WC 2015 – TdN

Titolo nota 28/01/2015

N4 $\quad 2p^2 - 3p - 1 = n^3 \qquad p$ primo, $n > 0$.

$$p(2p-3) \mid n^3+1 = (n+1)(n^2-n+1)$$

$$p \mid n+1 \quad \text{oppure} \quad p \mid n^2-n+1$$

Caso $p \mid n+1$: $\quad n^3 < 2p^2 \leq p^3 \implies n < p$

$$p \geq n+1$$

$\implies p = n+1.$

Sostituiamo : si ottiene

$$0 = n^3 - 2n^2 - n + 2 = (n-2)(n+1)(n-1)$$

sol. intere positive : $n = 1, 2 \implies p = 2, 3$

FUNZIONANO

—

Caso $p \mid n^2-n+1$:

$$n^2 - n + 1 = kp$$

$$p(2p-3) = (n+1)(n^2-n+1) = (n+1)kp$$

Eliminando p, ottengo

$$p = \frac{(n+1)k + 3}{2}$$

Oss: k, $n+1$ DISPARI.

Sostituiamo in $\square$!

Otteniamo un'equazione di 2° grado in :

$$2n^2 - (k^2+2)n - (k^2+3k-2) = 0.$$

Ci vuole Δ = quadrato.

$$\Delta = k^4 + 12k^2 + 24k - 12$$

$$\Delta = (k^2+6)^2 = k^4 + 12k^2 + 36$$

$(k^2+6)^2 < \Delta$ se $k \geq 3$

$\Delta < (k^2+7)^2$ se $2k^2 - 24k + 61 > 0$

sicuramente per $k \geq 9$.

$k \geq 9 \Rightarrow \Delta \neq \square$

Basta considerare i valori di k dispari e < 9.

Otteniamo la tabella

$k=1$	$\Delta = 25$	
$k=3$	$\Delta = 249$	$\neq \square$
$k=5$	$\Delta = 1033$	$\neq \square$
$k=7$	$\Delta = 3265$	$\neq \square$

Sostituendo $k=1$, l'equazione di 2° grado diventa

$$2n^2 - 3n - 2 = 0$$

UNICA SOL. INTERA positiva è $n=2 \rightarrow p=7$

GIÀ VISTA !!

N5 Alcuni tentativi iniziali.

$n = 30$

n non funziona se $\exists\, p \nmid n$ tale che $p^2 < n$.

Se cerco $n > 30$ "buono", n deve essere divisibile per 30

$2^2 < n$ $3^2 < n$ $5^2 < n$

Quindi $n \geq 60 \Rightarrow 7 \mid n$ $(7^2 = 49 < n)$

Un eventuale numero n buono > 30 sarebbe multiplo di $2, 3, 5, 7$

Induttivamente, se

$$p_{n+1}^2 < p_1 p_2 p_3 \cdots p_n \qquad n \geq 4$$

devo aggiungere anche il fattore p_{n+1}.
DISUGUAGLIANZA VERA SEMPRE $\Rightarrow$ devo aggiungere tutti i primi, assurdo. (e si otterrebbe che il massimo n cercato è 30).

Postulato di Bertrand: $\forall n \ \exists p$ con $n < p \leq 2n$
$\downarrow$ TEOREMA

$$p_{n+1}^2 < (2p_n)^2 = 4p_n^2$$

Quindi basta vedere che

$$4p_n^2 < p_1 p_2 \cdots p_n, \quad 4p_n < p_1 p_2 \cdots p_{n-1}$$

$4p_n < 8p_{n-1}$: quindi basta

$$8p_{n-1} < p_1 \cdots p_{n-1}$$
$$8 < p_1 \cdots p_{n-2}$$

VERO $n-2 \geq 3$ $n \geq 5$

$n = 4$ SI CONTROLLA $p_5 = 11$

$$p_{n+1}^2 < p_1 \cdots p_n = (p_1 \cdots p_k)(p_{k+1} \cdots p_n)$$

Se prendo $k \leq n/2$ $p_1 \cdots p_k < p_{k+1} \cdots p_n$

Quindi basta $p_{n+1} < p_1 \cdots p_k$

$n - k = k$ (pari) $n - k = k+1$ (dispari)

