Stage Senior 2015 – Livello Medium

Stampato integrale delle lezioni

Autori vari

Indice

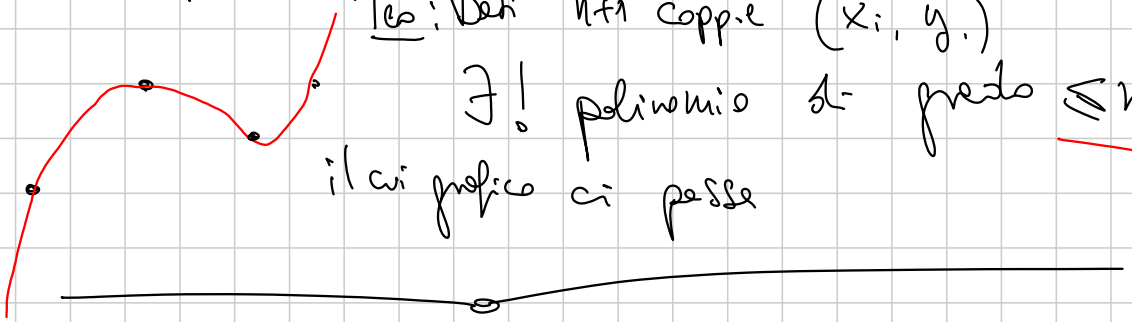
A3 medium Pol

Titolo nota 06/09/2015

$x_i \neq x_j$ per $i \neq j$

Interpolazione:

Teo: Dati $n+1$ coppie (x_i, y_i) $\exists!$ polinomio di grado $\leq n$ il cui grafico ci passa



Unicità: se ne ho due, $p(x), q(x)$

$p(x) - q(x)$ ha $n+1$ zeri (ed è di grado n)

Esistenza:

Strategia 1: sistemone lineare

$$a(x) = a_0 + a_1 x + \dots + a_n x^n$$

$$\begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^n \\ \vdots & & & & \vdots \\ 1 & \cdots & & & x_n^n \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{bmatrix}$$

Fatto: questa matrice (matrice di Vandermonde) è invertibile (se $x_i \neq x_j \ \forall\, i \neq j$)

Metodo 2: aggiusto un coefficiente per volta

(x_0, y_0) (x_1, y_1) (x_2, y_2) (x_3, y_3)

sistemo x_0 — sistemo x_1 senza rovinare x_0 — sistemo x_2 senza rovinare x_0, x_1

$$y_0 + \frac{(x-x_0)}{x_1-x_0}\cdot(y_1-y_0) + \frac{(x-x_0)(x-x_1)}{(x_2-x_0)(x_2-x_1)} + \dots$$

(Forma di Newton)

Metodo 3: aggiusto un termine per volta, in modo uno indipendente dell'altro

Sarebbe bello avere tanti polinomi $L_i(x)$ tali che $L_i(x_i) = 1$ $L_i(x_j) = 0$ per $i \neq j$ (e grado $\leq n$)

In questo modo, il poli. di interpolazione è $p(x) = \sum_{i=0}^{n} y_i L_i(x)$.

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

Polinomi (base) di Lagrange

Ogni pol. di grado n è comb. lineare dei L_i

Analogamente nell'altro metodo, base di Newton

$$1, \quad \frac{x-x_0}{x_1-x_0}, \quad \frac{(x-x_1)(x-x_2)}{(x_2-x_1)(x_2-x_3)}, \quad \dots$$

Se i nodi sono $0, 1, 2, \dots n$, la base

di Newton è $1, \frac{x}{1}, \frac{x(x-1)}{2\cdot 1}, \frac{x(x-1)(x-2)}{3\cdot 2\cdot 1}$

"polinomi binomiali" $\binom{x}{k}$.

Oss: stesse dim. del teo. cinese del resto

$$\begin{cases} x_0 \equiv y_0 \ (m_0) \\ \vdots \\ x_k \equiv y_k \ (m_k) \end{cases} \qquad L_i = \prod_{j \neq i} m_j \cdot (\text{inverso di } m_j \text{ modulo } i)$$

$p(x) = x^3 - 2$

$p(0)$	$p(1)$	$p(2)$	$p(3)$	$p(4)$	$p(5)$	$p(6)$	...
-2	-1	6	25	62	123	214	...
	1	7	19	37	61	91	...
		6	12	18	24	30	...
			6	6	6	6	...
				0	0	0	...

In tutti i polinomi, si arriva a una riga di zeri.

Dim: nella seconda riga, ci sono $q(0), q(1), q(2)\dots$ dove $q(x) = p(x+1) - p(x)$.

$q(x)$ ha grado $(\deg p) - 1$

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

Quindi a ogni step scende di un grado

Come si ricostruisce $p(x)$ dalla tabella?

Idea: queste tabelle si comportano in modo molto semplice sulla base di Newton:

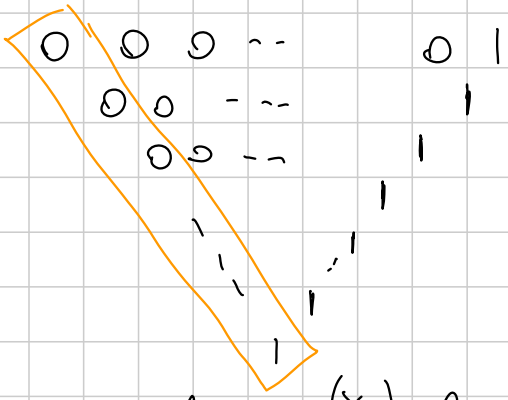
$p(x) = \binom{x}{k}$ quanto fa $\binom{n+1}{k} - \binom{n}{k}$? $\binom{n}{k-1}$

$\binom{x}{k} \to \binom{0}{k} \quad \binom{1}{k} \quad \binom{2}{k} \quad \dots \quad \binom{k}{k} \quad \binom{k+1}{k} \quad \binom{k+2}{k} \quad \dots$

$\binom{x}{k-1} \to \binom{0}{k-1} \quad \binom{1}{k-1} \quad \dots \quad \binom{k-1}{k-1} \quad \binom{k}{k-1} \quad \binom{k+1}{k-1}$

$\binom{0}{k-2} \quad \dots \quad \dots$

In particolare, scrivendo i valori



Nella prima colonna, $\binom{x}{k}$ ha k zeri e poi un 1

E se invece parto da $a_0\binom{x}{0} + a_1\binom{x}{1} + a_2\binom{x}{2} + \dots + a_k\binom{x}{k}$,

nella prima colonna ho

a_0

a_1

a_2

$\ddots$

a_k

0

0

0

$\ddots$

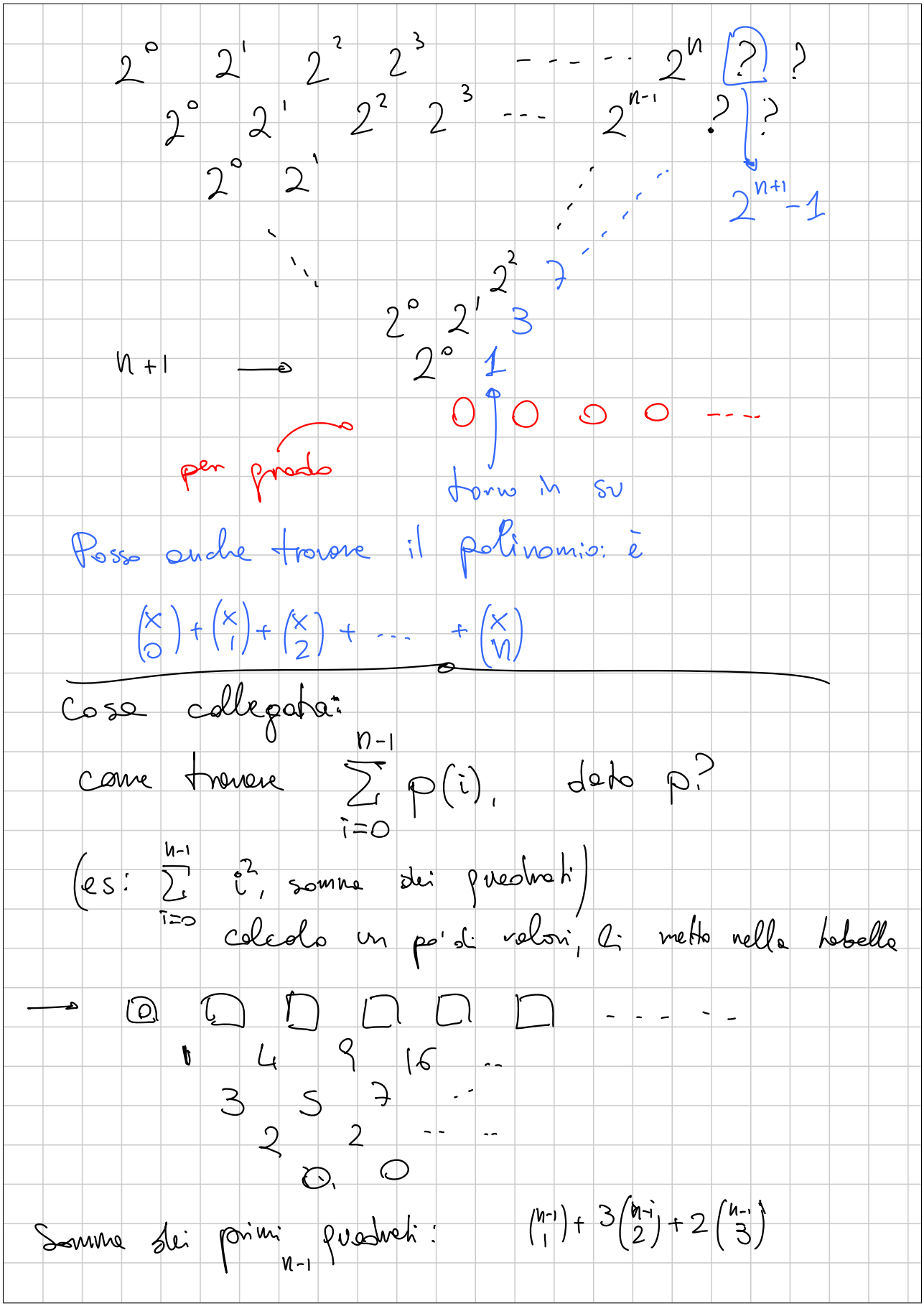
Quindi: se nella prima colonna trovo $a_0, a_1, \dots a_k$, il polinomio era $a_0\binom{x}{0} + a_1\binom{x}{1} + \dots + a_k\binom{x}{k}$.

(in particolare, nella riga subito prima degli zeri viene $n! a_n$)

(parentesi... Quali sono i polinomi tali che $p(n) \in \mathbb{Z}$ per ogni $n \in \mathbb{Z}$? $\frac{x(x-1)}{2}$, ...
Sono esattamente le c.l. intere delle basi di Newton)

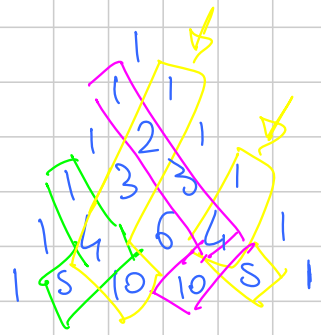
Esercizio che non potete non aver visto:
Trovare $p(x)$ tale che $p(k) = 2^k$ per $k = 0, 1, \dots n$, di grado n. Quanto vale $p(n+1)$?

Dim: faccio la tabellona!


2^0 2^1 2^2 2^3 ---- 2^n ? ?
2^0 2^1 2^2 2^3 --- 2^{n-1} ? ?
2^0 2^1
$2^{n+1}-1$
2^0 2^1 2^2 7
2^0 2^1 3
2^0 1
n+1
per grado
torno in su
Posso anche trovare il polinomio: è
$\binom{x}{0}+\binom{x}{1}+\binom{x}{2}+\dots+\binom{x}{n}$
Cosa collegata:
come trovare $\sum_{i=0}^{n-1} p(i)$, dato p?
(es: $\sum_{i=0}^{n-1} i^2$, somma dei quadrati)
calcolo un po' di valori, li metto nella tabella
0 1 4 9 16 ..
3 5 7 ..
2 2 .. ..
0 0
Somma dei primi $n-1$ quadrati: $\binom{n-1}{1}+3\binom{n-1}{2}+2\binom{n-1}{3}$

Metodo più industriale:

base di Newton + "Hockey-stick formula"



$$\sum_{i=1}^{n} \binom{i}{k} = \binom{n+1}{k+1}$$

(problema per il premio: trovare una dim. combinatorica di questa formula)

Come si trova per esempio,

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

$$\text{H-S} = 2\binom{n+1}{3} + \binom{n+1}{2} = 2\frac{(n+1)(n)(n-1)}{3 \cdot 2 \cdot 1} + \frac{(n+1)n}{2 \cdot 1} =$$

$$= (n+1)n \left[\frac{n-1}{3} + \frac{1}{2} \right] = (n+1)n \frac{2n-2+3}{6} \quad \checkmark$$

$$x_{k+2} = \alpha x_{k+1} + \beta x_k$$

polinomio caratteristico $\lambda^2 = \alpha\lambda + \beta$ (⋆)

radici λ_1, λ_2

soluzioni: $X_k = r \cdot \lambda_1^k + s \cdot \lambda_2^k$

r, s determinati da cond. iniziali

$X_{k+3} = \square X_{k+2} + \square X_{k+1} + \square X_k$ $\quad r\lambda_1^k + s\lambda_2^k + t\lambda_3^k$

Se (*) è reale e ha due radici complesse, allora sono coniugate, $re^{i\vartheta}$, $re^{-i\vartheta}$

posso scrivere anche la soluzione come

$$u r^k \frac{e^{ik\vartheta} + e^{-ik\vartheta}}{2} + v r^k \frac{e^{ik\vartheta} - e^{-ik\vartheta}}{2i} =$$

$$= u r^k \cos k\vartheta + v r^k \sin k\vartheta$$

Se (*) ha radici doppie?

