N4 R. DVORNICICH

Titolo nota 12/09/2008

Recall: (1) $\left(\frac{n}{p}\right) = n^{\frac{p-1}{2}} = (-1)^m$ $(p \nmid n)$

m è il numero dei resti $> \frac{p}{2}$ di

$n, 2n, \dots, \frac{p-1}{2}n$.

(2) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ $\left(\begin{array}{ll} +1 & \text{se } p \equiv \pm 1 \pmod 8 \\ -1 & \text{se } p \equiv -3 \pmod 8 \end{array}\right)$

Q.R. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ $p \neq q$ primi dispari.

-1 se $p \equiv q \equiv 3 \pmod 4$ $+1$ altrimenti.

<u>Dim.</u> $p \neq q$. Per ogni k con $1 \leq k \leq \frac{p-1}{2}$

$$kq = q_k p + r_k \qquad q_k = \left[\frac{kq}{p}\right] \qquad 1 \leq r_k \leq p-1$$

$a_1, \dots, a_\ell$ resti da $kq < p/2$

$b_1, \dots, b_m$ resti da $kq > \frac{p}{2}$.

$$a = \sum a_i \qquad b = \sum b_j \qquad a+b = \sum r_k.$$

$$\{a_1, \dots, a_\ell\} \cup \{p-b_1, \dots, p-b_m\} = \left\{1, \dots, \frac{p-1}{2}\right\}.$$

<u>Oss.</u> $1+2+\dots+\frac{p-1}{2} = \frac{p^2-1}{8} = a+mp-b.$

$$\frac{p^2-1}{8} q = \sum_{k=1}^{(p-1)/2} kq = p \sum_{k=1}^{(p-1)/2} q_k + \underbrace{\sum_{k=1}^{(p-1)/2} r_k}_{= a+b}$$

Differenza:

$$\frac{p^2-1}{8}(q-1) = p \sum_{k=1}^{(p-1)/2} q_k + \underbrace{\cancel{a} + b - \cancel{a} - mp + b}_{= 2b - mp}$$

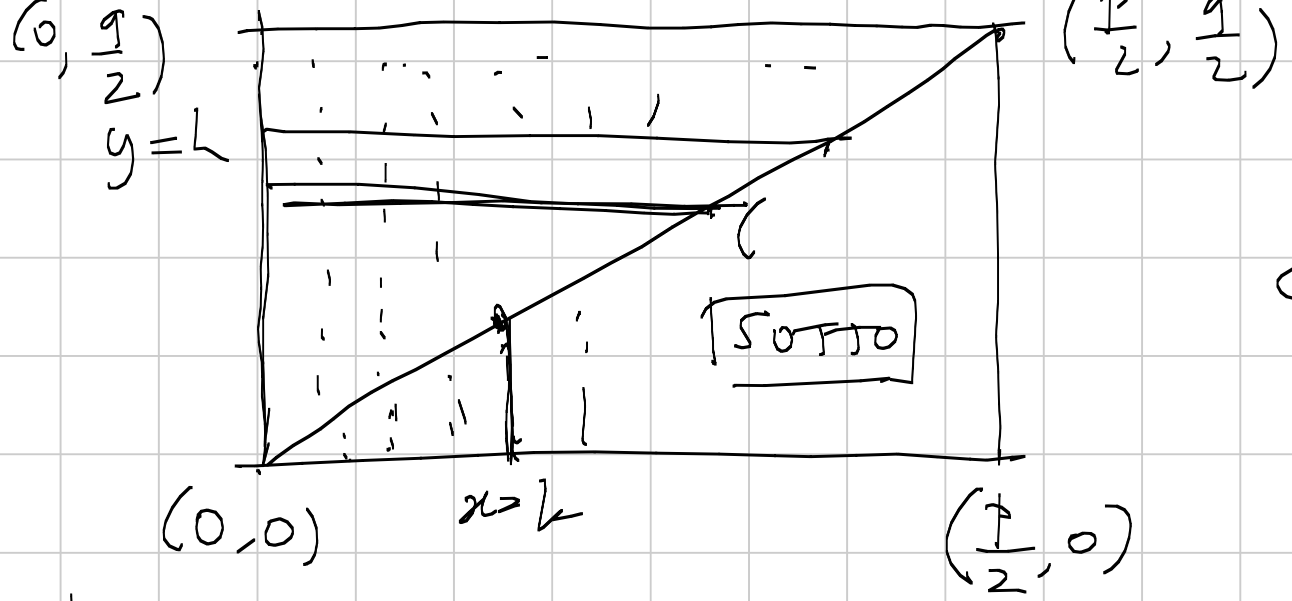
$$0 \equiv \frac{p^2-1}{8}(q-1) \equiv \sum_{k=1}^{(p-1)/2} q_k - m \pmod 2$$

