MISCELLANEA

Titolo nota 25/01/2008

$p(x)$ coeff. interi MONICO grado pari

$p(n)$ quadr. per ∞ valori di $n \in \mathbb{N}$

Tesi: $p(x) = [q(x)]^2$ con $q(x)$ a coeff. interi

$$p(x) = x^{2k} + \boxed{a_{2k-1}}\, x^{2k-1} + \boxed{a_{2k-2}}\, x^{2k-2} + \dots$$

$$q(x) = x^k + b_{k-1}\, x^{k-1} + b_{k-2}\, x^{k-2} + \dots$$

$$[q(x)]^2 = x^{2k} + \boxed{2b_{k-1}}\, x^{2k-1} + \boxed{\left(b_{k-1}^2 + 2b_{k-2}\right)} x^{2k-2} + \dots$$

Nei coeff. di $[q(x)]^2$ ogni volta si aggiunge un coeff di $q(x)$

Ottengo un sistema con k incognite (i coeff. di $q(x)$)
"TRIANGOLARE" e ogni equazione
è lineare nella variabile "NUOVA"

$$\begin{aligned} ax &= \dots \\ bx + cy &= \dots \\ dx + ey + fz &= \dots \end{aligned}$$

Posso permettermi k equazioni,
quindi posso sistemare tutti i coeff.
fino ad a_k.

Trovo quindi

$$p(x) = \underbrace{[q(x)]^2}_{\text{grado } 2k} + \overset{\text{grado } \leq k-1}{r(x)}$$

"Piccola seccatura: $q(x)$ ha coeff. razionali".

Moltiplicando per il denom. arrivo a

$$P(x) = [Q(x)]^2 + R(x) \qquad \text{a coeff. interi}$$

$$P(n) = [Q(n)]^2 + R(n)$$

$P(n) \to$ Quadrato, $Q(n) \to$ Quadrato, $R(n) \to \neq 0$

voglio dim. che $R(n)$ ha infinite radici

A^2 e B^2 o sono uguali, oppure k^2-2k+1, k^2, k^2+2k+1

$A^2 - B^2 \sim A+B$

m è un quadrato $\sim 2\sqrt{m}$

$A = \sqrt{P(n)}$

$B = Q(n)$

$A+B \sim$ grado k

cresce come n^k

Ma $A^2 - B^2$ è $R(n) \leftarrow$ cresce al + come n^{k-1}

ASSURDO

Lemma per liberarsi dei razionali

$p(x) \in \mathbb{Z}[x]$ $\qquad$ $q(x) \in \mathbb{Q}[x]$

MONICO

$$p(x) = [q(x)]^2$$

$\Rightarrow \quad q(x) \in \mathbb{Z}[x].$

[Lemma di GAUSS] Se $p(x) = q(x) \cdot r(x)$

coeff. interi $\qquad$ coeff. raz. $\qquad$ coeff. raz

$\Rightarrow \exists\, c \in \mathbb{Q}$ t.c. $\quad c\,q(x)$ ha coeff. interi

$\dfrac{r(x)}{c}$ " " "

— o — o —

Oss. 1   La monicità è necessaria

Oss. 2   Il grado pari è necessario $p(x) = x^3$

Ci sono altri esempi non monomi ?

SI! : $x^3 (x+7)^{2008}$

FUNZIONALE $\quad f : (0,+\infty) \longrightarrow (0,+\infty)$

$$f(x+f(y)) = f(x+y) + f(y) \qquad \forall x>0 \ \forall y>0$$

1 $\quad \cancel{x} + f(y) = \cancel{x} + y \qquad\qquad x + f(y) = y$

$$x = y - f(y)$$

Se potessi porre $x = y - f(y)$ avrei

$$\cancel{f(\quad)} = f(\underbrace{2y - f(y)}) + \cancel{f(\quad)}$$

Avrei trovato un valore per cui $f = 0$ → VIETATO

→ NON POSSO FARE LA SOSTITUZIONE

→ cioè $x \le 0$, cioè $y - f(y) \le 0$, cioè $\boxed{f(y) \ge y}$.

