WC 2017 - TdN

Note Title 25/01/2017

Esercizio N4

$$k = \frac{(m+n)^2}{4m(m-n)^2+4} \qquad (m \geq n)$$

Tesi: Se k è un intero, allora k è un quadrato perfetto.

$m+n = x \qquad m-n = y \qquad x>0 \quad y \geq 0$.

$$m = \frac{x+y}{2} \qquad n = \frac{x-y}{2}$$

$$k = \frac{x^2}{2(x+y)y^2+4}.$$

$$x^2 - 2ky^2x - 2ky^3 - 4k = 0.$$

Equazione di 2° grado nella x.

$$\frac{\Delta}{4} = k^2y^4 + \boxed{2ky^3} + 4k \quad \leftarrow$$

voglio che sia un quadrato perfetto.

$$\frac{\Delta}{4} \approx k^2y^4 = (ky^2)^2$$

$$\frac{\Delta}{4} = (ky^2+a)^2 = \square$$

$$\frac{\Delta}{4} = k^2y^4 + 2ak y^2 + a^2$$

$$a \approx y$$

$$\frac{\Delta}{4} \approx (k y^2 + y)^2$$

Vorrei dimostrare che

$$(k y^2 + y - 1)^2 < \frac{\Delta}{4} < (k y^2 + y + 1)^2$$

Disuguaglianza a sinistra: equivale a

$$k^2y^4 + y^2 + 1 + 2ky^3 - 2ky^2 - 2y < k^2y^4 + 2ky^3 + 4k$$

$$(y-1)^2 - 2ky^2 < 4k$$

$$(y-1)^2 < 2k(y^2+2)$$

$$2k > \frac{(y-1)^2}{(y^2+2)} < 1$$

ovviamente vero.

Disuguaglianza di destra:
equivale a

$$k(4 - 2y^2) < (y+1)^2$$

ovviamente vero per $y \geq 2$ (a sinistra c'è un termine negativo).

Conclusione: se $y \geq 2$ ho necessariamente

$$\frac{\Delta}{4} = (ky^2 + y)^2 = k^2y^4 + 2ky^3 + 4k$$

da cui $y^2 = 4k$

$4k$ è un quadrato $\Rightarrow$ k è un quadrato

Restano i casi $y=0$, $y=1$.

$y=0$ $\quad k = \frac{4m^2}{4} = m^2$ ok.

$y=1$ $\quad x^2 - 2kx - 6k = 0$

$$k = \frac{x^2}{2x+6} = \frac{x^2}{2(x+3)}$$

$(x^2, x+3) \mid 9$ $\qquad x+3 \mid x^2 - 9$

Provare i divisori di 9 e non funziona

NS

P INSIEME DEI PRIMI

$M \subseteq P$ SUO SOTTOINSIEME NON VUOTO

SE $p_1, p_2, \dots, p_k$ DISTINTI $\in M$

ALLORA I DIVISORI PRIMI

DI $(p_1 \cdot p_2 \cdot \dots \cdot p_k + 1) \in M$.

Th. $M = P$

---

i) M È INFINITO.

SUPPONIAMO M FINITO E SIANO

$p_1 < p_2 < \dots < p_m$ I SUOI PRIMI.

DALL'IPOTESI I DIVISORI PRIMI

DI $(p_1 \cdot p_2 \cdot \ldots \cdot p_n) + 1$ STANNO IN M.

SE $q \mid p_1 \cdots p_n + 1$, q PUÒ ESSERE UN p_i?

SE $q = p_i$ ALLORA

$q \mid p_1 \cdots p_n \longrightarrow q \mid 1$

PERCIÒ $q \neq p_i \quad \forall 1 \leq i \leq n$.

ESISTE UN DIVISORE PRIMO DI $p_1 \cdots p_n + 1$?

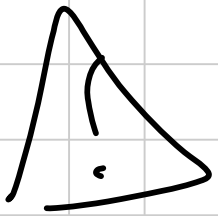
SÌ, PERCHÉ È ≥ 2.

$q \in M$, MA $q \notin M$ PERCHÉ $q \neq p_i$.

ASSURDO.

M FINITO → ASSURDO

M INFINITO → NON POSSO FARE IL PRODOTTO DEI SUOI ELEMENTI.

 M DEVE PURE ESSERE NON VUOTO

---

ii) LAVORIAMO PER ASSURDO E SUPPONIAMO q PRIMO CON $? \notin M$.

VEDIAMO GLI ELEMENTI DI M MODULO q.

LE CLASSI DI RESTO DI $\mathbb{Z}_q$:

$\{0, 1, \dots, q-1\}$

SIA C L'INSIEME DELLE CLASSI DI RESTO r TALI CHE ESISTONO FINITI $p_i \in M$ t.c.

