\alpha = \sin\beta\cos\alpha$

$h = \sin\alpha\cos\beta$

$\Rightarrow$

$$\sin(\alpha+\beta) = \sin\alpha\cos\beta + \sin\beta\cos\alpha$$
$$\sin(\alpha-\beta) = \sin\alpha\cos\beta - \sin\beta\cos\alpha$$
$$\cos(\alpha\pm\beta) = \cos\alpha\cos\beta \mp \sin\alpha\sin\beta$$

se $\alpha=\beta$

f. di duplicaz.:

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

f. di bisez.:

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

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

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

(tg α, tg β, tg α, tg β)

$$\boxed{tg(2\alpha) = \frac{2tg(\alpha)}{1-tg^2(\alpha)}}$$

Prostaferesi, Werner, parametriche

pr $\sin\alpha + \sin\beta = 2\sin\frac{\alpha+\beta}{2}\cdot\cos\frac{\alpha-\beta}{2}$

w $\sin\alpha\sin\beta = \frac{1}{2}\left[\sin(\alpha+\beta) + \sin(\alpha-\beta)\right]$

par

$$t = tg\frac{\alpha}{2}$$

$$tg\,\alpha = \frac{2t}{1-t^2}$$

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

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

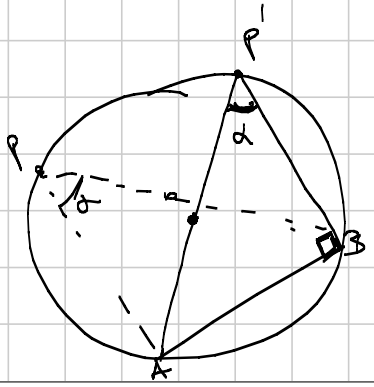
$1+t^2 > 0$ sempre definita

$$\sin\alpha = \cos\alpha\, tg\,\alpha = \frac{2t}{t^2+1}$$

Particolari sui triangoli

Teorema (dei seni)

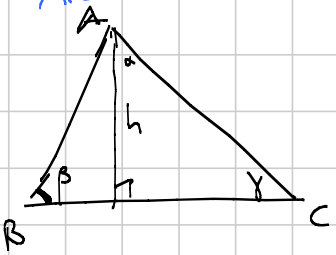
$$\overline{AB} = 2R\sin\alpha$$



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

□

Area



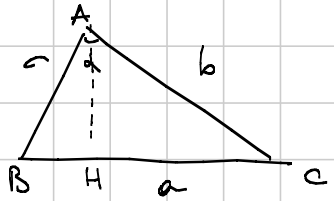
$$\mathcal{A}_{ABC} = \frac{1}{2} b h = \frac{1}{2} ac \sin\beta =$$

$$\sin\beta = \frac{b}{2R}$$

$$\Rightarrow \mathcal{A}_{ABC} = \frac{1}{2} ac \sin\beta = \frac{abc}{4R}$$

□

Teorema (di Carnot o dei coseni)



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

Dim $b^2 + c^2 - a^2 = (AH^2 + CH^2) + (BH^2 + AH^2) - (BH + CH)^2 =$

$= 2AH^2 + \cancel{CH^2} + \cancel{BH^2} - \cancel{CH^2} - \cancel{BH^2} - 2BH\,CH =$

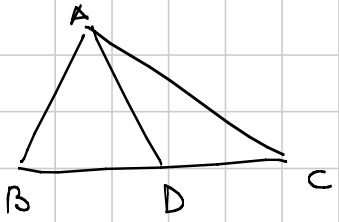
$= 2\,AH\,AH - 2\,BH\,CH =$

$= 2\,c\sin\beta\, b\sin\gamma - 2\,c\cos\beta\, b\cos\gamma = -2bc(\,?\,)$

$= -2bc\cos(\beta+\gamma) = -2bc\cos(\pi-\alpha) = 2bc\cos\alpha$ □

Esercizi

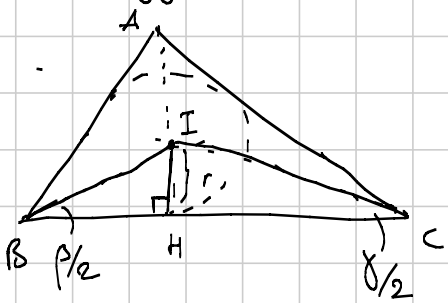
- Teorema (di Stewart)



$$a(BD\,CD + AD^2) = b^2 BD + c^2 CD$$

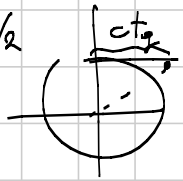
Hint: Carnot su $\widehat{ABD}$ e $\widehat{ADC}$

- Raggio C. inscritta



$$\frac{IH}{BH} = tg\,\beta/2 \qquad \frac{IH}{CH} = tg\,\gamma/2$$

$$r = IH$$



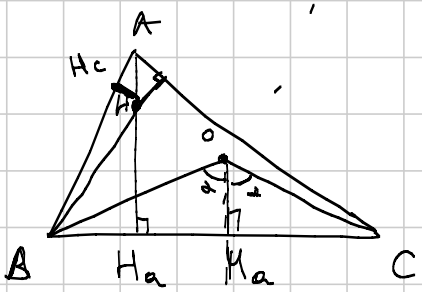
$$\frac{BH}{IH} = \frac{1}{tg\,\beta/2} = \frac{\cos\beta/2}{\sin\beta/2} = ctg\,\beta/2$$

$$\frac{a}{r} = \frac{BH + CH}{r} = ctg\,\beta/2 + ctg\,\frac{\gamma}{2}$$

$$\Rightarrow \quad r = \frac{a}{ctg\,\beta/2 + ctg\,\frac{\gamma}{2}}$$

esiste?

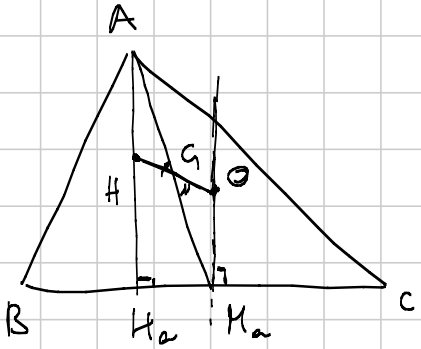
- Ortocentro, Baricentro e circocentro sono allineati.



$$\overline{OM_a} = OB\cos\alpha = R\cos\alpha$$

$$\overline{AH} = \frac{AH_c}{\sin\beta} = \frac{b\cos\alpha}{\sin\beta} = 2R\cos\alpha$$

$$\Rightarrow 2OM_a = AH$$

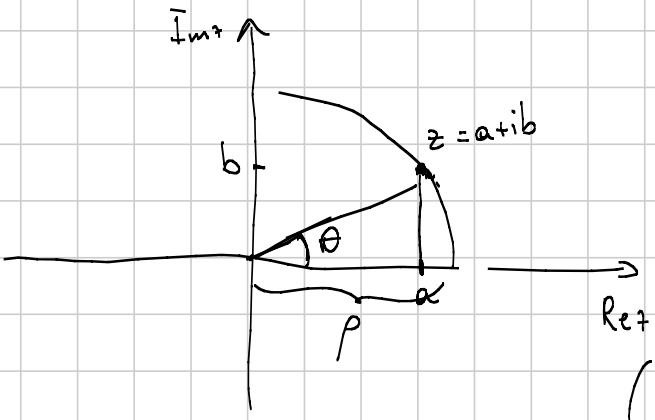


$\overline{AG} = 2\overline{GM_a}$ è proprio il baricentro!

□

NUMERI COMPLESSI

$$\mathbb{C} = \{ a+ib \mid a,b \in \mathbb{R},\ i^2 = -1 \}$$

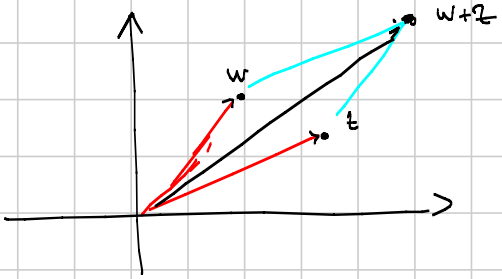


$z = a+ib$
$\uparrow \quad \uparrow$
$\text{Re}z \quad \text{Im}z$

$z = \rho\cos\theta + i\rho\sin\theta =$
$= \rho(\cos\theta + i\sin\theta)$
forma polare
$(\rho e^{i\theta}) \leftarrow$

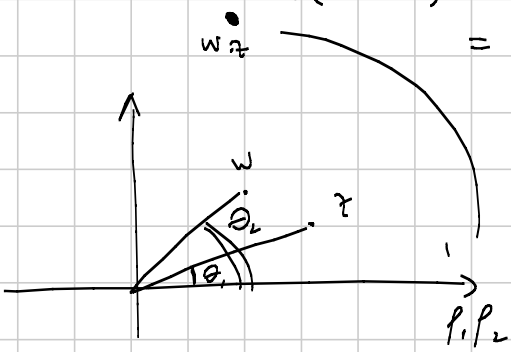
Operazioni

SOMMA : $w+z = (a+ib)+(c+id) = (a+c)+i(b+d)$



PRODOTTO

$w \cdot z = (a+ib)(c+id) = ac + aid + ibc + (-1)bd =$
$= (ac-bd) + i(ad+bc)$



$w \cdot z = \rho_1(\cos\theta_1 + i\sin\theta_1)\rho_2(\cos\theta_2 + i\sin\theta_2)$

$= \rho_1\rho_2(\cos\theta_1\cos\theta_2 + i\sin\theta_2\cos\theta_1 +$
$+ i\sin\theta_1\cos\theta_2 + (-1)\sin\theta_1\sin\theta_2)$

$= \rho_1\rho_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2))$

(θ si chiama argomento)
(ρ si chiama modulo)

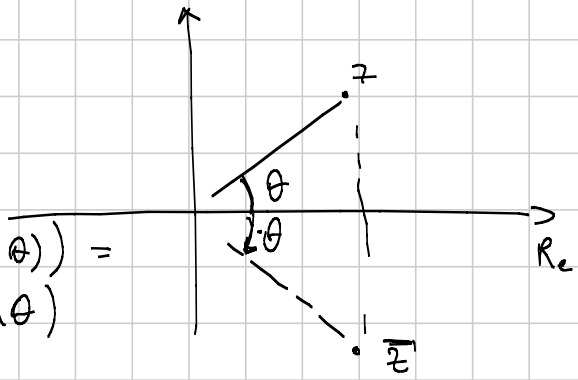
$zw = \rho_1\rho_2(\cos\quad) \overset{?}{=} \rho_1\rho_2 e^{i(\theta_1+\theta_2)}$

SÌ e ci piace

- coniugio

$z = a+ib$

$\bar{z} = a-ib$



$\bar{z} = \rho(\cos\theta + i\sin(-\theta)) = \rho(\cos\theta - i\sin\theta)$

Come calcoliamo il modulo?