1° FATTO

② Se avessi $f(y) = y$ per qualche $y > 0$, avrei

$$f(\cancel{x+f(y)}) = f(\cancel{x+y}) + f(y)$$

$\to f(y) = 0 \to$ VIETATO $\boxed{f(y) > y \quad \forall y > 0}$

2° FATTO

③ $g(y) = f(y) - y$ DEFINIZIONE DI UNA FUNZIONE

$g: (0, +\infty) \longrightarrow (0, +\infty)$

$f(x) = g(x) + x$ riscrivo l'eq. usando g !

$$\underbrace{\cancel{x} + \cancel{y} + \cancel{g(y)}}_{x+f(y)} + \underbrace{g(x+y+g(y))}_{g(x+f(y))} = \underbrace{g(x+y) + \cancel{x} + \cancel{y}}_{f(x+y)} + \underbrace{\cancel{g(y)} + y}_{f(y)}$$

$$g(\underbrace{x+y}_{z}+g(y)) = g(\underbrace{x+y}_{z}) + y$$

$$\boxed{g(z+g(y)) = g(z) + y \quad \forall y>0 \quad \forall z>y}$$ 3° FATTO

④ Supponiamo g non iniettiva: $g(a) = g(b)$ $(a \neq b)$

Metto a e b al posto di y:

$$g(z+g(a)) = g(z) + a$$

$$\parallel$$

$$g(z+g(b)) = g(z) + b$$

Deve essere $z > a$
$z > b$

$\Rightarrow a = b.$ $\Rightarrow$ $\boxed{g \text{ è iniettiva}}$ 4° FATTO

⑤ SERVE $a>b$ e $a>c$

$$\cancel{g}(\underbrace{a+g(b)}_{z}+g(c)) = g(a+g(b)) + c = g(a) + b + c$$

SERVE
$a > b+c$

$$\Rightarrow = \cancel{g}(a+g(b+c))$$

Grazie all'iniettività ho

$$\boxed{g(b)+g(c) = g(b+c) \qquad \forall b>0 \ \forall c>0}$$ 5° FATTO

⑥ Ritorno a $g(z+g(y)) = \cancel{g(z)}+y$

$$\Big\downarrow \text{5° FATTO}$$

$$\cancel{g(z)} + g(g(y))$$

$\Rightarrow$ $\boxed{g(g(y)) = y}$ 6° FATTO $\forall y>0$

⑦ Dal 6° fatto segue che g è crescente (strett.)

⑧ <u>Lemma</u> $g:(0,+\infty)\to(0,+\infty)$ crescente + $g(g(x))=x$
$\Rightarrow$ $g(x)=x$ sempre.

Idea Se fosse $g(x) > x$ avrei

$$g(g(x)) > g(x) > x$$

Se fosse $g(x) < x$ avrei

$$g(g(x)) < g(x) < x$$ FINE

Nota g, nota f. VERIFICA !!!

SUCC. PER RICORRENZA: $a_0 = 2 \qquad a_{n+1} = 2a_n^2 - 1$

$$\cos(2x) = 2\cos^2 x - 1$$

Quindi se $\quad \cos x = a_0, \quad a_1 = \cos(2x)$

$$a_2 = \cos(4x), \dots, a_n = \cos(2^n x)$$

$$\cos x = \frac{1}{2}\left(e^{ix} + e^{-ix}\right)$$

$$\cos(2^n x) = \frac{1}{2}\left(e^{ix2^n} + e^{-ix2^n}\right) \qquad e^{ix} = A, \quad e^{-ix} = \frac{1}{A}$$

Quindi

$$a_n = \cos(2^n x) = \frac{1}{2}\left\{A^{2^n} + \left(\frac{1}{A}\right)^{2^n}\right\}$$

Se voglio calcolare A, impongo che valga per $n=0$

$$2 = a_0 = \frac{1}{2}\left\{A + \frac{1}{A}\right\} \qquad A + \frac{1}{A} = 4$$

$$A^2 - 4A + 1 = 0 \qquad A = 2 \pm \sqrt{3}$$

Finale $$\boxed{a_n = \frac{1}{2}\left\{ \left(2+\sqrt{3}\right)^{2^n} + \left(2-\sqrt{3}\right)^{2^n} \right\}}$$

