MISCELLANEA

Note Title 23/01/2020

M2 Per quali n esiste $g(x) : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ tale che $g(x), g(x)+x, \dots, g(x)+100x$ siano tutte bigezioni $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$?

Oss Se $g(x)$ e' una bigezione,

$$\{1, 2, \dots, n\} = \{g(1), g(2), \dots, g(n)\}$$

$$\Rightarrow \quad 1+2+\dots+n = g(1)+g(2)+\dots+g(n)$$

$$\sum_{x=1}^{n} x \equiv \boxed{\sum_{x=1}^{n} \big(g(x)\big) \equiv \sum_{x=1}^{n} \big(g(x)+x\big)} \equiv \dots$$

$$\equiv \sum_{x=1}^{n} \big(g(x)+100x\big) \pmod{n}$$

$$0 \equiv \sum_{x=1}^{n} x \equiv \frac{n(n+1)}{2} \pmod{n}$$

Se una tale $g(x)$ esiste, n e' DISPARI

Esempi: provo $g(x) = x$, le 101 funzioni sono

$x, \quad 2x, \quad 3x, \quad \dots, \quad 101x$

che sono tutte bigezioni se e solo se

$$(n, 101!) = 1$$

$$\sum_{x=1}^{n} g(x)^2 \equiv \sum_{x=1}^{n} (g(x)+x)^2 \equiv \sum_{x=1}^{n} (g(x)+2x)^2 \quad (n)$$

$$\sum g(x)^2 \equiv \sum_{x=1}^{n} \left(g(x)^2+2x\,g(x)+x^2\right) \equiv \sum \left(g(x)^2+4x\,g(x)+4x^2\right)$$

$$\Rightarrow \quad 0 \equiv \underbrace{\sum_{x=1}^{n} \left(2x\,g(x)+x^2\right)}_{\text{questa} \times 2} \equiv \underbrace{\sum_{x=1}^{n} \left(4x\,g(x)+4x^2\right)}_{-\ \text{questa}}$$

$$0 \equiv -\cancel{2} \sum_{x=1}^{n} x^2 \quad (\text{mod } n)$$

(tanto n e' dispari)

$$0 \equiv \frac{n(n+1)(2n+1)}{6} \quad (\text{mod } n)$$

$$0 \equiv n(n+1)(2n+1) \quad (6n)$$

$$0 \equiv (n+1)(2n+1) \quad (6)$$

$$\Rightarrow \quad (n, 3) = 1$$

Strategia:

