Stage Senior 2015 – Livello Basic

Stampato integrale delle lezioni

Autori vari

Indice

Algebra 1 - Senior 2015 - Gioacchino

Titolo nota 23/08/2015

Polinomi

Che cos'è un polinomio?

$$P(x) = \underbrace{a_n}_{\text{coefficiente}} \underbrace{x^{n}}_{\text{parte letterale}} + a_{n-1}x^{n-1} + \dots + a_0$$

~~Quest~~. Cos'è il grado di un polinomio? Il max exp a cui compare elevata la x

- Coeff. direttivo: a_n
- Polinomio monico: $a_n = 1$

Grado di un pol. costante $\neq 0$ è 0!

Dove sono i coefficienti?

- $\mathbb{R} \to$ reali
- $\mathbb{Z} \to$ interi $\qquad \mathbb{Z} \subseteq \mathbb{Q}$
- $\mathbb{Q} \to$ razionali
- $\mathbb{C} \to$ complessi

$\mathbb{Z}/\mathbb{Q}$

DIVISIONE EUCLIDEA $\quad a > 0,\ b > 0$

Per i numeri $\longrightarrow \exists!\ q, r$ t.c. $a = qb + r$ con $0 \leq r < b$

Per i polinomi $\longrightarrow$ Dati $a(x)$ e $b(x)$

$\exists!\ r(x), q(x)$ t.c. $a(x) = b(x)q(x) + r(x)$

e $0 \leq \deg r(x) < \deg b(x)$ $\vee$ $r(x) = 0$

Dim: x Induzione ... formalizzata usando l'algoritmo.

sul deg del dividendo.

$$
\begin{array}{l|l}
x^4 \qquad\qquad +3x+1 & x^2+x+1 \\
\hline
-x^4-x^3-x^2 & x^2-x \\
\hline
\quad -x^3-x^2+3x+1 & \\
\quad +x^3+x^2+x & \\
\hline
\qquad\qquad 4x+1 &
\end{array}
$$

$$x^4+3x+1=(x^2+x+1)(x^2-x)+4x+1$$

Attenzione! Se i coeff. di $a(x)$ e $b(x)$ sono in $\mathbb{Q}$, anche quelli di $q(x)$ e $r(x)$ lo sono?
(Stessa cosa per $\mathbb{R}$, $\mathbb{C}$)
Se i coeff. di $a(x)$ e $b(x)$ sono in $\mathbb{Z}$, anche quelli di $q(x)$ e $r(x)$ sono in $\mathbb{Z}$?
NON È DETTO! (Sono, a priori, in $\mathbb{Q}$).
Sono in $\mathbb{Z}$ se $b(x)$ è monico.

$$
\begin{array}{l|l}
3x^2+1 & 2x+1 \\
\hline
-3x^2-\frac{3}{2}x & \frac{3}{2}x-\frac{3}{4} \\
\hline
\quad -\frac{3}{2}x+1 & \\
\quad +\frac{3}{2}x+\frac{3}{4} & \\
\hline
\qquad +\frac{7}{4} &
\end{array}
$$

Massimo comune divisore

per i numeri

- Dati a, b $a>0$ $b>0$ si dice $MCD(a,b)=d$ ie numero $d>0$ t.c. $d|a \wedge d|b$ e se $\exists$ c t.c. $c|a$ e $c|b \to c|d$
- Th. Bézout. Dati $a,b>0$ $\exists$ r,s t.c. $ar+bs=d=MCD(a,b)$

Per i polinomi

Dati $a(x), b(x)$ si dice $MCD(a(x),b(x))=d(x)$ ie polinomio monico t.c. $d(x)|a(x) \wedge d(x)|b(x)$ e se $\exists$ $c(x)$ t.c. $c(x)|a(x)$ e $c(x)|b(x) \to c(x)|d(x)$

- Dati $a(x), b(x)$ $\exists$ $r(x), s(x)$ t.c. $a(x)r(x)+b(x)s(x)=d(x)$

Conseguenza della divisione

Def. α radice di $P(x) \iff P(\alpha)=0$

Ruffini **Th.** $P(\alpha)$ è il resto della divisione di $P(x)$ per $(x-\alpha)$

Dim. Per il th. di divisione $\exists\ q(x), r(x)$ t.c.

$$P(x) = (x-\alpha)\,q(x) + r(x)$$

costante / zero

Perché $\circ\ r(x)=0$ $\circ\ 0 \le \deg r(x) < \deg(x-\alpha)$

$r(x)$ è una costante che chiamo r

$$P(x) = (x-\alpha)\,q(x) + r$$

valuto in α

$$P(\alpha) = r$$

C.1. Se α è una radice $\xrightarrow{\text{Per def.}} P(\alpha)=0 \xrightarrow{\text{RUFFINI}}$ il resto della divisione di $P(x)$ per $x-\alpha$ è $0 \longrightarrow$

$\longrightarrow P(x) = (x-\alpha)\,Q(x)$ senza resto.

Quindi se $P(\alpha)=0 \longrightarrow P(x) = (x-\alpha)\,Q(x)$

Oss. Ho un polinomio di grado n di cui conosco $\alpha_1,\dots,\alpha_n$ radici distinte. Com'è fatto?

$$P(\alpha_1)=0 \longrightarrow P(x) = (x-\alpha_1)\,Q(x)$$

$$P(\alpha_2) = (\alpha_2-\alpha_1)\,Q(\alpha_2)$$

$$\overset{\shortparallel}{0} \implies Q(\alpha_2)=0 \longrightarrow Q(x) = (x-\alpha_2)\,R(x)$$

E così via...

Quindi è fatto così $P(x) = c(x-\alpha_1)\dots(x-\alpha_n)$

Oss. $P(x)$ a coeff. interi a, b due interi.

Considero il polinomio $Q(x) = P(x) - P(b)$

Quanto vale $Q(b)$? $Q(b) = P(b) - P(b) = 0$

$$Q(x) = (x-b)\,R(x)$$

$$P(x) - P(b) = (x-b)\,R(x)$$

$$P(a) - P(b) = (a-b)\,R(a)$$

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

x^2+1 $\quad 3 \to 10$ $\quad 7 \to 50$ $\qquad 7-3 \mid 50-10$ ✓

Th. Un polinomio di grado n non può avere più di n radici

Per induzione su n — P.B. $n=1$ ok.

Dim. Suppongo che sia vera fino a n

n+1 P.a. suppongo che abbia $+$ $(n+1)$ radici.

Ne scelgo una α_1

$P(x) = (x-\alpha_1)\,Q(x)$ → ha grado n x hp induttiva ha al più n radici

Quindi $P(x)$ ha al più $(n+1)$ radici

IDENTITÀ POLINOMI → $P(x)$ e $Q(x)$

Se due polinomi di grado n coincidono su $n+1$ valori, allora sono identici.

Perché $R(x) = P(x) - Q(x)$ → ha al max grado n. Quindi ha al max n radici.

Ma $R(\alpha_1) = \ldots = R(\alpha_{n+1}) = 0$

Quindi deve essere il caso che $P(x) - Q(x) = 0$.

$P(x) = Q(x)$.

Domanda Se conosco la valutazione in $x_1, \ldots, x_{n+1}$ di $P(x)$ di grado n

$P(x_1) = y_1$

$\vdots$

$P(x_{n+1}) = y_{n+1}$

Riesco a scrivere $P(x) = ?$

Sì: INTERPOLAZIONE DI LAGRANGE

Idea: Cerchiamo un polinomio che valga 1 su x_1 e 0 su $x_2, \ldots, x_{n+1}$

$$a_1(x) = \frac{(x-x_2)\cdot\ldots\cdot(x-x_{n+1})}{(x_1-x_2)\cdot\ldots\cdot(x_1-x_{n+1})}$$

$$a_2(x) = \frac{(x-x_1)(x-x_3)\cdot\ldots\cdot(x-x_{n+1})}{(x_2-x_1)\cdot(x_2-x_3)\cdot\ldots\cdot(x_2-x_{n+1})}$$

$\vdots$

$a_{n+1}(x) = \ldots$

Dico che $p(x) = y_1 a_1(x) + \ldots + y_{n+1} a_{n+1}(x)$

$$p(x_1) = y_1 + 0 = y_1$$
$$p(x_2) = y_2$$
$$\vdots$$
$$p(x) = \sum_{j=1}^{n+1} \left(y_j \prod_{i \neq j} \frac{(x - x_i)}{(x_j - x_i)} \right) \qquad i = 1, \dots, n+1 \quad i \neq j$$

Es.

$(1,2)$ $\quad p(1) = 2$

$(3,4)$ $\quad p(3) = 4$

$(5,6)$ $\quad p(5) = 6$

A voi

α_1 è radice $\quad p(x) = (x-\alpha_1)\, q(x) \qquad$ UFD

$$p(x) = \dots (x-\alpha_1)^k \dots$$

$k \overset{\text{def}}{:=}$ molteplicità di α_1

Si può definire la derivata formale di un polinomio

$$p(x) = \sum_{i=0}^{m} a_i \cdot x^i$$
$$p'(x) \underset{\text{def}}{:=} \sum_{i=0}^{m} i\, a_i\, x^{i-1}$$

$$\left(a(x)\, b(x) \right)' = a'(x)\, b(x) + a(x)\, b'(x)$$

Se α ha molt. k

$p(x) = (x-\alpha)^k q(x) \qquad q(\alpha) \neq 0$

$p(\alpha) = 0 \qquad p'(\alpha) = k(x-\alpha)^{k-1} q(x) + (x-\alpha)^k q'(x)$

$p'(\alpha) = 0 \qquad \vdots$

$\vdots$

$p^{(k-1)}(\alpha) = 0 \qquad p^{(k)}(x) = k!\, q(x) + (x-\alpha) \cdot \text{ROBA}$

$p^{(k)}(\alpha) \neq 0$

Come sono fatte le radici razionali di un polinomio a coeff. interi?

$$p(x) = a_n x^n + \dots + a_1 x + a_0 \qquad a_i \in \mathbb{Z}$$

Suppongo che $x = \frac{p}{q}$ sia radice $(p,q)=1$

$$a_n \frac{p^n}{q^n} + \dots + a_1 \frac{p}{q} + a_0 = 0$$

$$\underbrace{a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1}}_{\text{multiplo di } p} + a_0 q^n = 0$$

$$a_n p^n + \underbrace{a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n}_{\text{multiplo di } q} = 0$$

$-a_0 q^n =$ multiplo di p

$p \mid a_0 q^n$

$p \mid a_0$

$a_n p^n =$ multiplo di q

$q \mid a_n p^n$

$q \mid a_n$

Conclusione: Possono solo essere $\dfrac{\text{divisori } a_0}{\text{divisori } a_n}$ (con segno)

Conseguenza: Se $a_n = 1$

Un polinomio monico a coeff. interi se ha una radice razionale, questa non può altro che essere intera

($\mathbb{Z}$ è INTEGRALMENTE CHIUSO)

Esercizietto $\exists$ $p(x)$ a coeff. interi a, b, c distinti interi

t.c.

$p(a) = b \quad p(b) = c \quad p(c) = a$

Teorema fondamentale dell'algebra

Qualsiasi polinomio a coeff. $\mathbb{C}$ si fattorizza (in modo unico) in prodotto di fattori lineari su $\mathbb{C}$.

$$p(x) = c\prod_{i=1}^{m}(x-\alpha_i)$$

$p \downarrow$ grado m

α_i sono a priori complessi.

α_i potrebbero essere anche uguali

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

$$x^n-1$$

Le soluzioni si chiamano radici n-esime dell'unità

$$\omega = \cos\left(\frac{2\pi}{m}\right) + i\sin\left(\frac{2\pi}{m}\right) = e^{i\frac{2\pi}{m}}$$

È una radice?

$$\left(e^{i\frac{2\pi}{m}}\right)^m - 1 = \underbrace{e^{i2\pi}}_{\cos 2\pi + i\sin 2\pi \,=\, 1 + 0 \,=\, 1} - 1 = 0$$

Le altre sono $\omega^2, \dots, \omega^{n-1} + \omega + 1 \to$ sono m

$$\omega^2 = e^{i\frac{2\pi}{m}\cdot 2} = \cos\left(\frac{2\pi}{m}\cdot 2\right) + i\sin\left(\frac{2\pi}{m}\cdot 2\right)$$

In generale sono $\omega^k = e^{i\frac{2\pi}{m}\cdot k} = \cos\left(\frac{2\pi}{m}\cdot k\right) + i\sin\left(\frac{2\pi}{m}\cdot k\right)$

$$x^n - 1 \underset{\text{in } \mathbb{C}}{=} \prod_{i=0}^{n-1}(x-\omega^i) \qquad \omega = e^{i\frac{2\pi}{m}}$$

Def. radice primitiva dell'unità (di ordine d) è un numero t.c. $x^d = 1$
$x^i \neq 1 \quad \forall\, i = 1, \dots, d-1$

Considero $x^n - 1 = 0$ radici n-esime dell'unità
Prendo z una di queste radici.
Essendo $z^n = 1$, $\exists$ il minimo d t.c. $z^d = 1$, ovvero l'ordine di questa radice.
Che relazione c'è fra d e n?
$d \mid n$.

Se n non è multiplo di d, $n = ad + r \quad 0 < r < d$

$$\begin{cases} z^n = z^{ad+r} = 1 \\ z^d = 1 \end{cases} \Rightarrow z^r = 1$$

Ma no! Perché d era il più piccolo

Oss. Radici n-esime dell'unità

$$\underbrace{1}_{1} \quad \underbrace{\quad}_{a_1} \quad \underbrace{\quad}_{a_2} \quad \dots \quad \underbrace{\quad}_{n}$$

ordine

$\phi(a_1) \quad \phi(a_2) \quad \dots \quad \phi(n)$

$a_1 \mid n$
$a_2 \mid n$

$\phi(n) :=$ # di numeri coprimi con n, + piccoli di n

$\phi(5) = 4 \qquad 1\,2\,3\,4$

$(x-1)(x-\omega)\dots(x-\omega^{n-1})$
$\uparrow \qquad \uparrow$
$1 \qquad n$

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

$$\Phi_d(x) = \prod_{\substack{\alpha_i \\ \text{rad. primitiva} \\ \text{di ordine } d}} (x - \alpha_i) = \text{Polinomio ciclotomico di ordine } d$$

→ I polinomi ciclotomici hanno coeff. interi (X Induzione...)
Esercizio
→ sono irriducibili su $\mathbb{Q}$

$$x^3-1 = \underbrace{(x-1)}_{\text{la radice di ordine 1}}\underbrace{(x^2+x+1)}_{(x-\omega)(x-\omega^2) = \Phi_3(x)}$$

$$x^2-1 = \underbrace{(x-1)}_{\text{la rad. di ordine 1}}\underbrace{(x+1)}_{\text{la rad. di ordine -1}}$$

$\Phi_2(x)$

$$x^4-1 = (x-1)(x+1)\underbrace{(x^2+1)}_{\Phi_4(x)}$$

$$x^5-1 = (x-1)\underbrace{(x^4+x^3+x^2+x+1)}_{\Phi_5(x)}$$

$$x^6-1 = \underbrace{(x-1)}_{\text{di ordine }1}\underbrace{(x^2+x+1)}_{\text{di ordine }3}\underbrace{(x+1)}_{\text{di ordine }2}\underbrace{(x^2-x+1)}_{\text{di ordine }6} \longrightarrow \Phi_6(x)$$

$$x^7-1 = (x-1)\underbrace{(x^6+x^5+\dots+1)}_{\Phi_7(x)}$$

$$x^8-1 = (x-1)(x+1)(x^2+1)\underbrace{(x^4+1)}_{\text{di ordine }8} \quad \Phi_8(x)$$

$$x^9-1 = \underbrace{(x-1)}_{1}\underbrace{(x^2+x+1)}_{3}\underbrace{(x^6+x^3+1)}_{9} \longrightarrow \Phi_9(x)$$

Ho una radice primitiva 3ª dell'unità.

$$\Phi_3(x) = x^2+x+1 \longrightarrow \omega^2+\omega+1=0$$

Fattorizzazioni in $\mathbb{R}$

Coniugio $\quad z = a + bi$

$\bar{z} = a - bi$

Mostra $\quad \overline{z+w} = \bar{z} + \bar{w}$

$\overline{zw} = \bar{z}\,\bar{w}$

$z = a+bi \qquad \{zw\} = (ac-bd) + (ad+bc)i$

$w = c+di \qquad \overline{zw} = (ac-bd) - (ad+bc)i$

$\bar{z} = a-bi \qquad \bar{z}\,\bar{w} = (a-bi)(c-di) =$

$\bar{w} = c-di \qquad = ac - adi - bci - bd =$

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

$$\boxed{(\bar{z})^n = \overline{(z^n)}} \qquad \overline{\mathbb{R}} = \mathbb{R} \qquad \overline{i\mathbb{R}} = -i\mathbb{R}$$

1° fatto $\quad$ Un polinomio a coeff. reali se ha una radice complessa ha anche la sua coniugata come radice

$$a_n x^n + \ldots + a_0 \qquad a_i \in \mathbb{R}$$

$$a_n z^n + \ldots + a_1 z + a_0 = 0 \qquad z \in \mathbb{C}$$

$$\overline{a_n z^n + \ldots + a_1 z + a_0} = \overline{0}$$

$$\overline{a_n z^n} + \ldots + \overline{a_1 z} + \overline{a_0} = 0$$

$$\overline{a_n}\,\overline{z^n} + \ldots + \overline{a_1}\,\bar{z} + \overline{a_0} = 0$$

$$a_n (\bar{z})^n + \ldots + a_1 \bar{z} + a_0 = 0$$

$$\Downarrow$$

$\bar{z}$ è una radice

$$p(x) = (x-\alpha_1)\cdot\ldots\cdot(x-\alpha_j)\cdot\underbrace{(x-z_1)\cdot(x-\bar{z}_1)}_{\downarrow}\cdot\ldots$$

$$(x^2 - \bar{z}_1 x - z_1 x + z_1\bar{z}_1)$$

$$\underline{(x^2 - (\bar{z}_1 + z_1)x + z_1\bar{z}_1)} \in \mathbb{R}[x]$$

$z_1 = a + bi$ $\qquad z_1 + \overline{z_1} = 2a = 2\,\mathrm{Re}(z_1)$

$\overline{z_1} = a - bi$ $\qquad z_1\overline{z_1} = (a+bi)(a-bi) = a^2+b^2 = |z|^2$

<u>Corollario</u> Ogni polinomio su $\mathbb{R}$ si fattorizza come fattori lineari + fattori quadratici

Esercizi
$(64, 65, 69, 70, 74, 75)^{+3}$ pag. 13
11 pag 23

- Per quali n $\quad x^2 + x + 1 \mid x^{2n} + x^n + 1$

- $\begin{cases} x+y+z = a \\ x^2+y^2+z^2 = b^2 \\ x^3+y^3+z^3 = a^3 \end{cases}$ Fissati a, b

68 - 72 - 73 - 77 - 78 + sistema + 11 / + $p(a)$, $p(b)$, $p(c)$ + $x^{2n}+x^n+1$

$a - b \mid b - c$

$a - b \mid a - c$

$a - c \mid b - a$

Su $\mathbb{Q}$

$$1 + x + \dots + x^{1023} \overset{\text{PARZ}}{=} (x+1)(1 + x^2 + \dots + x^{1022}) = \dots$$

Trucco : $$\frac{\boxed{x^{1024} - 1}}{x-1} = \frac{(x^{512}-1)(x^{512}+1)}{x-1} = \frac{\cancel{(x-1)}(x+1)(x^2+1)\dots(x^{512}+1)}{\cancel{x-1}}$$

$$= (x+1)\underbrace{(x^2+1)}_{\Phi_4(x)}\cdots\underbrace{(x^{512}+1)}_{\Phi_{1024}(x)}$$

72

$p(2) = a$

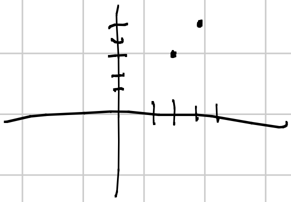
$p(a) = a + 2$

Determinare i poss. valori di a.

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

$a - 2 = \begin{matrix} +1 \\ -1 \\ +2 \\ -2 \end{matrix} \longrightarrow a = \begin{matrix} +3 \\ +1 \\ +4 \\ 0 \end{matrix}$

- $p(2) = 3$, $p(3) = 5$, $p(x) = 2x - 1$ ✓



- $p(2) = 1$, $p(1) = 3$, $p(x) = -2x + 5$ ✓
- $p(2) = 4$, $p(4) = 6$, $p(x) = x + 2$ ✓
- $p(2) = 0$, $p(0) = 2$, $p(x) = -x + 2$ ✓

Sia α radice di $x^3 - x + 1$

$\boxed{\alpha^3 - \alpha + 1 = 0} \xrightarrow{\text{ISOLO}} \alpha = \alpha^3 + 1 \longrightarrow \alpha^3 = (\alpha^3 + 1)^3 =$

$= \alpha^9 + 3\alpha^6 + 3\alpha^3 + 1$

$\downarrow$

$\alpha^9 + 3\alpha^6 + 2\alpha^3 = -1$

Quanto vale $\alpha^9 + 3\alpha^6 + 2\alpha^3$?

$\alpha^3 = \alpha - 1$

$\alpha^9 = (\alpha^3)^3 = (\alpha - 1)^3 = \alpha^3 - 3\alpha^2 + 3\alpha - 1 =$

$= \alpha - 1 - 3\alpha^2 + 3\alpha - 1 =$

$= -3\alpha^2 + 4\alpha - 2$

$\alpha^6 = (\alpha^3)^2 = (\alpha - 1)^2 = \alpha^2 - 2\alpha + 1$

$\alpha^3 = \alpha - 1$

Le sommo $-3\alpha^2 + 4\alpha - 2 + 3(\alpha^2 - 2\alpha + 1) + 2(\alpha - 1)$

$\cancel{-3\alpha^2} + \cancel{4\alpha} - 2 + \cancel{3\alpha^2} - \cancel{6\alpha} + 3 + \cancel{2\alpha} - 2 = -1$

$\alpha^3 = \alpha - 1$

Quanto vale $\alpha^{17} - 16\alpha^{14} + \alpha^5$

$\alpha^{17} = \alpha^2 \cdot (\alpha^3)^5 = \dots$

77. (S-G)

$$x^4 + 4y^4 = \overbrace{x^4 + 4x^2y^2 + 4y^4} - 4x^2y^2 =$$
$$= (x^2 + 2y^2)^2 - (2xy)^2 =$$
$$= (x^2 + 2xy + 2y^2)(x^2 - 2xy + 2y^2)$$

78 $(a^2+b^2)(c^2+d^2) =$
$$= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 + 2abcd - 2abcd =$$
$$= (ac+bd)^2 + (ad-bc)^2$$

$z = a + bi \qquad |z| = \sqrt{a^2+b^2}$

$w = c + di \qquad |w| = \sqrt{c^2+d^2}$

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

$$|zw| = \sqrt{(ac-bd)^2 + (ad+bc)^2}$$
$$\shortparallel$$
$$|z||w|$$
$$\shortparallel$$
$$\sqrt{a^2+b^2}\sqrt{c^2+d^2}$$

11. $P(z)$ ha grado 2002 $\underbrace{\alpha_i}_{\text{radici}} \neq \alpha_j \quad \forall i, j$

$\exists\, a_1, \dots, a_{2002}$ t.c.

se $P_1(z) = z - a_1$

$P_{n+1}(z) = P_n(z)^2 - a_{n+1}$

allora $P(z) \mid P_{2002}(z)$

Sol. Ho bisogno che $P_{2002}(\alpha_i) = 0 \quad \forall i = 1, \dots, 2002$

Supponiamo $P_{n-1}(\alpha_1) = \ldots = P_{n-1}(\alpha_{n-1}) = 0$

Posso scegliere a_n in modo che

$\underbrace{P_n(\alpha_1) = \ldots = P_n(\alpha_n)}= 0$?

$P_n(z) = P_{n-1}(z)^2 - a_n$

Per avere, ad es., $P_n(\alpha_1) = 0$

$\cancel{P_n(\alpha_1)} = \cancel{P_{n-1}(\alpha_1)}^2 - a_n \longrightarrow a_n = 0$

$P_n(\alpha_n) = \underbrace{P_{n-1}(\alpha_n)^2}$

Passo base Scelgo a_1 in modo che

$P_1(\alpha_1) = -P_1(\alpha_2)$

$\alpha_1 - a_1 = -(\alpha_2 - a_1)$

$\alpha_1 - a_1 = a_1 - \alpha_2$

$$\boxed{\frac{\alpha_1+\alpha_2}{2} = a_1}$$

$P_1(\alpha_1) = \alpha_1 - a_1 = \alpha_1 - \frac{\alpha_1+\alpha_2}{2} = \frac{2\alpha_1 - \alpha_1 - \alpha_2}{2} = \frac{\alpha_1 - \alpha_2}{2}$

$P_1(\alpha_2) = \alpha_2 - a_1 = \alpha_2 - \frac{\alpha_1+\alpha_2}{2} = \frac{\alpha_2 - \alpha_1}{2}$

Domanda $P_2(z) = P_1(z)^2 - a_2$

$P_2(\alpha_1) \overset{?}{=} P_2(\alpha_2)$

Quindi

$P_2(\alpha_1) = P_2(\alpha_2)$

Scelgo a_2 in modo che

$\rightarrow$ $P_2(\alpha_1) = -P_2(\alpha_3)$

$\shortparallel$

$(P_2(\alpha_2))$

$P_1(\alpha_1)^2 - a_2 = -(P_1(\alpha_3)^2 - a_2)$

$P_1(\alpha_1)^2 - a_2 = a_2 - P_1(\alpha_3)^2$

$$a_2 = \frac{P_1(\alpha_1)^2 + P_1(\alpha_3)^2}{2}$$

$$\begin{array}{lllllll} & \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{2001} & \alpha_{2002} \\ P_2 & k & k & -k & & & \\ P_3 & h & h & h & -h & & \\ \end{array}$$

$$\overset{\shortparallel}{P_2^2} - \underline{a_3}$$

$$\begin{array}{lllllll} P_{2001} & w & w & \cdots & w & -w \end{array}$$

$$P_{2002}(z) = P_{2001}^2(z) - a_{2002}$$

Scelgo $a_{2002} = w^2$, quindi

$$P_{2002}(\alpha_i) = \underset{\substack{\shortparallel \\ w^2}}{P_{2001}^2(\alpha_i)} - w^2 \leq 0 \quad \forall i = 1, \ldots, 2002$$

Idea: $\underbrace{x^2+y^2+z^2}$

(x,y,z)
(x,z,y)
(y,z,x)
(y,x,z)
(z,x,y)
(z,y,x)

Ogni espressione simmetrica si scrive come funzione delle simmetriche elementari

$s = x+y+z$
$q = xy+yz+xz$
$p = xyz$

$$x^2+y^2+z^2 = (x+y+z)^2 - 2(xy+yz+zx) = s^2 - 2q$$

$$x^3+y^3+z^3 =$$

$$x^3+y^3+z^3 - 3xyz = (x+y+z)(\underset{\sim\sim\sim}{x^2+y^2+z^2} - xy - yz - xz) = s(s^2 - 3q)$$

$$x^3+y^3+z^3 = s^3 - 3sq + 3p$$

Es. $x^2y + xy^2 + xz^2 + x^2z + yz^2 + y^2z$

$\vdots$

Algebra 2

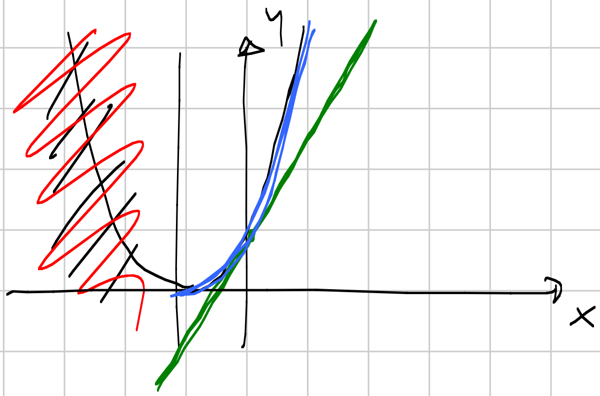
ma_go

Titolo nota 24/08/2015

(0) Bernoulli: $\boxed{x \geq -1}$ reale, $n \in \mathbb{N}$ intero ≥ 0

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

es $2^n \geq 1+n \quad \forall n \ldots$



(1) Riarrangiamento

$a_1, a_2, \ldots, a_n$
$b_1, \ldots, b_n$) reali.

$a_1 \cdot b_1 + a_2 \cdot b_2 + \ldots + a_n \cdot b_n$
$a_1 \cdot b_2 + a_2 \cdot b_1 + \ldots + a_n \cdot b_1$

σ perm. di $\{1, \ldots, n\}$

$a_1 \cdot b_{\sigma(1)} + a_2 \cdot b_{\sigma(2)} + \ldots + a_n \cdot b_{\sigma(n)}$

tra queste qual è la più grande?
quale la più piccola?

$a_1 = 1$, $a_2 = 2$
$b_1 = 3$, $b_2 = 4$ $\longrightarrow$ $1 \cdot 3 + 2 \cdot 4 = 11$

$\vee$

$\longrightarrow$ $1 \cdot 4 + 2 \cdot 3 = 10$

---

ipotesi di comodo: $a_1 \le a_2 \le \dots \le a_n$
$b_1 \le b_2 \le \dots \le b_n$

<u>thm</u> (Riarrangiamento)

$$a_1 b_1 + \dots + a_n b_n \ge a_1 b_{\sigma(1)} + \dots + a_n b_{\sigma(n)} \ge$$
$$\ge a_1 b_n + a_2 b_{n-1} + \dots + a_n b_1$$

<u>dim</u> Le permutazioni sono prodotto di trasposizioni.

Cosa succede quando uno fa una trasposizione?

Immaginate di scambiare $i \leftrightarrow j$

σ, τ due permutaz. che diff. per una trasposizione.

$$a_1 b_{\sigma(1)} + \dots + a_n b_{\sigma(n)} \overset{?}{\gtrless} a_1 b_{\tau(1)} + \dots + a_n b_{\tau(n)}$$

nota $\underbrace{a_i b_{\sigma(i)} + a_j b_{\sigma(j)} \gtrless a_i b_{\tau(i)} + a_j b_{\tau(j)}}_{= \text{il caso } n=2}$ $\quad \tau(i) = \sigma(j)$, $\tau(j) = \sigma(i)$ $\quad (i<j)$

quello più grande sarà quello per cui $\sigma(i) < \sigma(j)$

[c'è nascosta un'induzione.] $\square$

es $\quad ab + bc + ca \leq a^2 + b^2 + c^2 \quad (a, b, c$ reali$)$.

un altro accoppiam. $\quad (a, b, c) \quad (a_i)$ $\quad$ max tra tutti gli accoppiam.