Da ieri ho che

$$\left(\frac{q}{p}\right) = (-1)^m \equiv (-1)^{\sum q_k} \equiv (-1)^{\sum \left[\frac{kq}{p}\right]}$$

$$\left(\frac{p}{q}\right) = (-1)^{\sum \left[\frac{hp}{q}\right]}$$

Q.R. $\iff$ $\displaystyle\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] + \sum_{h=1}^{(q-1)/2} \left[\frac{hp}{q}\right] \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2$



$qx = py$

Punti interi sulla diagonale? <u>No</u>

di punti interi interni al rettangolo $= \frac{p-1}{2} \cdot \frac{q-1}{2}$.

SOTTO: Per $k = 1, \dots, \frac{p-1}{2}$ sulla diagonale ho

$\left(k, \frac{q}{p}k\right) \rightarrow \left[\frac{qk}{p}\right] = q_k$

TOTALE SOTTO $= \sum \left[\frac{kq}{p}\right]$

$h = 1, \dots, \frac{q-1}{2}$ sulla diagonale $\left(\frac{p}{q}h, h\right)$

Punti sulla riga h , $\left[\frac{ph}{q}\right]$

$$\left(\frac{95}{1997}\right) = \left(\frac{5}{1997}\right)\left(\frac{19}{1997}\right) = \left(\frac{1997}{5}\right)\left(\frac{1997}{19}\right)$$

$$= \left(\frac{2}{5}\right)\left(\frac{2}{19}\right) = (-1)(-1) = +1$$

$$m = \prod p_i \qquad \left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$