$p_i \equiv r \ (q)$

SIA D L'INSIEME DELLE CLASSI DI RESTO r PER CUI ESISTONO INFINITI $p_i \in M$ t.c.

$p_i \equiv r \ (q)$

OVVIETÀ: $C \cap D = \emptyset$

$C \cup D = \mathbb{Z}_q$

$0 \notin C$ PERCHÉ: QUANTI SONO I PRIMI $\equiv 0 \ (q)$? 0 o 1

SE $-1 \in D$: CHE SUCCEDE!

PRENDO $p \in D$ T.C. $p \equiv -1 \ (q)$

q DIVIDE $p+1 \rightarrow 0 \in \mathbb{N}$: ASSURDO!

M INFINITO $\rightarrow$ D HA ALMENO UN ELEMENTO.

PERCHÉ:

PIGEON HOLE SULLE q CLASSI DI RESTO

HO ∞ PRIMI E q CASSETTI.

IDEA: POSSO FARE PRODOTTI A PIACERE DI PRIMI IN $\mathbb{N}$ LA CUI CLASSE DI RESTO STIA IN D: NE HO INFINITI.

SIA S L'INSIEME DEI PRODOTTI DEGLI ELEMENTI DI D (ANCHE RIPETUTI), MODULO q.

S SARÀ UN SOTTOINSIEME DI $\{0, 1, \dots, q-1\}$ E SARÀ IL SOTTOINSIEME DEGLI ELEMENTI:

$$d_1^{\alpha_1} \cdot d_2^{\alpha_2} \cdot d_3^{\alpha_3} \cdots d_k^{\alpha_k} \pmod q$$

CON $d_i \in D$, α_i INTERI POSITIVI.

CHIARAMENTE $D \subseteq S$:

$d \in D \rightarrow d^1 \in S$

$1 \in S$

PRENDO UN $d \in D$ A CASO:

$d^{q-1} \in S \rightarrow 1 \in S$

A COSA SERVE?

SE $S \in S$ ESISTONO PRIMI $p_1, p_2, \dots, p_n$ IN M TALI CHE:

$S \equiv p_1 \cdot p_2 \cdot \dots \cdot p_n \pmod{q}$

$d_1^{\alpha_1} \cdot d_2^{\alpha_2} \cdot d_3^{\alpha_3} \dots d_m^{\alpha_m}$ con $d_i \in D$

T

↳ d_1 COME CLASSI DI RESTO RAPPRESENTA INFINITI PRIMI DI M, QUINDI ALMENO α_1: POSSO SCEGLIERE PRIMI $p_{1,1}; p_{1,2}; \dots; p_{1,\alpha_1}$ TALI CHE

$$p_{1,j} \equiv d_1 \ (q)$$

PERCHÉ $d_1 \in D \rightarrow$ CE NE SONO INFINITI

LO STESSO PER $d_2, d_3, \dots, d_m$

PERCIÒ:

$$S \equiv d_1^{\alpha_1} \cdot d_2^{\alpha_2} \cdot \dots \cdot d_m^{\alpha_m} \equiv \prod_{i=1}^{m} \left(\prod_{j=1}^{\alpha_i} p_{i,j} \right) (q)$$

SONO TUTTI PRIMI DISTINTI CHE STANNO IN M.

QUINDI: SE $S \in \mathcal{S}$, ALLORA ESISTONO $p_i \in M$ t.c. $p_1 \cdots p_n \equiv S \pmod{q}$.

RITORNIAMO A C.

ORA PONIAMO

$Z = 1$ SE NON ESISTONO PRIMI IN M CON CLASSE DI RESTO IN C.

$$Z = \prod p$$

p ABBIA CLASSE DI RESTO MODULO q IN C

POSSO DEFINIRE LA PERCHÉ QUESTI p SONO FINITI.

CONSIDERIAMO $Z S + 1 \mod q$ AL VARIARE DI $S \in \mathcal{S}$

z_S SARÀ PRODOTTO DI PRIMI DISTINTI DI M: RAPPRESENTATI

- z È PRODOTTO DI PRIMI DI C OPPURE È ± 1;
- S È PRODOTTO DI PRIMI RAPPRESENTATI DA D (MODULO q)

PERCIÒ z_{S+1} MODULO q SI ESPRIME COME $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ CON $p_i \in M$ OPPORTUNI (PRENDENDO TUTTI QUELLI CON CLASSE DI RESTO FINITA)

$\forall s \in S$ ESISTONO $p_i \in M$ t.c.

$$p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \equiv z_{S+1} \ (q)$$

SE $p \mid p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \rightarrow p \in M$

SE $p \mid p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ ALLORA $p \in C$?