$\quad (a, b, c) \quad (b_i)$

"senza perdita di generalità" WLOG

$a \leq b \leq c$

$a \leq b \leq c$

per riarrangiam., abbiamo finito.

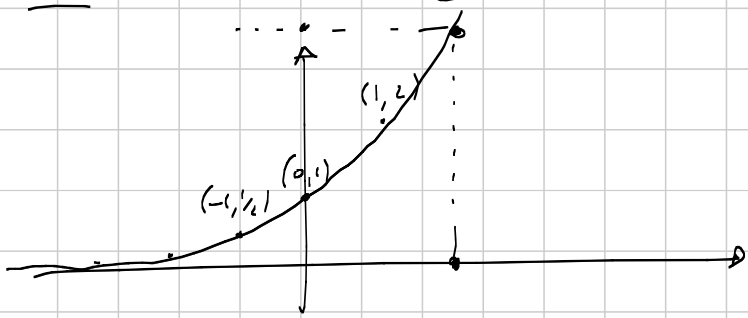
tentazione: $\quad ac + \cancel{b^2} + ca \leq a^2 + \cancel{b^2} + c^2$.

perché non è WLOG

$$\boxed{ac + b^2 + ac \overset{?}{\leq} ab + bc + ca}$$

non è simmetrica: NO WLOG!

es $\qquad a^b \cdot b^c \cdot c^a \leq a^a b^b c^c \qquad a, b, c > 0$



$y = 2^x$

$37 = 2^x$

$x = \log_2 37$

$37 \cdot 87 = 2^z \qquad z = \log_2 37 \cdot 87$

$2^{x+y} = 2^x \; 2^y \qquad \qquad = x + y = \log_2 37 + \log_2 87$

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

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

$\log_2 37^{87} = 87 \cdot \log_2 37 \quad$ (es.)

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

accoppiati "non dritti" . $\leq$ "accoppiati dritti"

RIARR.

---

② Medie (basic)

$QM \geq AM \geq GM$

$x_1, \dots, x_n > 0$ reali

$$QM = \sqrt{\frac{x_1^2 + \dots + x_n^2}{n}}$$

$$AM = \frac{x_1 + \dots + x_n}{n}$$

$$GM = (x_1 \cdot x_2 \cdots x_n)^{1/n}$$

$$\underline{1} \qquad x_1 \leq \dots \leq x_n \rightsquigarrow \underbrace{\frac{x_1+x_n}{2}}_{a}, \underbrace{\frac{x_1+x_n}{2}}_{b}, x_2, \dots, x_{n-1}$$

(stessa somma $\Rightarrow$ stessa AM)

$$QM(a,b,x_i)^2 = a^2 + b^2 + \underline{x_2^2 + \dots + x_{n-1}^2}$$

$$\updownarrow$$

$$QM(x_1, \dots, x_n)^2 = x_1^2 + x_n^2 + \underline{(x_2^2 \dots x_{n-1}^2)}$$

Capire se $a^2 + b^2 \leq x_1^2 + x_n^2$

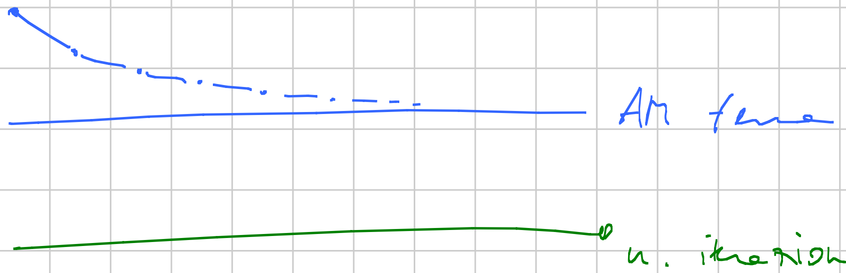
$$2\left(\frac{x_1+x_n}{2}\right)^2 < \frac{x_1^2 + x_n^2}{2}$$

AM - QM su due: $\sqrt{\frac{x^2+y^2}{2}} \geq \left(\frac{x+y}{2}\right)^2$

$$2(x^2+y^2) \geq (x+y)^2$$

$$\cancel{2}x^2 + \cancel{2}y^2 \geq \cancel{x^2} + \cancel{y^2} + 2xy$$

$$(x-y)^2 = x^2 - 2xy + y^2 \geq 0$$



non funziona perché "andare all'infinito è pericoloso".

dim "vera": sostituisco a $(x_1, x_n) \longrightarrow (A, \underbrace{x_1+x_n-A}_{y})$, $A = AM(x_1, \dots, x_n)$

che succede?

$$AM(A, x_2, \dots, x_{n-1}, y) = A = AM(x_i)$$

$$QM(A, x_2, \dots, x_{n-1}, y)^2 = A^2 + y^2 + (x_2^2 + \dots + x_{n-1}^2)$$

$$QM(x_1 \dots x_n)^2 = x_1^2 + x_n^2 + (\quad '' \quad)$$

Confrontare A^2+y^2 con $x_1^2+x_n^2$?

$$A^2 + (x_1 + x_n - A)^2 = A^2 + x_1^2 + x_2^2 + 2x_1x_2 - 2A(x_1+x_n) + A^2$$

$$\lessgtr$$

$$x_1^2 + x_n^2$$

$$\cancel{2}A^2 - \cancel{2}A(x_1+x_n) + \cancel{2}x_1x_n \gtrless 0$$

$$(A - x_1)(A - x_n) \leq 0$$

$x_1 = \min x_i$

$x_n = \max x_i$

$A = AM(x_i)$

$\downarrow$

≤ 0 , in più è

< 0 se

$x_1 \neq x_n \ldots$

[nascosta un'induzione]

<u>es.</u> $ab + bc + ca \leq a^2 + b^2 + c^2$ (2)

$$ab+bc+ca = \frac{(a+b+c)^2 - (a^2+b^2+c^2)}{2} \leq a^2+b^2+c^2$$

$$\frac{(a+b+c)^2}{9} \leq \frac{3(a^2+b^2+c^2)}{9}$$

$$AM(a,b,c)^2 \leq QM(a,b,c)^2$$

- $x + 2y + 3z \geq 6$ se $xy^2z^3 = 1$

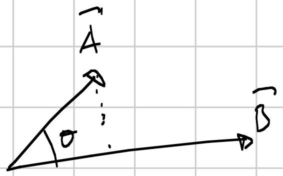
$$xy^2z^3 = GM(x,y^2,z^3)^3 = GM(x,y,y,z,z,z)^6$$

$$AM(x,y,y,z,z,z) \sim GM(x,y,y,z,z,z)^6$$

$$AM(x,y,y,z,z,z) = \frac{x+2y+3z}{6} \geq 1 \quad \checkmark$$

(3) <u>CAUCHY - SCHWARZ</u>

<u>obiettivo</u> "$|\cos\theta| \leq 1$"



$$\vec A \cdot \vec B = \|\vec A\| \cdot \|\vec B\| \cdot \cos\theta .$$

$$|\cos\theta| \le 1 \Rightarrow$$

$$|\vec A \cdot \vec B| \le \|\vec A\| \cdot \|\vec B\|$$

$\vec A = (a_1, a_2)$

$\vec B = (b_1, b_2)$

$$\vec A \cdot \vec B = a_1 b_1 + a_2 b_2$$

$\vec A = (a_1, a_2, a_3)$

$\vec B = \dots$

$$\vec A \cdot \vec B = a_1 b_1 + a_2 b_2 + a_3 b_3$$

$\vec A = (a_1, \dots, a_n)$

$\vec B = (b_1, \dots, b_n)$

$$\vec A \cdot \vec B \overset{\text{def}}{=} a_1 b_1 + \dots + a_n b_n$$

$$\|\vec A\|^2 = \vec A \cdot \vec A = a_1^2 + \dots + a_n^2$$

$$\|\vec A\|^2 = a_1^2 + a_2^2$$

$$\|\vec A\|^2 = \vec A \cdot \vec A = a_1^2 + a_2^2 + a_3^2$$

thm (CS) $(\vec A \cdot \vec B)^2 \le \|\vec A\|^2 \cdot \|\vec B\|^2$

$$\left(\sum_i a_i b_i\right)^2 \le \left(\sum a_i^2\right) \cdot \left(\sum b_i^2\right)$$

dim ① $\vec C_t$ vettore $(t \in \mathbb{R})$

$$\vec C_t = \vec A + t\vec B$$

$$0 \le \|\vec{C}_t\|^2 = \vec{C}_t \cdot \vec{C}_t = (\vec{A} + t\vec{B}) \cdot (\vec{A} + t\vec{B})$$

$$= \underbrace{\vec{A} \cdot \vec{A}}_{\|A\|^2} + 2t\,\underbrace{(\vec{A} \cdot \vec{B})}_{A \cdot B} + t^2 \underbrace{\vec{B} \cdot \vec{B}}_{\|B\|^2}$$

$$0 \le \|A\|^2 + 2t(A \cdot B) + \|B\|^2 t^2 \qquad \forall t$$

$$\Downarrow$$

$$\Delta/4 \le 0$$

$$(A \cdot B)^2 - \|A\|^2 \|B\|^2 \le 0 \,. \quad \text{win.} \ \ddot\smile$$

$=$ in CS se e solo se $A \parallel B$ $\left(\begin{array}{l} A = tB \\ \text{oppure } B = tA \end{array}\right)$

$\square$

<u>dim</u> (2) (per casa) $\quad x^2 \ge 0$

$$(a_i b_j - a_j b_i)^2 \ge 0 \quad \forall i, \forall j.$$

$$\Downarrow$$

$$\sum (a_i b_j - a_j b_i)^2 \ge 0. \quad (= CS) \ \square.$$

<u>es</u> $\quad ab + bc + ca \le \underbrace{a^2 + b^2 + c^2}_{\text{norma}^2 \text{ del vettore } (a,b,c)} \qquad (3)$

$$\underset{A}{(a,b,c)} \cdot \underset{B}{(b,c,a)}$$

C.S. $\quad (ab + bc + ca)^2 = (A \cdot B)^2 \le \|A\|^2 \cdot \|B\|^2 = (a^2 + b^2 + c^2)^2$

es (Lemma di Titu) $\quad a_i > 0,\ x_i > 0$

$$\frac{\left(\sum_i a_i\right)^2}{\sum x_i} \le \sum_i \frac{a_i^2}{x_i}$$

$$A \cdot B \le \|A\| \cdot \|B\|$$

$$\underbrace{\left(\sum_i a_i\right)^2}_{A\cdot B} \le \underbrace{\left(\sum a_i^2/x_i\right)}_{A = \left\|\frac{a_1}{\sqrt{x_1}},\dots,\frac{a_n}{\sqrt{x_n}}\right\|^2}\underbrace{\left(\sum x_i\right)}_{B = \left\|\sqrt{x_1},\dots,\sqrt{x_n}\right\|^2}$$

Per CS, abbiamo finito. $\square$

4 JENSEN (& Convessità).

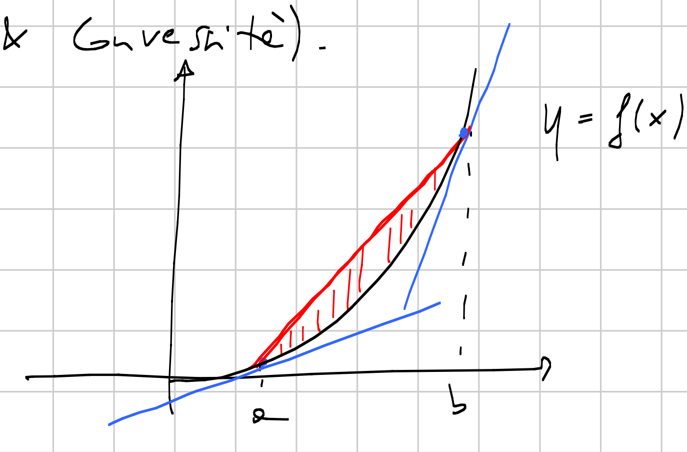
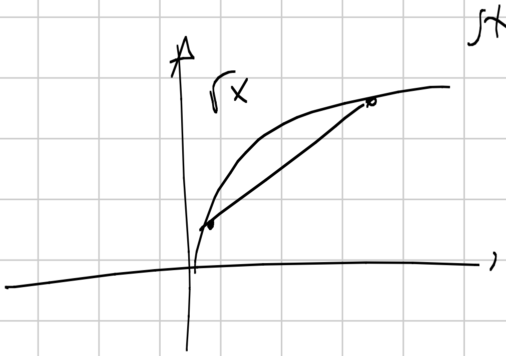
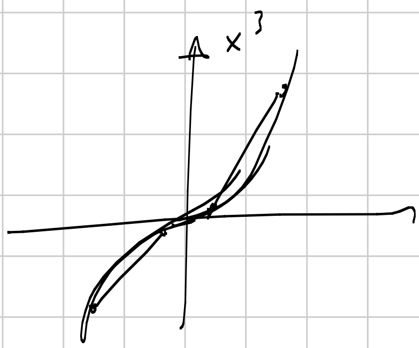


grafico di f tra a e b
sta sotto (il grafico del) segmento.

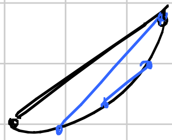




una funzione che ha la proprietà in $[0,37]$

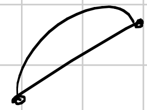
per tutti i punti a, b ✓ si

chiama **convessa** in $[0,37]$



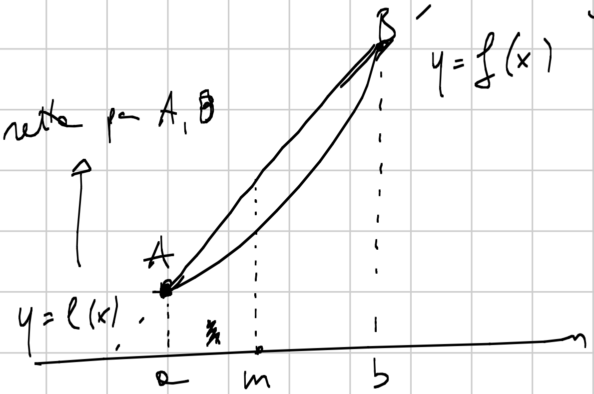
se ha la proprietà opposta

si dice **concava**.



---

cosa vuol dire che "il grafico sta sotto il segmento"?



$$f(m) \leq \ell(m)$$

comb. convessa di a, b

$$m = \lambda a + \mu b \quad \text{con } \lambda + \mu = 1, \ \lambda, \mu \geq 0$$

$$“\lambda = \frac{m-a}{b-a}, \quad \mu = \frac{b-m}{b-a}” .$$

$$f(\lambda a + \mu b) \leq \ell(\lambda a + \mu b) \overset{es}{=} \lambda f(a) + \mu f(b)$$

thm (Jensen) f è convessa, $\lambda_1 + \dots + \lambda_m = 1$, $\lambda_i \geq 0$

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

dim (es.).

"sposta il problema" verso la convessità.

es $\boxed{\bullet\ x^{\alpha} \text{ è convessa } \forall \alpha \geq 1,\ \forall x \geq 0}$

• $1/x^n$ è convessa per $x > 0$ $\forall n > 0$.

• a^x sono convessi $\forall x$, $\forall a > 0$

• x^n è concava $\forall n$ dispari, $\forall x \leq 0$

• $\log x$ è concava $\forall x > 0$

• x^{α} è concava per $x > 0$ e $\alpha \leq 1$ (reale)

es Medie generalizzate.

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

$$\text{Media } p\text{-esima} = \left(\frac{x_1^p + \dots + x_n^p}{n}\right)^{1/p}$$

thm Media p-esima $\leq$ Media q-esima se $p < q$.

dim Mi riconduco a AM $\leq$ Media q-esima con $q > 1$

(es. per voi).

$q > 1$, $f(x) = x^q$ è convessa.

per Jensen: $f(\lambda_1 x_1 + \dots + \lambda_n x_n) \leq \lambda_1 f(x_1) + \dots + \lambda_n f(x_n)$

$$\lambda_1 x_1^2 + \dots + \lambda_n x_n^2$$

scelgo $\lambda_1 = \dots = \lambda_n = \frac{1}{n}$

$$(A_n)^2 \leq \frac{x_1^2 + \dots + x_n^2}{n} = (M_2)^2 \qquad \square$$

(5) Nesbitt.

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geq \frac{3}{2} \qquad \forall a,b,c > 0.$$

dim intelligente (CS) Lemma di Titu.

$$\sum_i \frac{a_i^2}{x_i} \qquad \sum x_i \quad \left(\sum_i a_i\right)^2$$

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

a_i x_i

$$\frac{\left(\sum_i a_i\right)^2}{\sum_i x_i} \leq \sum \frac{a_i^2}{x_i} = LHS$$

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

$$\cancel{2}LHS \geq \frac{(a+b+c)^2}{\cancel{2}(ab+bc+ca)} \overset{?}{\geq} \frac{3}{\cancel{2}}$$

$$a^2+b^2+c^2+2(ab+bc+ca) \geq 3(ab+bc+ca) \text{ vera!}$$

$\square$

dim (2) Jensen.

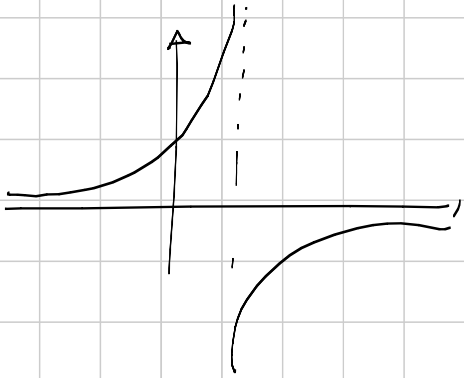
Posso supporre che $a+b+c=1$ (di omogeneità. normalizz.)

$$\frac{a}{b+c} = \frac{a}{1-a} = f(a)$$

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

per la convessità, non conta

$$\frac{x}{1-x} = \frac{x-1}{1-x} + \frac{1}{1-x} = -1 + \frac{1}{1-x}$$



è convessa per $x<1$

ok!

$$f(a)+f(b)+f(c) = \left(\frac{1}{3}f(a) + \frac{1}{3}f(b) + \frac{1}{3}f(c)\right)\cdot 3$$

$$\geq 3\cdot f\left(\frac{a+b+c}{3}\right) = f\left(\frac{1}{3}\right)\cdot 3 = \frac{\frac{1}{3}}{1-\frac{1}{3}}\cdot 3$$

$$= 3/2.$$

dim 3

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

WLOG $a \leq b \leq c$

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

$\Downarrow$ RIARR $\quad \frac{1}{b+c} \le \frac{1}{a+c} \le \frac{1}{a+b}$

$\frac{a}{a+b} + \frac{b}{b+c} + \frac{c}{c+a} \qquad \frac{a}{a+c} \quad \frac{b}{a+b} \quad \frac{c}{b+c}$

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

RR : $\quad LHS \geq \frac{a}{a+b} + \frac{b}{b+c} + \frac{c}{c+a}$

RA : $\quad LHS \geq \frac{b}{a+b} + \frac{c}{b+c} + \frac{a}{c+a}$

RV : $\quad 2LHS \geq 1 + 1 + 1 = 3$

- trovare il minimo di

$\longrightarrow \quad x + 2y + 3z$ al variare di

$x, y, z > 0$ t.c. $x^3 \cdot y^2 \cdot z = 9$

$\longrightarrow$ • min $\left(\sqrt{x+y+z} - \sqrt{x-1} - \sqrt{y-1} - \sqrt{z-1}\right)$

se $x, y, z \geq 1$, $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 2$

- dim che $\left(\frac{1}{n} \sum_i a_i b_{n+1-i}\right) \leq \left(\frac{\sum_i a_i}{n}\right)\left(\frac{\sum b_i}{n}\right) \leq$

$\leq \left(\frac{1}{n} \sum a_i b_i\right)$

se $a_1 \leq \dots \leq a_n$

$b_1 \leq \dots \leq b_n$

+ es. 86, 88 pp. 15-16

+ es 5, 6, 9 p. 24

Cominciamo a correggere?

2) $\min \sqrt{x+y+z} - \left(\sqrt{x-1} + \sqrt{y-1} + \sqrt{z-1}\right)$

con i vincoli $x,y,z \geq 1$, $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1$.

claim $\min = 0$.

$$\sqrt{x+y+z} \geq \sqrt{x-1} + \sqrt{y-1} + \sqrt{z-1}$$

$$\cancel{x}+\cancel{y}+\cancel{z} \geq \cancel{x}+\cancel{y}+\cancel{z} - 3 + 2\left(\sqrt{(x-1)(y-1)} + \sqrt{(y-1)(z-1)} + \sqrt{\ }\right)$$

$$\sum_{cyc} 2\sqrt{(x-1)(y-1)} \overset{?}{\leq} 3$$

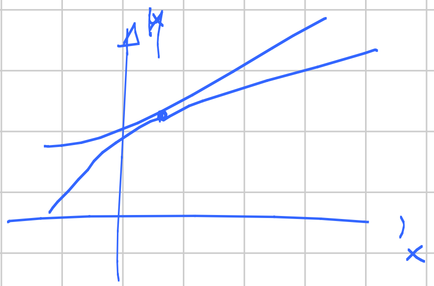
$$\xrightarrow{} \overset{AM-GM}{\leq} \sum_{cyc} (x-1)+(y-1) \overset{?}{\leq} 3$$

$= x=y=z=\frac{3}{2}$

max $2(x+y+z-3)$ col vincolo $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=2$

$A(x) \leq B(x)$

$A(x) = B(x)$ solo in $x=\pi$



- $xy + yz + zx = 2xyz$

$\longrightarrow \quad xy + yz + zx \geq 3(xyz)^{2/3}$

$2xyz \geq 3(xyz)^{2/3} \Longrightarrow xyz \geq \left(\frac{3}{2}\right)^3$

$x + y + z \geq \frac{9}{2}$

QM - AM: $\sqrt{x-1}, \sqrt{y-1}, \sqrt{z-1}$ $\quad \geq 9/2$

$$\frac{\sqrt{x-1} + \sqrt{y-1} + \sqrt{z-1}}{3} \leq \sqrt{\frac{x+y+z-3}{3}}$$

nel modo infido: min $= 0$

$$\underbrace{\sqrt{x+y+z}}_{\text{prodotto di due norme}} \geq \underbrace{\sqrt{x-1} + \sqrt{y-1} + \sqrt{z-1}}_{\text{prodotto scalare}}$$

$\sqrt{x+y+z} = \|\overset{A}{(\sqrt{x}, \sqrt{y}, \sqrt{z})}\| \rightsquigarrow B = \left(\frac{\sqrt{x-1}}{\sqrt{x}}, \sqrt{\frac{y-1}{y}}, \sqrt{\frac{z-1}{z}}\right)$

C.S. $\quad A \cdot B = RHS \leq \|A\| \cdot \overset{ok.}{\|B\|}$

$\longrightarrow 1 - \frac{1}{x} + 1 - \frac{1}{y} + 1 - \frac{1}{z} = 1.$

5 $\quad x_1\sqrt{y_1} + \dots + x_n\sqrt{y_n} = 9n \qquad \longrightarrow$ stima QM (x_i)

$x'{y'}^{1/2}$

$y' \longrightarrow y_1 + \dots + y_n = 8n$

$$QM^2(x_i) = \frac{x_1^2 + \dots + x_n^2}{n} \longleftarrow x^2$$

$$B = (\sqrt{y_1}, \dots, \sqrt{y_n}) \longrightarrow \|B\|^2 = 8n$$

$$A = (x_1, \dots, x_n) \longrightarrow \|A\|^2 = QM(x_i)^2 \cdot n$$

vincolo: $A \cdot B$

C.S. $(A \cdot B)^2 \leq \|B\|^2 \cdot \|A\|^2$

$$\overset{\shortparallel}{81 \cancel{n^2}} \leq 8\cancel{n} \cdot \cancel{n} \cdot QM^2 \Longrightarrow$$

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

Cosa serve per avere $=$?

$=$ in CS $\Longleftrightarrow$ $A \,/\!/\, B$.

$\Longleftrightarrow$ $x_i = \lambda\sqrt{y_i}$ $\forall i$ (per un certo λ)

$$QM(x_i)^2 = \frac{\sum \lambda^2 y_i}{n} = \lambda^2 \frac{\sum y_i}{n} = \lambda^2 8.$$

vincolo: $\sum x_i \sqrt{y_i} = 9n$

$$\overset{\shortparallel}{\sum \lambda y_i} = \lambda \cdot 8n \Longrightarrow \lambda = \frac{9}{8}$$

6. trovare la migliore C t.c. $(x-y)(2y-x) \leq Cxy$

vincoli $0 \leq \cancel{y} \leq x \leq 2y$ reali.

$2 \geq \frac{x}{y} \geq 1$, $\frac{x}{y} = t$

posso supporre $x, y \neq 0$.

$$\frac{(x-y)(2y-x)}{xy} \leq C .$$

$$\min C = \max_{x,y,\dots} \left(\frac{(x-y)(2y-x)}{xy}\right).$$

$$\frac{(x-y)(2y-x)}{xy} = \left(1 - \underbrace{\frac{y}{x}}_{1/t}\right)\left(2 - \underbrace{\frac{x}{y}}_{t}\right) =$$

$1 \leq t \leq 2$

$$= (2-t)\left(1 - \frac{1}{t}\right) =$$

$$= 2 - \frac{2}{t} - t + 1 = 3 - \frac{2}{t} - t$$

$$\max(\text{——}) = 3 - \min\left(\frac{2}{t} + t\right)$$

$$\sqrt{\frac{2}{t} \cdot t} = \sqrt{2} \overset{\text{AMGM}}{\leq} \frac{\frac{2}{t} + t}{2} \Rightarrow$$

$$\min\{\quad\} \geq 2\sqrt{2} \Rightarrow$$

$$\max\{ - \text{——} \} = 3 - 2\sqrt{2} \Rightarrow C = 3 - 2\sqrt{2}$$

$= \Leftarrow$ $2/t = t \Rightarrow t = \sqrt{2}$ ✓

$$(c-3)xy + x^2 + 2y^2 \geq 0 \quad \rightsquigarrow \quad (c-3)t + t^2 + 2 \geq 0$$

$$(x - y\sqrt{2})^2 \geq 0$$

$$2y^2 + x^2 - 2\sqrt{2}\,xy$$

Algebra 3

marzo

Titolo nota 26/08/2015

Successioni, ricorrenze, eq. funzionali.

(1) Progressioni aritmetiche e geom.

$x_0, x_1, x_2, x_3, \ldots$ in progr aritm.

se $x_n - x_{n-1}$ è costante $\rightsquigarrow d$
RAGIONE

se $\frac{x_{n+1} + x_{n-1}}{2} = x_n$

es $0, 1, 2, 3, 4, \ldots$

$x_n = ?$ in termini di x_0, n, d

$$x_n = x_0 + nd$$

$x_0, x_1, \ldots, x_n, \ldots$ in progr geom se:

$\sqrt{x_{n+1} \cdot x_{n-1}} = x_n \quad \forall n$

$\Updownarrow$?

x_{n+1}/x_n è costante $\rightsquigarrow \alpha$

$1, 2, 4, 8, 16 \ldots$

$1, 0, 0, 0, 0, \ldots$

$X_n = ?$ $\qquad X_n = X_0 \cdot \alpha^n.$

oss. se $\alpha > 0$, $X_0 > 0$ ARITM $\longleftrightarrow$ GEOM

X_n geom $\Longrightarrow$ $\log X_n$ aritm.

Succ. per ricorrenza:

$$A: \begin{cases} X_0 = X_0 \\ X_{n+1} = X_n + d \end{cases}$$

$$G: \begin{cases} X_0 = X_0 \\ X_{n+1} = \alpha X_n \end{cases}$$

$$S: \begin{cases} X_0 = 2 \\ X_{n+1} = \text{num. di lettere che mi servono per scrivere } X_n \end{cases}$$

$$S: \begin{cases} X_0 = 12 \\ X_{n+1} = \text{num di divisori di } X_n + \text{num. di potenze di } X_{n-3} \text{ che sono } < 1000000 \end{cases}$$

– Ce ne sono alcune che sono più "ragionevoli".

"lineari"

$$\begin{cases} X_0 = x_0 \\ X_{n+1} = a X_n + b \end{cases}$$

X_n in funzione dei parametri (a, b, X_0) ed n?

X_0

$X_1 \quad a X_0 + b$

$X_2 \quad a^2 X_0 + ab + b$

$X_3 \quad a^3 X_0 + a^2 b + ab + b$

$X_4 \quad a^4 X_0 + a^3 b + a^2 b + ab + b$

$\vdots$

<u>quindi</u> $x_n = a^n \cdot x_0 + b(a^{n-1} + a^{n-2} + \dots + a + 1)$

<u>dim</u> (per induzione).

<u>in alternativa</u>: $\rightarrow y_{n+1} = a y_n$ ← la forma

$x_n = y_n + k$ per un certo k.

$x_{n+1} = a x_n + b$

$y_{n+1} - k = a(y_n - k) + b$

$y_{n+1} = a y_n + \boxed{b + k - ak}$

$b + k - ak = 0$

$\Rightarrow (1-a)k = -b$

$= 0$ se

$k = b/(a-1)$

$x_n - \frac{b}{a-1}$ è una progr. geom. di ragione $\alpha = a$

che parte da $x_0 - \frac{b}{a-1}$

$$x_n - \frac{b}{a-1} = a^n \left(x_0 - \frac{b}{a-1}\right) \Rightarrow x_n = a^n x_0 + \frac{1-a^n}{1-a} b$$

<u>es</u> trovare l'errore!

Succ. per ricorrenza da due termini precedenti.

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

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, ...

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

$$\begin{cases} x_{n+1} = a x_n + b x_{n-1}. \\ x_0 = \text{fissato.} \\ x_1 = \text{fissato.} \end{cases}$$

Non è mica che $x_n = \lambda^n$ funziona? (cioè soddisfa la ricorr.)

$x_n = \lambda^n \rightsquigarrow \lambda^{n+1} = a\lambda^n + b\lambda^{n-1} \rightsquigarrow$

$\lambda^2 - a\lambda - b = 0 \Rightarrow \lambda$ radice di $x^2 - ax - b$.