$z\bar{z} = (a+ib)(a-ib) = a^2+b^2 = \rho^2\cos^2\theta + \rho^2\sin^2\theta = \rho^2(\sin^2\theta+\cos^2\theta) = \rho^2 = |z|^2$

Pag 3 n° 1, 2, 4, 7, 11

Pag 32 n° 1, 4, 8, 9

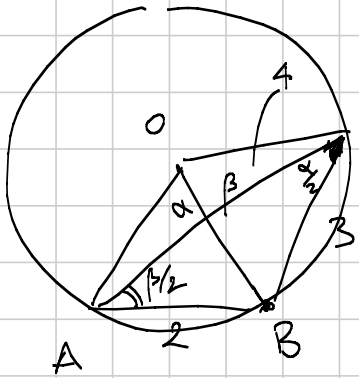
CORREZIONE

1 $\sum_{n=0}^{90}\sin^2(n) = \sum_{n=0}^{44}\left[\sin^2(90-n) + \sin^2(n)\right] + \sin^2(45)$

$\cos^2 n$

$= 45 + \frac{1}{2}$

4



Teorema di Carnot su $\widehat{ABC}$

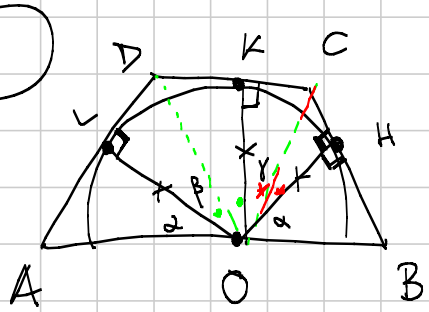
$$2^2 = 3^2 + 4^2 - 2\cdot 3\cdot 4\cos\frac{\alpha}{2}$$

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

$$\Rightarrow \cos\alpha = 2\cos^2\frac{\alpha}{2} - 1 = 2\cdot\frac{7^2}{8^2} - 1$$

$$= \frac{49-32}{32} = \frac{17}{32}$$

9



$$AB^2 = 4\,BC\cdot AD$$

$$AB = AO + OB$$

$$BC = CH + HB$$

$$AD = AL + LD$$

$$CH = \frac{r\sin\gamma}{\cos\gamma} = r\,tg\gamma$$

$$HB = AL = r\,tg\alpha$$

$$LD = r\,tg\beta$$

$$AO = OB = \frac{r}{\cos\alpha}$$

$$\Rightarrow \quad AB = \frac{2r}{\cos\alpha}$$

$$BC = r(tg\alpha + tg\gamma)$$

$$AD = r(tg\alpha + tg\beta)$$

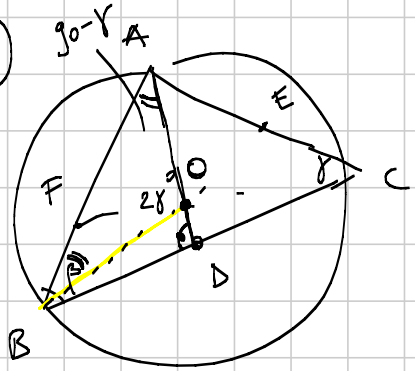
$$\frac{4r^2}{\cos^2\alpha} = 4r^2(tg\alpha + tg\beta)(tg\alpha + tg\gamma)$$

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

$$\left[\cancel{tg^2\alpha + 1} = \cancel{tg^2\alpha} + tg\alpha\, tg\beta + tg\alpha\, tg\gamma + tg\beta\, tg\gamma \right]$$

$\alpha + \beta + \gamma = 90°$ [es 13 p. 33 !] D

(8)



$$\frac{1}{AD} + \frac{1}{BE} + \frac{1}{CF} = \frac{2}{AO}$$

» vale $\frac{(180 - 2\gamma)}{2} = 90 - \gamma$

» vale $180 - (90-\gamma) - \beta = 90 - \beta + \gamma$

Uso teorema dei seni

$$\frac{AD}{\sin\beta} = \frac{AB}{\sin(\gamma)} = \frac{AB}{\sin(90-\beta+\gamma)} = \frac{AB}{\cos(\beta-\gamma)} = \frac{2R\sin\gamma}{\cos(\beta-\gamma)}$$

$$AD = \frac{2R\sin\gamma\sin\beta}{\cos(\beta-\gamma)}$$ gli altri due si trovano allo stesso modo

$$\frac{\cos(\beta-\gamma)}{2R\sin\beta\sin\gamma} + \frac{\cos(\alpha-\beta)}{2R\sin\alpha\sin\beta} + \frac{\cos(\gamma-\alpha)}{2R\sin\alpha\sin\gamma} = \frac{2}{R}$$

$$\sin\alpha\cos(\beta-\gamma) + \sin\beta\cos(\alpha-\gamma) + \sin\gamma\cos(\beta-\alpha) = 4\sin\alpha\sin\beta\sin\gamma$$

$$\sin\alpha\cos\beta\cos\gamma + \sin\alpha\sin\beta\sin\gamma + \text{———} = 4\sin\alpha\sin\beta\sin\gamma$$

$$\cos\alpha\cos\beta\cos\gamma \qquad\qquad \cos\alpha\cos\beta\cos\gamma$$

$$\frac{\sin\alpha}{\cos\alpha} + \cancel{\tg\alpha\tg\beta\tg\gamma} + \tg\beta + \cancel{\tg\alpha\tg\beta\tg\gamma} +$$
$$+ \tg\gamma + \cancel{\tg\alpha\tg\beta\tg\gamma} = 2\tg\alpha\tg\beta\tg\gamma$$

$$\tg\alpha\tg\beta\tg\gamma = \tg\alpha + \tg\beta + \tg\gamma$$

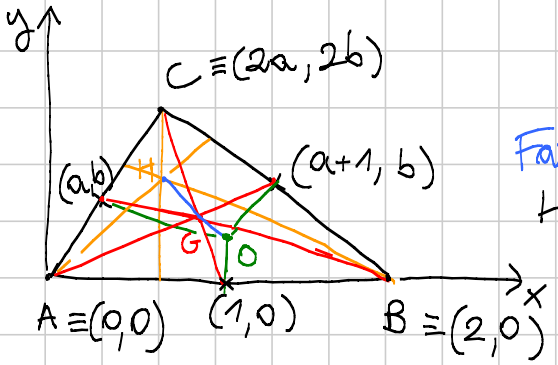
$\alpha+\beta+\gamma = 180°$ [Es 11. p3 ▽.]

□

BUON PRANZO!

Geometria 2

Note Title 9/4/2016



Fatto (Euclero)
H, G, O allineati

calcolo $G \equiv \left(\frac{2}{3}(1+a), \frac{2}{3}b\right)$

calcolo H
sta su h_C $\quad x = 2a$
sta su h_A $\quad y = \frac{1-a}{b}x$
$\left(2a, \frac{2a-2a^2}{b}\right)$

coeff. ang. di CB
$\frac{2b}{2a-2} = \frac{b}{a-1}$

calcolo O
sta sull'asse di AB : $x = 1$
sta sull'asse di AC : $y = -\frac{a}{b}x + \frac{a^2}{b} + b$
$\left(1, -\frac{a}{b} + \frac{a^2}{b} + b\right)$

coeff. ang. di HG
$$\frac{\frac{1}{b}\left(2a - 2a^2 - \frac{2}{3}b^2\right)}{2a - \frac{2}{3} - \frac{2}{3}a} = \frac{\frac{2}{b}\left(a - a^2 - \frac{1}{3}b^2\right)}{\frac{2}{3}(2a-1)}$$

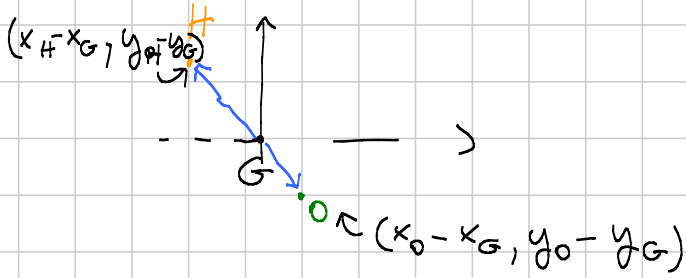
$?$ $=$

coeff. ang. di OG
$$\frac{\frac{1}{b}\left(-a + a^2 + b^2 - \frac{2}{3}b^2\right)}{1 - \frac{2}{3} - \frac{2}{3}a} = -\frac{\frac{1}{b}\left(a - a^2 - \frac{1}{3}b^2\right)}{-\frac{1}{3}(2a-1)}$$

$=$ YES!

BONUS :

$$y_H - y_G = -2(y_O - y_G)$$
$$x_H - x_G = -2(x_O - x_G)$$

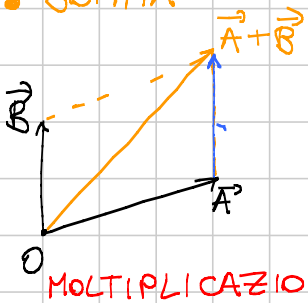


$$\rightarrow \boxed{\overline{HG} = 2\overline{GO}}$$

VETTORI

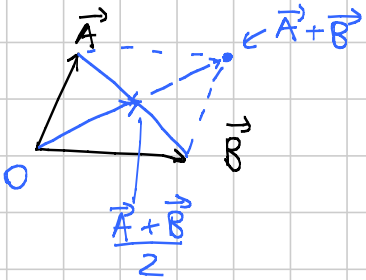
cosa posso fare con vettori?

- SOMMA

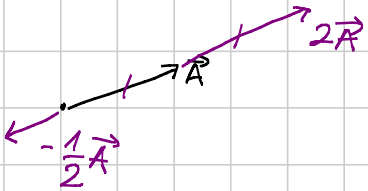


Si scrivono bene:

- pto medio di AB



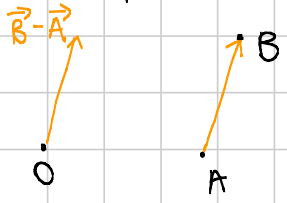
- MOLTIPLICAZIONE PER "SCALARI"



- retta per O e A

$\lambda\vec{A}$ ↖ numero reale

- retta per A e B



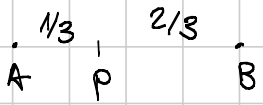
$$\lambda(\vec{B}-\vec{A}) + \vec{A} = \lambda\vec{B} + (1-\lambda)\vec{A}$$

- segmento AB $\quad \lambda \in [0,1]$

$\vec{P} = \lambda \vec{B} + (1-\lambda)\vec{A}$

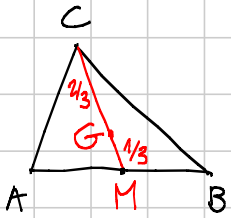
$\frac{\overline{AP}}{\overline{AB}} = \lambda$

esempio



$\vec{P} = \frac{1}{3}\vec{B} + \frac{2}{3}\vec{A}$

Baricentro di ABC



$\vec{M} = \frac{\vec{A}+\vec{B}}{2}$

$\vec{G} = \frac{2}{3}\vec{M} + \frac{1}{3}\vec{C} =$

$= \frac{1}{3}\vec{A} + \frac{1}{3}\vec{B} + \frac{1}{3}\vec{C}$

Ortocentro di ABC

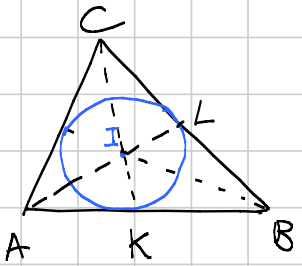
$\vec{H} - \vec{G} = -2(\vec{O} - \vec{G})$

$\vec{H} = 3\vec{G} - 2\vec{O} = \vec{A} + \vec{B} + \vec{C} - 2\vec{O}$

se metto l'origine in $\vec{O}$

$\rightsquigarrow \vec{H} = \vec{A} + \vec{B} + \vec{C}$

Incentro di ABC



$\frac{\overline{AK}}{\overline{KB}} = \frac{\overline{AC}}{\overline{CB}} = \frac{b}{a} \qquad \frac{\overline{AK}}{\overline{AB}} = \frac{b}{a+b}$

$\vec{K} = \frac{b}{a+b}\vec{B} + \frac{a}{a+b}\vec{A}$

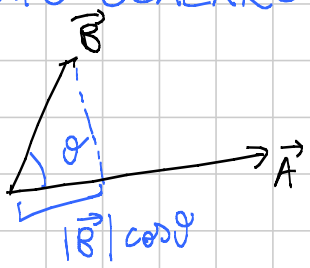
$\frac{\overline{CI}}{\overline{CK}} = \frac{\overline{AC}}{\overline{AC}+\overline{AK}} = \frac{b}{b+\overline{AK}} =$

$= \frac{b}{b + \frac{cb}{a+b}} =$

$= \frac{(a+b)b}{cb + ab + b^2}$

$\vec{I} = \vec{K} \cdot \frac{a+b}{a+b+c} + \vec{C} \cdot \frac{c}{a+b+c} = \frac{a\vec{A} + b\vec{B} + c\vec{C}}{a+b+c}$

• PRODOTTO SCALARE



$\langle \vec{A}, \vec{B} \rangle = |\vec{A}||\vec{B}| \cdot \cos\vartheta$

$\langle \vec{A}+\vec{B}, \vec{C} \rangle = \langle \vec{A}, \vec{C} \rangle + \langle \vec{B}, \vec{C} \rangle$

$\langle \lambda\vec{A}, \vec{B} \rangle = \lambda \langle \vec{A}, \vec{B} \rangle$

$\vec{A} \parallel \vec{B} \quad \langle \vec{A}, \vec{B} \rangle = |\vec{A}||\vec{B}|$

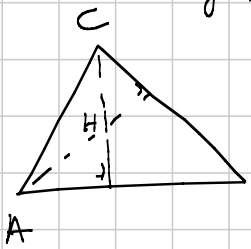
$\vec{A} \perp \vec{B} \quad \langle \vec{A}, \vec{B} \rangle = 0$

(nota: $\langle \vec{A}, \vec{A} \rangle = |\vec{A}|^2$)

in coordinate: $\langle \vec{A}, \vec{B} \rangle = x_A x_B + y_A y_B$

esempio: $\vec{H} = \vec{A} + \vec{B} + \vec{C}$ ... è vero?

