WC 2008 – Teoria dei Numeri

Titolo nota 23/01/2008

5. $$n^5 + n^4 + 1 = 7^m$$ SOL.: $n = 2$ $m = 2$

1. Certe volte si fattorizza!!

$$(n^2+n+1)(n^3-n+1) = 7^m$$

$$n^2+n+1 = 7^a \qquad n^3-n+1 = 7^b$$

Si esclude che $a=0$ oppure $b=0$

$$n^2+n = 7^a - 1 \qquad n(n+1) = 7^a - 1$$

$$n^3-n = 7^b - 1 \qquad n(n^2-1) = 7^b - 1$$

$$\underbrace{n(n+1)}_{7^a-1}(n-1) = 7^b - 1$$

$$\Rightarrow 7^a - 1 \mid 7^b - 1$$

2. $\boxed{\underline{\text{Lemma}} \quad 7^a - 1 \mid 7^b - 1 \Rightarrow a \mid b}$

Anche tra polinomi

Dim. $b = qa + r$

$$7^b - 1 = 7^{qa+r} - 1 = 7^{qa+r} - 7^r + 7^r - 1$$

$$= 7^r (7^{qa} - 1) + 7^r - 1$$

$$= 7^r (7^a - 1) \cdot \text{roba} + 7^r - 1$$

Poiché $7^a - 1 \mid 7^b - 1$, deve essere $7^a - 1 \mid 7^r - 1$

NO perchè il secondo è + piccolo (a meno che $r = 0$, ma allora $a \mid b$)

Ora $b = ka$

$$n^2+u+1 = 7^a$$

$$\underbrace{u^3-u+1}_{\text{LHS}} = 7^b = 7^{ka} = \underbrace{(u^2+u+1)^k}_{\text{RHS}}$$

$k=1$ si tratta a mano

Hope: fare il conto

Se $k \geq 2$, allora $(u^2+u+1)^k \geq (u^2+u+1)^2 > u^3-u+1$

Uso di disuguaglianze

<u>Oss. generale</u>: sole congruenze $\rightarrow$ difficile dimostrare che ci sono solo alcune soluzioni

PROBLEMA 6

Lemma 1

p primo, $a_1, \dots, a_p$ sist. fond. di residui (tutte le classi)

k esponente $\leq p-2$. (anche $k=0$)

Allora $a_1^k + a_2^k + \dots + a_p^k \equiv 0 \quad (p)$

Vale anche: • se considero solo classi prime con p
• vale anche per tutti i k t.c. $(p-1) \nmid k$

Idea della dim.: escludo la classe 0 modulo p, le altre sono potenze del generatore

$$\{a_1, \dots, a_{p-1}\} = \{1, g^1, g^2, \dots, g^{p-2}\}$$

$$\Rightarrow \quad a_1^k + \dots + a_{p-2}^k = 1 + g^k + g^{2k} + \dots + g^{(p-2)k}$$

geometrica $\rightarrow$ $= \dfrac{(g^k)^{p-1} - 1}{g^k - 1}$ $\leftarrow$ p divide questo (FLT)

$\leftarrow$ p non divide questo (k NO MULTIPLO di p−1)

— o — o —

$\boxed{\underline{\text{Lemma 2}}}$ Se $p(x)$ è un pol. a coeff. interi di grado $\leq p-2$ e $a_1, \dots, a_p$ sono tutti i residui modulo p, allora

$$p(a_1) + p(a_2) + \dots + p(a_p) \equiv 0 \quad (p)$$

__Dim.__ Applico Lemma 1 a tutti i monomi che compongono $p(x)$ (basta che non ci siano monomi di grado multiplo di $p-1$)

Oss. $a_1^{p-1} + a_2^{p-1} + \dots + a_p^{p-1}$ (o esponente multiplo di $p-1$)

↳ TUTTI UNI TRANNE UNO!

$\equiv p-1 \quad (p).$

— o — o —

$\sum_{j=0}^{n} \binom{n}{j}^4$ divisibile per i $p \in \left(n, \frac{4n+2}{3}\right]$

$n = p-1 \leadsto$ si vede bene, ma...

$n = p-2 \leadsto$ si vede bene che funziona

$n = p-3 \qquad \binom{n}{j} = \binom{p-3}{j} = (p-3)(p-4$

$$\binom{p-3}{0} = 1 \qquad \binom{p-3}{1} = p-3 \equiv -3$$

$$\binom{p-3}{2} = \frac{(p-3)(p-4)}{2} \equiv \frac{3\cdot 4}{2}$$

$$\binom{p-3}{3} = \frac{(p-3)(p-4)(p-5)}{2\cdot 3} \equiv (\pm 1)\,\frac{\cancel{3}\cdot 4\cdot 5}{2\cdot \cancel{3}} = \pm\,\frac{4\cdot 5}{2}$$

$$\boxed{\binom{p-3}{4} = \frac{(p-3)(p-4)(p-5)(p-6)}{2\cdot 3\cdot 4} \equiv (\pm 1)\,\frac{\cancel{3}\cdot \cancel{4}\cdot 5\cdot 6}{2\cdot \cancel{3}\cdot \cancel{4}} = \pm\,\frac{5\cdot 6}{2}}$$