Es. $\lambda^2 = 4\lambda - 4$ $\quad r\ 2^k + sk \cdot 2^k$

Se ho una radice λ_i con molteplicità m

$$\underbrace{\lambda_i^k,\ k\lambda_i^k,\ k^2\lambda_i^k, \dots}_{m \text{ termini}}$$

Se ho "termini nodi" aggiuntivi

Per es: $x_{k+2} = 4x_{k+1} - 4x_k + 5^k$ (**) non omogenea

Osservazione 1: Se x_k, y_k solvono (**),
allora $z_k := x_k - y_k$ solve $z_{k+2} = 4z_{k+1} - 4z_k$. omogenea
e questa la so risolvere $z_k = r2^k + sk2^k$

Se scopro (in qualche modo) una soluzione y_k della (**) (con i suoi valori iniziali),
allora ogni altra soluzione x_k è della forma

$$x_k = z_k + y_k = r2^k + sk2^k + y_k$$

sol. generale della omogenea — sol. particolare, scelta da me, della non om.

Quanti modi di andare da (tutte spente) — una sì e una no

sono: un modo speciale di andare da tutte spente a una sì e una no (+) tutti i modi di andare da "tutte spente" a "tutte spente"

Come si trova una sol. particolare?
Esempio: provo un multiplo di 5^k

$$c \cdot 5^{k+2} = 4c5^{k+1} - 4c5^k + 5^k$$

$$2SC = 20C - 4C + 1 \qquad C = \frac{1}{9}$$

$y_k = \frac{1}{9} 5^k$ è sol. di (**)
con cond. in. $y_0 = \frac{1}{9}$ $y_1 = \frac{5}{9}$ ok

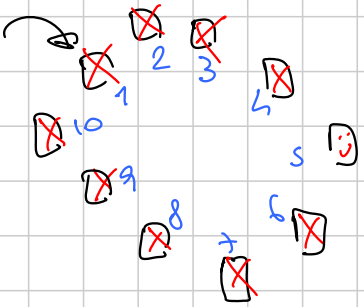
Se avessi avuto $x_{k+2} = 4x_{k+1} - 4x_k + 2^k$
($\lambda = 2$ già sol.) ~ provo $(ak^2 + bk + c)2^k$

Se avessi avuto $x_{k+2} = 4x_{k+1} - 4x_k + 7 \cdot 1^k$ ~
mult. di 1^k

$$x_{k+2} = 4x_{k+1} - 4x_k + 9k$$
1^k $k \cdot 1^k$

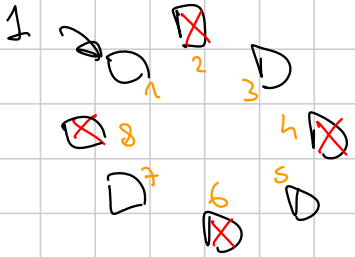
Problema di Josephus:

parto da qui



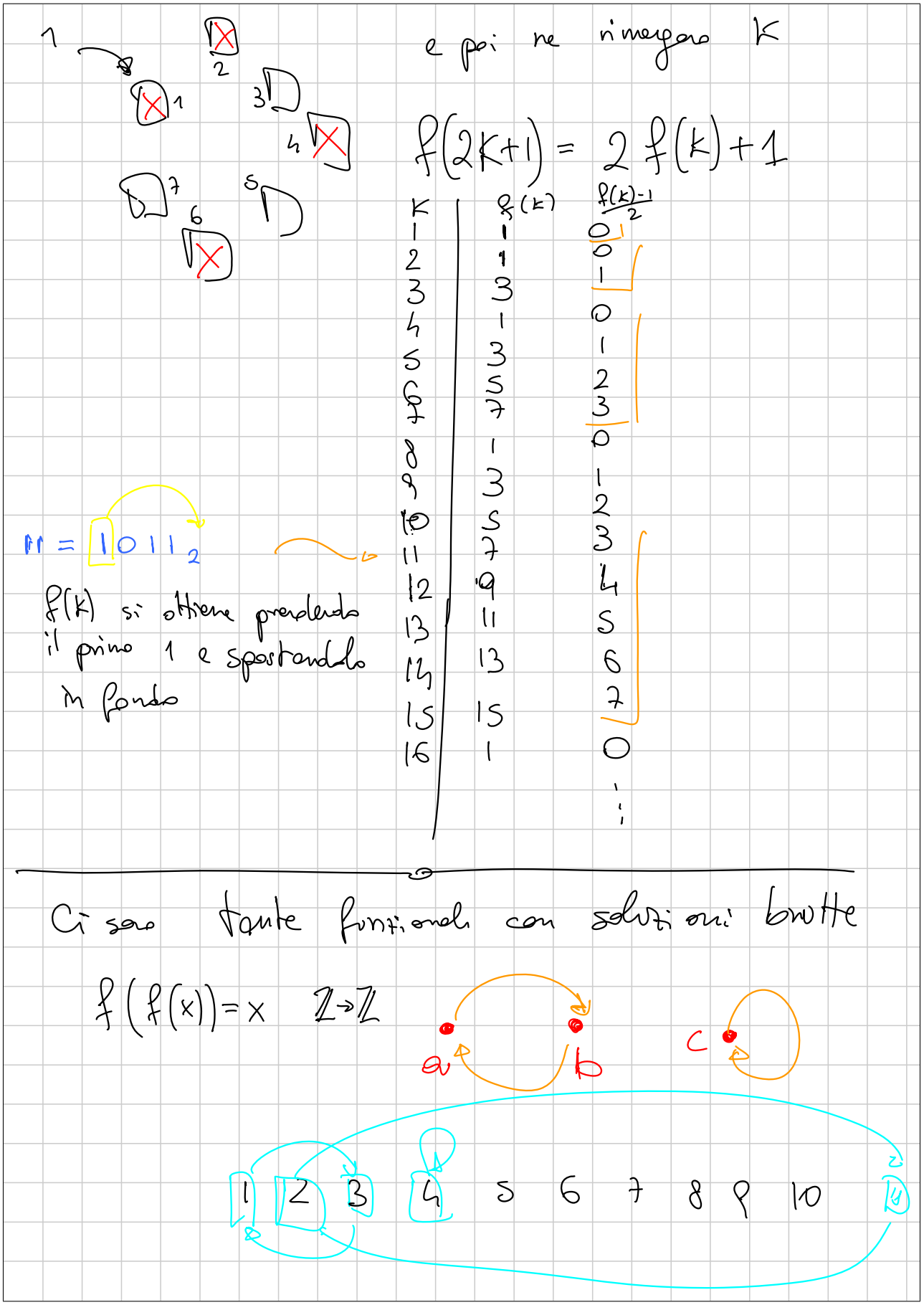
con 10 persone, sopravvive il #5.

$f(k) = \{$ posizione dell'ultimo rimasto partendo da k persone $\}$



$$f(2k) = 2f(k) - 1$$

Se invece sono dispari, muoio quelli pari, l'1


e poi ne rimangono K
f(2K+1) = 2f(K)+1
K
f(K)
f(K)-1/2
n = 1011₂
f(k) si ottiene prendendo il primo 1 e spostandolo in fondo
Ci sono tante funzioni con soluzioni brutte
f(f(x)) = x Z→Z
a
b
c
1 2 3 4 5 6 7 8 9 10 11

$\mathbb{R} \to \mathbb{R}$

$[f(x)]^2 = x^2$ $\quad \begin{cases} f(x) = x \\ f(x) = -x \end{cases}$

$\begin{cases} f(x) = x & \text{per un certo insieme } S \\ f(x) = -x & \text{per gli altri } (\mathbb{R} \setminus S) \end{cases}$

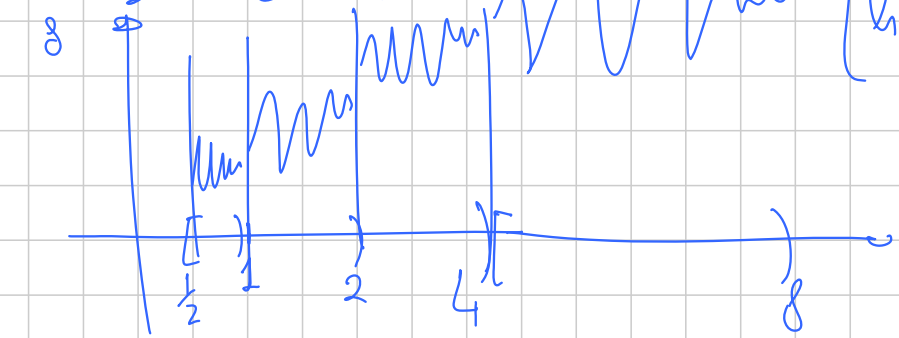
$f(x^2) - f(x) = 1, \qquad f : (1, \infty) \to \mathbb{R}$

idea 1: trasformo quell' x^2 in un $2x$

pongo $x = e^y \rightsquigarrow f(e^{2y}) - f(e^y) = 1 \quad \forall y \in (0, \infty)$

pongo $g(y) := f(e^y) \rightsquigarrow g(2y) - g(y) = 1 \quad (*)$

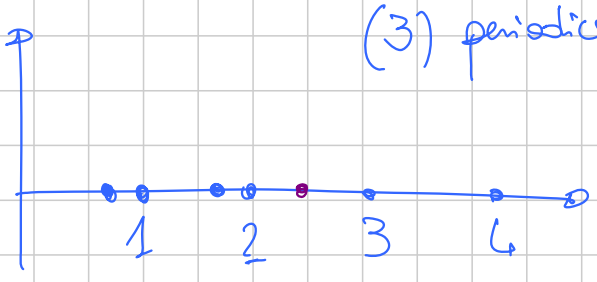
Quali sono le sol. di $(*)$? $\quad [h(y + \log 2) = h(y) + 1]$



Esistono funzioni che (1) risolvono ~~$f(x+y) = f(x) + f(y)$~~

(2) periodica di periodo 1

(3) periodica di periodo π



Basi di Hamel:

Voglio costruire insiemi di elementi <u>indipendenti</u> su $\mathbb{R}$

S indipendente se non c'è una comb. lineare (finita) (non nulla) di elementi di S a coeff. razionali che fa 0

Es:

$\{1, \sqrt{2}\}$ è indipendente perché $q_1 \cdot 1 + q_2 \cdot \sqrt{2} = 0$ solo se $q_1 = q_2 = 0$

$\left\{1+\sqrt{2}, \frac{3}{2}+\frac{7}{5}\sqrt{2}, 5+18\sqrt{2}\right\}$ è non indipendente

Dato S indipendente (anche infinito), ho due casi: o c'è α tale che $S \cup \{\alpha\}$ è indip. oppure ogni $\alpha \in \mathbb{R}$ si scrive come comb. lineare di el. di S

"A un certo punto", aggiungendo el., arrivo nel caso 2

Un S "saturo" si chiama base di Hamel.

Se io scelgo $f(s)$ a piacere per ogni $s \in S$, posso estendere questa funzione a $\mathbb{R}$:

dato α, $\alpha = q_1 s_1 + q_2 s_2 \dots q_k s_k$ per qualche $q_i \in \mathbb{Q}$, $s_i \in S$

$$f(\alpha) = q_1 f(s_1) + q_2 f(s_2) + \dots + q_k f(s_k)$$

f costruita così soddisfa l'eq. di Cauchy

È mio diritto: prendere $\{1, \pi\}$, trovare $S \supseteq \{1, \pi\}$, costruire f che risolve la Cauchy, tale che $f(1) = f(\pi) = 0$ e f(un altro el. della base) $\neq 0$.

$$f(\dots) + f(\dots) + \boxed{2 \times f(k)} \neq 0$$

↓ assume tutti i valori $\in \mathbb{R}$, se $f(k) \neq 0$.

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

$$\begin{cases} f(xy) = f(x) f(y) \\ f(x+y) = f(x) f(y) \\ f(xy) = f(x) + f(y) \end{cases}$$

TI Senior 2015 $\quad ffx = f0$

$f(xy + f(x)) = f(7xy)$ ha sol. non costanti?

$f(z + f(x)) = f(7z) \quad \forall z, x \in \mathbb{R}$

$a, b \in \operatorname{Im} f$

$\mathbb{Z}$ e $\frac{\mathbb{Z}}{7} + f(x)$ $\forall x$ stanno nella stessa scatola

Per es., solo 0, 1 nell'immagine

z sta nella stessa scatola di: $\frac{z}{7}$ e $\frac{z}{7}+1$

$$f(x) = \begin{cases} 0 & x \in \mathbb{Q} \\ 1 & x \notin \mathbb{Q} \end{cases}$$

TST01: trovare tutte le $f: \mathbb{R}^+ \to \mathbb{R}^+$

P: $f(x + yf(x)) = f(x)f(y)$ e $\exists$ solo un # finito di x tali che $f(x)=1$

"$f^{-1}(1)$ finito"

$P(1,1)$: $f(1+f(1)) = [f(1)]^2$

Step 1: sia α t.c. $f(\alpha)=1$; allora

$P(\alpha,\alpha)$: $f(\alpha+\alpha) = 1$ ⇝ $f(2\alpha)=1$

⇝ non può esserci nessun valore α t.c. $f(\alpha)=1$, se no ce ne sono ∞

Step 2: iniettività.

Suppongo di avere $f(a)=f(b)$: $b>a$ pongo

$x=a$ $\quad b = x + yf(x)$ (ci riesco?) $\quad y = \frac{b-a}{f(a)}$

Mi viene

$P\left(a, \frac{b-a}{f(a)}\right)$: $f(b) = f(a) f\left(\frac{b-a}{f(a)}\right)$

⇝ $f\left(\frac{b-a}{f(a)}\right) = 1$, impossibile!

Step 3:

$$f(x+yf(x)) \overset{P(x,y)}{=} f(x)f(y) = f(y)f(x) \overset{P(y,x)}{=} f(y+xf(y))$$

$$x+yf(x) = y+xf(y)$$

$$y(f(x)-1) = x(f(y)-1) \qquad \frac{f(y)-1}{y} = \frac{f(x)-1}{x} = \text{costante}$$

$$\Rightarrow f(x) = cx+1$$

BMO '07 $f:\mathbb{R}\to\mathbb{R}$ t.c.

P: $f(f(x)+y) = f(f(x)-y)+4yf(x)$

Oss: $f(x)=x^2$ è soluzione, quindi non ho speranze di dimostrare iniettività & suriettività

Idea 1: $P(x, f(y))$:

$$f(f(x)+f(y)) = f(f(x)-f(y))+4f(y)f(x)$$

$$f(f(x)-f(y)) \overset{P(x,y)}{=} f(f(x)+f(y))-4f(x)f(y) \overset{P(y,x)}{=} f(f(y)-f(x))$$

f pari sugli oggetti che si scrivono come $f(\text{roba})-f(\text{altra roba})$

Cosa sta in $\mathrm{Im}f - \mathrm{Im}f$?