$$n = \prod q_j$$

<u>dispari</u>

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$$

$$\left(\frac{m}{n}\right) = \prod \left(\frac{p_i}{q_j}\right)$$

$$p \mid 4n^2+1 \implies p \equiv 1 \pmod 4$$

$$4n^2+1 \equiv 0 \pmod p$$

$$-1 = \square \mod p$$

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

$$p \mid 3x^2+y^2$$

$$(x,y) = d$$

$$x = x_1 d \quad y = y_1 d$$

$$p \mid d^2(3x_1^2+y_1^2)$$

$$(x_1, y_1) = d$$

$$p \mid 3x_1^2+y_1^2 \implies \left(\frac{-3}{p}\right) = 1, (0)$$

3, 5, 7, 11, 13

$-3, 5, -7, -11, 13$

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

$$p \equiv 1 \pmod 3$$

BMO 4

$$y^2 = x^5 - 4$$

mod 11 $\quad x^5 \equiv \pm 1, 0$

$y^2 \quad 0, 1, 3, 4, 5, 9$

$y^2+4 \quad 4, 5, 7, 8, 9, 2$

$(y+2i)(y-2i) = y^2 + 4 = x^5$

$\text{MCD}(y+2i, y-2i) \mid (2y, 4i)$

$y + 2i = \varepsilon (a+ib)^5$

$y - 2i = \varepsilon^{-1} (a-bi)^5$

$(a+bi)^5 = \underline{a^5 - 5a^3b^2 + 5ab^4} + i(5a^4b - 5a^2b^3 + b^5)$

$b(5a^4 - 5a^2 + b^4) = 2$

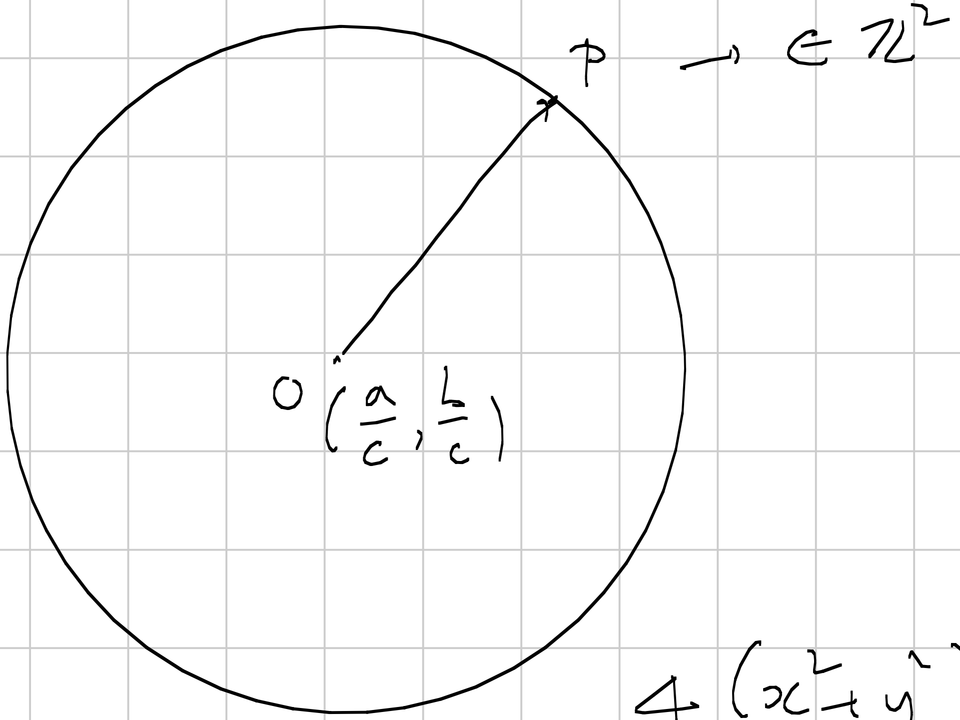
SHORTLIST IMO 2004 N7.

p primo dispari, n intero positivo.
Nel piano ci sono 8 punti a coordinate intere in una circonferenza di diametro p^n.
Dimostrare che esiste un triangolo fra questi 8 punti tale che i quadrati delle lunghezze dei lati sono interi divisibili per $\underline{p^{n+1}}$.

Centro del cerchio $O = \left(\frac{a}{c}, \frac{b}{c}\right)$ con $(a,b,c) = 1$.

$a, b, c \in \mathbb{Z}$.

$c = p^{\gamma} c_1$, $p \nmid c_1$.



$$\vec{OP} = \left(\frac{x}{c}, \frac{y}{c}\right)$$

$$x + a \equiv y + b \equiv 0 \pmod{c}$$

$$\frac{x^2+y^2}{c^2} = \frac{p^{2n}}{4}$$

$$4(x^2+y^2) = p^{2n} \cdot c^2 = p^{2n+2\gamma} c_1^2 .$$

Se $p \equiv 3 \pmod{4}$ $\qquad p^{n+\gamma} \mid (x, y)$

Quadrato della distanza tra due punti a coordinate intere divisibile per p^{2n}. O.K.

Se $p \equiv 1 \pmod{4}$ $\qquad p = (r+si)(r-si)$

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

$$(x+yi) = (r+si)^k (r-si)^{2n+2\gamma-k} (u+vi)$$

Primo caso: $\gamma > 0$ $(p \mid c)$

$(x,p) = (y,p) = 1$. Questo dice che si può avere solo $k=0$ o $k = 2n+2\gamma$.

Se prendo 5 p.ti interi sulla circonferenza almeno 3 devono avere lo stesso valore di k, p. es $k = 2n+2\gamma$.