$\lambda \qquad \mu$

$x_n = \alpha\lambda^n$ e $x_n = \beta\mu^n$ funzionano.

$x_n = \alpha\lambda^n + \beta\mu^n$ funziona!

Sono tutte? $\quad x_0 = \text{fissato} \longrightarrow x_0 = \alpha\lambda^0 + \beta\mu^0$

$x_1 = \text{fissato} \longrightarrow x_1 = \alpha\lambda + \beta\mu$

da queste si ricavano α e β.

Se $\lambda = \mu$: $\quad \begin{cases} \alpha + \beta = x_0 \\ \lambda\alpha + \mu\beta = x_1 \end{cases} \rightsquigarrow \begin{cases} \alpha+\beta = x_0 \\ \alpha + \beta = x_1/\lambda. \end{cases}$

Se $\lambda = \mu$ cerco anche sol. delle forme $x_n = n \cdot \lambda^n$.

es. verificare che funziona (e che si possono ricavare α, β).

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

$$\frac{1+\sqrt{1+4}}{2} = \phi \quad \text{(RAPP. AUREO)}$$

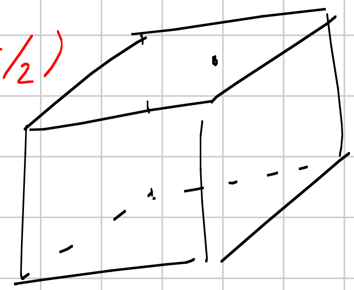
$$\frac{1-\sqrt{1+4}}{2} = -\frac{1}{\phi} = \psi$$

$$F_n = \alpha \phi^n + \beta \psi^n$$

$$\begin{cases} \alpha + \beta = 0 & \longrightarrow \quad \alpha = -\beta \\ \alpha\varphi + \beta\psi = 1 & \longrightarrow \quad (\varphi - \psi)\cdot\alpha = 1 \end{cases}$$

$$\alpha = \frac{1}{\varphi - \psi} = \frac{1}{\sqrt{5}}.$$

es (SNS '15/2)



la parte dal soffitto / pavim.

Ga $1/5$ $\longrightarrow$ soffitto / pavim.

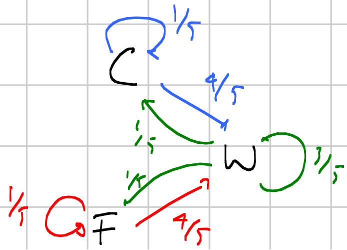
Ga $1/5$ $\longrightarrow$ in una delle 4 pareti.

la parte da 1 parete
- $1/5$ soffitto
- $1/5$ pavim.
- $1/5$ su una delle altre pareti

qual è la prob. che al passo n-esimo sia sul soffitto.

Diamo dei nomi: W_n (pareti), f_n (pavim.), C_n (soffitto).

$$(W_0, f_0, C_0) = (0, 0, 1)$$



$$\begin{cases} W_{n+1} = \frac{4}{5} c_n + \frac{3}{5} w_n + \frac{4}{5} f_n \\ C_{n+1} = \frac{1}{5} c_n + \frac{1}{5} w_n \\ f_{n+1} = \frac{1}{5} f_n + \frac{1}{5} w_n \end{cases} \qquad c_n = ?$$

$\longleftarrow$ ulote

$$\underline{\text{oss}} \quad d_{n+1} = c_{n+1} - f_{n+1} = \frac{1}{5}\left(c_n - f_n\right) = \frac{d_n}{5}$$

$$d_n = \left(\frac{1}{5}\right)^n \Longrightarrow c_n = f_n + \left(\frac{1}{5}\right)^n$$

$$\begin{cases} W_{n+1} = \frac{4}{5} c_n + \frac{3}{5} w_n + \frac{4}{5}\left(c_n - \left(\frac{1}{5}\right)^n\right) \\ c_{n+1} = \frac{1}{5} c_n + \frac{1}{5} w_n \end{cases} \rightsquigarrow w_n = 5c_{n+1} - c_n$$

$$\hookrightarrow \begin{cases} W_{n+1} = \frac{8}{5} c_n + \frac{3}{5} w_n - \frac{4}{5}\left(\frac{1}{5}\right)^n \\ \text{—} \rightsquigarrow c_{n+2} = \frac{1}{5} c_{n+1} + \frac{1}{5} w_{n+1} \end{cases}$$

$$c_{n+2} = \frac{1}{5} c_{n+1} + \frac{8}{25} c_n + \frac{3}{25} w_n - \frac{4}{25}\left(\frac{1}{5}\right)^n$$

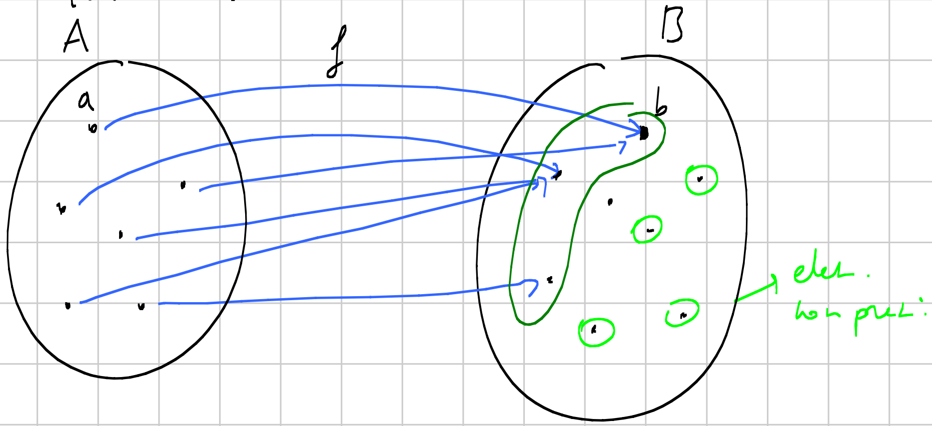
$$c_{n+2} = \frac{1}{5} c_{n+1} + \frac{8}{25} c_n + \frac{3}{5} c_{n+1} - \frac{3}{25} c_n - \frac{4}{25}\left(\frac{1}{5}\right)^n.$$

$$c_{n+2} = \frac{4}{5} c_{n+1} + \frac{1}{5} c_n \left(- \frac{4}{25}\left(\frac{1}{5}\right)^n\right) \to \text{ignoro}$$

$$c_{n+3} = \frac{4}{5} c_{n+2} + \frac{1}{5} c_{n+1} - \frac{1}{5} \cdot \left[\frac{4}{25} \cdot \left(\frac{1}{5}\right)^n\right]$$

Equaz. funzionali.

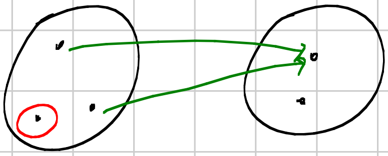
Un'eq. funz. è un'equazione la cui incognita è una funzione.



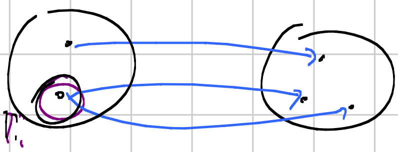
$f: A \to B$ $\qquad f(a) = b$

$f: a \mapsto b$ $\quad$ \$\mapsto \$

non è una funzione:



f è obbligata a rispondere ad un elem. $a \in A$, è obbligata a dirgli esattam. dove andare.



funzione $\neq$ formula.

$f: A \to B$

A: dominio, B: codominio

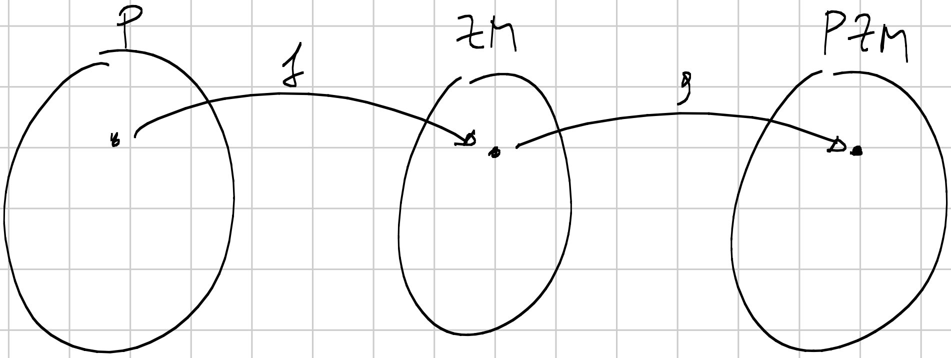
$f(A) = \{$elem. colpiti$\}$ = immagine di f.

nota $f(A)$ può essere più piccolo di B.

- f si dice suriettiva (surgettiva) se $f(A) = B$
- f si dice iniettiva se $f(a) = f(a') \Rightarrow a = a'$.

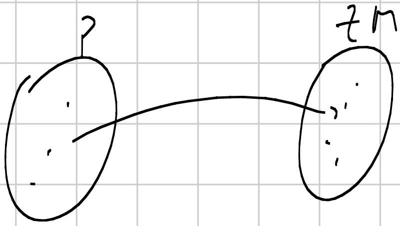
$$a \neq a' \Rightarrow f(a) \neq f(a').$$

Date due funzioni, ogni tanto si possono comporre

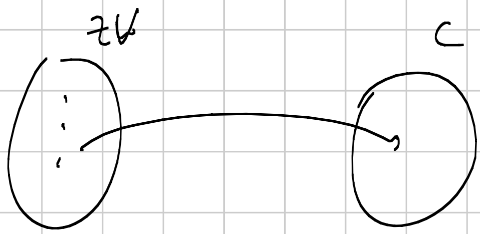


$\longrightarrow$ $g(f(x)) : x \longmapsto f(x) \longmapsto g(f(x))$.

$=$ $(g \circ f)(x)$ ("prima f").



??! no composizione



es $f : \mathbb{R} \longrightarrow \mathbb{R}$ t.c. $(f(x))^2 = x^2 \ \forall x$.

$$f(x)^2 = x^2 \iff f(x) = \pm x$$

può dipendere da x!!

$f(x) = x$

$f(x) = -x$

due soluzioni. NO

molto sbagliato.

$f(x) = |x|$, $f(x) = -|x|$.

$$f(x) = \begin{cases} x & x \in \mathbb{Q} \\ -x & x \in \mathbb{R} \setminus \mathbb{Q}. \end{cases}$$

le sol. sono una marea!

Basta, ad ogni punto x associare un segno (a caso).

$f(0) = 0$. (unica certezza).

es. se f è crescente $\Rightarrow f(x) = x$

es (equazione di Cauchy) trovare tutte le $f : \mathbb{Q} \to \mathbb{Q}$

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

metto $x = y = 0$: $\cancel{f(0+0)} = \cancel{f(0)} + f(0) \Rightarrow f(0) = 0$.

mettere $y=0$: $f(x) = f(x) + f(0)$ .. non dà altre info.

$\boxed{\text{metto } x=y=1 \quad : \quad f(2) = 2f(1)}$

metto $x=2, y=1$: $f(3) = f(2) + f(1) = 3f(1)$.

$f(n)$? mi aspetto $f(n) = nf(1)$. (induzione)

$f(1)$ determina $f(n)$ $\forall n$.

metto $x=y$ $\quad f(x+x) = f(x) + f(x) \longrightarrow f(2x) = 2f(x)$

metto $y=2x$ $\quad f(3x) = f(2x) + f(x) = 3f(x)$.

(stessa ind.)

$$f(nx) = nf(x). \qquad (A)$$

Voglio calcolare $f(1/2)$. Uso (A) con $n=2$, $x = 1/2$.

$$f(2 \cdot 1/2) = 2 \cdot f(1/2) \Rightarrow f(1/2) = \tfrac{1}{2} f(1)$$

$f(1/3)$? $\quad f(1/3) = 1/3 \cdot f(1)$ .. $\quad f(1/n) = \frac{1}{n} f(1)$

$$f(a/b) = f(a \cdot 1/b) = a \cdot f(1/b) = \frac{a}{b} f(1)$$

Chiamiamo $k = f(1)$.

Se f è una sol., allora $f(x) = kx$.

<u>NON</u> abbiamo finito!

$f(x) = kx$ soddisfa l'eq. iniziale?

$k(x+y) = f(x+y) = f(x) + f(y) = kx + ky$. ok.

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

Ci sono una marea di soluzioni dell'eq. di Cauchy

$$f(x+y) = f(x) + f(y) \quad \text{sui reali.}$$

es • f è limitata sull'intervallo $[0,1]$ $\Longrightarrow$ sol. è det.

$\exists M > 0$ costante t.c. $f(x) \leq M$ $\forall x \in [0,1]$.

• f è monotòna (cioè cresc. o decrescente)

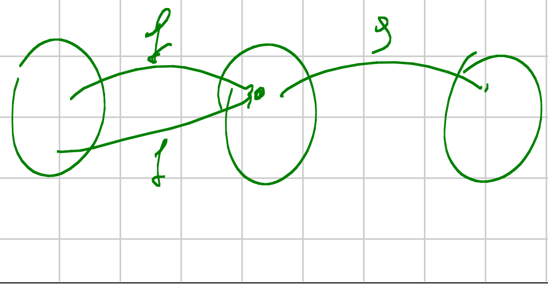
• f è continua.

es trovare tutte le $f : \mathbb{Z} \to \mathbb{Z}$ t.c.

$$f(f(n)) = n+1 \quad \forall n \in \mathbb{Z}.$$

oss! f è iniettiva.

[più in generale, se $g \circ f$ è iniettiva allora f è iniettiva]

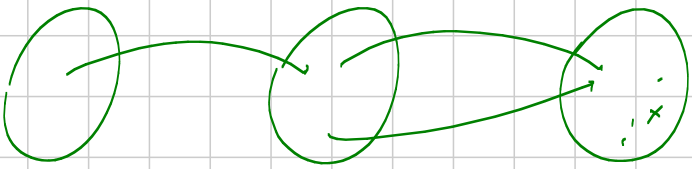


$f(x) = x \qquad g(x) = x^2$

$f: \mathbb{N} \to \mathbb{Z} \qquad g: \mathbb{Z} \to \mathbb{N}$

oss 2 f è suriettiva.

[in gen. se $g \circ f$ è suriettiva allora g è suriettiva]



oss 3 = 1 + 2 f è bigettiva. (iniettiva + suriettiva).

$f(f(n)) = n+1$.

$f(n)+1 = f(f(f(n))) = f(n+1)$

sto applicando $f(f(x)) = x+1$ con $x = f(n)$.

→ questo ci dice che $f(n) = f(0) + n \quad \forall n$.

(sembra venire per induzione) → ovvio è induzione!

quanto può fare $f(0)$?

applico con $n = f(0)$

$f(f(0)) = 1$

$f(0) + f(0) = 2f(0) \longrightarrow 2f(0) = 1.$ ↯.

non ha soluzioni.

es 90, 91 p. 16~

es 4, 6, 7, 9, 10 p. più avanti

es 4 $f : \mathbb{R} \to \mathbb{R}$ monotone t.c.

$$f(x + f(y)) = y + f(x) \longrightarrow f(?)$$

$x = 0$: $f(f(y)) = \underbrace{y + f(0)}_{\text{bijettiva!}}$ $\Longrightarrow f$ bijettiva

$y = 0$ $f(f(0)) = 0 + f(0) \Longrightarrow \cancel{f}(f(0)) = \cancel{f}(0) \Longrightarrow$

$f(0) = 0$.

(basta l'iniettività di f).

$\Longrightarrow f(f(y)) = y \quad \forall y$.

monotone $\longrightarrow$ Cauchy?

Come si vede più Cauchy? $\boxed{y = f(z)}$

$$f(x + \underbrace{f(f(z))}) = f(x) + f(z)$$

$$f(x + z) = f(x) + f(z) \xrightarrow{\text{Cauchy}} f(x) = kx \quad \forall x$$

$$f(x + f(y)) = k(x + ky) = kx + k^2 y$$

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

$$\cancel{kx} + k^2y = y + \cancel{kx} \Longleftarrow k = \pm 1 .$$

$$\cancel{f(x) = \pm x} \qquad f(x) = x$$

Sol. $f(100) = \pm 100$.

$$f(x) = -x$$

es 6

$$x_{n+1} = 6x_n - 2\sum_{k=0}^{n} x_k = 6x_n - 2x_n - 2\sum_{k=0}^{n-1} x_k$$

$$- \quad x_n = 6x_{n-1} - 2\sum_{k=0}^{n-1} x_k$$

$$x_{n+1} - x_n = 6x_n - 6x_{n-1} - 2x_n$$

$$x_{n+1} - \cancel{x_n} = \cancel{4}^{5} x_n - 6x_{n-1}$$

$$x^2 - 5x + 6 < \begin{matrix} 2 \\ 3 \end{matrix}$$

Cavillo: ricavo x_1 dalla ricorsione iniziale

$$x_1 = 6x_0 - 2x_0 = 4$$

es 7 idea $\frac{\sqrt{2}}{4}(1+\sqrt{2})^n$ ~ compare nella sol. di un'eq. per ricorrenza a 2 termini.

$$\frac{\sqrt{2}}{4}\underline{(1+\sqrt{2})^n} + \beta\underline{(\sqrt{2}-1)^n}$$

$\to$ Sol. gen. di una ricorsione

$$X_n = a X_{n-1} + b X_{n-2}$$

$$x^2 - ax - b = \left(x - (\sqrt{2}+1)\right)\left(x - (\sqrt{2}-1)\right)$$

$$= x^2 - x\sqrt{2} + 1$$

prendo $1-\sqrt{2}$ invece di $\sqrt{2}-1$

$\rightsquigarrow$

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

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

prendo $\beta = -\frac{\sqrt{2}}{4}$ e prego che vengano interi:

$$X_0 = 0$$

$$x_1 = \frac{1}{2\sqrt{2}}\left((\sqrt{2}+\cancel{1}) - (\cancel{1}-\sqrt{2})\right) = 1$$

x_i interi.

posso ricavare le classi di resto di x_i mod 7

$$X_n = \frac{1}{2\sqrt{2}}\left(1+\sqrt{2}\right)^n - \frac{1}{2\sqrt{2}}\left(1-\sqrt{2}\right)^n$$ $\to$ molto piccolo

per $n>2$ $\quad x_n$ è l'intero più vicino a $\frac{1}{2\sqrt{2}}\left(1+\sqrt{2}\right)^n$

e per n pari $X_n = \left\lfloor \frac{(1+\sqrt{2})^n}{2\sqrt{2}} \right\rfloor$

per n dispari $X_n = \lceil \quad \rceil = \lfloor \quad \rfloor + 1$

es 9 Modo contoso: $X_n = \alpha\left(\frac{1+\sqrt{5}}{2}\right)^n + \beta\left(\frac{1-\sqrt{5}}{2}\right)^n$

per qualche α e β.

Compaiono ad mezz delle $\sqrt{5}$ (al denom.)

$$X_{4091} = \alpha \cdot \sum_{k=0}^{4091} \binom{4091}{k} \frac{\sqrt{5}^k}{2^n} + \beta \sum_{k=0}^{4091} \binom{4091}{k} \frac{(-\sqrt{5})^k}{2^n}$$

se α e β sono fatti bene tutte le cose con $(\sqrt{5})^{2h+1}$ si semplificano

↳ resta una cosa che non ha più delle radici.

Modo furbo Ricavare le sol. della seguente mod. 4091.

λ^n sarà una sol. della ricorsione?

$$\lambda^2 - \lambda - 1 = 0 \quad (\text{mod } 4091)$$

$$\lambda^2 - 2 \cdot \left(\cancel{\tfrac{1}{2}}\right)^{e} \cdot \lambda - 1 \equiv 0 \qquad e = \text{inv. di } 2 \text{ mod } 4091$$

$$\lambda^2 - 2\cdot 2046\cdot\lambda + (2046)^2 \equiv 2046^2 + 1$$

$$(\lambda - 2046)^2 \equiv 1023 + 1 = 1024 = 32^2$$

$$2046^2 = \left(\frac{4091+1}{2}\right)^2 = \boxed{\cancel{\frac{4091}{2}\left(\frac{4091+1}{2}\right)}} + \frac{4091+1}{4}$$

$$\frac{2046}{2} = 1023$$

$$\lambda - 2046 \equiv \pm 32 \pmod{4091}.$$

$$\lambda_1, \lambda_2 = 2046 \pm 32$$

$$\alpha\cdot\lambda_1^n + \beta\cdot\lambda_2^n \quad \text{sono tutte le sol.}$$

$$X_{4091} = \alpha\cdot\lambda_1^{4091} + \beta\cdot\lambda_2^{4091} \equiv$$

$$\equiv \alpha\cdot\lambda_1 + \beta\lambda_2 \equiv X_1 = 1$$

$$X_{4091} - 1 \equiv 0 \pmod{4091}$$

es 10

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

$$x = 0, \quad f(f(y)) = f(0)^2 + y \Rightarrow f \text{ bijettiva}$$

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

$$\exists\,\alpha \text{ t.c. } f(\alpha) = 0 \qquad x = \alpha \qquad f(f(y)) = y$$

Sost. a x $f(z)$

$$x f(x) = f(z)\cdot f(f(z)) = z \cdot f(z)$$

$$\begin{cases} f(z\cdot f(z) + f(y)) = f(f(z))^2 + y \\ f(z\cdot f(z) + f(y)) = f(z)^2 + y \end{cases}$$

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

$\Rightarrow$ $f(z) = \pm z$ (segno dipende da z)

Suppongo che ci siano x, y t.c. $f(x) = x$, $f(y) = -y$

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

$\downarrow$

$x^2 - y$

$-x^2 + y$

Sol. se $y = 0$

Sol. se $x = 0$

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

uniche sol.

Combinatoria 1 - Basic

TESS

Titolo nota 22/08/2015

- Conteggi
- Double-Counting (D-C)

Conteggi

- somma $A = B \cup C$, $\boxed{B \cap C = \emptyset}$ DISGIUNTI
  $\Rightarrow \#A = \#B + \#C$

- prodotto $A = B \boxed{\times} C$ INDIPENDENTI
  $\Rightarrow \#A = \#B \cdot \#C$

Es banali

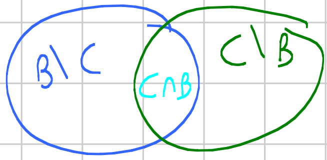
Permutazioni $= n!$

Funzioni da A a B $= \#B^{\#A}$

Coeff. Binomiali $[x^k y^{n-k}] (x+y)^n =: \binom{n}{k}$

Principio Inclusione-Esclusione

$A = B \cup C$, ma non so niente di $B \cap C$



$$= A = B\setminus C \cup C\cap B \cup C\setminus B$$

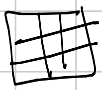
$$\#A = \#B\setminus C + \#C\cap B + \#C\setminus B$$
$$= \#B + \#C\setminus B$$
$$= \#B + \#C - \#C\cap B$$

In generale:

$$A = \bigcup_{i=1}^{n} B_i$$

$$\#A = \sum_{i=1}^{n} \#B_i - \sum_{i,j=1,\, i\neq j}^{n} \#(B_i \cap B_j) + \sum_{i,j,k} \#(B_i\cap B_j \cap B_k) - \dots + (-1)^n \# \bigcap_{i=1}^{n} B_i$$

TI-2015 n° 5



colorare con 2 colori
senza sottoquadrati 2x2 tutti bianchi

i B_i sono gli insiemi che contengono
le colorazioni con l'i-esimo angolo 2x2
bianco e nessuna condizione sui colori
delle altre caselle

configurazioni buone =

Σ tutte le conf. possi: $-$ Σ quelle con 1 2x2 bianco
$+$ Σ quelle con 2 2x2 bianchi $-$ ... 3 $+$ ... 4

$= 2^9$ $\quad = 4 \cdot 2^5$

$= 4\cdot 2^3 + 2\cdot 2^2$ $\quad = 4 \cdot 2^1$ $\quad = 1$

Le funzioni surgettive da A a B

di funzioni surg. =

di tutte $-$ # funzioni che lasciano 1 elemento
$+$ ... ne lasciano 2 $-$ 3 $+$ ...

=

~~#~~ A = a
B = b

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

TF 2014 n° 4

Quante sono le funzioni da $f:\{1,\dots,2014\}\to\{1,\dots,4\}$
con $\# \operatorname{Im} f = 3$

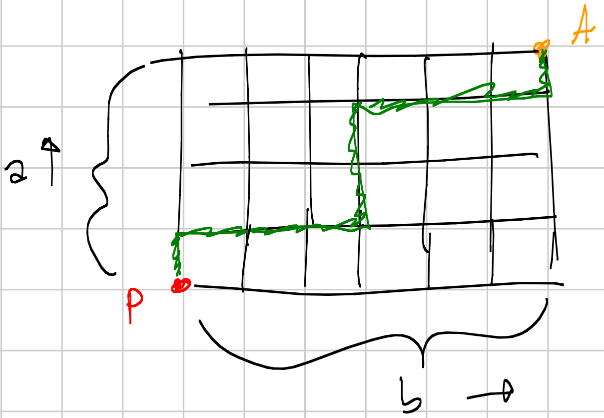
Sol: $4\cdot 3^{2014} - \binom{4}{2}\cdot 2^{2014} + \binom{4}{3}\cdot 1^{2014}$

– bigezione

$f : A \to B$ bigettiva

$\# A = \# B$

Es: i cammini monotoni



I passi consentiti sono solo ↑ e →

$f : \{\text{cammini monotoni}\} \to \{\text{stringhe di } \overset{\#a}{\uparrow} \text{ e } \overset{\#b}{\to}\}$

a associo ↑ → → → ↑ ↑ _ _

$f^{-1}(f) = Id$

$\Rightarrow$ # cammini monotoni sono $\binom{a+b}{b}$

IMO 2011 – 4

n pesi $2^0, 2^1, \ldots, 2^{n-1}$

da mettere su una bilancia a 2 piatti

Contare il numero di modi di piazzarli in modo che dopo ogni aggiunta di un peso il piatto a destra sia + pesante di quello a sx

Sol: cerco di ricondurmi al caso n−1

Chiamo $A_n = \{$ modi di piazzare n pesi $\}$

Cerco una mappa $f : A_n \to A_{n-1}$

$f(\text{modo}_n)$ = la sequenza dei pesi trascurando il più piccolo (2^0)

$2^3 d, 2^4 d, 2^2 s, 2^0 s, \dots$

$f \downarrow$

$2^3 d, 2^4 d, 2^2 s, \dots$

$g \downarrow$ (dimezzo i pesi)

$2^2 d, 2^3 d, 2^1 s, \dots$

$g \circ f$ è la vera funzione

Quante volte ottengo la sistemazione X

il peso 2^0 — al primo posto → 1

al secondo → 2

⋮

all'ultimo posto → 2

ci sono sempre $2n-1$ sistemazioni con n pesi che vengono mappate nella sistemazione X ($\forall$ scelta di X)

$$\# A_n = (2n-1) \cdot \# A_{n-1}$$

$$\# A_n = (2n-1)!! = (2n-1)(2n-3) \cdot \ldots \cdot 1$$

- ricorsione

legge su una successione $a_0, a_1, a_2, \ldots$

$$a_{n+1} = f(a_n) \quad \text{es. base}$$

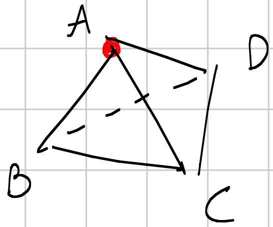
$$a_{n+1} = f(a_n, a_{n-1}, \ldots, a_{n-k})$$

$$a_{n+1} = f(a_n, \ldots, a_1)$$

ancora + complicato

$$a_{n+1} = f(a_n, \ldots, a_1, n)$$

es. fattoriale $f_n = n \cdot f_{n-1}$



la pulce saltella di vertice in vertice, partendo da A

Calcolare (ricorsivamente) il numero di modi di tornare in A dopo n salti

È utile distinguere dove si può trovare la pulce dopo n salti

distinguo $A_n :=$ # modi per tornare in A
$B_n :=$ # modi per non tornare in A

$$\begin{cases} A_n = B_{n-1} \\ B_n = 3 \cdot A_{n-1} + 2 \cdot B_{n-1} \end{cases}$$

$$\rightsquigarrow A_{n+1} = 2A_n + 3A_{n-1}$$

$A_0 = 1$, $A_1 = 0$; $A_2 = 3$, $A_3 = 6$, $A_4 = 21$

Problema per casa: la pulce si muove su un cubo

D – C

L'idea è cercare di calcolare (o stimare) una quantità in modi diversi

Es banale (ma non troppo)

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

1	2	3	...	n
n	...	3	2	1

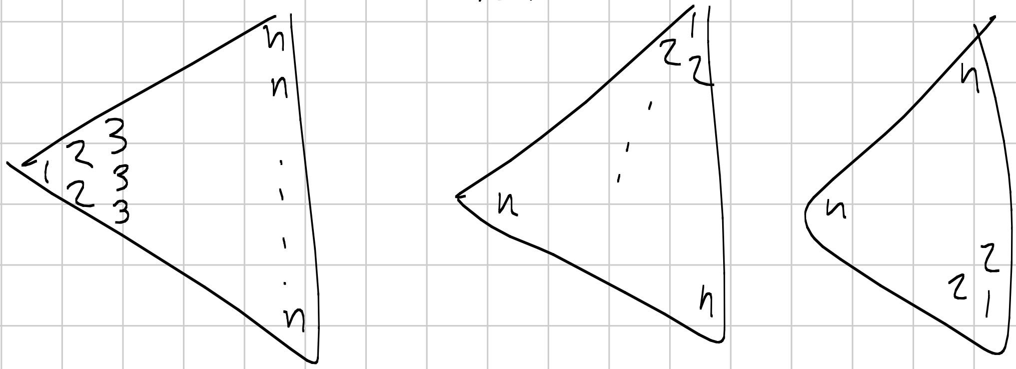
n

Sia Q la somma della tab

$$2\sum_{i=1}^{n} i \underset{\text{per righe}}{=} Q \underset{\text{per colonne}}{=} n \cdot (n+1)$$

Es 2 :

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



poi metto in pila i 3 piani

$$3\sum_{i=1}^{n} i^2 = Q = (2n+1)\cdot \#\text{colonne}$$

per piani   per colonne

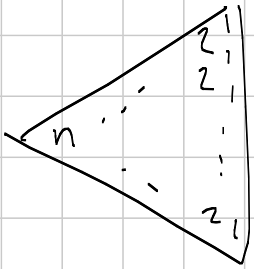
$$\#\text{colonne} = \frac{n(n+1)}{2}$$

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

T1 2015 n° 6

Voglio calcolare $\displaystyle\sum_{i=1}^{2014} i(2015-i)$

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



faccio le 3 rotazioni e le impilo

$$3\sum_{i=1}^{n} i(n+1-i) = Q = (n+2)\,\frac{n(n+1)}{2}$$

(nell'es 6 $\displaystyle\sum_{\sigma\in I} f(\sigma)$)

Il D-C dimostra P.I.E.

vogliamo calcolare la cardinalità dell'unione di insiemi qualsiasi

$$\# \bigcup B_i = \sum \# B_i - \sum \# B_i \cap B_j + \ldots$$

mi chiedo un elemento $x \in \bigcup B_i$ quante volte compare a dx

es $x \in \bigcup_I B_i \setminus \bigcup_J B_j$

IMO 2015 n° 1

$S = \{$alcuni punti nel piano$\}$

S è equilibrato se $\forall A, B \in S$
$\exists C \in S : AC = BC$

S è eccentrico se $\forall A, B, C \in S$
non $\exists P \in S : PA = PB = PC$

per quali n esiste un equ e ecc?