Se scelgo x t.c. $f(x)\neq 0$ (se non c'è allora $f\equiv 0$).

$y=\frac{a}{4f(x)}$, allora

$P\left(x, \frac{a}{4f(x)}\right): f(\text{mostro}) - f(\text{mostro}) = a$

ho ogni reale sta in $\mathrm{Im}f - \mathrm{Im}f$.

Quello qui sopra dimostra $f(a)=f(-a)\ \forall a\in\mathbb{R}$

Il testo mi dà $f(f(x)+f(y))$.

Riesco a fare $f(f(x)+f(y)+f(z))$?

[Altra idea tipica: faccio $x\mapsto x+a$ e vedo cosa cambia, $P(x+a,y)-P(x,y)$]

$$f\left(f(x)+f(y)+z\right) \overset{P(x,f(y)+z)}{=} f\left(f(x)-f(y)-z\right) + 4f(x)f(y) + 4f(x)z$$

simm. in x,y — simm. in x,y

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

Ponendo di nuovo $f(x)-f(y)=t$ (perché posso?)

viene

$$f(t-z)-f(-t-z) = -4tz \qquad \forall z\in\mathbb{R},\ \boxed{\forall t\in\mathbb{R}}$$

→ perché?

SL2005 trovare $f:\mathbb{R}^+\to\mathbb{R}^+$ t.c.

$$f(x)f(y) = 2f\left(x+yf(x)\right) \qquad \forall x,y\in\mathbb{R}^+$$

Step 1: provo a rendere uguali due termini

$P(x,x): \quad x[f(x)]^2 = 2f(x+xf(x))$ inutile

$y = x + yf(x)$ se $y = \frac{x}{1-f(x)}$. Riesco a renderli uguali se $f(x) < 1$

In tal caso $P\left(x, \frac{x}{1-f(x)}\right): \quad f(x) f\left(\frac{x}{1-f(x)}\right) = 2f(\square)$

$\Rightarrow f(x) = 2$ ... ma $f(x) < 1$!

$\Rightarrow f(x) < 1$ è impossibile $\quad \mathrm{Im} f \subseteq [1, +\infty)$

Step 2:

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

a b roba

$a \in \mathrm{Im} f, \ b \in \mathrm{Im} f \Rightarrow \frac{ab}{2} \in \mathrm{Im} f$

Es: se no avessi $m = \min \mathrm{Im} f$, allora

$P(f^{-1}(m), f^{-1}(m)): \quad m^2 = 2f(\text{roba}) \geq 2m$

$\Rightarrow m \geq 2$

(ma un minimo negativo l'immagine non ce l'ha)

Alternativa:

Supponiamo che $a < 2$ stia nell'immagine:

Allora ci sta anche $a \frac{a^2}{2} = \left(\frac{a}{2}\right)^n \cdot a$ per ogni n

... $\frac{a}{2} \cdot \frac{a}{2} \cdot \frac{a}{2}$

Se $a_n < 2$, per n abbastanza grande ottengo $\left(\frac{a}{2}\right)^n \cdot a < 1$, ma è assurdo perché non ho elementi < 1 nell'immagine

Step 3: crescenza

$$f(x)f(y) = 2f\left(x + yf(x)\right)$$

Dati $a < b$, posso avere $x = a$, $b = x + yf(x)$

$$y = \frac{b-a}{f(a)}$$

$$P\left(a, \frac{b-a}{f(a)}\right): \quad f(a)f(\text{mostro}) = 2f(b)$$

$$f(b) = \frac{f(\text{mostro})}{2} f(a) \geq f(a)$$

$= \text{sse } f(\text{mostro}) = 2$

crescenza debole

A me piacerebbe crescenza forte

$a < b \Rightarrow f(a) < f(b)$ cresc. forte

$a \leq b \Rightarrow f(a) \leq f(b)$ cresc. debole

$\Leftarrow$ ✗ falso

2 casi:

- $\text{Im } f \subseteq (2, \infty)$: allora, f strettamente crescente

e pure iniettiva

$$f(x)f(y) = 2f\left(x + yf(x)\right)$$

$P(x,y)$ & $P(y,x)$

$$f\left(x+yf(x)\right) \overset{?}{=} f\left(y+xf(y)\right)$$

finito se so iniettività

- caso 2: $\exists\ b$ t.c. $f(b)=2$

Allora $P(b,b)$: $2\cdot 2 = 2f(b+2b) \Rightarrow f(3b)=2$

Se $f(b)=2$, allora anche $f(3b)=2$, $f(9b)=2$,

$f(27b)=2$, ...

e per crescenza debole dev'essere f costante $=2$.

C2 Medium

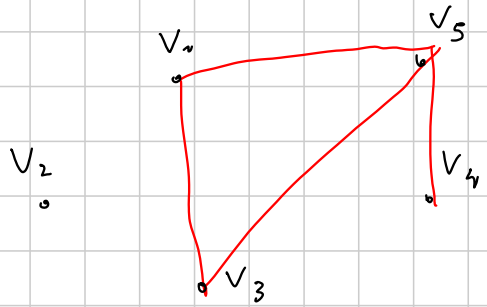
Andrea

Titolo nota 05/09/2015

GRAFO = (V, E)

V insieme finito, contenente i "vertici"

E è un insieme, contiene alcune coppie (non ordinate) di vertici distinti, dette "archi"



CAMMINO = sequenza di vertici, ognuno collegato al precedente e al successivo

Esempio V_4 V_5 V_3 V_1 V_3 V_5 V_1

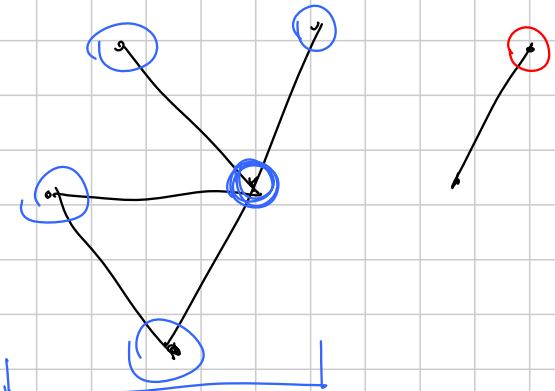
~~CAMMINO SEMPLICE~~ : non contiene due volte lo stesso vertice

CAMMINO CHIUSO : l'ultimo vertice è uguale al primo

CICLO cammino semplice, a parte l'ultimo vertice che è uguale al primo (e con almeno 3 vertici distinti).

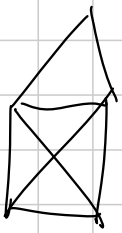
GRAFO CONNESSO Dati un vertice di partenza e uno

di arrivo, c'è un cammino che li collega



PROBLEMA DEI CIRCUITI EULERIANI

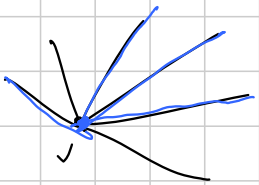
Ho un grafo, riesco a disegnarlo senza staccare mai la matita?



Esiste un cammino chiuso che contiene esattamente una volta ogni arco?

È necessario che:

- il grafo sia connesso (a parte punti isolati);
-



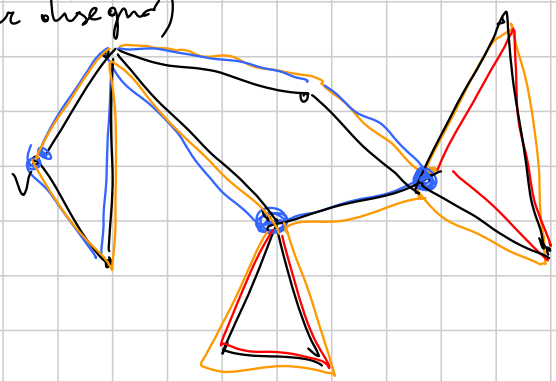
Serve che tutti i vertici abbiano grado pari, compreso il vertice di partenza e arrivo

GRADO di un vertice V in un grafo = n° di archi che escono da quel vertice V = $\deg(V)$

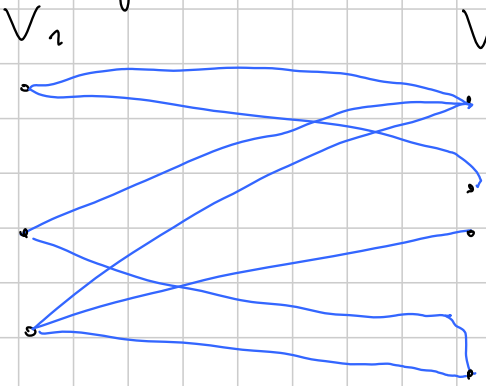
$$\sum_{v \text{ vertice}} \deg(v) = 2|E|$$

Teorema (Eulero) Se un grafo è connesso e i gradi sono pari, allora esiste un **circuito euleriano**

DIM (qui disegno)



GRAFO BIPARTITO: i vertici V sono divisi in due sottoinsiemi V_1 e V_2 ($V_1 \cap V_2 = \emptyset$ $V_1 \cup V_2 = V$) e gli archi collegano un vertice in V_1 con uno in V_2



Dato un grafo connesso (V, E), come possiamo capire se è bipartito?
È necessario che ogni cammino chiuso abbia lunghezza pari.

Teorema (grafi bipartiti) Se un grafo è connesso e i suoi cammini chiusi hanno tutti lunghezza pari, allora è bipartito.

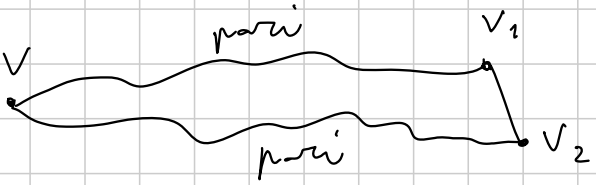
DIM Scelgo un vertice v e lo metto in V_1.

Definizione Dati due vertici w_1, w_2 di un grafo connesso, la distanza è la minima lunghezza di un cammino da w_1 a w_2. $d(w_1, w_2)$

IDEA Metto in V_1 i vertici w per cui $d(v, w)$ è pari

e in V_2 i vertici w per cui $d(v, w)$ è dispari

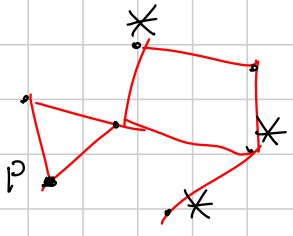
Perché funziona? Se per assurdo ci fosse un $w_1 \in V_1$ e un $w_2 \in V_1$ collegati da un arco, otterrei un cammino chiuso dispari così:



Similmente per $w_1, w_2 \in V_2$

Se un grafo non è bipartito, allora c'è un cammino chiuso di lunghezza dispari. In realtà c'è anche un ciclo di lunghezza dispari (esercizio)

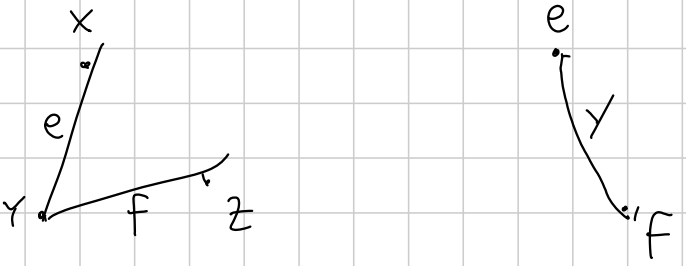
PROBLEMA



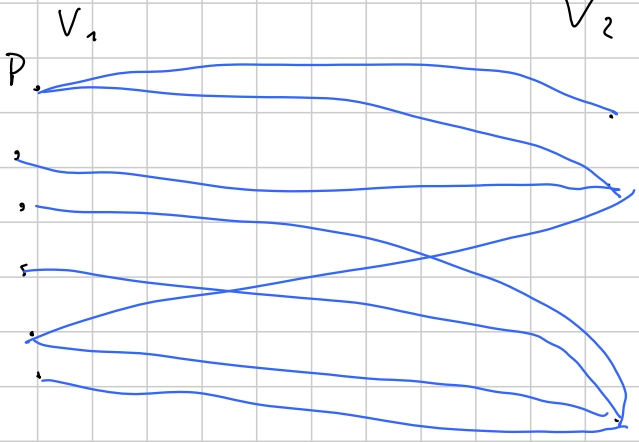
Su ogni vertice c'è una lampadina, accesa o spenta

Una pulce vuole spegnere tutte le lampadine. La pulce può saltare lungo gli archi e deve partire e tornare in P. Ogni volta che arriva in un vertice, cambia lo stato di quella lampadina. (Anche P ha una lampadina).
Per quali grafi la pulce è sicura, qualsiasi sia la configurazione di lampadine accese e spente, di partenza?
OSS Serve un grafo connesso.

Precisazioni P è fissato, la pulce può passare più volte in P

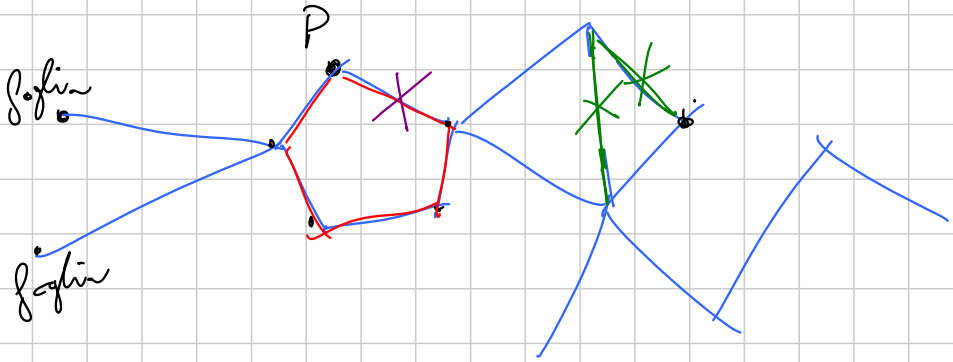


Cosa succede con un grafo bipartito?