I corr. $x+yi$ sono tutti divisibili per $(r+si)^{2n+2\gamma}$ e quindi anche le differenze

$|P_iP_j|^2$ divisibile per $|r+si|^{2(2n+2\gamma)} = p^{2n+2\gamma}$.

2° caso $\gamma = 0$ $(p \nmid c)$.

Cerchiamo eventuali p.ti con $k=n$.

$$x+yi = p^n (u+vi)$$

$p^n \mid x \quad p^n \mid y \qquad x = p^n x_1 \quad y = p^n y_1$

$$4(x_1^2 + y_1^2) = c^2$$

$$-\frac{c}{2} \leq x_1, y_1 \leq \frac{c}{2}$$

Le classi di x_1 e y_1 mod c sono fissate

Quindi ci può essere al più uno di questi punti, salvo che uno dei due $= \pm \frac{c}{2}$ e l'altro 0.

Se prendiamo 7 punti interi sulla circonferenza almeno 5 hanno $k \neq n$.

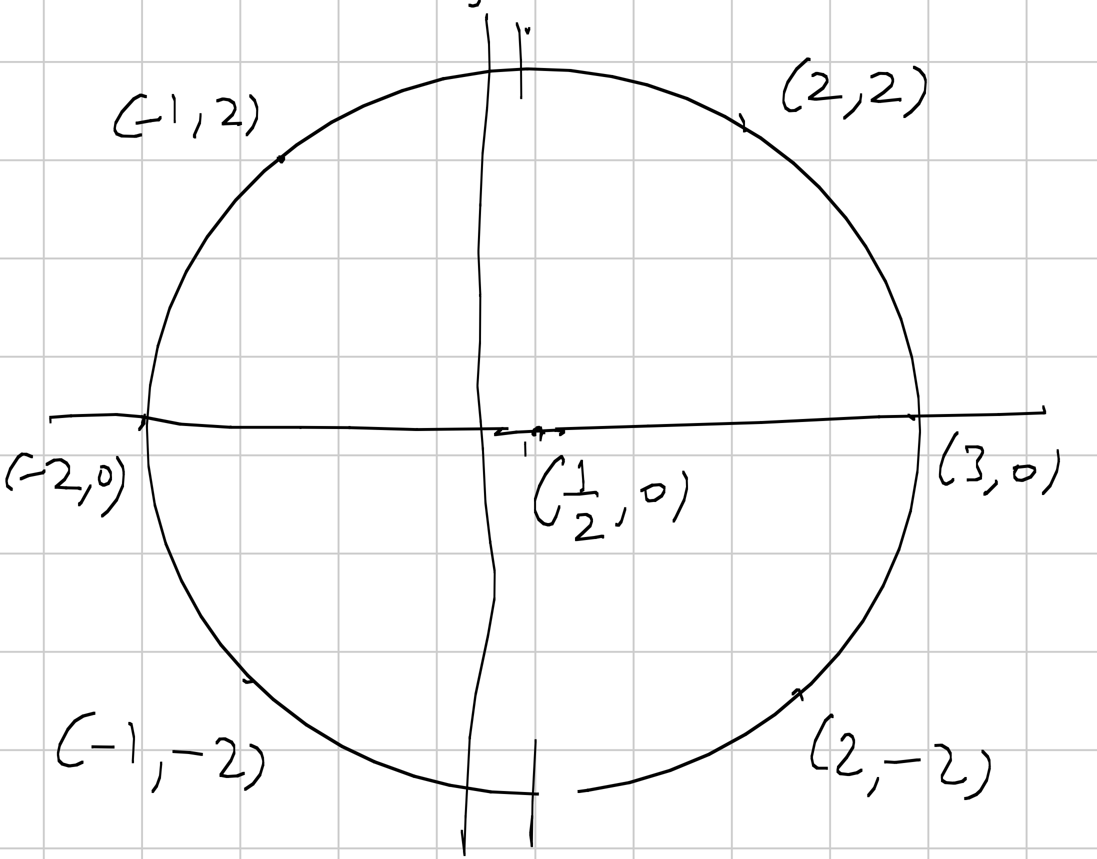
Per simmetria, almeno 3 avranno $k > n$

TUTTI DIVISIBILI PER $(r+si)^{n+1}$.

