PREIMO 2014 — N — Pomeriggio

Titolo nota 28/05/2014

N5 Molteplicità m di 1 in $f(X)$: vuol dire $f(1)=0$ $f'(1)=0$, ..., $f^{(m-1)}(1)=0$ $f^{(m)}(1)\neq 0$.

$f(1)=$ ovvio $\quad f(1)=\sum a_i = 0$

$$f(X) = a_1 + a_2 X + \dots + a_{p-1} X^{p-2}$$

$$f'(X) = a_2 + 2a_3 X + \dots + (p-2)a_{p-1} X^{p-3}$$

$$f'(1) = a_2 + 2a_3 + (p-2)a_{p-1} = \sum_{i=1}^{p-1} (i-1)a_i$$

$$= \sum_{i=1}^{p-1} i a_i - \sum_{i=1}^{p-1} a_i = f(1) = 0.$$

Q = residui quadratici, N = non residui quadratici

$$\sum_{i=1}^{p-1} i a_i = \sum_{i\in Q} i - \sum_{i\in N} i.$$

$$\frac{p(p-1)}{2} = \sum_{i\in Q} i + \sum_{i\in N} i$$

SOMMA PARI $\Rightarrow \frac{p-1}{2}$ pari cioè $p\equiv 1 \pmod 4$

$p\equiv 3 \pmod 4 \Rightarrow f'(1)\neq 0$

$p\equiv 1 \pmod 4 \quad -1 = \square$

Nella somma ci sono coppie $\{i, p-i\}$ $\begin{cases} \text{entrambi in } Q \\ \dots \text{ in } N \end{cases}$

che sommate insieme danno p

n° coppie $= \frac{p-1}{4}$ (quadrati) $+ \frac{p-1}{4}$ non quadrati.

si ANNULLANO

$p\equiv 5 \pmod 8 \Rightarrow p\equiv 1 \pmod 4 \quad f'(1)=0 \quad (X-1)^2 \mid f(X)$

Oss. $p\equiv 5 \pmod 8 \quad \left(\frac{2}{p}\right) = -1$

Divido Q in Q^+ e Q^-, N in N^+ e N^-

$Q^+ = \{i\in Q \mid i > \frac{p}{2}\}$ $\quad Q^- = \{i\in Q \mid i < \frac{p}{2}\}$

N^+, N^- analoghi.

$r \to p-r \qquad Q^+ \to Q^- \qquad N^+ \to N^-$

$$\sum_{r\in Q^+} r^2 = \sum_{r\in Q^-} (p-r)^2 = \frac{p^2(p-1)}{4} - 2p\sum_{r\in Q^-} r + \sum_{r\in Q^-} r^2$$

$$\sum_{r\in Q} r^2 = \frac{p^2(p-1)}{4} - 2p\sum_{r\in Q^-} r + 2\sum_{r\in Q^-} r^2 .$$

e analoga per N.

$r \to 2r$ $\quad Q_- \to N_{pari}$

$r \to p-2r$ $\quad Q_- \to N_{dispari}$

$$\sum_{r\in N} r^2 = \sum_{r\in Q^-} (2r)^2 + \sum_{r\in Q^-} (p-2r)^2$$

$$= \frac{p^2(p-1)}{4} - 4p\sum_{r\in Q^-} r + 8\sum_{r\in Q^-} r^2 .$$

Combinando, si ottiene (verificare)

$$\sum_{r\in Q} r^2 - \sum_{r\in N} r^2 = 2p\sum_{r\in Q^-} r - 6\sum_{r\in Q^-} r^2 \quad \leftarrow (\otimes)$$

e anche

$$= -2p\sum_{r\in N^-} r + 6\sum_{r\in N^-} r^2 . \quad (\otimes\otimes)$$

Supponiamo $f''(1)=0$ (assurdo : $\mathrm{mcd}\geq 3$)

$$f''(1) = \sum_{i=1}^{p-1} (i-1)(i-2)a_i = \boxed{\sum_{i=1}^{p-1} i^2 a_i} - 3\sum_{i=1}^{p-1} i a_i + 2\sum_{i=1}^{p-1} a_i$$