Ogni cammino chiuso ha lunghezza pari, quindi se la pulce parte e torna in P, nel percorso opera un numero pari di cambiamenti. Se all'inizio c'è una quantità dispari di lampadine accese, la pulce non riuscirà nell'impresa

Se esiste un ciclo dispari, allora c'è speranza

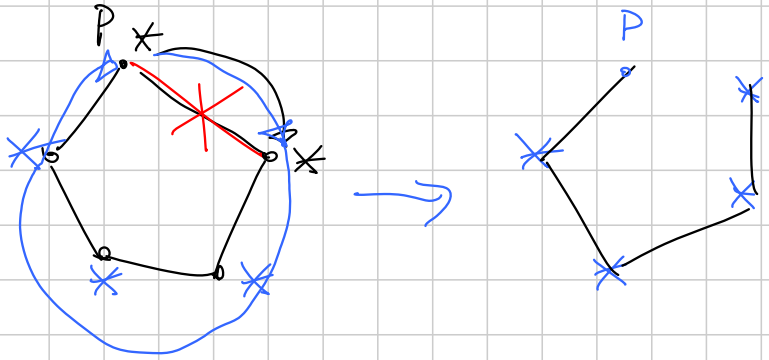


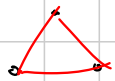
OSS Se crediamo nella congettura possiamo semplificare il grafo cancellando uno alla volta tutti i vertici che non toccano il ciclo dispari né disconnettono il grafo.

Definizione Un albero è un grafo connesso senza cicli.

OSS Se ora tolgo un arco dal ciclo dispari, rimane un albero.

OSS Posso cambiare P, per esempio supporre che sia sul ciclo dispari. Spengo le foglie dell'albero ottenuto una a una; rimane P

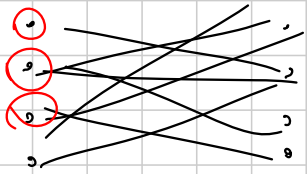


Problema di Turán Ho un grafo con n vertici senza triangoli (senza configurazioni del tipo )

Quanti archi ha al massimo? $(n \geq 3)$

- Un albero ha $n-1$ archi
- Un grafo bipartito con $\lfloor \frac{n}{2} \rfloor$ vertici da una parte e $\lceil \frac{n}{2} \rceil$ vertici dall'altra e tutti gli archi possibili ha $\lfloor \frac{n^2}{4} \rfloor$, che già sono un buon numero

(la stima sciocca è $\binom{n}{2} = \frac{n^2-n}{2}$



Idea: diamo dei pesi ai vertici

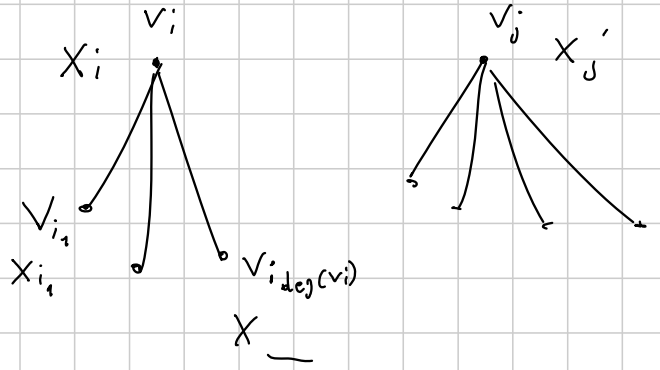
$V = \{v_1, v_2, \dots, v_n\}$. v_i ha peso $x_i \geq 0$

Imponiamo $\sum_{i=1}^{n} x_i = n$ cioè il peso medio è 1.

Cerchiamo di massimizzare $S = \sum_{\substack{0 \leq i < j \leq n \\ \{v_i, v_j\} \in E}} x_i \cdot x_j$

OSS Se tutti gli $x_i = 1$ allora $S = |E|$

<u>OSS.</u> Se ho due vertici non collegati v_i, v_j, mi conviene spostare tutto il peso di uno sull'altro



<u>OSS</u> Il massimo si ha in una configurazione in cui tutti i vertici con peso non nullo sono collegati da un arco (formano una "cricca")

<u>OSS</u> L'algoritmo termina, perché a ogni passo aumenta il numero di x_i nulli.

Alla fine il peso rimane su al più due vertici v_i, v_j. Allora $S = x_i \cdot x_j \leq \left(\frac{x_i + x_j}{2}\right)^2 = \frac{n^2}{4}$

$|E| \leq \frac{n^2}{4}$ e visto che $|E|$ è intero...

In generale se un grafo su n vertici non contiene cricche di r vertici, allora ci sono al più

$$\left(1 - \frac{1}{r-1}\right)\frac{n^2}{2} \quad \text{archi}$$

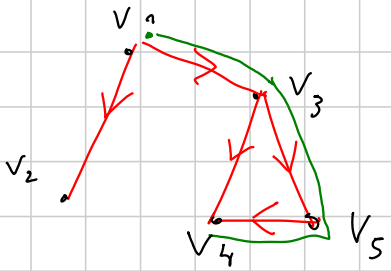
(Dovrebbero funzionare gli stessi argomenti)

(Caro-Wei)

PROBLEMA Ho un grafo con n vertici e con $|E|$ archi, cerco un'anticricca (insieme di vertici a due a due scollegati). Quanto grande la riesco a trovare? Almeno

$$\frac{n}{2|E|/n + 1}$$

GRAFO ORIENTATO Grafo in cui gli archi hanno una direzione privilegiata

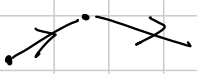
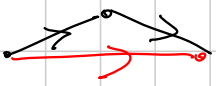


Di solito tra due vertici si suppone che ci sia al massimo un arco (e nel caso non l'altro)

CAMMINO Come prima ma devo muovermi rispettando le orientazioni

CICLO Cammino chiuso semplice

GRAFO ORIENTATO ACICLICO Non esistono cicli orientati (ma magari ne esistono di non orientati)

ORDINE PARZIALE Grafo orientato aciclico in cui ogni  si completa a una 

Altrimenti un ordine parziale è un insieme V con una relazione $\prec$ tra alcune coppie di elementi, per cui

- $V \not\prec V$
- $V \prec W \prec Z$ allora $V \prec Z$
- $V \prec W$ allora $W \not\prec V$

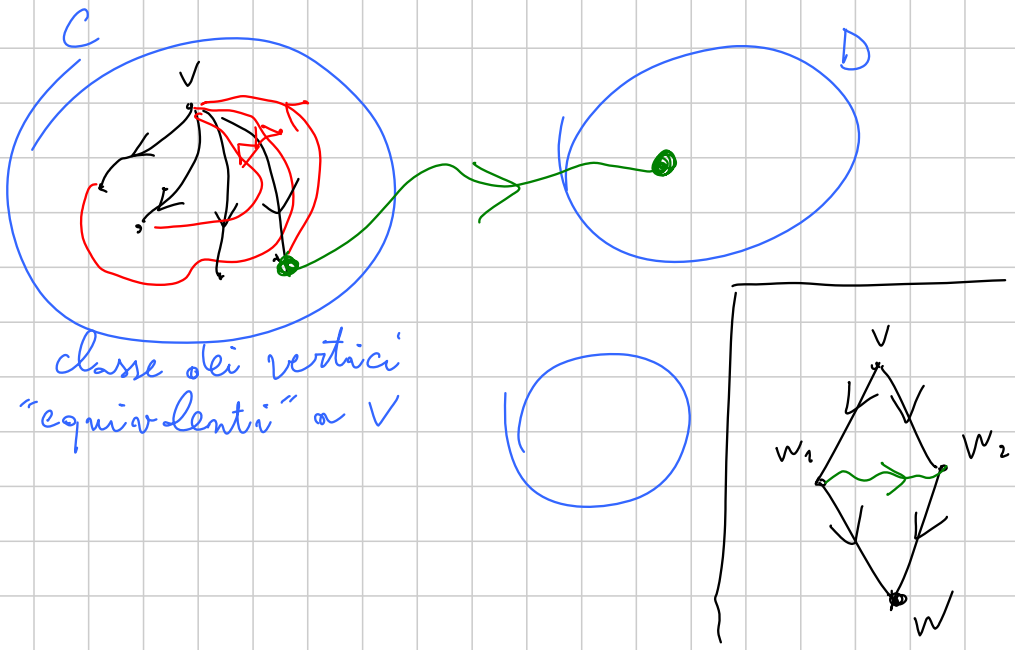
Esempio S insieme, $\left(\mathcal{P}(S), \subsetneq\right)$ è un ordine parziale

Esempio $\{1, 2, 3, \dots\}$ con l'ordine della divisibilità

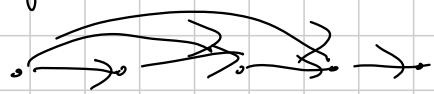
$m \prec n$ se $m \mid n$ e $m \neq n$

Dato un grafo orientato, diciamo che $V \prec W$ se c'è un percorso orientato da W a V.

È un ordine parziale? Sì, ma tra le classi di vertici equivalenti



CATENA: sottoinsieme di un ordine parziale in cui tutti gli elementi sono confrontabili.



ANTICATENA: sottoinsieme / / / / / / / / / / sono inconfrontabili

. . . . .

Esempio $\mathbb{R}^2 = \{(x,y) \text{ con } x,y \in \mathbb{R}\}$ — è un ordine parziale

$(x,y) \prec (a,b)$ se $x \leq a$ e $y \leq b$

$(1,1) \prec (2,2) \prec (3,3) \prec \dots$ è una catena

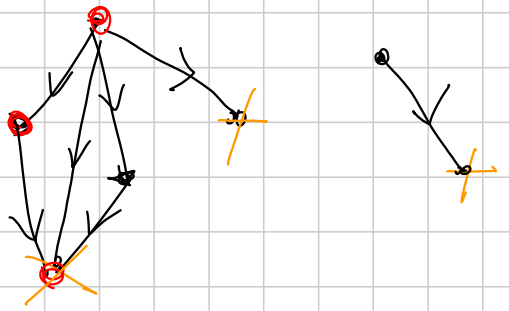
$(1,-1), (2,-2), (3,-3), \dots$ è una anticatena

TEO (Dilworth) 1) Prendiamo un insieme S (finito) parzialmente ordinato. Supponiamo che la massima lunghezza di una catena sia K. Allora si può partizionare S in K anticatene.

2) Come il punto 1, in cui si scambiano le parole "catena" e "anticatena"

OSS Se nel punto 1 provo a dividere S in meno di K sottoinsiemi, uno di questi contiene due elementi della catena lunga, e questi sono confrontabili $\Rightarrow$ questo sottoinsieme non è un'anticatena.

DIM di 1



X sono i minimali

Definizione In un ordine parziale S un elemento m si dice MINIMALE se è minore o inconfrontabile con ogni altro

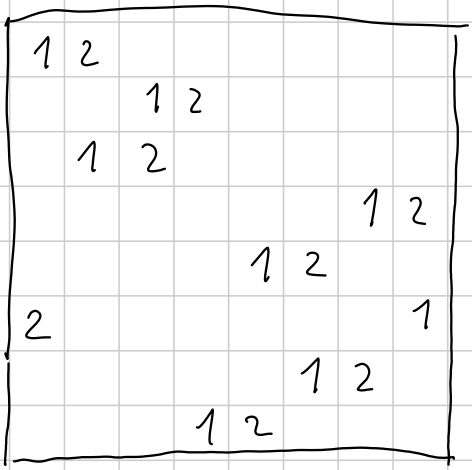
OSS I minimali sono un'anticatena

OSS Ci sarebbe l'analogo concetto di MASSIMALE...

OSS Ogni catena di lunghezza massima k termina con un minimale.

(estesa)

Induzione su k, oppure su $|S|$



Scacchiera $n \times n$

Un 1 su ogni riga e su ogni colonna già dato.

Poss aggiungere un 2 su ogni riga e su ogni colonna (a destra degli 1).

1		2	
	1		2
		1	2
	2		1
2			1

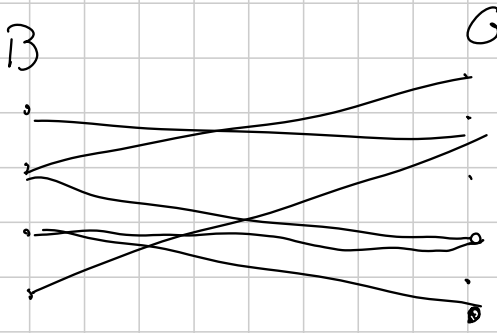
Si riesce ad aggiungere un 3?
E se sì, poi come andrà per il 4?

LEMMA DEI MATRIMONI (Teo. di Hall)
C'è un insieme di ragazzi B e un insieme di ragazze G. Ad ogni ragazzo piacciono alcune ragazze. Lo scopo è dare ad ogni ragazzo una moglie diversa, tra quelle che gli piacciono.
In quali casi è possibile?

OSS È necessario che $|G| \geq |B|$

Di più: se $A \subseteq B$, posso definire

$$\Gamma(A) = \{ g \in G \text{ per cui esiste almeno un } b \in A \text{ t.c. } g \text{ piace a } b \}$$



Serve $|A| \leq |\Gamma(A)|$.
Il teorema asserisce che se $\forall A \subseteq B$ vale $|\Gamma(A)| \geq |A|$, allora c'è un modo di creare

i matrimoni.

DIM Induzione su $|B|$. Passo base $|B| = 0, 1$ ok.

PASSO INDUTTIVO

Ci sono due possibilità:

① $\forall A \subseteq B$ con $A \neq \emptyset$, $A \neq B$, vale $|\Gamma(A)| > |A|$

② $\exists A \subseteq B$ con $A \neq \emptyset$, $A \neq B$ per cui $|\Gamma(A)| = |A|$

Nel caso ① creo un matrimonio a caso (tra b e g) e riduco il numero di ragazzi.