(origine in $\vec{O}$)



$\vec{H} - \vec{C} \overset{?}{\perp} \vec{B} - \vec{A}$

$\langle \vec{H} - \vec{C}, \vec{B} - \vec{A} \rangle =$

$= \langle \vec{A} + \vec{B}, \vec{B} - \vec{A} \rangle =$

$= \langle \vec{A}, \vec{B} \rangle + \langle \vec{B}, \vec{B} \rangle - \langle \vec{A}, \vec{A} \rangle - \langle \vec{A}, \vec{B} \rangle$

$= R^2 - R^2 = 0$

altro esempio: $\overline{OI}$ in funzione di R e r

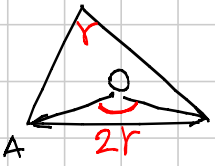
mettiamo origine in O

$\overline{OI}^2 = \langle \vec{I}, \vec{I} \rangle = \left(\frac{1}{a+b+c}\right)^2 \langle a\vec{A} + b\vec{B} + c\vec{C}, \; " \; \rangle$

$= \left(\frac{1}{2p}\right)^2 \left(\sum_{cyc} a^2 \langle \vec{A}, \vec{A} \rangle + \sum_{cyc} 2ab \langle \vec{A}, \vec{B} \rangle \right) =$

$= \left(\frac{1}{2p}\right)^2 \left[R^2(a^2+b^2+c^2) + \sum_{cyc} 2ab R^2 \cos 2\gamma \right] =$

$\cos^2\gamma - \operatorname{sen}^2\gamma = 1 - 2\operatorname{sen}^2\gamma$



$= \left(\frac{1}{2p}\right)^2 \left[R^2(a^2+b^2+c^2) + \sum_{cyc} 2ab R^2 - 4 \sum_{cyc} ab R^2 \operatorname{sen}^2\gamma \right]$

$$= \frac{1}{(2p)^2}\left[R^2(a+b+c)^2 - 4\sum_{cyc} R\frac{c}{2}\cancel{2S}\right] =$$

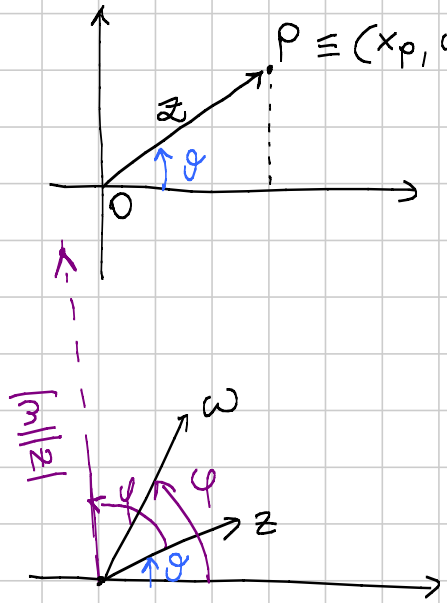
$$= \left(\frac{1}{2p}\right)^2\left[R^2(a+b+c)^2 - 4RS(a+b+c)\right]$$

$$= R^2 - \frac{\cancel{4}^{2}RS}{\cancel{2p}} = R^2 - 2Rr$$

BONUS: $R^2 - 2Rr \geq 0 \rightarrow R(R-2r) \geq 0$

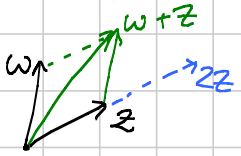
$R \geq 2r$

Complessi



$z = x_P + i y_P =$
$= |z|(\cos\vartheta + i\sin\vartheta)$
$= |z| e^{i\vartheta}$

- si sommano



- si moltiplicano

(per numeri reali E per altri complessi)

$$zw = |z||w| e^{i\vartheta} e^{i\varphi} = |z||w| e^{i(\vartheta+\varphi)}$$

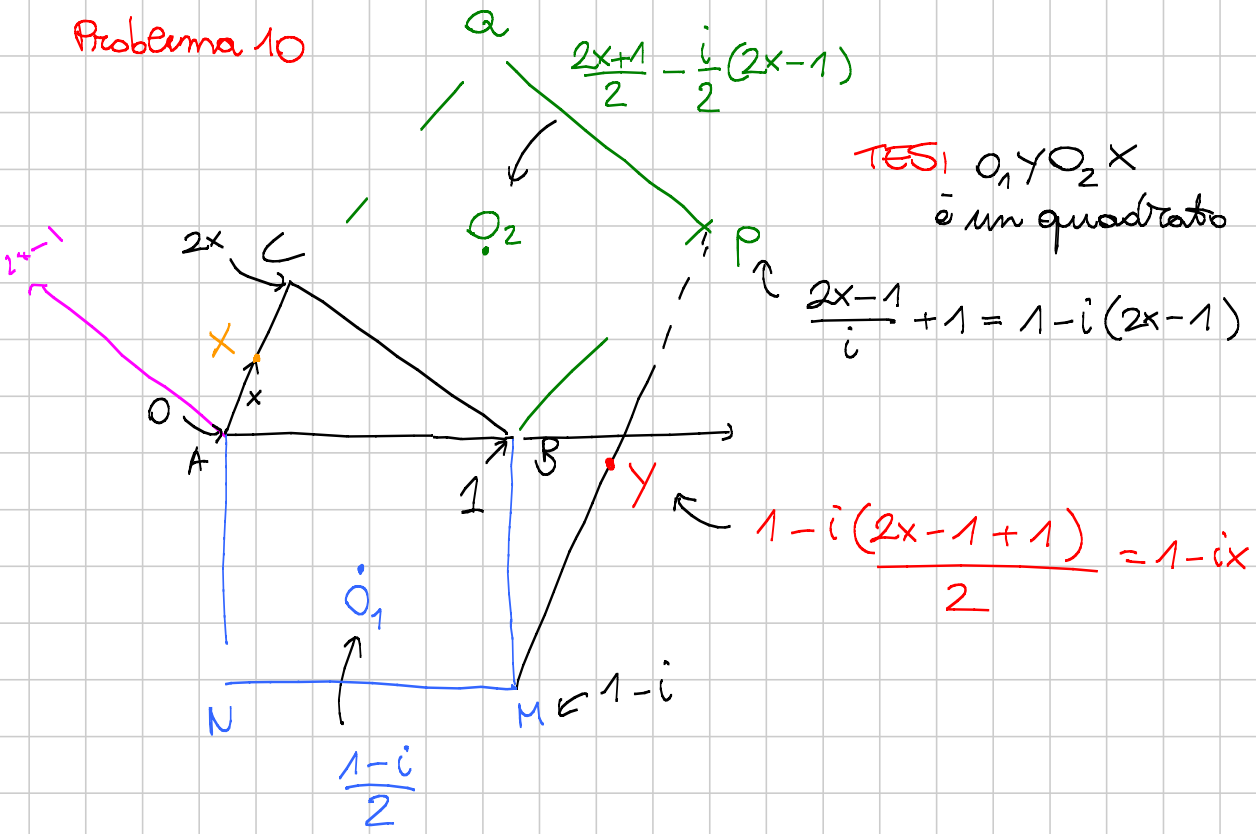
Rotazioni di angoli particolari si scrivono estremamente bene:

↰ → moltiplico per i

↗ 45° → per $\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$

↗ 60° ---

Problema 10



$\vec{XO_2}$ = $\vec{XO_1}$ ruotato di $\curvearrowleft 90°$

$$\left(\frac{1-i}{2} - x\right) i \stackrel{?}{=} \frac{2x+1}{2} - \frac{i}{2}(2x-1) - x$$

$$i\frac{1}{2} + \frac{1}{2} - ix \quad (=) \quad \frac{1}{2} - ix + \frac{i}{2}$$

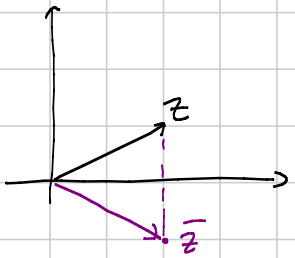
Ok!

faccio lo stesso con altri due lati del quadrato ...

– ... si "coniugano"

$z = a + ib$

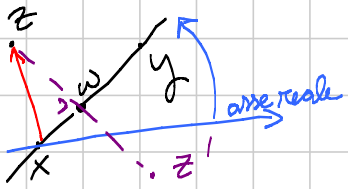
$\bar{z} = a - ib$



$$\mathrm{Re}\, z = \frac{z + \bar{z}}{2}$$

$$\mathrm{Im}\, z = \frac{z - \bar{z}}{2}$$

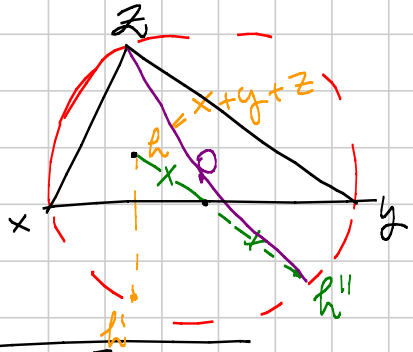
$$z\bar{z} = |z|^2$$



$$\left[\frac{(z-x)}{(y-x)}\right](y-x)+x=z'$$

$$w=\frac{z+z'}{2}$$

Esempio



$$x\bar{x}=y\bar{y}=z\bar{z}=1$$

$$\left[\frac{h-x}{y-x}\right](y-x)+x=$$

$$=\left[\frac{x+y+z-x}{y-x}\right](y-x)+x=$$

$$=\frac{\bar{y}+\bar{z}}{\bar{y}-\bar{x}}(y-x)+x=\frac{(\bar{y}+\bar{z})(y-x)+x(\bar{y}-\bar{x})}{\bar{y}-\bar{x}}$$

$$=\frac{y\bar{y}+\bar{z}y-\bar{y}x-\bar{z}x+x\bar{y}-x\bar{x}}{\bar{y}-\bar{x}}=$$

$$=\frac{\bar{z}(y-x)}{(y-x)}$$

ha modulo 1!

Calcolo h''

$$-\left(h-\frac{x+y}{2}\right)+\frac{x+y}{2}=-x-y-z+x+y=$$

$$=-z$$

importanti!

8, 6, 16, 20, 9

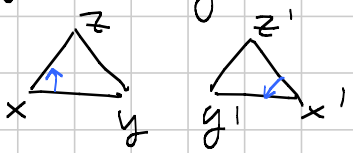
Parentesi bonus: come si può scrivere la condizione di similitudine di due triangoli in complessi?

6. $\vec{M} = \frac{\vec{A}+\vec{B}}{2}$

$\vec{CM} \quad \vec{M} - \vec{C} = \frac{\vec{A}+\vec{B}-2\vec{C}}{2}$

$|\vec{CM}|^2 = \left\langle \frac{\vec{A}+\vec{B}-2\vec{C}}{2}, \frac{\vec{A}+\vec{B}-2\vec{C}}{2} \right\rangle$

$\frac{z-x}{y-x} = \frac{z'-x'}{y'-x'}$



origine nel circocentro

$\rightarrow \frac{1}{4}\left(\langle\vec{A},\vec{A}\rangle + \langle\vec{B},\vec{B}\rangle + 4\langle\vec{C},\vec{C}\rangle + 2\langle\vec{A},\vec{B}\rangle - 4\langle\vec{A},\vec{C}\rangle - 4\langle\vec{B},\vec{C}\rangle\right)$

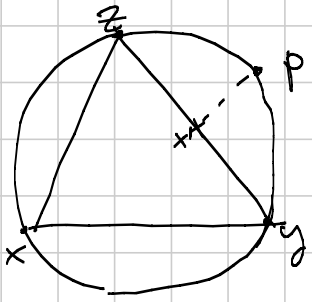
$= \frac{1}{4}\left(6R^2 + 2R^2\cos 2\gamma - 4R^2\cos 2\beta - 4R^2\cos 2\alpha\right) =$

$= \frac{1}{4}\left(-2R^2\operatorname{sen}^2\gamma + 4R^2\operatorname{sen}^2\beta + 4R^2\operatorname{sen}^2\alpha\right) =$

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

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

16

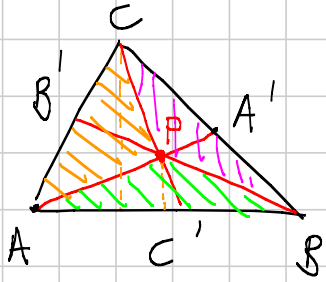


$x\bar{x} = y\bar{y} = z\bar{z} = 1 = p\bar{p}$

Geometria 3

Note Title 9/6/2016

Teorema di Ceva



AA', BB', CC' concorrono $\iff$

$\star \quad \frac{AC'}{C'B} \cdot \frac{BA'}{A'C} \cdot \frac{CB'}{B'A} = 1$

dimostriamo $\Rightarrow$)

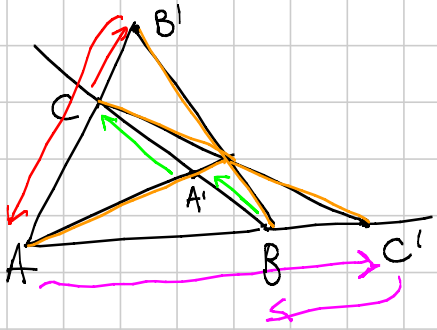
$$\frac{AC'}{C'B} = \frac{[APC']}{[C'PB]} = \frac{[ACC']}{[CC'B]} = \frac{[PCA]}{[PCB]}$$

$\left(\frac{AC'}{C'B} = \lambda \right.$ $\left.\begin{array}{l} [APC'] = \lambda [C'PB] \\ [ACC'] = \lambda [CC'B] \\ [PCA] = \lambda [PCB] \end{array}\right]$ differenza

$$\star = \frac{[PCA]}{[PCB]} \cdot \frac{[PBA]}{[PCA]} \cdot \frac{[BCP]}{[BPA]} = 1.$$

(ora $\Leftarrow$ è facile).