NO!

PERCHÉ SE $p \in C \rightarrow p \mid Z$, MA $Z \mid p_1 \cdot \ldots \cdot p_n$ PERCHÉ HO SCELTO I PRIMI DI Z TRA I p_i.

PRECISAZIONE IMPORTANTE: NEI VARI p_i T.C. $\prod p_i \equiv Z_S(n)$ PRENDO TUTTI I FATTORI DI Z.

QUINDI SE $p \mid p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \rightarrow p \in D \rightarrow p \in S$

$\mathbb{Z}_{S+1}$ (q)

ESISTE $s \in S$ TALE CHE

$\mathbb{Z}_{S+1} \neq S$. (INTESO MODULO q)

DIMOSTRAZIONE

SIANO $s_1, \dots, s_n$ GLI ELEMENTI

DI S.

$\mathbb{Z}_{s_i+1} \not\equiv \mathbb{Z}_{s_j+1}$ (q)

(SE $s_i \equiv s_j$ ↓ OVVIO)

$\updownarrow$

$s_i \not\equiv s_j$ (q)

(SE $\mathbb{Z}_{s_i+1} \equiv \mathbb{Z}_{s_j+1}$ ↓ $\mathbb{Z}_{s_i} \equiv \mathbb{Z}_{s_j} \to s_i \equiv s_j$)

$\mathbb{Z} \not\equiv 0 \ (q)$ ← $\mathbb{Z}_{s_i} \equiv \mathbb{Z}_{s_j} \to s_i \equiv s_j$

SENNÒ $q \in \mathbb{N}$

$s \mapsto \mathbb{Z}_{s+1}$ MODULO q

$\mathbb{Z}_{s+1} \mapsto s$; $\dfrac{(\mathbb{Z}_{s+1}) - 1}{\mathbb{Z}} = s$

$x \mapsto \frac{x-1}{2}$ (INVERSA DI $x \mapsto 2x+1$)

SAPPIAMO CHE $1 \in S$.

SAPPIAMO CHE $0 \notin S$ (ALTRIMENTI $0 \in \mathbb{N}$)

$1 \mapsto 0$

SE $2S+1$ MANDASSE S IN S, POICHÉ È INIETTIVA, LA SUA INVERSA DOVREBBE MANDARLO IN SE STESSO.

O ENTRA IN S, QUINDI UN ELEMENTO DI S DEVE USCIRNE.

SE $2S+1$ FOSSE SURIETTIVA (E DOVREBBE SE MANDA S IN S) 1 AVREBBE UNA

CONTROIMMAGINE IN S (MA DOVREBBE ESSERE $\emptyset$, ASSURDO!).

PERCIÒ $\exists\, t \in S$ t.c.

$Zt+1 \notin S$ → PRENDO $Z \cdot p_1 \cdots p_n = Zt$ (q)

p_1 MA

ESISTONO PRIMI $p_1, p_2, \ldots, p_n$ t.c.

$p_1 \cdot \ldots \cdot p_n \cdot Z + 1 \notin S$ (q)

$\forall s \in S$.

OPPURE

Z INCLUSO NEI p_i

CONSIDERIAMO LA SUA FATTORIZZAZIONE

$r_1^{\beta_1} \cdot r_2^{\beta_2} \cdot \ldots \cdot r_m^{\beta_m} = Z \cdot p_1 \cdot \ldots \cdot p_n + 1$

SE $Zt+1 \equiv 0$ (q): FINE, PERCHÉ

UN QUALCHE $r_i = q$.

SE $2t+1 \not\equiv 0 \pmod q$.

$r_i \pmod q \in C$? NO, ALTRIMENTI $r_i \mid Z$, ASSURDO

$r_i \pmod q \in D$

$r_1^{\beta_1} \cdot r_2^{\beta_2} \cdot \ldots \cdot r_m^{\beta_m} \pmod q \in S$

ASSURDO!

L'ASSURDO SI HA NELL'AVER SUPPOSTO $2s+1 \not\equiv 0 \pmod q$.