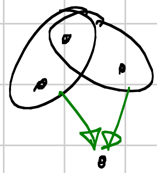
Soluzione

con 4 mi pare di non riuscirci

la prima cond. mi fornisce una funzione

$f : \{ \text{coppie in } S \} \to S$

se $\#S = 4$ ho 6 coppie
un punto viene preso da 2 coppie



conto le coppie su n elementi $\binom{n}{2}$

conto (anzi stimo) quante coppie forniscono lo stesso punto equidistante

Prendiamo il punto P che è immagine (secondo f) di più coppie sia Q il numero di volte che è imm.

se voglio ecc $\left\lfloor \frac{n-1}{2} \right\rfloor \geq Q$

per pigeonhole $Q \geq \left\lceil \frac{\binom{n}{2}}{n} \right\rceil$

$$\left\lfloor \frac{n-1}{2} \right\rfloor \geq \left\lceil \frac{n(n-1)}{n \cdot 2} \right\rceil$$

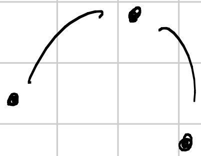
$$\left\lfloor \frac{n-1}{2} \right\rfloor \geq \left\lceil \frac{n-1}{2} \right\rceil$$

Per n pari non ho speranza.

Grafo

(V, E) $\quad V$ è l'insieme dei vertici

e $E \subseteq V^2$ è l'insieme degli archi



se il grafo è non orientato allora $(v_i, v_j) \in E$

$\Rightarrow (v_j, v_i) \in E$

altrimenti è detto orientato - diretto

tante volte non c'è (v_i, v_i)

dato $v_i \in V$, $\deg(v_i) = \#$ archi che coinvolgono v_i

$$\sum_{v_i \in V} \deg(v_i) = ?$$

un arco, che contributo dà a questa somma?

$$\sum_{v_i \in V} \deg(v_i) = \sum_{e_i \in E} 2 = 2\#E$$

Es dal Senior 2002 C1 - 10

sono in un grafo :

$\# V = 12k$

$\forall A \in V, \quad \deg(A) = 3k+6$

$\forall A, B \in V, \quad \exists$ esattamente N vertici che sono collegati a entrambi

Le ipotesi parlano di strutture del tipo

Sia Q = il numero di nel grafo

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

conto per gli estremi

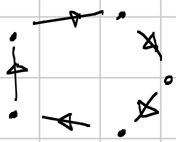
conto per vertici

$$N = \frac{12k \binom{3k+6}{2}}{\binom{12k}{2}} = P(k) + \frac{R(k)}{D(k)}$$

viene intero solo per $k = 3$

Esercitazione

20 città 18 aerei

- 
- $\forall$ città $\exists \geq 3$ aerei che la visitano

- $\forall$ arco, $\exists \leq 1$ aereo che lo percorre

Dimostrare che il grafo è connesso

Dimostrare che non potete spaccare il grafo in 2 o più componenti connesse

Altri esercizi:

P. 18 97, 104-106
alcuni punti (≥ 2) degli es. 114, 115, p. 19

- Ad uno stage prendono parte 72 stagisti. Al test ciascuno risolve almeno un esercizio. Dimostrare che $\exists$ un insieme non vuoto di problemi t.c. il numero di stagisti che li ha risolti tutti è pari

- Un quadrato 6×6 è tassellato con 2×1. Dimostrare che esiste un taglio orizz. o verticale del quadrato 6x6 che non taglia nessun 2x1

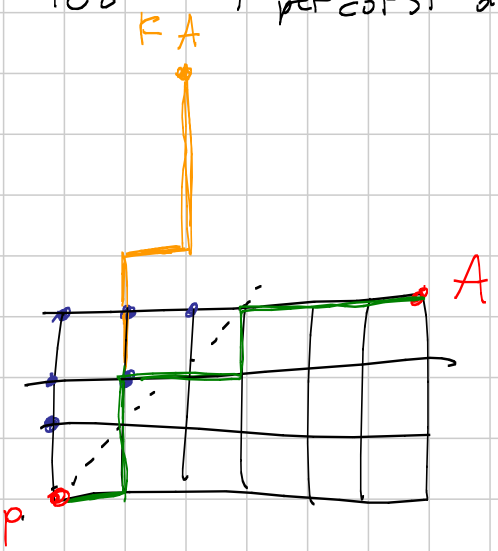
Soluzione problemi dell'esercitazione

Es 104–106

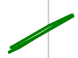
104 - 2ª parte $\qquad \#\text{modi} = \dfrac{(m+n+p)!}{m!\,n!\,p!} =: \binom{m+n+p}{m,n,p}$

105 tutti i possibili – tutti i cattivi
(passano per (5,5))

106 i percorsi da P a A senza •



Anche qui i buoni sono tutti – i cattivi

 è un cattivo

Costruisco una bigezione $f: \{\text{cattivi}\} \to \{P \to FA \text{ percorsi}\}$

Dimostro che f è una bigezione

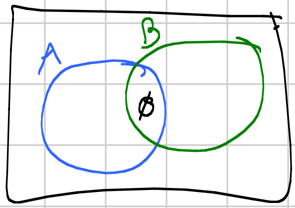
e concludo dicendo che i buoni sono

$$\binom{m+n}{n} - \binom{m+n}{n-1} \underset{?}{=} \frac{\binom{m+n}{n}}{n}$$

per casa verificatela, o confutatela

Es 114 e 115

$$\#\{(A,B)\in Y^2 : A\cap B=\emptyset\}$$



X

Conto a partire dagli elementi di X

un $x\in X$ può stare in $A\setminus B$ $\quad B\setminus A$ $\quad X\setminus A\cup B$

quindi ci sono $3^{\#X} = 3^n$

$$\sum_{(A,B,C)\in Y^3} |A\cap B\cup(X\setminus C)|$$

anche qui se conto per elemento è più facile

quante volte compare $x\in X$ nella somma?

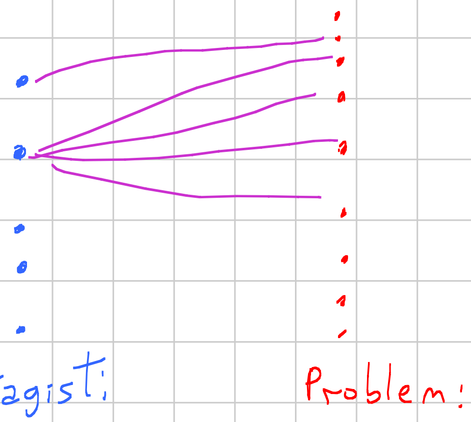
$x \in A, x \in B \quad \vee \quad x \notin C$

si sommano (p.i.e.) i 2 casi

se vogliamo calcolare il caso $x \in A$ e $x \in B$

Scegliamo A e B senza tener conto di x (4^{n-1} possibili scelte) poi metto x sia in A che in B

- Il problema degli stagisti



Scegliamo S un sottoinsieme di problemi chiamiamo n_S = # di stagisti che ha risolto tutti i problemi in S

$$Q = \sum_{S \subseteq P, S \neq \emptyset} n_S$$

Quante volte lo stagista i compare nella somma?

$$Q = \sum_{i \in O} (2^{m_i} - 1)$$ dove m_i è il # di

problemi che i ha risolto.

Per l'ipotesi ogni addendo $2^{m_i}-1$ è dispari

$\Rightarrow$ Q è pari

ma allora, almeno un S è t.c. n_S è pari.

– dal TST 15 B1

20 città con 18 aerei

Prendiamo una componente connessa C di n città e a aerei;

Q = la somma dei gradi di C

$$6n \leq Q = 2\#E_C = 2\cdot 5a = 10a$$

ogni aereo porta 5 archi alla componente C

$$\frac{Q}{2} \leq \binom{n}{2} \qquad Q \leq n(n-1)$$

$$+ \Rightarrow n(n-7) \geq 0 \Rightarrow n \geq 7$$

7	8	9	10
13	12	11	10

$m + m + m$

$6n \le 10a \qquad 3n \le 5a$

$10a \le n(n-1)$

$n=7, \quad a \geq 5 \qquad$ non torna

$n=8 \qquad a \geq 5 \qquad a \le 5$

$n=9 \qquad a \geq 6 \qquad a \le 7$

$n=10 \qquad a \geq 6 \qquad a \le 9$

Oss finale: i gradi sono pari

$\rightarrow$ fa cadere $n=8$

per $n=10 \qquad a \le 8 \quad \rightarrow$ cade (aerei ≤ 18)

$n=9$ anche $n=11$

$a=7 \qquad \rightarrow \qquad a \le 11$

cade anche $n=9$

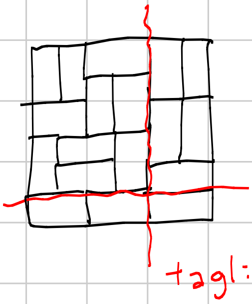
il numero di archi è $7 \cdot 5$, al max 36

$\Rightarrow$ i 2 vertici dell'arco mancante hanno grado dispari.

— 6×6 da tassellare con 2×1

$\Rightarrow$ c'è un taglio

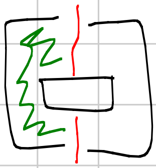
Contiamo i "blocca-tagli" $= Q$



$Q = 18$

$Q \geq 10$

Oss. finale: non posso bloccare un taglio con una sola tessera



$\rightarrow Q \geq 2 \cdot 10$

Combinatoria 2 - Basic

TESS

Titolo nota 25/08/2015

Tecniche combinatoriche

Problemi di esistenza e di non esistenza

Esistenza

Costruttiva
- mostrare l'esempio
- induzione
- algoritmi
  - uso di invarianti (false)
  - greedy

Non costruttive
- per assurdo
- pigeonhole
- principio dell'estremale

Non Esistenza

- invarianti (vere)
- colorazioni
- D - C

Invarianti

Abbiamo un sistema dinamico (che varia) a causa di mosse - cambiamenti periodici

un'invariante è una quantità legata al sistema che non varia mossa dopo mossa

Prototipo di esempio

ho un sistema, delle regole, config. iniziale A una finale B e voglio dimostrare che non posso passare da A a B

In questo caso trovo Q invariante e noto che $Q(A) \neq Q(B)$

Esempio banale:

Ho una scacchiera 8×8 bianca e nera al solito

$\boxed{\text{mosse}}$: - inverto il colore in una riga

- " " colonna
- " in un quadrato 2X2

Posso raggiungere una configurazione con tutte le caselle bianche tranne il quadratino in alto a DX?

NO, la quantità Q = la parità delle bianche

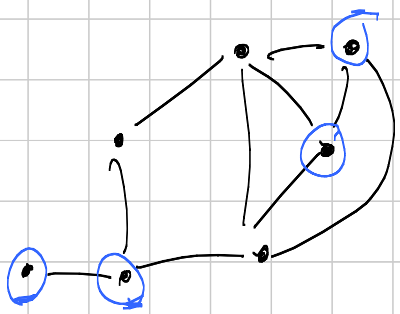
mosse: 1) prima ho b bianche e 8 - b nere

dopo ne ho 8 - b e b ✓

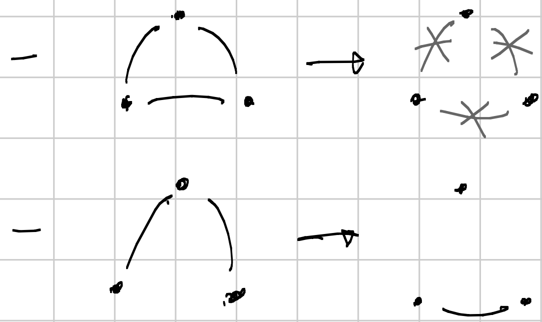
2) =

3) prima ne ho 6 branche e 4-6 nere
dopo - - - 4-6 6 ✓

C2 - 8 (dal Senior 2002)



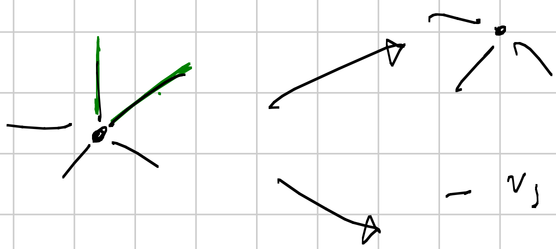
Alberto e Barbara fanno delle mosse:



Quando qualcuno non può più effettuare mosse perde

Dimostrare che l'esito non dipende dalle mosse fatte

Q. è, per ogni vertice v_i è la parità del grado



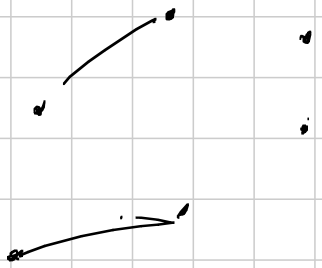
$\deg(v_i)$ cala di 2

– v_i è il vertice della V → cala di 2

– v_j non " " → non cambia

So che un config. è finale quando

$\deg(v_i) < 2 \quad \forall i$



Devo mostrare che raggiungo una conf. finale

$|E|$ diminuisce ad ogni mossa di 3 o di 1

→ osservo che la parità di $|E|$ cambia ad ogni mossa

So contare quanti archi ci saranno alla fine

saranno $\dfrac{\#\{\text{vertici con } \deg(v_i) \equiv 1 \ (2)\}}{2}$

so quanti sono all'inizio

so quanti cambiamenti di parità mi occorrono

→ so chi fa l'ultima mossa

Esercizio 118 (p.20)

a, b, c mosse sono: scelgo a, b

li sostituisco con $\frac{3a-4b}{5}, \frac{4a+3b}{5}$

L'invariante è $a^2+b^2+c^2$

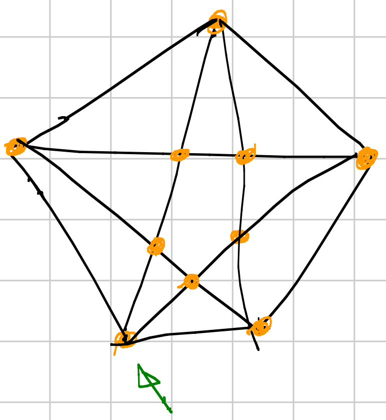
prima ho a^2+b^2

dopo ho $\frac{9a^2 - 12\cdot 2ab + 16b^2}{25} + \frac{16a^2 + 12\cdot 2ab + 9b^2}{25}$

$10, 8, 15 \longrightarrow 12, 13, 14$

$\sum \square = 389 \neq \sum \square = > 400$

Problemino



Scelgo un segmento (diagonale o lato) e cambio stato alle lampadine che trovo

Voglio spegnerle tutte

Q. = la parità delle 5 dentro

Problemino:

alla lavagna ci sono scritti alcuni numeri (interi)
ad ogni mossa posso scegliere un x e aggiungere $2x+1$

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

Ad un certo punto vedo scritto 2010

dimostrare che anche all'inizio c'era 2010

Sol: se sommo numeratore e denominatore ottengo la stessa cosa

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

$$\searrow \frac{\frac{a}{b}}{\frac{a}{b}+2} = \frac{a}{a+2b} \to 2(a+b)$$

la somma tra num e den raddoppia

se alla fine ho $\frac{2010}{1}$ la somma è dispari

Alla fine ho che la somma num + den

ottiene un 2 in più

BST 15 - B1

ci sono tanti numeri scritti su dei cartellini

ad ogni mossa posso prendere

a, b e sostituirli con i cartellini

a+b e a+b

All'inizio ci sono tutti 1

voglio dimostrare che dopo X mosse

la somma complessiva è aumentata Y volte

Uso il prodotto

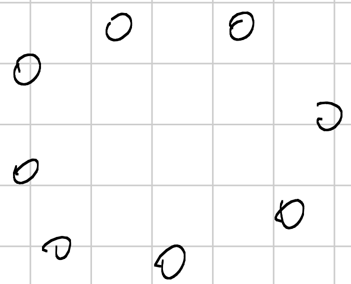
Prima è $P\,ab$, poi è $P(a+b)^2$

voglio trovare il rapporto $\frac{P(a+b)^2}{P\,ab}$ minimo

il rapporto è almeno 4

Poi stimo la somma con AM-GM

Problemino



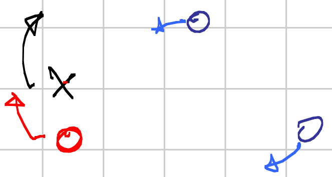
n-agono

le pile di monete sono $1, 2, 3, \dots, n$

mosse sono: scelgo 2 monete e le sposto una ↻ e una ↺

Spostare tutto su un vertice. quale?

Invariante: somma delle distanze da un vertice



Non funziona esattamente ma mi basta prendere modulo n

Principio dell'estremale

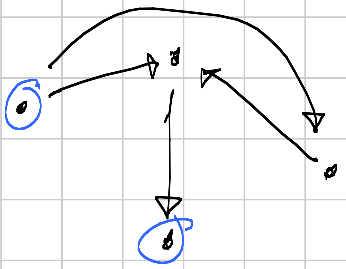
Ho tanti oggetti e ne voglio 1 che abbia una certa proprietà P

Scelgo una quantità Q associata ad ogni vertice e scelgo uno di quelli che ha Q minima o massima

Verificate che quell'oggetto verifica P

Supponendo per assurdo che non verifichi P dimostrate che potete variare di poco l'oggetto e ottenerne uno con Q più piccola o grande

Es: C2-5 (2002)

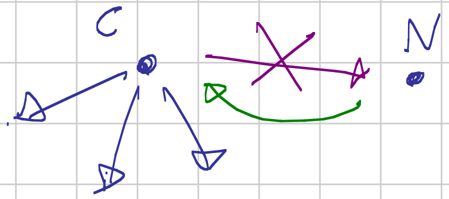


Dimostrate che esiste un vertice dal quale potete andare dovunque

(versione duale: c'è un vertice nel quale potete sempre arrivare)

Scelgo come Q il numero di città che posso raggiungere

Supponiamo x assurdo che quella con Q massimo non raggiunge tutte le altre



Da N posso raggiungere più città che non da C

Teorema di Sylvester

S è un insieme finito di punti nel piano

tale che se sceglete $p_1, p_2 \in S$ allora

$\exists\ p_3 \in S$ allineato con p_1 e p_2
(p_1, p_2, p_3 tutti diversi)

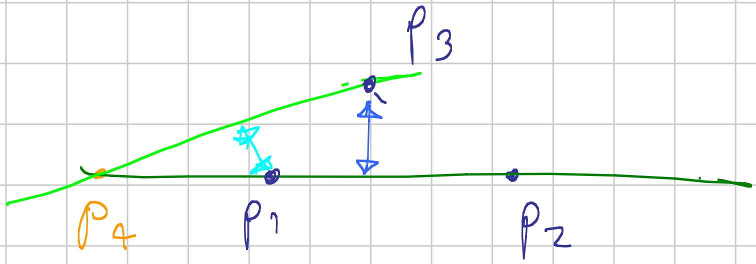
$\Rightarrow$ S è $\subseteq$ retta

Dim: prendiamo le terne (p_1, p_2, p_3)

e consideriamo $Q(p_1, p_2, p_3) =$

la distanza tra p_3 e la retta per p_1 e p_2

Prendiamo la terna che minimizza questa quantità e che sia > 0 (per assurdo)



Algoritmi greedy

Voglio costruire qualche oggetto e per farlo seguo un algoritmo

Alcune volte funziona una tecnica del tipo: adesso faccio la cosa migliore al momento

BST 2014 n°7

Ho alcuni pesi che in totale sommano a n (intero). Voglio posizionare questi pesi su k scatole in modo che su ciascuna ce ne sia ≤ 1. So che i pesi sono tutti ≤ 1. Determinare (in funzione di n) il minimo k.

Sol: se prendo tutti i pesi da $\frac{1}{2}+\varepsilon$, non posso metterne 2 nella stessa. Mi escono al massimo $2n-1$ pesi.

Speriamo che il minimo k sia $2n-1$

L'algoritmo che seguo è questo:

prendo il peso più grosso e lo metto nella scatola più vuota

Se per assurdo non riesco a finire vuol dire che mi rimane un peso p

$\Rightarrow$ in ogni scatola ho $> 1-p$

in tutto dentro le scatole ho $> (1-p)(2n-1)$

Il peso complessivo è

$$n > (1-p)(2n-1) + p$$

il peso nelle scatole — quello che mi rimane

$$p(2n-2) > n-1$$

$p > \frac{1}{2}$

Però avevo già messo $> (2n-1)\frac{1}{2}$ +

e mi rimane $> \frac{1}{2}$ =

$n > n$ Assurdo

Esercizi

P. 19, 20 116, 117, 120, 122, 123

125

P 31 15, 13

- Un grafo ha almeno un arco.
Dimostrate che è possibile dividere i vertici in 2 insiemi in modo che gli archi tra i 2 insiemi sono $\geq$ di quelli interni agli insiemi.

116 Q = parità della somma

$n \equiv 1, 2 \ (4)$

117 $Q = \sum_{i=0}^{1006} (A_{2i} - A_{2i+1})$

120 1 2 3 A_i = # pedine sul vertice i

n

$$Q = \sum_{i=0}^{n-1} i A_i \pmod n$$

122 $\dots, X, Y, \dots$ e $X > Y$

$\to Y+1, X$

$\to X-1, X$

L'idea è cercare un'invariante che cresce e mostrare che ha un tetto

$(x_1, \dots, x_n)$

$\sum_i i x_i$

x, y $y+1 \quad x$ $x-1 \quad x$

$i \quad i+1$

$ix+(i+1)y \overset{?}{\leq} i(y+1)+(i+1)x$ $i(x-1)+(i+1)x$

$y \overset{?}{\leq} i + x$

$\leq$

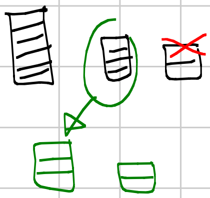
$(i+1)y \leq -i + ix + x$

$\hookrightarrow \leq (i+1)(x-1)$

$-(i+1) \overset{?}{\leq} -i$

Potevo usare dei pesi che crescevano di più

123



$$Q = \sum_i a_i^2$$

sicuramente diminuisce

$$(a+b)^2 \to a^2+b^2$$

Quante sono al max le mosse di tipo a)? $\sum a_i$

Quante sono al max le mosse di tipo b)? $\sum (a_i - 1)$

$$Q' = 2\sum a_i - \#\text{colonne}$$

Per casa 121

125 Prendo il più piccolo

$$\begin{array}{ccc} & b_1 & \\ b_4 & \boxed{a} & b_2 \\ & b_3 & \end{array}$$

$$a = \frac{b_1+b_2+b_3+b_4}{4}$$

$$a \le b_i$$

$$a \le \frac{\sum b_i}{4}$$

$$\Rightarrow a = b_i$$

ad ogni passo vedo sempre lo stesso numero

C2-15 $\quad P_n = \{ 2^n, 2^{n-1}\cdot 3, \dots, 3^n \}$

$Y \subseteq P_n \qquad S_Y$ è la somma

$\forall$ reale r : $\quad 0 \le r \le 3^{n+1} - 2^{n+1}$

$\exists\, Y$: $\quad 0 \le r - S_Y \le 2^n$

Sol: Approccio greedy

Prendo il + grande peso p tale che, detto Y l'insieme costruito al passo prec,

$S_{Y \cup \{p\}} \le r$

Perché funziona?
Supponiamo ora che rimanga con

Y t.c. $\quad S_Y \le r$, ma non $r \le 2^n + S_Y$

e che detto p il peso + piccolo rimasto

valga $\quad S_Y + p > r$

Quindi ho che $\quad 2^n + S_Y < r$

$\qquad\qquad\qquad\qquad S_Y + p > r$

$\Rightarrow \quad p > 2^n$

Avrò usato i pesi

$$\underbrace{2^n, 2^{n-1}\cdot 3, 2^{n-2}\cdot 3^2, \dots, 2^{n-r}\cdot 3^r}_{\text{blocco consecutivo di pesi che ho già preso}}, \text{ altro ma non } p$$

poi c'è p e poi ci sono gli altri.

Consideriamo ora il primo peso tra che ho usato. È vero che potevo usare p_i?

In quel caso ci stava $2^{n-i}3^i$ $\tilde{y}$

non ci stava p

però ho

$$S_{\tilde{y}} + 2^{n-i}3^i \le r$$

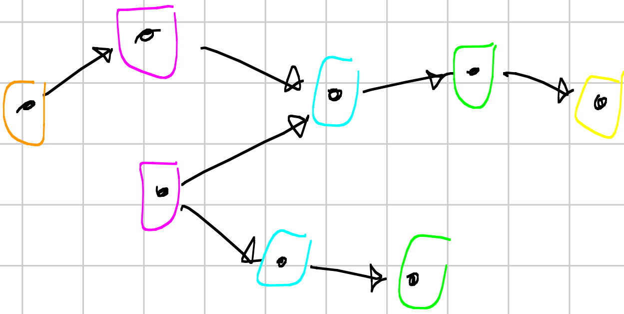
$$S_{\tilde{y}} + p > r$$

ma non si era verificato $r - S_{\tilde{y}} \le 2^n$

$$r - S_{\tilde{y}} > 2^n$$

$$S_{\tilde{y}} + 2^n < r$$

C2-13

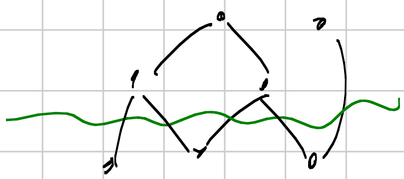


Il numero di colori è la massima lunghezza di un cammino $= h$

Induzione sul numero di vertici (di solito)
↳ stavolta su h

Prendo i vertici che non hanno alcuna uscita, li coloro con un colore e passo al grafo rimanente (ne esiste qualcuno perché è aciclico)
Sul grafo rimanente la lunghezza massima è $h-1$, per ipotesi induttiva posso colorarlo con $h-1$ colori

— (Problemino anonimo)



Scelgo la suddivisione in 2 t.c.

massimizzi il # archi tra le 2 parti

Oss: ogni vertice ha + amici dall'altra parte per ogni v_i ho a_i vertici dalla stessa parte e b_i dall'altra.

$$a_i \leq b_i$$

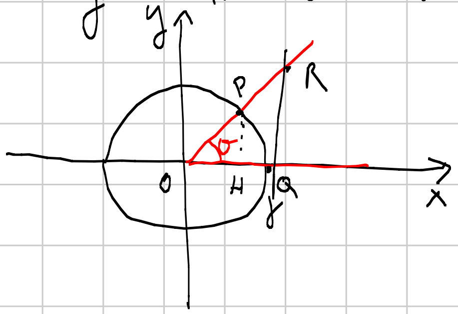
$$\sum_{i}^{n} a_i \leq \sum b_i$$

$2\#$archi interni $\leq 2\#$ archi in mezzo

G1 - basic - Senior '15 - Gioacchino

Titolo nota 22/08/2015

Consideriamo la circonferenza goniometrica: (γ)



Sia θ un angolo.

1) Misuriamo, a partire dal semiasse positivo delle x in senso antiorario, un angolo θ (es. $\theta = 30°$) e traccio una semiretta

Sia P l'int. di questa con la circ. gon.

$PH \stackrel{\text{def}}{=} \sin\theta$

$OH \stackrel{\text{def}}{=} \cos\theta$ $\rightsquigarrow P(\cos\theta, \sin\theta)$

C.1 Pitagora su $P\hat{O}H$: $PH^2 + OH^2 = 1 \to \boxed{\sin^2\theta + \cos^2\theta = 1}$

$\boxed{\text{Tg}}$ Traccio da Q la $\perp$ all'asse x. Interseca la semiretta in R.

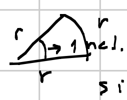
$QR \stackrel{\text{def}}{=} \tan\theta$

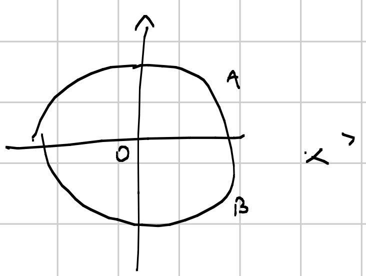
C.2 $P\hat{O}H \sim R\hat{O}Q \to \dfrac{PH}{OH} = \dfrac{QR}{OQ} \to \boxed{\dfrac{\sin\theta}{\cos\theta} = \tan\theta}$

Inciso $\pi \rightsquigarrow 180°$

$\pi : 180° =$ ang. in rad : ang. in gradi

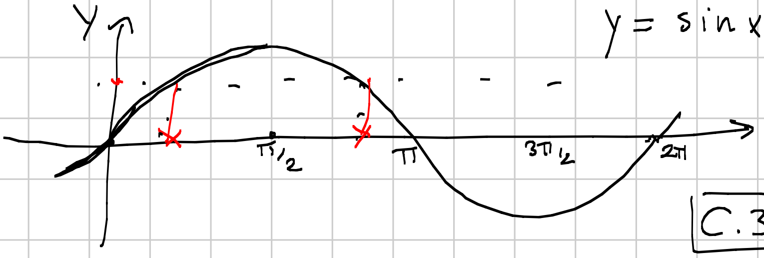
Per chi volesse ...





Angoli	sin	cos	tan
0	0	1	0
$\frac{\pi}{6}$	$\frac{1}{2}$	$\frac{\sqrt{3}}{2}$	$\frac{1}{\sqrt{3}} = \frac{\sqrt{3}}{3}$
$\pi/4$	$\sqrt{2}/2$	$\sqrt{2}/2$	1
$\pi/3$	$\sqrt{3}/2$	$1/2$	$\sqrt{3}$
$\pi/2$	1	0	n.d.