LE DIFFERENZE PURE

IL QUADRATO DEI MODULI DIV. per p^{n+1} $\blacksquare$

Oss 6 punti non bastano.



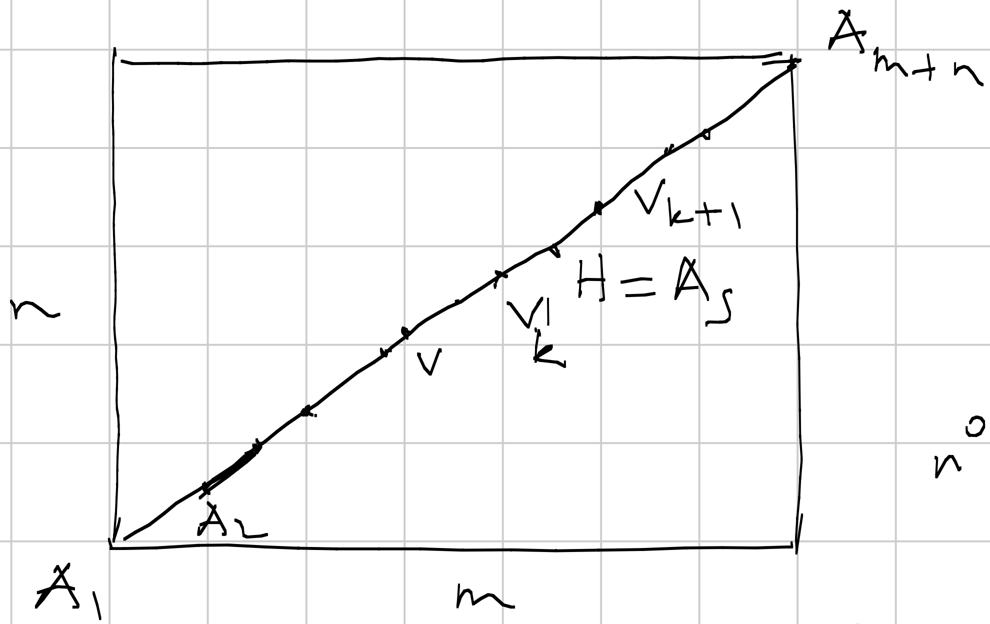
$p = 5$

$n = 1$

QUADRATI DELLE LUNGHEZZE DIV. per 5^2.

BMO 4 (2003?)

m, n dispari $(m,n)=1$.



Calcolare

$$A_1A_2 - A_2A_3 + A_3A_4 \dots + A_{m+n-1}A_{m+n}$$

n° segmenti $= m+n-1$
dispari

$\boxed{m>n}$

$$VV' = \frac{\sqrt{m^2+n^2}}{m}$$

I segmenti di tipo HV o VH sono in n° pari e quelli di tipo V_1V_2 sono dispari e vengono a segni alterni.

Il contributo alla somma dato dai segmenti di tipo V_1V_2 è:

$$\frac{\sqrt{m^2+n^2}}{m}.$$

Punto "orizzontale": $y = \ell$ intero $1 \le \ell \le n-1$.

$$H = \left(\frac{m}{n}\ell, \ell\right) = \left(q_\ell + \frac{r_\ell}{n}, \ell\right) = A_s$$

Divisione euclidea: $m\ell = q_\ell n + r_\ell$

$$A_{s-1} = V_k \qquad A_{s+1} = V_{k+1}$$

<u>Claim</u>: $s = \ell + q_\ell + 1$

Si parte da $A_1 = (0,0)$ e si incontrano q_ℓ pti verticali e ℓ pti orizzontali.