N 6 / Sia q un primo; g un polinomio

Lemma 1: Se $g(x) = a_k x^k + \dots + a_0$

$$\sum_{i=0}^{q-1} g(i) \equiv -a_{q-1} - a_{2(q-1)} - \dots \quad (q)$$

Lemma 2: Se $\deg g \leq q-1$

e $g(i) \equiv 0 \ (q) \ \forall i \Rightarrow g$ è il polinomio nullo modulo q

Lemma 3: Se $\deg \leq q-1$, $d \in \mathbb{N}$

$$g(x+d) = g(x) + d \cdot g'(x) + \frac{d^2}{2} \cdot g''(x) + \dots$$

$$= \sum_{i=0}^{q-1} g^{(i)}(x) \cdot \frac{d^i}{i!}$$

$$g(x) = a_k x^k + \dots + a_0$$

$$g'(x) = k a_k x^{k-1} + \dots + a_1$$

"Dim":

$$g(x+d) = a_k (x+d)^k + a_{k-1}(x+d)^{k-1} + \dots$$

$$= a_k \left(x^k + k d x^{k-1} + \dots\right) + a_{k-1}\left(x^{k-1} + (k-1) d x^{k-2} + \dots\right)$$

$$= \sum_{i=0}^{k} a_i \left(\sum_{j=0}^{i} x^j \binom{i}{j} d^{i-j} \right)$$

$$= \sum_{i=0}^{k} a_i \left(\sum_{j=0}^{i} x^j \frac{i\cdot(i-1)\cdots(i-j+1)}{j!} d^{i-j} \right)$$

$$= g(x) + d\left[a_k k x^{k-1} + \dots\right] + d^2\left[\binom{k}{2} a_k x^{k-2} + \binom{k-1}{2} a_{k-1} x^{k-3} + \dots\right] + \dots \frac{k(k-1)}{2}$$

$$= g(x) + d\,g'(x) + \frac{d^2}{2} g''(x) + \frac{d^3}{3!} g'''(x) + \dots$$

---

a) $\Rightarrow$ b)

Usiamo il lemma 3 su f

Vogliamo $\sum_{i=1}^{k} (a_{i+1} - a_i)^2 \equiv 0$

Sappiamo $a_i \equiv f(i) \pmod p$

Sostituiamo, e vogliamo allora

$$\sum_{i=1}^{p} \left(f(i+d) - f(i) \right)^2 \equiv 0$$

$$\| \quad d f'(x) + \dots$$

Se f ha grado $\leq \frac{p-1}{2}$

$\Rightarrow f'$ ha grado $\leq \frac{p-3}{2}$

Tutta la parentesi è un polinomio

di grado al più $\frac{p-3}{2}$

e quindi $\left(f(x+d) - f(x) \right)^2$

è un polinomio di grado

al più $p-3$

$\Rightarrow$ applichiamo il lemma 1

e la somma $\sum \left(f(i+d) - f(i) \right)^2 \equiv 0$

b ⇒ a

- Esiste un polinomio $h(x)$ [unico] tale che $h(i) \equiv a_i \pmod p$

$$h(x) = \sum_{i=1}^{p} \left(1 - (x-i)^{p-1}\right) \cdot a_i$$

$(x-i)^{p-1}$: è 0 in $x=i$ → elevo a $p-1$ → 0
$\neq 0$ in $x \neq i$ → 1

Sappiamo che

$$\sum_{i=1}^{p} (a_{i+d} - a_i)^2 \equiv 0$$

$a_{p+d} = a_d$

$a_{i+d} - a_i =$

$a_{i+d} - a_{i+p}$

↓

a meno di una traslazione $j = i+d$,

è la stessa di $a_j - a_{j+(p-d)}$

⇒ La condizione del testo

vale per tutti i d !

$$\sum (a_{i+d} - a_i)^2 \equiv \sum (h(i+d) - h(i))^2$$

$$\equiv 2\sum h(i)^2 - 2\sum h(i)h(i+d) \equiv 0$$

Usiamo il Lemma 3:

$$h(i+d) = h(i) + d\,h'(i) + \dots$$

$$d \sum h(i)h'(i) + d^2 \sum \frac{h(i)h''(i)}{2} +$$

$$d^3 \sum \frac{h(i)h'''(i)}{3!} + \dots + d^K \sum \frac{h(i)h^{(K)}(i)}{K!}$$

$$\equiv 0 \qquad \forall d = 0, 1, \dots, p-1$$

$K = \deg h \leq p-1$

$$\Rightarrow \quad \sum h(i)h^{(j)}(i) \equiv 0 \quad \forall j$$

$h(x) = a_k x^k + \dots + a_0$

se $k \leq \frac{p-1}{2}$ ok

se $k > \frac{p-1}{2}$

- prendiamo $j = 2k - p + 1 \geq 1$

  il polinomio $h(x) h^{(j)}(x)$

  ha grado $p-1$

  $\sum h(i) h^{(j)}(i) \equiv 0 \iff a_k \cdot \overbrace{k(k-1)\cdots(k-j+1)}^{\not\equiv 0} a_k \equiv 0$

  $\Rightarrow a_k \equiv 0$

  assurdo!