$y = \sin x$

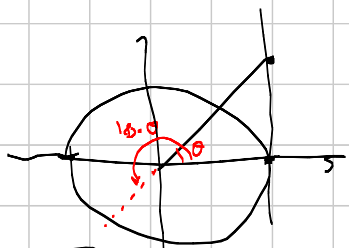


$2\pi : 360°$

$\boxed{C.3}$ Il seno ha periodicità 2π

$\sin(x+2\pi) = \sin x \quad \forall x \in \mathbb{R}$

e analogamente vale per il coseno.



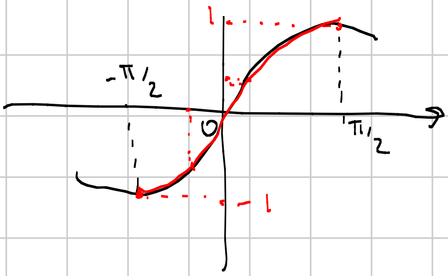
Remind: f iniettiva $\Leftrightarrow$ $f(x)=f(y) \Rightarrow x=y$

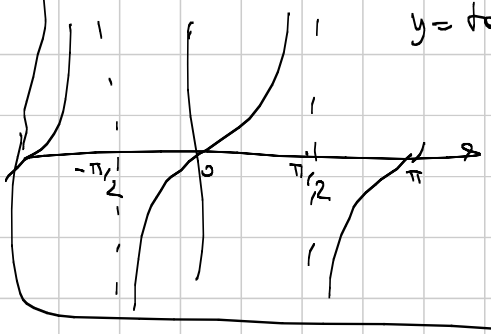
$\boxed{C.4}$ La tan ha periodicità π.

$\tan(x+\pi) = \tan x \quad \forall x \in \mathbb{R}$

Oss: sin, cos, tan non sono iniettive! (su $\mathbb{R}$...)

$y = \tan x$

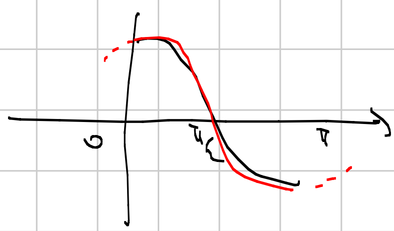




$f(x) = \sin x$ fra $-\pi/2$ e $\pi/2$ è iniettiva, quindi invertibile. La sua inversa si chiama funzione arcsin.

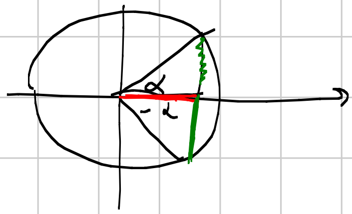
$f(x) = \cos x$ fra 0 e π è inv. La sua inversa si chiama funzione arccos.

$f(x) = \tan x$ fra $-\pi/2$ e $\pi/2$ ...



$\boxed{\text{ESERCIZIO}}$ Disegnare i grafici delle funz. inverse.

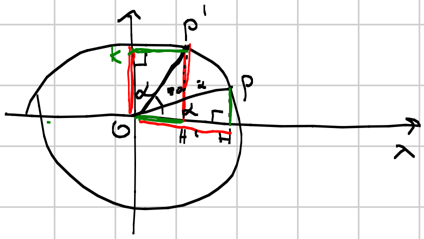
Oss. su archi associati



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

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

$\tan(-\alpha) = -\tan\alpha$



cong.

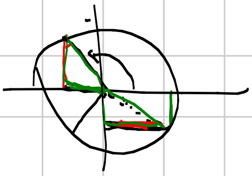
$\cos(90-\alpha) = OH' = P'K \cong PH = \sin\alpha$

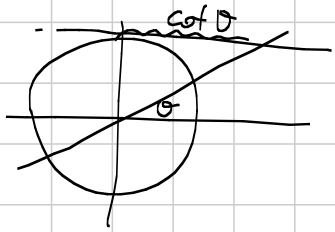
$\sin(90-\alpha) = P'H' = OK = OH = \cos\alpha$

$O\hat{K}P'$? $O\hat{H}P$

$K\hat{O}P = \alpha$

$\tan(90-\alpha) = \dfrac{\cos\alpha}{\sin\alpha} = \dfrac{1}{\tan\alpha} = \cot\alpha$





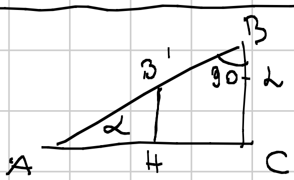
Dimostra

Esercizio Le funzioni goniometriche di $90+\alpha$, $180-\alpha$.

Rifare la dim. per $90-\alpha$ con $\alpha > 90$.

Q. Come si fa il seno di una somma.

Inciso



$AB' = 1$

$B'H = \sin\alpha$

$AH = \cos\alpha$

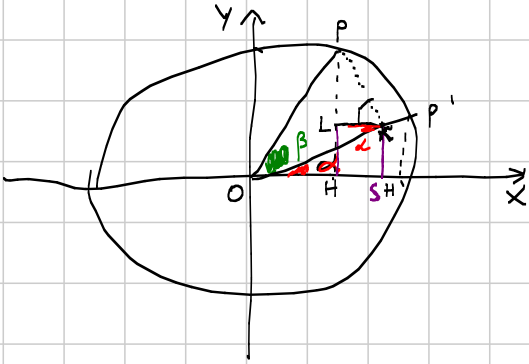
$A\hat{B}'H \sim A\hat{B}C$

$\dfrac{AB}{AB'} = \dfrac{BC}{B'H}$

$AB = \dfrac{BC}{\sin\alpha}$

$\boxed{BC = AB\sin\alpha}$

Analogamente $\boxed{AC = AB\cos\alpha}$



$$\boxed{\sin(\alpha+\beta) = \sin\alpha\cos\beta + \sin\beta\cos\alpha}$$

$$\begin{cases} PK = \sin\beta \\ OK = \cos\beta \end{cases}$$

$L\hat{K}O = \alpha$

$P\hat{K}L = 90 - \alpha$

$PL = PK\sin(90-\alpha) = \sin\beta\cos\alpha$

nel tr. $P\hat{L}K$

lmkôs ...

Si ma ha $\boxed{LH = \sin\alpha\cos\beta}$

$\sin(\alpha+\beta)$

$\parallel$

$$PH = PL + LH = \sin\beta\cos\alpha + \sin\alpha\cos\beta$$

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

$$\cos(\alpha+\beta) \overset{?}{=} \sin(90-(\alpha+\beta)) = \sin((90-\alpha)-\beta) =$$
$$= \sin(90-\alpha)\cos\beta - \sin\beta\cos(90-\alpha)$$
$$= \cos\alpha\cos\beta - \sin\beta\sin\alpha$$

$$\cos(\alpha-\beta) = \dots \quad = \cos\alpha\cos\beta + \sin\beta\sin\alpha$$

$\boxed{\text{Esercizio: } \tan(\alpha+\beta) = ?}$

DUPLICAZIONE

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

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

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

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

In conclusione

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

$$\tan 2\alpha = \frac{2\tan\alpha}{\tan^2\alpha + 1}$$

BISEZIONE

$\sin\frac{\alpha}{2}$, $\cos\frac{\alpha}{2}$

Le ricaviamo da

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

$$\alpha \to \alpha/2$$

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

$$\sin^2 \alpha/2 = \frac{1-\cos\alpha}{2} \quad ! \quad \sin \alpha/2 = \pm\sqrt{\frac{1-\cos\alpha}{2}}$$

In un triangolo $\oplus$

$$\cos 2\alpha = 2\cos^2\alpha - 1$$

$$\alpha \to \alpha/2$$

$$\vdots$$

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

$$\tan\frac{\alpha}{2} \overset{\text{def}}{=} \frac{\sin\frac{\alpha}{2}}{\cos\frac{\alpha}{2}} = \frac{2\sin\alpha/2 \cdot \sin\alpha/2}{2\sin\alpha/2 \cdot \cos\alpha/2} = \frac{1-\cos\alpha}{\sin\alpha}$$

$$\| $$

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

Parametriche

Idea: Esprimere seno e coseno in funzione di $\tan \alpha/2$.

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

$s = \sin\alpha$

$c = \cos\alpha$

$$= \quad t = \frac{1-c}{s} \quad (1) \qquad \alpha \neq 0, 180°$$

$$= \quad t = \frac{s}{1+c} \quad (2)$$

$(1)\cdot s \qquad st = 1 - c$

$$\boxed{c = 1 - st} \quad (3)$$

$(2)\cdot(1+c) \qquad t + tc = s$

Uso la (3) $\qquad t + t(1-st) = s$

$$2t - st^2 = s$$

$$2t = st^2 + s = s(t^2+1)$$

$$\boxed{s = \frac{2t}{t^2+1}}$$

Dalla 3 $\qquad c = 1 - \frac{2t}{t^2+1}\cdot t = \frac{t^2+1-2t^2}{t^2+1} = \boxed{\frac{1-t^2}{1+t^2}}$

Quindi $\sin\alpha = \dfrac{2\tan\alpha/2}{\tan^2\alpha/2 + 1}$

$\cos\alpha = \dfrac{1-\tan^2\alpha/2}{1+\tan^2\alpha/2}$

Esercizio: controlla il c.d.e. per ogni formula...

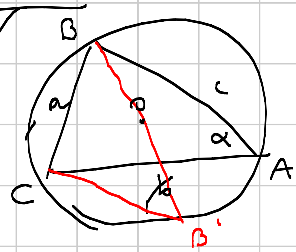
Prostaferesi, Werner (Es. 8 pagina 3)

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

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

Trigonometria

Th. 1



Triangolo A, B, C

a, b, c i lati opposti ad A, B, C

R il raggio della cfr. circoscritta

r il " " " inscritta

α, β, γ gli angoli in A, B, C

Teorema della corda (seni): In un triangolo

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

D.m. $BB' = 2R$

$B\hat{C}B' = 90°$

$BC = BB' \cdot \sin B\hat{B}'C =$

$= BB' \cdot \sin\alpha$

$\downarrow$

$a = 2R \cdot \sin\alpha$

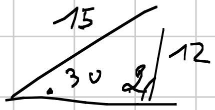
$\dfrac{a}{\sin\alpha} = 2R$ ∎

Cor.

Seni: In un triangolo il rapporto fra un lato

e il seno dell'angolo opposto è costante
(= 2R)

Es.



$$\frac{15}{\sin\alpha} = \frac{12}{\sin 30} = 24$$

$$\sin\alpha = \frac{15}{24} = \frac{5}{8}$$

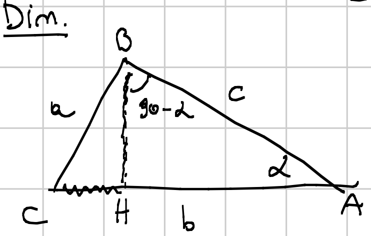
Th. di Carnot (coseni)

$$\to \cos\alpha = \frac{b^2+c^2-a^2}{2bc}$$

$$\cos\beta = \frac{a^2+c^2-b^2}{2ac}$$

$$\cos\gamma = \frac{b^2+a^2-c^2}{2ab}$$

Dim.



$AH = AB\cos\alpha = c\cos\alpha$

$BH = c\sin\alpha$

$CH = AC - AH = b - c\cos\alpha$

Scrivo Pitagora in $B\hat{C}H$

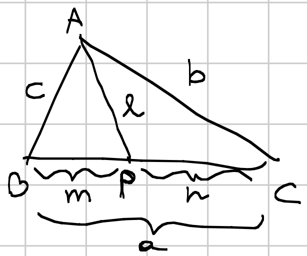
$$BC^2 = CH^2 + BH^2 = (b - c\cos\alpha)^2 + (c\sin\alpha)^2 =$$

$$a^2 = \quad '' \quad = b^2 - 2bc\cos\alpha + \underbrace{c^2\cos^2\alpha + c^2\sin^2\alpha} =$$

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

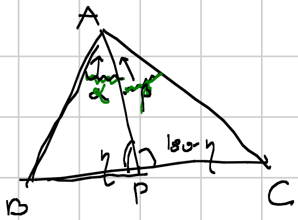
$$\cancel{2b}c\cos\alpha = \frac{b^2+c^2-a^2}{2bc} \quad \blacksquare$$

Th. Stewart (Es. 9 pagina 3)



$$b^2 m + c^2 n = a(l^2 + mn)$$

Es. Dim. Stewart.
e ricava la lungh. della mediana $\left(= \sqrt{\frac{2(b^2+c^2)-a^2}{4}}\right)$
e bisettrice



Oss.

Th. dei seni su $A\hat{B}P$

$$\frac{AB}{\sin\eta} = \frac{BP}{\sin\alpha} \qquad (1)$$

$\sin(180-\eta)=\sin\eta$
$\cos(180-\eta)=-\cos\eta$

Th. dei seni su $A\hat{P}C$

$$\frac{AC}{\sin(180-\eta)} = \frac{AC}{\sin\eta} = \frac{PC}{\sin\beta} \qquad (2)$$

Divido (1)/(2)

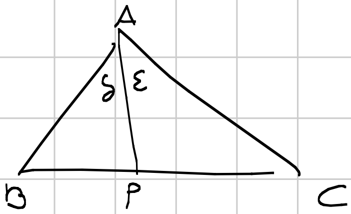
$$\frac{AB/\cancel{\sin\eta}}{AC/\sin\eta} = \frac{BP/\sin\alpha}{PC/\sin\beta}$$

$$\frac{AB}{AC} = \frac{BP}{PC}\,\frac{\sin\beta}{\sin\alpha}$$

$$\frac{BP}{PC} = \frac{c}{b}\,\frac{\sin\alpha}{\sin\beta}$$

Attenzione! α e β non in not. standard! Sono gli angoli staccati dalla ceviana

Th.



$$\boxed{\frac{BP}{PC} = \frac{c}{b}\,\frac{\sin\delta}{\sin\varepsilon}}$$

Es 3 pag. 3

$$1-\cot 23 \overset{?}{=} \frac{2}{1-\cot 22}$$

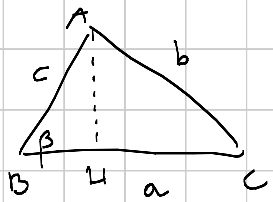
$$\frac{\sin 23-\cos 23}{\sin 23} \overset{?}{=} \frac{2\sin 22}{\sin 22-\cos 22}$$

$$\cancel{\sin 23\sin 22} - \sin 23\cos 22 - \cos 23\sin 22 + \cos 22\cos 23 \overset{?}{=} \cancel{2}\sin 22\sin 23$$

$$\cos 22\cos 23 - \sin 22\sin 23 \overset{?}{=} \sin 23\cos 22 + \sin 22\cos 23$$

$$\cos 45 \overset{!}{=} \sin 45$$

Area di un triangolo



S , A

$$S = \frac{BC \cdot AH}{2} = \frac{ac \sin\beta}{2}$$

$$S = \frac{1}{2} ac \sin\beta$$

$$\frac{1}{2} ab \sin\gamma$$

$$\frac{1}{2} bc \sin\alpha$$

A parole: L'area è il $\frac{1}{2}$ prodotto fra due lati e il seno dell'angolo compreso fra loro.

$$S = \frac{1}{2} ac \sin\beta$$

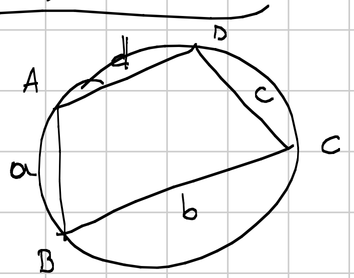
$$\frac{b}{\sin\beta} = 2R \qquad \sin\beta = \frac{b}{2R}$$

$$\frac{1}{2} ac \frac{b}{2R} = \frac{abc}{4R}$$

$$S = \frac{abc}{4R} \longrightarrow R = \frac{abc}{4S}$$

$\boxed{\text{Es.}}$

Gener. Erone



Brahamagupta

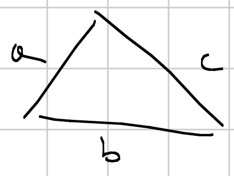
$$s = \frac{a+b+c+d}{2}$$

$$S = \sqrt{(s-a)(s-b)(s-c)(s-d)}$$

$$d \to 0$$

$$s = \frac{a+b+c}{2}$$

Erone



$$p = \frac{a+b+c}{2}$$

$$S = \sqrt{p(p-a)(p-b)(p-c)}$$

NUMERI COMPLESSI

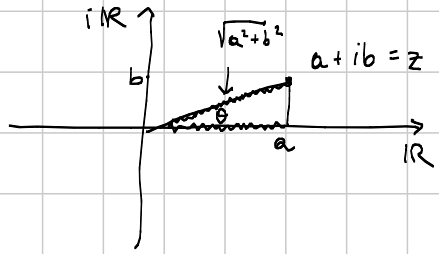
$\boxed{z = a + bi}$ $\qquad i^2 = -1$

$a \in \mathbb{R}$ parte reale, $b \in \mathbb{R}$ parte immaginaria

SOMMA $\quad a+bi+c+di = (a+c)+(b+d)i$

PRODOTTO $\quad (a+bi)(c+di) = ac+adi+bci-bd = (ac-bd)+(ad+bc)i$

Rapp. sul piano di Gauss.



RAPP. POLARE $\quad a+bi = \sqrt{a^2+b^2}\left(\frac{a}{\sqrt{a^2+b^2}} + \frac{b}{\sqrt{a^2+b^2}}i\right)$

$\qquad (\cos\theta + \sin\theta\, i)$

NORMA DI z

$|z| = \rho = \sqrt{a^2+b^2}$ MODULO del N. COMPLESSO

θ = argomento

$e = 2{,}78\ldots$

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

e^x

cos

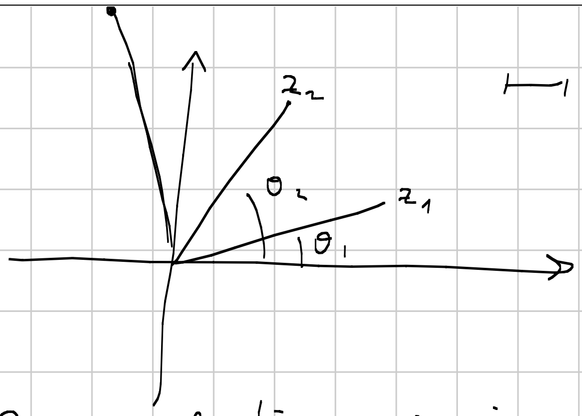
sin

$z_1 = \rho_1 e^{i\theta_1}$

$z_2 = \rho_2 e^{i\theta_2}$

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

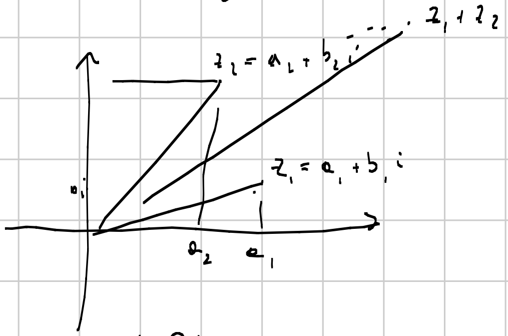
$z_1 z_2$



Cosa vuol dire, sul piano di Gauß moltiplicare per un numero complesso z

= ROTOMOTETIA ↗ di ragione $|z|$ (ρ)

↓ dell'argomento di z



Somma = Regola del parallelogramma

DE-MOIVRE

$\cos 2\alpha = \cos^2\alpha - \sin^2\alpha$ $\qquad$ $\sin 2\alpha = 2\sin\alpha\cos\alpha$

$\cos 3\alpha = ?$ $\qquad$ $\sin 3\alpha = ?$

$\vdots$

$\cos n\alpha = ?$ $\qquad$ $\sin n\alpha = ?$

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

$$z^n = e^{i\underbrace{n\theta}} \overset{\downarrow}{=} \cos(n\theta) + i\sin(n\theta) \quad \downarrow$$

$$z^n = (\cos\theta + i\sin\theta)^n = \sum_{k=0}^{n} \binom{n}{k} \cos^{n-k}\theta\,(i\sin\theta)^{k}$$

$$= \underline{\underline{A}} + iB \quad \downarrow$$

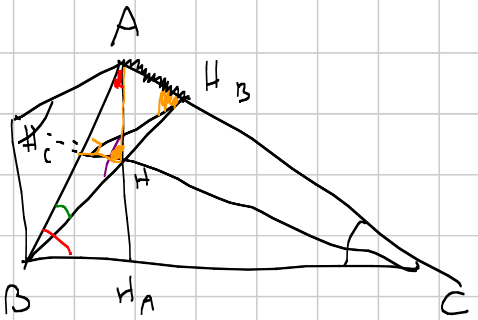
$$\cos(n\theta) = \binom{n}{0}\cos^n\theta - \binom{n}{2}\cos^{n-2}\theta\sin^2\theta + \dots$$

$$\sin(n\theta) = \binom{n}{1}\cos^{n-1}\theta\sin\theta - \binom{n}{3}\cos^{n-3}\theta\sin^3\theta - \dots$$

Pag. 3 7 - 8 - 9 - 10 (B rettangolo)

Pag. 32 10 - 11 - 13 (1 - 5) - 14 (1 - 3 - 6 - 8)

?



AH

$$\begin{cases} A\hat{H}B \\ B\hat{A}H = 90 - \beta \\ A\hat{B}H = 90 - \alpha \\ A\hat{H}B = \alpha + \beta = 180 - \gamma \end{cases}$$

Seni: $\dfrac{AH}{\sin(90-\alpha)} = \dfrac{AB}{\sin(180-\gamma)}$

$$AH = \frac{c\cos\alpha}{\sin\gamma} = 2R\cos\alpha$$

H_BH_C

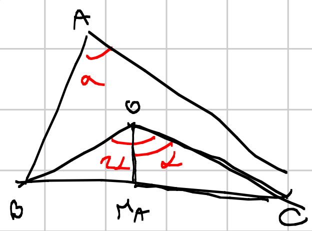
$$\begin{cases} A\hat{H}_BH_C \\ A\hat{H}_BH_C = \beta \\ A\hat{H}_CH_B = \gamma \end{cases}$$

$A\hat{H}_BH_C = A\hat{H}H_C = \beta$ perché AH_CHH_B è un quad. ciclico

Seni: $\dfrac{AH_B}{\sin A\hat{H}_CH_B} = \dfrac{H_BH_C}{\sin\alpha} \rightarrow H_BH_C = \dfrac{AH_B\sin\alpha}{\sin\gamma}$

Ma $AH_B = c\cos\alpha \rightarrow H_BH_C = \dfrac{c\cos\alpha\sin\alpha}{\sin\gamma} = 2R\cos\alpha\sin\alpha = R\sin 2\alpha$

OM_A



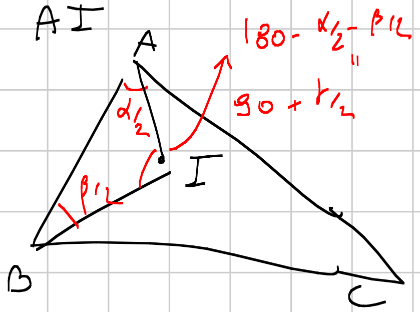
$O\hat{M}_A C$

Dicono $\sqrt{R^2 - \frac{a^2}{4}}$

$OM_A = R\cos\alpha$ (la metà di AH..)

$OM_A = \frac{AH}{2}$

AI



$\alpha/2 + \beta/2 + \gamma/2 = 90$

$A\hat{B}I$

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

$$\frac{AI}{\sin\beta/2} = \frac{AB}{\sin(90+\gamma/2)} = \frac{AB}{\cos\gamma/2}$$

$$AI = \frac{c\sin\beta/2}{\cos\gamma/2} = \frac{2c\sin\beta/2\,\sin\gamma/2}{\sin\gamma}$$

$$= 4R\sin\beta/2\,\sin\gamma/2$$

G3 + Pow $\longrightarrow$ OI

$$OI^2 = R^2 - 2Rr.$$

Es. 8

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

Verifica diretta

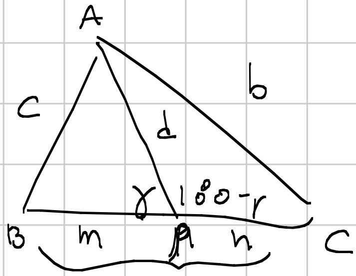
$$\sin\alpha + \sin\beta = 2\sin\frac{\alpha+\beta}{2}\cos\frac{\alpha-\beta}{2}$$

$\alpha + \beta = p$ $\qquad \alpha = \frac{p+q}{2}$

$\alpha - \beta = q$ $\qquad \beta = \frac{p-q}{2}$

$$2\sin\frac{p+q}{2}\cos\frac{p-q}{2} = \frac{1}{\cancel{2}}(\sin p + \sin q)$$

Es. 9 Stewart



$$man + dad = bmb + cnc$$

$$a(mn + d^2) = b^2 m + c^2 n$$

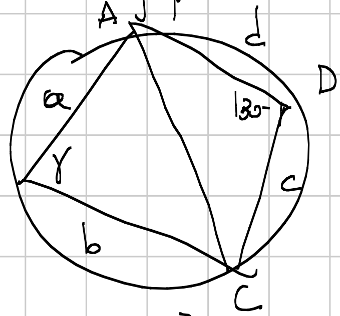
Idea: $c^2 = d^2 + m^2 - 2md\cos\gamma$

$b^2 = d^2 + n^2 + 2nd\cos\gamma$

Sostituisco e viene.

Es 5.10 gen.

Brahamagupta



$$S = \sqrt{(s-a)(s-b)(s-c)(s-d)}$$

$$AC^2 = a^2 + b^2 - 2ab\cos\gamma$$

$$\| $$

$$d^2 + c^2 + 2dc\cos\gamma$$

$$a^2 + b^2 - 2ab\cos\gamma = d^2 + c^2 + 2dc\cos\gamma$$

$$\cos\gamma = \frac{a^2+b^2-c^2-d^2}{2(ab+cd)}$$

[ABC] [ADC]

$$S = \frac{1}{2}ab\sin\gamma + \frac{1}{2}cd\underbrace{\sin(180-\gamma)}_{\sin\gamma} =$$

$$= \frac{1}{2}(ab+cd)\sin\gamma$$

$$\sin^2\gamma = 1 - \cos^2\gamma = 1 - \frac{(a^2+b^2-c^2-d^2)^2}{4(ab+cd)^2} =$$

$$= \frac{[2(ab+cd)]^2 - (a^2+b^2-c^2-d^2)^2}{4(ab+cd)^2} =$$

$$= \frac{(\underbrace{a^2+2ab+b^2}-\underbrace{c^2+2cd-d^2})(c^2+d^2+2cd-a^2-b^2+2ab)}{4(ab+cd)^2} =$$

$$= \frac{[(a+b)^2-(c-d)^2][(c+d)^2-(a-b)^2]}{4(ab+cd)^2} =$$

$$= \frac{(a+b+c-d)(a+b-c+d)(c+d+a-b)(c+d+b-a)}{4(ab+cd)^2} =$$

$$s - d = \frac{a+b+c+d}{2} - d = \frac{a+b+c-d}{2}$$

$$= \frac{\cancel{4}(s-d)(s-c)(s-b)(s-a)}{(ab+cd)^2}$$

$$\sin\gamma = \frac{2\sqrt{(s-d)(s-c)(s-b)(s-a)}}{(ab+cd)}$$

Quindi $S = \frac{1}{\cancel{2}}\cancel{(ab+cd)}\frac{\cancel{2}\sqrt{(s-a)(s-b)(s-c)(s-d)}}{\cancel{(ab+cd)}}$

$$= \sqrt{(s-a)(s-b)(s-c)(s-d)}$$

E come $S = \sqrt{p(p-a)(p-b)(p-c)}$

Tropolo $16S^2 = -a^4 - b^4 - c^4 + 2a^2b^2 + 2b^2c^2 + 2c^2a^2$

Es. 13

$\{ r = 4R\sin\frac{\alpha}{2}\sin\frac{\beta}{2}\sin\frac{\gamma}{2}$

$$\sin^2\frac{\alpha}{2} = \frac{1-\cos\alpha}{2} = \frac{1-\frac{b^2+c^2-a^2}{2bc}}{2} = \frac{2bc+a^2-b^2-c^2}{4bc} =$$

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

$$= \frac{(a+b-c)(a+c-b)}{4bc} =$$

$$= \frac{\cancel{2}(p-c)\cancel{2}(p-b)}{\cancel{4}bc} =$$

$$= \frac{(p-c)(p-b)}{bc}$$

$$p = \frac{a+b+c}{2}$$

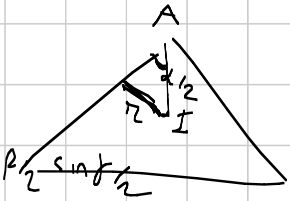
$$p-c = \frac{a+b+c}{2} - c = \frac{a+b-c}{2}$$

$$\sin\frac{\alpha}{2} = \sqrt{\frac{(p-c)(p-b)}{bc}} \qquad \sin\frac{\beta}{2} = \sqrt{\frac{(p-a)(p-c)}{ac}}$$

$$4R\sin\frac{\alpha}{2}\sin\frac{\beta}{2}\sin\frac{\gamma}{2} = 4R\sqrt{\frac{(p-c)(p-b)}{bc}}\sqrt{\frac{(p-a)(p-c)}{ac}}\sqrt{\frac{(p-b)(p-a)}{ab}}$$

$$= 4R\frac{(p-a)(p-b)(p-c)}{abc} =$$

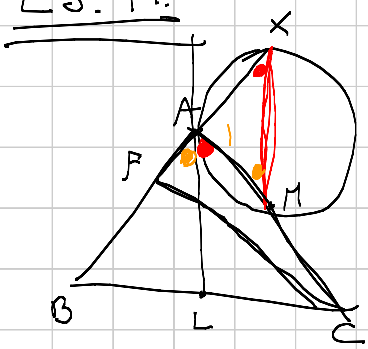
$$= \cancel{4R}\,\frac{S^2}{\cancel{(P)abc}} = \frac{S}{p} = r$$



$$AI = 4R \sin\frac{\beta}{2}\sin\frac{\gamma}{2}$$

$$r = AI \cdot \sin\frac{\alpha}{2} = 4R\sin\alpha/2\,\sin\beta/2\,\sin\gamma/2$$

ES. 11.