* vorrei dim. che $\displaystyle\sum_{x=1}^{n} x^k \equiv 0 \quad (n)$

* da questo vorrei dedurre che

$$(n, k+1) = 1 \quad (\rightsquigarrow k = p-1)$$

Consideriamo

$$f(x) = \sum_{x=1}^{n} \left(g(x) + kx \right)^h$$

Ipotesi: $f(0) = f(1) = \dots = f(100)$

$\boxed{\text{DIFFERENZE FINITE}}$ $\quad f(x) \rightsquigarrow$

$$\Delta f(x) = f(x+1) - f(x)$$

$$\Rightarrow \quad \Delta f(0) = \Delta f(1) = \dots = \Delta f(99) = 0$$

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

$$= \Big(f(x+2) - f(x+1) \Big) - \Big(f(x+1) - f(x) \Big)$$

$$\Delta^2 f(0) = \Delta^2 f(1) = \dots = \Delta^2 f(98) = 0$$

... avanti così, e se $h \leq 100$ troviamo

$$\Delta^h f(0) = \dots = \Delta^h f(100-h) = 0$$

$$\Delta(x^m) = (x+1)^m - x^m =$$

$$= \cancel{x^m} + m x^{m-1} + \dots - \cancel{x^m}$$

$$\Delta^2(x^m) = m(m-1)x^{m-2} + \dots$$

$$\Delta^m(x^m) = m!$$

Nel nostro caso, $f(k) = \sum_{x=1}^{n} (g(x)+kx)^h$

$$\Rightarrow \Delta^h f(0) \equiv 0 \ (n) \qquad (*)$$

$$\parallel$$

$$h! \cdot \sum_{x=1}^{n} x^h$$

Per induzione mostriamo che $(n, p) = 1$

se $p \leq 101$

$p = 2, 3$ fatti

$p = 5$: uso $(*)$ con $h = 4$ e trovo

$$\cancel{4!} \sum_{x=1}^{n} x^4 \equiv 0 \ (n)$$

per induz, $(4!, n) = 1$

p: uso $(*)$ con $h = p-1$ e trovo

$$\cancel{(p-1)!} \sum x^{p-1} \equiv 0 \ (n)$$

Sotto-problema: $\sum_{x=1}^{n} x^{p-1} \equiv 0 \ (n) \Rightarrow p \nmid n$

Se $n = pq$ con $(p, q) = 1$:

$$\cancel{q} \underbrace{\sum_{x=1}^{p} x^{p-1}} \equiv 0 \ (p), \text{ assurdo}$$

$\equiv -1$

Caso generale: se $n = p^k \cdot q$ con $(p,q)=1$

$$\sum_{x=1}^{q \cdot p^k} x^{p-1} \equiv 0 \quad (p^k)$$

$$\text{|||}$$

$$\cancel{q} \sum_{x=1}^{p^k} x^{p-1}$$

Mostro per induz. su K che

$$\sum_{x=1}^{p^k} x^{p-1} \not\equiv 0 \quad (p^k)$$

$\boxed{K \rightsquigarrow K+1}$

$$\sum_{x=1}^{p^{k+1}} x^{p-1} = \sum_{j=0}^{p-1} \sum_{i=1}^{p^k} \left(i + j \cdot p^k\right)^{p-1}$$

$$\equiv \sum_{j=0}^{p-1} \sum_{i=1}^{p^k} \left(i^{p-1} + (p-1)\, i^{p-2}\, j p^k \right)$$

$$\equiv p \sum_{i=1}^{p^k} i^{p-1} + (p-1)\, p^k \underbrace{\left(\sum_{i=1}^{p^k} i^{p-2}\right)\left(\sum_{j=0}^{p-1} j\right)}_{\substack{\equiv 0 \ (p) \\ \text{(esercizio)}}}$$

$$\equiv p \left(\sum_{i=1}^{p^k} i^{p-1} \right) \not\equiv 0 \quad (\text{mod } p^{k+1})$$

$$(x-a)(x-b)(x-c) = (x-d)(x-e)(x-f)$$

$x+y+z$
$xy+yz+zx$
xyz

$x+y+z$
$x^2+y^2+z^2$
$x^3+y^3+z^3$

$$(n)\quad 0 \equiv \sum_{x \in \mathbb{Z}/n\mathbb{Z}} x(x-1)\cdots(x-(p-2)) \equiv$$

$$\equiv \sum_{x \in \mathbb{Z}/n\mathbb{Z}} (p-1)! \binom{x}{p-1}$$

$$0 \equiv (p-1)! \binom{n}{p} \pmod{p^k}$$

$$\Rightarrow p \nmid n$$

$$P(x,y,z) = P(x,y,xy-z) = P(x,zx-y,z) = P(zy-x,y,z)$$

$$\Rightarrow \quad P(x,y,z) = Q(x^2+y^2+z^2-xyz)$$

↑ Ovvio: tutti questi vanno bene

Idea: induzione su $\deg P$

$\boxed{\text{SE SAPESSI}}$ CHE $\quad P(x,y,z) = a(xyz)^d$ + roba di grado $<d$

allora $\quad P(x,y,z) - a(xyz - x^2-y^2-z^2)^d$

avrebbe le stesse simmetrie ma grado inferiore, da cui la tesi per induzione.