Se $A \subseteq B \setminus \{b\}$, $A \neq \emptyset$, $|\Gamma(A) \setminus \{g\}| \geq |\Gamma(A)| - 1 \geq |A|$ perché siamo nel caso ①

Nel caso ② divido il problema in due: cerco di far sposare A con $\Gamma(A)$, e separatamente $B \setminus A$ con $G \setminus \Gamma(A)$. Verifichiamo che valgano le ipotesi:

$\forall C \subseteq A \quad \Gamma(C) \subseteq \Gamma(A)$ e $|C| \leq |\Gamma(C)|$

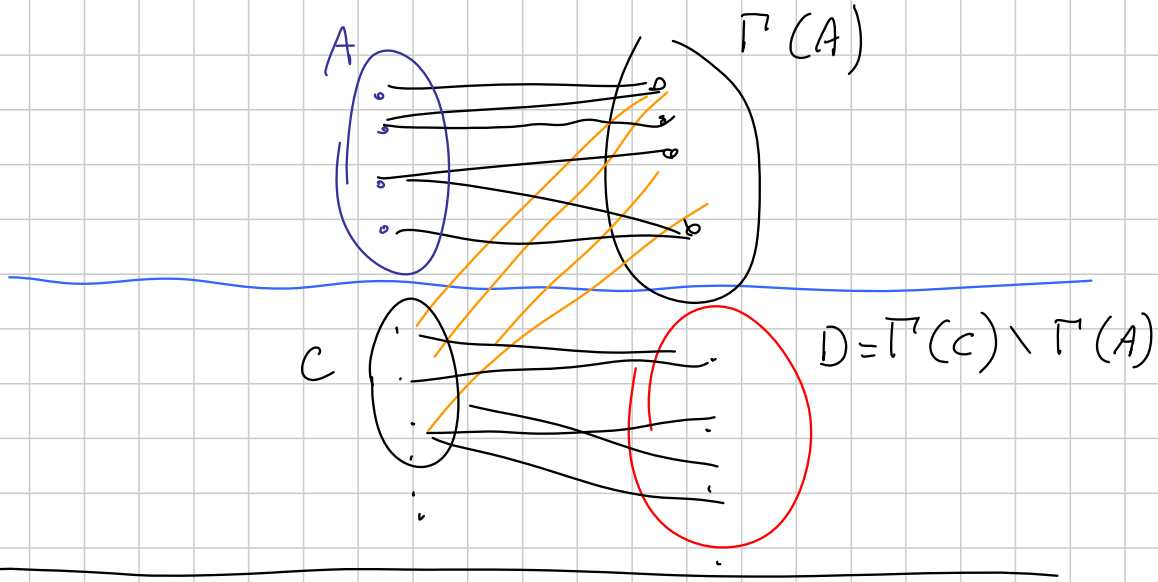
$\forall C \subseteq B \setminus A$ devo verificare che $|C| \leq |\Gamma(C) \cap (G \setminus \Gamma(A))|$

Considero $A \cup C$ che ha $|A| + |C|$ elementi

$$\Gamma(A \cup C) = \Gamma(A) \cup \left(\Gamma(C) \cap (G \setminus \Gamma(A))\right)$$

che ha $|\Gamma(A)| + |\Gamma(C) \cap (\sim)| \geq |A \cup C|$

$|A| + |\sim|$ $\qquad = |A| + |C|$



LEMMA AUSILIARIO PER I MATRIMONI. Supponiamo che $\forall b$ e g collegati, $\deg(b) \geq \deg(g)$. Allora è possibile organizzare i matrimoni, in quanto sono soddisfatte le ipotesi del lemma di Hall.

COROLLARIO Se $\deg(b) \geq \deg(g)$ sempre, allora esistono i matrimoni.

1		2	3	
	1	3		2
		1	2	3
3	2		1	
2	3			1

Si può far sposare a ogni riga una colonna diversa, tra quelle nella cui intersezione non c'è scritto nulla? I gradi sono tutti uguali, quindi sì per il corollario.

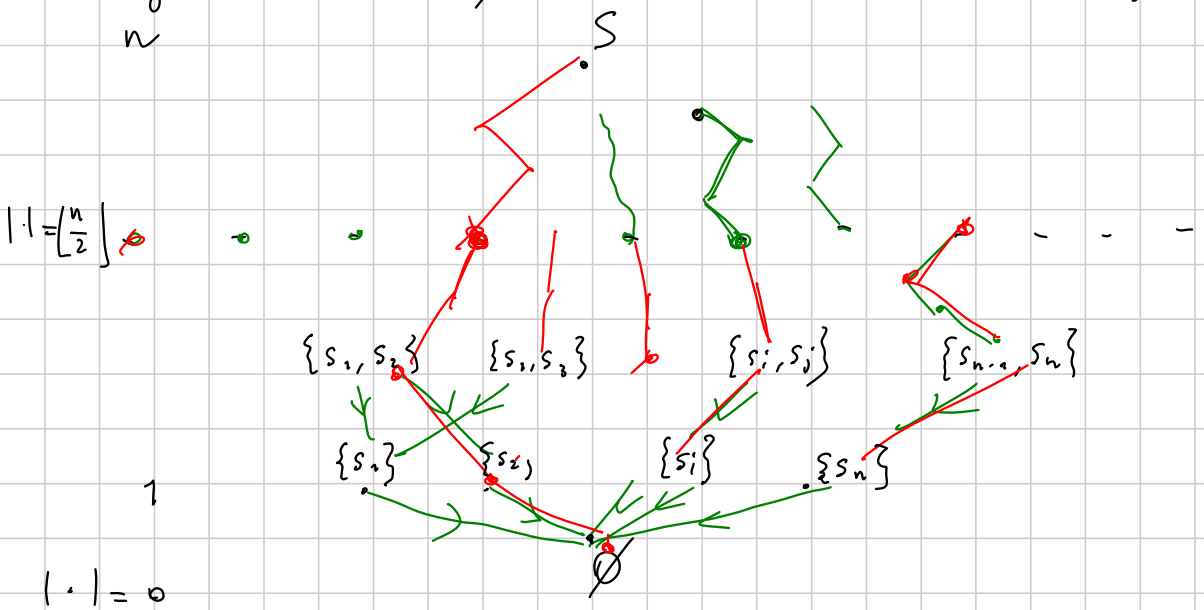
Problema di Sperner S insieme di n elementi. $(\mathcal{P}(S), \subseteq)$ è un orline parziale. Cerchiamo un'anticatena di dimensione massima. Quanto sarà grande?

Idea Prendo tutti gli insiemi di una certa cardinalità X: così sono sicuro che nessuno ne includerà un altro.

Come X scelgo $\left\lfloor \frac{n}{2} \right\rfloor$ perché tra gli $\binom{n}{X}$ il più grande è $\binom{n}{\lfloor \frac{n}{2} \rfloor}$.

Effettivamente non si fa di meglio

Disegniamo $\mathcal{P}(S)$ $\qquad S = \{s_1 - - s_n\}$



$k < \frac{n}{2}$. Vogliamo creare matrimoni tra

$B = \{$ sottinsiemi di k elementi $\}$ e $G = \{$ sott. di $k+1\}$

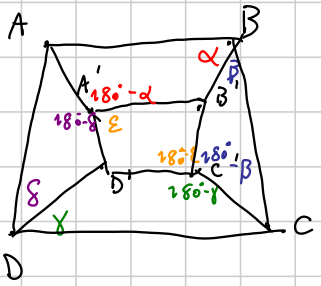
Usiamo il corollario: ogni lo conosce $n-k$

elementi di G. Viceversa, ogni g conosce $k+1$ elementi. $k+1 \leq n-k$ segue da $k < \frac{n}{2}$ e k intero.

G3 MEDIUM Anér

Titolo nota 06/09/2015

PROBLEMA A,B,C,D,A',B',C',D' punti del piano t.c. quadrilateri $A'B'C'D'$, $ABB'A'$, $BCC'B'$, $CDD'C'$ e $DAA'D'$ sono ciclici. Allora $ABCD$ è ciclico



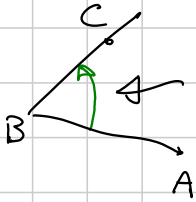
DIM $\alpha+\beta+\gamma+\delta = 180°$

$180°-\alpha + 180°-\beta + 180°-\gamma + 180°-\delta = 540°$

$\Downarrow$

$\alpha+\beta+\gamma+\delta = 180°$

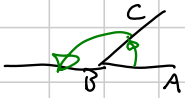
Angoli orientati:

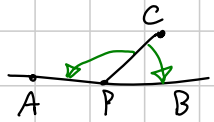


$\measuredangle ABC$ è l'angolo di cui ruotare la retta AB in senso antiorario perché diventi parallela a BC

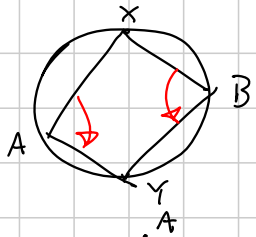
Consideriamo gli angoli orientati modulo $180°$

Proprietà: $\star\ \measuredangle ABC = -\measuredangle CBA$



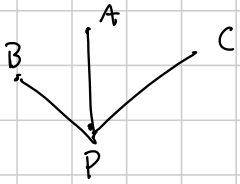
$\times$: 

A,P,B allineati $\iff \measuredangle CPA = \measuredangle CPB$

$*$: 

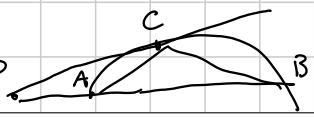
A,B,X,Y concicli $\iff \measuredangle XAY = \measuredangle XBY$

$\star\measuredangle ABC + \measuredangle BCA + \measuredangle CAB = 0$ sempre

$\star$: 

$\measuredangle APC = \measuredangle APB + \measuredangle BPC$

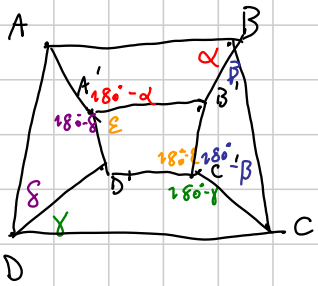
PC è tg a $\mathrm{cfr}(ABC)$ $\iff \measuredangle PCA = \measuredangle CBA$

$\star$ 

Tesi $\measuredangle ABC = \measuredangle ADC$

$\measuredangle ABB' + \measuredangle B'BC = \measuredangle ADD' + \measuredangle D'DC$

$\measuredangle AA'B' + \measuredangle B'C'C = \measuredangle AA'D' + \measuredangle D'C'C$

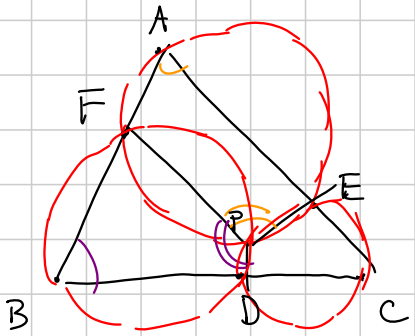


$\measuredangle AA'B' + \measuredangle D'A'A + \measuredangle B'C'C + \measuredangle CC'D' = 0$

$\measuredangle D'A'B' + \measuredangle B'C'D' = 0$ è equivalente alla tesi, ed è vera

---

Teorema di Miquel



ABC triangolo, $D \in BC$ retta

$E \in CA$, $F \in AB$.

Γ_A circoscritta a AFE

Γ_B // DBF

Γ_C // CDE

Tesi: $\Gamma_A, \Gamma_B, \Gamma_C$ concorrono

DIM Chiamo P la 2ª intersezione tra Γ_A e Γ_B oltre a F. (Se Γ_A e Γ_B sono tangenti, allora $P = F$ e quando scrivo FP intendo la tangente comune)

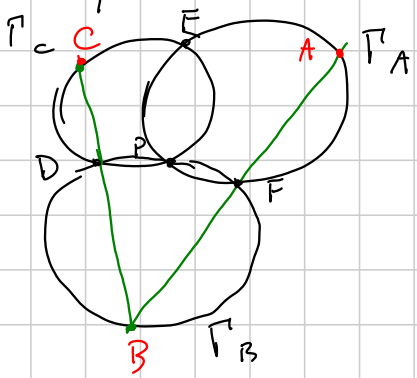
Tesi: $\measuredangle DPE = \measuredangle DCE$

Supponiamo che $\measuredangle DPE = \measuredangle DPF + \measuredangle FPE =$

$= \measuredangle DBF + \measuredangle FAE = \measuredangle CBA + \measuredangle BAC =$

$= \measuredangle BCA = \measuredangle DCE$

Miquel "inverso"



$\Gamma_A, \Gamma_B, \Gamma_C$ si incontrano in P
e a coppie in D, E, F.

AFB allineati, BDC allineati.

Allora CEA allineati

DIM Tesi: $\sphericalangle CEP + \sphericalangle PEA = 0$

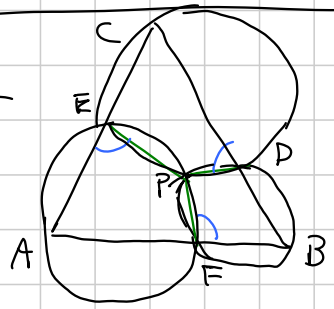
$\parallel$

$\sphericalangle CDP + \sphericalangle PFA$

$\parallel$

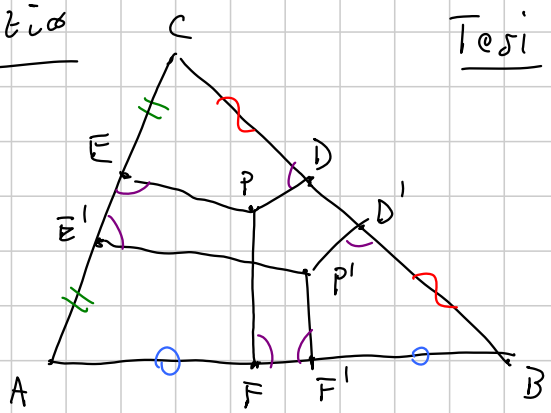
$\sphericalangle BDP + \sphericalangle PFB$ che si fa a 0

OSS



I tre angoli azzurri sono uguali

Esercizio

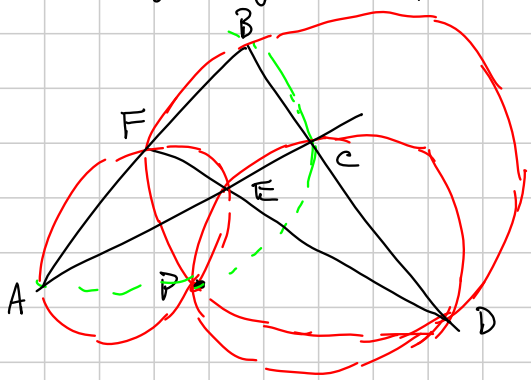


Tesi Gli angoli viola sono tutti uguali

1° TEOREMA DI MIQUEL Date 4 rette l, m, n, p queste determinano 4 triangoli (prese a 3 a 3), i quali hanno 4 circ. circoscritte.
Tesi: queste 4 circonferenze concorrono

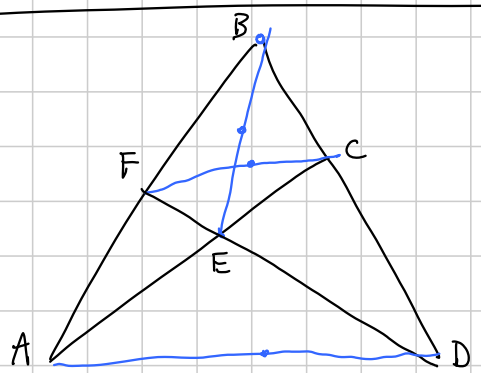
OSS Basta dimostrare che 3 di queste concorrono (esercizio: giustificare per bene)

DIM



Applico Miquel a ABC con i punti D, E, F.