$\vdots$

$$\binom{p-3}{J} = \pm\,\frac{(J+1)(J+2)}{2}$$

$$\sum_{J=0}^{p-3} (\pm)^4\,\frac{(J+1)^4(J+2)^4}{2^4} = \sum_{J=0}^{p-3} P(J)$$

Per applicare il Lemma 2 dovrei sommare fino a $J = p-1$

FORTUNA: i 2 termini mancanti sono $\equiv 0 \ (p)$

$$\sum_{J=0}^{p-3} \binom{p-3}{J}^4 \equiv \sum_{J=0}^{p-3} P(J) \equiv \sum_{J=0}^{p-1} P(J) \equiv 0$$

Lemma 2

se $\deg(P) \leq p-2$

In generale se $n = p-k$

$$\binom{p-k}{J} \equiv \pm \frac{(J+1)(J+2)\cdots(J+k-1)}{(k-1)!} \qquad \binom{k+J-1}{J} = \binom{k+J-1}{k-1}$$

$$\binom{p-k}{J} = \frac{(p-k)(p-k-1)\cdots(p-k-J+1)}{1\cdot 2\cdot\ldots\cdot J} \equiv \pm \frac{k(k+1)\cdots(k+J-1)}{J!}$$

$$\sum_{j=0}^{p-k} \binom{n}{j}^4 \equiv \sum_{j=0}^{p-k} P(j) \equiv \sum_{j=0}^{p-1} P(j) \equiv 0 \quad (p)$$

se $\deg P \leq p-2$

$$\deg P = 4(k-1) \leq p-2 \qquad p-k=n \qquad k=p-n$$

$$4(p-n-1) \leq p-2 \qquad 4p-4n-4 \leq p-2$$

$$3p \leq 4n+2$$

Col il 2008 è tutto uguale fino a

$$2008(p-n-1) \leq p-2 \rightsquigarrow 2007p \leq 2008n + 2006$$

Vanno bene tutti: $p \in \left(n, \underbrace{\frac{2008n+2006}{2007}}_{kn}\right)$

ESERCIZIO 4

<u>Lemma 2</u> $a \geq 2$ intero, p primo dispari

Allora a^p+1 ha un fattore primo che

$(a+1)$ non ha

TRANNE il caso $a=2$ $p=3$ $a+1=3$
$a^3+1=9$

<u>Lemma 3</u> $a \geq 2$ intero, n intero (dispari) con un fattore dispari

Allora a^n+1 ha un fattore primo che $(a+1)$ non ha
(tranne ...)

<u>Dim</u> $n = d \cdot k$ $\quad a^n+1 = (a^k)^d+1 =$

dispari e primo

$a^{kd}+1$ è del tipo $(a^k)^d+1$, quindi ha un fattore nuovo rispetto a a^k+1, il quale a sua volta ha tutti i fattori di $a+1$ (k dispari)

— o — o —

a^m+1 divide $(a+1)^n$

Se m è dispari è impossibile (tranne ...)
Tutto si riduce a dimostrare che m è dispari.

$\boxed{1^\circ \text{ caso}}$ a^m+1 ha un fattore primo p dispari

$\Rightarrow a^m+1 \equiv 0 \ (p) \Rightarrow p \mid (a+1)^n \Rightarrow p \mid a+1$

$\Rightarrow a \equiv -1 \ (p) \Rightarrow a^m+1 \equiv (-1)^m+1$

Se m è pari questo è $\equiv 2 \ (p)$, quindi $\not\equiv 0$

$\boxed{2^o \text{ caso}}$ $a^m+1 = 2^k$ IMPOSSIBILE

$k=1$ si fa a mano

Se $k \geq 2$ $\rightarrow$ RHS $\equiv 0$ (4)
Se m è pari LHS $\equiv 1, 2$ (4) $\Rightarrow$ m è dispari

Con poca fatica si vede che $a^m+1=2^k$ non ha soluzioni

— o — o —

Lemma 1 Considerianno $\frac{a^p+1}{a+1}$ e $a+1$

Quali fattori primi possono avere in comune? SOLO p

$$(a^p+1) = \underbrace{(a+1)}\underbrace{(a^{p-1}-a^{p-2}+\dots-a+1)}$$

L'unico fattore comune è al + p

$$\boxed{\text{Se } \frac{a^p+1}{a+1} \text{ è divisibile per } p, \text{ allora } \frac{a^p+1}{a+1} \equiv p \pmod{p^2}}$$

Idea di Dim. Lemma 2 a partire da Lemma 1

Tutti i primi in comune hanno esponente 1 in quello che dovrebbe essere il fattore + grande.

$$MCD\left(a+1, \frac{a^p+1}{a+1}\right) \text{ divide sempre } p$$

perchè il MCD tra i polinomi è p

$$q \mid a+1 \implies a \equiv -1 \ (q)$$

$$a^{p-1} - a^{p-2} + a^{p-3} + \dots - a + 1 \equiv 1 + 1 + \dots + 1 \equiv p \ (q)$$