Minimizzare $\frac{BX}{CF}$

$L\hat{A}M = A\hat{X}M$

perché insistono su $\overset{\frown}{AM}$

$X\hat{M}A = B\hat{A}L$

in $A\hat{X}M$

$$\frac{AX}{\sin\color{orange}{\bullet}} = \frac{AM}{\sin\color{red}{\bullet}}$$

$$AX = \frac{b}{2}\,\frac{\sin\color{orange}{\bullet}}{\sin\color{red}{\bullet}} = \frac{b^2}{2c}$$

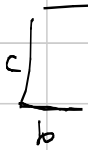
$\frac{\sin\color{orange}{\bullet}}{\sin\color{red}{\bullet}} = \frac{b}{c}$ Usando la formula che vi ho dato.

$$BX = AB + AX = c + \frac{b^2}{2c} = \frac{2c^2+b^2}{2c}$$

$$CF = b\sin\alpha$$

Infine $\frac{BX}{CF} = \frac{b^2+2c^2}{2bc\sin\alpha}$

$\alpha = \pi/2$ (90) perché in questo modo $\frac{1}{\sin\alpha}$ è minimo.



$$\frac{b^2+2c^2}{2bc} \geq \sqrt{2}$$

$$b^2 - 2\sqrt{2}bc + 2c^2 \geq 0$$

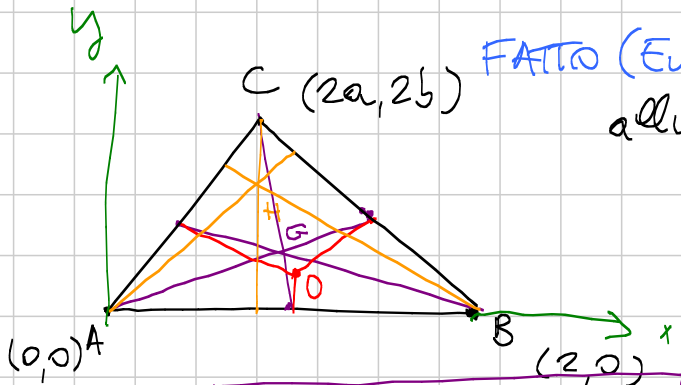
$$(b-\sqrt{2}c)^2 \geq 0$$

se $b - \sqrt{2}c = 0$

L'uguaglianza si ha se $\alpha = 90°$, $b/c = \sqrt{2}$.

Geometria 2

Titolo nota 24/08/2015



FATTO (Eulero) H, G, O allineati.

$$\boxed{G \equiv \left(\frac{2}{3}(a+1), \frac{2}{3}b\right)}$$

H sta su h_C $\qquad x_H = x_C = 2a$

retta AC $\qquad y = \frac{b}{a}x$

H sta su h_B $\qquad y_H = -\frac{a}{b}x_H + \frac{2a}{b}$

$$\boxed{H \equiv \left(2a, -\frac{2a^2}{b} + \frac{2a}{b}\right)}$$

O sta sull'asse di AB $\rightarrow$ $x_O = 1$

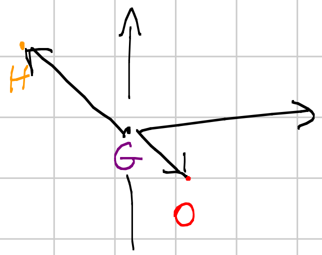
O sta sull'asse di AC $\rightarrow$ $y_O = -\frac{a}{b}x_O + \frac{a^2}{b} + b$

$$\boxed{O \equiv \left(1, -\frac{a}{b} + \frac{a^2}{b} + b\right) \equiv \left(1, \frac{a(a-1)}{b} + b\right)}$$

concludere: allineamento!

$$\frac{x_O - x_G}{y_O - y_G} = \frac{x_H - x_G}{y_H - y_G}$$

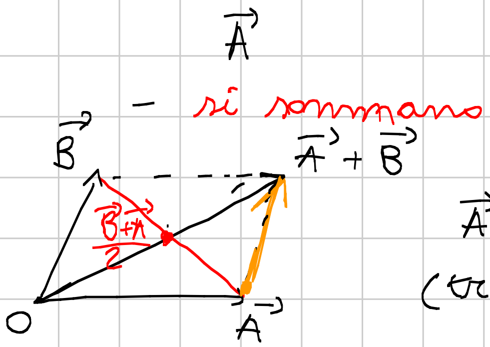
$$\frac{-\frac{2}{3}a + \frac{1}{3}}{\frac{a(a-1)}{b} + \frac{1}{3}b} \boxed{\overset{?}{=}} \frac{\frac{4}{3}a - \frac{2}{3}}{-\frac{2a(a-1)}{b} - \frac{2}{3}b}$$



$$x_H = -2x_O$$
$$y_H = -2y_O$$

VETTORI

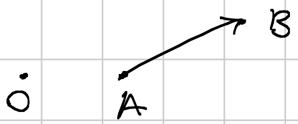
- si moltiplicano per scalari
- si sommano



$\vec A + \vec B$ (traslazione)

→ PTO MEDIO di A e B $\quad \dfrac{\vec A + \vec B}{2}$

→ retta per A e B

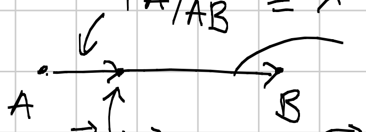


$(\vec B - \vec A)\lambda + \vec A \qquad \lambda \vec B + (1-\lambda)\vec A$

→ segmento per A, B $\quad \lambda \in [0, 1]$

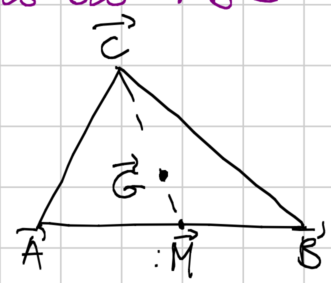
$\overline{PA}/\overline{AB} = \lambda$

$(1-\lambda)\overline{AB}$



$\vec P = \lambda \vec B + (1-\lambda)\vec A$

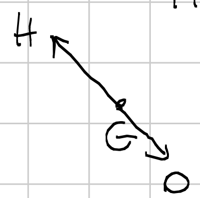
Baricentro di ABC



$$\vec M = \frac{\vec A + \vec B}{2}$$

$$\vec G = \frac{1}{3}\vec C + \frac{2}{3}\vec M = \frac{\vec A + \vec B + \vec C}{3}$$

Ortocentro di ABC



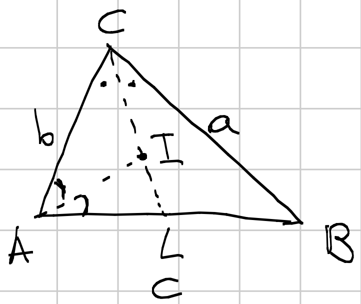
$$\vec{H} - \vec{G} = -2(\vec{O} - \vec{G})$$

$$\vec{H} = 3\vec{G} - 2\vec{O} = \vec{A} + \vec{B} + \vec{C} - 2\vec{O}$$

se metto l'origine in O

$$\vec{H} = \vec{A} + \vec{B} + \vec{C}$$

Incentro di ABC



$$\vec{L} = \lambda\vec{A} + (1-\lambda)\vec{B}$$

$$\lambda = \frac{BL}{AB} = \frac{BC}{BC+AC} = \frac{a}{a+b}$$

$$\vec{L} = \frac{a}{a+b}\vec{A} + \frac{b}{a+b}\vec{B}$$

Teorema della bisettrice su ALC

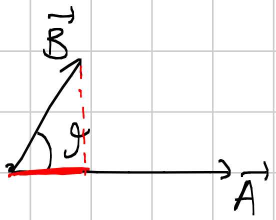
$$\frac{IL}{CL} = \frac{AL}{AL+AC} = \frac{c \cdot \frac{b}{a+b}}{\frac{cb}{a+b} + b} = \frac{c\cancel{b}}{c\cancel{b} + a\cancel{b} + b^{\cancel{2}}} =$$

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

$$\vec{I} = \frac{\vec{C} \cdot c}{a+b+c} + \vec{L}\,\frac{b+c}{a+b+c} = \frac{a\vec{A} + b\vec{B} + c\vec{C}}{a+b+c}$$

i vettori ...

hanno il PRODOTTO SCALARE



$$\langle \vec{A}, \vec{B} \rangle = |A||B| \cos\vartheta$$

se A, B allineati

$$\langle \vec{A}, \vec{B} \rangle = |A||B| \quad (\langle \vec{A}, \vec{A} \rangle = |A|^2)$$

se $\vec{A} \perp \vec{B}$

$\langle \lambda \vec{A}, \vec{B} \rangle = \lambda \langle \vec{A}, \vec{B} \rangle \qquad \langle \vec{A}, \vec{B} \rangle = 0$

$\langle (x_A, y_A), (x_B, y_B) \rangle = x_A x_B + y_A y_B$

$|\langle \vec{A}, \vec{B} \rangle| \le |\vec{A}|\,|\vec{B}|$ CS

esercizio

$\vec{H} = \vec{A} + \vec{B} + \vec{C}$ (origine è in O)

(era vero??)

$$\langle \vec{B} - \vec{A}, \vec{H} - \vec{C} \rangle = \langle \vec{B} - \vec{A}, \vec{A} + \vec{B} \rangle =$$

$$= \cancel{\langle \vec{B}, \vec{A} \rangle} + \langle \vec{B}, \vec{B} \rangle - \langle \vec{A}, \vec{A} \rangle - \cancel{\langle \vec{A}, \vec{B} \rangle}$$

$$= R^2 - R^2 = 0$$

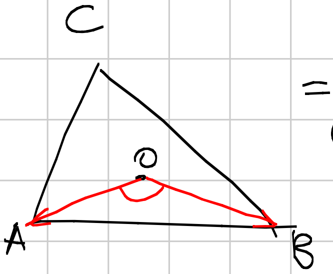
$\overline{OI}^2$ in funzione di r, R — metto l'origine in O

$$\left\langle \frac{a\vec{A} + b\vec{B} + c\vec{C}}{a+b+c}, \text{''} \right\rangle =$$

$$= \frac{1}{(2p)^2} \langle a\vec{A} + b\vec{B} + c\vec{C}, a\vec{A} + b\vec{B} + c\vec{C} \rangle$$

$$= \frac{1}{(2p)^2} \Big[\sum_{cyc} a^2 \underbrace{\langle \vec{A}, \vec{A} \rangle}_{R^2} + \sum_{cyc} 2ab \langle \vec{A}, \vec{B} \rangle \Big] =$$

$$\sum_{cyc} 2ab R^2 \cos 2\gamma =$$



$$= \frac{R^2}{(2p)^2} \Big[\sum_{cyc} a^2 + \sum_{cyc} 2ab - \sum_{cyc} 4ab\,\mathrm{sen}^2\gamma \Big]$$

$\cos 2\gamma = \cos^2\gamma - \mathrm{sen}^2\gamma = 1 - 2\,\mathrm{sen}^2\gamma$

$$= \frac{R^2}{\cancel{(2p)^2}} \cancel{(2p)^2} - \frac{4R^2}{(2p)^2} 2S \sum_{cyc} \mathrm{sen} A =$$

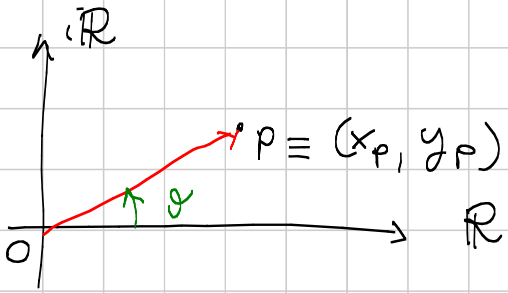
$$= R^2 - \frac{4R^{\cancel{2}}\cancel{2}S}{(2p)^2}(a+b+c) =$$

$$= R^2 - \frac{4RS}{2p} = R^2 - 2Rr$$

$$= R(R-2r)$$

BONUS: $R \geq 2r$

NUMERI COMPLESSI



$$p = x_p + i y_p = |p|\, e^{i\vartheta}$$

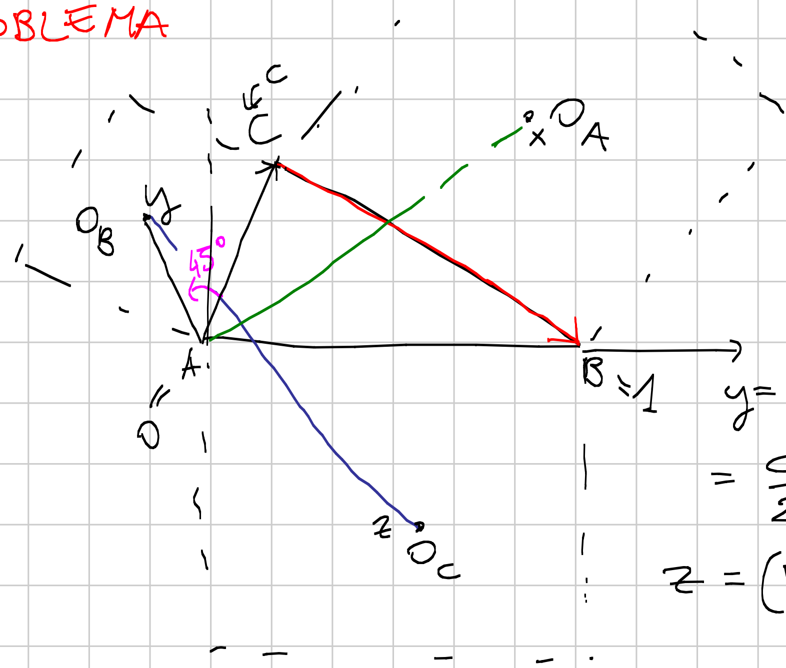
- si sommano (esattamente come vettori/pti in coordinate)
- si moltiplicano "per scalari" (per numeri reali)
- si moltiplicano

$$x = |x|\, e^{i\vartheta} \qquad y = |y|\, e^{i\varphi}$$

$$xy = |x||y|\, e^{i(\vartheta+\varphi)}$$

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

PROBLEMA



$$y = c\cdot\left(\frac{\sqrt2}{2} + \frac{i\sqrt2}{2}\right)\frac{\sqrt2}{2} = \frac{c}{2}(1+i)$$

$$z = \left(\frac{\sqrt2}{2} - \frac{i\sqrt2}{2}\right)\frac{\sqrt2}{2} = \frac{1}{2}(1-i)$$

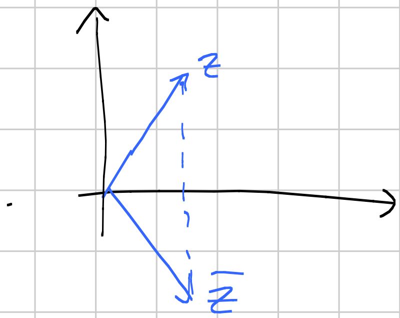
$$x = (1-c)\left(\frac{\sqrt2}{2} + \frac{i\sqrt2}{2}\right)\frac{\sqrt2}{2} + c = \frac{(1-c)(1+i)+2c}{2} = \frac{(1+c)}{2} + \frac{i}{2}(1-c)$$

$$z - y = \frac{(1-c)}{2} + \frac{1}{2}(-1-c)i$$

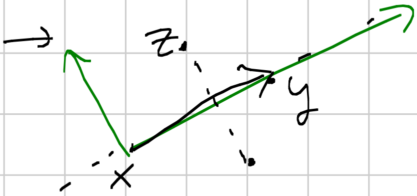
$$i(z-y) = \frac{1}{2}(1+c) + i\frac{(1-c)}{2} = x$$

$AO_A \perp O_BO_C \to$ altezze $\to$ concorrono...

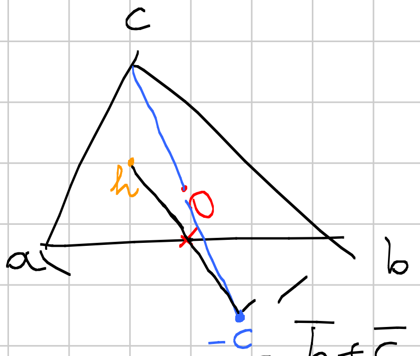
numero complesso z



$$z = a + ib$$
$$\bar z = a - ib$$
$$\operatorname{Re} z = \frac{z+\bar z}{2} \qquad |z|^2 = z\bar z$$
$$\operatorname{Im} z = \frac{z-\bar z}{2}$$



$$\frac{1}{2} z + \frac{1}{2}\left[\overline{\left(\frac{z-x}{y-x}\right)}(y-x)+x\right]$$



$h=a+b+c$

$a\bar a = b\bar b = c\bar c = 1$

$$\overline{\left(\frac{\cancel{a}+b+c-\cancel{a}}{b-a}\right)}\cdot(b-a)+a$$

$$= \frac{\bar b+\bar c}{\bar b-\bar a}(b-a)+a =$$

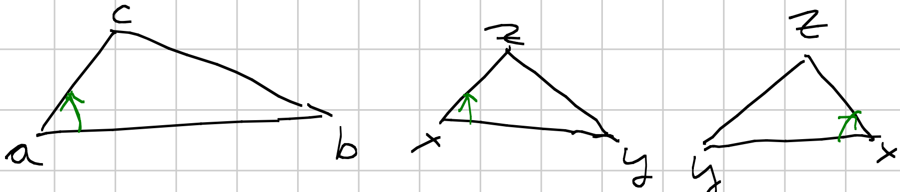
$$= \frac{\cancel{b\bar b}+\bar c b-\cancel{a\bar b}-a\bar c+\cancel{a\bar b}-\cancel{a\bar a}}{\bar b-\bar a}$$

$$= \bar c\,\frac{b-a}{\overline{b-a}}$$ ← ha modulo 1 !

pto medio $\frac{a+b}{2}$ $\quad (-1)\left(a+b+c-\frac{a+b}{2}\right)+\frac{a+b}{2} =$

$= -c$

- Similitudini



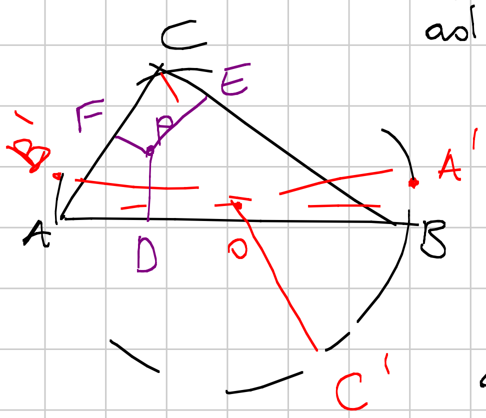
se nel primo verso

$$\frac{c-a}{b-a} = \frac{z-x}{y-x}$$

$$= \frac{\bar z-\bar x}{\bar y-\bar x}$$

se riflesso

triangolo ABC



A', B', C' diam. opposti a A, B, C, Γ

D, E, F proiezioni di un P sui lati.

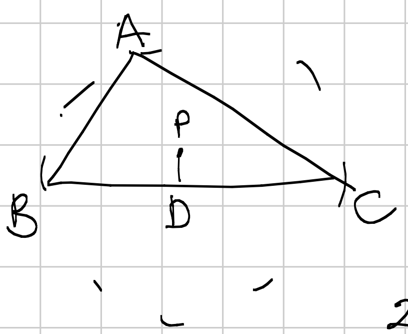
X, Y, Z simmetrici di C', A', B' risp a D, E, F

TESI: $\widehat{XYZ} \sim \widehat{ABC}$

Problemi:
1, 2, 3
"analitica"

$\boxed{6, 16}$ ← + difficili e "importanti": fateli prima o poi!!

$\boxed{10, 8, 9}$ ← + facili, di riscaldamento



$$\frac{1}{2}\left(\overline{\frac{p-b}{c-b}}\right)(c-b)+\frac{b}{2}+\frac{p}{2}=$$

$$=d$$

$$2d=\frac{\bar{p}c-\bar{b}c-\bar{p}b+\cancel{\bar{b}b}+b\bar{c}-\cancel{b\bar{b}}}{\bar{c}-\bar{b}}$$

$\bar{c}=1/c$

$\bar{b}=1/b$

$$+p\bar{c}-p\bar{b}$$

$$=\frac{bc\,(\bar{p}c-c/b-\bar{p}b+b/c+p/c-p/b)}{b-c}=$$

$$=\frac{bc\left(\bar{p}(c-b)+p\,\frac{b-c}{bc}+\frac{b^2-c^2}{bc}\right)}{b-c}=$$

$$= bc(-\bar{p}) + p + b + c = p + b + c - bc\bar{p}$$

$$2d = p + b + c - bc\bar{p}$$

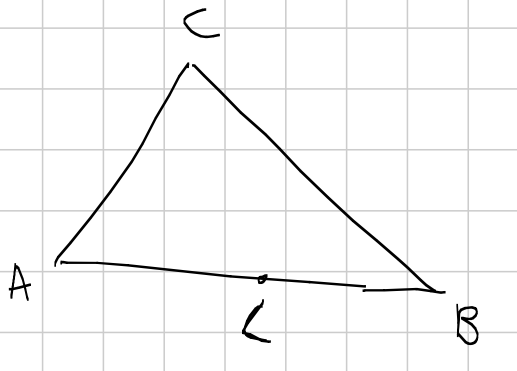
$$d = \frac{x-a}{2} \iff 2d = x - a$$

$$x = 2d + a =$$

$$= a + b + c - bc\bar{p} + p$$

$$\frac{y-x}{z-x} = \frac{-ab\bar{p} + bc\bar{p}}{-ac\bar{p} + bc\bar{p}} = \frac{b(c-a)}{c(b-a)} =$$

$$= \frac{c}{b}\,\frac{\frac{a-c}{ac}}{\frac{a-b}{ab}} = \frac{a-c}{a-b}$$



$$\vec{C'} = \frac{\vec{A} + \vec{B}}{2}$$

$$\langle \vec{C'} - \vec{C}, \vec{C'} - \vec{C} \rangle =$$

$$= \left\langle \frac{\vec{A}}{2} + \frac{\vec{B}}{2} - \vec{C}, \frac{\vec{A}}{2} + \frac{\vec{B}}{2} - \vec{C} \right\rangle$$

$$= \frac{R^2}{4} + \frac{R^2}{4} + R^2 + \frac{|A||B|}{2}\cos 2\gamma - |A||C|\cos 2\beta - |B||C|\cos 2\alpha$$

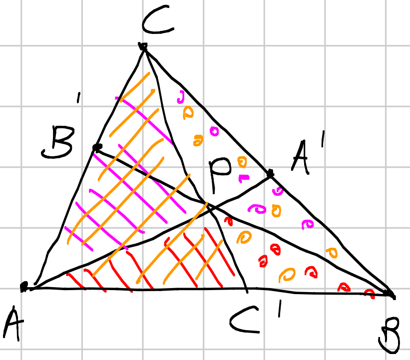
$$= \cancel{\frac{R^2}{2}} + \cancel{R^2} + \cancel{\frac{R^2}{2}} - \cancel{2R^2} + \cancel{2}\frac{R^2}{\cancel{2}}\operatorname{sen}^2\gamma - 2R^2\operatorname{sen}^2\beta - 2R^2\operatorname{sen}^2\alpha$$

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

Geometria 3

Titolo nota 9 26/08/2015

Teorema di Ceva



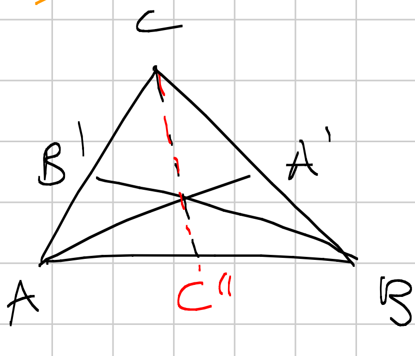
ceviane

AA', BB', CC' concorrono (in un pto P) $\iff \dfrac{AC'}{C'B}\,\dfrac{BA'}{A'C}\,\dfrac{CB'}{B'A} = 1$ (*)

$$\Longrightarrow \quad \frac{AC'}{C'B} = \frac{[ACC']}{[CC'B]} = \frac{[APC']}{[PBC']} = \frac{[APC]}{[CPB]}$$

$$(*) \quad \cancel{\frac{[APC]}{[CPB]}}\,\cancel{\frac{[BPA]}{[APC]}}\,\cancel{\frac{[CPB]}{[BPA]}} = 1$$

$\Longleftarrow$

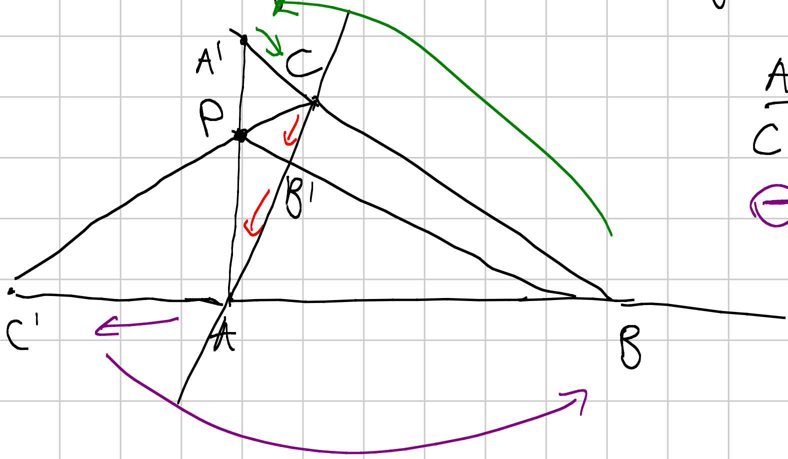


$$\frac{AB'}{B'C}\,\frac{CA'}{A'B}\cdot\frac{BC''}{C''A} = 1$$

$C' \neq C'' \Rightarrow$ le ceviane AA', BB', CC' NON concorrono

- - - - - -

Più in generale: uso segmenti "orientati"

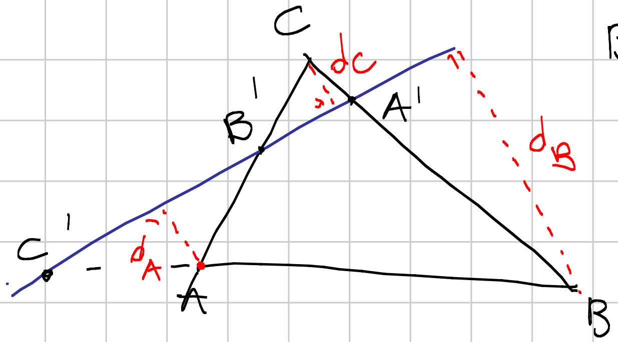


$$\frac{AC'}{C'B} \cdot \frac{BA'}{A'C} \cdot \frac{CB'}{B'A} = 1$$

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

Bonus: controllare che la dim. funzioni ancora anche con A', B', C' sui prolungamenti.

Menelao



A', B', C' su BC, AC, AB (anche sui prolungamenti)

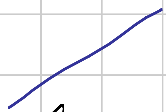
$$\frac{BA'}{A'C} \cdot \frac{CB'}{B'A} \cdot \frac{AC'}{C'B} = -1$$

$\Longleftrightarrow$ A', B', C' sono allineati

$\Leftarrow$
$$\frac{BA'}{A'C} = \frac{d_B}{d_C}$$
$$\frac{CB'}{B'A} = \frac{d_C}{d_A}$$
$$\frac{AC'}{C'B} = -\frac{d_A}{d_B}$$

$\longrightarrow$ prodotto $= -1$

d'altra parte, darà luogo a

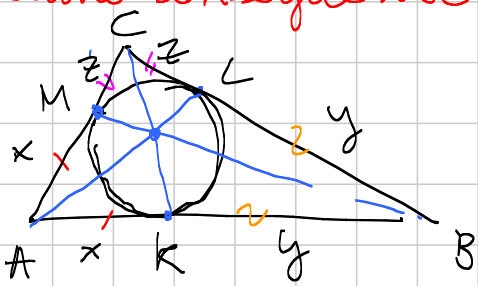


1 o

nel disegno 3 rapporti negativi

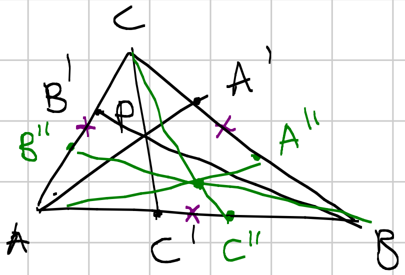
altra freccia PER ASSURDO.

Alcune conseguenze di CEVA:



$$\frac{x}{y}\,\frac{y}{z}\,\frac{z}{x} = 1$$

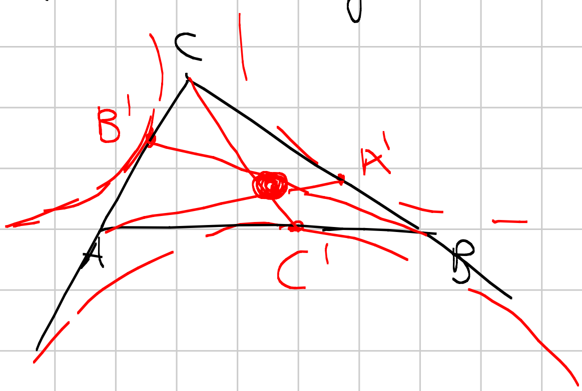
pto di Gergonne



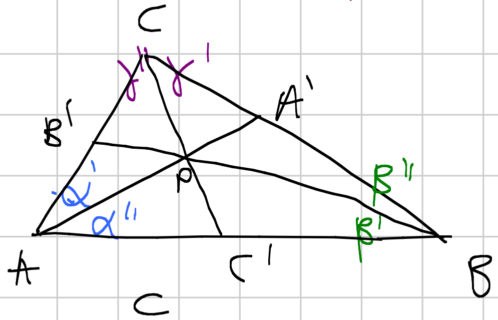
$AC'' = C'B$
$C''B = AC'$

le ceviane verdi concorrono nel coniugato isotomico di P.