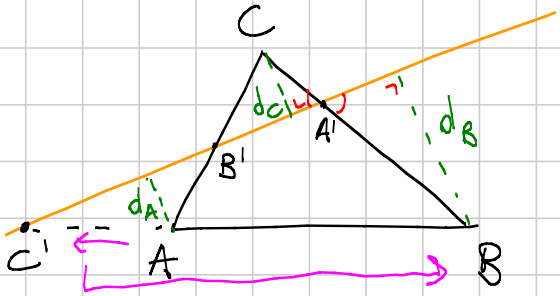
NOTA: posso usare Ceva con "segmenti orientati"



$\frac{AC'}{C'B} \cdot \frac{BA'}{A'C} \cdot \frac{CB'}{B'A}$

(−) (+) (−)

Teorema di Menelao



A', B', C' (su BC, AC, AB) sono allineati $\iff$

$\star$ $\dfrac{BA'}{A'C} \cdot \dfrac{CB'}{B'A} \cdot \dfrac{AC'}{C'B} = -1$

$\Rightarrow$)

$$\frac{BA'}{A'C} = \frac{d_B}{d_C}$$

$$\frac{CB'}{B'A} = \frac{d_C}{d_A}$$

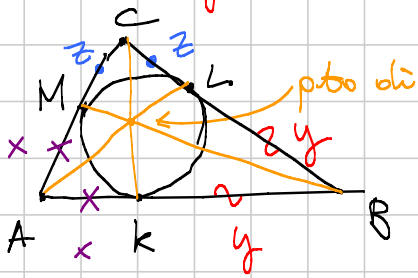
$$\frac{AC'}{C'B} = -\frac{d_A}{d_B}$$

(nel mio disegno)

$\star = \dfrac{d_B}{d_C}\left(-\dfrac{d_A}{d_B}\right)\left(\dfrac{d_C}{d_A}\right) = -1$

Funziona perché se taglio con ℓ ottengo 1 o 3 rapporti negativi.

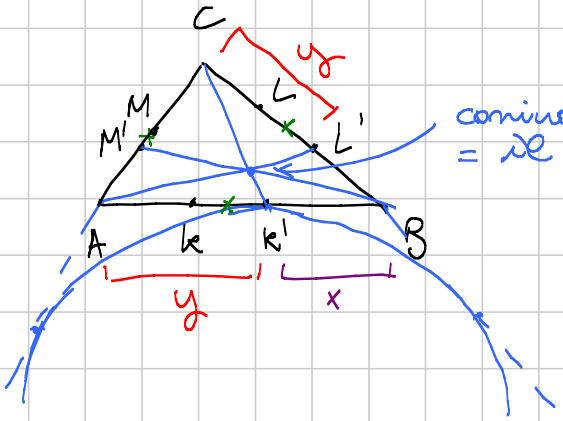
Qualche conseguenza di Ceva:



pto di Gergonne

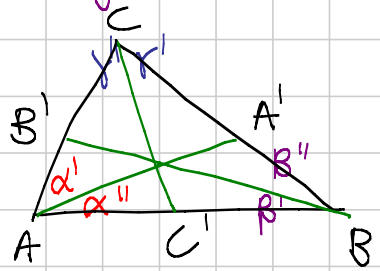
$\dfrac{x}{y} \cdot \dfrac{y}{z} \cdot \dfrac{z}{x} = 1$

$\Rightarrow$ AL, BM, CK concorrono!



coniugato isotomico di Gergonne = il pto di Nagel

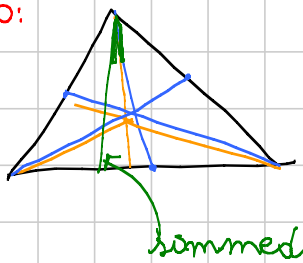
Ceva trigonometrico



AA', BB', CC' concorrono $\iff$

$$\frac{\operatorname{sen}\alpha'}{\operatorname{sen}\alpha''} \cdot \frac{\operatorname{sen}\beta'}{\operatorname{sen}\beta''} \cdot \frac{\operatorname{sen}\gamma'}{\operatorname{sen}\gamma''} = 1$$

Esempio:



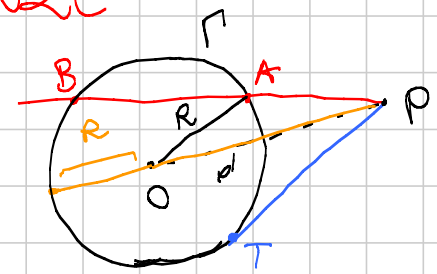
mediane

bisettrici

simmediana

le simmediane concorrono nel coniugato isogonale del baricentro...

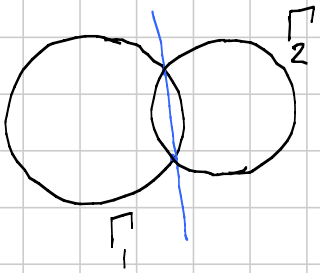
POTENZE



$$\operatorname{pow}_\Gamma(P) = PA \cdot PB = (d-R)(d+R) = d^2 - R^2$$

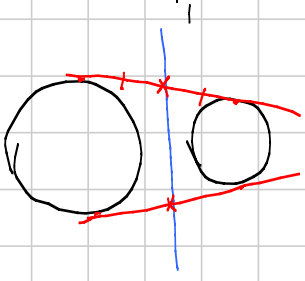
Nota $P \equiv (x_P, y_P)$ $\quad \Gamma : (x-x_0)^2 + (y-y_0)^2 - R^2 = 0$

$$\operatorname{pow}_\Gamma(P) = (x_P - x_0)^2 + (y_P - y_0)^2 - R^2$$



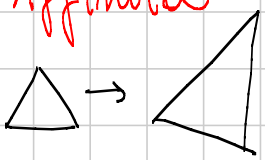
qual è il luogo dei pti P t.c. $\operatorname{pow}_{\Gamma_1}(P) = \operatorname{pow}_{\Gamma_2}(P)$?

È una RETTA (nell'eq. x^2 cancellano i termini di deg 2) detta asse radicale ...



TRASFORMAZIONI

- **Affinità**

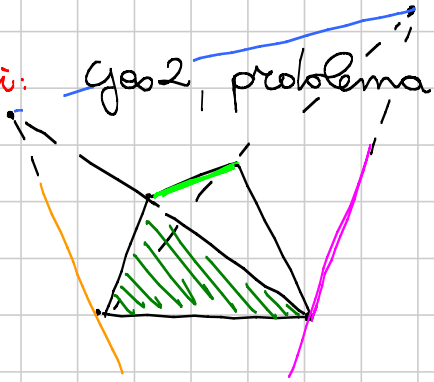


Coordinate: $(x,y) \mapsto (ax+by+c, dx+ey+f)$
$ae \neq bd$
aree si moltiplicano per $ae-bd$.

✓ conservano: collinearità (rette → rette), parallelismo, concorrenza, rapporti di segmenti sulla stessa retta (e.g. pti medi...), rapporti di aree

✗ NON si conservano: angoli, rapporti di segmenti, perpendicolarità, circonferenze

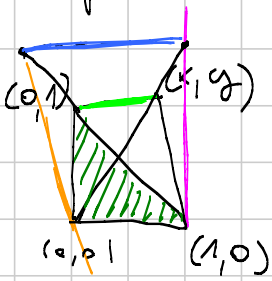
Esempi: geo2, problema 9

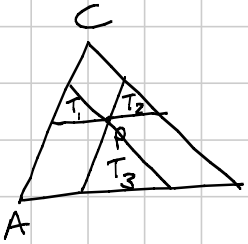


$\parallel$

tesi invariante per affinità

⇝ posso fare i conti su

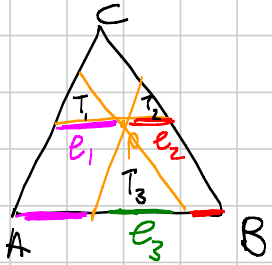




$T = [ABC]$

Tesi: $\sqrt{T_1}+\sqrt{T_2}+\sqrt{T_3} = \sqrt{T}$
è invariante per affinità!

posso ridurmi a:

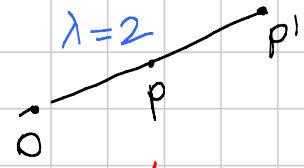


$$\ell_1 + \ell_2 + \ell_3 = \ell$$

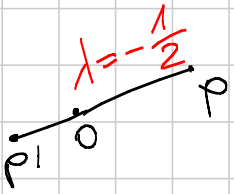
$$\sqrt{\frac{\sqrt{3}}{4}\ell_1^2} + \dots = \sqrt{\frac{\sqrt{3}}{4}\ell^2}$$

- Omotetie

omotetia di centro O e ragione $\lambda \in \mathbb{R} \setminus \{0\}$

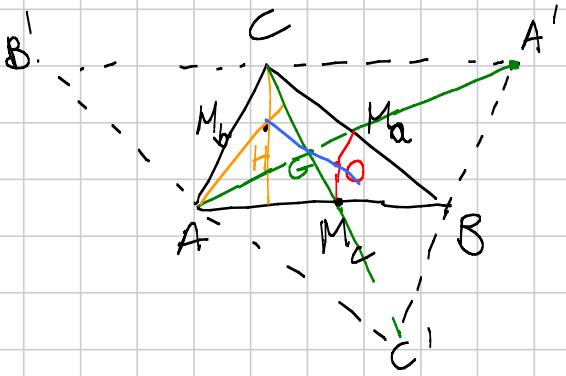


$P \to P'$ sulla retta OP tale che $OP' = \lambda OP$



✓ conservano: rette → rette, angoli, circonf. → circonf., rapporti di seg./aree (si moltiplicano per λ^2)

(in coordinate se il centro è nell'origine omotetia = moltiplicare per λ $z \mapsto \lambda z$)



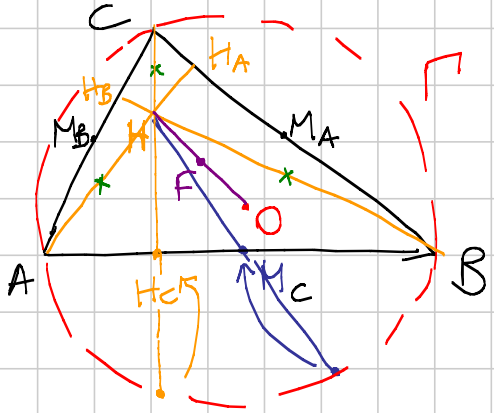
Retta di Eulero
omotetia di centro G, ragione -2

$A, B, C \to A', B', C'$
$(A'B' \parallel AB \dots)$
$M_c \to C$ $M_a \to A$ $M_b \to B$

assi di ABC → perpendic. a $A'B'$, $B'C'$, $C'A'$ per C, A, B
= perp. a AB, BC, CA per C, A, B
= altezze di ABC

↝ il circocentro di ABC O → incontro assi di $A'B'C'$ = incontro delle altezze di ABC : H.