$\neq 0$ $\qquad = 0$

$$\boxed{\sum_{i\in Q} i^2 - \sum_{i\in N} i^2}$$

$f''(1)=0 \iff \sum_{i\in Q} i^2 = \sum_{i\in N} i^2$

Ugnagliando a zero $(\otimes)$ e $(\otimes\otimes)$ e mettendole nelle formule precedenti, troviamo

$$\sum_{r\in Q} r^2 = \frac{p^2(p-1)}{4} - \frac{4}{3}p\sum_{r\in Q^-} r$$

$$= \frac{p^2(p-1)}{4} - \frac{4}{3}p\sum_{r\in N^-} r$$

da cui $\quad \sum_{r\in Q^-} r = \sum_{r\in N^-} r$

$$\sum_{r\in Q^-\cup N^-} r = \sum_{r<\frac{p}{2}} r = \frac{p^2-1}{8} \to \text{dispari}$$

$p = 8k+5 \qquad p^2-1 = 64k^2+80k+24$ $\qquad$ ASSURDO

N6 (I divisori primi di $\left(\prod_{p\in A} p\right)-1$ appartengono a M

$A \subsetneq M$ $M \subseteq$ primi)

Oss $2 \in M$ $A=\{p\}$ $p \neq 2$ $2 \mid p-1$

Supponiamo M finito, $M=\{2, p_2, \dots, p_k\}$ $P=\prod_{p\in M} p$

$A=\{2, p_3, \dots p_k\}$ $2p_3 \dots p_k - 1 = \frac{P}{p_2} - 1 = p_2^{\alpha}$ (1)

$A'=\{p_3 \dots, p_k\}$ $p_3 \dots p_k - 1 = \frac{P}{2p_2} - 1 = 2^{\beta} p_2^{\gamma}$. (2)

$P = 2p_2(2^{\beta} p_2^{\gamma}+1) = p_2^{\alpha+1} + p_2$

$2^{\beta+1} p_2^{\gamma} + 2 = p_2^{\alpha} + 1$

$\Rightarrow$ $2 \equiv 1 \pmod{p_2}$ ASSURDO.

(Verificare i casi rimanenti)

$2, p_1, p_2$ $P \simeq \pm 1 \pmod 3$

$A\{p\}$ $A\{2, p\}$

$p-1$ $2p-1$

$M\{2, 3, \dots p_k\}$ $\frac{P}{2} - 1 = 2^k$ $\frac{P}{3} - 1 = 3^m$

$2^{k+1} + 2 = 3^{m+1} + 3$

$2^{k+1} - 3^{m+1} = 1$

$2, 3 \in M$ $2 \cdot 3 - 1 = 5 \longrightarrow 5 \in M$

$3 \cdot 5 - 1 = 14 \longrightarrow 7 \notin M$

$3 \cdot 5 \cdot 7 \cdot (\text{tutti gli altri}) - 1 = 2^k$

Rivedere il caso M infinito. $M = \{2, p_2, p_2p_3, \dots\}$

Assurdo: $\exists q \notin M$

$2, \quad 2p_2, \quad 2p_2p_3, \dots$ mod q.

$\Rightarrow$ ce ne sono due uguali

$$2p_2p_3 \cdots p_i \equiv 2p_2p_3 \cdots p_i p_{i+1} \cdots p_j \pmod q$$

$$\underbrace{2p_2p_3 \cdots p_i}_{q \text{ non divide}} (p_{i+1} \cdots p_j - 1) \equiv 0 \pmod q$$

q divide $\quad q \in M$ ASSURDO.

N7 Partenza: trovare $N, 2N$ che siano entrambi somme di quadrati distinti.

(+ un'altra condizione, da vedere dopo)

$N = 29 = 5^2 + 2^2 \qquad 2N = 58 = 7^2 + 3^2$

$$M = \sum_{k=0}^{4N-2} (2kN+1)^2$$

Teor: $P > M \Rightarrow P$ è somma di quadrati distinti

$(N = a_1^2 + \cdots + a_m^2, \quad 2N = b_1^2 + \cdots + b_n^2) \Leftarrow$

Divido P per $4N$, $\quad P = 4Nq + r \qquad 0 \le r \le 4N-1$

$$\sum_{k=0}^{r-1} (2kN+1)^2 \equiv r \pmod{4N}$$

Se $r \ge 1$ $\qquad P = \sum_{k=0}^{r-1} (2kN+1)^2 + 4Nt$

quadrati distinti

(se $r = 0$ pongo $P = 4Nt$)

