WC 2019 Teoria dei Numeri

Note Title 1/27/2019

PROBLEMA N4

$X \in \mathbb{Q} \longrightarrow$ ESISTE UNA SEQUENZA $X_0, X_1, X_2, \dots$ TALE CHE:

$X_0 = X$

$X_n = 2X_{n-1}$ o $X_n = 2X_{n-1} + \frac{1}{n}$ $\forall n \geq 1$

$\exists\, n \geq 1$ t.c. X_n È INTERO

SE NOI ABBIAMO $\frac{a}{b}$:

STRATEGIA: "DIMINUIRE" b (IN QUALCHE SENSO)

$\frac{a}{b} \nearrow \frac{2a}{b}$

$\frac{a}{b} \searrow \frac{2a}{b} + \frac{1}{n} = \frac{2an + b}{bn}$ → BISOGNA SCEGLIERE n GIUSTO

$$\frac{a}{b} = x_n$$

$$x_{n+k} = \frac{a \cdot 2^k}{b}$$

ALTRA OSSERVAZIONE (OVVIA): A UN CERTO PUNTO b DIVENTERÀ DISPARI.

CONSEGUENZA: SE b È UNA POTENZA DI 2 HO FINITO.

INDUZIONE: SUL PIÙ GRANDE FATTORE PRIMO DI b (CON MOLTEPLICITÀ).

SUPPONIAMO DI SAPERE CHE SE:

$$b = m \cdot p^k \quad \text{CON}$$

$p >$ QUALSIASI PRIMO CHE DIVIDE m

LA TESI È VERA PER OGNI $X = \frac{c}{d}$ CON

$d = \tilde{m} \cdot p^j$ CON $j < k$ E $\tilde{m}$ CON

PRIMI MINORI DI p.

SCRITTA COSÌ NON BASTA:

BISOGNA ASSUMERE CHE QUESTO PER OGNI PUNTO DI PARTENZA:

NON PIÙ $X_0 = x$, MA $X_n = x$

PASSO BASE:

$$p = 2 \rightarrow X_n = \frac{a}{2^k} \Longrightarrow \text{FINE}$$

PASSO INDUTTIVO:

$$X_n = \frac{a}{b} \quad \text{CON} \quad b = m \cdot p^k$$

CON FATTORI PRIMI DI $m < p$

$$X_{n+j} = \frac{2^j a}{b}$$

ALLA PRIMA MOSSA DEL II TIPO, ABBIAMO:

$$X_{n+r} = \frac{2^r \cdot a}{b} + \frac{1}{n+r} =$$

$$= \frac{(n+r)\cdot 2^r \cdot a + b}{b(n+r)} = \frac{(n+r)\cdot 2^r \cdot a + m \cdot p^k}{m \cdot p^k \cdot (n+r)}$$

VORREMMO $n+r$ DELLA FORMA ADEGUATA:

$$\frac{1}{p^k m} + \frac{1}{n} = \frac{c}{p^{k-1} d} \qquad \text{con } (d,p)=1$$

DOBBIAMO SCEGLIERE $n = p^k \cdot J$ con $(J,p)=1$

$$n+r = p^k \cdot s$$

$$\frac{\cancel{p^k} \cdot s \cdot 2^{(p^k \cdot s - n)} \cdot a + m \cdot \cancel{p^k}}{m \cdot p^k \cdot \cancel{p^k} \cdot s} =$$

$$\equiv \frac{m + a \cdot 5 \cdot 2^{(p^k \cdot 5 - n)}}{m \cdot p^k \cdot 5}$$

VOGLIAMO:

- 5 NON ABBIA FATTORI PRIMI $\geq p$
- $m + a \cdot 5 \cdot 2^{(p^k \cdot 5 - n)} \equiv 0 \ (p)$

$5 = (p-1) \cdot t$ ✓

$$m + a \cdot (p-1) \cdot t \cdot 2^{(t(p-1)p^k - n)} \equiv$$

$$m - at \cdot 2^{-n} \ (p)$$

SCELGO t TALE CHE

$$m - at \cdot 2^{-n} \equiv 0 \ (p)$$

QUESTO È POSSIBILE QUANDO:

- $m \not\equiv 0 \ (p)$ ✓
- $2 \not\equiv 0 \ (p)$ ✓ $p > 2$
- $a \not\equiv 0 \ (p)$ ✓ $(a, b) = 1$

TROVIAMO t T.C. $t \equiv T \ (p)$

CON $0 < T < p$ CHE SODDISFA

LA CONGRUENZA.

DOBBIAMO DIRE CHE IL t CHE SCEGLIAMO

PUÒ ESSERE ARBITRARIAMENTE GRANDE.

SE TROVIAMO t ANCHE $t \cdot 2^{p-1}$ FUNZIONA.

ESISTE UN t ARBITRARIAMENTE GRANDE.

