TEORIA DEI NUMERI

Note Title 22/01/2020

① $f(n!) = f(n)!$

$m - n \mid f(m) - f(n)$

Soluzioni: $f(n) = 1 \quad \forall n$

$f(n) = 2 \quad \forall n$

$f(n) = n \quad \forall n$

$f(1!) = f(1)!$ $\qquad$ $f(2) = f(2)!$

$1! = 1$

$f(1)$

$\Rightarrow \quad f(1), f(2) \in \{1, 2\}$

$6 - 1 \mid f(6) - f(1)$ $\quad = 1$ $\quad 5 \mid f(6) - 6$

$6 - 2 \mid f(6) - f(2)$ $\quad = 2$ $\quad 4 \mid f(6) - 6$

$6 - 3 \mid f(6) - f(3)$ $\quad = 3$ $\quad 3 \mid f(6) - 6$

$6 - 4 \mid f(6) - f(4)$ $\quad = 4$ $\quad 2 \mid f(6) - 6$

$6 - 5 \mid$

$(n+1)! - n! \mid f((n+1)!) - f(n!)$

$= f(n+1)! - f(n)!$

$(n+1)! - n! = n \cdot n!$

$= n!$

Se so $f(n) = n$ trovo

$$n \cdot n! \mid f(n+1)! - n!$$

$$f(n+1)! \equiv n! \pmod{n \cdot n!}$$

$$\Rightarrow f(n+1) < 2n$$

Caso 1: $f(1) = f(2) = 1$

$$2 \mid 2k-2 \mid f(2k) - f(2) \Rightarrow f(2k) \text{ dispari}$$

$$\| \; 1$$

$$2 \mid (2k+1) - 1 \mid f(2k+1) - f(1) \Rightarrow f(2k+1) \text{ dispari}$$

Se $f(n) > 1 \Rightarrow f(n!) = f(n)!$ pari, assurdo

f è la costante 1

Caso 2: $f(1) = 2$, $f(2) = 1$

$f(2k)$ dispari,

$$(\text{mod } 2) \quad 1 \equiv f(6) = f(3)! \Rightarrow f(3) = 1$$

$$3 - 1 \mid f(3) - f(1) \quad \text{assurdo}$$

Caso 3: $f(1) = 1$, $f(2) = 2$

Per induz: $f(n) = n$.

$n \cdot n! \mid f(n+1)! - \underbrace{f(n)!}_{n!}$

$\Rightarrow \quad f(n+1) < 2n$

e $\quad (n+1) - 1 \mid f(n+1) - f(1)$

$n \mid f(n+1) - 1$

Quindi $f(n+1) \in \{1, n+1\}$, $f(n+1) = 1$

trovo un assurdo $\Rightarrow$ finisco per induz.

Caso $f(1) = f(2) = 2$ Induzione facile

dice $f(n) = 2 \quad \forall n$

Pb.2 $P(X)$ NON COSTANTE A COEFF. INTERI

$$\begin{cases} a_0 = n \text{ INTERO POSITIVO} \\ a_{k+1} = P(a_k) \quad \text{PER } k \geq 0 \end{cases}$$

$\forall b$ INTERO POSITIVO $\exists k$, $\exists n > 1$ INT. POS.

t.c. $a_k = n^b$

$\Longrightarrow$ $P(X)$ HA GRADO 1

i) Se $\deg P(x) \geq 2$, x, $P(x)$, $P(P(x))$, $P(P(P(x)))$ ...

VALE SEMPRE CHE ESISTE C t.c.

SE $|x| > C \longrightarrow |P(x)| > \frac{1}{2}|x|^2$

PER hp. $\exists\, a_k$ t.c. $|a_k| > c$

BASTA SCEGLIERE b t.c. $2^b > c$

ii) SE $P(x)$ È MONICO

$$P(x) = x^d + Q(x)$$

$$\deg Q(x) \leq d-1$$

SE ESISTONO INFINITI INTERI m t.c.

$P(m)$ È UNA POTENZA d-ESIMA

$$\Longrightarrow P(x) = R(x)^q$$

BASTA SCEGLIERE $b = d, 2d, 3d, 4d, \dots$

TROVIAMO INFINITI k t.c. $P(a_k)$ È UNA POTENZA d-ESIMA

iii) GUARDARE MODULO p^m.

SE PRENDIAMO $b = \phi(p^m)$

SE $(z,p) = 1 \rightarrow z^{\phi(p^m)} \equiv 1 \ (p^m)$

SE $(z,p) \neq 1 \rightarrow z^{\phi(p^m)} \equiv 0 \ (p^m)$

$\phi(p^m) \geq m$

$b = \phi(p^m), 2\phi(p^m), 3\phi(p^m), \dots$

iv) RAGIONIAMO MODULO p^m

$n \xrightarrow{P} a_1 \xrightarrow{P} a_2 \xrightarrow{P} a_3 \rightarrow \dots \rightarrow a_k \xrightarrow{P}$

$n = a_0$

$a_k \equiv 0,1 \ (p^m)$

CHI È?

$a_{k+1} \xrightarrow{P} a_{k+2}$

$a_k \equiv a_{k+1} \pmod{p^m}$ $\left(\text{NON NEC. CON } a_k \equiv 0,1 \pmod{p^n}\right)$

$\downarrow$

$P(a_k) \equiv P(a_{k+1}) \pmod{p^m}$

$\downarrow$

$a_{k+1} \equiv a_{k+2} \pmod{p^n}$

$p^m \mid a_{k+1} - a_k \rightarrow p^m \mid a_{k+2} - a_{k+1}$

SE $p^m \mid a_{k+1} - a_k$ QUANTO PUÒ VALERE

$a_k \pmod{p^m}$!