— o — o —

Se $P(x) = P(-x) \quad \rightsquigarrow \quad P(x) = Q(x^2)$

$P(x,y,z) = P(x,y,-z) \rightsquigarrow P(x,y,z) = Q(x,y,z^2)$

$P(x) = P(2-x) \quad \rightsquigarrow \quad P(x) = Q((x-1)^2)$

$R(t) = P(1+t) = P(2-(t+1)) = P(1-t) = R(-t)$

$R(t) = Q(t^2) \qquad 1+t = x \rightsquigarrow t = x-1$

$P(x) = P(a-x) \quad \rightsquigarrow \quad P(x) = Q\left(\left(x-\frac{a}{2}\right)^2\right)$

$P(x,y,z) = P(x,y,a-z) \rightsquigarrow P(x,y,z) = Q\left(x,y,\left(z-\frac{a}{2}\right)^2\right)$

$P(x,y,z) = P(x,y,xy-z) \rightsquigarrow P(x,y,z) = \hat{Q}\left(x,y,\left(z-\frac{xy}{2}\right)^2\right)$

$$= \hat{Q}\left(x,y,z^2-zxy+\frac{x^2y^2}{4}\right)$$

$$= \hat{\hat{Q}}(x,y,z(z-xy))$$

$$\hat{\hat{Q}}(x,y,z) = \sum_{i,j,k} a_{i,j,k}\, x^i y^j z^k$$

$$\hat{\hat{Q}}(x,y,z(z-xy)) = \sum_{i,j,k} a_{ijk}\, x^i y^j [z(z-xy)]^k$$

Qual è il termine di grado + grande?

Guardo tutte le terne (i,j,k) per cui $a_{ijk} \neq 0$ e tra queste faccio in modo che

$$i+j+3k \quad \text{sia max}$$

Questo mi produce un monomio del tipo $x^{i+k} y^{j+k} z^k$ che nessuno può cancellare!!

Per cancellarlo dovrebbe avere $x^{i'+k'} y^{j'+k'} z^{k'} \Rightarrow k=k'$, $j=j'$, $i=i'$

Conseguenza: usando solo l'uguaglianza "che cambia la z" scopriamo che il termine di grado più alto in $P(x,y,z)$ è unico e ha l'esponente di $z \leq$ esp. di x e y.

— o — o —

$\boxed{\text{DELIRIO}}$ Supponiamo di sapere che $P(x,y,z)$ è costante sulla superficie di eq.

$$x^2+y^2+z^2-xyz=4$$

$(2,0,0)$ e $(2,2,2)$ verificano

Allora

$$P(x,y,z)-P(2,0,0) = (x^2+y^2+z^2-xyz-4)\,Q(x,y,z)$$

grado + basso e stesse simmetrie

$$P(x,y,z)-P(2,0,0) = (x^2+\dots-4)\,Q(x,y,z) + \text{resto}$$

$$\text{resto} = A(x,y)\,z + B(x,y)$$

Idea: se x e y sono piccoli, diciamo $|x| \leq 1$ e $|y| \leq 1$, allora esistono 2 valori di z t.c.

$$x^2+y^2+z^2-4xyz=4$$

$$z^2-4xyz+x^2+y^2-4=0$$

Per tali x e y l'eq. di 1° grado in z: $A(x,y)\,z+B(x,y)=0$ ha 2 radici distinte $\Rightarrow A(x,y)=B(x,y)=0$

Se A e B si annullano in un $\square$, allora sono $\equiv 0$
(questo va dimostrato)

$$u+v+w=0 \Rightarrow \cos^2 u+\cos^2 v+\cos^2 w = 4\cos u \cos v \cos w + 1$$

$$x^2+y^2+z^2-4xyz=4$$

$$x=2\cos u \qquad y=2\cos v \qquad z=2\cos w \qquad ☺$$

$$F(u,v,w) = P(2\cos u, 2\cos v, 2\cos w)$$

Cosa diventano le simmetrie di P?

$$F(u,v,w) = F(u,-v,u-v) \quad \text{e simili}$$

da cui per involuzione delle simmetrie del tipo

$$F(u,v,w) = F(u,v+2u,w-2u)$$

e poi ovviamente

$$F(u+2k\pi, v+2\ell\pi, w-2(k+\ell)\pi)$$

Giocando con queste simmetrie si dim. che F è costante su un denso del piano $u+v+w=0$.