<u>2nd Claim</u>: $\ell + q_\ell \equiv r_\ell \pmod 2$

Infatti $\ell + q_\ell - r_\ell \equiv m(\ell + q_\ell - r_\ell) =$

$$q_e n + r_e + m q_e - m r_e \equiv \underset{\overset{\shortparallel}{0}}{(m+n)} q_e + \underset{\overset{\shortparallel}{0}}{(1-m)} r_e \equiv 0 \pmod 2$$

r_e pari $\iff$ s dispari $\qquad -A_{s-1}A_s + A_s A_{s+1}$

r_e dispari $\iff$ s pari $\qquad A_{s-1}A_s - A_s A_{s+1}$

r_e pari contributo $\qquad \dfrac{\sqrt{m^2+n^2}}{m}\left(-\dfrac{r_e}{n} + \dfrac{n-r_e}{n}\right)$

r_e dispari " $\qquad \dfrac{\sqrt{m^2+n^2}}{m}\left(\dfrac{r_e}{n} - \dfrac{n-r_e}{n}\right)$

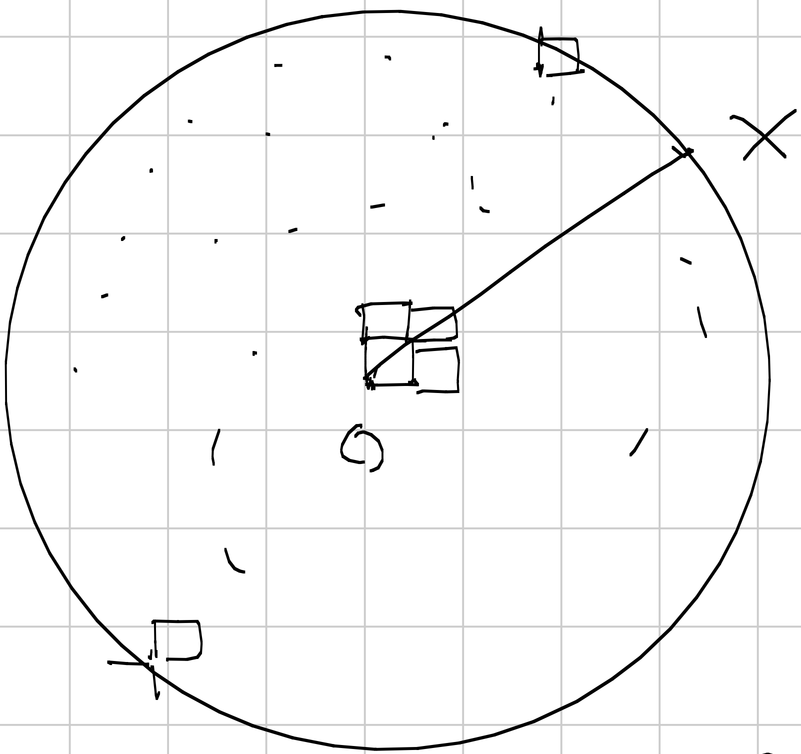
TOT. CONTRIBUTI È:

$$\frac{\sqrt{m^2+n^2}}{m} \cdot 2\left\{\frac{1-2+3 \qquad -(n-1)}{n}\right\} = -\frac{\sqrt{m^2+n^2}}{m} \cdot \frac{n-1}{n}$$

TOTALE (H+V) $\qquad \dfrac{\sqrt{m^2+n^2}}{m}\left\{1 - \dfrac{n-1}{n}\right\} = \dfrac{\sqrt{m^2+n^2}}{mn}$.

$$r(n) = \#\{(x,y) \in \mathbb{Z}^2 \mid x^2+y^2=n\}$$

$$R(X) = \sum_{n \le X} r(n)$$



I quadratini ricoprono un cerchio di raggio $X-\sqrt{2}$ e sono inclusi in un cerchio di raggio $X+\sqrt{2}$

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

$$\pi(X^2 + 2\sqrt{2}\,X + 2)$$

$$\sim \pi X^2$$

IMO 1997, 6.

$f(n)$ = n° di modi di scrivere n come somma di potenze di 2. (se due esp. differiscono per l'ordine → uguali)

Es.: $f(4)=4$ $\quad 4 \quad 2+2 \quad 2+1+1 \quad 1+1+1+1$.