VERIFICO PER INDUZIONE
QUESTA FORMULA

La stessa formula vale modulo p (spero che 3 sia un quadrato mod p)

$$a_n = \frac{1}{2}\left(A^{2^n} + \frac{1}{A^{2^n}}\right) = \frac{1}{2}\,\frac{A^{2^{n+1}} + 1}{A^{2^n}}$$

$$p \mid a_n \iff A^{2^{n+1}} + 1 \equiv 0 \ (p) \iff A^{2^{n+1}} \equiv -1 \ (p)$$

$$\Rightarrow A^{2^{n+2}} \equiv 1 \ (p) \underset{\text{FLT}}{\Longrightarrow} \operatorname{ord}_p(A) \mid 2^{n+2}$$

$\Rightarrow$ ord è una potenza di 2 $\Rightarrow$ ordine è 2^{n+2}

$\Rightarrow 2^{n+2} \mid p-1 \Rightarrow p \equiv 1 \mod 2^{n+2}$

$\Rightarrow (p+1)(p-1)$ è multiplo di 2^{n+3}

guadagno un fattore 2.

TUTTO QUESTO FUNZIONA se esiste A t.c.

$$A + \frac{1}{A} = 4 \pmod p \iff \sqrt{3} \text{ esiste mod } p.$$

$(\iff p \equiv \pm 1 \mod 12)$
GRL

$$A \overset{"}{=}\!\!" \; 2+\sqrt{3} = \frac{(\sqrt{3}+1)^2}{2} = \left(\frac{\sqrt{3}+1}{\sqrt{2}}\right)^2 = B^2$$

$$a_n = \frac{1}{2}\left(A^{2^n} + \frac{1}{A^{2^n}}\right) = \frac{1}{2}\left(B^{2^{n+1}} + \frac{1}{B^{2^{n+1}}}\right)$$

HO GUADAGNATO

Invece di lavorare in $\mathbb{F}_p$, lavoriamo in $\mathbb{F}_{p^2}$

$$\mathbb{F}_{p^2} = \{ a + b\sqrt{3} : a \in \mathbb{F}_p, \; b \in \mathbb{F}_p \}$$

$\mathbb{F}_{p^2}$ posso sommare, moltiplicare, dividere...

$\mathbb{F}_{p^2}^*$ = elementi diversi da 0 chiusi rispetto al prodotto

$$\frac{a+b\sqrt{3}}{c+d\sqrt{3}} \cdot \frac{c-d\sqrt{3}}{c-d\sqrt{3}} = \frac{\cdots}{c^2-3d^2}$$

$$c^2-3d^2=0$$
$$\frac{c^2}{d^2}=3$$

Quanti el. ha $\mathbb{F}_{p^2}^*$: p^2-1

$\mathrm{ord}_{\mathbb{F}_{p^2}^*} B = 2^{n+3}$ Ma ord | num. el. (FLT)

$$\Rightarrow 2^{n+3} \mid p^2-1$$

$\sqrt{2} \in \mathbb{F}_{p^2}^*$, cioè $\sqrt{2}$ si scrive come $a+b\sqrt{3}$?

SI: $\to$ o $\sqrt{2} \in \mathbb{F}_p$ (cioè 2 è un $\square$ mod p)

<u>Lemma</u> Se 2 non è un quadrato mod p, allora si scrive nella forma $b\sqrt{3}$

Motivo: $b\sqrt{3} \overset{?}{=} \sqrt{2}$ $\qquad b^2 \cdot 3 \overset{?}{=} 2$

$$b^2 \overset{?}{=} \frac{2}{3} \qquad b = \sqrt{\frac{2}{3}}$$

Se 2 non è un $\square$ e 3 è non un $\square$, allora $2 \cdot 3$ e $\frac{2}{3}$ sono $\square$

Dim: 2 non $\square$ $\Leftrightarrow$ $2 = g^{2k+1}$

3 " $\square$ " $3 = g^{2R+1}$