COROLLARIO da fare:
le ceviane relative ai pti di tangenza degli excerchi interni ai lati concorrono (nel coniugato isotomico di Gergonne)

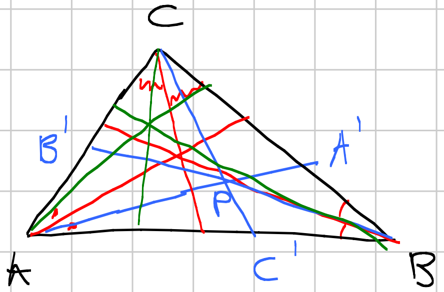


Ceva TRIGONOMETRICO



AA', BB', CC' concorrono $\Longleftrightarrow$

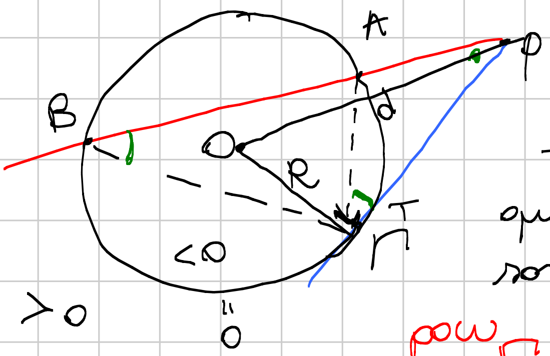
$$\frac{\operatorname{sen}\alpha'}{\operatorname{sen}\alpha''}\cdot\frac{\operatorname{sen}\beta'}{\operatorname{sen}\beta''}\cdot\frac{\operatorname{sen}\gamma'}{\operatorname{sen}\gamma''} = 1$$



le simmetriche delle ceviane concorrenti blu rispetto alle bisettrici concorrono nel "coniugato isogonale" di P (simmediane...)

~ o ~

POTENZE



(teorema tg/sec)

$PT^2 = PA \cdot PB$

+ 2 sec + corda ...

questi teoremi sono un fatto:

$pow_\Gamma(P) = PA \cdot PB$ "è ben definita"

↑ segmenti orientati

$pow_\Gamma(P) = d^2 - R^2$

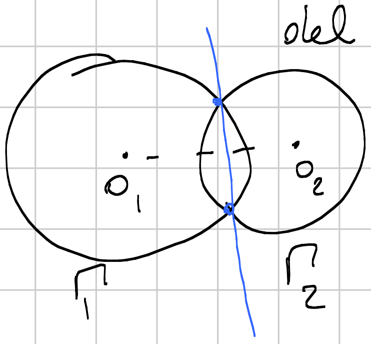
NOTA: come si calcola $pow_\Gamma(P)$ in coordinate?

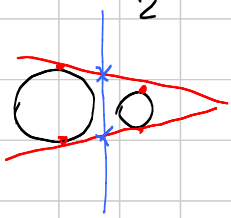
$\Gamma: (x-x_0)^2 + (y-y_0)^2 - R^2 = 0$

$P: (x_P, y_P)$

$pow_\Gamma(P) = d(P,O)^2 - R^2 = (x_P-x_0)^2 + (y_P-y_0)^2 - R^2$

domanda: 2 circonferenze; ci sono pti del piano che hanno $pow_{\Gamma_1}(P) = pow_{\Gamma_2}(P)$? Quali?





(equazione in analitica)

il luogo di questi pti è una retta detta asse radicale, ortogonale alla congiungente i centri.

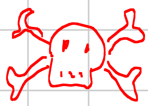
AFFINITÀ

in coordinate $(x,y) \mapsto (ax+by+c,\ dx+ey+f)$

$ae \neq bd$

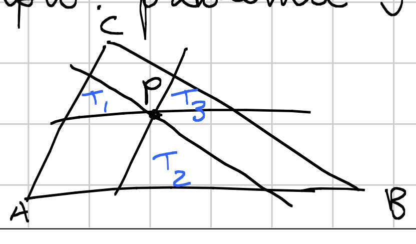
Aree si moltiplicano per $ae-bd$

affinità conservano parallelismo, collinearità (rette → rette), concorrenza, rapporti di segmenti sulla stessa retta.

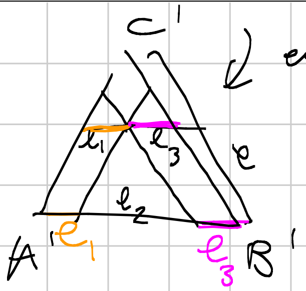
 angoli, perpendicolarità, circonferenze

posso mandare un triangolo in qualunque triangolo!

Esempio: problema 9

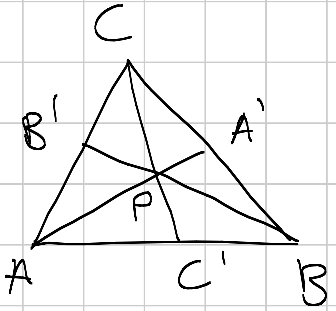


$$\sqrt{T_1}+\sqrt{T_2}+\sqrt{T_3}=\sqrt{T}$$



ii) equilatero

tesi è equivalente a:
$l_1 + l_2 + l_3 = l$
ovvio!



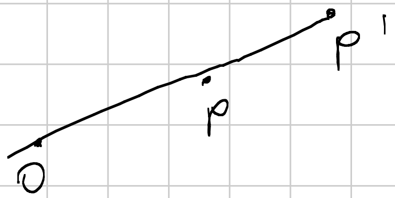
cese 6. 2004

$\frac{AP}{PA'} = x$ y z cicliche

TESI: $xyz = x+y+z+2$

OMOTETIE

omotetia di centro O e ragione $\lambda \in \mathbb{R} \setminus \{0\}$



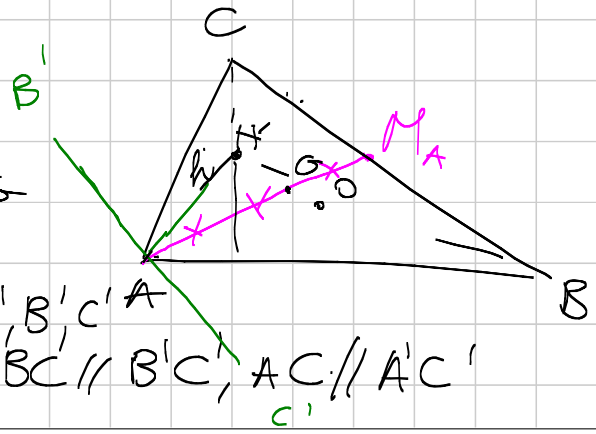
P va in P' sulla retta OP tale che $OP' = \lambda OP$ (con segno)

conservano "tutto"! angoli, rapporti...

in vettori/complessi omotetia di centro origine
$z \mapsto \lambda z$

Retta di Eulero

omotetia di centro G e ragione -2.



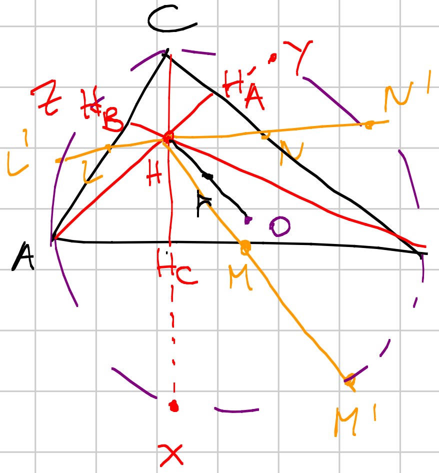
$G \to G$ $ABC \to A'B'C'$

$AB \parallel A'B'$, $BC \parallel B'C'$, $AC \parallel A'C'$

$M_A, M_B, M_C \to A', B', C'$
pti medi di $B'C'$ ecc...

dove va O? assi di $AB, \dots \to$ altezze di $\widehat{ABC}$
perciò $O \to H$

Circonferenza di Feuerbach



omotetia di ragione $1/2$ in H.

$O \to F$ pto medio di OH

$\Gamma \to$ circonferenza Γ' di centro F e raggio $R/2$

$X, Y, Z \to H_C, H_A, H_B$ che quindi stanno su Γ'.

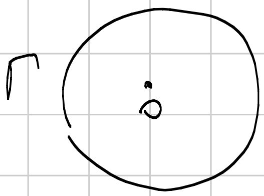
$M', N', L' \to M, N, L$ che stanno su Γ'

anche i pti medi di AH, BH, CH stanno su Γ'.

Γ' "circonferenza dei 9 pti".

INVERSIONE piano $\setminus \{O\}$ ↺

centro O, circonferenza Γ di centro O di raggio R



$\cdot P$

$P \to P'$ sulla semiretta OP
$OP \cdot OP' = R^2$

l'interno della circonferenza va fuori, l'esterno dentro, Γ in se stessa.

$O \to$ "moralmente" nel pto all'∞

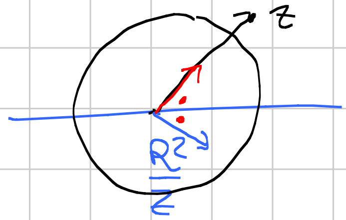
circonferenze per $O \leftrightarrow$ rette non per O

rette per $O \to$ rette per O

circonferenze non per $O \leftrightarrow$ circonferenze non per O.

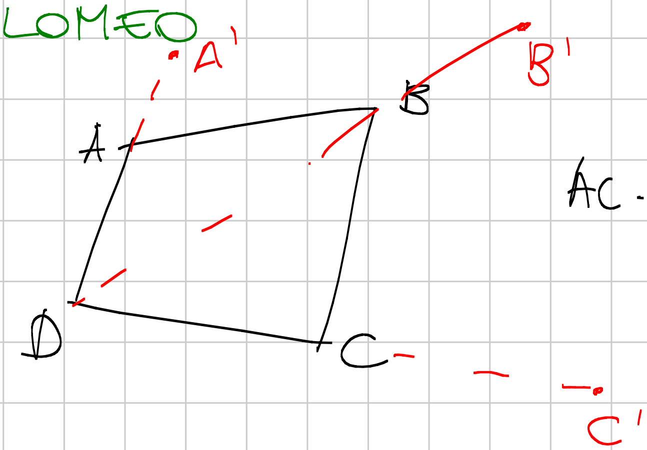
conserva angoli!

NOTA: in complessi inversione di centro 0 e raggio R



$$z \mapsto \frac{R^2}{\bar z}$$

TOLOMEO



$$AC \cdot BD \leq AD \cdot BC + AB \cdot CD$$

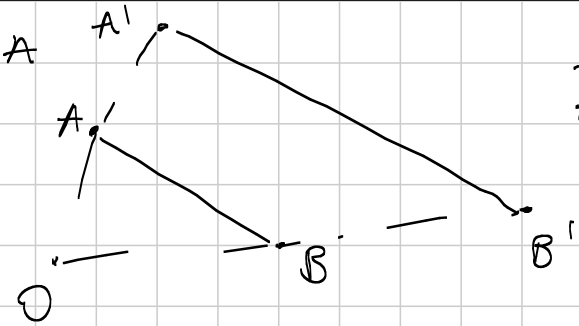
$=$ $\Longleftrightarrow$ ciclico

inverto in D con raggio R

$A'C' \leq A'B' + B'C'$ $\quad = \Longleftrightarrow A', B', C'$ allineati

$\Longleftrightarrow A, B, C$ stanno su circ. per D

LEMMA



$$\overline{A'B'} = \frac{\overline{AB}\ R^2}{\overline{OA}\cdot\overline{OB}}$$

ES. 3, 4, 6, 12, 11

importante

SENIOR 2015 – N1

Titolo nota 23/08/2015

- NUMERI PRIMI

  $p > 1$ divisibili solo per sé stesso e per 1

  2, 3, 5, 7, ...

- FATTORIZZAZIONE UNICA

  Ogni numero intero positivo ammette un'unica fattorizzazione come prodotto di primi

  1 = prodotto di nessun numero primo $= 2^0 \cdot 3^0 \cdot 5^0 \dots$

  $12 = 2^2 \cdot 3 \cdot 5^0 \cdot 7^0 \dots$

  $2^{\dots} \cdot 3^{\dots} \cdot 5^{\dots} \dots$

- DIVISIBILITÀ

  $a \mid b$ "a divide b" se b è un multiplo di a, ovvero $b = k \cdot a$ con k intero

  $a \neq 0$

  Oss: $\pm 1 \mid b$ per ogni b intero

  $a \mid 0$ per ogni $a \neq 0$ intero

Fatto: $a \mid b$ se e solo se per ogni primo p che divide a (p compare nella fattorizz. di a con esponente k) $p^k \mid b$

$a|b$ e $b|c \Rightarrow a|c$

Quindi $p^k|a$ e $a|b \Rightarrow p^k|b$

Viceversa: $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$

$b = p_1^{\beta_1} \dots p_r^{\beta_r} p_{r+1}^{\beta_{r+1}} \dots p_{r+s}^{\beta_{r+s}}$

se $\alpha_1 \le \beta_1$

$\alpha_2 \le \beta_2$

$\vdots$

$$\frac{b}{a} = p_1^{\overset{\geq 0}{\beta_1 - \alpha_1}} \cdot p_2^{\overset{\geq 0}{\beta_2 - \alpha_2}} \dots p_{r+1}^{\beta_{r+1}} \dots \quad \text{intero}$$

$\Rightarrow a|b$

- MCD a, b interi non entrambi nulli:

(a,b) è il più grande divisore comune tra a e b

Es: $(12, 15) = 3$

Proprietà: se $d|a$ e $d|b$, allora $d\,|\,(a,b)$

$p|d$ p primo

VALUTAZIONE p-ADICA $v_p(x)$ (x intero) è il massimo esponente k tale che $p^k|x$

$v_2(12) = 2$

$v_p(d) \le v_p(a)$ perché $d|a$

$v_p(d) \le v_p(b)$ perché $d|b$

$v_p(d) \le \min\big(v_p(a), v_p(b)\big) = v_p\big((a,b)\big)$

$(12, 15) = 3$

$12 = 2^2 \cdot 3$, $15 = 3 \cdot 5$

• ALGORITMO DI EUCLIDE

$$\boxed{(a,b) = (a+b, b)}$$

DIM: Vogliamo dimostrare che $d = (a,b)$ è il MCD tra $a+b$ e b

• $d \mid a+b$ e $d \mid b$

ok perché $d \mid a$ e $d \mid b \Rightarrow d \mid a+b$

• Quindi $d \mid (a+b, b)$

Sia $d' = (a+b, b)$.
$d' \mid b$
$d' \mid a = (a+b) - b$
$\Downarrow$
$d' \mid (a,b) = d$

Conclusione: $d \mid d'$ e $d' \mid d \Rightarrow d = d'$

$(a,b) = (a+b, b)$
$(a,b) = (a-b, b)$]
Più in generale: $(a,b) = (a+kb, b)$ per qualsiasi k intero.

ES: $k=2$ $(a,b) = (\underbrace{a+b}_{\text{INDUZIONE}}, b) = (a+b+b, b) = (a+2b, b)$

$(123, 36) = 3$

$(a,b) = (a+kb, b)$

$123 = 36 \cdot 3 + 15$

$(123, 36) = (123 - \overbrace{36 \cdot 3}^{108}, 36) =$
$= (15, 36)$

$$
\begin{aligned}
&= (36, 15) \\
&= (36 - 15 \cdot 2, 15) \\
&= (36 - 30, 15) \\
&= (6, 15) \\
&= (15, 6) \\
&= (15 - 6 \cdot 2, 6) \\
&= (3, 6) \\
&= (6 - 3 \cdot 2, 3) \\
&= (0, 3)
\end{aligned}
$$

$(a, 0) = |a|$ $a \neq 0$

$$
\begin{aligned}
123 &= \boxed{36} \cdot 3 + \boxed{15} \\
36 &= \boxed{15} \cdot 2 + \boxed{6} \\
15 &= \boxed{6} \cdot 2 + \boxed{3} \\
6 &= 3 \cdot 2 + \boxed{0}
\end{aligned}
$$

MCD (l'ultimo resto $\neq 0$)

- COMBINAZIONI LINEARI DI NUMERI INTERI

$123, 36$

Quali numeri potete scrivere nella forma $123x + 36y$?
(con x, y interi)

$123 - 36$

a, b si dicono "coprimi" o "primi tra loro"
se $(a, b) = 1$

a, b $\quad (a,b) \mid ax + by$ per ogni x, y

Oss 1:

$(123, 36) = 3$ $\qquad 123x + 36y = 9$

$41x + 12y = 3$

Oss 2: Si può ottenere (a,b) come combinazione lineare

$$123 = \boxed{36} \cdot 3 + \boxed{15}$$
$$36 = \boxed{15} \cdot 2 + \boxed{6}$$
$$15 = \boxed{6} \cdot 2 + \boxed{3} \quad \text{MCD}$$
$$6 = 3 \cdot 2 + \boxed{0}$$

$$\begin{aligned} 3 &= \boxed{15} - \boxed{6} \cdot 2 \\ &= \boxed{15} - \left(\boxed{36} - \boxed{15} \cdot 2\right) \cdot 2 \\ &= \boxed{15} \cdot 5 - \boxed{36} \cdot 2 \\ &= \left(\boxed{123} - \boxed{36} \cdot 3\right) \cdot 5 - \boxed{36} \cdot 2 \\ &= \boxed{123} \cdot 5 - \boxed{36} \cdot 17 \end{aligned}$$

$3 = 123x + 36y \qquad x = 5, \quad y = -17$

Oss 3 Per ottenere un multiplo di (a,b) come comb. lineare di a e b ... ?

$$(a,b) = a \cdot x_0 + b \cdot y_0$$

$$k \cdot (a,b) = a \cdot \underbrace{(kx_0)}_{x} + b \cdot \underbrace{(ky_0)}_{y}$$

$3 = 123x + 36y \qquad x_0 = 5, \quad y_0 = -17$

$$\left[\begin{array}{l} 3 = 123x + 36y \qquad x, y \text{ interi} \\ 3 = 123 \cdot \underbrace{5}_{x_0} + 36 \cdot \underbrace{(-17)}_{y_0} \end{array}\right.$$

$$0 = 123(x - \underbrace{x_0}_{5}) + 36(y - \underbrace{y_0}_{-17})$$

$$123(x - x_0) = -36 \cdot (y - y_0)$$

$$41(x - x_0) = -12 \cdot (y - y_0)$$

$$12 \mid x - x_0 \qquad x - x_0 = 12k \qquad k \text{ intero}$$

$$41 \cdot \cancel{12}k = -\cancel{12} \cdot (y - y_0)$$

$$y - y_0 = -41k$$

$$x = x_0 + 12k = 5 + 12k$$

$$y = y_0 - 41k = -17 - 41k$$

$(5 + 12k, -17 - 41k)$ al variare di k intero sono tutte le soluzioni intere dell'equazione

$$123x + 36y = 3$$

$\rightarrow$ $ax + by = t \cdot (a, b)$ $\qquad a, b, t$ fissati

Cercare le soluzioni (x, y)

- Trovare una coppia x_0, y_0 particolare

$\rightarrow$ $ax_0 + by_0 = t(a, b)$

$$a(x - x_0) + b(y - y_0) = 0$$

$$\underbrace{\frac{a}{(a,b)}}(x-x_0) = -\underbrace{\frac{b}{(a,b)}}(y-y_0) \qquad \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$$

$$x - x_0 = \frac{b}{(a,b)}k$$

$$y - y_0 = -\frac{a}{(a,b)}k$$

Conclusione: le soluzioni sono $\begin{cases} x = \frac{b}{(a,b)}k + x_0 \\ y = -\frac{a}{(a,b)}k + y_0 \end{cases}$

al variare di k intero

$k=0 \longrightarrow \begin{array}{l} x = x_0 \\ y = y_0 \end{array}$

- EQUAZIONI DIOFANTEE

0) $ax+by=c$ "equazione diofantea lineare"

$$3^x + 58y^7 + z^4 = 9$$

1) $xy = 15$

$3 \cdot 5$

x	y
1	15
3	5
5	⋮
15	
−1	
−3	
−5	
−15	

2) $x^2 - y^2 = 9$

$(x+y)(x-y) = 3^2$

$x+y$	$x-y$
$\boxed{1}$	$\boxed{9}$
3	3
$\boxed{9}$	$\boxed{1}$
-1	-9
-3	-3
-9	-1

$\begin{cases} x+y=1 \\ x-y=9 \end{cases}$

$2x=10 \qquad x=5$

$2y=-8 \qquad y=-4$

$\begin{cases} x+y = d \\ x-y = \frac{9}{d} \end{cases} \qquad d \mid 9$

$2x = d + \frac{9}{d}$

$\left[\begin{array}{l} x = \dfrac{\overset{a}{d} + \overset{b}{\frac{9}{d}}}{2} \\ y = \dfrac{d - 9/d}{2} \end{array}\right.$

2bis) $x^2 - y^2 = 14$ $\qquad \begin{cases} x+y=a \\ x-y=b \end{cases} \qquad ab=14$

$\left.\begin{array}{l} x = \frac{a+b}{2} \\ y = \frac{a-b}{2} \end{array}\right\}$ non sono mai interi!

3) $xy + x + y = 11$

$xy + x + y + 1 = 12$

$(x+1)(y+1) = 12$

$x+1$	$y+1$
1	
2	
3	
⋮	

4) $5xy + 3x + y = 3$

$\uparrow$

$+a$

$\left[\begin{array}{l} \cancel{5x}y + 3x + y + a = (5x + \alpha)(y + \beta) \\ \cancel{5xy} + 5\beta \cdot x + \alpha \cdot y + \alpha\beta \end{array}\right.$

$\alpha = 1$
$\beta = 3/5$

$$5xy + 3x + y + 3/5 = (5x+1)(y + 3/5)$$

$$= 3 + a = 3 + 3/5$$

$$(5x+1)(y+3/5) = 3 + 3/5$$

$$(5x+1)(5y+3) = 18$$

$18 = ab$ $\quad \begin{cases} 5x+1 = a \\ 5y+3 = b \end{cases}$ $\quad$ $a = 18$, $b = 1$ no!

$a = 1$, $b = 18$ $\quad$ $x = 0$, $y = 3$

$a = 6$, $b = 3$ $\quad$ $x = 1$, $y = 0$

3) $xy + x + y = 11$

Ricaviamo x

$$x(y+1) = 11 - y$$

$$x = \frac{11-y}{y+1} = \frac{12-(y+1)}{y+1} = \frac{12}{y+1} - 1$$

$$x = \underbrace{\frac{12}{y+1} - 1}$$

Quando $\frac{12}{y+1} - 1$ è intero?

$y+1 \mid 12$

5) $\frac{3x^2 - 4x + 7}{x-3}$ $\quad$ per quali ~~x è~~ interi x è intero?

$3x(x-3)$

~~$3x^2 - 4x +$~~

$$\frac{3x^2-4x+7}{x-3} = \frac{r}{x-3} + \underbrace{\text{quoziente}}$$

$r = ?$

$r = 3\cdot 3^2 - 4\cdot 3 + 7 = 22$

$\frac{22}{x-3}$ intero $\quad x-3$ divisore di 22

...

6) $\frac{x^3+5}{x^2-1}$ per quali x interi è intero?

$$= \frac{x+5}{x^2-1} + \frac{x}{}$$

$|x+5| \geq |x^2-1|$

oppure $x+5=0$

CONGRUENZE

Domanda: che giorno sarà il 3/9/2016 ?
sabato (giovedì + 2)

$$365 = \underbrace{52}\cdot 7 + \underline{\underline{1}}$$

"modulo 7"

Qual è il resto della divisione di 365 per 7 ?

a, b interi m intero ≥ 2

$a \equiv b \ (m)$ "a è congruo a b modulo m"

se $m \mid a - b$

equiv: $a = b + km$ per qualche k intero

equiv: a e b hanno lo stesso resto nella divisione per m.

$m = 7$

		…	−4	−3	−2	−1
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	…				

7 colonne

- 365
- 365 + 15

Proprietà:
se $a \equiv a' \ (m)$
e $b \equiv b' \ (m)$
allora $a + b \equiv a' + b' \ (m)$

$365 \equiv 1 \ (7)$
$15 \equiv 1 \ (7)$
$365 + 15 \equiv 1 + 1 \ (7)$

$$a = a' + km$$
$$b = b' + hm$$
$$a+b = a' + km + b' + hm = a'+b' + (k+h)m$$

$$a \equiv a' \ (m) \quad \& \quad b \equiv b' \ (m)$$
$$\Rightarrow \quad ab \equiv a'b' \ (m)$$
$$ab = (a'+km)(b'+hm) = a'b' + m(\underbrace{kb' + ha' + khm})$$

$$365 \cdot 365 \equiv 1 \cdot 1 \equiv 1 \quad (7)$$

$$365^3 \equiv \underline{365 \cdot 365} \cdot 365 \equiv 1 \cdot 1 \cdot 1 \equiv 1 \quad (7)$$

$m = 2$ Lavorare modulo 2 è come ragionare con le parità

$$\underline{P} + D = D$$
$$0 + 1 \equiv 1 \quad (2)$$
$$P \cdot D = P$$
$$0 \cdot 1 \equiv 0 \quad (2)$$

— ∘ —

Come si comportano le potenze?

$m = 6$
$$2015 \equiv 5 \equiv -1 \quad (6)$$
$$2015^2 \equiv (-1)^2 \equiv 1 \quad (6)$$
$$2015^3 \equiv (-1)^3 \equiv -1 \quad (6)$$
$$\vdots$$

$m = 5$
$$333 \equiv 3 \quad (5)$$
$$333^2 \equiv 3^2 = 9 \equiv 4 \quad (5)$$
$$333^3 \equiv 333^2 \cdot 333 \equiv 4 \cdot 3 = 12 \equiv 2 \quad (5)$$
$$333^4 \equiv 2 \cdot 3 = 6 \equiv 1 \quad (5)$$

$333^5 \equiv 1 \cdot 3 \equiv 3$

4
2
1

$333^{\boxed{2015}} \equiv 333^{\boxed{3}} \equiv 2 \quad (5)$

$\boxed{2015} \equiv \boxed{3} \quad (4)$

ATTENZIONE: GLI ESPONENTI NON SI DEVONO RIDURRE MODULO m

$m = 12$ $\qquad 10^k$

$10 \equiv 10 \equiv -2 \quad (12)$] ANTIPERIODO 1

$10^2 \equiv (-2)^2 = 4 \quad (12)$ } PERIODO 1

$10^3 \equiv -8 \equiv 4 \quad (12)$

$10^4 \equiv 4 \quad (12)$

$10^{2015} \equiv \cancel{8} \; 4$

In generale: a^k modulo m al variare di k

c'è un antiperiodo + periodo

PROBLEMA: Un multiplo di 5 può essere $\equiv 4 \ (7)$?

Sì. Es: $25 \equiv 4 \ (7)$

- $5x \equiv 4 \ (7)$
- $5x = 4 + 7k$ Equazione diofantea lineare

Risolvere congruenze del tipo $ax \equiv b \ (m)$
è come risolvere equazioni del tipo $ax - m \cdot k = b$
incognite: x, k.

$5 \equiv -2 \ (7)$

$-2x \equiv 4 \ (7)$

$x \equiv -2 \ (7)$

Si può dividere per 2 a destra e a sinistra perché $2 \nmid 7$

$-2x \equiv 4 \quad (6) \qquad x = 1 \ \checkmark$

$-x \equiv 2 \quad (6) \qquad x = 1$ NO!

Dividere entrambi i membri di una congruenza per a si può fare a patto che $(a, m) = 1$

ES $-2 \equiv 4 \ (6)$ VERO
$-1 \equiv 2 \ (6)$ FALSO

$ab \equiv ac \ (m) \overset{?}{\Longrightarrow} b \equiv c \ (m)$

$\downarrow \qquad\qquad \downarrow$

$m \mid ab - ac = a(b-c) \Rightarrow m \mid b - c$

Se a ha fattori in comune con m, può essere che siano importanti perché $a(b-c)$ sia multiplo di m.

$ax \equiv b \ (m) \qquad ax - km = b$

$x = x_0 + \frac{m}{(a,m)} \cdot t$ al variare di t intero

ES: $2x \equiv 1 \ (4)$ NO. $\quad 2x - 4k = 1$

MORALE: • per avere soluzioni $(a,m) \mid b$

• se c'è almeno una soluzione x_0

tutte le soluzioni sono: $x = x_0 + \frac{m}{(a,m)} \cdot t$

CASO PARTICOLARE $(a,m) = 1$

$ax \equiv b \ (m)$ • c'è soluzione

• soluzioni: $x_0 + m \cdot t$

Se ci interessa x mod m, c'è un'unica soluzione!

La congruenza $ax \equiv b \ (m)$ ha esattamente una soluzione

se $b=1$

"inverso moltiplicativo di a mod m"

ES: $2x \equiv 1 \ (5) \rightarrow x \equiv 3 \ (5)$

3 è l'inverso di 2 mod 5

$3 \cdot 2 \equiv 1 \ (5)$

ESERCIZI:

BREVI (pagg. 9, 10, 11) | 38, 39, 40, 41
43, 44, 45

LUNGHI (pag 39) | 6, 8, 9

• Dimostrare che $\frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{n}$ non è mai intero per alcun valore di n.