ESERCIZIO



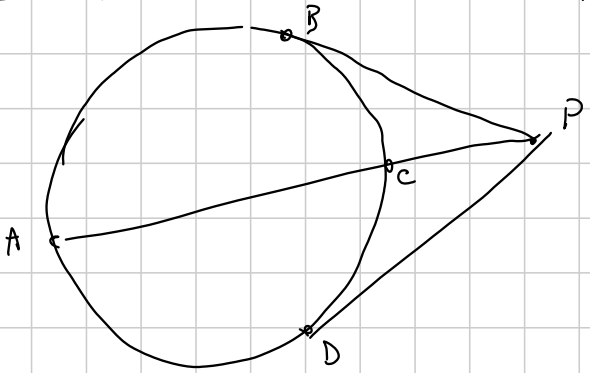
4 rette
4 triangoli
4 ortocentri allineati su una retta ℓ

I 3 punti medi di BE, CF, AD sono allineati su una retta S

$\ell \perp S$

(Consiglio: tracciare le circ. di diametri AD, BE, CF e cercare il "centro radicale")

QUADRILATERI ARMONICI



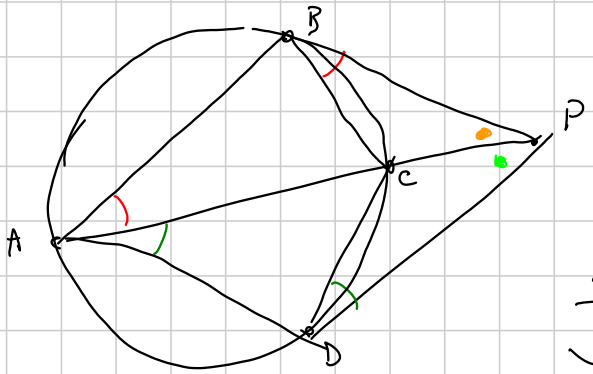
$AB \cdot CD = AD \cdot BC$

DEF Un quadril. $ABCD$ si dice armonico se è ciclico

e $AB \cdot CD = AD \cdot BC$

Teo Sia $ABCD$ ciclico. Allora $ABCD$ è armonico se e solo se le tangenti alla cfr. circo. per B e per D concorrono con AC, se e solo se qualcosa di simile accade per le tg in A, in C e la retta BD.

DIM Supponiamo AC, t_{g_B}, t_{g_D} concorrenti in P

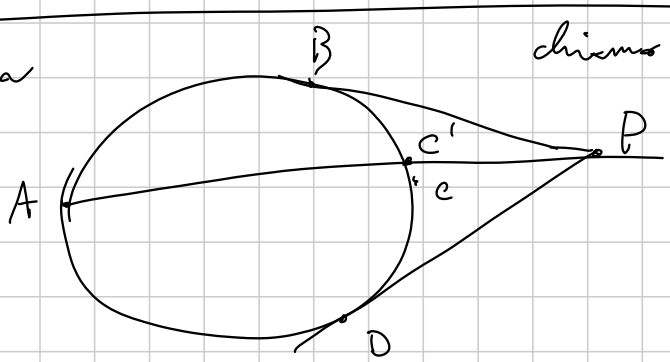


$PBC \sim PAB$
$PCD \sim PDA$
} per angoli

$$\frac{AB}{BC} = \frac{AP}{BP} \quad ; \quad \frac{AD}{DC} = \frac{AP}{DP}$$

segue la tesi perché $PB = PD$

Viceversa



chiamo $P = t_{g_B} \cap t_{g_C}$

$PA \cap cfr = C'$

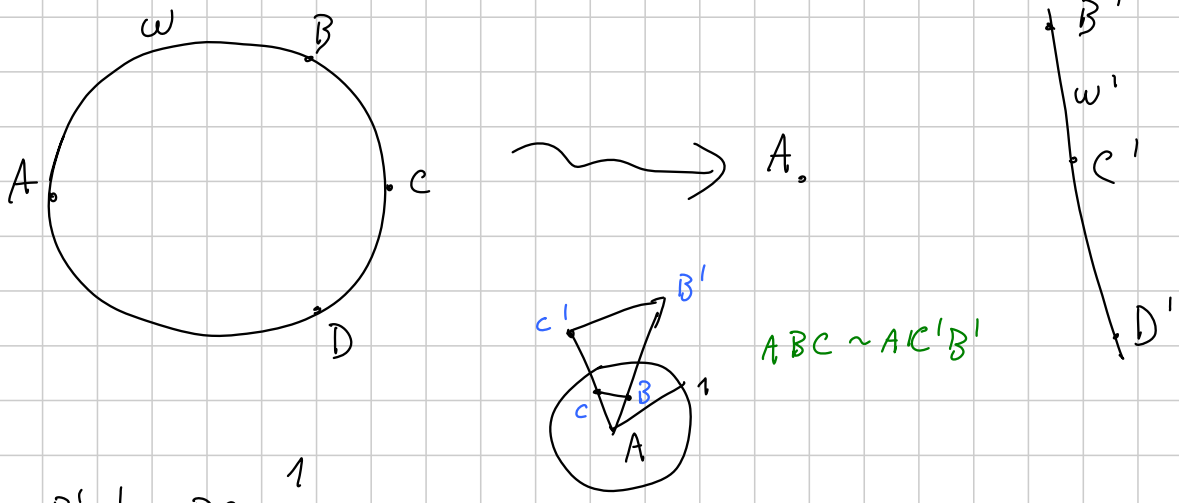
Voglio dimostrare che $C \equiv C'$. C, C' sono sull'arco $\overset{\frown}{BD}$ che non contiene A. $B\hat{C}D = B\hat{C'}D$

Per ipotesi e usando l'altra freccia $\frac{BC}{CD} = \frac{BA}{AD} = \frac{BC'}{C'D}$

Allora $BCD \sim BC'D$ e ora noto che $BD = BD \Rightarrow BCD \cong BC'D$

e ora è chiaro che $C \equiv C'$.

Altra caratterizzazione: prendo $ABCD$ armonico e applico un'inversione centrata in A (di raggio 1)



$$B'C' = BC \cdot \frac{1}{AB \cdot AC}$$

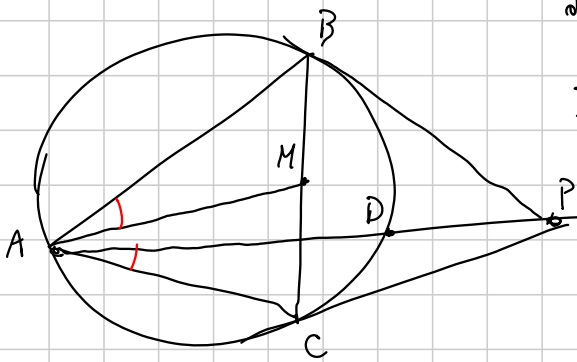
!! sono uguali !!!

$$C'D' = CD \cdot \frac{1}{AC \cdot AD}$$

Morale Se $ABCD$ è armonico e inverto in A, C' sarà il pto medio di $B'D'$. E viceversa (ricontrollare)

LEMMA DELLA SIMMEDIANA

Simmediana = retta simm. della mediana rispetto alla bisettrice



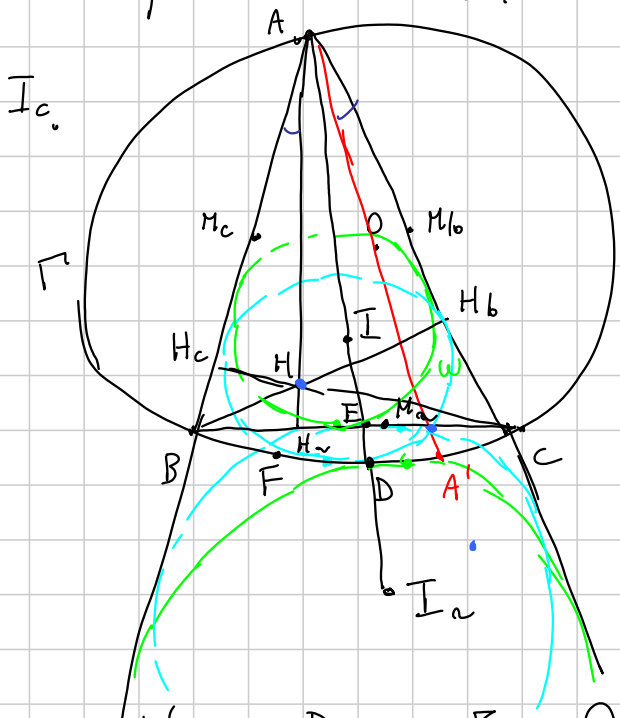
Tesi: AD, tg_B, tg_C concorrono

o equivalentemente

$ABDC$ è armonico

Vediamo la costruzione "inversione + simmetria"

Dato ABC inscritto in Γ, applichiamo la seguente trasformazione: prima inversione con centro in A e raggio $= \sqrt{AB \cdot AC}$; poi simmetrizziamo rispetto alla bisettrice di $\widehat{BAC}$.



$ACFB$ è armonico.

$B \longleftrightarrow C$

$BC \longleftrightarrow \Gamma$

$M_a \longleftrightarrow F$

$I \overset{\text{esercizio}}{\longleftrightarrow} I_a$

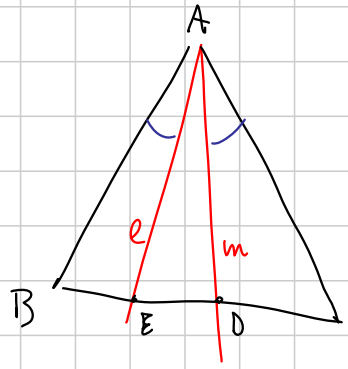
$I_b \longleftrightarrow I_c$

$M_b \longleftrightarrow$ simm. di A risp. a B

$A' \longleftrightarrow H_a$ $\quad D \longleftrightarrow E$ $\quad O \longleftrightarrow$ simm. A risp. a BC

$H \longleftrightarrow$ inverso risp. a Γ di $AO \cap BC$

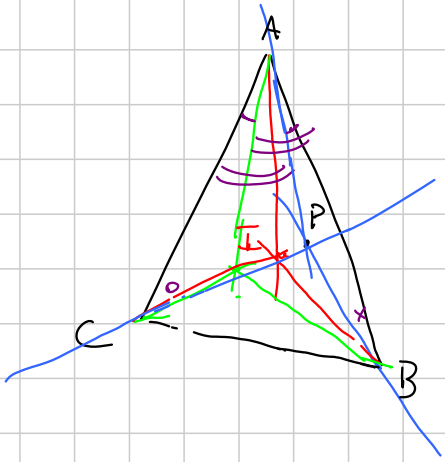
$\omega \longleftrightarrow$ cfr tg. esternamente a Γ, e tg a AB, AC



Se $\sphericalangle BAE = \sphericalangle DAC$ allora l'inv. + simm. scambia le due cevviane AE, AD.

Queste cevviane si dicono isogonali

CONIUGATO ISOGONALE



Simmetrizzo le rette AP, BP, CP rispettivamente rispetto a AI, BI, CI.

Le tre nuove rette concorrono in P', detto coniug isog. di P rispetto al ta. ABC

ortocentro circentro

Esercizi: - H e O sono coniugati isogonali

- P, Q con. isogonali, li proietto sui 3 lati di ABC, ottengo 6 proiezioni. Questi 6 pti sono su una cfr centrata sul pto medio di PQ

TEORIA DEI NUMERI 2 MEDIUM (DARKCRYSTAL)

Titolo nota 05/09/2015

SOMME DI QUADRATI (& ancora residui)

a è RQ mod p $\iff$ $a^{\frac{p-1}{2}} \equiv 1 \pmod p$

Cor: -1 è RQ mod p $\iff$ $p \equiv 1 \pmod 4$ oppure $p = 2$

Lemma: a, b interi, $p \mid a^2 + b^2$ e $p \equiv 3 \pmod 4$

Allora $p \mid a$ E $p \mid b$

Dim Se $p \mid a$ FINE, quindi supponiamo $p \nmid a$.