Circonferenza di Feuerbach



omotetia di centro H e ragione $1/2$.

$O \to F$ pto medio di OH

$\Gamma \to \Gamma'$ circ. di centro F e raggio $R/2$

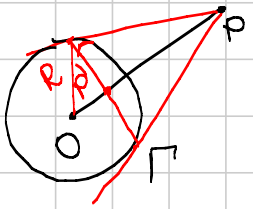
→ H_A, H_B, H_C stanno su Γ'.

→ pti medi M_A, M_B, M_C stanno su Γ'

→ anche i 3 pti "x" stanno su Γ'

" circonferenza dei 9 pti "

– Inversione circolare



inversione risp. a una circ. Γ : piano $\setminus \{O\} \to$

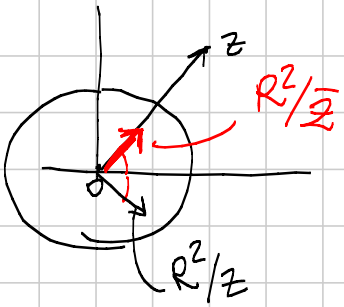
$P \to P'$ sulla semiretta OP

$OP \cdot OP' = R^2$

Nota: esterno ↔ interno

è una "involuzione"

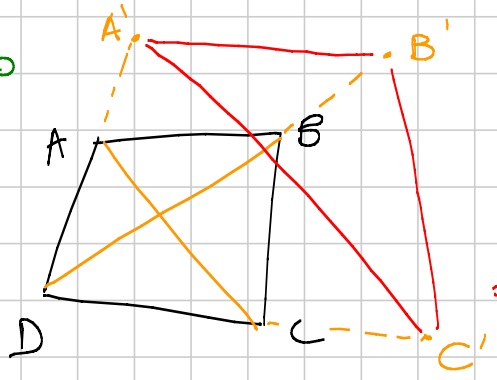
in complessi se il centro è nell'origine $z \mapsto \frac{R^2}{\bar{z}}$



✓ conserva angoli!

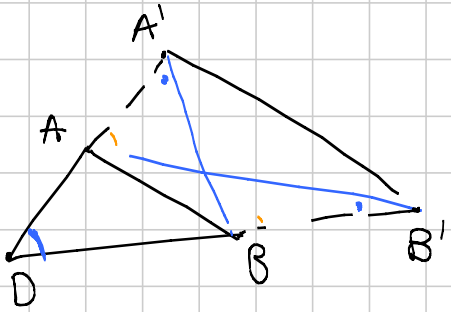
- Γ ↺
- rette per O ↺
- rette non per O → circonferenze per O
- circonferenze per O → rette non per O
- circonf. non per O → circonf. non per O

Tolomeo



$AC \cdot BD \leq AD \cdot BC + AB \cdot CD$
= vale $\Leftrightarrow$ ABCD ciclico

LEMMA $\overline{A'B'} = \dfrac{\overline{AB}\, R^2}{\overline{AD} \cdot \overline{DB}}$



$\overline{DA'} = R^2/\overline{AD}$
$\overline{DB'} = R^2/\overline{DB}$

$\overline{DA'} : \overline{DB'} = \overline{DB} : \overline{AD}$
$\widehat{ADB} \sim \widehat{B'DA'}$

$$\frac{\overline{A'B'}}{\overline{AB}} = \frac{\overline{DA'}}{\overline{DB}} = \frac{R^2}{\overline{AD} \cdot \overline{DB}}$$

$\sim$

tornando a Tolomeo...

$$\overline{A'C'} \leq \overline{A'B'} + \overline{B'C'}$$

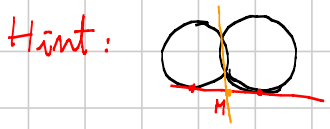
$$\frac{R^2 \overline{AC}}{\overline{AD}\,\overline{DC}} \leq \frac{R^2 \overline{AB}}{\overline{AD}\,\overline{BD}} + \frac{R^2 \overline{BC}}{\overline{DB}\,\overline{DC}}$$

$$\overline{AC}\cdot\overline{DB} \leq \overline{AB}\,\overline{CD} + \overline{BC}\,\overline{AD}$$

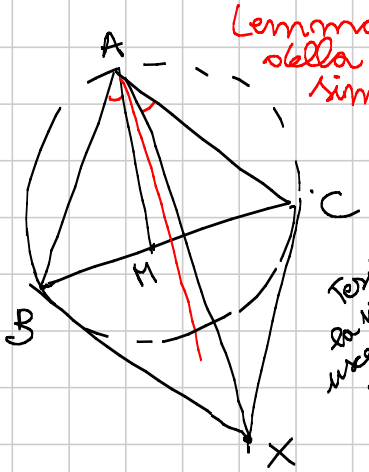
$=$ $\Leftrightarrow$ A', B', C' sono allineati
$\Leftrightarrow$ A, B, C stanno su una circonferenza per D
($=$ $ABCD$ ciclico)

IMO 2016.1

Hint: inverto in A in modo da scambiare B e C



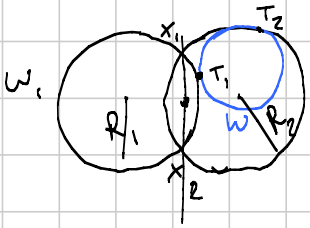
Lemma della simmediana



Tesi: la simmediana uscente da A passa per X

Problemi: 6, 12

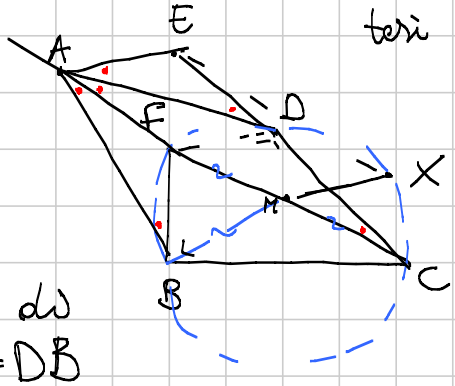
EGMO 2016.4



Hp. $R_1 = R_2$

TESI: $X_1T_1 \cap X_2T_2 \in \omega$

IMO 1



tesi BD, FX, ME concorrono

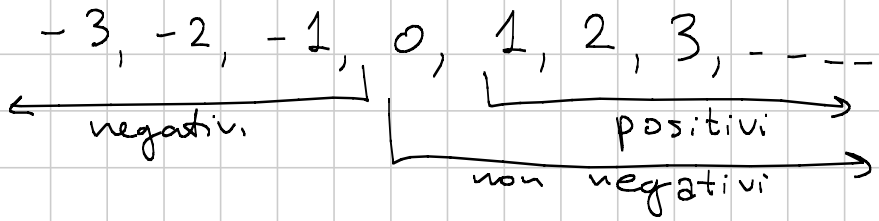
* ω è $\odot BCF$; D sta su ω
* X sta su ω
* F è l'incentro di DAB e $DA = DB$
* B, F, E sono allineati

$x_1 \, L T_2' X_2'$ ciclico

Teoria dei Numeri 1

Note Title 9/3/2016

Kirill Kuzmin



$b \geq 2$ Si possono scrivere in base b

$$2016 = 2 \cdot 1008 =$$

$$= 2 \cdot 2 \cdot 504 = 2 \cdot 2 \cdot 2 \cdot 252 =$$

$$= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 126 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 63 =$$

$$= 2^5 \cdot 3^2 \cdot 7$$

I numeri come 2, 3, 5, 7, 11 etc. che non sono rappresentabili come prodotto di numeri più piccoli sono detti "primi"

I numeri primi sono infiniti

a, b interi $a \mid b$ se $b = k \cdot a$

"a divide b"

Primi: > 1 che hanno come divisori positivi solo 1 e se stesso.

Ogni numero si può scrivere come prodotto di primi IN MODO UNICO

$2016 = 2^5 \cdot 3^2 \cdot 7$ $\quad 2015 = 5 \cdot 13 \cdot 31$

2017 è primo

Altro modo di definire i primi

Esempio: mn pari, allora m pari oppure n pari

$2 \mid mn$, allora $2 \mid m$ o $2 \mid n$

Questo vale per ogni primo p:

$p \mid mn$ allora $p \mid m$ o $p \mid n$

$10 \mid 4 \cdot 25$ ma $10 \nmid 4$ e $10 \nmid 25$

10 non è primo.

$1 \mid$ intero $\quad$ intero $\mid 0$

$2 \mid 2016$ $\quad$ $2^5 \| 2016$ ← divide esattamente

① $2^5 \mid 2016$

$2^6 \nmid 2016$

$10 \nmid 2016$

a, b interi $b > 0$

$a = 2016 \quad b = 10$

$a = qb + r$ resto $2016 = 0 \cdot 10 + 2016$

$q = 0 \quad r = a$

c'è un'unica scrittura per cui $0 \le r \le b-1$

$2016 = 201 \cdot 10 + 6$ Divisione euclidea

Resto

Quando $b \mid a$? Quando il resto è 0

Massimo Comun Divisore

$d = MCD(a,b) = (a,b)$ $\quad a = 102$, $b = 30$

$d \mid a \quad d \mid b$

Massimo: se $c \mid a$, $c \mid b$, allora $c \mid d$

$MCD(102,30) = 6$

$MCD(a,b) = MCD(a+b,b) = MCD(a-b,b)$

$a = bq + r$ divisione euclidea

$= MCD(b,r)$

Come si calcola

Modo 1: Fattori primi in comune

Modo 2: Algoritmo di Euclide

a	b	
102	30	
1	0	102
0	1	30
1	−3	12
−2	7	6
5	−17	0

$102 = 3 \cdot 30 + 12$

$= 102 - 3 \cdot 30$

$30 = 2 \cdot 12 + 6$

$= 30 - 2 \cdot 12$

$6 = -2 \cdot 102 + 7 \cdot 30$

Teorema di Bézout

$MCD(a,b) = ha + kb$

Come ottenere le altre coppie?

$MCD(a,b) = ha + kb = ha + kb + n\frac{ab}{MCD(ab)} - n\frac{ab}{MCD(a,b)}$

$= \left(h + n\frac{b}{(a,b)}\right)a + \left(k - n\frac{a}{(a,b)}\right)b$

$6 = (-2 + n \cdot 5)102 + (7 - n \cdot 17)30$

Quando $MCD(a,b) = 1$ ↔ primi tra loro, coprimi, relativamente primi

Succede quando non hanno fattori primi in comune

$a = 3 \quad b = 5 \qquad 1 = 2 \cdot 3 + (-1) \cdot 5$

Diofantee (dovete cercare soluzioni intere)

$\longrightarrow x \cdot 3 + y \cdot 5 = 2016$

$(2 - n \cdot 5)3 + (-1 + n \cdot 3)5 = 1$

$x = 2016(2 - n \cdot 5) \qquad y = 2016(-1 + n \cdot 3)$

n intero qualunque

$x \cdot 102 + y \cdot 30 = 9$

$x \cdot 102 + y \cdot 30 = 4$

In generale $ax+by=c$ ha soluzione se e solo se $MCD(a,b) \mid c$

$$x^2 - y^2 = 9$$

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

$x+y$	$x-y$
9	1
3	3
1	9
−1	−9
−3	−3
−9	−1

$x+y=9$, $x-y=1$ ok

$x=5$, $y=4$

$$x^2 - y^2 = 14$$

$$(x+y)-(x-y) = 2y$$

$$14 = (x+y)(x-y)$$

$x+y$	$x-y$	
14	1	$x=7{,}5$, $y=6{,}5$ NO!
7	2	No
⋮	⋮	

In generale un numero 2 dispari NON si può scrivere come differenza di quadrati

---

$$xy + x + y + 1 = 11 + 1$$

$$(x+1)(y+1) = 12 = 2^2 \cdot 3$$

$$xy + x + y + 1 = 12$$

$x+1$	$y+1$	
12	1	$x=11$, $y=0$
6	2	$x=5$, $y=1$
⋮	⋮	

$xy + x + y = 11$

$xy + x = 11 - y$

$x(y+1) = 11 - y$

$x = \dfrac{11-y}{y+1}$ → quando è intero?