N5 $a_1, a_2, \dots, a_K$ SONO LE POTENZE DI a MODULO p, SE SOLO ANCHE UNA PROGRESSIONE ARITMETICA (IN QUALCHE ORDINE) MODULO p

σ PERMUTAZIONE DI $\{1, \dots, K\}$:

$\exists a, b$ t.c. $a + ib \equiv a_{\sigma(i)} \pmod p$

$\forall\ 1 \le i \le K$

ALLORA $K = p-1$ (CIOÈ I RESIDUI SONO TUTTI $\iff$ a È UN GENERATORE)

$a \neq 1, -1 \iff K > 2$

$a_1 = 1$ $\qquad$ $a_1 = 1$ $\quad a_2 = -1$

PER LIBERARSI DELL'ORDINE DEGLI a_i, CONSIDERIAMO LE SOMME SIMMETRICHE A LORO ASSOCIATE.

AD ESEMPIO:

a, b, c:

$$a+b+c$$
$$ab+ac+bc$$
$$abc$$

FUNZIONI SIMM. ELEMENTARI

COEFF. DI $(x-a)(x-b)(x-c)$

(SEGNI ALTERNI)

SE $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ CON $|A| = |B| = k$

ALLORA $A = B \iff$ LE k SOMME SIMMETRICHE ELEMENTARI (NEI LORO ELEMENTI) COINCIDONO

$$\prod_{a \in A} (x-a) \equiv \prod_{b \in B} (x-b) \quad (p)$$

SE $x < p$ LO STESSO RISULTATO SI PUÒ DIRE CON LE POTENZE SIMMETRICHE (SOMME DI NEWTON):

a, b, c: $a+b+c$

$a^2+b^2+c^2$

$a^3+b^3+c^3$

...

VALE LO STESSO RISULTATO DI PRIMA (SE $x < p$) CON LE POTENZE SIMMETRICHE.

SE $a_1, a_2, \dots, a_k$ SONO LE POTENZE DI a, ALLORA:

$$\prod_{i=1}^{k} (X - a_i) \equiv X^k - 1 \ (p)$$

CON $k \mid p-1$, $k > 2$

$$\sum_{i=1}^{k} a_i \equiv 0 \ (p)$$

a_i RADICI DI $X^n - cX^{n-1} + \dots$

$$\sum_{i=1}^{n} a_i = c$$

(ANCHE MODULO p)

È LO SVILUPPO DEL PRODOTTO

IL SECONDO TERMINE ($K > 2$):

$$0 \equiv \sum_{i<j} a_i a_j \quad (p)$$

$$\sum a_i^2 + \sum_{i \neq j} a_i a_j \qquad 2\sum_{i<j} a_i a_j$$

$$\frac{\left(\sum a_i\right)^2 - \left(\sum a_i^2\right)}{2} \;\|\; \frac{-\sum a_i^2}{2}$$

$$\sum_{i=1}^{K} a_i^2 \equiv 0 \quad (p)$$

TUTTE LE FUNZIONI SIMMETRICHE DI GRADO $\leq n$ SI SCRIVONO COME SOMME E PRODOTTI DELLE FUNZIONI SIMMETRICHE ELEMENTARI DI GRADO $\leq n$

$$z_i = a + ib \quad \text{con} \quad a, b \in \mathbb{Z}/p\mathbb{Z}$$

$$b \not\equiv 0 \ (p)$$

$$0 \equiv \sum_{i=1}^{k} (a + ib) \equiv ka + \frac{k(k+1)}{2} b \ (p)$$

$$0 \equiv \sum_{i=1}^{k} (a + ib)^2 \equiv \sum_{i=1}^{k} a^2 + 2ab \cdot i + b^2 \cdot i^2 \equiv$$

$$\equiv k a^2 + 2ab \cdot \frac{k(k+1)}{2} + b^2 \cdot \frac{k(k+1)(2k+1)}{6} \ (p)$$

$$\equiv 0$$

$$ka + \frac{k(k+1)}{2} b \equiv 0 \ (p) \qquad 3 \le k \le p-1$$

$$a \equiv -b \cdot \frac{(k+1)}{2} \ (p)$$

$$b^2 \left(\frac{(k+1)^2}{4} - \frac{(k+1)^2}{2} + \frac{(k+1)(2k+1)}{6} \right) \equiv 0 \ (p)$$

$$b \not\equiv 0 \ (p)$$

$$-3(k+1)^2 + 2(k+1)(2k+1) \equiv 0 \ (p)$$

$$(k+1)(4k+2-3k-3) \equiv 0 \ (p)$$

$$(k+1)(k-1) \equiv 0 \ (p)$$

- $k \equiv 1 \ (p) \rightarrow k = 1$ CONTRO LE IPOTESI
- $k \equiv -1 \ (p) \rightarrow k = p-1$