L'ipotesi è $a^2 \equiv -b^2 \pmod p$

$\iff -1 \equiv (b \cdot a^{-1})^2 \bmod p$

Ma questo è impossibile (perché $p \equiv 3 \bmod 4$) ☠

Oss Supponiamo $x^2 \equiv -1 \bmod p$. (*)

$\operatorname{ord}_p(x) = 4 \mid p-1$

perché $x^4 \equiv 1 \pmod p$, quindi ord $\mid 4$, ma

ord $\neq 2$ ($\neq 1$) per (*)

Primi $\equiv 1 \mod 4$

$5 = 2^2 + 1^2$ ma $5 \nmid 2$, $5 \nmid 1$

Fatto Se $p \equiv 1 \mod 4$, $\exists\, a$ e b t.c. $p = a^2 + b^2$

Dim Per induzione: siano $p_1, p_2, \dots$ i primi $\equiv 1\ (4)$. $p_1 = 5 = 1^2 + 2^2$

Sia p il prossimo primo $\equiv 1\ (4)$

Esiste $c \in \mathbb{N}$ t.c. $p \mid c^2 + 1$, perché -1 è RQ.
$\left(0 \le c \le \frac{p-1}{2}\right)$

$0 < c^2 + 1 \le \left(\frac{p-1}{2}\right)^2 + 1 < p^2$, quindi

$$c^2 + 1 = Kp \quad \text{con } K < p$$

Idea Passare da $m^2 + n^2 = Kp$ a $(m')^2 + (n')^2 = K'p$ con $K' < K$ (se $K \ge 2$)

Come si scrive: prendo K minimo per cui esistono $m, n \in \mathbb{N}_{>0}$ t.c. $m^2 + n^2 = Kp$

Identità $(x^2+y^2)(z^2+w^2) = (xz - yw)^2 + (xw + yz)^2$

$N(x+iy) \quad N(z+iw) \quad N((x+iy)(z+iw))$

Sia q un divisore primo di K $\left(q \le K < p\right)$

- se $q \equiv 3\ (4)$, $q \mid m, n$ quindi

$$\left(\frac{m}{q}\right)^2 + \left(\frac{n}{q}\right)^2 = \left(\frac{K}{q^2}\right) \cdot p,$$

assurdo perché k era minimo possibile

- se $q \equiv 1 \ (4)$ o $q = 2$. Per hp. induttiva

$$q = a^2 + b^2$$

Partiamo da $\dfrac{m^2+n^2}{a^2+b^2} = \left(\dfrac{k}{a^2+b^2}\right) p$

$$m^2+n^2 = N(m+ni) \qquad a^2+b^2 = N(a+bi)$$

$$\frac{m+ni}{a+bi} = \frac{(m+ni)(a-bi)}{a^2+b^2} = \frac{(am+bn)+i(an-bm)}{a^2+b^2}$$

↓ Norme

$$\frac{m^2+n^2}{a^2+b^2} = \frac{(am+bn)^2+(an-bm)^2}{q^2} =$$

$$= \left(\frac{am+bn}{q}\right)^2 + \left(\frac{an-bm}{q}\right)^2$$

Basta mostrare che $\dfrac{am+bn}{q}$ e $\dfrac{an-bm}{q}$ sono interi.

- $q = a^2+b^2$ divide m^2+n^2, e possiamo supporre $q \nmid m$, $q \nmid n$ (e $q \neq 2$)

$m^2 \equiv -n^2 \ (q)$, cioè $m \equiv (\pm)\alpha n \ (q)$, dove $\pm\alpha$ sono le radici quadrate di -1 mod q

- $q \mid a^2+b^2 \implies b \equiv \pm\alpha a \ (q) \quad (1)$

Tesi: $\frac{am+bn}{q}$ intero e $\frac{an-bm}{q} \in \mathbb{Z}$

$$am+bn \equiv a\cdot \alpha n + bn \equiv n\left(b+\alpha a\right) \quad (2)$$

Cambiando b in $-b$, possiamo supporre (1) che $b \equiv -\alpha a \pmod q$, quindi $(2) \equiv 0 (q)$

$$an-bm \equiv an+\alpha am \equiv a(n+\alpha m)$$

$$\equiv a\alpha\left(m+\alpha^{-1}n\right)$$

$$\equiv a\alpha(m-\alpha n) \equiv 0 \quad (q)$$

$$\alpha^2 \equiv -1 \pmod q \implies \alpha \equiv -\alpha^{-1} \ (q) \qquad \square$$

Simbolo di Legendre

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \text{ è Res. Quad mod } p \\ -1 & \text{se } a \text{ NON è R. Q. mod } p \\ 0 & \text{se } p \mid a \end{cases}$$

Se $a, b \not\equiv 0 \pmod p$, abbiamo

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \pmod p$$

(Eulero)

$$\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

$$\Rightarrow \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Esempio Modulo $p \neq 2, 3$ almeno uno fra 2, 3 e 6 è un quadrato: se $\left(\frac{2}{p}\right) = -1$ e $\left(\frac{3}{p}\right) = -1$, allora

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = +1 \quad (\text{cioè } 6 \equiv \square \ (p))$$

Esempio X^4+1 è irriduc / $\mathbb{Q}$ ma riducibile mod p per ogni p.

- X^4+1 è irrid / $\mathbb{Q}$ (è ciclotomico)
- $$X^4+1 = \left(X - \frac{1+i}{\sqrt{2}}\right)\left(X - \frac{1-i}{\sqrt{2}}\right)\left(X - \frac{-1+i}{\sqrt{2}}\right)\left(X - \frac{-1-i}{\sqrt{2}}\right)$$

$$X^4+1 = (X^2+i)(X^2-i)$$

$$= (X^2+1+\sqrt{2}\,X)(X^2+1-\sqrt{2}\,X)$$

$$= (X^2-1+\sqrt{2}\,i\,X)(X^2-1-\sqrt{2}\,i\,X)$$

Oss: uno tra -1, 2 e -2 è un RQ mod p

$p = 5$ $\quad 2^2 \equiv -1 \ (5)$ $\quad$ " $\quad i \equiv 2 \ (5)$ "

$$X^4 + 1 = (X^2 + 2)(X^2 - 2) \mod 5$$

Se p è t.c. $\left(\frac{-1}{p}\right) = 1$, sia $a \in \mathbb{N}$ t.c. $a^2 \equiv -1 \ (p)$.

Allora $\quad X^4 + 1 \equiv (X^2 + a)(X^2 - a) \mod p$

RECIPROCITÀ QUADRATICA

p, q primi dispari. Allora

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

In soldoni: • se $p \equiv 1\ (4)$ o $q \equiv 1\ (4)$ abbiamo

p quadrato mod q $\iff$ q quadrato mod p

• se invece $p \equiv q \equiv 3\ (4)$, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

$$\left(\frac{17}{347}\right) = \left(\frac{347}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right)$$

$$= -\left(\frac{7}{3}\right) = -1$$

$$\left(\frac{10}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{5}{7}\right)$$

Lemma $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{se } p \equiv \pm 1\ (8) \\ -1, & \text{se } p \equiv \pm 3\ (8) \end{cases}$

Dim

$$\begin{aligned} 1 &\equiv (-1)(-1) \quad (p) \\ 2 &\equiv (2)(-1)^2 \quad (p) \\ 3 &\equiv (-3)(-1)^3 \quad (p) \\ &\vdots \\ s := \tfrac{p-1}{2} &\equiv \left((-1)^{s-1} s\right)(-1)^s \quad (p) \end{aligned}$$

$$s! \equiv (-1)(2)(-3) \cdots (\pm s)\,(-1)^{s(s+1)/2}$$

$$\frac{p-1}{2}! \equiv (2)(4)(6)\dots(p-1)\cdot(-1)^{s(s+1)/2} \pmod p$$

$$\equiv 2^{\frac{p-1}{2}}\cdot(1\cdot 2\cdot\dots\cdot s)\cdot(-1)^{(p^2-1)/8} \pmod p$$

$$\equiv 2^{\frac{p-1}{2}}\cdot \frac{p-1}{2}!\cdot(-1)^{(p^2-1)/8} \pmod p$$

$$\left(\frac{2}{p}\right) \equiv (2)^{\frac{p-1}{2}} \equiv (-1)^{(p^2-1)/8} \pmod p$$ ∎

Esercizio $2b^2+3 \mid a^2-2$

Soluzione • Idea 1: $2b^2+3 \equiv \begin{cases} 5 \pmod 8 \\ 3 \pmod 8 \end{cases}$

$\Rightarrow \exists\, p \mid 2b^2+3,\quad p \equiv \pm 3 \pmod 8$

Assurdo, perché $a^2 \equiv 2 \ (p) \Rightarrow \left(\frac{2}{p}\right) = +1$

$\Rightarrow p \equiv \pm 1 \pmod 8$

• Idea 2: $\forall p \mid 2b^2+3,\quad \left(\frac{2}{p}\right) = 1$

$p \mid 2b^2+3 \iff 2b^2 \equiv -3 \ (p)$

$\iff (2b)^2 \equiv -6 \ (p)$

$\iff \left(\frac{-6}{p}\right) = 1$

$$\left(\frac{-6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-3}{p}\right) \Rightarrow \left(\frac{-3}{p}\right) = 1$$

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$$ ("perché -3 è un primo $\equiv 1 \pmod 4$")

$$1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}}$$

$$= \left(\frac{p}{3}\right) \implies p \equiv 1 \ (3)$$

In generale: se $q \equiv 3 \ (4)$, $\left(\frac{-q}{p}\right) = \left(\frac{p}{q}\right)$

Assurdo: ogni primo che divide $2b^2+3$ è $\equiv 1 \ (3)$,

ma $2b^2 + 3 \equiv 2 \mod 3$

Esempio Calcoliamo $\sum_{n \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{1-3n^2}{p}\right) \pmod p$

$$\sum_{n \in \mathbb{Z}/p\mathbb{Z}} (1-3n^2)^{\frac{p-1}{2}} \equiv \sum_{n \in \mathbb{Z}/p\mathbb{Z}} \left(1 + \left(\frac{p-1}{2}\right)(-3n^2) + \underbrace{\text{ROBE}}_{\cdots} + (-3n^2)^{\frac{p-1}{2}}\right)$$

$$\overset{\text{LEMMONE}}{\equiv} \sum_{n \in \mathbb{Z}/p\mathbb{Z}} (-3)^{\frac{p-1}{2}} n^{p-1} \equiv -\left(\frac{-3}{p}\right) \mod p$$

Ex (ADVANCED) $p > 100$, $r \in \mathbb{N}$. Allora $\exists a, b \in \mathbb{N}$

t.c. $r \equiv a^2 + b^5 \mod p$

Idea: tesi $\iff \exists b$ t.c. $\left(\frac{r-b^5}{p}\right) = +1$

Calcolare $\sum_{b=0}^{p-1} \left(\frac{r-b^5}{p}\right)$

e mostrare che è $\not\equiv 0 \mod p$

IMO SL (2006)

$$\frac{x^7-1}{x-1} = y^5 - 1 \qquad x \geq 2 \qquad y \in \mathbb{N}$$

Soluzione Sia p un divisore di $\frac{x^7-1}{x-1}$.

Claim: se $p \mid x-1$, allora $p = 7$

Dim: sta nel guadagno di un primo. Comunque,

$$v_p(x^7-1) \overset{\text{LTE}}{=} v_p(x-1) + v_p(7)$$

$$v_p\left(\frac{x^7-1}{x-1}\right) = v_p(7) \quad \text{e' } \neq 0 \text{ solo se } p=7$$

Per $p=2$: se $x \equiv 1 \ (4)$, $v_2(x^7-1) = v_2(x-1) + v_2(7)$

$$v_2\left(\frac{x^7-1}{x-1}\right) = 0$$

Altrimenti $x \equiv 3 \ (4)$, $x^7 \equiv 3 \ (4)$, quindi

$$v_2(x^7-1) = 1 \qquad v_2(x-1) = 1$$

$$v_2\left(\frac{x^7-1}{x-1}\right) = 0$$

$$x^7 - 1 = (x-1)(x^6 + x^5 + \dots + 1)$$

Claim Se $p \mid x^7 - 1$ ma non $x - 1$, allora

$$\mathrm{ord}_p(x) = 7 \mid p - 1$$

Dim: $x^7 \equiv 1 \pmod p$, quindi $\mathrm{ord}_p(x) \mid 7$, quindi

o $\boxed{\mathrm{ord}_p(x) = 1}$ o $\mathrm{ord}_p(x) = 7$ (SI)

$\Downarrow$

$x \equiv 1 \pmod p$ contro l'ipotesi (NO)

FATTO I fattori primi di $\frac{a^p - 1}{a - 1}$ sono o uguali

a p o $\equiv 1 \pmod p$

$$\frac{x^7 - 1}{x - 1} = \boxed{(y - 1)}\,\boxed{(y^4 + y^3 + y^2 + y + 1)}$$

che valori può assumere mod 7?
Soltanto 0 o 1

che valori assume mod 7?
0 o 1
contraddizione!
NON CI SONO SOLUZIONI

Cioè: $y \equiv 1, 2 \mod 7$

Ma $1^4 + 1^3 + 1^2 + 1^1 + 1 \equiv 5 \mod 7$

e $2^4 + 2^3 + 2^2 + 2^1 + 1 \equiv 3 \mod 7$

ESERCIZIO $b^a \mid a^b - 1$

Soluzione • Studiare $v_p(a^b - 1)$

• soluzioni piccole: $a = 1$, b qualunque
$b = 1$, $a = 2$
$b = 2$, $a = 3$

• Applichiamo LTE(?) NO: non sappiamo che $p \mid a - 1$.

Idea: se $d = \mathrm{ord}_b(a)$, posso applicare LTE a
$(a^d)^{b/d} - 1$

• $\mathrm{ord}_p(a) \mid (b, p-1)$

Riflesso condizionato da Senior basic: prendo p il PIÙ PICCOLO PRIMO

Per questo p, $(b, p-1) = 1$ e quindi $a \equiv 1 \ (p)$

$$v_p(a^b - 1) = v_p(a - 1) + v_p(b)$$

IV

$$v_p(b^a) = a\, v_p(b)$$

$$\Rightarrow \quad v_p(b) \cdot (a-1) \leq v_p(a-1) < (a-1)$$

Puzza di assurdo! Cosa può andare storto?

• $a = 1$ $(v_p(a-1) = 0)$ ✓

- non esiste p, cioè $b = 1$ ✓
- magari la disug. è vera! no, non succede
- $p = 2$, non posso (proprio ...) usare LTE
  b è pari

Uso LTE per $p = 2$

$$v_2(b^a) \le v_2(a^b - 1) = v_2\left((a^2)^{b/2} - 1\right)$$

$$v_2(b) \cdot a = v_2(a^2 - 1) + v_2(b/2)$$

$$= v_2(a^2 - 1) + v_2(b) - 1$$

$$v_2(b) \cdot (a - 1) + 1 \le v_2(a^2 - 1)$$

$$\Downarrow$$

$$2^{1 + v_2(b)(a-1)} \le 2^{v_2(a^2-1)} \le a^2 - 1$$

- Se $v_2(b) \ge 2$, $\text{LHS} = 2^{2a-1} \le a^2 - 1$ MAI
- Quindi $v_2(b) = 1$, $2^a \le a^2 - 1$, che è vera solo per $a = 3$

Quindi ci siamo ridotti a $b^3 \mid 3^b - 1$

Achtung: NON abbiamo dimostrato che $b = 2$!