$\dfrac{-y+11}{y+1} = \dfrac{-y-1+12}{y+1} = -1 + \dfrac{12}{y+1}$

INTERO se e solo se intero, e questo sappiamo farlo

Congruenze

m intero ≥ 2

$a \equiv a' \pmod m$ se

"a è congruo ad a' modulo m"

$m \mid a - a'$ se e solo se a ed a' danno lo stesso resto diviso per m

Che giorno della settimana sarà il 3 settembre 2017?

domenica

sabato +1

$365 = 52 \cdot 7 + 1$

3 settembre 2015 era giovedì

sabato −2

$a \equiv a' \pmod m$

$b \equiv b' \pmod m$

Allora $a+b \equiv a'+b' \pmod m$

$a-b \equiv a'-b' \pmod m$

$ab \equiv a'b' \pmod m$

$(a+b) - (a'+b') = (a-a') + (b-b')$

↑ divisibile per m ↑ divisibile per m

$ab - a'b' = ab - ab' + ab' - a'b' = a(b-b') + b'(a-a')$

divisib per m divisib per m

$0, 1, \dots, m-1$

significa

n umero $\equiv 0 \pmod 3$ divisibile per 3

$\equiv 1 \pmod 3$ dà resto 1 diviso per 3

Se so che $a \mid b$ e conosco i resti della divisione di a e di b per m riesco a trovare il resto di $\frac{b}{a}$?

Risposta: NON sempre

$m=2$ $6/2 = 3$ $8/2 = 4$

NON si può se $MCD(m,a) > 1$

Se $MCD(m,a) = 1$ sì

$m=5$ $36 : 3 = 12$ $36 = 3 \cdot 12$

mod 5 1 3 2

$3 \times 2 = 6 \equiv 1 \pmod 5$

$1 = 2 \cdot 3 - 1 \cdot 5$

Trovare $\frac{b}{a}$ modulo m se $b \equiv 1 \pmod m$ a è coprimo con m

$1 = ka + hm$

k è detto "inverso di a modulo m" $a^{-1} \pmod m$

$27 : 3 \mod 5$ è

$2 \cdot (3^{-1} \pmod 5) \equiv 2 \cdot 2 \pmod 5 = 4$

---

modulo 4 $\quad 6/2 = 3 \quad 10/2 = 5 \equiv 1$

$a, a^2, a^3, \dots \pmod m$

$a, a^2, a^3, \dots, a^k, \dots, a^{k+h} \equiv a^k \pmod m$

$a^{k+h} \equiv a^k \pmod m$

$a^{k+h+1} \equiv a(a^{k+h}) \equiv a \cdot a^k \equiv a^{k+1} \pmod m$

$a^{k+h+2} \equiv a^{k+2} \pmod m$

Mod 24, potenze di 2

$2, 4, 8, 16, 8, 16, 8, \dots$

$3^{2016} \equiv 3^4 \equiv 1 \pmod{10}$

$3, 9, 7, 1, 3, 9, 7, 1$

perché $2016 \equiv 4 \pmod 4$ — è il periodo delle potenze di 3 modulo 10

$a \bmod 3$	$a^2 \bmod 3$
0	0
1	1
2	1

$a \bmod 4$	$a^2 \bmod 4$
0	0
1	1
2	0
3	1

$x^2 - y^2$ non può essere $2 \cdot$ dispari $\equiv 2 \pmod 4$

$0 - 0 \equiv 0$
$0 - 1 \equiv -1 \equiv 3$
$1 - 0 \equiv 1$
$1 - 1 \equiv 0$

$a^2 \bmod 5$ può essere solo $0, 1, -1 \equiv 4$
$a^4 \bmod 5$ può essere solo $0, 1$
$a^2 \bmod 8$ può essere solo $0, 4, 1$
$a^4 \bmod 16$ solo $0, 1$
$a^3 \bmod 7$ può essere solo $0, 1, -1 \equiv 6$
$a^3 \bmod 9$ $0, 1, -1 \equiv 8$

Base: 38, 40, 42, 51, a desiderio
Altri: 6, 8, 9, 10

$$7 = q_1^2 + q_2^2 + q_3^2$$

q_1, q_2, q_3 razionali

Soluzioni agli esercizi

38 Se $p \mid ab$ allora $p \mid a$ o $p \mid b$

VERO (DEF)

Se $p^2 \mid ab$ allora $p^2 \mid a$ oppure $p^2 \mid b$

NO: se $p \mid a$ e $p \mid b$ è falso

$p \mid a-b$, allora $p \mid a+b$ Falso

vero se $p=2$

Se $p^2 \mid a^3$, allora $p^6 \mid a^6$

$p \mid p^2$ $p \mid a \cdot a \cdot a$ allora $p \mid a$ VERO

Se $p^2 \mid b^3$, allora $p^2 \mid b$ FALSO

$p \mid (a,b)$ $p \mid (a^2, ab)$

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

VERO

$\frac{n+3}{n+1} = \frac{n+1+2}{n+1} = 1 + \frac{2}{n+1}$ Intero se $n+1 \mid 2$

$\frac{15-3n}{2n^2+1}$ $\frac{2n^2+1}{-3n+15} = (an+b) + \frac{c}{-3n+15}$

$n \leq -4$ } se succede questo, il VA del NUM
$n \geq 6$ } è più piccolo del VA del DEN

$n = -3, -2, \dots, 5$ Finiti casi, provare tutti

$|15 - 3n| \leq (2n^2 + 1)$

---

5 $\_\_\_\_\_02$

qualcosa $\cdot 100 + 2 = 2(qc \cdot 50 + 1)$ dispari

modulo 4: $0 + 2 \equiv 2$

$n = p_1^{h\alpha_1} \cdots p_k^{h\alpha_k}$ → NON è una potenza

---

6 $p^4 - q^4$ $p > q \geq 10$ primi

Sia M il MCD cercato

Sia r un primo > 10

Perché $r \nmid M$? $p > r$ $q = r$

$p^4 - r^4$ non è divisibile per r

$2, 3, 5, \cancel{7}$

$13, 11$ $13^4 - 11^4 \mod 7$

$(-1)^4$ $(-3)^4$

$1 - 4 \equiv -3$

$x^4 \mod 5$ può essere solo $1, \cancel{0}$

$p^4 - q^4$ ha un fattore 5

$(13^4 - 11^4) = (13^2 + 11^2)(13 + 11)(13 - 11)$

290 NO 5 NO 5

$5 \| M$

↑ un solo fattore 3

$p^4 - q^4$ $\quad 3 \mid M$

$1 - 1 \equiv 0 \pmod 3$

$p^4 - q^4$ $\quad 16 \mid M$

$1 - 1 \equiv 0 \pmod{16}$

$17^4 - 13^4 = (17^2 + 13^2)(17+13)(17-13)$

$30 \qquad 4$

un solo fattore 2, sempre

mod 4

$p^2 \equiv 1$

$q^2 \equiv 1$ $\quad p^2 + q^2 \equiv 2$

3 Fattori 2

$M = 2^4 \cdot 3 \cdot 5$

---

8 $\quad MCD(100 + n^2,\ 100 + (n+1)^2)$

$n > 0$ intero

$= MCD(100 + n^2,\ 2n + 1)$

Se $\quad a \mid 100 + n^2, \quad a \mid 2n + 1$

Allora $\quad a \mid 200 + 2n^2 \qquad a \mid 2n^2 + n$

e quindi $\quad a \mid n - 200, \quad a \mid 2n - 400$

e perciò $\quad a \mid 401 \qquad 401$ è primo

$401 \mid 2n + 1 \qquad n = 200$

$200^2 + 100 = 100(1 + 400)$ OK

$(200+1)^2+100 = 100+200^2+2\cdot 200+1$

ok 401 ok

$y^2 = x^5 - 4$ Modulo 11

x^5 modulo 11 assume valori $0, 1, -1$

y	y^2
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

$x^5 - 4$

può fare solo $6, 7, 8$

NON esistono soluzioni modulo 11, e quindi nemmeno negli interi.

$7 = a_1^2 + a_2^2 + a_3^2$

$7d^2 = a^2 + b^2 + c^2$

$-d^2 \equiv a^2 + b^2 + c^2 \pmod 8$

0 Residui quadratici mod 8: 0, 1, 4

-0

-1

-4

3 dispari: NO

$1+1+0$ 2 disp, 1 pari NO

4

1 dispari: NO

3 pari OK! e allora anche d è pari

$7(2d')^2 = (2a')^2 + (2b')^2 + (2c')^2$

dividi per 4

$7d'^2 = a'^2 + b'^2 + c'^2$

Continuo a dividere i numeri per 2

NO! per la discesa infinita

Si può fare anche senza stando attenti ai dati iniziali

---

(9) $f(0)=0$ $f(1)=0$ $f(2n)=2f(n)+1$

$f(2n+1)=2f(n)$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f(n)$	0	0	1	0	3	2	1	0	7	6	5	4	3	2	1	0

0	1	10	11	100	101	110	111
0	0	1	0	11	10	01	00

$f(\not{1}\,0\,1\,\_) = (\_\_1\_0\_)$

$f(2n) = f(1\ \underbrace{\text{stringa}}_{n \text{ in base } 2}\ 0) = 2(\text{stringa}) + 1$

$\text{stringa}\ 0 + 1$

ok

$\text{stringa}\ 1$

$f(2n+1) = f(1\ \underbrace{\text{stringa}}_{n \text{ in base } 2}\ 1) = 2(\text{stringa}) =$

$= \text{stringa}\ 0$

Fatto 1: Ad ogni passaggio perdo ALMENO una cifra binaria

Questo basta per (2)

$a_{2002} = f^{2002}(m) = \underbrace{f(f(f\ldots f(m)\ldots))}_{2002 \text{ volte}}$ NOTAZIONE

NON SEMPRE $\sin^2(x) = (\sin x)^2$

ATTENZIONE ALLE NOTAZIONI !!!

$f^{2002}(m) = 0$

$f^{2001}(m) \neq 0$ ha almeno 1 cifra binaria

$f^{2000}(m)$ ha almeno 2 cifre binarie

m ha almeno 2002 cifre binarie

$m = 101010\_\_\_\_\_10$ (2002 cifre)

$f(m) = 10101\_\_\_\_\_01$

$f^2(m) = 1010\_\_\_\_\_10$

$10 = 2 \quad 1010 = 2^3+2 \quad 101010 = 2^5+2^3+2$

$m = 2^{2001} + 2^{1999} + \_\_\_ + 2^3 + 2 =$

$= 2\left(\sum_{i=0}^{1000} 2^{2i}\right) = 2 \cdot \frac{4^{1001}-1}{3}$

SENIOR 2016 – N2 BASIC

Note Title 9/5/2016

INVERSO MOLTIPLICATIVO mod m

a mod m $\qquad ax \equiv 1 \ (m)$?

$x =$ "inverso di a mod m"

a ammette inversi mod $m \iff (a,m) = 1$;
inoltre, se $(a,m) = 1$ c'è esattamente un inverso definito mod m.

Es: $m = 9$

a	0	1	2	3	4	5	6	7	8
a^{-1}	×	1	5	×	7	2	×	4	8

$m-1 \equiv -1$

Oss $d = (a,m)$. (Se $d > 1$), allora $d \mid ax$ per ogni x

$\Rightarrow ax \not\equiv 1 \ (m)$

$4x \equiv 1 \ (9)$ $\qquad 4x = 1, 1+9=10, 1+9\cdot 2 = 19, 1+9\cdot 3 = 28$

$2x \equiv 1 \ (9)$ $\qquad 2x = 1$ NO, $2x = 1+9$ Sì $\rightarrow x = 5$

$(a,m) = 1 \implies$ c'è esattamente un inverso di a mod m

$ax \equiv 1 \ (m)$

$\iff ax = km + 1$

$\iff ax - km = 1$

Algoritmo di Euclide

ha soluzioni $\iff (a,m) = 1$

inoltre $\boxed{x = x_0 + t \cdot m}$ sono tutte le soluzioni

Es Calcolare le ultime 4 cifre in base 8 di

$$\frac{2^{2016}-1}{3}.$$

$$\frac{2^{2016}-1}{3} \equiv \frac{0-1}{3} \quad (8^4)$$

$$\left(2^{2016}-1\right)\cdot 3^{-1} \equiv -3^{-1} \quad (8^4)$$

$8^4 \not\equiv 1 \pmod 3$ $\qquad \left(\frac{2\cdot 8^4+1}{3}\right)$

Es Ultima cifra di $\frac{2^{2016}-1}{3}$ in base 3 ?

$$\frac{2^{2016}-1}{3} \not\equiv \frac{1-1}{3} \not\equiv \frac{0}{3} \pmod 3$$

Ridurre mod 9 il numeratore

$$\text{numeratore} \equiv 6 \ (9) \qquad \text{num} = 6+9k$$

$$\frac{\text{num}}{3} = 2+3k$$

2^{2016}

$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 8 \equiv -1 \ (9)$
$2^4 = 16 \equiv 7 \ (9)$
$2^5 \equiv 5 \ (9)$
$2^6 \equiv 1 \ (9)$
$2^7 \equiv 1\cdot 2 \equiv 2 \ (9)$

$2^3 \equiv 4$
$2^9 \equiv 8$
$\vdots$

$2^{2016} \equiv 2^0 \equiv 1 \ (9)$

$2^{2016} - 1 \equiv 0 \ (9)$

$\Rightarrow \quad \frac{2^{2016}-1}{3} \equiv 0 \ (3)$

Quando si può dividere a destra e a sinistra in una congruenza?