N6. $k > 2$

$$\begin{cases} a_1 = 1 \\ a_2 = k \\ a_{n+1} = (k+1)\,a_n - a_{n-1} \end{cases}$$

$$\rightsquigarrow \quad t^2 - (k+1)t + 1 = 0$$

Radici: $\dfrac{k+1 \pm \sqrt{k^2+2k-3}}{2}$

Per $k = 2$ $\quad 1 \quad 2 \quad 5 \quad 13 \quad 34$

$\quad\quad\quad 1 \quad 3 \quad 8 \quad 21$

Radici: $\dfrac{3 \pm \sqrt{5}}{2} = \left(\dfrac{1 \pm \sqrt{5}}{2}\right)^2$

$$\frac{2k+2 \pm 2\sqrt{(k+3)(k-1)}}{4} = \left(\frac{\sqrt{k+3} \pm \sqrt{k-1}}{2}\right)^2$$

α, β

$\alpha \cdot \beta = 1$

$$a_n = c_1 \cdot \alpha^{2n} + c_2 \cdot \beta^{2n}$$

$$\begin{cases} a_0 = 1 \\ a_1 = 1 \end{cases} \qquad \left(\begin{array}{l} a_2 = (k+1)\,a_1 - a_0 \\ k = (k+1) \cdot 1 - a_0 \end{array} \right)$$

$$\begin{cases} c_1 + c_2 = 1 \\ c_1\alpha^2 + c_2\beta^2 = 1 \end{cases} \qquad c_2 = \frac{\alpha^2 - 1}{\alpha^2 - \beta^2} = \frac{\alpha^2 - \alpha\beta}{(\alpha-\beta)(\alpha+\beta)}$$

$$= \frac{\alpha}{\alpha+\beta}$$

$$c_1 = \frac{\beta}{\alpha+\beta}$$

$$a_n = \frac{\beta \cdot \alpha^{2n}}{\alpha+\beta} + \frac{\alpha \cdot \beta^{2n}}{\alpha+\beta} = \boxed{\frac{\alpha^{2n-1} + \beta^{2n-1}}{\alpha+\beta}}$$

$$a_3 = k^2 + k - 1 \equiv -1 \ (k)$$

$$a_4 = k^3 + 2k^2 - k - 1 \equiv -1 \ (k)$$

Consideriamo a_n mod k:

$$1, 0, -1, -1, 0, 1, 1, 0, -1, -1, 0, \dots$$

$$\uparrow \quad \uparrow \quad \uparrow$$

$$2 \quad 5 \quad 8$$

$$n \equiv 2 \pmod 3$$

Se $d \mid 2n-1$

$$\frac{\alpha^d + \beta^d}{\alpha+\beta} \cdot \left| \frac{\alpha^{2n-1} + \beta^{2n-1}}{\alpha+\beta} \right.$$

Rapporto: $$\frac{\alpha^{2n-1} + \beta^{2n-1}}{\alpha^d + \beta^d} = \alpha^{d(r-1)} - \alpha^{d(r-2)} \cdot \beta^d + \dots + \beta^{d(r-1)}$$

$$r := \frac{2n-1}{d}$$

LEMMA $d \mid 2n-1 \Rightarrow a_{\frac{d+1}{2}} \mid a_n$

Sia $p \mid 2n-1$. Allora $a_{\frac{p+1}{2}} \mid a_n$, e se $a_n = k^m$, allora $a_{\frac{p+1}{2}} \mid k^m$.

Se $\frac{p+1}{2} \not\equiv 2 \,(3)$, allora $\left(a_{\frac{p+1}{2}}, k\right) = 1$, assurdo.

Se $\frac{p+1}{2} \equiv 2 \,(3) \Rightarrow p \equiv 3 \,(3) \Rightarrow p = 3$

Siccome questo vale $\forall p$ che divide $2n-1$

$\Rightarrow 2n-1 = 3^a$

- $a = 1 \Rightarrow n = 2$ ovvio
- $a \geq 2 \Rightarrow 9 \mid 2n-1 \Rightarrow a_{\frac{9+1}{2}} \mid a_n$

$a_5 = k\underbrace{\left(k^3 + 2k^2 - 3\right)}_{\geq 13} \Rightarrow$ c'è un primo che divide a_5 ma non k, assurdo

$\underbrace{\left(\cdot, k\right) = 3}_{}$

DIM LEMMA • $\alpha^{2n} + \beta^{2n}$ è intero $\forall n$

$$\alpha^{2n+2} + \beta^{2n+2} = (\alpha^2 + \beta^2)(\alpha^{2n} + \beta^{2n}) - (\alpha^{2n-2} + \beta^{2n-2})$$

• $$\frac{\alpha^9 + \beta^9}{\alpha^3 + \beta^3} = \alpha^6 - \alpha^3\beta^3 + \beta^6$$

$$\frac{\alpha^{2n-1} + \beta^{2n-1}}{\alpha^d + \beta^d} = \text{combinazione di } (\alpha^{\text{pari}} + \beta^{\text{pari}})$$

□