Guardo (di nuovo) $\mathrm{ord}_b(3)$, anzi $\mathrm{ord}_p(3)$ dove p è un eventuale divisore dispari di b.

$$\mathrm{ord}_p(3) \mid (b, p-1)$$

Se scelgo p minimo, $(b, p-1) = 2$, cioè

$$3^2 \equiv 1 \mod p$$
$$8 \equiv 0 \mod p$$

che è improbabile per p dispari.

Quindi b è una potenza di 2 (non ha divisori dispari), quindi $b = 2^{v_2(b)} = 2$.

IMO 2000 Esiste $n \in \mathbb{N}$ t.c. $n \mid 2^n+1$ e n ha esattamente 2000 divisori primi distinti.

Soluzione $n=3$ divide 2^n+1

$$9 \mid 2^3+1 \mid 2^9+1 = 513 = 9 \cdot 57 = 27 \cdot 19$$

Oss: $v_3\left(2^9+1\right) = v_3(2+1) + v_3(9) = 3$

$n = 9 \cdot 19$ funziona: $9 \cdot 19 \mid 2^9+1 \mid 2^{9 \cdot 19}+1$

Sia p_3 un fattore primo di $2^{9 \cdot 19}+1$ diverso da 3 e da 19 (esiste per guadagno di un primo)

Allora $n_3 = 9 \cdot 19 \cdot p_3$ funziona:

$$9 \cdot 19 \cdot p_3 \mid 2^{9 \cdot 19}+1 \mid 2^{9 \cdot 19 \cdot p_3}+1$$

Iterazione: se ho costruito n_k, $2^{n_k}+1$ ha un fattore primo "nuovo" (p_{k+1}) e pongo $n_{k+1} = n_k \cdot p_{k+1}$. n_{2000} funziona.

PUTNAM QUALCOSA Sia $n \in \mathbb{N}$ e p e $\left(n, \frac{4n+2}{3}\right]$. ($p$ primo)

Allora $p \mid \sum_{j=0}^{n} \binom{n}{j}^4$

Oss. $\sum_{j=0}^{n} \binom{n}{j}^2 = \binom{2n}{n}$. Tutti i primi nell'intervallo $(n, 2n]$ dividono questa somma

Soluzione

Scriviamo $p = n + k$ con $k \geq 1$

$k = 3$

$$\binom{p-k}{j} \equiv \frac{(p-k)(p-k-1)\cdots(p-k-j+1)}{j!}$$

$$\equiv \frac{(-k)(-k-1)\cdots(-k-j+1)}{j!} \quad (p)$$

$$\equiv (\pm 1)\frac{(k+j-1)\cdots(k+1)(k)}{j!} \quad (p)$$

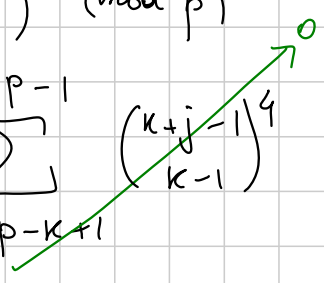
$$\equiv (\pm 1)\binom{k+j-1}{j} \mod p$$

$$\equiv (\pm 1)\binom{k+j-1}{k-1} \mod p$$

Quindi:

$$\sum_{j=0}^{n} \binom{n}{j}^4 \equiv \sum_{j=0}^{n=p-k} \binom{k+j-1}{k-1}^4 \pmod p$$

$$\equiv \sum_{j=0}^{p-1} \binom{k+j-1}{k-1}^4 - \sum_{j=p-k+1}^{p-1} \binom{k+j-1}{k-1}^4$$



$$= \sum_{j=0}^{p-1} \underbrace{\binom{k+j-1}{k-1}^4}_{Q(j)}$$

$$\deg Q(j) = 4(k-1) \overset{?}{\leq} p-1 = n+k-1$$

$$\iff (k-1) < n/3$$

$$\iff p-1 < 4n/3$$

$$\iff p \leq \frac{4n+2}{3}$$

□

ES (TEST INIZIALE)

$p_1, \dots, p_{2015}$ primi distinti > 100

Sia $\sum_{i=1}^{2015} \frac{1}{p_i^6+1} = a/b$ con $(a,b)=1$

Sia $c = ba^5$. Calcola $16^c \bmod 29$.

$\| \quad 2^{4c}$

Domanda: $c \bmod 7$ $\quad c \equiv ba^5 \equiv b/a$,

quindi basta $a/b \bmod 7 \equiv \sum_{i=1}^{2015} \frac{1}{2} \equiv$

$\equiv 4 \cdot 2015 \equiv 3$

$c \equiv b/a \equiv 5 \ (7)$ $\quad$ Risposta: $2^{20} \bmod 29$

$\|$

23

Interi di Gauss

$$\mathbb{Z}[i] = \{ m + i \cdot n \mid m, n \in \mathbb{Z} \}$$

$2+3i \in \mathbb{Z}[i]$

Domanda: $2+3i$ divide 13? Sì, perché

$$13 = (2+3i)(2-3i)$$

Divisibilità: $a+bi$ divide $c+di$ se esiste $e+fi$ tale che $c+di = (a+bi)(e+fi)$

$$\frac{13}{2+3i} = \frac{13(2-3i)}{(2+3i)(2-3i)} = \frac{13(2-3i)}{4+9} = 2-3i$$

Primi (di Gauss) $p = m+ni$ è primo se vale una (e quindi entrambe) tra:

- se $p \mid a \cdot b$ allora $p \mid a$ oppure $p \mid b$
- se $p = a \cdot b$ allora o a o b è invertibile

(in soldoni: uno tra a e b è $\pm 1, \pm i$)

13 non è un primo di Gauss! Infatti

$$13 = (2+3i)(2-3i)$$

2 non è un primo di Gauss

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

TEOREMA (FATTORIZZAZIONE UNICA)

$\forall n \in \mathbb{Z}[i]$ esistono primi (di Gauss) $p_1, \dots, p_k$, esponenti $e_1, \dots, e_k$, e un invertibile u tali che $n = u \cdot p_1^{e_1} \cdots p_k^{e_k}$ (unità)

e questa scrittura è (essenzialmente) unica: se $u_1 p_1^{e_1} \cdots p_k^{e_k} = u_2 q_1^{f_1} \cdots q_k^{f_k}$, allora (a meno di permutare) $e_1 = f_1, \dots, e_k = f_k$,

$p_1 = v_1 q_1, \dots, p_k = v_k q_k$ con v_i unità.

Esempio $13 = (2+3i)(2-3i) = -i(-3+2i)(2-3i)$

differiscono per i (che è un'unità)

Esercizio $2+3i$ è primo. (e $2-3i$ anche)

Supponiamo che $2+3i = (a+bi)(c+di)$.

$2-3i = (a-bi)(c-di)$

$13 = (a^2+b^2)(c^2+d^2)$

Siccome 13 è primo (in $\mathbb{Z}$), $a^2+b^2 = 1$, cioè $a+bi \in \{1, -1, i, -i\}$

Definizione $N(a+bi) = a^2+b^2$

Conseguenza Se $N(a+bi)$ è un primo (in $\mathbb{Z}$),

allora $a+bi$ è primo (in $\mathbb{Z}[i]$)

Fatto 3 è un primo di Gauss (ma $N(3)=9$)

Dim $3 = (a+bi)(c+di)$

$9 = (a^2+b^2)(c^2+d^2)$ ← Norma

Wlog $3 \mid a^2+b^2$. Ma allora $3 \mid a$, $3 \mid b$, quindi $9 \mid a^2+b^2$, quindi $c^2+d^2=1$, cioè $c+di$ è un'unità

Teorema I primi di Gauss sono:

- i primi (di $\mathbb{Z}$) congrui a 3 mod 4
- gli $a+bi$ t.c. $N(a+bi)$ è un primo di $\mathbb{Z}$ (necess. $=2$, o $\equiv 1\ (4)$)

Conseguenza della fattorizzazione unica

Sia $p \equiv 1\ (4)$. Sappiamo che $\exists\, c \in \mathbb{N}$ t.c. $p \mid c^2+1$

Negli interi di Gauss, $p \mid (c+i)(c-i)$ ma $p \nmid c+i$ e $p \nmid c-i$

(Infatti: $p \mid c+i$ vuol dire che Re e Im di $\frac{c+i}{p}$ sono intere, il che è falso)

Cioè p non è primo di Gauss, quindi non è irriducibile: $p = (a+bi)(c+di)$

Prendo le norme: $p^2 = (a^2+b^2)(c^2+d^2)$, dove $a^2+b^2 \neq 1$ e $c^2+d^2 \neq 1$, perché $a+bi$ e $c+di$ non sono unità.

$$\Rightarrow \boxed{a^2+b^2 = p}$$

Unità: se u è invertibile sia v l'inverso

$$1 = u \cdot v$$

$$1 = N(1) = N(u \cdot v) = N(u) \cdot N(v)$$

$$\Rightarrow N(u) = 1 \Rightarrow u \in \{\pm 1, \pm i\}$$

Esempio In quali modi si può scrivere 65 come somma di quadrati?

$$65 = 13 \cdot 5 = (2+3i)(2-3i)(2+i)(2-i)$$

$$a^2+b^2 = N(a+bi) = 65$$

$$a+bi = p_1^{e_1} \cdots p_k^{e_k}$$

$$65 = a^2+b^2 = N(p_1)^{e_1} \cdots N(p_k)^{e_k}$$

$N(p_1) = 5$, $e_1 = 1$; $N(p_k) = 13$, $e_k = 1$

$$a+bi \in \{(2+3i)(2+i),\ (2+3i)(2-i),\ (2-3i)(2+i),\ (2-3i)(2-i)\}$$

$$= \{1+8i,\ 7+4i,\ 7-4i,\ 1-8i\}$$

CATALAN DEI POVERI

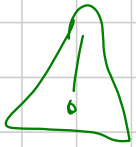
Risolvere $x^2+1 = y^n$ (NO SOLUZIONI) tranne $x=0$

Dimostrazione $(x+i)(x-i) = y^n$

Oss preliminari
- basta fare il caso n primo $\geq p$
- $p=2$ $\quad 1 = (y-x)(y+x)$
- Parità di x e y? Modulo 4 $\Rightarrow$ x pari e y è dispari

$$\mathrm{mcd}(x+i, x-i) = \mathrm{mcd}(x+i, 2i)$$

$$= \mathrm{mcd}(x+i, 2)$$



Tentazione $\rightarrow = 1$, perché $\frac{x+i}{2} \notin \mathbb{Z}[i]$

ma questo è come dire $(15, 6) = 1$ perché $15/6$ non è intero

$$= \mathrm{mcd}(x+i, (1+i)^2)$$

Oss: $1+i$ è primo, perché $N(1+i) = 2$

Voglio dimostrare che $(x+i, 1+i) = 1$, cioè che nessun primo divide entrambi.

$$(x+i, 1+i) = (x-1, 1+i) = \begin{cases} 1+i \\ 1 \end{cases}$$

Domanda: $1+i \mid x-1$?

Se sì, $(X-1) = (1+i)(a+bi)$

$\downarrow N$

$(X-1)^2 = 2\cdot(a^2+b^2)$,

assurdo modulo 2 (X è pari)

$(X+i)(X-i) = y^p \Rightarrow \quad X+i = u(a+bi)^p$

$X-i = \bar{u}(a-bi)^p$

Oss: ogni unità è una potenza p-esima

$\left[ab = y^3 \qquad a = c^3 \quad b = d^3 \right.$

$\left. a = -c^3 \rightsquigarrow \quad a = (-c)^3 \right]$

1 ok $\qquad -1 = (-1)^p \qquad i = (\pm i)^p$

$-i = (\mp i)^p$

Quindi $X+i = (a+bi)^p$ per qualche $a, b \in \mathbb{Z}$

$$X+i = a^p + p\cdot a^{p-1} bi + \binom{p}{2} a^{p-2}(bi)^2 + \dots + (bi)^p$$

Considerando Im, $1 = b$ (un sacco di roba)

$\Rightarrow \quad b = \pm 1$

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

$3a^2 - 1 = 1$

Se prendo Im e poi modulo p, ottengo

$$1 \equiv \frac{1}{i}(bi)^p \pmod p$$

$$\equiv b^p \cdot i^{p-1}$$

$$\equiv b^p \cdot (-1)^{\frac{p-1}{2}} \mod p$$

$$\equiv b \cdot (-1)^{\frac{p-1}{2}} \mod p$$

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

$$X + i = (a \pm i)^p \xrightarrow{N} X^2 + 1 = (a^2+1)^p$$

$\Rightarrow a$ pari

Prendiamo di nuovo la parte immaginaria:

$$1 = \mathrm{Im}\left(\sum_{j=0}^{p} \binom{p}{j} a^j (\pm i)^{p-j}\right)$$

$$= \sum_{\substack{j=0 \\ j \text{ pari}}}^{p} \binom{p}{j} a^j (\pm i)^{p-j-1}$$

Hope: magari non torna per congruenze modulo 2^k.

$$1 = 1 + \sum_{\substack{k=1 \\ j=2k}}^{\frac{p-1}{2}} \binom{p}{2k} a^{2k} (\pm i)^{p-1-2k}$$

Claim: $v_2\left(\binom{p}{2k} a^{2k}\right) > v_2\left(\binom{p}{2} a^2\right) \quad \forall k > 1$

Oss 1: wlog $v_2(a) = 1$ (caso peggiore)

Oss 2: $$v_2\left(\binom{p}{2}a^2\right) = v_2\left(\frac{p(p-1)}{2}\right) + 2$$
$$= v_2(p-1) + 1$$

$$v_2\left(\binom{p}{2k}a^{2k}\right) = v_2\left(\frac{p(p-1)}{2k(2k-1)}\binom{p-2}{2k-2}\cdot a^{2k}\right)$$
$$= 2k + v_2(p-1) - 1 - v_2(k)$$

Disug. da dimostrare:

$$2k + v_2(p-1) - 1 - v_2(k) > v_2(p-1) + 1$$
$$2(k-1) > v_2(k)$$

Basta $k < 2^{2(k-1)}$ vera $\forall k \geq 2$