CORREZIONE

38) $p^2 | a^3 \Rightarrow p^6 | a^6$? SI

$\Rightarrow p|a \Rightarrow$

40) $a = \dfrac{n+7}{2n+1} = \dfrac{13/2}{2n+1} + \dfrac{1}{2}$

$$\begin{array}{r|l} n+7 & 2n+1 \\ \hline -n-\frac{1}{2} & \frac{1}{2} \\ \hline \frac{13}{2} & \end{array}$$

$2a = \dfrac{13}{2n+1} + 1$ $\qquad 2n+1 \mid 13$

41) $x^3 - y^3 = 7004$

- mod 7 : $x^3 - y^3 \equiv 4 \ (7)$

$x^3 \equiv 0, 1, -1$

$0^3 = 0$
$1^3 = 1$
$2^3 = 8 \equiv 1$
$3^3 \equiv 27 \equiv -1$

- $\underbrace{(x-y)}_{a}\underbrace{(x^2+xy+y^2)}_{b} = 2^2 \cdot 17 \cdot 103$

$\begin{cases} x-y = a \\ x^2+xy+y^2 = b \end{cases}$ $\qquad ab = 2^2 \cdot 17 \cdot 103$

- $x^2+xy+y^2 > 0 \qquad a, b > 0$
- $x > y$

$|x-y| \leq \cancel{2} \max(x,y)$

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

$\begin{cases} x-y = a \\ (x-y)^2 + 3xy = b \end{cases}$ $\qquad \begin{cases} x-y = a \\ 3xy = b - a^2 \end{cases}$

$$\begin{cases} x-y=a \\ xy = \underbrace{\frac{b-a^2}{3}} \end{cases}$$

$ab = 70x$

$a^2 \equiv 1\ (3)$

$a \equiv 1\ (3)$

$a \equiv 2\ (3)$

$b \equiv 1\ (3)$

$x - y \leq x^2 + xy + y^2$

$y = -z$ $\quad$ $\underbrace{x + z} \leq x^2 + z^2 - xz$

$x \leq z$ $\quad$ $x^2 + z(\underbrace{z-x}_{\geq 0})$

$x = z$ a parte

$z - x \geq 1$ $\quad$ $x^2 + z(z-x) \geq x^2 + z \geq x + z$

⑥ $d =$ MCD $\quad p^4 - q^4 \quad p, q$ numeri primi di ≥ 2 cifre

$p = 13$
$q = 11$ $\quad p^4 - q^4 = 2^5 \cdot 3 \cdot 5 \cdot 29 \leftarrow$

$d \mid 2^5 \cdot 3 \cdot 5 \cdot 29$

- fattore 2 $\quad p^4 - q^4 = \underbrace{(p^2+q^2)}(\underbrace{p+q}_{A})(\underbrace{p-q}_{B})$

mod 4

p, q dispari

$p \equiv 1\ (4)$
$p \equiv 3\ (4)$ $\quad \Rightarrow p^2 \equiv 1\ (4)$

$p^2 + q^2 \equiv 2\ (4)$

$v_2(p^2+q^2) = 1$

$A + B = 2p \equiv 2\ (4)$

Uno dei due è $\equiv 2\ (4)$ e l'altro $\equiv 0\ (4)$

$2^4 \mid p^4 - q^4$

$(p+q)(p-q)$ mod 8

$p + q \equiv 2\ (8)$

$p - q \equiv 4\ (8)$

$$\left.\begin{aligned} p &\equiv 3\ (8) \\ q &\equiv -1\ (8) \end{aligned}\right] \quad \begin{aligned} p &= 19 \\ q &= 23 \end{aligned}$$

$v_2(d) = 4$

- fattore 3 $\quad p^4 - q^4 \quad \begin{aligned} p &\equiv 1\ (3) \\ p &\equiv 2\ (3) \end{aligned} \to p^2 \equiv 1\ (3) \to p^4 \equiv 1\ (3)$

$$p^4 - q^4 \equiv 1 - 1 \equiv 0\ (3)$$

$v_3(d) = 1$

- fattore 5 $\quad p^4 - q^4 \quad \begin{aligned} p &\equiv 1\ (5) \\ p &\equiv 2\ (5) \\ p &\equiv 3\ (5) \\ p &\equiv 4\ (5) \end{aligned} \quad \begin{aligned} p^2 &\equiv 1\ (5) \\ p^2 &\equiv 4\ (5) \end{aligned} \to p^4 \equiv 1\ (5)$

$$p^4 - q^4 \equiv 1 - 1 \equiv 0\ (5)$$

$v_5(d) = 1$

- fattore 29 $\quad p = 29 \quad q \neq 29$

$$29 \nmid p^4 - q^4$$

$$d = 2^4 \cdot 3 \cdot 5$$

(8)
$$\begin{aligned} d_n &= (100 + n^2,\ 100 + (n+1)^2) \\ &= (100 + n^2,\ 100 + (n+1)^2 - (100 + n^2)) \\ &= (100 + n^2,\ \underline{2n+1}) \leftarrow \\ &= (200 + 2n^2,\ 2n+1) \\ &= (200 + 2n^2 - n(2n+1),\ 2n+1) \\ &= (200 - n,\ 2n+1) \\ &= (200 - n,\ 2n+1 + 2(200-n)) \end{aligned}$$

$(a,b) = (a + kb, b)$

$2n+1 = d \cdot k \qquad n = \dfrac{dk-1}{2}$

$100 + n^2 = d \cdot h$

$100 + \left(\dfrac{dk-1}{2}\right)^2 = dh$

$401 + d^2k^2 - 2dk = 4dh$

$401 \equiv 0\ (d) \qquad d \mid 401$

$= (\underline{200-n}, 401) \begin{cases} 1 \\ 401 \text{ se } 401 \mid 200-n \end{cases}$

$n \equiv 200 \ (401)$

$n = 200$
601

(9)

$f(0) = 0$ → $\begin{cases} f(2n) = 2f(n) + 1 \\ f(2n+1) = 2f(n) \end{cases}$

$f(1) = 0$

$f(10) = 1$

$f(11) = 0$

$f(100) = 11$

→ $f(101) = 10$

$\underset{2n}{f(1010)} = 2 \cdot f(\underset{n}{101}) + 1 = f(101)$ con aggiunto un 1 alla fine

$101 \to 010 = 10$

Per induzione:

	BASE 10	BASE 2	
passo base	0	[]	→ []
	1	1	→ 0

Passo induttivo: n implica $2n$

$f(2n) = 2f(n) + 1 \underset{\text{BASE 2}}{=} f(n)$ con un 1 alla fine

$= n$ con cifre scambiate & un 1 alla fine

$f(n$ con uno 0 alla fine$)$

n implica $2n+1$: uguale.

(a) $f(n) < n$ per $n \neq 0$

(b) $\underbrace{1010\ldots 10}_{2002}10$

- Servono almeno 2002 cifre
- Devo perdere solo una cifra alla volta

$$2\cdot(1+4+4^2+\ldots+4^{1000}) = 2\cdot\frac{4^{1001}-1}{3}$$

$\boxed{11}$ $\boxed{00}$ NO

(P) $\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots+\frac{1}{n} = \frac{p}{q}$ $\quad q = \text{mcm}(2,3,\ldots,n)$

q pari

$p = q/2 + q/3 + q/4 + \ldots + q/n$ = dispari

$2^k \leq n$ k massimo

PARI

$q/2^k$ è dispari

$v_2(q) = k$

Tutti gli altri sono pari!

$2^k \to q/m \leftarrow 2^k$ $\quad m \leq n$

$m = 2^k$

$m \geq 2^k \cdot 2 = 2^{k+1} > n$

SENIOR 2015 – N2 BASIC

Titolo nota 25/08/2015

- TEOREMA CINESE DEL RESTO

Es:
$$\begin{cases} x \equiv 2 \ (5) \\ x \equiv 3 \ (6) \end{cases} \qquad \begin{aligned} x &= 2+5k \\ x &= 3+6h \end{aligned}$$

$$2+5k = 3+6h$$

$$5k-6h = 1 \qquad \begin{aligned} k &= -1+6t \\ h &= -1+5t \end{aligned}$$

$$x = 2+5k = 2+5(-1+6t) = -3+30t$$
$$x \equiv -3 \ (30)$$

$$\begin{cases} x \equiv a \ (5) \\ x \equiv b \ (6) \end{cases} \qquad \left.\begin{aligned} 0 \le a \le 4 \\ 0 \le b \le 5 \end{aligned}\right\} \text{ soluzioni: tutte tra } 0 \text{ e } 29$$

mod 6, mod 30

mod 5 \ mod 6	0	1	2	3	4	5
0	0					
1		1				
2			2	27		
3				3		
4					4	

Teorema

$$\begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \\ \quad \vdots \\ x \equiv a_n \ (m_n) \end{cases} \qquad (m_i, m_j) = 1 \text{ per ogni } i \neq j$$

Allora c'è esattamente una soluzione mod $m_1 m_2 \dots m_n$.

Detto in un altro modo: $\begin{cases} \dots \\ \dots \\ \dots \\ \dots \end{cases} \iff x \equiv b \ (m_1 m_2 \cdots m_n)$

Esempio

$$\begin{array}{l} A \\ B \\ C \end{array} \begin{cases} x \equiv 33 \ (40) & 2^3 \cdot 5 \\ x \equiv 38 \ (45) & 3^2 \cdot 5 \\ x \equiv 13 \ (50) & 2 \cdot 5^2 \end{cases} \qquad \begin{cases} x \equiv 3 \ (4) \\ x \equiv 8 \ (16) \end{cases}$$

A. $\begin{cases} x \equiv 33 \ (8) \\ x \equiv 33 \ (5) \end{cases} \qquad x \equiv 1 \ (8) \quad x \equiv 3 \ (5)$

B $\begin{cases} x \equiv 2 \ (9) \\ x \equiv 3 \ (5) \end{cases}$

C $\begin{cases} x \equiv 1 \ (2) \\ x \equiv 13 \ (25) \end{cases}$

$\rightarrow x \equiv 1 \ (8)$
$\rightarrow x \equiv 1 \ (2)$ $\iff x \equiv 1 \ (8)$

1 (8)
1 3 5 7 (8)

$$\begin{cases} x \equiv 1 \ (8) \\ x \equiv 2 \ (9) \\ x \equiv 13 \ (25) \end{cases} \Big] \ x \equiv a \ (72).$$

$$\begin{cases} x \equiv 3 \ (5) \\ x \equiv 3 \ (5) \\ x \equiv 13 \ (25) \end{cases} \qquad x \equiv 13 \ (25)$$

$$x \equiv b \ (2^3 \cdot 3^2 \cdot 5^2)$$

- INVERSO MOLTIPLICATIVO

$(a, m) = 1 \qquad a$ ha esattamente un inverso moltiplicativo b modulo m

$ab \equiv 1 \ (m)$

- lo indichiamo con a^{-1} $\quad 1/a$
- si trova con l'alg. di Euclide

Esempio $\quad \frac{2}{3}(4^{1003}-1) \quad \bmod 11$

4
$4^2 \equiv 5$
$4^3 \equiv 20 \equiv 9$
$4^4 \equiv 3$
$4^5 \equiv 1$

$2(4^{1003}-1) \equiv 2(4^3-1)$
$\equiv 2(9-1) \equiv 5 \quad (11)$

$\frac{2}{3}(4^{1003}-1) \equiv \frac{5}{3} \quad (11) \equiv 5 \cdot 3^{-1} \quad (11)$

$\equiv \frac{2(4^{1003}-1)}{\cancel{3}} \cdot \cancel{3}\, 3^{-1}$

$\frac{2}{3}(4^{1000}-1)$ $\quad 3 \nmid 11$

mod 11

$\equiv 2 \cdot 4(4^{1000}-1)$ $\quad 11$

$4^{1000} \bmod 11^2$

$3^{-1} \equiv 4 \quad (11) \qquad$ perché $\quad 3 \cdot 4 = 12 \equiv 1 \quad (11)$

$3^{-1} \equiv 9 \quad (13) \qquad$ 14 $\quad 27/3 = 9$

- STRUTTURA MOLTIPLICATIVA mod p (primo)

  - Tutte le classi di congruenza $\not\equiv 0$ hanno un inverso
  - ordine di un elemento (o ordine moltiplicativo)

$a \not\equiv 0 \ (p)$

$a, a^2, a^3, \dots \ a^k \equiv 1 \ (p)$

$\mathrm{ord}_p(a) =$ il minimo $k > 0$ tale che $a^k \equiv 1 \ (p)$

Oss: $\overline{a^{-1}} =$ inverso di a

$$(a^{-1})^4 \cdot a^5 \equiv a \ (p)$$

$$a^{-1} \equiv a^{k-1} \ (p)$$

$$a \cdot \underbrace{a^{k-1}}_{\text{è l'inverso!}} \equiv a^k \equiv 1 \ (p)$$

$$a^{3k+5} \equiv a^5 \ (p) \quad \text{se} \quad k = \mathrm{ord}_p(a)$$

- Piccolo teorema di Fermat

$$\boxed{a^p \equiv a \ (p)} \qquad \text{per ogni } a$$
p primo

se $a \not\equiv 0 \ (p)$

$$a^p \cdot a^{-1} \equiv a \cdot a^{-1} \ (p)$$

$$\to a^{p-1} \equiv 1 \ (p)$$

Con le congruenze quando volete dividere, moltiplicate per l'inverso!

- Esiste un $k > 0$ t.c. $a^k \equiv 1 \ (p)$
- $\mathrm{ord}_p(a) \leq p-1$
- $\boxed{\mathrm{ord}_p(a) \mid p-1}$

$p = 7$

$$a, a^2, a^3, a^4 \equiv 1 \ (7), \ a^5, \ a^6 \equiv 1$$

$$a^{6-4} \equiv a^6 \cdot a^{-4} \equiv 1 \cdot (a^4)^{-1} \equiv 1 \cdot 1^{-1} \equiv 1$$

$$\mathrm{ord}_p(a) = k \nmid p-1$$

$$p-1 = k \cdot h + r$$

resto della div. per k

$0 < r < k$

$$a^{p-1} \equiv 1 \ (p)$$
$$a^k \equiv 1 \ (p)$$

$$\rightarrow a^{\underbrace{(p-1)-k\ell}_{0<r<k}} \equiv a^{p-1} \cdot ((a^k)^\ell)^{-1} \equiv 1 \cdot (1^\ell)^{-1} \equiv 1$$

ASSURDO

a^r

- $k = \text{ord}_p(a)$
  $\rightarrow a^n \equiv 1 \ (p)$ se e solo se $k \mid n$

$a \not\equiv 0 \ (p)$

$$\underbrace{\overset{a^0}{\overset{\parallel}{1}}, a^1, a^2, \dots,}_{\text{PERIODO } k} \overset{a^k}{\overset{\parallel}{1}}, a^{k+1}, \dots$$

- in un periodo ci sono solo classi di congruenza diverse
  $a^m \equiv a^n \quad m>n$
  $a^{m-n} \equiv 1 \ (p) \quad$ NO

Esempio $\quad p=5$

	a^0	a^1	a^2	a^3	a^4		$\text{ord}_5(a)$
$a \equiv 1 \ (5)$	1	1	1	1	1	...	1
$\rightarrow a \equiv 2 \ (5)$	1	2	4	3	1	...	4
$\rightarrow a \equiv 3 \ (5)$	1	3	4	2	1	...	4
$a \equiv 4 \ (5)$	1	4	1	4	1	...	2

$\text{ord}_p(a) \mid p-1 = 4$

1 piccolo t. di F.

- Cosa succede se $\text{ord}_p(a) = p-1$?
  il periodo contiene tutti i numeri da 1 a $p-1$
  in qualche ordine

a si dice <u>generatore</u> mod p

Se g è un generatore mod p

$g^0, g^1, g^2, \dots, g^{p-2}$ sono tutte le classi di congruenza $\not\equiv 0$

Qualsiasi classe di congruenza mod p $\not\equiv 0$ si può esprimere come potenza di un generatore.

- STRUTTURA MOLTIPLICATIVA mod m (se $(a,m)=1$ c'è l'inverso)
  - $\mathrm{ord}_m(a)$ $\quad (a,m)=1$

$$a, a^2, a^3, \dots, \quad a^k \equiv 1$$

se $(a,m) \neq 1$ non posso ottenere 1 come potenza di a !

$p \mid (a,m)$

$p \mid a^k$ per ogni k

$$a^k \not\equiv 1 \ (m) \qquad a^k \equiv 1 \ (m)$$

$$\Downarrow$$

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

- Teorema di Eulero-Fermat

$$a^{\varphi(m)} \equiv 1 \ (m) \quad \text{se } (a,m)=1$$

$\varphi(m) =$ il numero di elementi dell'insieme $\{1, 2, \dots, m-1\}$ coprimi con m

"funzione di Eulero"

<u>Es</u>: $\varphi(12) = 4$ $\quad \{1, 5, 7, 11\}$

Esempio $m = 12$

	a^0	a^1	a^2	a^3	a^4	$ord_m(a)$
$a \equiv 1$	1	1	1	1	1	1
$a \equiv 5$	1	5	1	5	1	2
$a \equiv 7$	1	7	1	7	1	2
$a \equiv 11 \equiv -1$	1	-1	1	-1	1	2

Teo E.F.

- $\boxed{ord_m(a) \mid \varphi(m)}$ Dimostrazione: uguale al caso $m = p$ primo
- $m = p$ primo $\quad \varphi(p) = p-1$
  $a^{p-1} \equiv 1 \ (p)$

:(Non c'è un generatore!

Teorema

DOMANDA: Quando c'è un generatore?

RISPOSTA:
$m = 2$
$m = 4$
$m = p^n$ $\quad p$ primo dispari
$m = 2p^n$ $\quad$ "

Dimostrazione del t. di Eulero - Fermat

$(a,m) = 1$ $\qquad$ TESI: $a^{\varphi(m)} \equiv 1 \ (m)$

$b_1, b_2, \dots, b_{\varphi(m)}$ $\quad$ le classi di congruenza coprime con m

$\downarrow$

$ab_1, ab_2, \dots, ab_{\varphi(m)}$

Es: $m = 12$
1, 5, 7, 11

$a = 7$
7, 11, 1, 5

OSS: la riga sotto è una permutazione di quella sopra

$$ab_i \equiv ab_j \quad (m)$$
$$\Downarrow$$
$$b_i \equiv b_j \quad (m)$$

Quindi le classi di cong. della riga sotto sono tutte diverse

$$b_1 b_2 \cdots b_{\varphi(m)}$$
$$ab_1 ab_2 \cdots ab_{\varphi(m)} \equiv \underbrace{a^{\varphi(m)}} b_1 b_2 \cdots b_{\varphi(m)}$$

$$\cancel{b_1 b_2 \cdots b_{\varphi(m)}} \equiv a^{\varphi(m)} \cancel{b_1 b_2 \cdots b_{\varphi(m)}} \quad (m)$$
$$1 \equiv a^{\varphi(m)} \quad (m)$$

$\square$

- φ DI EULERO
  - $\varphi(p) = p-1$ se p è primo
  - $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$
    $\{1,2,3,\dots,p^k\} \leftarrow$ ce ne sono p^k
    tolgo quelli multipli di p
    $p, 2p, 3p, \dots, p^{k-1} \cdot p \leftarrow$ ce ne sono p^{k-1}
  - $\varphi(m)$ P.I.E.

T.C.R.

Lemma $\varphi(mn) = \varphi(m) \cdot \varphi(n)$ se $(m,n)=1$
"φ è moltiplicativa"

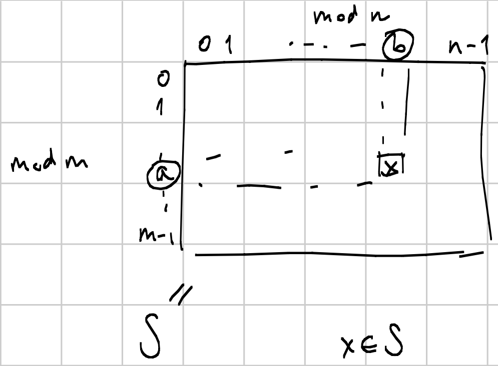
$\to S = \{0,1,2,3,\dots,mn-1\}$ $\quad S^* =$ elem. di S coprimi con mn

$S_1 = \{0,1,\dots,m-1\}$ $\quad S_2 = \{0,1,\dots,n-1\}$

$S_1^* =$ elementi di S_1 coprimi con m

$S_2^* =$ " " S_2

coprimi con n



$$\begin{cases} x \equiv a \ (m) \\ x \equiv b \ (n) \end{cases}$$

$x \in S$

x è coprimo con mn ?

deve essere coprimo con m
e coprimo con n

$x \equiv a \ (m) \qquad a \in S_1^*$

$x \equiv b \ (n) \qquad b \in S_2^*$

$x \in S^* \Rightarrow a \in S_1^*$ e $b \in S_2^*$

$\Leftarrow$

Dim Per assurdo. se $x \notin S^*$

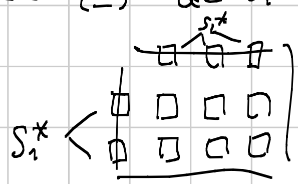
$(x, mn) \neq 1$

$\Rightarrow (x, m) \neq 1$ oppure $(x, n) \neq 1$

wlog $(x, m) \neq 1$

$x \equiv a (m) \qquad a \notin S_1^*$

$x \in S^* \Leftrightarrow a \in S_1^*$ e $b \in S_2^*$ Assurdo



$$|S^*| = |S_1^*| \cdot |S_2^*|$$

$$\downarrow \qquad \downarrow \qquad \downarrow$$

$$\varphi(mn) = \varphi(m) \cdot \varphi(n)$$

$\square$

$\varphi(p^k) = p^{k-1}(p-1)$

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \Rightarrow \varphi(m) = \varphi(p_1^{a_1})\,\varphi(p_2^{a_2} \cdots p_r^{a_r}) =$$

$$= \varphi(p_1^{a_1})\,\varphi(p_2^{a_2}) \cdots \varphi(p_r^{a_r})$$

$$= p_1^{a_1 - 1}(p_1 - 1) \cdot p_2^{a_2 - 1}(p_2 - 1) \cdots$$

- RESIDUI QUADRATICI, RESIDUI K-ESIMI, POTENZE...

mod p Quali sono le classi di congruenza che si possono ottenere da un quadrato perfetto?

Es: $p = 3$ $\quad x^2 \equiv 0, 1 \ (3)$

x		x^2
0	$\to$	0
1	$\to$	1
2	$\to$	1

$p = 5$

x	x^2
0	0
1	1
2	4
3	4
4	1

In generale: mod p ci sono $\frac{p-1}{2}$ residui quadratici $\not\equiv 0$ $\quad (p \neq 2)$

$$x \overset{f}{\longmapsto} x^2$$

$f(x) \equiv f(-x)$ $\qquad (-x)^2 \equiv x^2$

$0 \to 0$

$x \not\equiv 0 \qquad x \not\equiv -x \ (p)$ $\qquad x,\ -x \to x^2$

$x \to x^2$
$-x \to x^2$
$\cancel{y} \to x^2$

$x^2 \equiv y^2 \ (p)$

$p \mid x^2 - y^2 = (x+y)(x-y)$

$p \mid x - y \qquad y \equiv x \ (p)$

oppure $p \mid x + y \qquad y \equiv -x \ (p)$

I quadrati sono $\frac{p-1}{2}$ più lo 0.

mod p (Come sono fatte le potenze?)

Quante sono le potenze n-esime?

$0 = 0^n$

Sia g un generatore mod p

mod p $\quad \{1, 2, 3, \ldots, p-1\} = \{g^0, g^1, g^2, \ldots, g^{p-2}\}$

I generatori trasformano problemi moltiplicativi in problemi additivi.

$\downarrow$ eleviamo alla n

$\{g^0, g^n, g^{2n}, g^{3n}, \ldots, g^{(p-2)n}\}$

$\frac{p-1}{(n, p-1)}$

• $g^{kn} \equiv g^{hn} \ (p)$?

$\cdot \, g^{-hn}$

$g^{kn-hn} \equiv 1 \ (p)$

$g^{(k-h)n} \equiv 1 \ (p)$

$\mathrm{ord}_p(g) \mid (k-h)n$

$\shortparallel$

$$p-1$$

$$p-1 \mid (k-h)n$$

$$\iff \frac{p-1}{(n,\ p-1)} \Bigm| k-h$$

$$\iff k \equiv h \quad \left(\frac{p-1}{(n,p-1)}\right)$$

Ci sono $\left|\frac{p-1}{(n,p-1)}\right|$ potenze n-esime mod p

$$\underbrace{\frac{p-1}{(n,p-1)}}_{\displaystyle = \mathrm{ord}_p(g^n)} \qquad \mathrm{ord}_p(g^n) \to \underbrace{g^0, g^n, g^{2n}, g^{3n}, \dots, g^{kn}}_{}, \quad g^{kn} = 1$$

Es: $n=2$, p dispari $\quad \frac{p-1}{(2,p-1)} = \frac{p-1}{2}$

Es: $y^{2} = x^{5} - 4 \qquad \frac{p-1}{(n,p-1)} \qquad (n,p-1)$ è grande

0, 1, -1

vogliamo che $p-1$ abbia tanti fattori in comune con gli esponenti

mod 11 ci sono $5+1$ quadrati

ci sono $2+1$ potenze quinte $\to 0, 1, -1$

mod 7 quante potenze quinte? Tutte

$$(5,\ 7-1) = 1$$

$n = p^k$ $\quad p$ dispari $\quad$ ci sono $\frac{\varphi(p^k)}{(n, \varphi(p^k))}$ potenze n-esime coprime con p^k

ESERCIZI pag 11 49, 51, 53, 54, 66

pag 40 7, 9, 10

CORREZIONE

I generatori mod m (quando esistono) generano le classi di cong. coprime con m.

$m = 12$ 1, 5, 7, 11

49 $\quad n^2 + 5n + 16 = 169y$

$n^2 + 5n + 16 \equiv 0 \quad (13^2)$

$n^2 + 5n + 16 \equiv 0 \quad (13)$

$x^2 + 5x + 16 = 0$ $\quad$ x numero ~~reale~~ complesso

$$x = \frac{-5 \pm \sqrt{5^2 - 16 \cdot 4}}{2}$$

$$\left(x + \frac{5}{2}\right)^2 + 16 - \frac{25}{4} = 0$$

$$x + \frac{5}{2} = \pm\sqrt{\frac{25}{4} - 16}$$

$n^2 + 5n + 16 \equiv 0 \quad (13)$

$n^2 + 5n + 3 \equiv 0 \quad (13)$

$$n^2 + 5n + 3 \equiv \left(n + \frac{5}{2}\right)^2 + 3 - \frac{25}{4} \equiv \frac{1}{4}\left((2n+5)^2 + 0\right) \equiv \frac{1}{4}(2n+5)^2$$

14
27
40

$$\equiv 10(2n+5)^2$$

$$\cancel{10}(2n+5)^2 \equiv 0 \quad (13)$$

$$2n+5 \equiv 0 \quad (13)$$

$$n \equiv -5/2 \equiv -5\cdot 7 \equiv 4 \quad (13)$$

$n \equiv 4\ (13)$

$$\underline{n^2+5n+3} \equiv n^2-8n+16 = (n-4)^2$$

$\boxed{n = 13k+4}$

$$0 \equiv n^2+5n+16 = (13k+4)^2 + 5(13k+4) + 16 \equiv$$

$$\equiv 13\cdot 4\cdot 2\cdot k + 16 + 5\cdot 13\cdot k + 20 + 16$$

$$\equiv 13(8k+5k) + 52$$

$$\equiv \cancel{13^2}k + 52 \quad (13^2)$$

WHAT IF...

$$\cancel{13}k + \cancel{52}^{4} \equiv 0 \ (13^2)$$

$$13^2 \mid 13k+52$$

$$13 \mid k+4$$

$$k \equiv -4\ (13)$$

$$k = -4 + 13h$$

$$n = 13(-4+13h)+4$$

$$n \equiv -4\cdot 13 + 4 \quad (13^2)$$

(51) $x^2 \equiv 2 \ (100)$

$\Downarrow$ $4 \mid 100$

$x^2 \equiv 2 \ (4)$ $\quad [x^2 \equiv 0,1 \ (4)]$

$\underline{n^k \equiv 2\ (4)}$ NO

(53) $x^2 + 3y = 2$

$$y = \frac{2-x^2}{3}$$

$\boxed{x^2 \equiv 2\ (3)}$ $\quad [x^2 \equiv 0,1 \ (3)]$

54 $3^y - x^2 = 41$

mod 4 $\quad (-1)^y - x^2 \equiv 1 \quad (4)$

$(-1)^y$: 1, −1 $\qquad x^2$: 0, 1

• x è pari

• $(-1)^y \equiv 1$ (4) cioè y è pari

$y = 2z$

$3^{2z} - x^2 = 41$

$\overbrace{(\underbrace{3^z}_{t} + x)}^{70}(\underbrace{3^z}_{t} - x) = 41$

a	b
41	1
1	41
~~−1~~	~~−41~~
~~−41~~	~~−1~~

$3^z = \dfrac{a+b}{2}$ NO

66 (a) $a^x \equiv 1 \quad (10)$ $\qquad$ Sono 4 (10)

1, 3, 7, 9

(b) $x^2 \equiv a \quad (19)$ $\qquad$ Quanti? $\dfrac{p+1}{2} = 10$

(c) $x^3 \equiv 2a \quad (21)$

TCR $\iff \begin{cases} x^3 \equiv 2a \ (3) \\ x^3 \equiv 2a \ (7) \end{cases}$

$x^3 \equiv 2a$ (3) $\longrightarrow x^3 \equiv x \ (3)$ $\qquad$ $x \equiv 2a$ (3) ha sempre soluzione, qualsiasi sia a.

$x^3 \equiv 2a$ (7): $\dfrac{p-1}{(n, p-1)} = \dfrac{6}{(3,6)} = 2$

$\underbrace{0, 1, -1}$

$2a \equiv \begin{cases} 0 \\ 1 \\ -1 \end{cases} \quad (7)$

$\boxed{a \equiv \begin{cases} 0 \\ 4 \\ 3 \end{cases} \quad (7)}$

(d) $3^x \equiv a \ (30)$

3
$3^2 = 9$
$\vdots$

$x>0$
(altrim. c'è la sol. $a \equiv 1 \ (30)$)

$$\begin{cases} 3^x \equiv a \ (3) \leftarrow \\ 3^x \equiv a \ (10) \leftarrow \end{cases} \begin{cases} a \equiv 0 \ (3) \\ a \equiv 3, 9, 7, 1 \ (10) \end{cases}$$ 4 soluzioni per a mod 30

$3, 9, 27, 21$

(e) $x^3 \equiv 2a \ (14)$

$x^3 \equiv 0 \ (2) \Rightarrow$ $\underline{x \text{ pari}}$

$x^3 \equiv 2a \ (7)$

---

7 p Esistono infiniti n t.c. $p \mid 2^n - n$

$2^n \equiv n \ (p)$

$$\begin{cases} 2^n \equiv 1 \ (p) \longrightarrow \operatorname{ord}_p(2) \mid n \\ n \equiv 1 \ (p) \end{cases}$$

Ci basta $p-1 \mid n$
ovvero $n \equiv 0 \ (p-1)$

$$\begin{cases} n \equiv 0 \ (p-1) \\ n \equiv 1 \ (p) \end{cases}$$ TCR: esiste una soluzione mod $\underline{p(p-1)}$

$2^n \equiv n \ (p)$

$a \qquad a$

$$\begin{cases} 2^n \equiv a \ (p) \\ n \equiv a \ (p) \end{cases}$$

(9) $\forall\, d, m, n$ $\quad\exists$ progressione aritmetica con

$x,\ x+d,\ x+2d,\ x+3d,\ \dots,\ x+(m-1)d$

tutti multipli di qualche potenza n-esima >1

$$\longrightarrow \begin{cases} x \equiv 0 \ (p_1^n) \\ x+d \equiv 0 \ (p_2^n) \leftarrow \\ \vdots \\ x+(m-1)d \equiv 0 \ (p_m^n) \end{cases}$$

$p_1, p_2, \dots, p_m$ primi distinti

$$\begin{cases} x \equiv 0 \ (p_1^n) \\ x \equiv -d \ (p_2^n) \\ \vdots \\ x \equiv -(m-1)d \ (p_m^n) \end{cases}$$

TCR

Esiste una sol. per x mod $p_1^n \cdots p_m^n$