IDEA Trovare un numero $m < p_1 \cdots p_k$ NON divisibile per nessuno dei $p_1, p_2, \ldots, p_n$
In questo caso, m ha un fattore primo $\neq p_1, \ldots, p_n$ e quindi $\geq p_{n+1}$ ($p_{n+1} \leq m < p_1 \cdots p_k$)

"COSTRUZIONE": considero i numeri

$$a_1 = p_1 p_2 \cdots p_{k-1} \cdot 1 - 1$$
$$a_2 = p_1 p_2 \cdots p_{k-1} \cdot 2 - 1$$

--- ---

$a_{p_k} = p_1 p_2 \cdots p_{k-1} \cdot p_k - 1$

Abbiamo p_k numeri, tutti minori di $p_1 \cdots p_k$ e tutti relativamente primi con $p_1, \ldots, p_{k-1}$

Per ogni primo $p \in \{p_k, p_{k+1}, \ldots, p_n\}$
al massimo uno degli a_i è divisibile per p
(sono a due a due non congrui modulo p)

$n-k+1$ primi $\qquad \#\, a_i = p_k$.

Ne devo eliminare al massimo $n-k+1$
se $n-k+1 < p_k$ ne resta uno libero

Ricordo che in ogni caso $n-k \leq k+1$
Mi basta

$$k+2 < p_k$$

vero per $k \geq 4$ $\qquad (6 < 7)$
$(n \geq 9)$

CASI INIZIALI: VERIFICA IMMEDIATA.

N6 $\qquad p > 5$

H_ϕ: $\exists k$ tale che $p \mid k^2+5$.
T_S: $\exists m, n > 0$ $\qquad p^2 = m^2 + 5n^2$

1° passo: trovare interi non nulli a, b tali che
$a^2 + 5b^2 =$ "h con h "piccolo".

Osservazione $\qquad p \mid a^2+5b^2 \iff p \mid a^2 - k^2 b^2$
$(a^2+5b^2 - a^2 + k^2 b^2 = (k^2+5)b^2$ div. per $p)$

Ora $\qquad a^2 - k^2 b^2 = (a+kb)(a-kb)$.
Quindi voglio trovare a, b non nulli, tali che $p \mid a+kb$

Principio dei cassetti:

CONSIDERO $S = [\sqrt{p}]$

$$X = \{ x + ky \mid 0 \le x, y \le S \}$$

$$|X| = (S+1)^2 > p. \qquad (\text{OK per } k \text{ grande})$$

Ci sono due elementi distinti di X che sono congrui modulo p. $x_1 + ky_1 \equiv x_2 + ky_2 \pmod p$

Prendo la differenza

$$0 \neq a + kb = (x_1 - x_2) + k(y_1 - y_2) \equiv 0 \pmod p$$

entrambi ✓ diversi da zero.

Oss. a e b sono diversi da zero.

(Se uno fosse divisibile per p, lo sarebbe anche l'altro)

cioè 0 — cioè 0

$$|a|, |b| < S < \sqrt{p}$$

$$a^2 + 5b^2 < p + 5p = 6p$$

Ho i casi $a^2 + 5b^2 = p, 2p, 3p, 4p, 5p$

- caso $a^2 + 5b^2 = p$. Mandpolando, ottengo

$$(a^2+5b^2)^2 = \underbrace{(a^2 - 5b^2)^2}_{m} + 5\underbrace{(2ab)^2}_{n} = p^2$$

- caso $a^2 + 5b^2 = 4p \rightarrow$ a e b sono pari.

$$\left(\frac{a}{2}\right)^2 + 5\left(\frac{b}{2}\right)^2 = p \rightarrow \text{caso precedente}$$

- caso $a^2 + 5b^2 = 5p \rightarrow 5 \mid a$

Divido per 5 $\quad 5\left(\frac{a}{5}\right)^2 + b^2 = p \rightarrow$ caso precedente

- caso $a^2 + 5b^2 = 2p \rightarrow$ a e b sono DISPARI

$$\frac{(a^2+5b^2)^2}{4} = \left(\frac{a^2 - 5b^2}{2}\right)^2 + 5(ab)^2 = p^2$$

- caso $a^2 + 5b^2 = 3p \rightarrow$ a e b non sono divisibili per 5

$a+b \equiv 0 \pmod 3$ oppure $a-b \equiv 0 \pmod 3$

Formule: $\left(\frac{a-5b}{3}\right)^2 + 5\left(\frac{a+b}{3}\right)^2 = 2p$

$\left(\frac{a+5b}{3}\right)^2 + 5\left(\frac{a-b}{3}\right)^2 = 2p$ → caso precedente

— o —

IN7 $(2^n-1)(3^n+1) \neq \square$.