<u>Tesi:</u>

$$2^{n^2/4} < f(2^n) < 2^{n^2/2}$$

$$2^n = x_0 + 2x_1 + 2^2 x_2 + \dots + 2^n x_n .$$

$x_i = $ (n° addendi $= 2^i$)

Cerco le n-ple $(x_1, \dots, x_n)$ tali che

$$2x_1 + 2^2 x_2 + \dots + 2^n x_n \leq 2^n .$$

$$x_i \leq 2^{n-i}$$

Ci sono n casi "eccezionali" $\quad x_i = 2^{n-i} \quad x_j = 0 \; j \neq i$

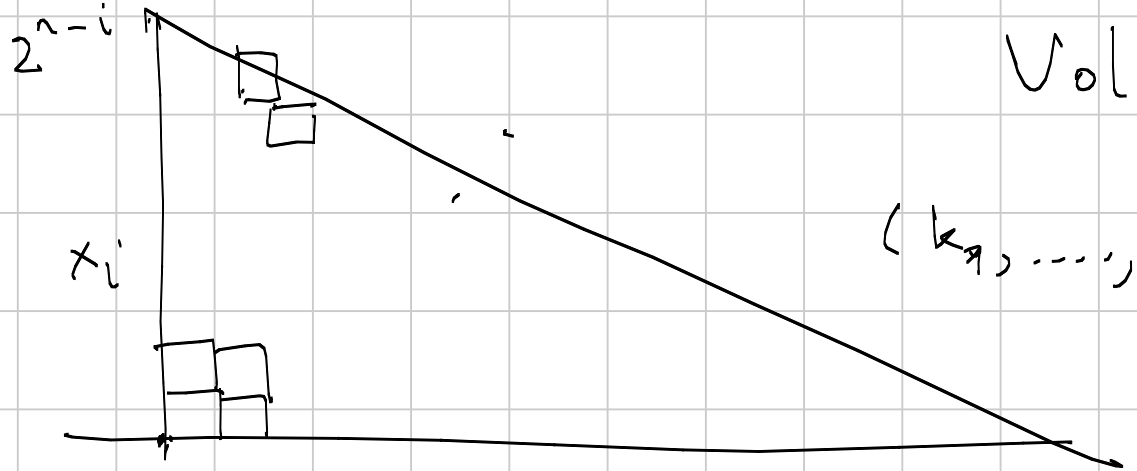
In tutti gli altri casi $x_i < 2^{n-i} \quad \forall i$

Questi casi sono al massimo $2^{n-1} \cdot 2^{n-2} \cdot \ldots \cdot 2^0 = 2^{\frac{n(n-1)}{2}}$

TOT. $\le n + 2^{\frac{n(n-1)}{2}} < 2^{\frac{n^2}{2}}$

$n \geq 3$

$$2x_1 + 2^2 x_2 + \ldots + 2^n x_n \le 2^n$$



$$\mathrm{Vol} = \frac{1}{n!}\, 2^{\frac{n(n-1)}{2}}$$

$(k_1, \ldots, k_n)$

$\perp$

IPERCUBO

$(k_1+1, \ldots, k_n+1)$

$$2[x_1] + 2^2[x_2] + \ldots + 2^n[x_n] \le 2^n$$

N° punti interi $\geq$ Vol $\approx \frac{1}{n!} 2^{\frac{n(n-1)}{2}} \overset{?}{>} 2^{n^2/4}$

$n \geq 12$?

$$2x_1 + 2^2 x_2 + \dots + 2^{n-2} x_{n-2} \leq 2^n$$

lati $\quad 2^{n-1} \quad 2^{n-2} \quad \dots \quad 2^2$

$$\text{Vol} = \frac{1}{(n-2)!} 2^{\frac{n(n-1)}{2} - 1} \overset{?}{>} 2^{n^2/4}$$

$n = 4 \qquad \frac{1}{2} \cdot 2^5 > 2^4$