Scrivo t in base 2 (dividendo esponenti pari e dispari)

$$t = \sum_i 2^{2\lambda_i} + \sum_j 2^{2\mu_j+1}$$

$$P = \sum_{k=0}^{r-1} (2kN+1)^2 + 4\left(\sum a_i^2\right)\left(\sum (2^{\lambda_i})^2\right) + \left(\sum b_s^2\right) \cdot 4 \sum (2^{\mu_j})^2$$

(Uso $4N = 2N \cdot 2$:

Distinti: Basta che fra i a_i $\dots$

$a_r \mid a_{r'}$ $\quad b_s \mid b_{s'}$ $\quad a_r \mid b_s$ $\quad b_s \mid a_r$ non ci stiamo facendo dei 2

N8 Si cercano (a,b,c) tali che $a^n+2^n \mid b^n+c \quad \forall n>0$

Qualche condizione necessaria:

voglio che $b^n+c \equiv 0 \quad (a^n+2^n) \Rightarrow b^n \equiv -c \quad b^{3n} \equiv -c^3$

$b^{3n}+c \equiv 0 \quad (a^{3n}+2^{3n}) \Rightarrow b^{3n}+c \equiv 0 \quad (a^n+2^n)$

$$c^3 \equiv c \pmod{a^n+2^n}$$

$$c^3-c = c(c+1)(c-1) \equiv 0 \pmod{a^n+2^n}$$

n grande $\Rightarrow c(c+1)(c-1)=0 \qquad c=0,1$

c=0 $\quad a=2 \quad a^n+2^n = 2^{n+1}$ vorrei che $2^{n+1} \mid b^n$

Basta che $b=4k$ $\rightarrow$ soluzioni

$a=2, \ b=4k, \ c=0 \qquad (k \neq 0)$

Supponiamo $a \neq 2$. Osservo che l'insieme dei primi che dividono a^n+2^n è infinito. (questo conclude che è impossibile)

- a pari, $a=2a_1 \quad a^n+2^n = 2^n(a_1^n+1)$

$$\left(a_1^{2^k}+1, \ a_1^{2^\ell}+1\right) \mid 2$$

- a dispari $\quad \left(a^{2^r}+2^{2^r}, a^{2^s}+2^{2^s}\right)=1$

Ne segue che questo caso non dà soluzioni.

---

c=1 a non può essere pari

(se no $a^2+2^2 \mid b^2+1$, impossibile mod 4)

Quindi a dispari e $2a \neq \square$

$$2a = \ell^2 p_1 \cdots p_t \qquad (t \geq 1)$$

$$b = m^2, \quad b = p_k p_{k+1} \cdots p_{t+s} m^2$$

$p_1 \ p_2 \ \cdots \ p_k \ \cdots \ p_t$

$p_k \ \cdots \ p_t \ \cdots \ p_{t+1}$ $\quad \|$

Scopo: trovare un primo p tale che $\neq$ distanti

$$\left(\frac{2a}{p}\right) = -1 \qquad \left(\frac{b}{p}\right) = 1$$

$$(2a)^{\frac{p-1}{2}} \equiv -1 \pmod p \qquad 2^{\frac{p-1}{2}} \equiv -a^{\frac{p-1}{2}} \pmod p$$

$$2^{\frac{p-1}{2}} + a^{\frac{p-1}{2}} \equiv 0 \pmod p$$

$$p \mid 2^n + a^n \quad \text{per } n = \frac{p-1}{2}$$

$$b^{\frac{p-1}{2}} \equiv 1 \pmod p, \qquad b^{\frac{p-1}{2}} + 1 \equiv 2 \not\equiv 0 \pmod p.$$

$\Rightarrow$ IMPOSSIBILE

$$\left(\frac{p\eta}{p}\right) = -1 \qquad \left(\frac{p\xi}{p}\right) = 1$$

Conclusione: Le uniche soluzioni sono

$$(a,b,c) = (2, \pm k, 0) \qquad k \neq \square.$$