PER ASSURDO: $\exists n$ tale che viene un quadrato.

Oss. (facile): n è pari.

(Se n è dispari $2 \| 3^n+1$)

$n = 2k$

L'equazione diventa

$$\left((2^k)^2-1\right)\left((3^k)^2-1\right) = \square$$

Ne segue che $\exists r, s$ d (d libero da quadrati) tali che

$$(2^k)^2 - 1 = dr^2 \qquad (3^k)^2 - 1 = ds^2$$

Consideriamo l'equazione di Pell * (* $d \neq 1$)

$$x^2 - dy^2 = 1$$

Questa equazione ha per soluzioni

$(2^k, r)$ $(3^k, s)$

Sol. positive di Pell sono

$(1,0) = (a_0, b_0)$, (a_1, b_1), ..., (a_n, b_n) ...

dove $(a_n + b_n\sqrt{d}) = (a_1 + b_1\sqrt{d})^n$.

Soddisfano una ricorrenza:

$a_{n+1} + b_{n+1}\sqrt{d} = (a_n + b_n\sqrt{d})(a_1 + b_1\sqrt{d})$

$= (a_n a_1 + b_n b_1 d) + (a_n b_1 + b_n a_1)\sqrt{d}$

a_{n+1} $\qquad$ b_{n+1}

Cambiando indice, ho $\qquad b_n = a_{n-1} b_1 + b_{n-1} a_1$

$$b_n b_1 d = a_{n-1} b_1^2 d + b_{n-1} a_1 b_1 d$$
$$= a_{n-1}(a_1^2 - 1) + a_1 (a_n - a_{n-1} a_1)$$
$$= a_{n-1} + a_1 a_n$$

RICORRENZA: $\qquad a_{n+1} = 2a_1 a_n - a_{n-1}$

a

- $a = a_1$: a deve essere pari.
  (se a fosse dispari, tutti gli a_i sarebbero dispari). NON VOGLIO (vorrei $a_i = 2^k$)

- $a_{n+1} \equiv a_{n-1} \pmod 2$ $\qquad a_{2h} \equiv 1 \pmod 2$
  $a_{2h+1} \equiv 0 \pmod 2$

- congruenza modulo a : $\qquad a_{2h} \equiv \pm 1 \pmod a$
  $a_{n+1} \equiv -a_{n-1} \pmod a$ $\qquad a_{2h+1} \equiv 0 \pmod a$

Ne segue che $\qquad a_{2h+1} = 2^k \Rightarrow \quad a = 2^r$

Per concludere, voglio dimostrare che $3 \mid a$ che contraddice $a = 2^r$.

- $a \equiv 1 \pmod 3$ $\qquad$ sono entrambi assurdi
- $a \equiv 2 \pmod 3$

Se $a \equiv 1 \pmod 3$ la successione mod 3 è
$1, 1, 1, 1, \ldots$ $\quad \ldots \rightarrow$ NESSUNA POTENZA DI 3.

Se $a \equiv 2 \pmod 3$ la successione mod 3 è
$1, 2, 1, 2, \ldots$ $\quad \rightarrow$ NESSUNA POTENZA DI 3.

$a \equiv 1 \quad (3)$ $\qquad a_{n+1} \equiv 2a_n - a_{n-1}$
$a \equiv 2 \quad (3)$ $\qquad a_{n+1} \equiv 4a_n - a_{n-1} \equiv a_n - a_{n-1}$

$a_0 \equiv 1$ $a_1 \equiv 1$ $a_2 \equiv 1$

$a_0 \equiv 1$ $a_1 \equiv 2$ $a_2 \equiv 1$

ok !!