$\underbrace{8^{-1}}_{1} \cdot 8x \equiv \underbrace{24 \cdot 8^{-1}}_{3 \cdot 8 \cdot 8^{-1} \equiv 3} \ (31) \quad \overset{?}{\Rightarrow} \quad x \equiv 3 \ (31)$ Sì

$8x \equiv 24 \ (32) \quad \overset{?}{\Rightarrow} \quad x \equiv 3 \ (32)$ NO

$8 \quad 8 \quad (32,8)$

$8x = 24 + 32k$
$\Leftrightarrow \quad x = 3 + 4k$
$\Rightarrow \quad x \equiv 3 \ (4)$

$8x \equiv 24 \ (18)$
$8 \quad 8 \quad 2 = (8,18)$

$\Leftrightarrow \quad 8x = 24 + 18k$
$4x = 12 + 9k$
$4x \equiv 12 \ (9)$
$4 \quad 4$
$x \equiv 3 \ (9)$

TEOREMA CINESE DEL RESTO

$$\begin{cases} x \equiv 1 \ (3) \\ x \equiv 2 \ (4) \end{cases}$$

$x = 10$ va bene.
$x = 10 + 12k$ va bene
$x \equiv 10 \ (12)$

$$\begin{cases} x = 1 + 3k \\ x = 2 + 4h \end{cases}$$

$$1 + 3k = 2 + 4h$$

$$\Rightarrow \quad 3k - 4h = 1$$

ci sono soluzioni.

$$\begin{cases} k = k_0 + 4t \\ h = h_0 + 3t \end{cases}$$

$$\begin{cases} x = 1 + 3k = 1 + 3(k_0 + 4t) = (1 + 3k_0) + 12t \\ x = 2 + 4h = 2 + 4(h_0 + 3t) = (2 + 4h_0) + 12t \end{cases}$$

$$x \equiv (?) \ (12)$$

Teorema (*) $\begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \end{cases}$ con $(m_1, m_2) = 1$

Esiste b (unico mod $m_1 m_2$) tale che il sistema (*) è equivalente a $\boxed{x \equiv b \ (m_1 m_2)}$

$$\begin{cases} x \equiv 8 \ (9) \\ x \equiv 1 \ (16) \\ x \equiv -1 \ (6) \end{cases} \iff \begin{cases} x \equiv -1 \ (3) \\ x \equiv -1 \ (2) \end{cases}$$

$$x \equiv -1 \ (12) \iff \begin{cases} x \equiv -1 \ (2^2) \\ x \equiv -1 \ (3) \end{cases}$$

$$\begin{cases} x \equiv 8 \ (9) \\ x \equiv 1 \ (16) \end{cases} \iff \boxed{x \equiv 17 \ (9 \cdot 16)}$$

ATTENZIONE:

$x \equiv -1 \ (12) \iff \begin{cases} x \equiv -1 \ (2) \\ x \equiv -1 \ (3) \end{cases}$

- Scomporre ogni congruenza in potenze di primi
- Confrontare le congruenze relative agli stessi primi

Es: $\begin{cases} x \equiv 9 \ (27) \\ x \equiv 80 \ (81) \end{cases} \Rightarrow x \equiv 80 \ (27)$

- Ricostruire la soluzione modulo $\prod_i p_i^{\alpha_i}$

$17, 33, \ldots$

$\begin{cases} X \equiv ? \pmod{\text{mcm dei moduli}} \\ \text{non c'è soluzione} \end{cases}$

PERIODICITÀ DELLE POTENZE mod m

Es: potenze di 3 mod 20

$3^0 = 1$
$3^1 \equiv 3$
$3^2 \equiv 9$
$3^3 \equiv 7$
$3^4 \equiv 7 \cdot 3 \equiv 1$

3
9
7
⋮

$(3, 20) = 1$

Antiperiodo $= 0$, Periodo $= 4$.
$(a, m) = 1$

Es: potenze di 2 mod 20

$2^0 \equiv 1$
$2^1 \equiv 2$
$2^2 \equiv 4$
$2^3 \equiv 8$
$2^4 \equiv 16$
$2^5 \equiv 32 \equiv 12$
$2^6 \equiv 24 \equiv 4$

8
16
12
4
8
16
12
⋮

$(2, 20) > 1$

$2^k \bmod 20 \iff 2^k \bmod 4$ e $\bmod 5$

$(?, 5)$

$(a, m) = 1$; vogliamo studiare le potenze di $a \bmod m$.

Fatto 1 Non c'è antiperiodo

Ovvero la prima potenza "già vista" è un 1 mod m

$a^0, a^1, a^2, a^3, \dots, a^k, \dots, a^h$

$a^k \equiv a^h \pmod m$ $\quad h > k \geq 0$

$\Rightarrow 1 \equiv a^{h-k} \pmod m$

a^0

$k = 0$ era il vero "primo momento" di ripetizione.

La prima ripetizione è un 1.

Def ordine moltiplicativo di a mod m

$\text{ord}_m(a) =$ minimo $h>0$ tale che $a^h \equiv 1 \ (m)$

Ovvero: è il <u>periodo</u> delle potenze di a

Es: $\text{ord}_{20}(3) = 4$

Fatto 2 $a^k \equiv 1 \ (m) \iff \text{ord}_m(a) \mid k$.

PICCOLO TEOREMA DI FERMAT

$m = p$ primo

$a^p \equiv a \ (p)$ per ogni a

ovvero: $a^{p-1} \equiv 1 \ (p)$ per ogni a non multiplo di p.

Dim $S = \{1, 2, 3, \dots, p-1\}$ $\quad (p \nmid a)$

$\downarrow \cdot a$

$\{a, 2a, 3a, \dots, (p-1)a\} = S$

Esempio: $p = 7$, $a = 2$

$\{1, 2, 3, 4, 5, 6\}$

$\downarrow$

$\{2, 4, 6, 1, 3, 5\}$

$i, j \in \{1, \dots, p-1\} = S$

$i \neq j \Rightarrow ai \not\equiv aj \ (p)$

perché, se per assurdo $ai \equiv aj \ (p)$, allora dividendo per a trovo $i \equiv j \ (p)$

Prodotto degli elementi di S: $(p-1)!$ / $(p-1)! \cdot a^{p-1}$

$(p-1)! \equiv (p-1)! \cdot a^{p-1} \ (p)$

$\Rightarrow a^{p-1} \equiv 1 \ (p)$. $\square$

$a^{p-1} \equiv 1 \pmod p$ se $p \nmid a$.

$\rightarrow$ $\boxed{\operatorname{ord}_p(a) \mid p-1}$

Esempi $p = 11$

a^0	a^1	a^2	a^3	a^4	a^5
1	5	3	4	9	1
1	10	1			

- $a = 5$
- $a = 10 \equiv -1$
- $a = 2$
- $a = 1$

$\operatorname{ord}_{11}(5) = 5 \mid p-1 = 10$

$\operatorname{ord}_{11}(10) = 2$

$\operatorname{ord}_{11}(2) = 10$

$\operatorname{ord}_{11}(1) = 1$

Esempio Dimostrare che, se $p \mid x^2+x+1$, allora $p=3$ oppure $p \equiv 1 \pmod 3$.

$x^2+x+1 \equiv 0 \pmod p$

$\downarrow \cdot(x-1)$

$x^3-1 \equiv 0 \pmod p$

$x^3 \equiv 1 \pmod p \Rightarrow \boxed{\operatorname{ord}_p(x) \mid 3}$

$\operatorname{ord}_p(x) = 1 \Rightarrow x \equiv 1 \pmod p \Rightarrow 1+1+1 \equiv 0 \pmod p \Rightarrow p = 3$

$\operatorname{ord}_p(x) = 3$

$3 \mid p-1$

$\Rightarrow p \equiv 1 \pmod 3$.

Esercizio: Come possono essere fatti i fattori primi di x^2+1?

Es (N2-10) $n \mid 2^n+1 \Rightarrow 3 \mid n$ $(n \geq 1)$

$2^n \equiv -1 \ (n)$

Sia p un fattore primo che divide n.

$n = p \cdot m$

$n \mid 2^n+1 \Rightarrow p \mid 2^n+1$

$2^n \equiv -1 \ (p)$

$2^{pm} \equiv -1 \ (p)$ $\quad$ $2^{pm} \equiv (2^m)^p \equiv 2^m \ (p)$

$\mid 2^m \equiv -1 \ (p) \mid$

elevando al quadrato: $2^{2m} \equiv 1 \ (p)$

$\Rightarrow \cdot \ ord_p(2) \mid 2m$

ci ricordiamo che $\cdot \ ord_p(2) \mid p-1$

Prendiamo come p il più piccolo primo che divide n $(p \geq 3)$

$ord_p(2) \mid (2m, p-1) \mid 2$

$\Rightarrow ord_p(2) = \begin{cases} 1 \Rightarrow 2 \equiv 1 \ (p) \text{ assurdo} \\ 2 \Rightarrow 2^2 \equiv 1 \ (p) \end{cases}$

ovvero $3 \equiv 0 \ (p) \Rightarrow p = 3.$

TEOREMA DI EULERO

$(a, m) = 1 \Rightarrow \boxed{a^{\varphi(m)} \equiv 1 \ (m)}.$

$\varphi(m) =$ # elementi di $\{1, \dots, m\}$ coprimi con m.

Es: $m = p$ primo, $\varphi(p) = p-1$

$a^{p-1} \equiv 1 \ (p)$

Dim: è come quella del LFT.

$S = \{1, \dots, p-1\} \longrightarrow S = \{$ elementi coprimi con m tra 1 e $m\}$

$\downarrow \cdot a$

$\{a, 2a, \dots\}$

$|S| = \varphi(m)$

$\downarrow \cdot a$

S

$a^{\varphi(m)} \equiv 1 \pmod m$

$(a,m) = 1 \Rightarrow \boxed{\operatorname{ord}_m(a) \mid \varphi(m)}$

GENERATORI

$\operatorname{ord}_p(a) \mid p-1$

modulo p

Domanda: qualsiasi divisore di $p-1$ è l'ordine moltiplicativo di qualcosa?

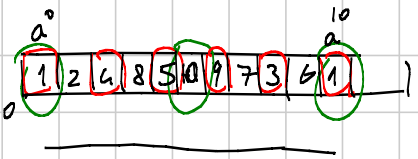
Se c'è un g tale che $\operatorname{ord}_p(g) = p-1$, allora $\forall\, d \mid p-1$

$g^{\frac{p-1}{d}}$ ha proprio ordine d.

$p = 11$

$a = 2$

$\operatorname{ord}_{11}(2) = 10$



$d = 5$

$g^{\frac{p-1}{d}} = 2^{\frac{10}{5}} = 2^2$

$d = 2$

$g^{\frac{p-1}{d}} = 2^{\frac{11-1}{2}} = 2^5$

Teorema Esiste sempre (mod p) almeno un elemento g di ordine $p-1$.

GENERATORE mod p.

g è un generatore $\iff \{g^0, g^1, g^2, \dots, g^{p-2}\} = \{1, 2, \dots, p-1\}$ mod p

Es Tutti i primi $\equiv 1 \pmod 3$ dividono qualche x^2+x+1.

$$p \mid x^2+x+1 \Rightarrow x^3 \equiv 1 \pmod p$$

$\operatorname{ord}_p(x) = 1 \to p=3$, $\operatorname{ord}_p(x) = 3 \to 3 \mid p-1$.

Vogliamo costruire x con $\operatorname{ord}_p(x)=3$.

Esiste!

$$x \equiv g^{\frac{p-1}{3}} \pmod p$$

$$x^2+x+1 \underset{\text{posso scriverlo se } x \neq 1 \pmod p}{\equiv} \frac{x^3-1}{x-1} \equiv \frac{g^{\frac{p-1}{3}\cdot 3}-1}{x-1} \equiv \frac{g^{p-1}-1}{x-1} \equiv 0 \pmod p$$

$$g^{\frac{p-1}{3}} \not\equiv 1 \pmod p$$

QUANTE SONO LE POTENZE k-ESIME mod p ?