$\equiv 0,1 \pmod{p^m}$

$a_1, a_2, \dots, a_k \equiv a_{k+1} \equiv a_{k+2} \equiv \dots \equiv a_j \equiv \dots \pmod{p^m}$

VOI SAPPIAMO CHE INFINITI a_j SONO $\equiv 0,1 \pmod{p^m}$

$p^m \mid a_{k+n} - a_k \rightsquigarrow a_k \equiv 0,1 \ (p^m)$

$p^m \mid a_{k+1} - a_k \longrightarrow p^m \mid a_k^2 - a_k$

$p^m \mid P(a_k) - a_k \rightarrow p^m \mid a_k^2 - a_k$

$\Downarrow$

$P(a_k) - a_k \mid a_k^2 - a_k$

$\forall k \geq 0$

v) IDEA: $P(n) - n \mid n^2 - n$ PER INFINITI INTERI $n \Longrightarrow P(x) - x \mid x^2 - x$ COME POLINOMIO

(VERA SE $P(x) - x$ È MONICO, MA IN GENERALE "QUASI VERA")

ESISTE UN INTERO POSITIVO L T.C.

$P(x) - x \mid L(x^2 - x)$

$P(n) - n \mid n^2 - n$ PER INFINITI INTERI

- deg $P(x) \geq 3$:

$$|P(n) - n| \geq \frac{1}{2}|n|^3 > |n^2 - n|$$

$\forall\, n$ t.c. $|n| > C_1$

- deg $P(x) = 2$
  - SE $P(x) = ax^2 + bx + c$ CON $|a| \geq 2$ $\forall\, n$ t.c. $|n| > C_2$

$$\rightarrow |P(n) - n| \geq \frac{3}{2}|n|^2 > |n^2 - n|$$

  - $a = 1$

$x^2 + (b-1)x + c \mid x^2 - x \longrightarrow x^2 + (b-1)x + c \mid bx + c$

(PER INFINITE SCELTE DI x)

$\rightsquigarrow \quad b=0, \ c=0$ $\qquad P(x)=x^2$ ①

- $d=-1$

$-x^2+(b-1)x+c \,|\, x^2-x \rightarrow -x^2+(b-1)x+c$ |

(PER ∞ SCELTE DI x) $\qquad (b-2)x+c$

$\rightsquigarrow \quad b=2, \ c=0$ $\qquad P(x)=-x^2+2x$ ②

① SI ESCLUDE NOTANDO CHE SE n NON È UNA POTENZA d-ESIMA CON d DISPARI NESSUN P_K LO SARÀ

② PRENDENDO $b=2, 4, \dots$

N3) $x^3+y^3+z^3-3xyz =$

$= (x+y+z)\left((x-y)^2+(y-z)^2+(z-x)^2\right)\cdot\frac{1}{2}$

$\theta=\sqrt[3]{q}, \quad A=\{n\theta\}, \quad B=\{n\theta^2\}$

$x_0=nq, \quad y_0=\lfloor n\theta^2 \rfloor \theta, \quad z_0=\lfloor n\theta \rfloor \theta^2$

$=nq-B\theta \qquad =nq-A\theta^2$

$LHS = n^3q^3 + L\zeta^3\theta^3 + L\zeta^3\theta^6 - 3nqL\zeta\theta L\zeta\theta^2 \in \mathbb{Z}$

perché $\theta^3 = q \in \mathbb{Z}$

e inoltre $\left.\begin{array}{l} LHS > 0 \\ LHS \in \mathbb{Z} \end{array}\right\} \Rightarrow LHS \geq 1$ ✳

$$2 \leq (3nq - B\theta - A\theta^2)\cdot\left((B\theta)^2 + (A\theta^2)^2 + (B\theta - A\theta^2)^2\right)$$

$$\leq 3nq \cdot 2\left(B\theta + A\theta^2\right)^2 = 3nq \cdot 2\theta^4\left(\frac{B}{\theta} + A\right)^2$$

$$\leq 6nq^{17/3}(A+B)^2$$

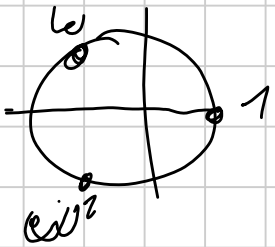
$$A + B \geq \sqrt{\frac{2}{6nq^{17/3}}} = \sqrt{\frac{1}{3q^{17/3}}} \cdot n^{-\frac{1}{2}}$$

✳

$$(a + \sqrt{d}b)(a - \sqrt{d}b) = a^2 - db^2 = \prod_{\theta \in \{\pm\sqrt{d}\}}(a + \theta b)$$

$$x^3 + y^3 + z^3 - 3xyz = (x+y+z)(x+\omega y+\omega^2 z)(x+\omega^2 y+\omega z)$$

$\omega = e^{\frac{2\pi i}{3}}$



$q \in \mathbb{Z}$ $\quad \sqrt[3]{q}, \ \omega\sqrt[3]{q}, \ \omega^2\sqrt[3]{q}$

$$\prod\left(a + b\theta + c\theta^2\right) = a^3 + qb^3 + q^2c^3 - 3qabc$$

$\theta \in \{\sqrt[3]{q}, \omega\sqrt[3]{q}, \omega^2\sqrt[3]{q}\}$

✳