M1

A B 2 giocatori 2n

A sceglie $a_1 \dots a_{2n}$ $\sum a_i = 1$ $a_i \geq 0$

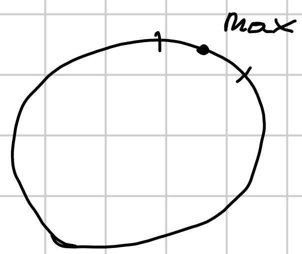
B li può ordinare su una circonferenza e $b_i = a_{\sigma(i)}$

calcola $M = \max\{ b_i \cdot b_{i+1}$ (con i mod 2n)$\}$

A vuole massimizzare, B minimizzare

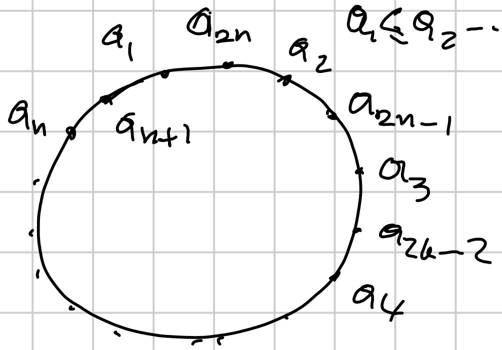
B deve risolvere il problema: dati $a_1 \dots a_{2n}$,

come ordinarli perché M sia minimo?



Per B la cosa migliore sarebbe alternare

$a_1 \leq a_2 \dots \leq a_{2n}$



Dovremmo controllare $a_2 a_{2n}$ $a_3 a_{2n-1}$ $a_4 a_{2n-2}$ ...

$\geq$ $\geq$ $\geq$

non $a_1 a_{2n}$ $a_2 a_{2n-1}$ $a_3 a_{2n-2}$ ...

A deve assicurarsi un prodotto "grandino".

(1) tutti uguali $\frac{1}{2n} \cdot \frac{1}{2n} = \frac{1}{4n^2}$

(2) $n-1 \to 0$ $\quad n+1 \to \frac{1}{n+1}$ ce ne saranno 2 vicini

$\to \left(\frac{1}{n+1}\right)^2$.

(3) 1 grande e 2n-1 uguali piccoli E' meglio?

$x \qquad \frac{1-x}{2n-1} \qquad \frac{x(1-x)}{2n-1} \to \frac{1}{4(2n-1)}$

(4) Un vicino di quello grande può pure essere 0!

$x \qquad \frac{1-x}{2n-2} \qquad \frac{1}{4(2n-2)} = \frac{1}{8(n-1)}$

Quindi A può sempre ottenere almeno $\frac{1}{8(n-1)}$

B può farsi che M sia sempre $\leq \frac{1}{8(n-1)}$?

Cioè, è vero che $a_2 a_{2n} \quad a_3 a_{2n-1} \cdots \leq \frac{1}{8(n-1)}$?

$a_k \cdot a_{2n+2-k} \qquad a_{2n+2-k} = y$

$a_{2n+2-k} \leq a_{2n+2-k+1} \cdots \leq a_{2n} \qquad a_{2n+2-k} \leq \frac{1}{k+1}$

E a_k? $\qquad a_{2n+2-k} \leq 1 - \sum_{i > 2n+2-k} a_i$

$a_k \leq a_{k+1} \leq \cdots \leq a_{2n+2-k} \leq \cdots \qquad a_{2n+2-k} \leq \frac{\sum a_i}{k} = \frac{2}{k}$

Perché a_k sia più grande possibile, $\overbrace{a_k = a_{k+1} = \cdots = a_{2n+2-k-1}}$

$2n+2-k-k$ termini $\qquad \sum_{i>2n+2-k} a_i = z$

$$(2n+2-2k) \quad a_k \leq 1 - \sum_{i>2n+2-k} a_i - a_{2n+2-k}.$$

$$a_k \, a_{2n+2-k} \leq 2 \frac{z(1-z)}{(2n+2-2k)2k}$$

Di nuovo, massimo in z è per $z = \frac{1}{2}$

Devo anche scegliere il peggior k possibile $\quad k=2$

$$\frac{1}{4 \cdot 2(n-1)} \qquad \frac{1}{8(n-1)}.$$