$x^2 = y^5+4$

quadrati mod 11: 5 più lo 0

potenze quinte mod 11: 2 (± 1) più lo 0

Fatto generale: ci sono $\frac{p-1}{(k, p-1)}$ potenze k-esime mod p (più lo 0).

$\{1^k, 2^k, 3^k, \dots, (p-1)^k\}$ ← quanti elementi diversi ha?

$\| $

$\{(g^0)^k, (g^1)^k, (g^2)^k, \dots, (g^{p-2})^k\}$ per qualche generatore g

$= \{g^0, g^k, g^{2k}, g^{3k}, \dots, g^{(p-2)k}\}$

Sono le potenze di $g^k \mod p$.

Il numero di potenze k-esime è uguale a $\mathrm{ord}_p(g^k)$.

$\mathrm{ord}_p(g^k) \mid p-1$

$k = p-1 \longrightarrow \mathrm{ord}_p(g^k) = 1$

$k = \frac{p-1}{2} \longrightarrow = 2$

$d \mid p-1 \quad k = \frac{p-1}{d} \longrightarrow = d$

Se $k \mid p-1$, allora $\mathrm{ord}_p(g^k) = \frac{p-1}{k}$

$\Rightarrow$ ci sono $\frac{p-1}{k}$ potenze k-esime.

Idea: guardare $\{g^0, g^k, g^{2k}, \dots, g^{(p-2)k}\} \mod p$

è un po' come guardare $\{0, k, 2k, \dots, (p-2)k\} \mod p-1$.

$d = (k, p-1)$

$k = h \cdot d$

$\{0, hd, 2hd, 3hd, \dots, (p-2)hd\} \mod p-1$

$\Updownarrow$ divido per d

$\{0, h, 2h, 3h, \dots, (p-2)h\} \mod \frac{p-1}{d}$

$\left(h, \frac{p-1}{d}\right) = 1$

$\{0, h, 2h, \dots, \left(\frac{p-1}{d} - 1\right)h\}$

sono tutti diversi

$\frac{p-1}{d}$ elementi distinti $= \left|\frac{p-1}{(k, p-1)}\right|$

Esercizi "base": 46, 47, 51, 54, 60, 61, 66.
Esercizi dalla pagina N2: 4, 6, 9.
Esercizio extra: primi che dividono x^2+1.

(54) $3^y - x^2 = 41$ mod 8

se y pari: $z^2 - x^2 = 41$ $(z = 3^{y/2})$ | $y=0$ a parte

$3 + 0 \equiv 1$
$1 + 4$

$3 + 0 \equiv 3$
$3 + 4 \equiv 7$
$1 + 0 \equiv 1$
$1 + 4 \equiv 5$

$\Rightarrow$ y pari
x è multiplo di 4.

(60) $A = 5^n + 3^n + 1$ primo $\overset{?}{\Rightarrow}$ $12 \mid n$? $(n \geq 1)$

- n pari ?

$n=1$ $A=9$
$n=3$ $A=\dots$

mod 3: $A \equiv (-1)^n + 1 \equiv 0$ (3)
(n dispari)

- $4 \mid n$?

$n \equiv 2$ (4)
$n=2 \rightarrow A = 25 + 1 + 1 = 35$

mod 5: $A \equiv 3^n + 1 \equiv 4 + 1 \equiv 0$ (5)

3, (4), 2, 1, ...

- $3 \mid n$?

mod 7 $7-1=6$ è multiplo di 3

n	0	1	2	3	4	5
5^n	1	5	4	−1	2	3
3^n	1	3	2	−1	4	5

(1)

1

3 2 0 -1 0 2 | 3

non va bene $n \equiv 2, 4 \ (6)$

$\Rightarrow \boxed{n \equiv 0 \ (6)}$

mod 9

ord | φ(m)

φ(9) = 6 ...

(66) $x^3 \equiv 2a \mod 14$ $\quad 0 \le a \le 100$

Per quali a esiste una soluzione?

$\begin{cases} x^3 \equiv 2a \ (2) \iff x \equiv 0 \ (2) \\ x^3 \equiv 2a \ (7) \end{cases}$

↳ per avere soluzioni, serve che 2a sia un cubo perfetto mod 7.

Quanti sono i cubi mod 7?

$\frac{7-1}{3} = 2$ $\quad 0, 1, -1$

$2a \equiv \begin{cases} 0 \\ 1 \\ -1 \end{cases} \ (7)$

$\longrightarrow$ $a \equiv \begin{cases} 0 \\ 4 \\ 3 \end{cases} \ (7)$

(4) $5^{5^{5^5}} \mod 10^5$

$\begin{cases} \mod 5^5 \longrightarrow \equiv 0 \\ \mod 2^5 \end{cases}$

$5^{5^{5^5}} \mod 2^5$ (*)

riduco l'esponente mod $\varphi(2^5) = 2^4$

$5^{5^5} \mod 2^4$ (*)

riduco l'esponente mod $\varphi(2^4) = 2^3$

$5^{5^5} \bmod 8 \equiv 5 \ (8)$

(*) $5^{5^{5^5}} \bmod 2^4 \equiv 5^5 \bmod 2^4 \equiv 5 \bmod 2^4$

$5, 9, -3, -15 \equiv 1$

(*) $5^{5^{5^{5^5}}} \bmod 2^5 \equiv 5^5 \bmod 2^5 \equiv 21 \bmod 32$

$$\begin{cases} x \equiv 0 \ (5^5) \\ x \equiv 21 \ (2^5) \end{cases}$$

$x = 5^5 k$ $\qquad$ $\cancel{5^5 k \equiv 21 \ (2^5)}$ ($5^5 \equiv 1 \equiv 21$)

$k \equiv 1 \ (2^5)$

$x \equiv 5^5 \cdot 1 = 3125 \ (10^5)$

$\boxed{03125}$

(6) $2^n \equiv 18 \ (385)$

$$\begin{cases} 2^n \equiv 18 \equiv 3 \ (5) \\ 2^n \equiv 18 \equiv 4 \ (7) \\ 2^n \equiv 18 \equiv 7 \ (11) \end{cases} \longrightarrow \begin{cases} n \equiv 3 \ (4) \\ n \equiv 2 \ (3) \\ n \equiv 7 \ (10) \end{cases}$$

$n \equiv \boxed{7} \ (20)$

$$\begin{cases} n \equiv 7 \ (20) \\ n \equiv 2 \ (3) \end{cases}$$

$7, \ 7+20, \ 7+20 \cdot 2$

$n \equiv 7 + 20 \cdot 2 \equiv 47 \ (60)$.

⑨ d, m, n

$$\begin{cases} a & \equiv 0 \pmod{p_1^n} \\ a+d & \equiv 0 \pmod{p_2^n} \\ a+2d & \equiv 0 \pmod{p_3^n} \\ a+3d & \vdots \\ \vdots & \\ a+(m-1)d & \equiv 0 \pmod{p_m^n} \end{cases}$$

$p_1, p_2, \dots, p_m$ primi distinti

$\Rightarrow \exists$ soluzioni!

EXTRA x^2+1 ← fattori primi?

$p \mid x^2+1 \Rightarrow p = 2$ oppure $p \equiv 1 \pmod 4$

$x^2 \equiv -1 \pmod p$

$x^4 \equiv 1 \pmod p$

$\Rightarrow \operatorname{ord}_p(x) \mid 4$

$\operatorname{ord}_p(x) = 1 \longrightarrow x \equiv 1 \pmod p \Rightarrow x^2+1 \equiv 2$, $2 \equiv 0 \pmod p \Rightarrow p = 2$

$= 2 \longrightarrow x^2 \equiv 1 \pmod p \Rightarrow x^2+1 \equiv 2 \equiv 0 \Rightarrow p = 2$

$= 4$

$4 \mid p-1$ ovvero $p \equiv 1 \pmod 4$.

$\operatorname{ord}_p(x) = 4$

$x = g^{\frac{p-1}{4}}$ per qualche generatore g.

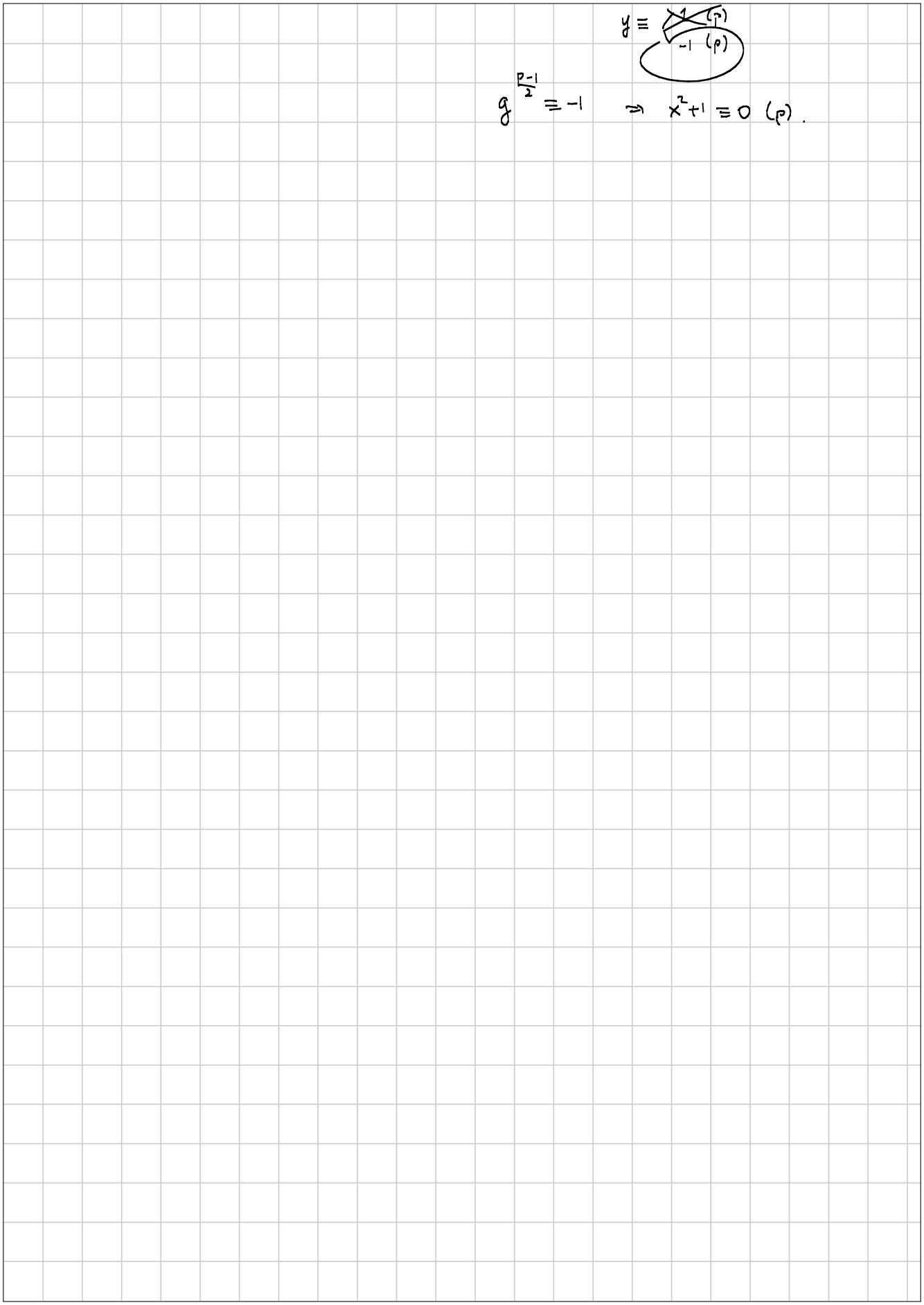
$x^2 + 1 \equiv g^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$

$g^{\frac{p-1}{2}} \equiv -1$ ($g^{\frac{p-1}{2}} = y$)

$y^2 \equiv g^{\frac{p-1}{2} \cdot 2} = g^{p-1} \equiv 1 \pmod p$

$y^2 \equiv 1 \pmod p$

$p \mid y^2 - 1 = (y+1)(y-1)$


$y \equiv$
(p)
-1
(p)
$g^{\frac{p-1}{2}} \equiv -1 \quad \Rightarrow \quad x^2+1 \equiv 0 \ (p)$.